Microsoft

Informe de defensa digital de Microsoft 2022

Aportar luz al panorama de las amenazas y permitir una defensa digital.

Índice

Los datos, las ideas y los acontecimientos recogidos en este informe abarcan desde julio de 2021 hasta junio de 2022 (año fiscal 2022 de Microsoft), a menos que se indique lo contrario.

Para obtener la mejor experiencia al ver y desplazarte por este informe, te recomendamos que utilices Adobe Reader, disponible como descarga gratuita en el sitio web de Adobe.

Introducción de Tom Burt

Vicepresidente corporativo, seguridad y confianza de los clientes

«Los billones de señales que analizamos de nuestro ecosistema mundial de productos y servicios revelan la ferocidad, el alcance y la escala de las amenazas digitales en todo el mundo».

Una instantánea de nuestro panorama...

Alcance y escala del panorama de amenazas

El volumen de ataques de contraseña ha aumentado a unos 921 ataques cada segundo, lo que supone un aumento del 74 % en solo un año.

Desmantelar la ciberdelincuencia

Hasta la fecha, Microsoft ha retirado más de 10 000 dominios utilizados por ciberdelincuentes y 600 utilizados por actores estado nación

Abordar las vulnerabilidades

El 93 % de nuestras actuaciones de respuesta a incidentes de ransomware revelaron que los controles de acceso con privilegios y movimiento lateral son insuficientes.

El 23 de febrero de 2022, el mundo de la ciberseguridad entró en una nueva era, la era de la guerra híbrida. Ese día, horas antes de que se lanzasen misiles y se desplegaran los tanques en las fronteras, agentes rusos lanzaron un ciberataque destructivo masivo contra objetivos del gobierno y sectores tecnológicos y financieros de Ucrania. Puedes obtener más información sobre estos ataques y las lecciones que se pueden aprender de ellos en el capítulo Amenazas de los estados nación de esta tercera edición anual del Informe de defensa digital de Microsoft (MDDR). Un aspecto clave de esas lecciones es que el cloud proporciona la mejor seguridad física y lógica contra los ciberataques, y permite avances en la inteligencia de amenazas y la protección de puntos de conexión que han demostrado ser sumamente valiosos en Ucrania.

Aunque cualquier estudio sobre los avances anuales en ciberseguridad debe comenzar ahí, el informe de este año proporciona un análisis detallado de muchos otros aspectos. En el primer capítulo del informe, nos centraremos en las actividades de los ciberdelincuentes, seguidas de las amenazas de los Estados nación que abordaremos en el segundo capítulo. Ambos grupos han aumentado considerablemente la sofisticación de sus ataques, lo que ha supuesto un aumento drástico de las consecuencias de sus acciones. Mientras que Rusia acaparaba los titulares, agentes iraníes escalaron sus ataques tras un cambio del poder presidencial, lanzando ataques destructivos contra Israel y operaciones de ransomware y de robo y filtración de datos («hack-and-leak») dirigidos a infraestructuras críticas de los Estados Unidos. China también aumentó sus iniciativas de espionaje en el Sudeste Asiático y en otros países meridionales con el objeto de contrarrestar la influencia de los Estados Unidos y robar datos e información críticos.

Agentes extranjeros también están utilizando técnicas muy eficaces para permitir operaciones de influencia propagandística en regiones de todo el mundo, como veremos en el tercer capítulo. Por ejemplo, Rusia ha realizado un importante esfuerzo para convencer a sus ciudadanos, y a los ciudadanos de muchos otros países, de que su invasión de Ucrania estaba justificada, al tiempo que ha desacreditado las vacunas de COVID de Occidente y ha promovido la eficacia de las suyas. Asimismo, los agentes dirigen cada vez más sus ataques a los dispositivos del Internet de las cosas (IoT) o a los dispositivos de tecnología de las operaciones (OT) como puntos de entrada a las redes e infraestructuras críticas, como se explica en el cuarto capítulo. Finalmente, en el último capítulo, proporcionamos los conocimientos y las lecciones que hemos aprendido durante el último año para defendernos de los ataques dirigidos a Microsoft y a nuestros clientes mientras revisamos los avances en ciberresiliencia de este año.

En cada capítulo se proporcionan las lecciones y los conocimientos clave aprendidos gracias a la posición estratégica exclusiva de Microsoft. Los billones de señales que analizamos de nuestro ecosistema mundial de productos y servicios revelan la ferocidad, el alcance y la escala de las amenazas digitales en todo el mundo. Microsoft está tomando medidas para defender a nuestros clientes y el ecosistema digital de estas amenazas; puedes obtener información sobre nuestra tecnología que identifica y bloquea miles de millones de intentos de phishing, robos de identidad y otras amenazas dirigidas a nuestros clientes.

Introducción de Tom Burt

Continuación

También utilizamos medios legales y técnicos para incautar y desconectar la infraestructura utilizada por los ciberdelincuentes y agentes de los Estados nación, y notificar a los clientes cuando son amenazados o atacados por un agente de Estados nación. Trabajamos para desarrollar características y servicios cada vez más eficaces que utilicen tecnología de IA/ML para identificar y bloquear las ciberamenazas. y para que los profesionales de seguridad puedan identificar y defenderse de las intrusiones cibernéticas de forma más rápida y eficaz.

Quizás lo más importante es que a lo largo del MDDR ofrecemos nuestros mejores consejos sobre las medidas que pueden emprender las personas, las organizaciones y las empresas para defenderse de estas crecientes amenazas digitales. La adopción de buenas prácticas de higiene cibernética es la mejor defensa y puede reducir considerablemente el riesgo de ciberataques.

El estado de la ciberdelincuencia

Los ciberdelincuentes siguen actuando como empresas con fines de lucro sofisticadas. Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad en la forma y el lugar en el que alojan la infraestructura operativa de sus campañas. Al mismo tiempo, los ciberdelincuentes son cada vez más frugales. Para reducir su carga de trabajo y aumentar la apariencia de legitimidad, los atacantes dirigen sus ataques a redes y dispositivos empresariales para alojar campañas de phishing o malware, o incluso utilizan su capacidad informática para la minería de criptomonedas.

> **Más información en la página 6**

«El uso de armas cibernéticas en la guerra híbrida de Ucrania marca el comienzo de una nueva era de conflictos».

Amenazas de los estados nación

Los agentes de los estados nación están lanzando ciberataques cada vez más sofisticados diseñados para eludir la detección y avanzar en sus prioridades estratégicas. La implementación de ciberamenazas en la guerra híbrida de Ucrania marca el comienzo de una nueva era de conflictos. Rusia también ha apoyado su guerra con operaciones de influencia propagandística, utilizando la tecnología para influir en las opiniones de Rusia, Ucrania y todo el mundo. Fuera de Ucrania, los agentes de los estados nación han aumentado su actividad y han comenzado a utilizar los avances en automatización, infraestructura en el cloud y tecnologías de acceso remoto para atacar a un conjunto más amplio de objetivos. Las cadenas de suministro de TI corporativas que permiten el acceso a objetivos finales han sido atacadas con frecuencia. La higiene de ciberseguridad cobró aún más importancia, ya que los agentes aprovecharon rápidamente las vulnerabilidades sin parches, utilizaron técnicas sofisticadas y de fuerza bruta para robar credenciales y ocultaron sus operaciones mediante el uso de software legítimo o de código abierto. Además, Irán se suma a Rusia en el uso de armas cibernéticas destructivas, incluido el ransomware, como la materia prima de sus ataques.

Estos desarrollos requieren una adopción urgente de un marco global coherente que priorice los derechos humanos y proteja a las personas del comportamiento online irresponsable de los países. Todas las naciones deben trabajar juntas para implantar normas y reglas que establezcan una conducta de estado responsable.

> **Más información en la página 30**

Dispositivos e infraestructura

La pandemia, junto con la rápida adopción de dispositivos con acceso a Internet de todo tipo como una forma de acelerar la transformación digital, ha aumentado enormemente la superficie de ataque de nuestro mundo digital. Como resultado, los ciberdelincuentes y los estados nación están aprovechando rápidamente las ventajas. Aunque la seguridad del hardware y el software de TI se ha reforzado en los últimos años, la seguridad de los dispositivos IoT y OT no ha seguido el mismo ritmo. Los actores de amenazas están atacando estos dispositivos para acceder a las redes y permitir el movimiento lateral, para establecer un punto de apoyo en una cadena de suministro o para interrumpir las operaciones de OT de la organización objetivo.

> **Más información en la página 56**

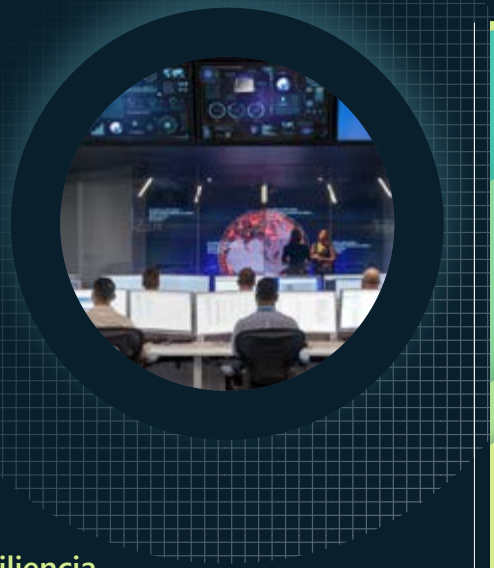
Introducción de Tom Burt

Continuación

Operaciones de ciberinfluencia

Los Estados nación utilizan cada vez más operaciones de influencia sofisticadas para distribuir propaganda e influir en la opinión pública tanto nacional como internacionalmente. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos. Los agentes, expertos manipuladores y concienzudos, utilizan los medios tradicionales junto con Internet y las redes sociales para aumentar enormemente el alcance, la escala y la eficiencia de sus campañas, y su influencia desmedida en el ecosistema de la información global. En el último año, hemos visto cómo estas operaciones se utilizaban como parte de la guerra híbrida de Rusia en Ucrania, pero también hemos visto a Rusia y otras naciones, como China e Irán, desplegar cada vez más operaciones propagandísticas en las redes sociales para ampliar su influencia global en una serie de asuntos.

Más información en la página 71



Ciberresiliencia

La seguridad es un factor clave del éxito tecnológico. La innovación y la mejora de la productividad solo se pueden lograr introduciendo medidas de seguridad que aumenten todo lo posible la resiliencia de las organizaciones a los ataques modernos. La pandemia ha obligado a Microsoft a cambiar las prácticas y tecnologías de seguridad para proteger a nuestros empleados dondequiera que trabajen. Durante este último año, los actores de amenazas continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido gestionar la prevalencia y complejidad de los diversos métodos de ataque y el aumento de la actividad de los estados nación. En este capítulo, analizamos los desafíos a los que nos enfrentamos y las defensas que hemos movilizado en respuesta con nuestros más de 15 000 partners.

Más información en la página 86

Nuestra posición estratégica única

37 000 mill.
de amenazas de correo electrónico bloqueadas

34 700 mill.
de amenazas de identidad bloqueadas

43 tn
de señales sintetizadas todos los días, utilizando sofisticados algoritmos de IA y análisis de datos para conocer las amenazas digitales y la ciberactividad criminal y protegernos de ellas.

Más de 8500
ingenieros, investigadores, científicos de datos, expertos en ciberseguridad, buscadores de amenazas, analistas geopolíticos, investigadores y equipos de respuesta en 77 países.

2500 mill.
de señales de amenazas analizadas diariamente

Más de 15 000
partners en nuestro ecosistema de seguridad que aumentan la ciberresiliencia de nuestros clientes.

Del 1 de julio de 2021 al 30 de junio de 2022

Introducción de Tom Burt

Continuación

Creemos que Microsoft, de forma independiente y a través de estrechas alianzas con otros miembros del sector privado, las administraciones públicas y la sociedad civil, tiene la responsabilidad de proteger los sistemas digitales que sustentan el tejido social de nuestra sociedad y promover entornos informáticos seguros para todas las personas, dondequiera que se encuentren. Esta responsabilidad es la razón por la que publicamos el MDDR cada año desde 2020. El informe es la culminación de la gran cantidad de datos recabados y de la investigación exhaustiva de Microsoft. Este informe ofrece nuestra perspectiva única sobre cómo está evolucionando el panorama de amenazas digitales y las medidas cruciales que se pueden emprender hoy para mejorar la seguridad del ecosistema.

Esperamos inculcar una sensación de urgencia que inste a los lectores a emprender medidas inmediatas a partir de los datos y los conocimientos que presentamos tanto aquí como en nuestras numerosas publicaciones de ciberseguridad a lo largo del año. Al considerar la gravedad de la amenaza para el panorama digital —y su traducción al mundo físico—, es importante recordar que todos estamos capacitados para tomar medidas que nos protejan a nosotros mismos, a nuestras organizaciones y a las empresas de las amenazas digitales.

Gracias por dedicar tiempo a leer el Informe de defensa digital de Microsoft de este año. Esperamos que en él encuentres información y recomendaciones valiosas que nos ayuden a defender colectivamente el ecosistema digital.

Tom Burt
Vicepresidente corporativo,
seguridad y confianza de los clientes

Nuestro objetivo con este informe es doble:

1. Arrojar luz al cambiante panorama de amenazas digitales para nuestros clientes, partners y partes interesadas, que abarcan un ecosistema más amplio, exponiendo los nuevos ciberataques y las tendencias en evolución de las amenazas históricamente persistentes.
2. Capacitar a nuestros clientes y partners para mejorar su ciberresiliencia y responder a estas amenazas.

El estado de la ciberdelincuencia

Los atacantes adaptan sus técnicas al mismo ritmo que se mejoran las defensas cibernéticas y aumenta el número de organizaciones que adoptan un enfoque de prevención proactivo.

Información general del

estado de la ciberdelincuencia

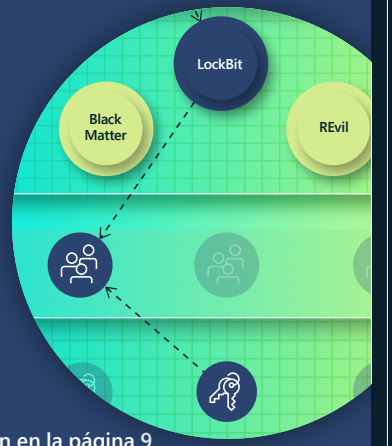
Los atacantes adaptan sus técnicas al mismo ritmo que se mejoran las defensas cibernéticas y aumenta el número de organizaciones que adoptan un enfoque de prevención proactivo.

Los ciberdelincuentes siguen actuando como empresas con fines de lucro sofisticadas. Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad en la forma y el lugar en el que alojan la infraestructura operativa de sus campañas. Al mismo tiempo, los ciberdelincuentes son cada vez más frugales. Para reducir su carga de trabajo y aumentar la apariencia de legitimidad, los atacantes dirigen sus ataques a redes y dispositivos empresariales para alojar campañas de phishing o malware, o incluso utilizan su capacidad informática para la minería de criptomonedas.

La ciberdelincuencia sigue aumentando conforme la industrialización de la economía de la ciberdelincuencia reduce los conocimientos necesarios para perpetrar un ataque gracias a un mayor acceso a las herramientas y la infraestructura.

Más información en la página 18

La amenaza del ransomware y la extorsión es cada vez más audaz con ataques dirigidos a gobiernos, empresas e infraestructuras críticas.

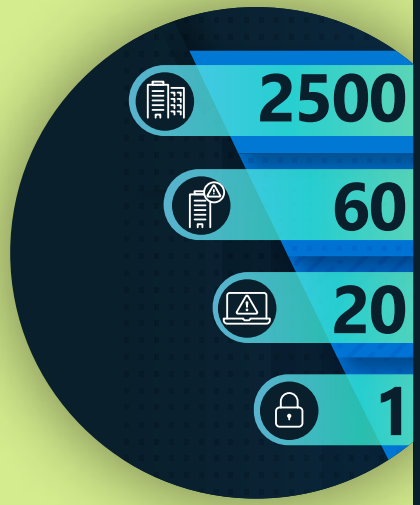


Más información en la página 9

Los atacantes amenazan cada vez más con revelar datos confidenciales para instar al pago del rescate.

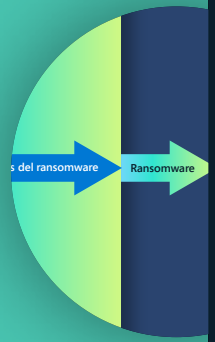
Más información en la página 10

El ransomware operado por humanos es más prevalente, habida cuenta de que un tercio de estos ataques tiene éxito y el 5 % de los objetivos atacados con ransomware paga el rescate.



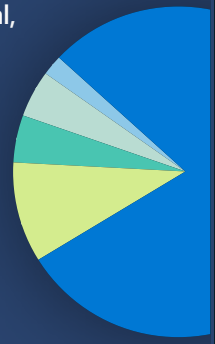
Más información en la página 9

La defensa contra el ransomware más eficaz incluye la autenticación multifactor, parches de seguridad frecuentes y principios de Confianza cero en toda la arquitectura de red.



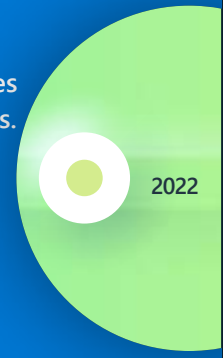
Más información en la página 13

Las estrategias de phishing de credenciales que atacan indiscriminadamente a todas las bandejas de entrada están aumentando y el ataque al correo electrónico empresarial, incluido el fraude en las facturas, entraña un riesgo de ciberdelincuencia importante para las empresas.



Más información en la página 21

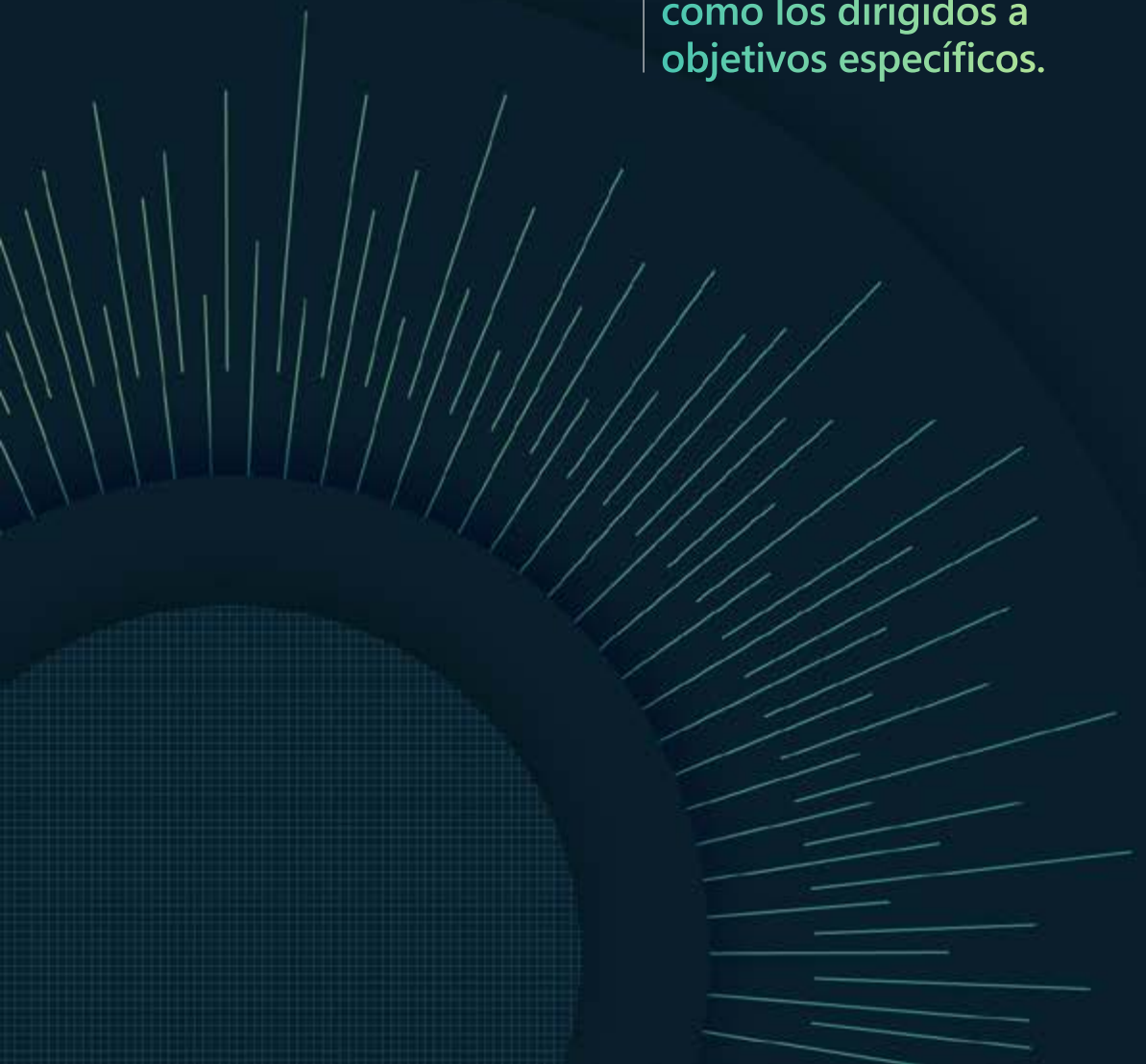
Para desestabilizar las infraestructuras maliciosas de los ciberdelincuentes y los agentes de los estados nación, Microsoft utiliza enfoques legales innovadores y alianzas públicas y privadas.



Más información en la página 25

Introducción

La ciberdelincuencia sigue aumentando, tanto los ataques aleatorios como los dirigidos a objetivos específicos.



A medida que mejoran las defensas cibernéticas y cada vez más gobiernos y empresas adoptan un enfoque de prevención proactivo, vemos que los atacantes usan dos estrategias para obtener el acceso necesario para ejercer la ciberdelincuencia. Un enfoque es una campaña con objetivos amplios basado en el volumen. El otro utiliza la vigilancia y ataques más selectivos para aumentar el margen de rentabilidad. Incluso cuando la obtención de ingresos no es el objetivo (como la actividad de los estados nación con fines geopolíticos), se utilizan ataques aleatorios y dirigidos. Este último año, los ciberdelincuentes continuaron utilizando la ingeniería social y aprovechando los temas de actualidad para maximizar el éxito de las campañas. Por ejemplo, mientras que los señuelos de phishing relacionados con la COVID se utilizaron con menos frecuencia, observamos un aumento de los señuelos que solicitan donaciones para ayudar a los ciudadanos de Ucrania.

Los atacantes se están adaptando y encontrando nuevas formas de implementar sus técnicas, aumentando la complejidad en la forma y el lugar en el que alojan la infraestructura operativa de sus campañas. Hemos observado que los ciberdelincuentes son cada vez más frugales y los atacantes ya no están pagando por la tecnología. Para reducir sus costes y aumentar la apariencia de legitimidad, algunos atacantes dirigen sus ataques cada vez más a las empresas para alojar campañas de phishing o malware, o incluso utilizan su capacidad informática para la minería de criptomonedas.

En este capítulo, examinaremos también el auge del «hacktivismo», una disrupción provocada por ciudadanos privados que perpetran ciberataques con nuevos objetivos sociales o políticos. Miles de personas de todo el mundo, tanto expertos como novatos, se han movilizado desde febrero de 2022 para lanzar ataques como la desactivación de sitios web y la filtración de datos robados como parte de la guerra entre Rusia y Ucrania. Es demasiado pronto para saber si esta tendencia continuará cuando terminen las hostilidades.

Las organizaciones deben revisar y reforzar periódicamente los controles de acceso e implementar estrategias de seguridad para defenderse de los ciberataques. Sin embargo, eso no es todo lo que pueden hacer. Explicamos cómo nuestra Unidad de delitos digitales (DCU) ha utilizado pleitos civiles para incautar infraestructura maliciosa utilizada por ciberdelincuentes y agentes de los estados nación. Debemos luchar colectivamente contra esta amenaza mediante alianzas tanto públicas como privadas. Esperamos que al compartir lo que hemos aprendido en los últimos 10 años, ayudemos a otras personas a comprender y considerar las medidas proactivas que pueden tomar para protegerse a sí mismos y al ecosistema más amplio de la amenaza creciente de la ciberdelincuencia.

Amy Hogan-Burney
Directora general, Unidad de delitos digitales

Ransomware y extorsión: una amenaza de nivel nacional

Los ataques de ransomware entrañan un mayor peligro para todas las personas, ya que las infraestructuras críticas, empresas de todos los tamaños y gobiernos estatales y locales son el blanco de delincuentes que se aprovechan de un creciente ecosistema de ciberdelincuencia.

En los últimos dos años, los incidentes de ransomware de gran repercusión mediática, como los que afectan a proveedores de infraestructuras críticas, atención sanitaria y servicios de TI, han atraído considerablemente la atención del público. A medida que los ataques de ransomware se vuelven más audaces en cuanto a su alcance, sus efectos son mayores. A continuación, se muestran ejemplos de ataques que ya hemos visto en 2022:

- En febrero, un ataque contra dos empresas afectó a los sistemas de procesamiento de pagos de cientos de gasolineras en el norte de Alemania.[1]
- En marzo, un ataque contra el servicio postal griego interrumpió temporalmente la entrega de correo y afectó al procesamiento de las transacciones financieras.[2]
- A finales de mayo, un ataque de ransomware contra organismos gubernamentales costarricenses obligó a declarar una emergencia nacional tras el cierre de hospitales y la interrupción de la recaudación de aranceles e impuestos.[3]
- También en mayo, un ataque causó retrasos y cancelaciones en los vuelos de una de las aerolíneas más grandes de la India, que dejó a cientos de pasajeros en tierra.[4]

El éxito de estos ataques y el alcance de su impacto real son el resultado de la industrialización de la economía de la ciberdelincuencia, que permite el acceso a herramientas e infraestructura y amplía las capacidades de los ciberdelincuentes al reducir los conocimientos necesarios para perpetrar un ataque.

En los últimos años, el ransomware ha dejado de basarse en el modelo en el que una única «banda» desarrolla y distribuye una carga útil de ransomware para convertirse en un modelo de ransomware como servicio (RaaS). El modelo RaaS permite a un grupo gestionar el desarrollo de la carga útil del ransomware y proporcionar servicios de pago y extorsión a través de filtraciones de datos a otros ciberdelincuentes (que son los que en realidad realizan los ataques de ransomware), que reciben el nombre de «afiliados», a cambio de un porcentaje de las ganancias. Este franquiciado de los ataques cibernéticos ha ampliado el número de atacantes. La industrialización de las herramientas de ciberdelincuencia ha hecho que sea más fácil para los atacantes realizar intrusiones, filtrar datos e implementar ransomware.

El ransomware operado por humanos[5] —un término acuñado por los investigadores de Microsoft para describir las amenazas realizadas por seres humanos que toman decisiones en cada etapa de los ataques en función de lo que descubren en la red de su objetivo y perfilan la amenaza a partir de ataques de ransomware básicos— sigue siendo una amenaza importante para las organizaciones.

Modelo basado en los datos de Microsoft Defender para punto de conexión (EDR) (enero-junio de 2022).

Ransomware y extorsión: una amenaza de nivel nacional

Continuación

Los ataques de ransomware han ampliado su impacto cuando la adopción de una estrategia de monetización doble de la extorsión se ha convertido en una práctica estándar. Esto implica la filtración de datos de dispositivos atacados, el cifrado de los datos en los dispositivos y la publicación o la amenaza con publicar los datos robados públicamente para instar a las víctimas a que paguen un rescate.

Aunque la mayoría de los atacantes de ransomware implementan el ransomware de forma oportunista en cualquier red a la que acceden, algunos compran el acceso a otros ciberdelincuentes, aprovechando las conexiones entre los agentes de acceso y los operadores de ransomware.

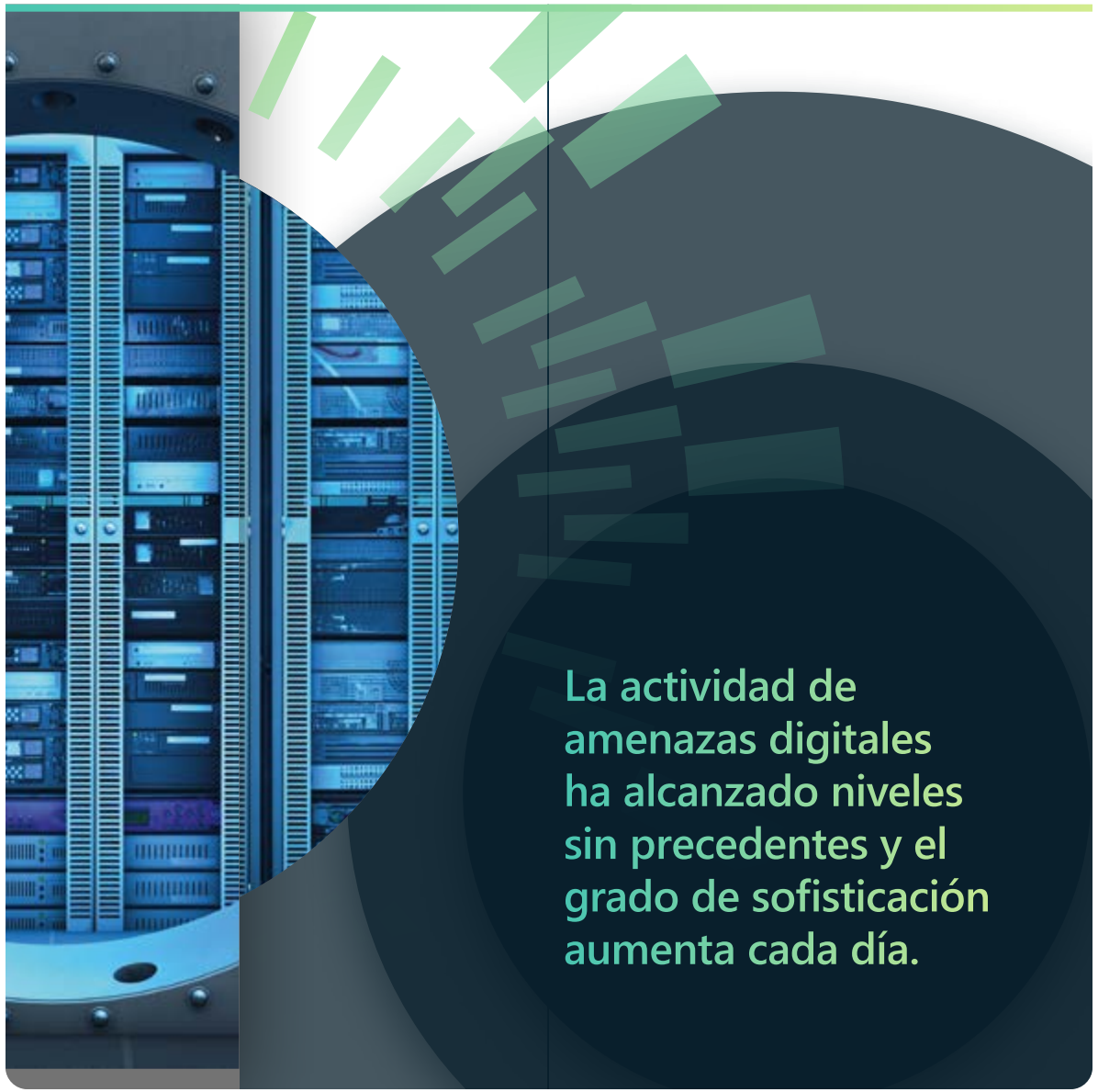
Nuestro amplio abanico de información de señales proviene de distintas fuentes (identidad, correo electrónico, puntos de conexión y cloud) y proporciona una idea de la creciente economía de ransomware, complementada con un sistema de afiliados que incluye herramientas diseñadas para los atacantes con menos conocimientos técnicos.

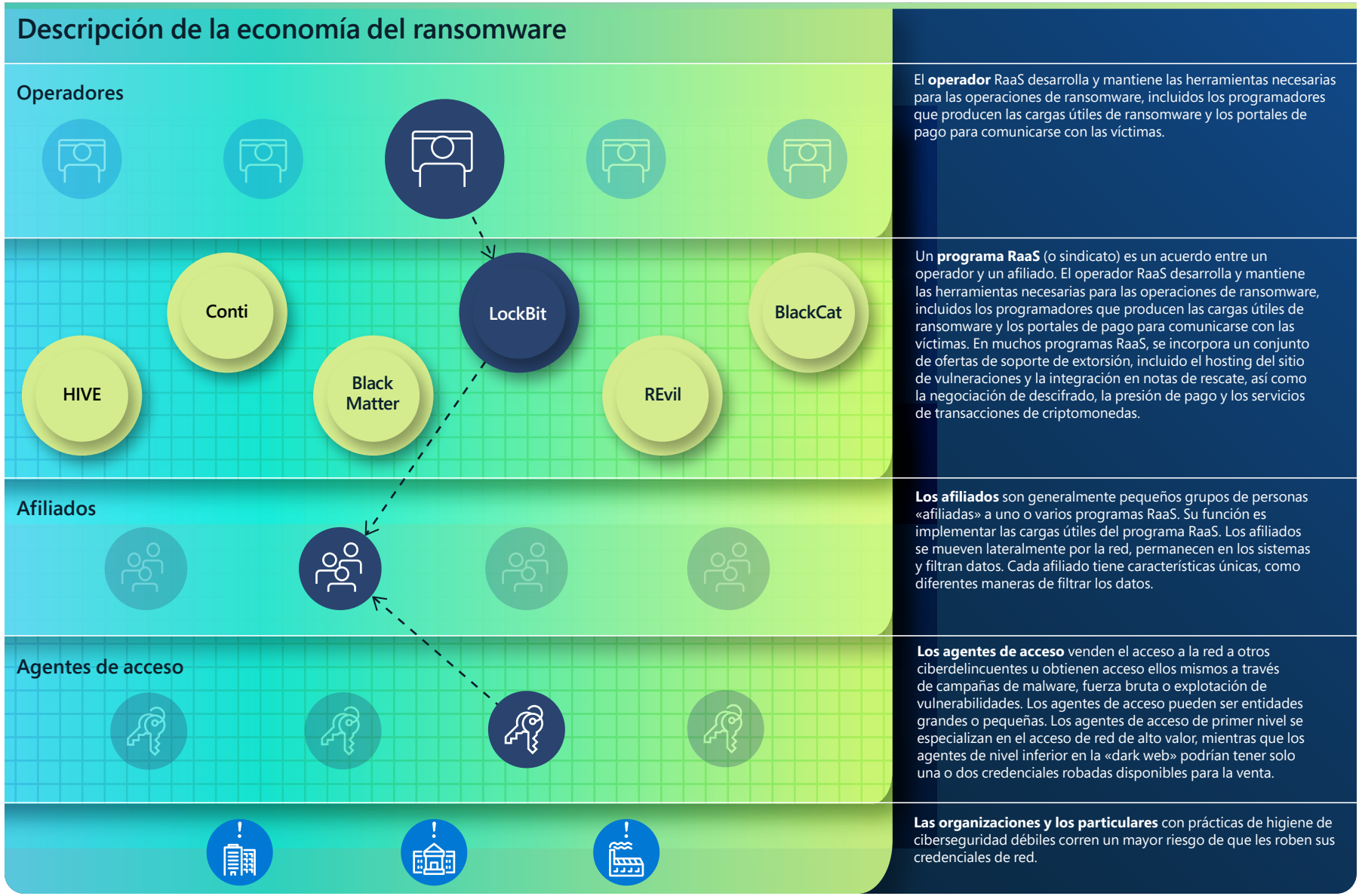
La expansión de las relaciones entre los ciberdelincuentes especializados ha aumentado la velocidad, la sofisticación y el éxito de los ataques de ransomware. Esto ha impulsado el cambio del ecosistema de ciberdelincuentes a agentes conectados con diferentes técnicas, objetivos y conocimientos que se apoyan entre sí para acceder inicialmente a los objetivos, implementar los servicios de pago y utilizar herramientas o sitios de descifrado o publicación.

Los operadores de ransomware ahora pueden comprar acceso a organizaciones o redes gubernamentales online u obtener credenciales y acceso a través de relaciones interpersonales con agentes cuyo objetivo principal es únicamente monetizar el acceso que han obtenido.

A continuación, los operadores utilizan el acceso comprado para desplegar una carga útil de ransomware adquirida en los marketplaces o foros de la «dark web». En muchos casos, las negociaciones con las víctimas las lleva a cabo el equipo de RaaS, no los propios operadores. Estas transacciones delictivas son fluidas y los participantes corren poco riesgo de ser arrestados y acusados gracias al anonimato de la «dark web» y a la dificultad de aplicar las leyes entre naciones.

Un esfuerzo continuado y bien dirigido contra esta amenaza requerirá una estrategia de todo el Gobierno en estrecha colaboración con el sector privado.





A diferencia de cómo el ransomware se presenta a veces en los medios de comunicación, es raro que una única variante de ransomware la pueda gestionar una sola «banda de ransomware» de principio a fin, sino que hay entidades distintas que crean el malware, obtienen acceso a las víctimas, implementan el ransomware y se encargan de las negociaciones de extorsión. La industrialización del ecosistema criminal ha creado:

- Agentes de acceso que acceden y entregan el acceso (acceso como servicio).
- Desarrolladores de malware que venden herramientas.
- Operadores y afiliados que realizan intrusiones delictivas.
- Proveedores de servicios de cifrado y extorsión que se hacen cargo de la monetización de los afiliados (RaaS).

Todas las campañas de ransomware gestionadas por humanos comparten dependencias comunes sobre los puntos débiles de seguridad. En concreto, los atacantes suelen aprovechar la mala higiene cibernética de una organización, que a menudo incluye la aplicación poco frecuente de parches y la no implementación de la autenticación multifactor (MFA).

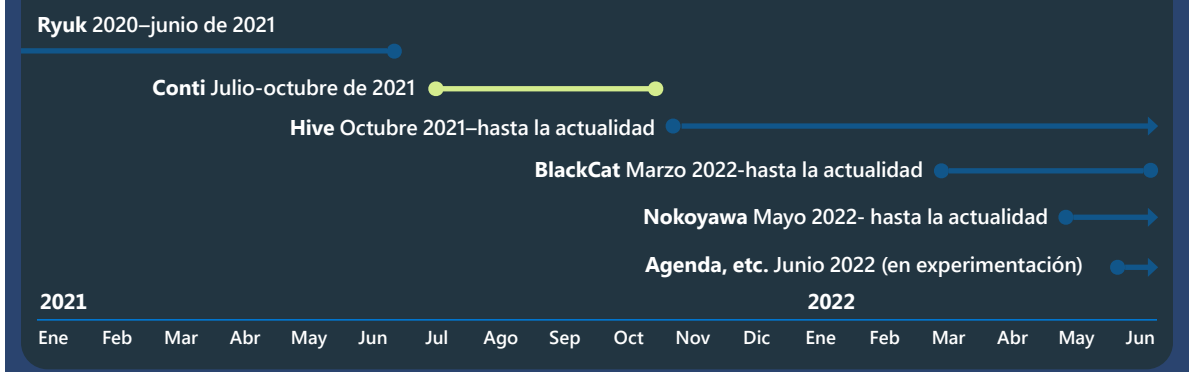
Caso práctico: La disolución de Conti

Conti, una de las principales variantes de ransomware de los últimos dos años, empezó a dejar de operar a mediados de 2022, y el Centro de inteligencia sobre amenazas de Microsoft (MSTIC, por sus siglas en inglés) observó una disminución importante de la actividad a finales de marzo y principios de abril. Observamos las últimas implementaciones del ransomware Conti a mediados de abril. Sin embargo, al igual que el cierre de otras operaciones de ransomware, la disolución de Conti no tuvo un impacto importante en las implementaciones de ransomware, ya que el MSTIC observó cómo los afiliados de Conti implementaban otras cargas útiles de ransomware, como BlackBasta, Lockbit 2.0, LockbitBlack e HIVE. Esto coincide con los datos de años anteriores y sugiere que cuando las bandas de ransomware dejan de operar, resurgen meses después o redistribuyen sus capacidades técnicas y recursos a nuevos grupos.

Nuestros equipos de inteligencia sobre amenazas de Microsoft rastrean a los actores de amenazas de ransomware como grupos individuales (etiquetados como DEV) en función de sus herramientas específicas, en lugar de controlarlos por el malware que utilizan. Esto significó que cuando los afiliados de Conti se dispersaron, pudimos seguir rastreando a estos DEV mediante el uso de otras herramientas o kits de RaaS. Por ejemplo:

- DEV-0230, que está afiliado a Trickbot, había sido un usuario prolífico de Conti. A finales de abril, el MSTIC observó que estaba usando QuantumLocker.
- DEV-0237 cambió del kit de ransomware de Conti a HIVE y Nokoyawa, incluido el uso de HIVE en el ataque del 31 de mayo contra organismos gubernamentales de Costa Rica.
- Se observó que DEV-0506, otro usuario prolífico del kit de ransomware Conti, estaba usando BlackBasta.

Ejemplo de un afiliado (DEV-0237) cambiando rápidamente de un programa RaaS a otro



Después de cerrar un programa RaaS como Conti, el afiliado de ransomware cambia a otro (Hive) casi inmediatamente.

RaaS hace evolucionar el ecosistema de ransomware y obstaculiza la atribución

Como el ransomware operado por humanos está dirigido por operadores individuales, los patrones de ataque varían en función del objetivo y van cambiando mientras se produce el ataque. En el pasado, observábamos una estrecha relación entre el vector de entrada inicial, las herramientas y las opciones de carga útil del ransomware en cada campaña de ataque de ransomware. Esto simplificaba la atribución. Sin embargo, el modelo de afiliados de RaaS desvincula esta relación. Por este motivo, Microsoft rastrea a los afiliados del ransomware que implementan cargas útiles en ataques específicos, en lugar de controlar a los desarrolladores de la carga de útil del ransomware que actúan como operadores.

O dicho de otra forma: ya no presuponemos que el desarrollador de HIVE sea el operador que está detrás de un ataque de ransomware HIVE; es más probable que sea un afiliado.

El sector de la ciberseguridad se ha esforzado por capturar adecuadamente esta delineación entre desarrolladores y operadores. El sector sigue informando a menudo de un incidente de ransomware por su nombre de carga útil, lo que da la falsa impresión de que una sola entidad, o grupo de ransomware, está detrás de todos los ataques que utilizan esa carga útil específica de ransomware y que todos los incidentes asociados con ella comparten técnicas e infraestructura comunes. Para respaldar a los defensores de la red, es importante obtener más información sobre las etapas que preceden a los ataques de diferentes afiliados, como la exfiltración de datos y los mecanismos adicionales de persistencia, y sobre las oportunidades de detección y protección que podrían existir.

Más que malware, los atacantes necesitan credenciales para que sus operaciones tengan éxito. La infección por ransomware operada con éxito de toda una organización depende del acceso a una cuenta con privilegios elevados.

Aspectos destacados de los ataques de ransomware operados por humanos

Durante el año pasado, los expertos en ransomware de Microsoft realizaron investigaciones de más de 100 incidentes de ransomware operados por humanos para rastrear las técnicas de los atacantes y saber cómo proteger mejor a nuestros clientes.

Es importante señalar que el análisis que compartimos aquí solo es posible para dispositivos inscritos y administrados. Los dispositivos no inscritos y no administrados representan la parte menos segura de los activos de hardware de una organización.

Técnicas de la fase de ransomware más prevalentes:

75 %

Usar herramientas de administración.

75 %

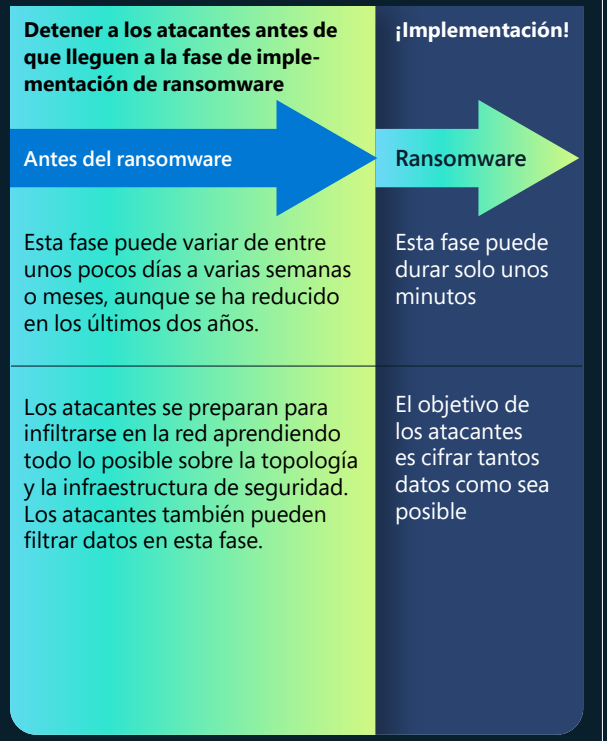
Usar la cuenta de usuario atacada con privilegios elevados para propagar cargas útiles maliciosas a través del protocolo SMB.

99 %

Intentar manipular productos de seguridad y copia de seguridad detectados con herramientas del sistema operativo.

El ataque típico operado por humanos

Los ataques de ransomware operados por humanos se pueden clasificar en la fase anterior al ransomware y en la fase de implementación del ransomware. Durante la fase previa al ransomware, los atacantes se preparan para infiltrarse en la red aprendiendo la infraestructura de seguridad y la tipología de la organización.



Nuestras investigaciones constataron que la mayoría de los agentes que estaban detrás de ataques de ransomware operados por humanos aprovechan puntos débiles de seguridad similares y comparten patrones y técnicas de ataque comunes.

Una estrategia de seguridad duradera

La lucha y prevención de ataques de esta naturaleza requiere un cambio en la mentalidad de una organización para centrarse en la protección integral necesaria para ralentizar y detener a los atacantes antes de que puedan pasar de la fase anterior al ransomware a la fase de implementación del ransomware.

Las empresas deben aplicar las prácticas recomendadas de seguridad de manera coherente y agresiva a sus redes con el objetivo de mitigar todo tipo de ataques. Debido a la decisión humana, los ataques de ransomware puede generar múltiples alertas de productos de seguridad aparentemente dispares que pueden perderse fácilmente o no detenerse a tiempo. La fatiga de alertas es real y los centros de operaciones de seguridad (SOC) pueden simplificar su vida observando las tendencias en sus alertas o agrupando alertas en incidentes para que puedan ver la imagen completa. Posteriormente, los SOC pueden mitigar las alertas mediante funciones de refuerzo de la seguridad, como reglas de reducción de la superficie de ataque. El refuerzo de la seguridad contra las amenazas comunes no solo puede reducir el volumen de alertas, sino también detener a muchos atacantes antes de que obtengan acceso a las redes.

Las organizaciones deben mantener altos estándares continuos de posición de seguridad e higiene de red para protegerse de los ataques de ransomware operados por humanos.

Conocimientos prácticos

Para entorpecer la economía de los ciberdelincuentes, es importante reforzar la seguridad, ya que les supondrá un coste extra.

1. Mejora la higiene de credenciales. Más que malware, los atacantes necesitan credenciales para que sus operaciones tengan éxito. La infección por ransomware operado por humanos de toda una organización depende del acceso a una cuenta con privilegios como un administrador de dominio o la capacidad de editar una política de grupo.
2. Controla la exposición de credenciales.
3. Prioriza la implementación de las actualizaciones de Active Directory.
4. Prioriza el refuerzo de la seguridad del cloud.
5. Reduce la superficie de ataque.
6. Refuerza la seguridad de los activos orientados a Internet y conoce tu perímetro.
7. Reduce la fatiga de alertas del SOC reforzando la seguridad de la red para reducir el volumen y dejar el ancho de banda para incidentes prioritarios.

Enlaces a información adicional (pueden estar en inglés)

- RaaS: Conocer la economía gig de la ciberdelincuencia y cómo protegerte de ella | Blog de seguridad de Microsoft
- Ataques de ransomware operados por humanos: un desastre evitable | Blog de seguridad de Microsoft

Perspectivas sobre el ransomware de los equipos de respuesta

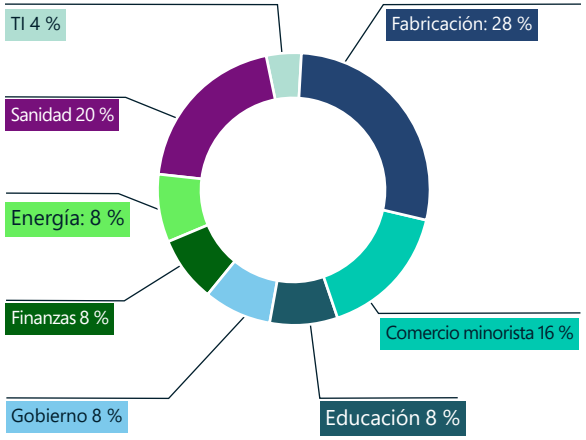
Organizaciones de todo el mundo experimentaron un crecimiento constante de los ataques de ransomware operados por humanos a partir de 2019. Sin embargo, las operaciones de las fuerzas de seguridad y los acontecimientos geopolíticos del último año tuvieron un impacto importante en las organizaciones de ciberdelincuentes.

La línea de servicio de seguridad de Microsoft ayuda a los clientes durante un ciberataque completo, desde la investigación hasta las actividades de contención y recuperación. Los servicios de respuesta y recuperación se ofrecen a través de dos equipos sumamente integrados: uno centrado en la investigación y los preparativos de recuperación y otro centrado en la contención y la recuperación. En este apartado se presenta un resumen de las conclusiones basadas en las interacciones de ransomware durante el último año.

93 %

Porcentaje de investigaciones de Microsoft durante las interacciones de recuperación de ransomware que mostraron controles de acceso con privilegios y movimiento lateral insuficientes.

Interacciones de incidentes y recuperación de ransomware por sector

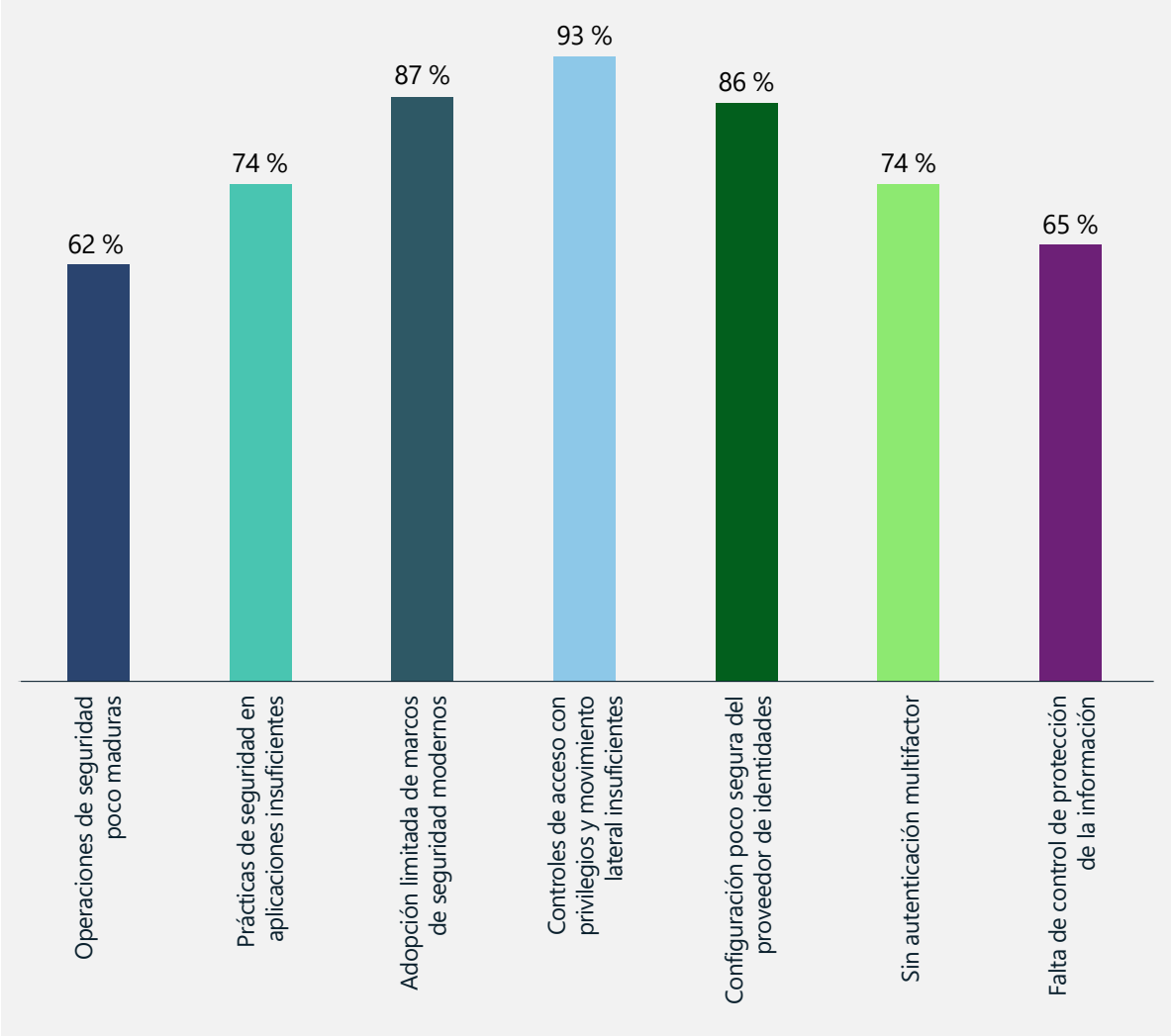


A medida que surgen nuevos grupos pequeños y amenazas, los equipos de defensa deben conocer la evolución de las amenazas de ransomware y protegerse de las familias de malware de ransomware previamente desconocidas. El enfoque de desarrollo rápido utilizado por los grupos de delincuentes ha llevado a la creación de ransomware inteligente empaquetado en kits fáciles de usar. Esto permite una mayor flexibilidad para lanzar ataques generalizados contra un mayor número de objetivos.

En las siguientes páginas se proporciona un análisis más detallado de los factores determinantes más observados para la protección débil contra el ransomware, agrupados en tres grupos de conclusiones:

1. Controles de identidad débiles
2. Operaciones de seguridad ineficientes
3. Protección de datos limitada

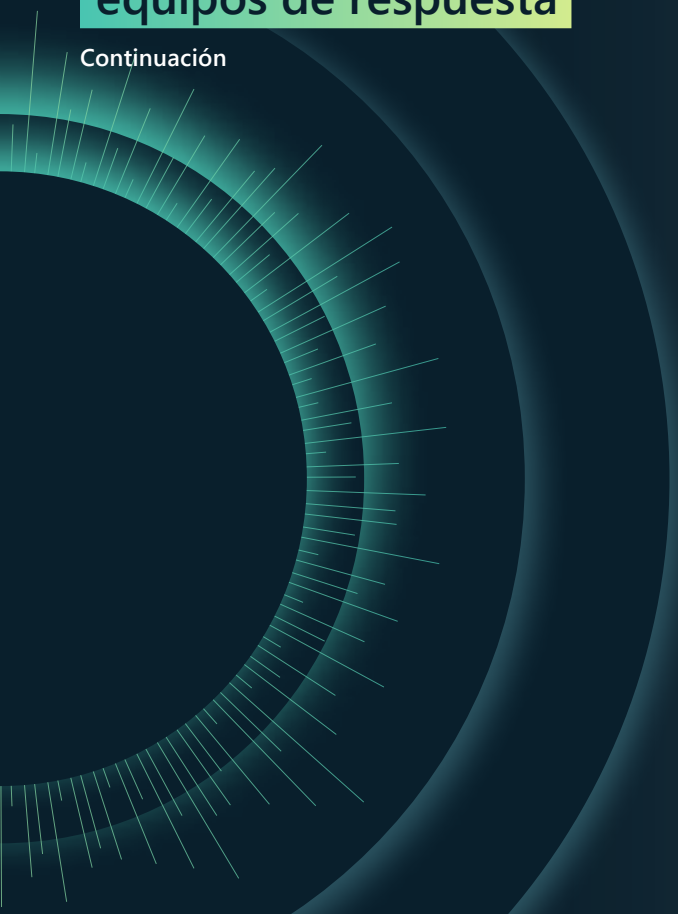
Resumen de los hallazgos más comunes en interacciones de respuesta a ransomware



La conclusión más común entre las interacciones de respuesta a incidentes de ransomware fueron los controles de acceso con privilegios y movimiento lateral insuficientes.

Perspectivas sobre el ransomware de los equipos de respuesta

Continuación



Los tres factores determinantes principales observados en nuestras interacciones de respuesta in situ:

① **Controles de identidad débiles:** los ataques de robo de credenciales siguen siendo uno de los principales factores determinantes

② **Los procesos de las operaciones de seguridad ineficaces** no solo presentan una ventana de oportunidad para los atacantes, sino que afectan considerablemente al tiempo de recuperación

③ Al final todo se reduce a los datos: a las organizaciones les cuesta implementar una **estrategia de protección de datos** eficaz acorde con sus necesidades empresariales

① Controles de identidad débiles

El ransomware operado por humanos sigue evolucionando y empleando métodos de robo de credenciales y movimiento lateral tradicionalmente asociados con ataques dirigidos. Los ataques exitosos suelen ser el resultado de campañas de larga duración que implican el ataque de los sistemas de identidad, como Active Directory (AD), que permiten a los operadores humanos robar credenciales, acceder a sistemas y mantenerse en la red.

Seguridad de Active Directory (AD) y Azure AD

88 %

Porcentaje de clientes afectados que no emplearon las prácticas recomendadas de seguridad de AD y Azure AD. Esto se ha convertido en un vector de ataque común, ya que los atacantes aprovechan las configuraciones erróneas y las posiciones de seguridad débiles de los sistemas de identidad críticos para obtener mayor acceso y causar mayor impacto en las empresas.

Acceso con privilegios mínimos y uso de estaciones de trabajo de acceso con privilegios (PAW)

Ninguna de las organizaciones afectadas implementó los principios adecuados de segregación de credenciales administrativas y principios de acceso con privilegios mínimos a través de estaciones de trabajo dedicadas durante la administración de sus identidades críticas y activos de gran valor, como los sistemas patentados y las aplicaciones críticas.

Seguridad de las cuentas con privilegios

88 %

Porcentaje de interacciones en las que la MFA no estaba implementada para cuentas sensibles y con privilegios elevados, lo que deja un vacío de seguridad para que los atacantes adquieran las credenciales y perpetren más ataques utilizando credenciales legítimas.

84 %

Los administradores del 84 por ciento de las organizaciones no utilizaron controles de identidad de privilegios como el acceso «just-in-time» para evitar un uso malintencionado de las credenciales con privilegios obtenidas.

Perspectivas sobre el ransomware de los equipos de respuesta

Continuación

② Operaciones de seguridad ineficaces

Nuestros datos muestran que las organizaciones que sufrieron ataques de ransomware tienen brechas importantes en sus operaciones de seguridad, herramientas y administración del ciclo de vida de los activos de tecnología de la información. De acuerdo con los datos disponibles, estas fueron las deficiencias más observadas:

Aplicación de parches:

68 %

Porcentaje de las organizaciones afectadas que no tenían un proceso eficaz de administración de vulnerabilidades y parches, y su gran dependencia de los procesos manuales y la aplicación automática de parches produjo grietas críticas. La fabricación y las infraestructuras críticas siguen teniendo problemas con el mantenimiento y la aplicación de parches de sistemas de tecnología de las operaciones (TO) heredados.

Falta de herramientas de operaciones de seguridad:

La mayoría de las organizaciones registraron una falta de visibilidad integral de la seguridad debido a la ausencia o configuración incorrecta de las herramientas de seguridad, lo que produjo una disminución de la eficacia de detección y respuesta.

60 %

Porcentaje de organizaciones que informaron de que no usaban una herramienta EDR[6], una tecnología fundamental para la detección y la respuesta.

60 %

Organizaciones que no invirtieron en tecnología de administración de eventos e información de seguridad (SIEM), lo que se tradujo en la supervisión de silos, una capacidad limitada para detectar amenazas de extremo a extremo y operaciones de seguridad ineficientes. La automatización sigue siendo una deficiencia importante en las herramientas y los procesos de SOC, lo que obliga al personal de SOC a dedicar innumerables horas a interpretar la telemetría de seguridad.

84 %

Porcentaje de las organizaciones afectadas que no habilitaron la integración de sus entornos multicloud en sus herramientas de operaciones de seguridad.

Procesos de respuesta y recuperación:

76 %

La falta de un plan de respuesta eficaz fue un área crítica observada en el 76 por ciento de las organizaciones afectadas, lo que impide una preparación adecuada de las crisis de la organización y afecta negativamente al tiempo de respuesta y recuperación.

③ Protección de datos limitada

Muchas organizaciones atacadas carecían de procesos de protección de datos adecuados, lo que afecta considerablemente al tiempo de recuperación y a la capacidad de reanudar las operaciones empresariales. Entre las deficiencias más comunes encontradas se incluyen:

Copias de seguridad inmutables:

44 %

Porcentaje de organizaciones que no tenían copias de seguridad inmutables para los sistemas afectados. Los datos también muestran que los administradores no tenían planes de copias de seguridad y recuperación para activos críticos como AD.

Prevención de pérdida de datos:

Los atacantes suelen encontrar una forma de poner en peligro los sistemas mediante la explotación de vulnerabilidades de la organización, la filtración de datos críticos para la extorsión, el robo de la propiedad intelectual o la monetización.

92 %

Porcentaje de organizaciones afectadas que no implementaron controles eficaces de prevención de pérdida de datos para mitigar estos riesgos, lo que dio lugar a una pérdida de datos crítica.

El ransomware disminuyó en algunas regiones y aumentó en otras

Este año hemos observado una reducción en el número general de casos de ransomware notificados a nuestros equipos de respuesta en Norteamérica y Europa en comparación con el año anterior. Al mismo tiempo, aumentaron los casos registrados en Latinoamérica.

Una interpretación de esta observación es que los ciberdelincuentes se han alejado de las áreas percibidas como más propensas a activar la vigilancia de las fuerzas del orden en favor de objetivos más débiles. Dado que Microsoft no observó una mejora sustancial en la seguridad de la red empresarial en todo el mundo para explicar la disminución de las llamadas de soporte relacionadas con ransomware, creemos que la causa más probable es una combinación de la actividad de las fuerzas del orden en 2021 y 2022, que aumentó el coste de la actividad delictiva, junto con algunos acontecimientos geopolíticos de 2022.

Una de las operaciones de RaaS más prevalentes pertenece a un grupo delictivo ruso conocido como REvil (también llamado Sodinokibi) que está activo desde 2019. En octubre de 2021, se desmantelaron los servidores de REvil como parte de la Operación GoldDust de la policía internacional.[7] En enero de 2022, 14 supuestos miembros rusos de REvil atacaron 25 ubicaciones asociadas a ellos.[8] Esta fue la primera vez que Rusia actuó contra operadores de ransomware en su territorio.

Aunque las actividades de las fuerzas del orden probablemente ralentizaron la frecuencia de los ataques en 2022, los actores de amenazas bien podrían desarrollar nuevas estrategias para evitar ser descubiertos en el futuro. Por otra parte, la tensión entre Rusia y los Estados Unidos debido a la seguridad de Ucrania parece haber puesto fin a la incipiente cooperación de Rusia en la lucha mundial contra el ransomware. Tras un breve período de incertidumbre seguido de las detenciones de REvil, Estados Unidos y Rusia cesaron su cooperación en la búsqueda de agentes de ransomware, lo que significa que los ciberdelincuentes podrían ver a Rusia como un lugar seguro una vez más.

De cara al futuro, prevemos que el ritmo de las actividades de ransomware dependerá de la respuesta a algunas preguntas clave:

1. ¿Actuarán los gobiernos para evitar que los delincuentes de ransomware operen dentro de sus fronteras o querrán desmantelar las operaciones de los agentes que operan desde suelo extranjero?
2. ¿Cambiarán los grupos de ransomware sus tácticas para eliminar la necesidad de ransomware y recurrir a ataques relacionados con la extorsión?
3. ¿Podrán las organizaciones modernizar y transformar sus operaciones de TI más rápido de lo que los criminales pueden aprovechar las vulnerabilidades?
4. ¿Los avances en el seguimiento y rastreo de los pagos de rescate obligarán a los destinatarios de un rescate a cambiar de táctica y de negociaciones?

Aunque las actividades de las fuerzas del orden probablemente ralentizaron la frecuencia de los ataques en 2022, los actores de amenazas bien podrían desarrollar nuevas estrategias para evitar ser descubiertos en el futuro.

Doble

Los ataques de ransomware disminuyeron en algunas regiones, pero las peticiones de rescate se duplicaron.

Conocimientos prácticos

1. Céntrate en estrategias integrales de seguridad, ya que todas las familias de ransomware se aprovechan de los mismos puntos débiles de seguridad para atacar una red.
2. Actualiza y mantén los aspectos básicos de seguridad para aumentar el nivel básico de protección de defensa en profundidad y modernizar las operaciones de seguridad. La migración al cloud permite detectar las amenazas más rápidamente y responder más rápido.

Enlaces a información adicional (pueden estar en inglés)

- Proteger tu organización del ransomware | Seguridad de Microsoft
- Siete maneras de reforzar tu entorno contra los ataques | Blog de seguridad de Microsoft
- Mejorar las defensas basadas en IA para entorpecer el ransomware operado por humanos | Equipo de investigación de Microsoft 365 Defender
- Security Insider: Explora los últimos conocimientos y actualizaciones sobre ciberseguridad | Seguridad de Microsoft

La ciberdelincuencia como servicio

La ciberdelincuencia como servicio (CaaS) es una amenaza creciente y cambiante para los clientes de todo el mundo. La unidad de delitos digitales (DCU) de Microsoft observó un crecimiento continuo del ecosistema de CaaS, con un número cada vez mayor de servicios online que facilitaron varios delitos cibernéticos, incluido BEC y ransomware operado por humanos. El phishing sigue siendo el método de ataque preferido, ya que los ciberdelincuentes pueden adquirir un gran valor robando y vendiendo el acceso a cuentas robadas.

En respuesta al mercado de CaaS en expansión, la DCU mejoró sus sistemas de escucha para detectar e identificar servicios de CaaS en todo el ecosistema de Internet, la «dark web», los foros examinados,[9] los sitios web dedicados, los foros de debate online y las plataformas de mensajería.

Los ciberdelincuentes ahora colaboran en diferentes zonas horarias y idiomas para obtener resultados específicos. Por ejemplo, un sitio web de CaaS administrado por una persona en Asia mantiene operaciones en Europa y crea cuentas malintencionadas en África. La naturaleza multijurisdiccional de estas operaciones presenta desafíos complejos para el cumplimiento de la ley. En respuesta, la DCU centra sus esfuerzos en deshabilitar la infraestructura delictiva malintencionada utilizada para facilitar los ataques de CaaS y colaborar con cuerpos de seguridad de todo el mundo para exigir responsabilidades a los delincuentes.

Los ciberdelincuentes utilizan cada vez más los análisis para maximizar el alcance, el ámbito y el beneficio. Al igual que las empresas legítimas, los sitios web de CaaS deben garantizar la validez de los productos y servicios para mantener una buena reputación. Por ejemplo, los sitios web de CaaS automatizan de forma rutinaria el acceso a cuentas atacadas para garantizar la validez de las credenciales robadas. Los ciberdelincuentes dejarán de vender cuentas específicas cuando se restablezcan las contraseñas o se corrijan las vulnerabilidades. Cada vez más, identificamos sitios web de CaaS que proporcionan a los compradores verificación a petición como un proceso de control de calidad. Como resultado, los compradores pueden confiar en que el sitio web de CaaS vende cuentas y contraseñas activas, al tiempo que reduce los posibles costes para el comerciante de CaaS si las credenciales robadas se restablecen antes de la venta.

La DCU también observó sitios web de CaaS que ofrecían a los compradores la opción de comprar cuentas atacadas en ubicaciones geográficas específicas, proveedores de servicios online designados y, en concreto, particulares, profesiones y sectores de la industria específicos. Las cuentas solicitadas con frecuencia son las de profesionales o departamentos que procesan facturas, como los directores financieros o «cuentas por cobrar». Del mismo modo, los sectores de la industria implicados en los contratos públicos suelen ser objetivos de los ataques debido a la cantidad de información disponible a través del proceso de licitaciones públicas.

Las investigaciones de la DCU en CaaS mostraron una serie de tendencias clave:

El número y la sofisticación de los servicios está aumentando.

Un ejemplo es la evolución de los shells web que suelen consistir en servidores web atacados utilizados para automatizar los ataques de phishing. La DCU observó que los distribuidores de CaaS simplificaban la carga de kits de phishing o malware a través de paneles web especializados. Posteriormente, los vendedores de CaaS intentan vender servicios adicionales al actor de amenazas a través del panel, como servicios de mensajes de spam y listas de destinatarios de spam especializadas basadas en atributos definidos, incluida la ubicación geográfica o la profesión. En algunos casos, hemos observado que se utiliza un único shell web en varias campañas de ataque, lo que sugiere que los atacantes podrían mantener un acceso persistente en el servidor atacado. También hemos observado un aumento de los servicios de anonimización disponibles como parte del ecosistema CaaS, así como ofertas para redes privadas virtuales (VPN) y cuentas de servidores privados virtuales (VPS). En la mayoría de los casos, la VPN/VPS ofrecida se adquirió inicialmente a través de tarjetas de crédito robadas. Los sitios web de CaaS también ofrecían un mayor número de protocolos de Escritorio remoto (RDP), shell seguro (SSH) y cPanels para su uso como plataforma para orquestar ataques cibernéticos. Los comerciantes de CaaS configuran RDP, SSH y cPanels con las herramientas y los scripts apropiados para facilitar varios tipos de ciberataques.

Los servicios de creación de dominios homoglifos requieren cada vez más pagos en criptomonedas.

Los dominios homoglifos se hacen pasar por nombres de dominio legítimos utilizando caracteres que tienen una apariencia idéntica o casi idéntica a otro carácter. El objetivo es engañar al usuario para que piense que el dominio homoglifo es un dominio auténtico. Estos dominios son una amenaza omnipresente y una puerta de entrada para una cantidad importante de delitos cibernéticos. Los sitios CaaS ahora venden nombres de dominio homoglifos personalizados, lo que permite a los compradores solicitar nombres de empresa y de dominio específicos para suplantarlos. Una vez recibido el pago, los comerciantes de CaaS utilizan una herramienta de generador de homoglifos para seleccionar el nombre de dominio y luego registrar el homoglifo malintencionado. El pago de este servicio es casi exclusivamente en criptomonedas.

2 750 000

Registros en sitios bloqueados con éxito por la DCU este año para adelantarse a los delincuentes que tenían previsto utilizarlos para vendérselos a ciberdelincuentes globales.

La ciberdelincuencia como servicio

Continuación

Los vendedores de CaaS incluyen cada vez más las credenciales pirateadas entre sus opciones de compra.

Las credenciales pirateadas permiten el acceso no autorizado a las cuentas de usuario, incluido el servicio de mensajería de correo electrónico, los recursos corporativos para compartir archivos y OneDrive para la Empresa. Si se obtienen las credenciales de administrador, los usuarios no autorizados podrían obtener acceso a archivos confidenciales, recursos de Azure y cuentas de usuarios de la empresa. En muchos casos, las investigaciones de la DCU identificaron el uso no autorizado de las mismas credenciales en varios servidores como un medio de automatizar la verificación de credenciales. Este patrón sugiere que el usuario atacado podría ser víctima de múltiples ataques de phishing o tener malware en el dispositivo que permite que los keyloggers de botnets obtengan credenciales.

Están surgiendo servicios y productos CaaS con características mejoradas para eludir la detección.

Un vendedor de CaaS ofrece kits de phishing con mayores capas de complejidad y funciones de anonimización diseñadas para eludir los sistemas de detección y prevención por tan solo 6 dólares al día. El servicio ofrece una serie de redireccionamientos que realizan comprobaciones antes de permitir el tráfico a la siguiente capa o sitio. Una de ellas ejecuta más de 90 comprobaciones de huella dactilar del dispositivo, incluido si se trata de una máquina virtual, recopilando detalles sobre el navegador y el hardware utilizados, entre otras cosas. Si se superan todas las comprobaciones, el tráfico se envía a una página de destino utilizada para el phishing.

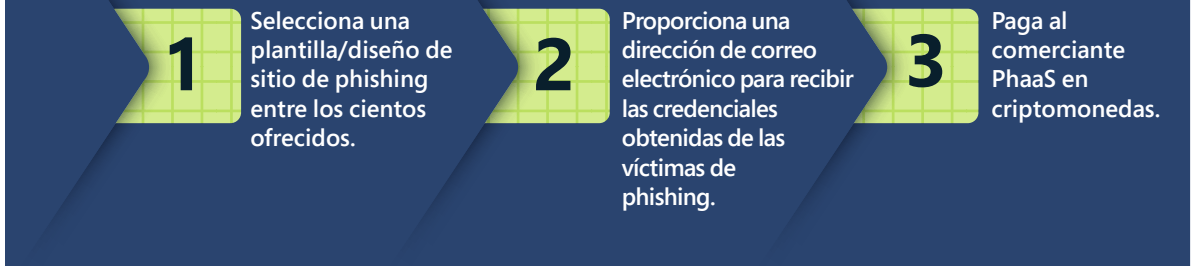
Los servicios de ciberdelincuencia «todo incluido» venden suscripciones a servicios administrados.

Normalmente, cada paso de la comisión de un delito online puede exponer a los actores de amenazas si la seguridad operativa es deficiente. El riesgo de exposición e identificación aumenta si se compran servicios en varios sitios de CaaS. La DCU observó una tendencia preocupante en la «dark web»: un aumento de los servicios que se ofrecen para anonimizar el código de software y convertir el texto del sitio web en genérico para reducir la exposición. Los proveedores de servicios completos por suscripción de ciberdelincuencia administran todos los servicios y garantizan resultados que reducen aún más los riesgos de exposición al OCN suscriptor. El menor riesgo ha aumentado la popularidad de estos servicios completos.

El phishing como servicio (PhaaS) es un ejemplo de un servicio de ciberdelincuencia completo. PhaaS es una evolución de los servicios anteriores conocidos como «servicios totalmente indetectables» (FUD, por sus siglas en inglés) y se ofrece en forma de suscripción. Los términos típicos de PhaaS incluyen mantener activos los sitios web de phishing durante un mes.

La DCU también identificó a un comerciante de CaaS que ofrecía ataques de denegación de servicio distribuido (DDoS) en un modelo de suscripción. Este modelo subcontrata la creación y el mantenimiento de la botnet necesaria para perpetrar los ataques del comerciante de CaaS. Cada cliente de la suscripción a DDoS recibe un servicio cifrado para mejorar la seguridad operativa y un año de soporte las 24 horas del día, los siete días de la semana. El servicio de suscripción DDoS ofrece diferentes arquitecturas y métodos de ataque, de manera que un comprador simplemente selecciona el recurso que desea atacar y el vendedor proporciona acceso a una serie de dispositivos expuestos en su botnet para perpetrar el ataque. El coste de la suscripción a DDoS es de 500 dólares.

PhaaS, los ciberdelincuentes ofrecen varios servicios en una sola suscripción. En general, un comprador solo debe realizar tres acciones:



Una vez que se han completado estos pasos, el comerciante de PhaaS crea servicios con tres o cuatro capas de recursos de redireccionamiento y hosting para atacar a usuarios específicos. Posteriormente, se lanza la campaña y se obtienen, verifican y envían las credenciales de la víctima a la dirección de correo electrónico proporcionada por el comprador. Por el pago de una prima, muchos comerciantes de PhaaS se ofrecen a alojar sitios de phishing en la blockchain pública para que cualquier navegador pueda acceder a ellos y los redireccionamientos puedan dirigir a los usuarios a un recurso de la contabilidad general distribuida.

El trabajo de la DCU para desarrollar herramientas y técnicas que identifiquen y paren a los ciberdelincuentes de CaaS es continuo. La evolución de los servicios CaaS presenta importantes desafíos, particularmente en el desmantelamiento de los pagos con criptomonedas.

Uso delictivo de las criptomonedas

Conforme se generaliza el uso de las criptomonedas, los delincuentes las utilizan cada vez más para eludir las medidas de las fuerzas del orden y contra el blanqueo de capitales (AML). Esto aumenta el desafío para las fuerzas del orden de rastrear y controlar los pagos con criptomonedas a los ciberdelincuentes.

El gasto mundial en soluciones de blockchain creció aproximadamente un 340 por ciento en los últimos cuatro años, mientras que las nuevas carteras de criptomonedas crecieron alrededor de un 270 por ciento. Hay más de 83 millones de carteras distintas en todo el mundo, y la capitalización total en el mercado de todas las criptomonedas fue de aproximadamente 1,1 billones de dólares a fecha del 28 de julio de 2022.[10]

Fuente: Twitter.com: @PeckShieldAlert (PeckShield es una empresa china de seguridad de blockchain).

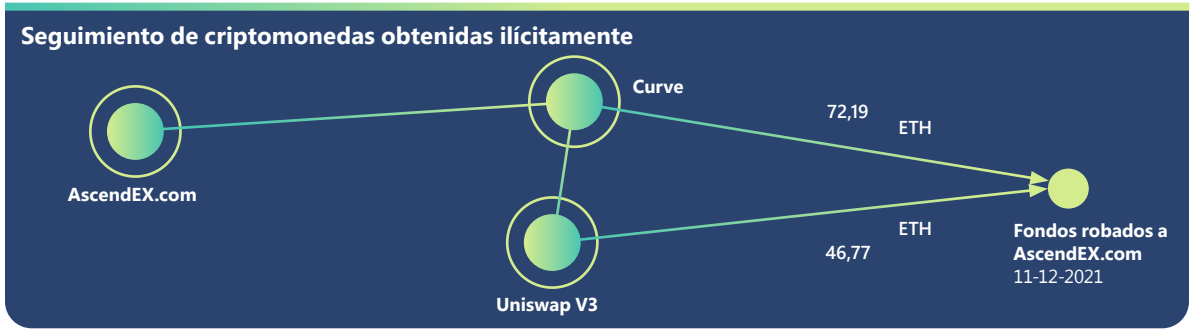
Rastreo de los pagos de ransomware

El ransomware es una de las mayores fuentes de criptomonedas obtenidas ilícitamente. En un esfuerzo por desmantelar la infraestructura técnica malintencionada utilizada en los ataques de ransomware (por ejemplo, el desmantelamiento de Zloader en abril de 2022[11]), la DCU de Microsoft rastrea las carteras delictivas para permitir la capacidad de seguimiento y recuperación de criptomonedas.

Los investigadores de la DCU han observado que los agentes de ransomware han desarrollado sus tácticas de comunicación con las víctimas para ocultar la pista del dinero. Originalmente, los ciberdelincuentes incluían direcciones de Bitcoin en sus notas de rescate. Sin embargo, esto permitía el seguimiento de las transacciones de pago en el blockchain, por lo que los agentes de ransomware dejaron de incluir las direcciones de las carteras y, en su lugar, utilizaban direcciones de correo electrónico o enlaces a sitios web de chat para comunicar las direcciones de pago del rescate a las víctimas. Algunos agentes incluso crearon páginas web e inicios de sesión únicos para cada víctima con el fin de evitar que los investigadores de seguridad y las fuerzas del orden obtuvieran las direcciones de las carteras de los delincuentes que se hacían pasar por víctimas. A pesar de los esfuerzos de los delincuentes por ocultar su rastro, algunos pagos de rescate todavía se pueden recuperar trabajando con las fuerzas del orden y las empresas de análisis de criptomonedas que pueden rastrear el movimiento en el blockchain.

Tendencia: blanqueo DEX de ganancias ilícitas

Un problema importante para los ciberdelincuentes es la conversión de las criptomonedas en moneda fiduciaria. Los ciberdelincuentes tienen varias vías potenciales de conversión, cada una de las cuales entraña un grado diferente de riesgo. Un método utilizado para reducir el riesgo es blanquear los ingresos a través de un intercambio descentralizado (DEX) antes de la retirada del dinero a través de las opciones de cobro de efectivo disponibles,



Con la herramienta de investigación de criptomonedas Chainalysis, la Unidad de delitos digitales de Microsoft descubrió que los hackers de AcendEX intercambiaron sus fondos robados con un DEX más pequeño llamado Curve además de con Uniswap. En este diagrama se ilustran las rutas de blanqueo que descubrió el equipo. Cada círculo representa un grupo y los números de cada línea representan la cantidad total de Ethereum transmitido con fines de blanqueo.

como intercambios centralizados (CEX), intercambios punto a punto (P2P) e intercambios de venta libre (OTC). Los DEX son un lugar de blanqueo atractivo porque a menudo no siguen las medidas de la lucha contra el blanqueo de capitales.

En diciembre de 2021, los hackers atacaron la plataforma global de comercio de criptomonedas AscendEx y robaron aproximadamente 77,7 millones de USD en criptomonedas a sus clientes.[12] AscendEx contrató empresas de análisis de blockchain y se puso en contacto con otros CEX para que las carteras que recibían fondos robados pudieran incluirse en la lista negra. Asimismo, las direcciones donde se enviaron las monedas se etiquetaron como tales en el explorador de blockchain Ethereum Etherscan.[13] Con el fin de eludir las alertas y las listas negras, los hackers enviaron 1,5 millones de USD en Ethereum a Uniswap, uno de los DEX más grandes del mundo, el 18 de febrero de 2022.[14]

La adopción de medidas de AML más contundentes por parte de los DEX podría amortiguar la actividad de blanqueo de dinero en sus plataformas y obligar a los ciberdelincuentes a utilizar otros métodos de ofuscación como el mezclado de monedas o los intercambios sin licencia. A modo de ejemplo, Uniswap anunció recientemente que va a empezar a usar listas negras para bloquear las carteras que se sabe que están involucradas en actividades ilícitas para que no realicen transacciones en el intercambio.[15]

Conocimientos prácticos

1. Si eres una víctima de la ciberdelincuencia que ha pagado al delincuente mediante criptomonedas, ponte en contacto con la policía local, quien podría ayudar a rastrear y recuperar los fondos perdidos.
2. Familiarízate con las medidas de ALM implantadas cuando selecciones un DEX.

Enlaces a información adicional (pueden estar en inglés)

- Defensa de amenazas basada en hardware contra criptohackers cada vez más sofisticados | Equipo de investigación de Microsoft 365 Defender

El cambiante panorama de las amenazas de phishing

Las estrategias de phishing de credenciales van en aumento y siguen siendo una amenaza importante para los usuarios de cualquier parte del mundo porque atacan indiscriminadamente a todas las bandejas de entrada. Entre las amenazas que nuestros investigadores rastrean y protegen, el volumen de ataques de phishing tiene órdenes de magnitud mayores que todas las demás amenazas.

Con los datos de Defender for Office, vemos actividad de correos electrónicos malintencionados e identidades atacadas. Azure Active Directory Identity Protection proporciona aún más información a través de alertas de eventos de identidades atacadas. Con Defender for Cloud Apps, vemos eventos de acceso a datos de identidades atacadas y Microsoft 365 Defender (M365D) permite establecer relaciones entre productos. La métrica de movimiento lateral procede de Defender para punto de conexión (alertas y eventos de comportamiento de ataque), Defender for Office (correo electrónico malintencionado) y, de nuevo, M365D para la relación entre los productos).

710 millones

Correos electrónicos de phishing bloqueados a la semana.

1 h 12 m

El tiempo medio que tarda un atacante en acceder a tus datos privados si eres víctima de un correo electrónico de phishing.[16]

1 h 42 m

El tiempo medio que tarda un atacante en comenzar a moverse lateralmente dentro de la red corporativa una vez que un dispositivo ha sido comprometido.[17]

Las credenciales de Microsoft 365 siguen siendo uno de los tipos de cuentas más buscados por los atacantes. Una vez que se han obtenido las credenciales de inicio de sesión, los atacantes pueden iniciar sesión en sistemas informáticos vinculados a la empresa para facilitar la infección por malware y ransomware, robar datos e información confidenciales de la empresa mediante el acceso a archivos de SharePoint y continuar la propagación de phishing enviando correos electrónicos maliciosos adicionales a través de Outlook, entre otras acciones.

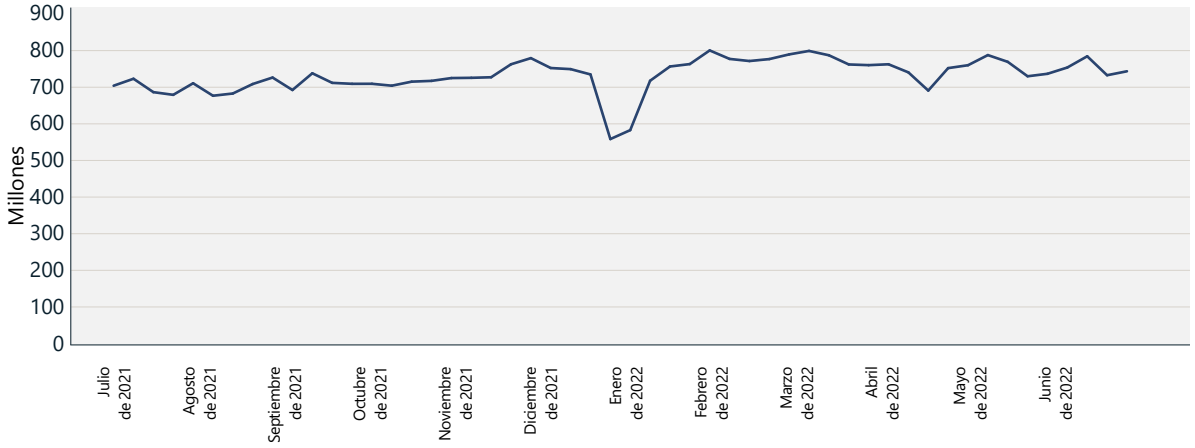
Además de las campañas con objetivos más amplios, el phishing de credenciales, las donaciones y la información personal, los atacantes dirigen sus ataques a empresas específicas para conseguir un mayor desembolso. Los ataques de phishing por correo electrónico dirigidos a empresas para obtener ganancias financieras se denominan conjuntamente «ataques BEC». Microsoft detecta millones de correos electrónicos de BEC cada mes, equivalentes al 0,6 por ciento de todos los correos electrónicos de phishing observados. Un informe del IC3[18] publicado en mayo de 2022 indica una tendencia al alza en las pérdidas expuestas por ataques BEC.

Las técnicas utilizadas en los ataques de phishing siguen aumentando en complejidad. En respuesta a las contramedidas, los atacantes encuentran nuevas formas de implementar sus técnicas y aumentan la complejidad en la forma y el lugar en el que alojan la infraestructura operativa de sus campañas. Esto significa que las organizaciones deben reevaluar periódicamente su estrategia para implementar soluciones de seguridad con el fin de bloquear correos electrónicos malintencionados y reforzar el control de acceso para las cuentas de usuario individuales.

531 000

Además de las direcciones URL bloqueadas por Defender for Office, nuestra Unidad de delitos digitales dirigió el desmantelamiento de 531 000 direcciones URL de phishing distintas alojadas fuera de Microsoft.

Correos electrónicos de phishing detectados



El número de detecciones de ataques de phishing a la semana sigue aumentando. La disminución entre diciembre y enero es una caída estacional prevista, que también se registró en el informe del año pasado. Fuente: Señales de Exchange Online Protection.

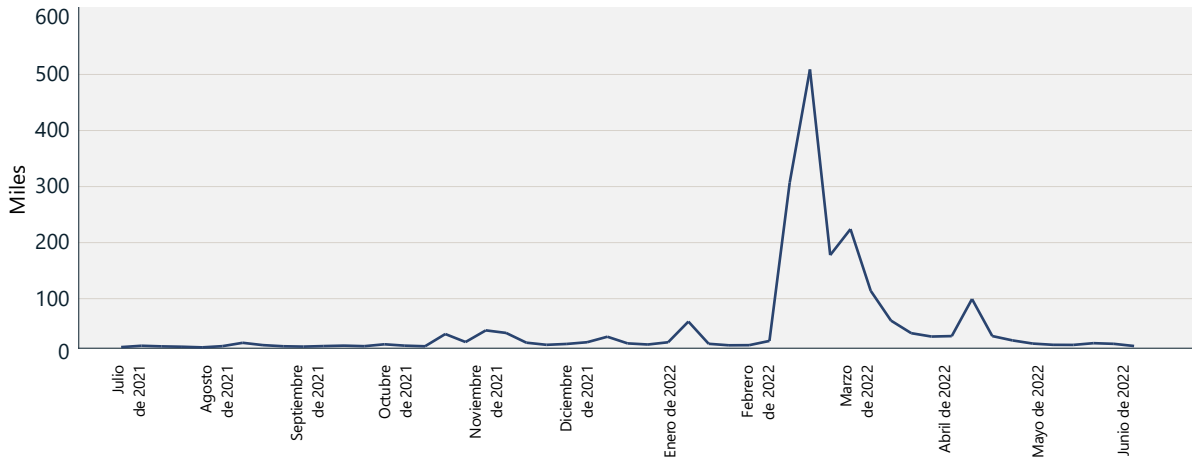
El cambiante panorama de las amenazas de phishing

Continuación

Seguimos observando un aumento constante año tras año de los correos electrónicos de phishing. El cambio al teletrabajo de 2020 y 2021 supuso un aumento importante de los ataques de phishing con el objetivo de aprovechar el cambiante entorno de trabajo. Los operadores de ataques de phishing adoptan rápidamente nuevas plantillas de correo electrónico mediante señuelos acordes con los principales acontecimientos mundiales, como la pandemia de COVID-19, y los temas vinculados a herramientas de colaboración y productividad como el intercambio de archivos en Google Drive u OneDrive. Aunque los temas relacionados con la COVID-19 han disminuido, la guerra de Ucrania se convirtió en un nuevo señuelo desde principios de marzo de 2022. Nuestros investigadores observaron un asombroso aumento de correos electrónicos que se hacían pasar por organizaciones legítimas en los que se solicitaban donaciones en las criptomonedas Bitcoin y Ethereum, supuestamente para apoyar a los ciudadanos ucranianos.

Solo unos días después del inicio de la guerra en Ucrania a finales de febrero de 2022, el número de correos electrónicos de phishing detectados que contenían direcciones Ethereum encontrados entre clientes de empresa aumentó drásticamente. El total de encuentros alcanzó su punto máximo en la primera semana de marzo, cuando medio millón de correos electrónicos de phishing contenían una dirección de la cartera Ethereum. Antes del inicio de la guerra, el número de direcciones de la cartera Ethereum en otros correos electrónicos detectados como phishing era considerablemente menor, con una media de pocos miles de correos electrónicos al día.

Correos electrónicos de phishing con direcciones de la cartera Ethereum



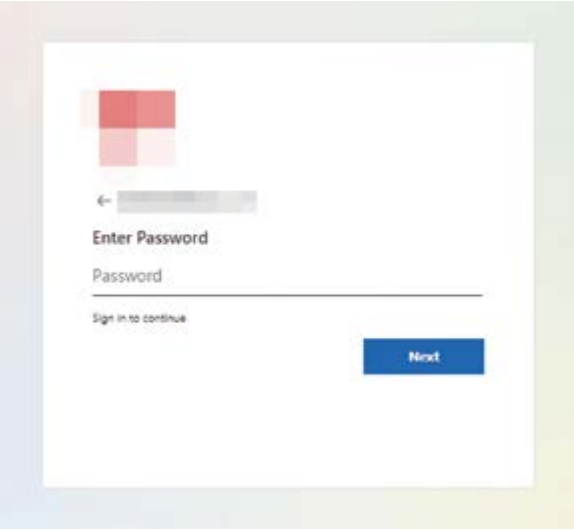
El total de correos electrónicos detectados como phishing que contenían direcciones de la cartera Ethereum aumentó al inicio del conflicto ucraniano-ruso y fue disminuyendo tras el inicio de la invasión.

Más que nunca, los suplantadores de identidad («phishers») se aprovechan de una infraestructura legítima para operar, lo que justifica el aumento de las campañas de phishing destinadas a atacar varios aspectos de una operación para que no tengan que comprar, alojar o operar las suyas propias. Por ejemplo, los correos electrónicos malintencionados pueden proceder de cuentas de remitente pirateadas. Los atacantes se benefician del uso de estas direcciones de correo electrónico que gozan de mayor reputación y se las considera más fiables que las cuentas y dominios recién creados. En algunas campañas de phishing más avanzadas, observamos cómo los atacantes prefieren enviar correos electrónicos de suplantación de identidad desde dominios que tienen la autenticación de correo electrónico (DMARC)[19] configurada incorrectamente con una política de «no hacer nada», lo que abre las puertas a la suplantación («spoofing») por correo electrónico.

Las grandes operaciones de phishing suelen utilizar servicios en el cloud y máquinas virtuales (VM) en el cloud para perpetrar ataques a gran escala. Los atacantes pueden automatizar completamente el proceso de implementación y entrega de correos electrónicos desde máquinas virtuales mediante retransmisiones de correo electrónico SMTP o infraestructura de correo electrónico en el cloud para beneficiarse del alto porcentaje de entrega y la reputación positiva de estos servicios legítimos. Si se permite el envío de correo electrónico malintencionado a través de estos servicios en el cloud, los defensores deben emplear sólidas funciones de filtrado de correo electrónico para impedir que los correos electrónicos entren en su entorno.

Las cuentas de Microsoft siguen siendo un objetivo prioritario para los operadores de phishing, como queda demostrado por las numerosas páginas de aterrizaje de phishing que se hacen pasar por la página de inicio de sesión de Microsoft 365. Por ejemplo, los phishers intentan simular la experiencia de inicio de sesión de Microsoft en sus kits de phishing generando una URL única personalizada para el destinatario. Esta URL apunta a una página web malintencionada desarrollada para obtener las credenciales, pero un parámetro de la URL contendrá la dirección de correo electrónico del destinatario específico. Una vez que el objetivo acceda a la página, el kit de phishing rellenará previamente los datos de inicio de sesión de los usuarios e incluirá un logotipo corporativo personalizado para el destinatario del correo electrónico, con el objetivo de imitar el aspecto de la página de inicio de sesión personalizada de Microsoft 365 de la empresa objetivo.

Página de phishing suplantando el inicio de sesión de Microsoft con contenido dinámico

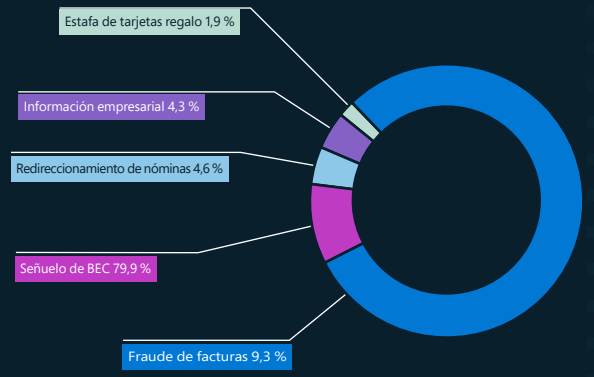


Aspectos destacados de los ataques al correo electrónico empresarial

Los ciberdelincuentes están desarrollando métodos y técnicas cada vez más complejos para eludir los ajustes de seguridad y dirigir sus ataques a particulares, empresas y organizaciones. En respuesta a ello, estamos invirtiendo importantes recursos para mejorar aún más nuestro programa de cumplimiento de BEC.

BEC es la ciberdelincuencia financiera más costosa, con una estimación de 2400 millones de dólares en pérdidas ajustadas en 2021, lo que representa más del 59 por ciento de las cinco principales pérdidas globales por delitos en Internet.[20] Para entender el alcance del problema y la mejor manera de proteger a los usuarios contra los ataques BEC, los investigadores de seguridad de Microsoft han realizado un seguimiento de los temas más comunes utilizados en los ataques.

Temas de BEC (de enero a junio de 2022)



Temas de BEC por porcentaje de aparición

Tendencias de BEC

Como punto de entrada, los atacantes de BEC intentan normalmente iniciar una conversación con las víctimas potenciales para establecer una relación. Haciéndose pasar por un colega o compañero de trabajo, el atacante dirige gradualmente la conversación hacia una transferencia monetaria. El correo electrónico de introducción, que rastreamos como un señuelo de BEC, representa cerca del 80 por ciento de los correos electrónicos de BEC detectados. Otras tendencias identificadas por los investigadores de seguridad de Microsoft en el último año son:

- Las técnicas más utilizadas en los ataques BEC observados en 2022 fueron el «spoofing»[21] y la suplantación.[22]
- El subtipo de BEC que causó más daños financieros a las víctimas fue el fraude en facturas (de acuerdo con el volumen y las cantidades en dólares solicitadas registradas en nuestras investigaciones de campañas de BEC).
- El robo de información empresarial, como informes de proveedores y contactos de clientes, permite a los atacantes elaborar fraudes convincentes en las facturas.
- La mayoría de las solicitudes de redirección de nóminas se enviaron desde servicios de correo electrónico gratuitos y rara vez desde cuentas pirateadas. El volumen de correo electrónico procedente de estas fuentes aumentó en torno al primer y el décimo día de cada mes, las fechas de pago más comunes.
- A pesar de ser vías de fraude conocidas, las estafas con tarjetas de regalo comprenden solo el 1,9 por ciento de los ataques de BEC detectados.

Conocimientos prácticos
Defensa contra el phishing

Para reducir la exposición de tu organización al phishing, se recomienda a los administradores de TI que implementen las siguientes políticas y características:

1. Exigir el uso de MFA en todas las cuentas para limitar el acceso no autorizado.
2. Habilitar funciones de acceso condicional para las cuentas con privilegios elevados para bloquear el acceso desde países, regiones y direcciones IP que normalmente no generan tráfico en tu organización.
3. Considerar la posibilidad de usar llaves de seguridad físicas para ejecutivos, empleados que participan en actividades de pago o compra y otras cuentas con privilegios.
4. Exigir el uso de navegadores con servicios de soporte como Microsoft SmartScreen para analizar las direcciones URL en busca de comportamientos sospechosos y bloquear el acceso a sitios web maliciosos conocidos.[23]
5. Usar una solución de seguridad basada en machine learning que ponga en cuarentena los mensajes con una alta probabilidad de ser correo de phishing y colocar las URL y los archivos adjuntos en un sandbox antes de que el correo electrónico llegue a la bandeja de entrada, como Microsoft Defender para Office 365.[24]
6. Habilitar las funciones de protección de suplantación y «spoofing» en toda la organización.
7. Configurar las políticas de acción DomainKeys Identified Mail (DKIM) y Domain-based Message Authentication Reporting & Conformance (DMREA) para evitar la entrega de correos electrónicos no autenticados que podrían suplantar la identidad de remitentes de confianza.
8. Auditar las reglas de permisos para crear inquilinos y usuarios y eliminar las excepciones generalizadas basadas en el dominio y la dirección IP. Estas reglas suelen tener prioridad y pueden permitir correos electrónicos malintencionados conocidos a través del filtrado de correo electrónico.
9. Ejecutar periódicamente simuladores de phishing para medir el riesgo potencial en toda la organización y para identificar y formar a los usuarios vulnerables.

Enlaces a información adicional (pueden estar en inglés)

- Desde el robo de cookies hasta BEC: los atacantes utilizan sitios de phishing de AiTM como punto de entrada para los fraudes financieros | Equipo de investigación de Microsoft 365 Defender, Centro de inteligencia sobre amenazas de Microsoft (MSTIC)

Engaños mediante homoglifos

Los ataques BEC y el phishing son tácticas comunes de ingeniería social. La ingeniería social desempeña un papel importante en la delincuencia y consiste en persuadir a un objetivo para que interactúe con el delincuente ganándose su confianza.

En el comercio físico, se utilizan las marcas comerciales para ganarse la confianza en el origen de un producto o servicio y la falsificación de productos es una vulneración de la marca comercial. Del mismo modo, los ciberdelincuentes se hacen pasar por un contacto que el objetivo conoce durante un ataque de phishing, utilizando homoglifos para engañar a las posibles víctimas.

Un homoglifo es un nombre de dominio utilizado para la comunicación por correo electrónico en los ataques BEC, en el que un carácter se sustituye por otro que es idéntico o casi idéntico en cuanto a su aspecto, con el fin de engañar a la víctima.

Técnicas de homoglifo utilizadas en los intentos de ataques BEC

Los ataques BEC generalmente tienen dos fases, la primera de las cuales implica la obtención de credenciales. Estos tipos de filtración de credenciales pueden ser el resultado de ataques de phishing o grandes filtraciones de datos. A continuación, las credenciales se venden o comercializan en la «dark web».

La segunda fase es la fase del fraude, en la que los atacantes utilizan las credenciales obtenidas para realizar un ataque sofisticado de ingeniería social empleando dominios de correo electrónico homoglifos.

Progresión de un ataque BEC

Técnica	% de dominios que muestran la técnica de homoglifo
sustituir l por I	25 %
sustituir i por l	12 %
sustituir q por g	7 %
sustituir rn por m	6 %
sustituir .cam por .com	6 %
sustituir 0 por o	5 %
sustituir ll por l	3 %
sustituir ii por i	2 %
sustituir vv por w	2 %
sustituir l por ll	2 %
sustituir e por a	2 %
sustituir nn por m	1 %
sustituir ll por I, sustituir l por i	1 %
sustituir o por u	1 %

Análisis de más de 1700 dominios homoglifos entre enero y julio de 2022. Aunque se utilizaron 170 técnicas de dominios homoglifos, el 75 % de los dominios solo utilizó 14 técnicas.

Un homoglifo en acción

Un dominio homoglifo que es idéntico a un dominio de correo que la víctima reconoce se registra en un proveedor de correo con un nombre de usuario idéntico. A continuación, se envía un correo electrónico desde el dominio secuestrado con nuevas instrucciones de pago.

Utilizando la inteligencia de código abierto y el acceso a las conversaciones de correo electrónico, el delincuente identifica a las personas que son responsables de la facturación y los pagos. A continuación, crean una suplantación de una dirección de correo electrónico de la persona que envía las facturas. Esta suplantación se compone de un nombre de usuario idéntico y un dominio de correo idéntico homoglifo del remitente original.

El atacante copia una cadena de correo electrónico que contiene una factura legítima y luego cambia la factura para incluir sus propios datos bancarios. Esta nueva factura modificada se vuelve a enviar desde el correo electrónico de suplantación homoglifo a la víctima. Como el contexto tiene sentido y el correo electrónico parece auténtico, a menudo la víctima sigue las instrucciones fraudulentas.

Conocimientos prácticos

1. Exige el uso de navegadores que admitan servicios para analizar las direcciones URL en busca de comportamientos sospechosos y bloqueen el acceso a sitios web maliciosos conocidos como Safe Links y SmartScreen.[25]
2. Usa una solución de seguridad basada en machine learning que ponga en cuarentena los mensajes con una alta probabilidad de ser correo de phishing y que coloque las URL y los archivos adjuntos en un sandbox antes de que el correo electrónico llegue a la bandeja de entrada.

Enlaces a información adicional (pueden estar en inglés)

- Centro de quejas de delitos de Internet (IC3) | Ataque al correo electrónico empresarial: una estafa de 43 000 millones de dólares
- Conocimientos de inteligencia de «spoofing»: Office 365 | Microsoft Docs
- Conocimientos de suplantación: Office 365 | Microsoft Docs

Una línea cronológica del desmantelamiento de botnets desde los primeros días de colaboración de Microsoft

Durante más de una década, la DCU ha trabajado para detener proactivamente los delitos cibernéticos, lo que ha permitido el desmantelamiento de 26 ataques de malware y de los estados nación. Conforme el equipo de DCU utiliza tácticas y herramientas más avanzadas para cerrar estas operaciones ilícitas, vemos que los ciberdelincuentes también desarrollan sus enfoques en un intento de mantenerse un paso por delante. A continuación presentamos una línea cronológica que muestra un ejemplo de las botnets desmanteladas por la DCU y las estrategias adoptadas por Microsoft para cerrarlas.

2008

Botnet Conficker

Descripción: un gusano de rápida propagación dirigido al sistema operativo Windows, que infectó millones de ordenadores y dispositivos de una red común; creó interrupciones de red en todo el mundo.

Colaboración: formación del grupo de trabajo Conficker, el primer consorcio de este tipo. Microsoft se asoció con 16 organizaciones de todo el mundo para derrotar al bot.

Respuesta de Microsoft: el grupo colaboró con muchas jurisdicciones internacionales y pudo desmantelar la botnet Conficker.

2009

Botnet Waledac

Descripción: una compleja botnet de spam con dominios de EE. UU. que recopiló direcciones de correo electrónico y distribuyó spam que infectó a 90 000 ordenadores en todo el mundo.[26]

Colaboración: creación de otro consorcio, el Centro de protección contra malware de Microsoft (MMPC, por sus siglas en inglés), con el objetivo de trabajar en estrecha colaboración con el mundo académico.[27]

Respuesta de Microsoft: Microsoft usó el enfoque de desmantelamiento escalonado de C2 y sorprendió a los agentes malintencionados incautando dominios con sede en los EE. UU. sin previo aviso.[28] Microsoft se hizo temporalmente con la propiedad de casi 280 dominios utilizados por los servidores de Waledac.

2011

Se forma la Unidad de delitos digitales de Microsoft

Colaboración: diseñada para frustrar la ciberdelincuencia que afecta al ecosistema de Microsoft a través de una estrecha integración entre un equipo de investigadores, abogados e ingenieros.

Enfoque de Microsoft: el objetivo es conocer mejor los aspectos técnicos de algunos ataques de malware y proporcionar estos conocimientos al equipo jurídico de Microsoft para desarrollar una estrategia de desmantelamiento eficaz.

2013

Botnet Rustock

Descripción: un bot de correo electrónico de spam en forma de troyano de puerta trasera que usó proveedores de Internet como infraestructura C2 principal; diseñado para vender productos farmacéuticos.

Colaboración: Microsoft forjó una asociación con Pfizer Pharmaceuticals para conocer los medicamentos vendidos por Rustock y trabajó en estrecha colaboración con agentes de la policía holandesa.[29]

Respuesta de Microsoft: Microsoft trabajó con los marshall de EE. UU. y la policía de los Países Bajos para desmantelar los servidores C2 en ese país. Registró y bloqueó todos los algoritmos futuros de generadores de dominios (DGA).

Botnet Sirefef/Zero Access

Descripción: una botnet publicitaria diseñada para dirigir a las personas a sitios web peligrosos que instalaba malware o robaba información personal; infectó a más de dos millones de ordenadores y costó a los anunciantes más de 2,7 millones de dólares al mes; principalmente en EE. UU. y Europa Occidental.

Colaboración: trabajó en estrecha colaboración con el FBI y el centro de delitos informáticos de la Europol para desmantelar la infraestructura punto a punto.

Respuesta de Microsoft: se incorporó a la red Zero Access, reemplazó los servidores C2 de los delincuentes y logró desmantelar los dominios del servidor de descarga.

2019

Botnet Trickbot

Descripción: una botnet sofisticada con infraestructura fragmentada en todo el mundo que dirigió sus ataques al sector de los servicios financieros; dispositivos IoT atacados.

Colaboración: Microsoft se asoció con Financial Services Information Sharing and Analysis Center (FS-ISAC) para desmantelar la botnet Trickbot.[30]

Respuesta de Microsoft: la DCU creó un sistema para identificar y rastrear la infraestructura del bot y generó notificaciones para los proveedores activos de Internet, respetando las leyes específicas de los distintos países.

2022

Enfoque continuado en el desmantelamiento

Descripción: Microsoft desmanteló la infraestructura de siete actores de amenazas en el último año, lo que evitó que distribuyeran malware adicional, controlaran los ordenadores de las víctimas y dirigieran sus ataques a otras víctimas.

Colaboración: en asociación con proveedores de servicios de Internet, gobiernos, fuerzas del orden y el sector privado, Microsoft compartió información para remediar a más de 17 millones de víctimas de malware en todo el mundo.

Perspectivas futuras

La DCU sigue innovando y su deseo es usar su experiencia en el desmantelamiento de botnets para llevar a cabo operaciones coordinadas que no se limiten al malware. Nuestro éxito continuo requiere ingeniería creativa, intercambio de información, teorías jurídicas innovadoras y asociaciones públicas y privadas.

Explotación de la infraestructura por parte de los ciberdelincuentes

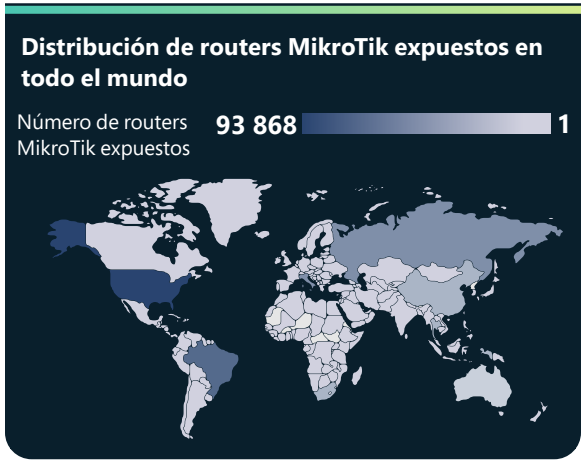
Puertas de enlace de Internet como infraestructura de mando y control para los delincuentes

Los dispositivos IoT son un objetivo cada vez más popular para los ciberdelincuentes que usan botnets de uso general. Cuando los routers no están actualizados y se exponen directamente a Internet, los actores de amenazas pueden utilizarlos para obtener acceso a las redes, perpetrar ataques malintencionados e incluso respaldar sus operaciones.

El equipo de Microsoft Defender para IoT investiga los equipos, que abarcan desde controladores de sistemas de control industrial heredados hasta sensores de IoT de última generación. El equipo investiga el malware específico del IoT y OT para incluirlo en la lista compartida de indicadores de riesgo.

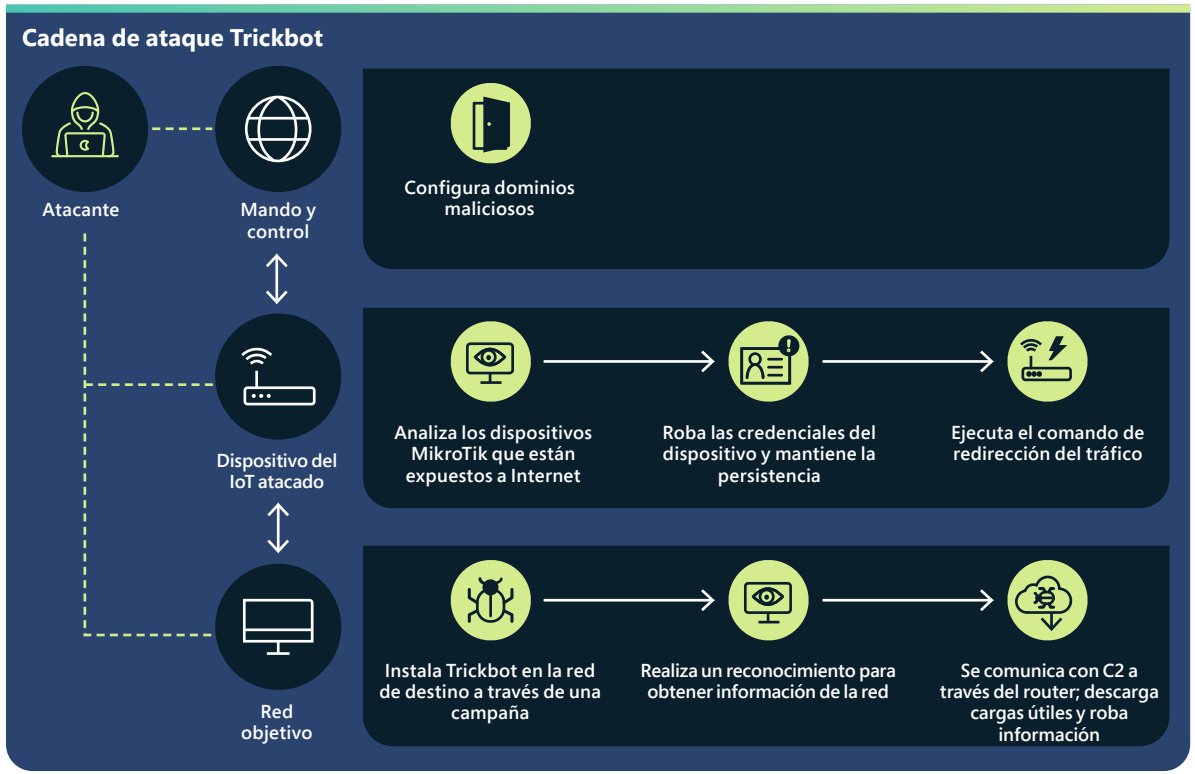
Los routers son vectores de ataque especialmente vulnerables porque están en todos los hogares y organizaciones con conexión a Internet. Hemos rastreado la actividad de los routers MikroTik, un router popular en todo el mundo tanto en hogares como en empresas, para identificar cómo se utilizan para el mando y el control (C2), para los ataques del sistema de nombres de dominio (DNS) y para la piratería de minería de criptomonedas.

Más concretamente, hemos identificado cómo los operadores Trickbot utilizan routers MikroTik atacados y los reconfiguran para usarlos como parte de su infraestructura C2. La popularidad de estos dispositivos recrudece la gravedad de su uso por parte de Trickbot, y su hardware y software únicos permiten a los actores de amenazas eludir las medidas de seguridad tradicionales, ampliar su infraestructura y atacar más dispositivos y redes.



Los routers expuestos corren el riesgo de sufrir vulnerabilidades potenciales.

Al rastrear y analizar el tráfico que contiene comandos del shell seguro (SSH), observamos cómo los atacantes usan los routers MikroTik para comunicarse con la infraestructura de Trickbot después de obtener credenciales legítimas para acceder a los dispositivos. Estas credenciales se pueden obtener mediante ataques de fuerza bruta, el aprovechamiento de vulnerabilidades conocidas con parches fácilmente disponibles y el uso de contraseñas predeterminadas. Una vez que se accede a un dispositivo, el atacante emite un comando único que redirige el tráfico entre dos puertos del router, estableciendo la línea de comunicación entre los dispositivos afectados por Trickbot y el C2.



Cadena de ataque Trickbot que muestra el uso de dispositivos IoT de MikroTik como servidores proxy para C2.

Hemos incluido nuestro conocimiento de los diversos métodos de ataque a dispositivos MikroTik, además de Trickbot, así como las vulnerabilidades y exposiciones comunes conocidas (CVE) en una herramienta de código abierto para dispositivos MikroTik, que puede extraer los artefactos forenses relacionados con los ataques a estos dispositivos.[31]

Los dispositivos que actúan como proxies inversos para el C2 de malware no son solo exclusivos de los routers Trickbot y MikroTik. En colaboración con el equipo RiskIQ de Microsoft, hemos rastreado todo el proceso hasta el C2 y, mediante la observación de los certificados SSL, hemos identificado los dispositivos Ubiquiti y LigoWave que también se han visto afectados.[32] Esta es una indicación clara de que los dispositivos IoT se están convirtiendo en componentes activos de ataques coordinados por los estados nación y un objetivo popular para los ciberdelincuentes que utilizan botnets de uso general.

Delincuentes de criptomonedas que explotan los dispositivos de IoT

Los dispositivos de puerta de enlace son un objetivo cada vez más valioso para los actores de amenazas, ya que el número de vulnerabilidades conocidas ha crecido constantemente año tras año. Se están utilizando para la minería de criptomonedas y otros tipos de actividades maliciosas.

A medida que las criptomonedas se han vuelto más populares, muchas personas y organizaciones han invertido en potencia informática y recursos de red de dispositivos como enrutadores para realizar minería de criptomonedas en el blockchain. Sin embargo, la minería de criptomonedas es un proceso que consume mucho tiempo y recursos con poca probabilidad de éxito. Para aumentar las probabilidades de éxito, los mineros se reúnen en redes distribuidas y cooperativas, recibiendo hashes relacionados con el porcentaje de la moneda que lograron extraer con sus recursos conectados.

El año pasado Microsoft observó un número creciente de ataques que explotaban los routers para redirigir los esfuerzos de minería de criptomonedas. Los ciberdelincuentes atacan los routers conectados a los grupos de minería y redirigen el tráfico de minería a sus direcciones IP asociadas con ataques de envenenamiento de DNS, lo que altera la configuración de DNS de los dispositivos objetivo. Los routers afectados registran la dirección IP incorrecta en un nombre de dominio determinado y envían sus recursos de minería (o hashes) a los grupos utilizados por los actores de amenazas. Estos grupos podrían extraer criptomonedas anónimas asociadas con actividades delictivas o utilizar hashes legítimos generados por los mineros para adquirir un porcentaje de la moneda que han extraído y obtener así su recompensa.

Puesto que la mitad de las vulnerabilidades conocidas detectadas en 2021 se debieron a la falta de parches, la actualización y la protección de los routers en las redes corporativas y privadas sigue siendo un desafío importante para los propietarios y administradores de dispositivos.

Ataque de dispositivos para la minería ilegal de criptomonedas

Los agentes de amenazas roban parte de los hashes del grupo original o trans-fieren recursos a su grupo, o los routers tienen malware que roban recursos para la minería.

El envenenamiento de DNS de dispositivos de puerta de enlace se aprovecha de actividades legítimas de minería y redirige los recursos a actividades de minería delictivas.

Las máquinas virtuales como infraestructura delictiva

La migración generalizada al cloud incluye a los ciberdelincuentes que aprovechan los activos privados de víctimas involuntarias obtenidos a través de phishing o distribución de programas de malware de interceptación de credenciales. Muchos ciberdelincuentes están optando por configurar sus infraestructuras malintencionadas en máquinas virtuales (VM), contenedores y microservicios basados en el cloud.

Una vez que el ciberdelincuente tiene acceso, puede producirse una secuencia de eventos para configurar la infraestructura, como una serie de máquinas virtuales a través de scripts y procesos automatizados. Estos procesos automatizados con scripts se utilizan para lanzar actividades maliciosas, incluidos ataques de spam por correo electrónico a gran escala, ataques de phishing y páginas web que alojan contenido malintencionado. Incluso pueden incluir la configuración de un entorno virtual a escala que realice la minería de criptomonedas, provocando que la víctima reciba una factura de cientos de miles de dólares a final de mes.

Los ciberdelincuentes saben que su actividad maliciosa tiene una duración limitada antes de que se detecte y se cierre. Por consiguiente, han escalado sus operaciones y ahora trabajan de forma proactiva conscientes de las contingencias. Se ha observado que preparan las cuentas pirateadas con antelación y supervisan sus entornos. En cuanto detectan una cuenta (configurada con cientos de miles de máquinas virtuales), pasan a la siguiente cuenta (ya preparada por scripts para que se active inmediatamente) y su actividad malintencionada continúa con poca o ninguna interrupción.

Al igual que la infraestructura en el cloud, la infraestructura on-premises se puede utilizar en ataques con entornos locales virtuales desconocidos para el usuario on-premises. Esto requiere que el punto de acceso inicial permanezca abierto y accesible. Los ciberdelincuentes también han explotado activos privados on-premises para iniciar una nueva cadena de infraestructura en el cloud, configurada para ocultar su origen con el fin de evitar la detección de creación de infraestructura sospechosa.

Conocimientos prácticos

1. Implementa una buena higiene cibernética y proporciona formación en ciberseguridad a los empleados con directrices para evitar que se conviertan en víctimas de un ataque de ingeniería social.
2. Realiza comprobaciones automáticas periódicas de anomalías de la actividad de los usuarios mediante detecciones a escala para ayudar a reducir este tipo de ataques.
3. Actualiza y protege los routers en redes corporativas y privadas.

¿El hacktivismo ha llegado para quedarse?

Aunque el hacktivismo no es un fenómeno nuevo, la guerra en Ucrania ha supuesto un aumento de los hackers voluntarios, incluidos algunos dirigidos por los gobiernos para desplegar herramientas cibernéticas con el fin de dañar la reputación o los activos de los opositores políticos, organizaciones e incluso estados nación.

En febrero de 2022, el gobierno ucraniano pidió a ciudadanos amateur privados de todo el mundo que perpetraran ciberataques en Rusia como parte de su poderoso «ejército informático» con 300 000 miembros.[33] Al mismo tiempo, grupos de hacktivistas establecidos como Anonymous, Ghostsec, Against the West, Belarusian Cyber Partisans y RaidForum2 comenzaron a perpetrar ataques en apoyo de Ucrania. Otros grupos, incluidos algunos de la banda de ransomware Conti, se pusieron del lado de Rusia.[34]

En los meses siguientes, las actividades de Anonymous fueron muy visibles. Los hackers que actuaban en nombre del grupo, o en el de uno de sus afiliados, desactivaron temporalmente miles de sitios web rusos y ucranianos, filtraron cientos de gigabytes de datos robados, hackearon los canales de televisión rusos para reproducir contenido a favor de Ucrania e incluso se ofrecieron a pagar en bitcoins los tanques rusos conquistados.

El auge de los hackers amateur

Las plataformas de redes sociales permitieron la organización y movilización rápidas de miles de hackers amateur, a quienes se les proporcionaron indicaciones para perpetrar ataques de fácil ejecución, como los ataques DDoS. Los organizadores aprovecharon Twitter, Telegram y foros privados para reunir a los hackers, organizar las operaciones y difundir manuales de instrucción de piratería informática.

Sin embargo, es probable que la mayoría de estos hackers tuvieran conocimientos limitados, incluso con instrucciones. Esto sugiere dos escenarios posibles: que cientos o miles de personas con conocimientos técnicos rudimentarios utilicen plantillas de ataque para perpetrar ataques hacktivistas futuros coordinados o individuales contra objetivos o que el final de las hostilidades en Ucrania acabe con su hacktivismo, al menos hasta que el siguiente acontecimiento social o político les inste a actuar.

Politización de los hackers

El mayor riesgo que representa esta movilización política es la implementación de hackers expertos en tecnología que podrían seguir perpetrando ciberataques contra objetivos de gobiernos extranjeros para apoyar sus propias prioridades nacionales, ya sea por iniciativa propia o a instancias de su gobierno.

Irán, China y Rusia ya utilizan el hacktivismo como fuente de contratación de sus grupos de piratería estatales. Por ejemplo, en abril de 2022, el grupo de hacking prorruso Killnet lanzó ataques DDoS contra ferrocarriles checos, aeropuertos regionales y el servidor del servicio civil checo, a pesar de que la República Checa no está directamente involucrada en la guerra.[35] Al mismo tiempo, algunos gobiernos podrían utilizar el hacktivismo como una cobertura para las operaciones tradicionales de ciberespionaje o sabotaje, como las actividades iraníes contra Israel.

En un entorno en el que los ataques DDoS vinculados al hacktivismo ha aumentado, a la industria tecnológica le resulta difícil descifrar rápidamente la diferencia entre el flujo de tráfico normal y anormal a un sitio web. Microsoft y sus partners han desarrollado un conjunto de herramientas que distinguen el tráfico DDoS malintencionado y lo rastrean hasta su origen. Asimismo, la plataforma Azure de Microsoft puede identificar máquinas en la plataforma que producen niveles extraordinariamente altos de tráfico de salida y cerrarlos.

La aparición del «protestware»

El «protestware» ha surgido como el resultado directo de las reacciones emocionales a la guerra entre Rusia y Ucrania. Algunos desarrolladores de software de código abierto utilizaron la popularidad de su software como un medio de expresión o actuación ante una situación geopolítica en desarrollo. Esto incluía archivos de texto inofensivos abiertos en un escritorio o un navegador para difundir mensajes de paz, pero también ataques dirigidos basados en la geolocalización de direcciones IP y acciones destructivas como la limpieza de un disco duro. Cuando se produzcan otros acontecimientos mundiales, cabe esperar que en el futuro veamos el resurgir del «protestware». Dado que, por lo general, se trata de casos en los que mantenedores de código abierto muy respetados deciden hacer declaraciones personales utilizando sus propios componentes de código abierto, actualmente no existe ninguna protección para impedir que se produzca este tipo de cambios en los paquetes de archivos de origen y los usuarios deben conocer su impacto potencial.

Las plataformas de redes sociales permitieron la organización y movilización de miles de hackers amateur, a quienes se les proporcionaron indicaciones para perpetrar ataques de fácil ejecución, como los ataques DDoS.

Conocimientos prácticos

1. El sector tecnológico debe reunirse para diseñar una respuesta integral a esta nueva amenaza.
2. Las principales empresas de tecnología, incluida Microsoft, tienen herramientas para identificar el tráfico malintencionado asociado con ataques DDoS y deshabilitar las máquinas responsables.
3. Los usuarios de código abierto deben estar especialmente vigilantes durante los momentos de conflictos geopolíticos.

Notas al pie

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. Detección y respuesta de puntos de conexión. https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. Un foro validado es un foro de debate online que requiere que un miembro existente avale la incorporación de un nuevo miembro.
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. Fuente de datos: Defender for Office (correo electrónico malintencionado/actividad de identidades atacadas), Azure Active Directory Identity Protection (eventos/alertas de identidades atacadas), Defender for Cloud Apps (eventos de acceso a datos de identidades atacadas) y M365D (relación de productos).
17. Fuente de datos: Defender para punto de conexión (alertas/eventos de comportamiento de ataque), Defender for Office (correo electrónico malintencionado) y M365D (relación de productos).
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. Autenticación de mensajes basada en dominio, informes y conformidad: un protocolo de autenticación, política e información diseñado para ofrecer a los propietarios de dominios de correo electrónico la capacidad de proteger su dominio del uso no autorizado.
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., n.º 1:10CV156, (E.D.Va. 22 de febrero de 2010).
27. Véase Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., 27 de septiembre de 2011.
28. En concreto, el artículo 65 del Reglamento Federal de Procedimientos Civiles permite a una parte utilizar dicho recurso si: 1) la parte sufrirá daños inmediatos e irreparables si no se concede la ayuda y 2) la parte intenta notificar a la otra parte puntualmente. Además, la ley exige que se aplique una prueba de equilibrio, que equilibra el derecho del acusado de notificar públicamente el alcance del daño.
29. Microsoft Corporation v. John Does 1-11, et. al., n.º 2:11cv222, (W.D. Wa. 9 de febrero de 2011).
30. Microsoft Corp. v. Does, n.º 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D. Va. 12 de agosto de 2021).
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

Amenazas de los estados nación

Los agentes de los Estados nación están lanzando ciberataques cada vez más sofisticados para eludir la detección y avanzar en sus prioridades estratégicas.

Información general de las amenazas de los Estados nación

Los agentes de los Estados nación están lanzando ciberataques cada vez más sofisticados para eludir la detección y avanzar en sus prioridades estratégicas. La implementación de ciberamenazas en la guerra híbrida de Ucrania marca el comienzo de una nueva era de conflictos.

Rusia también ha apoyado su guerra con operaciones de influencia propagandística, utilizando la tecnología para influir en las opiniones de Rusia, Ucrania y todo el mundo. Este primer conflicto híbrido a gran escala nos ha enseñado otras lecciones importantes. En primer lugar, las medidas de seguridad de las operaciones digitales y los datos se pueden mejorar, tanto en el ciberespacio como en el espacio físico, migrándolas al cloud. Los ataques iniciales rusos se dirigieron a servicios on-premises con malware «wiper» y centros de datos físicos específicos cuando se lanzaron los primeros misiles.

Ucrania respondió migrando rápidamente cargas de trabajo y datos a clouds a hiperescala alojados en centros de datos fuera de Ucrania. En segundo lugar, los avances en inteligencia sobre amenazas cibernéticas y protección de puntos de conexión basados en los datos y los servicios avanzados de IA y ML en el cloud han ayudado a Ucrania a defenderse de los ciberataques rusos.

En otros países, los agentes de los estados nación han aumentado su actividad y utilizan los avances en automatización, infraestructura en el cloud y tecnologías de acceso remoto para atacar a un conjunto más amplio de objetivos. Las cadenas de suministro de TI corporativas que permiten el acceso a objetivos finales han sido atacadas con frecuencia. La higiene de ciberseguridad cobró aún más importancia, ya que los agentes aprovecharon rápidamente las vulnerabilidades sin parches, utilizaron técnicas sofisticadas y de fuerza bruta para robar credenciales y ocultaron sus operaciones mediante el uso de software legítimo o de código abierto. E Irán se suma a Rusia en el uso de armas cibernéticas destructivas, incluido el ransomware, como la materia prima de sus ataques.

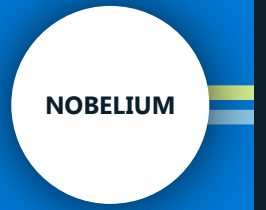
Estos desarrollos requieren una adopción urgente de un marco global coherente que priorice los derechos humanos y proteja a las personas del comportamiento online irresponsable de los países. Todas las naciones deben trabajar juntas para implantar normas y reglas de común acuerdo que establezcan una conducta de estado responsable.

Defensa de Ucrania: lecciones tempranas de la guerra cibernética: Microsoft On the Issues

Ampliación de los ataques a las infraestructuras críticas, en particular el sector de TI, los servicios financieros, los sistemas de transporte y la infraestructura de comunicaciones.

Más información en la página 35

Cadena de suministro de TI que se utiliza como puerta de enlace para acceder a los objetivos.



Más información en la página 36

Ampliación de los ataques globales de China, especialmente a las naciones más pequeñas del Sudeste Asiático, para obtener inteligencia y una ventaja competitiva.

Más información en la página 44

Tras el cambio de poder, Irán adoptó una postura más agresiva, amplió los ataques de ransomware más allá de los adversarios regionales a las víctimas de Estados Unidos y la UE, y dirigió sus ataques a infraestructuras críticas estadounidenses de alto perfil.

Más información en la página 46

La identificación y la rápida explotación de vulnerabilidades no identificadas se ha convertido en una táctica clave. La rápida implementación de actualizaciones de seguridad es clave para la defensa.

Más información en la página 39

Corea del Norte dirige sus ataques a compañías de defensa y aeroespacial, criptomonedas, canales de noticias, disidentes y organizaciones de ayuda, para lograr los objetivos del régimen: construir una defensa, reforzar la economía y garantizar la estabilidad interna.

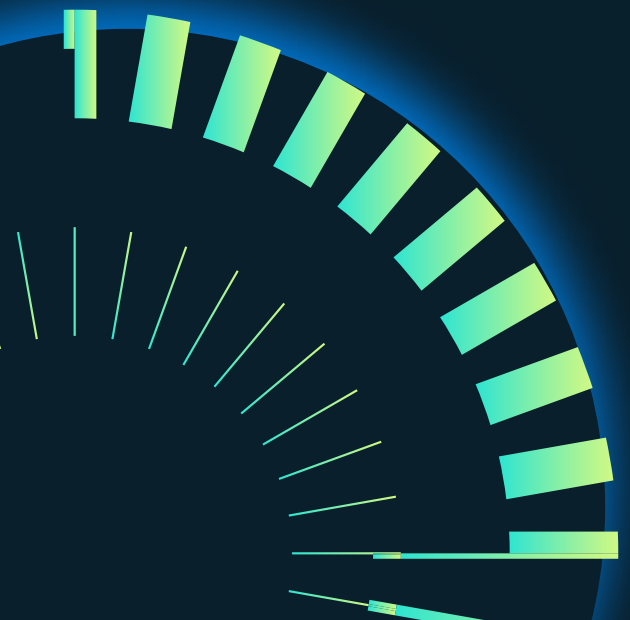
Más información en la página 49

Los cibermercenarios amenazan la estabilidad del ciberespacio, ya que este creciente sector de empresas privadas está desarrollando y vendiendo herramientas, técnicas y servicios avanzados para permitir que sus clientes (a menudo gobiernos) penetren en redes y dispositivos.

Más información en la página 52

Introducción

Después de los ataques de gran repercusión mediática de 2020 y 2021, los actores de amenazas de los Estados nación gastaron muchos recursos para adaptarse a las nuevas protecciones de seguridad implementadas por las organizaciones para defenderse contra las amenazas sofisticadas.



Al igual que las organizaciones empresariales, los adversarios comenzaron a utilizar los avances en automatización, infraestructura en el cloud y tecnologías de acceso remoto para ampliar sus ataques a un conjunto de objetivos más amplio. Estos ajustes tácticos dieron lugar a nuevos enfoques y ataques a gran escala contra las cadenas de suministro corporativas. La higiene de seguridad de TI cobró aún más importancia a medida que los agentes desarrollaban nuevas formas de explotar rápidamente las vulnerabilidades sin parches, ampliaban las técnicas para atacar las redes corporativas y ocultaban sus operaciones mediante software legítimo o de código abierto. Las nuevas técnicas de ataque proporcionaron vectores nuevos y más difíciles de detectar para obtener acceso a la red de un objetivo. Por último, conforme aumentaban los ataques físicos en la guerra, vimos cómo los ciberataques desempeñaban un papel destacado en la actividad militar.

El conflicto de Ucrania nos ofrece un ejemplo especialmente interesante de cómo los ciberataques evolucionan para impactar al mundo en paralelo con un conflicto militar de fondo. Los sistemas de energía, los sistemas de telecomunicaciones, los medios de comunicación y otras infraestructuras críticas se convirtieron en objetivos tanto de ataques físicos como de ciberataques. Los intentos de ataque a las redes que se observaban habitualmente como parte de campañas de espionaje y de filtración de información se centraron en la guerra híbrida en ataques de malware «wiper» contra sistemas de infraestructura críticas. La conexión de la seguridad de estos sistemas al cloud permitió la detección temprana y la interrupción de ataques potencialmente devastadores.[1]

Por primera vez en un evento cibernético importante, las detecciones de comportamiento basadas en machine learning utilizaron patrones de ataque conocidos para identificar y detener con éxito nuevos ataques sin tener un conocimiento previo del malware subyacente, incluso antes de que las personas conocieran las amenazas. También hemos confirmado lo valioso que es compartir la inteligencia sobre amenazas en tiempo real con los defensores que protegen estos sistemas, dándoles información esencial para prevenir los ataques activos y defenderse de ellos.

Los actores de amenazas de estados nación de todo el mundo siguen expandiendo sus operaciones de formas nuevas y antiguas. China, Corea del Norte, Irán y Rusia perpetraron ataques contra clientes de Microsoft. La cadena de suministro de servicios de TI se convirtió en un objetivo común cuando los atacantes cambiaron el foco hacia servicios ascendentes que pueden ser puntos de acceso a varias organizaciones. Esperamos que los atacantes continúen explotando las relaciones de confianza en las cadenas de suministro empresariales, lo que pone de relieve la importancia de la aplicación completa de reglas de autenticación, parches diligentes y configuración de cuentas para la infraestructura de acceso remoto y auditorías frecuentes de las relaciones con los partners para verificar su autenticidad.

Los agentes de los estados nación, al igual que los operadores de ransomware y los operadores delictivos, han respondido a una mayor exposición dirigiendo sus ataques a sistemas empresariales mal configurados o sin parches (infraestructura VPN/VPS, servidores on-premises y software de terceros) para perpetrar ataques «living off-the-land». Muchos han aumentado el uso de malware básico y herramientas del equipo rojo de código abierto para ocultar su actividad maliciosa.

Por consiguiente, mantener una buena higiene de seguridad informática mediante la aplicación de los parches prioritarios, la habilitación de características antimanipulación, el uso de herramientas de gestión de la superficie de ataque como RiskIQ para obtener una visión de fuera hacia dentro de la superficie de ataque y la habilitación de la autenticación multifactor en toda la empresa se ha convertido en una prioridad para defenderse proactivamente de muchos agentes sofisticados.

Los agentes de los Estados nación también han aumentado el uso del ransomware como táctica en sus ataques, a menudo reutilizando el malware de rescate creado por ese ecosistema delictivo en sus ataques. Hemos visto a agentes emplazados en Irán y en Corea del Norte utilizando herramientas de ransomware básico para dañar los sistemas objetivo, incluida a menudo las infraestructuras críticas, dentro de sus rivales regionales. Por último, hemos visto cómo ha aumentado la amenaza de cibermercenarios que desarrollan y venden herramientas, técnicas y servicios para ampliar los ataques contra soluciones vulnerables de terceros. La sofisticación y agilidad de los ataques perpetrados por los agentes de los estados nación seguirá aumentando cada año. Las organizaciones deben responder recibiendo información sobre estos cambios de los atacantes y desarrollar defensas en paralelo.

John Lambert
Vicepresidente e ingeniero distinguido, Centro de inteligencia sobre amenazas de Microsoft

Información contextual de los Estados nación

Las amenazas de los Estados-nación son actividades que se originan en un país en particular con la supuesta intención de promover los intereses nacionales. Los agentes de los Estados nación suponen algunas de las amenazas más avanzadas y persistentes a las que se enfrentan nuestros clientes, como el robo de propiedad intelectual, el espionaje, la vigilancia, el robo de credenciales y los ataques destructivos, entre otros.

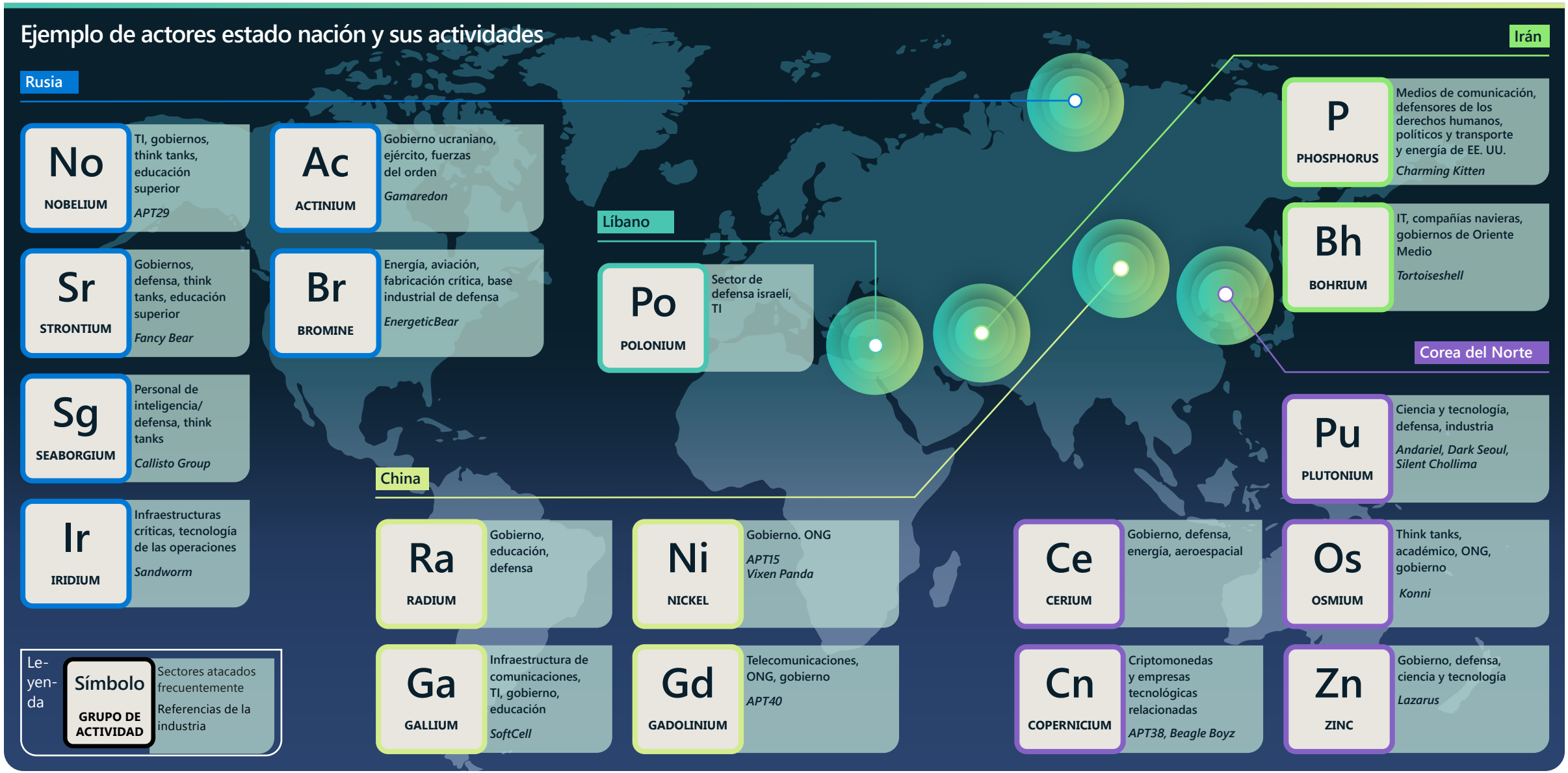
Invertimos una gran cantidad de recursos para detectar, conocer y contrarrestar estas amenazas. Cuando una organización o el titular de una cuenta es el objetivo o ha sufrido un ataque de actores estado nación, Microsoft envía una alerta en forma de notificación de Estados nación (NSN) directamente al cliente, la información que necesita para investigar la actividad. En junio de 2022, habíamos entregado más de 67 000 NSN desde que comenzamos en 2018.

Los datos de las alertas NSN de Microsoft se presentan en este capítulo para proporcionar una perspectiva de la actividad cuantificable. El nivel de actividad de los estados nación mostrado en los gráficos se basa en el número de NSN emitidas por Microsoft a los clientes en respuesta a la detección de agentes de estado nación que atacan o piratean al menos una cuenta en la organización del cliente.

Los cuatro Estados nación principales cuyos grupos de amenazas incluimos en este informe son Rusia, China, Irán y Corea del Norte. Representan los países de origen de los agentes que, según nuestras observaciones, han dirigido más ataques a clientes de Microsoft durante el último año. En el informe también se incluyen nuestras observaciones sobre los grupos de amenazas del Líbano y de los cibermercenarios, o los agentes ofensivos del sector privado.

Microsoft identifica los grupos de Estados nación con nombres de elementos químicos (como NOBELIUM), algunos de los cuales se muestran en la página siguiente. Utilizamos las designaciones DEV-#### como un nombre temporal proporcionado a una actividad de amenaza desconocida, emergente o en desarrollo, lo que nos permite rastrearla como un conjunto único de información hasta que alcancemos un alto grado de confianza sobre el origen o la identidad del agente que está detrás de la actividad.

Una vez que un DEV cumple los criterios, se convierte en un agente con nombre o se combina con los agentes existentes. A lo largo de este capítulo, citaremos algunos ejemplos de grupos de Estados nación y DEV para proporcionar una perspectiva más detallada de los objetivos de ataque, técnicas y análisis de las motivaciones. Aunque muchos de estos grupos utilizan las mismas herramientas que los ciberdelincuentes, presentan amenazas únicas en forma de malware a medida, la capacidad de descubrir y aprovechar vulnerabilidades de día cero e impunidad jurídica.


Ejemplo de actores estado nación y sus actividades
Rusia
No
NOBELIUM
TI, gobiernos, think tanks, educación superior
APT29
Ac
ACTINIUM
Gobierno ucraniano, ejército, fuerzas del orden
Gamaredon
Sr
STRONTIUM
Gobiernos, defensa, think tanks, educación superior
Fancy Bear
Br
BROMINE
Energía, aviación, fabricación crítica, base industrial de defensa
EnergeticBear
Sg
SEABORGIUM
Personal de inteligencia/ defensa, think tanks
Callisto Group
Ir
IRIDIUM
Infraestructuras críticas, tecnología de las operaciones
Sandworm
Líbano
Po
POLONIUM
Sector de defensa israelí, TI
China
Ra
RADIUM
Gobierno, educación, defensa
Ni
NICKEL
Gobierno. ONG
APT15
Vixen Panda
Ga
GALLIUM
Infraestructura de comunicaciones, TI, gobierno, educación
SoftCell
Gd
GADOLINIUM
Telecomunicaciones, ONG, gobierno
APT40
Irán
P
PHOSPHORUS
Medios de comunicación, defensores de los derechos humanos, políticos y transporte y energía de EE. UU.
Charming Kitten
Bh
BOHRIUM
IT, compañías navieras, gobiernos de Oriente Medio
Tortoiseshell
Corea del Norte
Pu
PLUTONIUM
Ciencia y tecnología, defensa, industria
Andariel, Dark Seoul, Silent Chollima
Ce
CERIUM
Gobierno, defensa, energía, aeroespacial
Os
OSMIUM
Think tanks, académico, ONG, gobierno
Konni
Cn
COPERNICIUM
Criptomonedas y empresas tecnológicas relacionadas
APT38, Beagle Boyz
Zn
ZINC
Gobierno, defensa, ciencia y tecnología
Lazarus
Leyenda
Símbolo
GRUPO DE ACTIVIDAD
Sectores atacados frecuentemente
Referencias de la industria

El cambiante panorama de las amenazas

La misión de Microsoft de rastrear la actividad de los actores estado nación y notificar a los clientes cuando vemos que están siendo atacados o corren peligro está arraigada en nuestra misión de proteger a nuestros clientes de los ataques.

Esta notificación es una parte crucial de nuestro compromiso de informar a los clientes si los ataques observados se logran prevenir mediante la protección de nuestros productos de seguridad o si los ataques llegan a término debido a debilidades de seguridad desconocidas. El seguimiento de las notificaciones a lo largo del tiempo ayuda a Microsoft a identificar tendencias de amenazas en evolución de los agentes y a centrar la protección de los productos en mitigar de forma proactiva las amenazas a los clientes en todos nuestros servicios en el cloud.

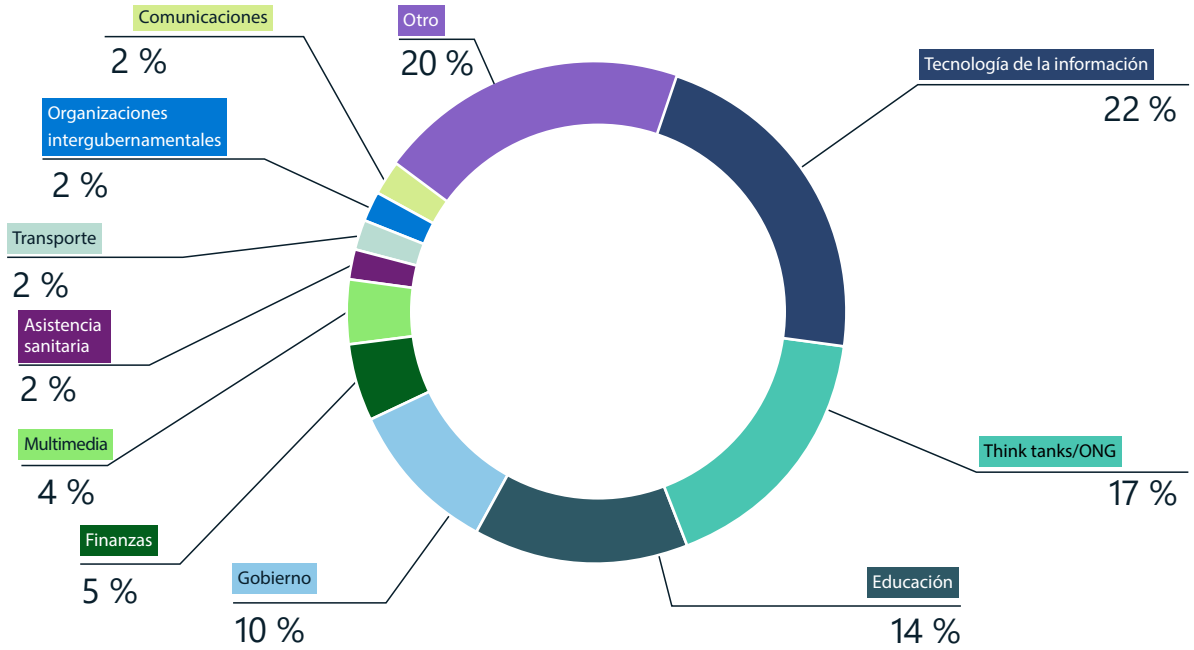
Este seguimiento también nos permite compartir datos e información sobre lo que vemos. Los analistas que rastrean a estos agentes y después de sus ataques utilizan una combinación de indicadores técnicos y conocimientos geopolíticos para conocer las motivaciones de los agentes, combinando el contexto técnico y global para crear nuevos conocimientos. Este proceso proporciona una perspectiva única de las prioridades de los ciberagentes de los estados nación y cómo sus motivaciones podrían reflejar las prioridades políticas, militares y económicas de los estados nación que los emplean.

Los desarrollos políticos del último año han conformado las prioridades y la tolerancia a los riesgos de los grupos de amenazas patrocinados por estados en todo el mundo. Ahora que se han roto las relaciones geopolíticas y representantes extremistas han adquirido más control en algunas naciones, los ciberataques se han vuelto más descarados y agresivos. Por ejemplo:

- Rusia atacó despiadadamente al gobierno ucraniano y a las infraestructuras críticas del país para complementar sus acciones militares sobre el terreno.[2]
- Irán buscó agresivamente el acceso a infraestructuras críticas de los Estados Unidos, como las autoridades portuarias.
- Corea del Norte continuó su campaña de robo de criptomonedas a empresas financieras y tecnológicas.
- China amplió sus operaciones de ciberespionaje global.

Aunque los agentes de los estados nación pueden ser técnicamente sofisticados y emplear una amplia variedad de tácticas, sus ataques a menudo pueden mitigarse con una buena higiene cibernética. Muchos de estos agentes utilizan medios relativamente poco tecnológicos, como los correos electrónicos de phishing, para distribuir malware sofisticado en lugar de invertir en desarrollar ataques personalizados o utilizar ingeniería social dirigida para lograr sus objetivos.

Sectores industriales atacados por los actores estado nación



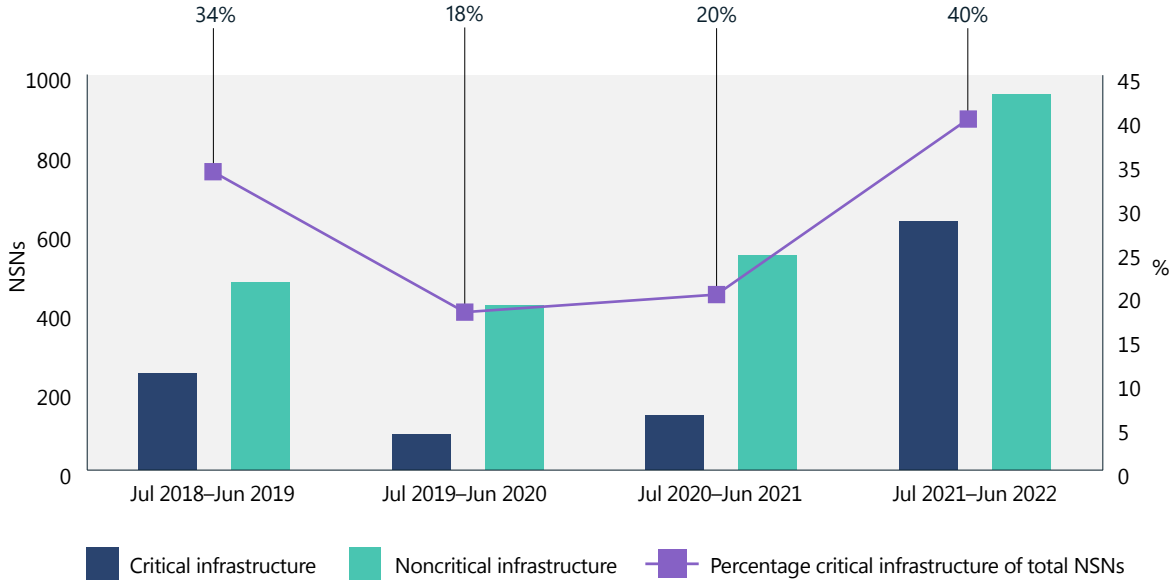
Los grupos de Estados nación atacaron una serie de sectores. Agentes de los estados ruso e iraní atacaron el sector de TI como un medio de acceder a los clientes de las empresas informáticas. Los think tanks, las organizaciones sin ánimo de lucro (ONG), las universidades y los organismos gubernamentales han seguido siendo otros objetivos comunes de los agentes de los estados nación.

Los agentes de los estados nación tienen una serie de objetivos que pueden provocar que sus ataques se dirijan a grupos específicos de organizaciones o individuos. En el último año, los ataques a la cadena de suministro han aumentado, centrándose especialmente en las empresas de TI. Mediante los ataques a proveedores de servicios de TI, los atacantes suelen ser capaces de alcanzar su objetivo original a través de una relación de confianza con la empresa que administra los sistemas conectados o de ejecutar posibles ataques a una escala mucho mayor que pongan en peligro a cientos de clientes de esta empresa en un solo ataque. Después del sector de TI, las entidades más atacadas fueron los think tanks, los organismos académicos vinculados a las universidades y los funcionarios. Estos son «objetivos débiles» deseables para el espionaje con el fin de recopilar información sobre temas geopolíticos.

El cambiante panorama de las amenazas

Continuación

Tendencias de infraestructuras críticas

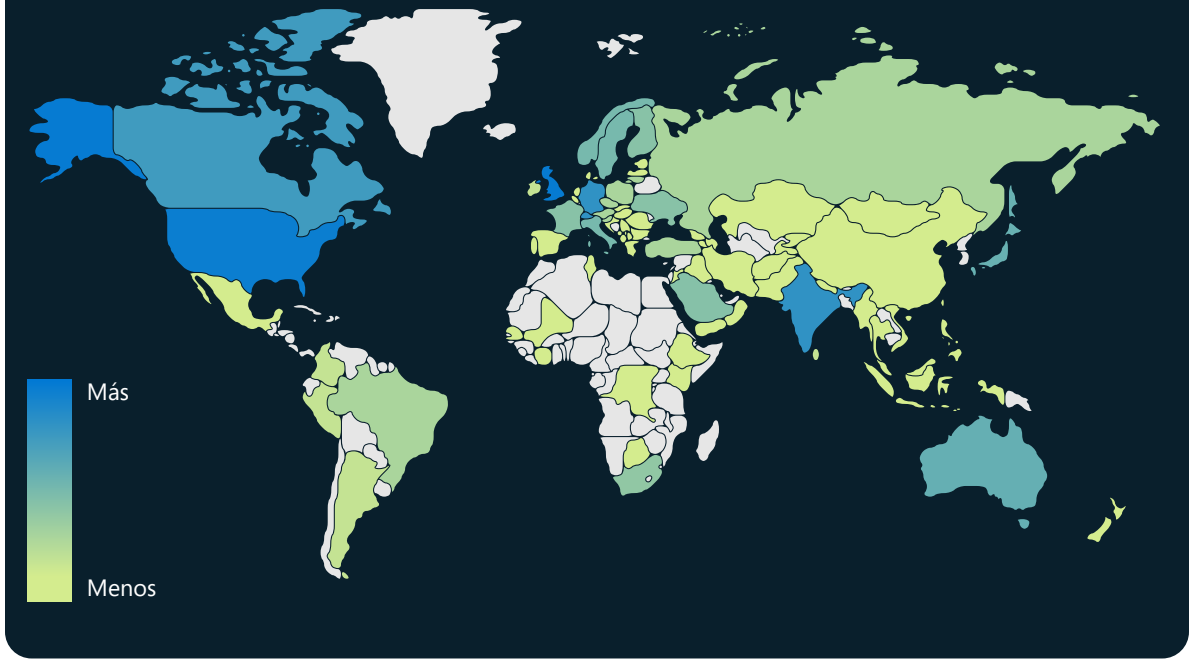


Los ataques de los grupos de estados nación a las infraestructuras críticas[3] aumentó el año pasado, centrados en las empresas del sector de TI, servicios financieros, sistemas de transporte e infraestructura de comunicaciones.

«Antes de la invasión de Ucrania, los gobiernos pensaban que los datos debían permanecer dentro de un país para estar protegidos. Tras la invasión, migrar los datos al cloud y moverlos fuera de las fronteras territoriales forma ahora parte de la planificación de la resiliencia y de un buen gobierno».

Cristin Flynn Goodwin,
asesora general asociada, Customer Security & Trust

Ataques por geografía de los actores estado nación



Los ataques cibernéticos de los grupos de Estados nación se extendieron por todo el mundo el año pasado, muy especialmente en las empresas estadounidenses y británicas. Las organizaciones de Israel, Emiratos Árabes Unidos, Canadá, Alemania, India, Suiza y Japón también se encuentran entre las más atacadas, según nuestros datos de NSN.

Conocimientos prácticos

1. Identifica y protege tus objetivos potenciales de datos de alto valor, tecnologías en riesgo, información y operaciones comerciales que podrían coincidir con las prioridades estratégicas de los grupos de estados nación.
2. Habilita las protecciones del cloud para proporcionar identificación y mitigación a escala de las amenazas nuevas y conocidas a tu red.

La cadena de suministro de TI como puerta de entrada al ecosistema digital

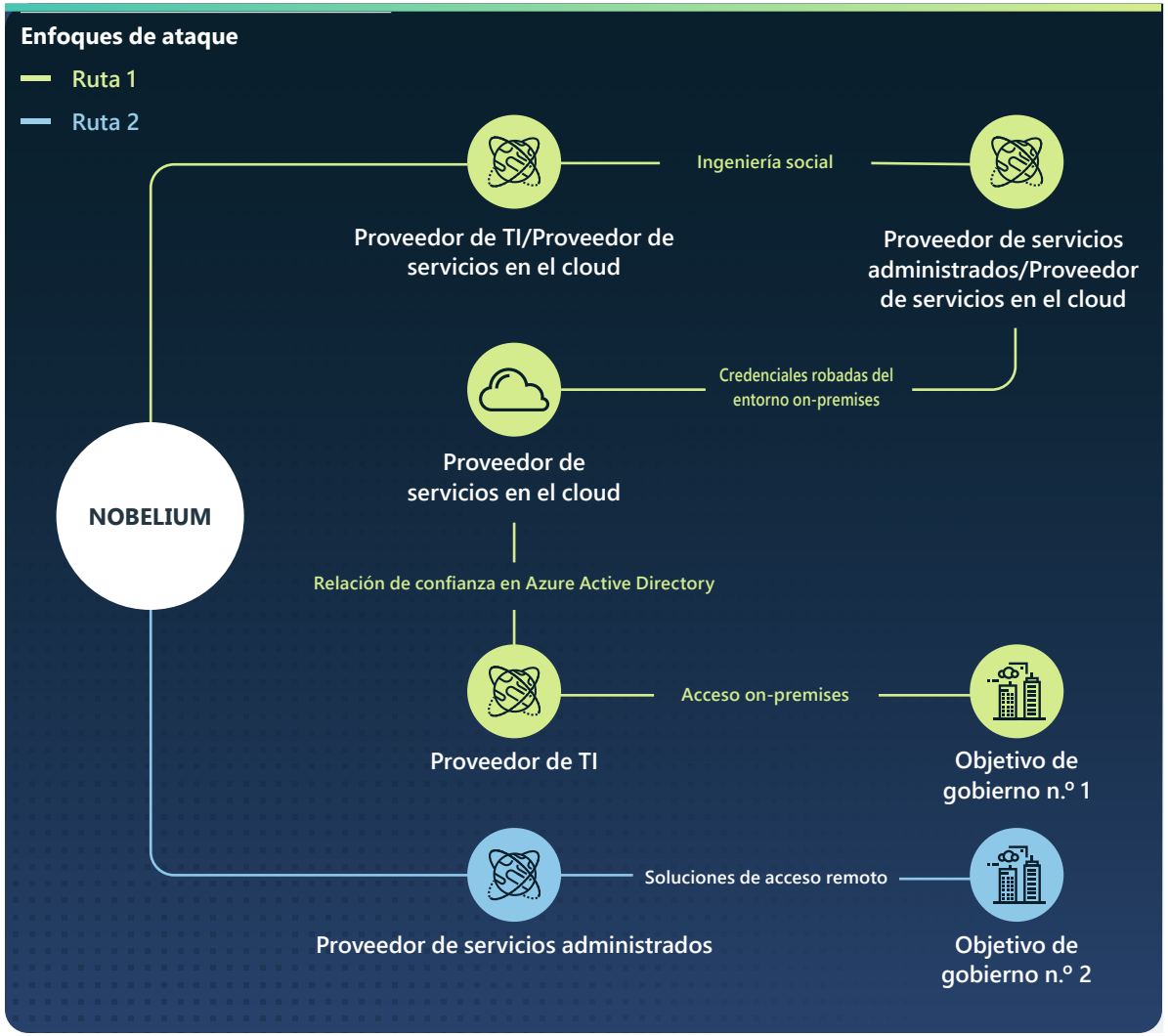
Los ataques de los Estados nación a los proveedores de servicios de TI podrían permitir a los actores de amenazas atacar otras organizaciones de interés aprovechando la confianza y el acceso que se concede a estos proveedores de la cadena de suministro. El año pasado, los grupos de ciberamenazas de Estados nación eligieron como objetivo a los proveedores de servicios de TI para atacar objetivos de terceros y obtener acceso a sus clientes en los sectores gubernamentales, políticos y de infraestructuras críticas.

Los proveedores de servicios de IT son objetivos intermediarios atractivos, ya que prestan servicio a cientos de clientes directos y miles de indirectos de interés para los servicios de inteligencia extranjeros. Si resultan atacados, las prácticas empresariales rutinarias y los privilegios administrativos delegados de los que disfrutan estas empresas podrían permitir a agentes malintencionados acceder y manipular las redes cliente de los proveedores de servicios de TI sin que salten inmediatamente las alertas.

El año pasado, NOBELIUM intentó atacar y aprovechar las cuentas con privilegios en soluciones en el cloud y otros proveedores de servicios administrados para intentar acceder a otras entidades de la cadena de suministro del ámbito gubernamental y político estadounidense y europeo.

NOBELIUM mostró cómo un enfoque de «ataque en cadena» podría dirigirse contra una entidad percibida como un adversario geopolítico. Este mismo año, el actor de amenazas intentó inmiscuirse, directamente o a través de terceros, en organizaciones sensibles emplazadas en estados miembro de la Organización de Tratado del Atlántico Norte (OTAN), que el gobierno ruso percibe como una amenaza existente. Entre julio de 2021 y principios de junio de 2022, el 48 por ciento de las notificaciones de clientes de Microsoft sobre la actividad de amenazas rusas a clientes de servicios online provinieron de empresas del sector de TI con sede en los países miembros de la OTAN, probablemente como puntos de acceso intermediarios. En general, el 90 por ciento de las notificaciones sobre la actividad de amenazas rusas durante el mismo período procedían de clientes emplazados en estados miembro de la OTAN, principalmente de los sectores de TI, organizaciones sin ánimo de lucro (ONG) y administraciones públicas, lo que sugiere una estrategia para buscar varios medios de acceso inicial a estos objetivos.

Ha habido un cambio de la explotación de la cadena de suministro de software a la explotación de la cadena de suministro de servicios de TI, dirigida a soluciones en el cloud y proveedores de servicios administrados para llegar a los clientes de estas empresas.



En este diagrama se ilustra el enfoque multivectorial de NOBELIUM para atacar sus objetivos finales y los daños colaterales para otras víctimas durante el proceso. Además de las acciones mostradas anteriormente, NOBELIUM lanzó ataques de phishing y «password spray» contra las entidades involucradas e incluso atacó la cuenta personal de al menos un empleado de la administración como otra posible ruta de ataque.

La cadena de suministro de TI como puerta de entrada al ecosistema digital

Continuación

A lo largo del año, el Centro de inteligencia sobre amenazas de Microsoft (MSTIC) detectó un número cada vez mayor de agentes del estado iraní y afiliados iraníes que atacaron empresas informáticas. En muchos casos, se detectó el robo de credenciales de inicio de sesión para obtener acceso a los clientes de estas empresas para una serie de objetivos, desde la obtención de inteligencia hasta ataques destructivos como represalia.

- En julio y agosto de 2021, DEV-0228 atacó a un proveedor de software empresarial israelí para atacar posteriormente a sus clientes en los sectores israelíes de defensa, energía y jurídico.[4]
- Desde agosto hasta septiembre de 2021, Microsoft detectó un aumento de los agentes del estado iraní cuyo objetivo eran empresas de TI con sede en la India. La inexistencia de problemas geopolíticos acuciantes que habría provocado este cambio sugiere que la elección de estos objetivos era para acceder indirectamente a filiales y clientes fuera de la India.
- En enero de 2022, DEV-0198, un grupo que consideramos afiliado al gobierno de Irán, atacó a un proveedor de soluciones en el cloud israelí. Según Microsoft, el agente probablemente usó credenciales obtenidas del proveedor para autenticarse en una empresa de logística israelí. El MSTIC observó que el mismo agente intentó perpetrar un ciberataque destructivo contra la empresa logística a finales de ese mes.
- En abril de 2022, vimos cómo POLONIUM, un grupo con sede en Líbano que pensamos que colabora con grupos del estado iraní en técnicas de cadena de suministro de TI, atacó a otra empresa de TI israelí para obtener acceso a organizaciones jurídicas y de defensa israelíes.[5]

Este último año de actividad muestra que los actores de amenazas como NOBELIUM y DEV-0228 conocen el panorama de las relaciones de confianza de una organización mejor que las propias organizaciones. Este aumento de las amenazas pone de relieve la necesidad de que las organizaciones conozcan y endurezcan las fronteras y los puntos de entrada de su patrimonio digital. También subraya la importancia de que los proveedores de servicios de TI supervisen rigurosamente su propio estado de ciberseguridad. Por ejemplo, las organizaciones deben implementar la autenticación multifactor y políticas de acceso condicional que hagan más difícil a los agentes malintencionados obtener cuentas con privilegios o propagarse por una red.

Realizar una revisión y una auditoría exhaustivas de las relaciones con los partners ayuda a minimizar los permisos innecesarios entre tu organización y los proveedores, y a eliminar inmediatamente el acceso a las relaciones que parezcan desconocidas. Un mayor conocimiento de los registros de actividad y la revisión de la actividad disponible facilita la detección de anomalías que podrían desencadenar una investigación adicional.

Dirigir los ataques a terceros permite a los estados nación atacar organizaciones sensibles aprovechando la confianza y el acceso en la cadena de suministro.

Conocimientos prácticos

1. Revisa y audita las relaciones de los proveedores en toda la cadena de suministro y los accesos con privilegios delegados para reducir al mínimo los permisos innecesarios. Retira el acceso a todas las relaciones con partners que parezcan desconocidas o que aún no se hayan auditado.[6]
2. Habilita el registro y revisa toda la actividad de autenticación para la infraestructura de acceso remoto y las redes privadas virtuales (VPN), centrándote en las cuentas configuradas con autenticación de un solo factor, para confirmar la autenticidad e investigar la actividad anómala.
3. Habilita la MFA en todas las cuentas (incluidas las cuentas de servicio) y asegúrate de que se aplique a todas las conexiones remotas.
4. Utiliza soluciones sin contraseña para proteger las cuentas.[7]

Enlaces a información adicional (pueden estar en inglés)

- NOBELIUM elige como objetivo privilegios administrativos delegados para permitir ataques más amplios | Centro de inteligencia sobre amenazas de Microsoft (MSTIC)
- Aumento de los ataques iraníes al sector de TI | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft
- Exposición de la actividad y la infraestructura de POLONIUM para atacar organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC)

Explotación rápida de vulnerabilidades

A medida que las organizaciones refuerzan sus posturas de ciberseguridad, los agentes de los estados nación responden buscando tácticas nuevas y únicas para perpetrar los ataques y eludir la detección. La identificación y explotación de vulnerabilidades previamente desconocidas (conocidas como «vulnerabilidades de día cero»), es una táctica clave en esta iniciativa.

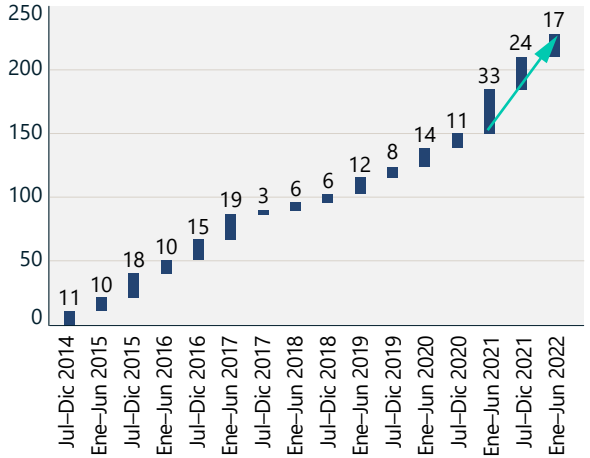
Las vulnerabilidades de día cero son un medio particularmente eficaz para la explotación inicial y las vulnerabilidades, una vez expuestas públicamente, pueden ser reutilizadas rápidamente por otros estados nación y agentes delictivos. El número de vulnerabilidades de día cero reveladas públicamente durante el último año es similar a las del año anterior, que fueron las más altas registradas.

A medida que los actores de amenazas —tanto los estados nación como los delictivos— se vuelven más expertos en aprovechar estas vulnerabilidades, observamos una reducción del tiempo entre el anuncio de una vulnerabilidad y la mercantilización de esa vulnerabilidad. Esto hace que sea esencial que las organizaciones pongan remedio inmediatamente a las amenazas. Asimismo, es fundamental que las organizaciones o las personas que descubran nuevas vulnerabilidades las divulguen de forma responsable o informen de ellas a los proveedores afectados lo antes posible, de acuerdo con procedimientos coordinados de divulgación de vulnerabilidades.

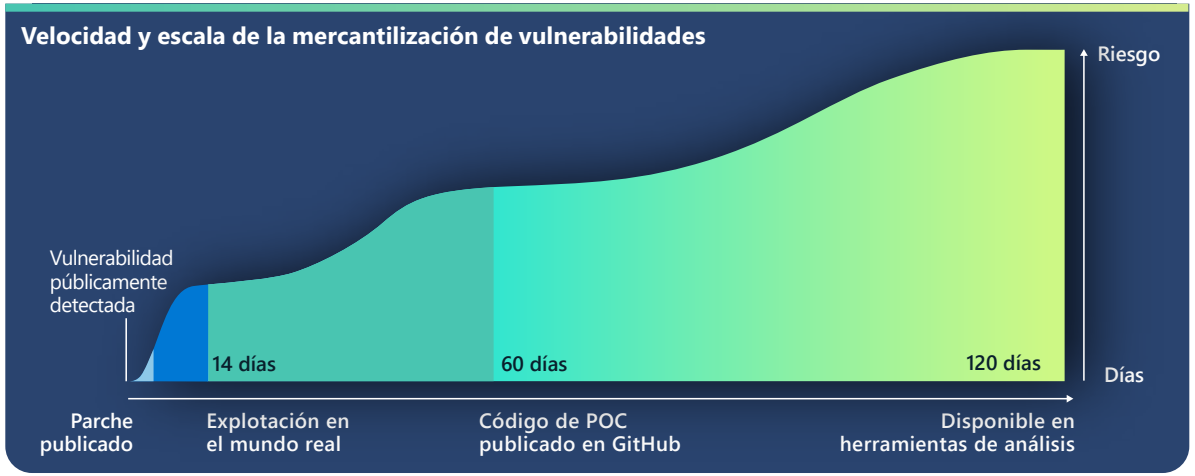
Esto garantiza que se identifiquen las vulnerabilidades y que se desarrollen puntualmente los parches para proteger a los clientes de las amenazas previamente desconocidas.

Muchas organizaciones presuponen que tienen menos probabilidades de ser víctimas de ataques de explotación de día cero si la administración de vulnerabilidades está integrada en la seguridad de su red. Sin embargo, la mercantilización de los ataques les está obligando a acelerar el ritmo. Los ataques de día cero a menudo son descubiertos por otros agentes y son reutilizados ampliamente en un período de tiempo corto, lo que deja en peligro los sistemas sin parches. Aunque las explotaciones de día cero pueden ser difíciles de detectar, las acciones posteriores a la explotación por parte de los agentes suelen ser más fáciles de detectar y, si proceden de software con todos los parches implementados, pueden servir de señal de advertencia de un ataque.

Parches publicados para vulnerabilidades de día cero



Número de ataques de día cero divulgados públicamente de la Lista de vulnerabilidades comunes y divulgaciones (CVE).



De media, solo se tarda 14 días en que un ataque esté disponible abiertamente una vez divulgada públicamente una vulnerabilidad. Esta vista proporciona un análisis de la línea cronológica de explotación de vulnerabilidades de día cero, junto con el número de sistemas vulnerables al ataque en cuestión y activos en Internet desde la primera divulgación pública.

Aunque los ataques de vulnerabilidad de día cero suelen dirigirse inicialmente a un conjunto limitado de organizaciones, se adoptan rápidamente en el ecosistema de actores de amenazas más amplio. Esto constituye el pistoletazo de salida para que los actores de amenazas aprovechen la vulnerabilidad lo más ampliamente posible antes de que sus objetivos potenciales instalen parches.

Aunque observamos que hay muchos actores estado nación que desarrollan explotaciones de vulnerabilidades desconocidas, los actores de amenazas de estados nación con sede en China son especialmente competentes en la detección y desarrollo de ataques de día cero. La normativa china sobre la divulgación de vulnerabilidades entró en vigor en septiembre de 2021, siendo la primera vez en el mundo que un gobierno requiere que las autoridades gubernamentales revisen las denuncias de vulnerabilidades antes de compartir la vulnerabilidad con el propietario del producto o servicio. Esta nueva normativa podría permitir a los funcionarios del gobierno chino almacenar las vulnerabilidades denunciadas para convertirlas en armas. El aumento del uso de ataques de día cero durante el último año por parte de agentes con sede en China refleja probablemente el primer año completo de requisitos de divulgación de vulnerabilidades en China para la comunidad de seguridad china y un paso importante en el uso de los ataques de día cero como prioridad de estado. Las vulnerabilidades descritas a continuación las desarrollaron e implementaron por primera vez actores estado nación con sede en China durante los ataques, antes de ser descubiertos y antes de que se propagaran a otros agentes del ecosistema de amenazas más amplio.

Explotación rápida de vulnerabilidades

Continuación

Incluso las organizaciones que no son un objetivo de los ataques de Estados nación tienen un plazo limitado para aplicar parches a las vulnerabilidades de día cero en los sistemas afectados antes de que sean explotadas por un ecosistema de agentes más amplio.

Estos ejemplos de vulnerabilidades recién identificadas muestran que las organizaciones tienen una media de 60 días desde el momento en que se corrige una vulnerabilidad y se publica en Internet un código de prueba de concepto (POC), que suelen obtener otros agentes para su reutilización. Asimismo, las organizaciones tienen una media de 120 días antes de que esté disponible una vulnerabilidad en las herramientas de análisis y explotación automatizadas de vulnerabilidades como Metasploit, que a menudo permiten realizar el ataque a gran escala. Esto pone de relieve que incluso las organizaciones que no son un objetivo de los actores de amenazas de estados nación tienen un plazo limitado para aplicar parches a las vulnerabilidades de día cero en los sistemas afectados antes de que esas vulnerabilidades sean explotadas por un ecosistema de agentes más amplio.

CVE-2021-35211 SolarWinds Serv-U

En julio de 2021, SolarWinds lanzó un aviso de seguridad para CVE-2021-35211, que Microsoft acreditó con una notificación.[8] En ese momento, descubrimos que el actor de amenazas de estados nación DEV-0322 estaba aprovechando la vulnerabilidad de SolarWinds Serv-U. Nuestro equipo de RiskIQ observó que había 12 646 direcciones IP que alojaban versiones conectadas a Internet de los dispositivos afectados entre el 15 de junio y el 9 de julio.

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

En septiembre de 2021, nuestros investigadores observaron que agentes afiliados a China estaban atacando a Zoho ManageEngine en varias entidades con sede en Estados Unidos. La vulnerabilidad se comunicó públicamente el 6 de septiembre como CVE-2021-40539 Zoho ManageEngine ADSelfService Plus, que las organizaciones suelen usar para gestionar el restablecimiento de contraseñas.[9] DEV-0322 aprovechó la vulnerabilidad más adelante en septiembre, usándola como vector inicial para obtener un punto de acceso en las redes y realizar acciones adicionales, incluido el volcado de credenciales, la instalación de binarios personalizados y la colocación de malware para mantener la persistencia. En el momento de su divulgación, RiskIQ observó 4011 instancias de estos sistemas activos y en Internet.

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

A finales de octubre de 2021, observamos que DEV-0322 aprovechaba una vulnerabilidad (CVE-2021-44077) en un segundo producto de Zoho ManageEngine, ServiceDesk Plus, un software de asistencia de TI con administración de activos. DEV-0322 usó esta vulnerabilidad para identificar y atacar entidades del sector sanitario, tecnología de la información, educación superior e industrial críticos. El 2 de diciembre, la Oficina Federal de Investigación (FBI) y la Cybersecurity and Infrastructure Security Agency (CISA) emitieron un aviso conjunto para advertir al público de los actores de amenazas de estados nación que estaban aprovechando la vulnerabilidad. En el momento de su divulgación, RiskIQ observó 7956 instancias de estos sistemas activos y en Internet.

CVE-2021-42321 Microsoft Exchange

Un ataque de día cero para una vulnerabilidad de Exchange CVE-2021-42321 se reveló durante la Tianfu Cup, una conferencia de ciberseguridad internacional y competiciones de hacking realizada el 16 y 17 de octubre de 2021 en Chengdu, China. Los investigadores de seguridad de Microsoft observaron que la vulnerabilidad de Exchange se usó en el mundo real el 21 de octubre, solo tres días después de que se diera a conocer. En el momento de su divulgación, RiskIQ observó 61 559 instancias de estos sistemas activos y en Internet. Seguimos observando actividad de ataque en noviembre de 2021.

CVE-2022-26134 Confluence

Un agente afiliado a China probablemente tenía el código de explotación de día cero de la vulnerabilidad Confluence (CVE-2022-26134) cuatro días antes de que la vulnerabilidad se diera a conocer públicamente el 2 de junio y probablemente lo utilizó en una entidad con sede en Estados Unidos. En el momento de su divulgación, RiskIQ observó 53 621 instancias de sistemas vulnerables a Confluence en Internet.

Las vulnerabilidades se están detectando y explotando a gran escala, y en plazos cada vez más cortos.

Conocimientos prácticos

1. Prioriza la aplicación de parches a las vulnerabilidades de día cero en cuanto se publiquen; no esperes a que se implemente el ciclo de administración de parches.
2. Documenta y haz inventario de todos los activos de hardware y software empresariales para determinar el riesgo y saber rápidamente cuándo empezar a aplicar parches.

Las tácticas cibernéticas en tiempo de guerra del Estado ruso amenazan a Ucrania y a otros países

Este año, agentes del estado ruso lanzaron operaciones cibernéticas para complementar la acción militar durante la invasión de Ucrania por parte de Rusia, utilizando a menudo las mismas tácticas y técnicas desplegadas contra objetivos fuera de Ucrania. Es fundamental que las organizaciones de todo el mundo tomen medidas para reforzar la ciberseguridad contra las amenazas digitales procedentes de los actores de amenazas afiliados a Rusia.

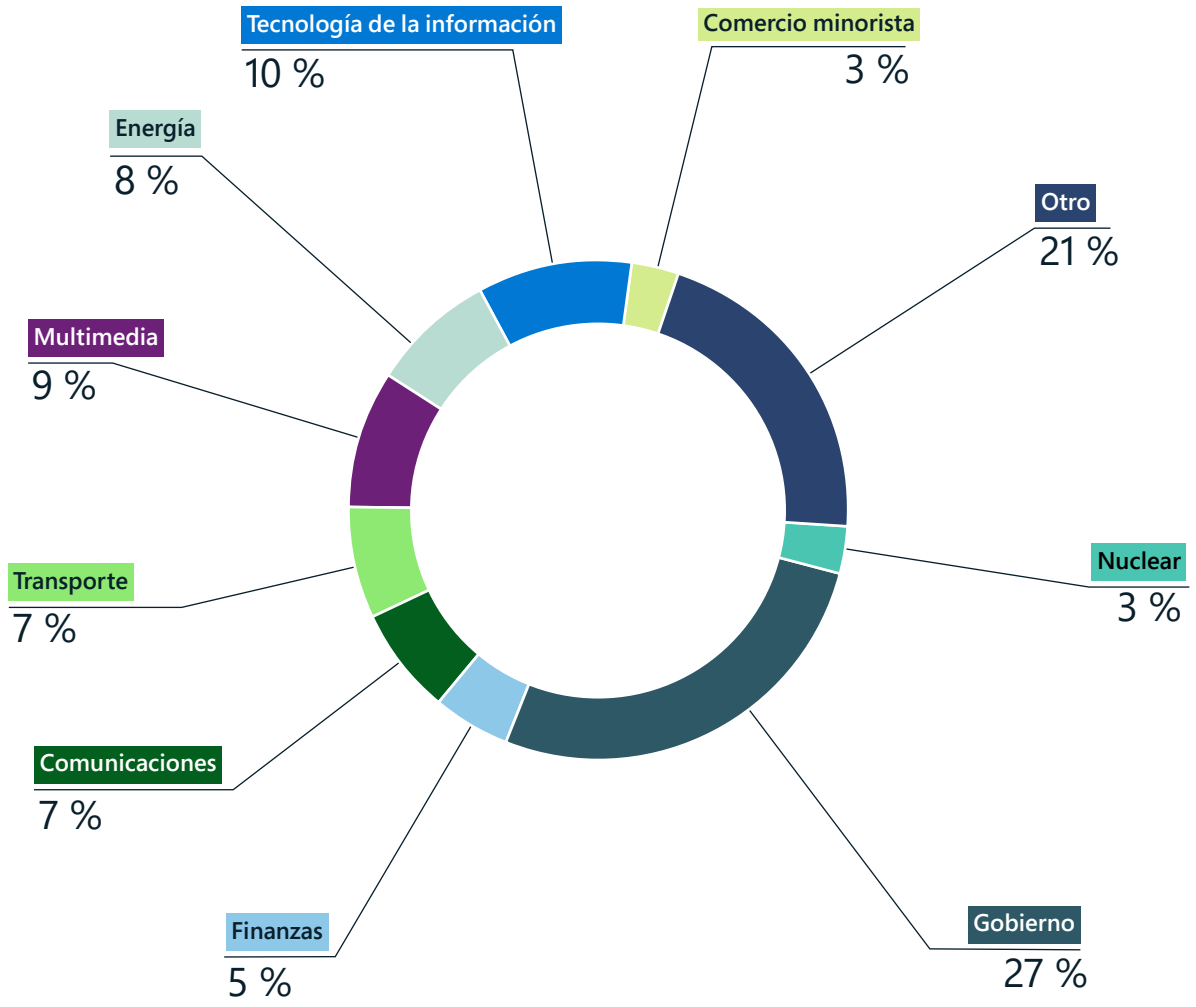
La situación sobre el terreno sigue fluctuando a medida que persiste el conflicto militar, y Ucrania y sus aliados deben estar preparados para defenderse si operadores cibernéticos del estado ruso aumentan la frecuencia o la intensidad de las intrusiones en línea de conformidad con sus objetivos militares. Durante los cuatro primeros meses de guerra, Microsoft observó que actores de amenazas asociados con el ejército ruso lanzaron varias oleadas de ciberataques destructivos contra casi 50 agencias y empresas ucranianas distintas e intrusiones centradas en el espionaje contra muchas otras. Sin incluir las operaciones contra clientes de servicios online, el 64 por ciento de la actividad de amenazas rusas contra objetivos conocidos se dirigió a organizaciones con sede en Ucrania entre finales de febrero y junio.

En cada operación, los actores de amenazas rusos emplearon muchas de las tácticas, técnicas y procedimientos (TTP) que observamos que se utilizaban antes de la invasión contra objetivos tanto de dentro como de fuera de Ucrania. El objetivo de estos agentes era destruir datos y pillar a los organismos gubernamentales ucranianos desprevenidos en el período inicial del conflicto. Desde entonces, han tratado de descarrilar el transporte de asistencia militar y humanitaria a Ucrania, interrumpir el acceso público a los servicios y medios de comunicación y robar información de inteligencia a largo plazo o de valor económico para Rusia.

Los ataques al transporte suponen una amenaza en un área de importancia crítica para los ciudadanos ucranianos que intentan sobrevivir al conflicto. Según una encuesta patrocinada por UNICEF en mayo, lo que más preocupaba a los encuestados de las zonas urbanas afectadas por los conflictos eran el transporte y el combustible, las interrupciones del suministro, la seguridad y el acceso limitado a los alimentos, los servicios médicos y los servicios financieros.[10] En junio, el coordinador de la crisis de la ONU en Ucrania afirmó que al menos 15,7 millones de personas en Ucrania necesitaban asistencia humanitaria urgente y que el número aumentaría mientras continuara la guerra.[11]

Fuera de Ucrania, Microsoft detectó iniciativas de intrusión de la red rusa contra 128 organizaciones de 42 países entre finales de febrero y junio. Estados Unidos fue el objetivo número uno de Rusia. Polonia, por donde transita gran parte de la asistencia militar y humanitaria internacional que llega a Ucrania, también fue un objetivo importante durante este período. Los actores de amenazas afiliados al estado ruso buscaban organizaciones en los países bálticos y redes informáticas en Dinamarca, Noruega, Finlandia y Suecia también en abril y mayo.

Sectores de la industria más atacados en Ucrania desde la invasión



Las organizaciones gubernamentales federales, estatales y locales de Ucrania han seguido siendo objetivos prioritarios de los grupos de amenazas del estado ruso y afiliados durante el conflicto. El foco puesto en las organizaciones del sector del transporte, energía, finanzas y medios de comunicación pone de relieve el riesgo que estas operaciones cibernéticas suponen para los servicios de los que dependen los ciudadanos ucranianos.

Las tácticas cibernéticas en tiempo de guerra del Estado ruso amenazan a Ucrania y a otros países

Continuación

Hemos visto un aumento de actividades similares dirigidas a los ministerios de asuntos exteriores de los países de la OTAN.

Los grupos de amenazas del Estado ruso se mostraron interesados en atacar las infraestructuras críticas tanto dentro como fuera de Ucrania el año pasado. IRIDIUM implementó el malware Industroyer2 en un esfuerzo fallido de dejar a millones de ucranianos sin electricidad. Fuera de Ucrania, BROMINE llevó a cabo intrusiones contra organizaciones involucradas en la fabricación y sistemas de control industrial a principios de 2022.

Los agentes del Estado ruso y sus afiliados dirigieron operaciones cibernéticas contra Ucrania, sus aliados y otros objetivos de valor de inteligencia este año utilizando muchos de los siguientes TTP:

«Spear phishing» con archivos adjuntos o enlaces maliciosos

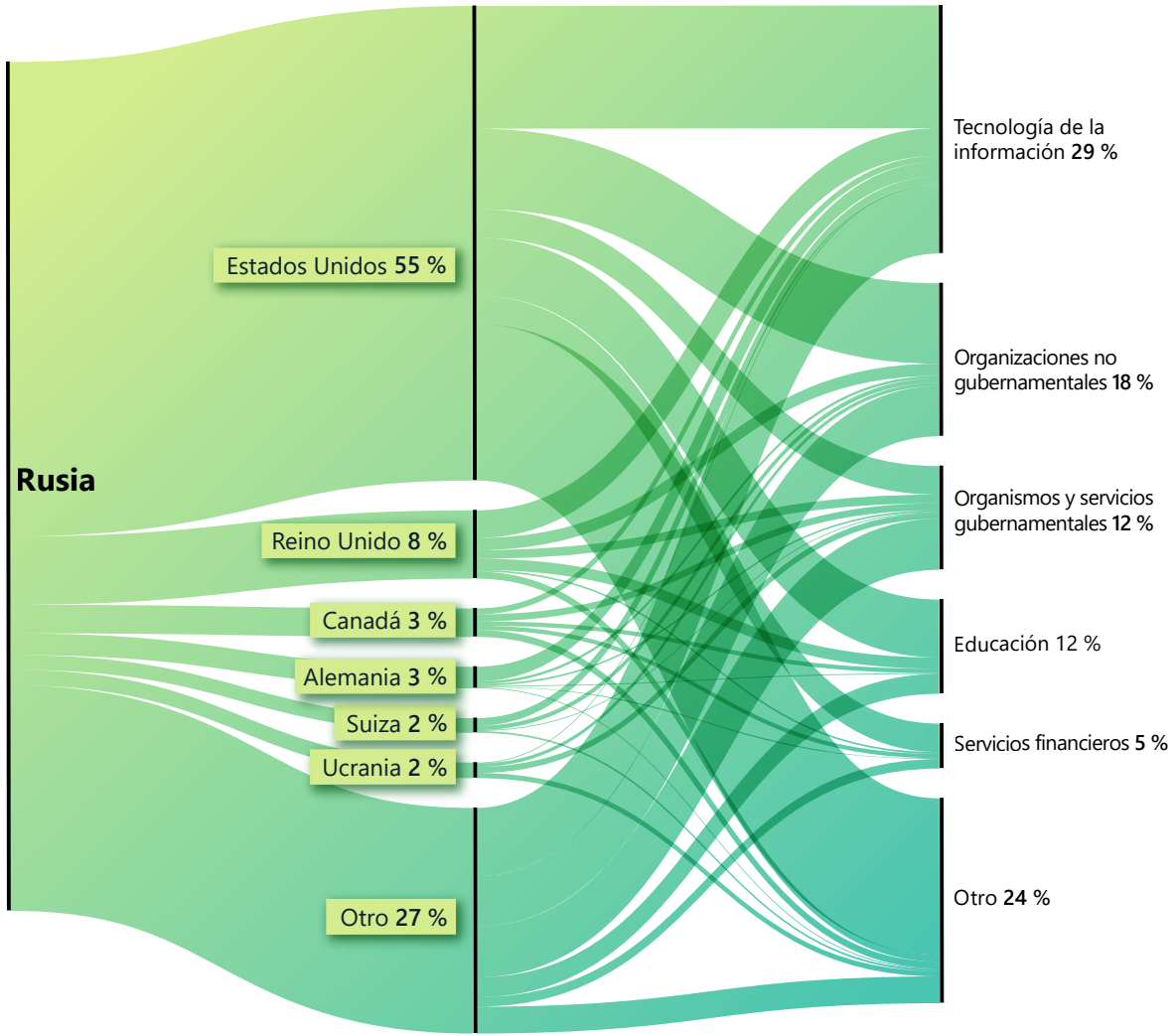
Los grupos del Estado ruso y sus afiliados, como ACTINIUM, NOBELIUM, STRONTIUM, DEV-0257, SEABORGIUM e IRIDIUM, utilizaron campañas de phishing para obtener acceso inicial a las cuentas y redes deseadas en organizaciones de dentro y fuera de Ucrania. Muchas campañas utilizaron cuentas atacadas o suplantadas en las organizaciones objetivo o dentro del mismo sector, y temas convincentes para atraer a las víctimas. NOBELIUM usó cuentas de diplomáticos atacadas para enviar correos de phishing con apariencia de comunicaciones diplomáticas a los empleados de los ministerios de asuntos exteriores de todo el mundo. STRONTIUM creó cuentas de suplantación de identidad basadas en nombres disponibles públicamente de los titulares de cuentas de think tanks de los Estados Unidos y envió mensajes de phishing para obtener acceso a las cuentas de esos think tanks. SEABORGIUM suplantó la identidad mediante señuelos relacionados con la información sobre el conflicto de Ucrania para obtener acceso inicial a cuentas de think tanks de relaciones internacionales de los países nórdicos.

Explotación de la cadena de suministro de servicios de IT para atacar a los clientes

A finales de 2021, agentes del Estado ruso atacaron a proveedores de servicios de TI y utilizaron el acceso para facilitar la desfiguración del sitio web y la implementación del malware destructivo Whispergate por DEV-0586 en enero.[12] DEV-0586 también atacó la red de una empresa de TI que creó sistemas de gestión de recursos para el Ministerio de Defensa de Ucrania y otras organizaciones de los sectores de comunicaciones y transporte, lo que indica que el grupo estaba explorando también opciones de ataques a terceros en esos sectores.

En todo el mundo, pero especialmente en los Estados Unidos y en Europa Occidental, NOBELIUM ha atacado a proveedores de servicios de TI para obtener acceso a las redes gubernamentales y otras redes sensibles a lo largo de 2021-2022 (véase la información sobre las vulnerabilidades de la cadena de suministro anteriormente en este capítulo).

Rusia: principales países y sectores industriales atacados



A pesar del mayor énfasis en las organizaciones con sede en Ucrania desde principios de 2022, las empresas con sede en Norteamérica y Europa Occidental seguían siendo las empresas de servicios online más atacadas por los agentes rusos. La campaña de NOBELIUM contra el sector de TI convierte a este sector en el más atacado el año pasado.

Las tácticas cibernéticas en tiempo de guerra del estado ruso amenazan a Ucrania y a otros países

Continuación

Explotación de aplicaciones orientadas al público para obtener acceso inicial a las redes

Desde al menos finales de 2021, STRONTIUM ha trabajado en el desarrollo y perfeccionamiento de su capacidad para atacar servicios orientados al público, como los servidores de Microsoft Exchange, para robar información. STRONTIUM aprovechó las vulnerabilidades de los servidores de Exchange para acceder a las cuentas gubernamentales ucranianas, así como a organizaciones militares y del sector de la defensa de Estados Unidos, Líbano, Perú y Rumanía, y otros organismos gubernamentales con sede en Armenia, Bosnia, Kosovo y Malasia. DEV-0586, también afiliado al ejército ruso, aprovechó las vulnerabilidades de servidor Confluence para obtener acceso inicial a las organizaciones gubernamentales y del sector de TI en Ucrania y otros países de Europa del Este.

Los agentes del Estado ruso y sus afiliados utilizan muchos de los mismos TTP para atacar organizaciones de interés durante las épocas de guerra y paz.

Uso de cuentas y protocolos administrativos y utilidades nativas para la detección de redes y el movimiento lateral

Después de obtener acceso inicial a una red, Microsoft observó cómo los agentes del Estado ruso aprovechaban las cuentas legítimas y las utilidades de software empleadas para realizar tareas de mantenimiento básicas con el fin de eludir la detección el mayor tiempo posible. Utilizaban identidades atacadas con capacidades administrativas y protocolos, herramientas y métodos de administración válidos para moverse lateralmente dentro de las redes sin atraer inmediatamente la atención de monitores automatizados y defensores de la red.

La higiene cibernética básica y el empleo de herramientas de detección y respuesta de puntos de conexión pueden ayudar a mitigar el impacto negativo de este tipo de operaciones en tiempos de paz, así como durante las épocas de guerra.

La imprevisibilidad del conflicto exige que organizaciones de todo el mundo tomen medidas para reforzar la ciberseguridad contra las amenazas digitales procedentes de los agentes del Estado ruso y sus afiliados.

Conocimientos prácticos

1. Minimiza el robo de credenciales y la explotación de cuentas protegiendo las identidades de los usuarios con la implementación de herramientas de protección de identidad de MFA y la aplicación del acceso con privilegios mínimos para proteger las cuentas y sistemas más sensibles y con privilegios.
2. Aplica actualizaciones para garantizar que todos tus sistemas obtengan el mayor nivel de protección lo antes posible y se mantengan actualizados.
3. Implementa soluciones antimalware, detección de puntos de conexión y protección de la identidad en toda la organización. Una combinación de soluciones de seguridad de defensa en profundidad, junto con personal capacitado y competente, puede capacitar a tu organización para identificar, detectar y prevenir intrusiones que afecten a tu negocio.
4. Permite investigaciones y recuperación en caso de que se detecte o se reciba una notificación de una amenaza en tu entorno haciendo una copia de seguridad de los sistemas críticos y habilitando el registro. Se recomienda absolutamente la implantación de un plan de respuesta a incidentes.

Enlaces a información adicional (pueden estar en inglés)

- Defensa de Ucrania: lecciones tempranas de la guerra cibernética | Microsoft On the Issues
- La guerra híbrida en Ucrania | Microsoft On the Issues
- Actividad de ciberamenazas en Ucrania: análisis y recursos | Centro de respuesta de seguridad de Microsoft (MSRC)
- Desmantelamiento de ciberataques dirigidos a Ucrania | Microsoft On the Issues
- Ataques de malware dirigidos al gobierno de Ucrania | Microsoft On the Issues
- MagicWeb: el truco posterior al ataque de NOBELIUM para autenticarse como cualquier persona | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Equipo de detección y respuesta (DART), Equipo de investigación de Microsoft 365 Defender

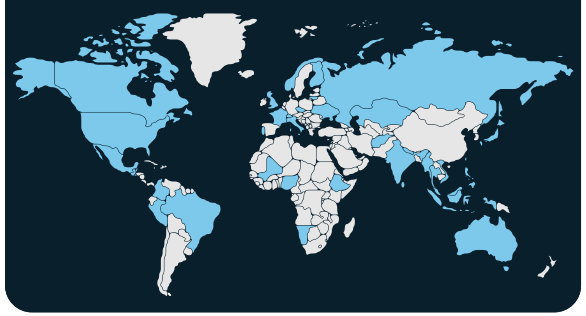
Ampliación de los ataques globales de China para obtener una ventaja competitiva

En el complejo clima geopolítico actual, los actores de amenazas del Estado chino y afiliados a China que realizan operaciones cibernéticas a menudo pretenden mejorar los objetivos estratégicos militares, económicos y de relaciones exteriores del país como parte del objetivo de China de lograr una ventaja competitiva. En el último año, Microsoft ha observado una actividad de amenazas generalizada en China dirigida a países de todo el mundo.

Desde mediados de 2021, China ha estado maniobrando para garantizar la estabilidad económica y financiera en medio de la peor oleada de la COVID-19 en dos años.[13] China siguió manteniendo una postura de equilibrio frente a los acontecimientos geopolíticos, como la lucha por equilibrar su asociación «ilimitada» con Rusia[14] y mantener su posición en el escenario mundial.[15] Asimismo, la posición de China frente a los Estados Unidos y sus aliados sobre Taiwán[16] y el mar del sur de China siguió tensando las relaciones extranjeras con muchos países.[17]

Los grupos de amenazas del Estado chino y afiliados de China aumentaron los ataques a naciones más pequeñas de todo el mundo centrándose en el Sudeste Asiático para obtener una ventaja competitiva en todos los frentes.

Países atacados por grupos del estado chino y afiliados

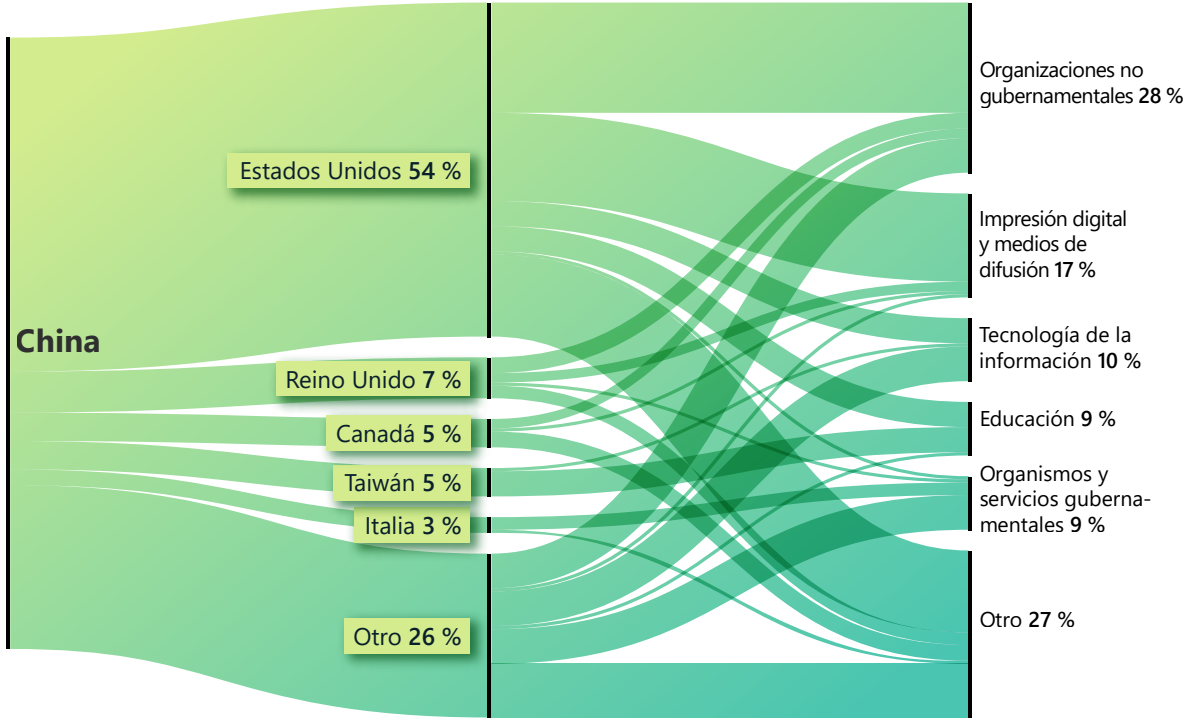


China también siguió ampliando su influencia económica a través de la Iniciativa de la Franja y la Ruta (BRI, por sus siglas en inglés) establecida anteriormente, en un intento de reactivar un marco de inversión integral con la UE[18] y de negociar un nuevo acuerdo comercial regional con 15 países de Asia Pacífico conocido como Asociación Económica Integral Regional.[19] Microsoft cree que China seguirá utilizando la recolección cibernética como herramienta para ayudar a avanzar en sus objetivos políticos, militares y económicos estratégicos de acuerdo con las operaciones cibernéticas observadas y la amplitud de las entidades atacadas.

Ataques cibernéticos diseñados probablemente para avanzar en los intereses económicos y militares.

Microsoft observó ataques generalizados a naciones más pequeñas de todo el mundo por parte de grupos de amenazas del Estado nación chino y afiliados, lo que sugiere que China probablemente está utilizando el ciberespionaje como un componente de su influencia económica y militar global.

China: principales países y sectores industriales atacados



Los think tanks/ONG, medios de comunicación, TI, gobierno y educación están entre los sectores más atacados por los grupos de amenazas con sede en China, probablemente para la recopilación de inteligencia y reconocimiento persistentes.

El conjunto de objetivos incluía, entre otros, a los países de África, el Caribe, Oriente Medio, Oceanía y Sur de Asia, centrándose especialmente en los países del Sudeste Asiático y las Islas del Pacífico.

De acuerdo con la estrategia de BRI de China, los grupos de amenazas con sede en China han dirigido sus ataques a entidades de Afganistán, Kazajistán, Mauricio, Namibia y Trinidad y Tobago.[20] Por ejemplo, Trinidad y Tobago fue el primer país caribeño en avalar la estrategia de BRI de China en 2018 y China lo considera un socio importante en la región. NICKEL ha realizado operaciones de red persistentes dirigidas a Trinidad y Tobago desde 2021. Por ejemplo, en marzo de 2022, NICKEL llevó a cabo actividades de reconocimiento dirigidas a un organismo gubernamental, probablemente con fines de recopilación de inteligencia.

Ampliación de los ataques globales de China para obtener una ventaja competitiva

Continuación

Mientras tanto, Microsoft observó que los grupos de amenazas del Estado chino y sus afiliados centraban sus operaciones de red contra entidades del Sudeste Asiático y se expandían a países de las islas del Pacífico a medida que China cambiaba sus prioridades militares y económicas para hacer frente a los desafíos del interés renovado de los Estados Unidos en la región. En enero de 2022, Microsoft observó que RADIUM estaba atacando a una empresa de energía y a un organismo gubernamental relacionado con la energía en Vietnam y un organismo gubernamental de Indonesia. Las actividades de RADIUM probablemente concuerden con los objetivos estratégicos de China en el mar del Sur de China.[21] A finales de febrero y principios de marzo, GALLIUM atacó más de 100 cuentas asociadas con una destacada organización intergubernamental (IGO) en la región del Sudeste Asiático. El momento en que GALLIUM atacó a la IGO en la región coincide con el anuncio de una reunión programada entre Estados Unidos y líderes regionales. Probablemente, los agentes de GALLIUM tenían la tarea de supervisar las comunicaciones y recopilar inteligencia antes del encuentro.

Conforme China ampliaba su influencia en los países de las islas del Pacífico, continuaron las actividades de los grupos de amenazas de China. En abril, China y las Islas Salomón firmaron un acuerdo de seguridad con el fin de «promover la paz y la seguridad». El acuerdo permite potencialmente a China desplegar a la policía armada y al ejército en las Islas Salomón.[22] En mayo, China organizó la segunda reunión de los ministros de asuntos exteriores de China y los países de las islas del Pacífico, y propuso promover una «asociación estratégica integral» para avanzar en los intereses políticos, culturales, de seguridad y de cambio climático, y también para luchar contra la pandemia.[23] Más o menos en la misma fecha, Microsoft identificó el malware GADOLINIUM en los sistemas gubernamentales de las Islas Salomón. RADIUM también ejecutó código malicioso en sistemas de una empresa de telecomunicaciones en Papúa Nueva Guinea. Creemos que estas actividades iban dirigidas probablemente a obtener inteligencia con el fin de apoyar la estrategia regional general de China.

Microsoft interrumpió las operaciones de DISRUPT, pero el grupo de amenazas muestra su persistencia.

En diciembre de 2021, la Unidad de delitos digitales de Microsoft (DCU) presentó alegaciones ante el Tribunal de Distrito de EE. UU. del Distrito Este de Virginia para pedir autorización para incautar 42 dominios de mando y control (C2) controlados por NICKEL. Estos dominios C2 se estaban utilizando en operaciones contra gobiernos, entidades diplomáticas y ONG de Centroamérica y Sudamérica, el Caribe, Europa y Norteamérica desde septiembre de 2019.[24] A través de estas operaciones, NICKEL logró acceso a largo plazo a varias entidades y filtró continuamente datos de algunas víctimas desde finales de 2019.

Mientras China siga estableciendo relaciones económicas bilaterales con más países (a menudo en acuerdos asociados con la BRI), la influencia mundial de China seguirá creciendo. Creemos que los actores de amenazas del estado chino y sus afiliados persiguen objetivos en sus sectores gubernamental, diplomático y ONG para obtener nuevos conocimientos, probablemente en busca de espionaje económico o de los objetivos tradicionales de obtención de inteligencia. Desde su desmantelamiento por parte de Microsoft. NICKEL ha dirigido sus ataques a varios organismos gubernamentales, probablemente intentando recuperar el acceso perdido. Entre finales de marzo y mayo de 2022, NICKEL volvió a atacar a cinco organismos gubernamentales en todo el mundo. Esto sugiere que el grupo consiguió puntos de entrada adicionales a esas entidades o recuperó el acceso a través de nuevos dominios C2. La insistencia de NICKEL en atacar repetidamente a los mismos organismos públicos en todo el mundo indica la importancia de la tarea.

China está siendo más asertiva con respecto a su postura sobre política exterior. Creemos que el espionaje económico y la obtención de inteligencia habilitados por los ciberataques probablemente continuarán.

Conocimientos prácticos

1. Impulsa la defensa cibernética para mitigar las ciberamenazas de forma proactiva. La persistencia de los actores de amenazas de China requiere que las organizaciones identifiquen, protejan, detecten y respondan a las posibles intrusiones puntualmente.
2. Los actores de amenazas utilizan tareas programadas[25] como un método habitual de persistencia y evasión de las defensas. Asegúrate de que tu entorno emplea directrices de seguridad adicionales para protegerlo de esta técnica usada habitualmente.[26]
3. Seguimos observando el uso de shells web como un vector inicial en las redes atacadas.[27] Las organizaciones deben reforzar sus sistemas contra ataques de shell web que puedan proporcionar a los atacantes acceso para ejecutar comandos remotos.[28]

Enlaces a información adicional (pueden estar en inglés)

- NICKEL dirige sus ataques a organizaciones gubernamentales de Latinoamérica y Europa | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft (DSU)
- Cómo proteger a las personas de los ciberataques recientes | Microsoft On the Issues

Irán acrecienta sus amenazas tras el cambio de poder

Microsoft ha observado cómo los grupos del Estado iraní y sus afiliados han aumentado el ritmo y el alcance de los ciberataques contra Israel, han expandido los ataques de ransomware más allá de los adversarios regionales a víctimas estadounidenses y europeas, y han dirigido sus ataques a infraestructuras críticas de alto perfil en EE. UU. para, como mínimo, estar preparados para posibles ciberataques destructivos.

El aumento de las agresiones cibernéticas por parte de los agentes del Estado iraní se ha producido tras el cambio de poder presidencial. En el verano de 2021, el presidente extremista Ibrahim Raisi sustituyó al presidente moderado Hassan Rouhani. En fuerte contraste con Raisi, que es un protegido del líder supremo y cercano aliado de los Cuerpos de la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés), la inclinación por la diplomacia del expresidente Rouhani a menudo lo ha puesto en contra del líder supremo y de los altos directivos de los IRGC.[29] Parece que las posiciones extremistas de la administración de Raisi han aumentado la predisposición de los agentes iraníes a tomar medidas más agresivas contra Israel y los países occidentales, especialmente los Estados Unidos, a pesar de que se haya reanudado el compromiso diplomático para reactivar el acuerdo nuclear con Irán.

Mayor ritmo y alcance de los ciberataques iraníes contra Israel

A las pocas semanas de que Raisi completara la formación de su equipo de política exterior,[30] agentes del Estado iraní reanudaron sus ciberataques destructivos contra Israel a un ritmo más rápido que el año anterior. Estos ataques de ransomware y «hack-and-leak» se perpetraron cada pocas semanas a partir de septiembre e implicaron al menos a tres agentes afiliados a Irán, lo que sugiere que los ataques podrían haber formado parte de una campaña nacional de represalias contra Israel. En al menos un caso, Microsoft identificó un ataque de ransomware contra una organización israelí a finales de 2021 cuyo objetivo era ocultar un ataque de eliminación de datos subyacente. El análisis del malware por parte de Microsoft determinó que el ransomware distribuido la víctima estaba programado para ejecutar malware «wiper» después del cifrado.

En 2022, los ciberataques iraníes aumentaron en cuanto a los objetivos y la forma de los ataques. En febrero, DEV-0198 intentó perpetrar un ataque destructivo contra infraestructuras críticas israelí. Microsoft también cree que un agente afiliado a Irán es el responsable más probable de un ciberataque sofisticado que activó las sirenas de un cohete de emergencia israelí en junio probablemente mediante software que ajusta el audio a través de redes IP.

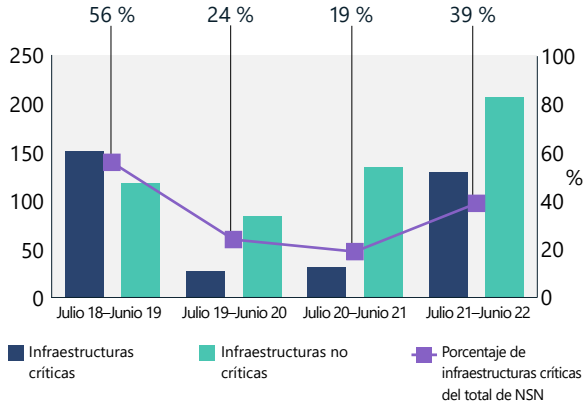
La amenaza iraní a las infraestructuras críticas de EE. UU. e Israel durante todo el año

Agentes del Estado iraní que Microsoft considera afiliados a los IRGC (PHOSPHORUS y DEV-0198) dirigieron ataques a infraestructuras críticas de alto perfil de EE. UU. e Israel desde finales de 2021 hasta mediados de 2022. El objetivo probable era proporcionar a Teherán opciones para tomar represalias contra los mismos sectores que altos funcionarios de los IRGC acusaron como responsables estadounidenses e israelíes de perturbaciones en Irán.[31] Creemos que esta actividad está relacionada con las declaraciones de finales de octubre de 2021 del general de los IRGC Gholamreza Jalali, jefe de la Organización de Defensa Pasiva de Irán, que se hizo eco de las declaraciones de otras figuras influyentes del régimen que acusaban a Estados Unidos e Israel de perpetrar ciberataques en puertos, ferrocarriles y estaciones de combustible de Irán.[32] Jalali repitió esta acusación en un discurso preparado durante la oración de los viernes subido en un podio con la imagen de un misil que tenía grabadas las letras «USA», lo que sugiere que sus superiores compartían el mismo punto de vista.[33]

PHOSPHORUS comenzó a analizar de forma generalizada las organizaciones estadounidenses en octubre de 2021 en busca de las vulnerabilidades Fortinet y ProxyShell sin parches. Una vez expuestos, estos sistemas sin parches se utilizaron para ejecutar ataques de ransomware, en varios casos contra infraestructuras críticas de los Estados Unidos y otras naciones occidentales. Estos fueron los primeros casos confirmados de ataques de ransomware asociados al Estado iraní fuera de Oriente Medio. Tras el ciberataque contra las estaciones de combustible de Irán a finales de octubre, Microsoft observó un aumento de los ataques de ransomware iraníes contra empresas estadounidenses, lo que sugiere una posible relación.

Al mismo tiempo, PHOSPHORUS dirigió sus ataques, a menudo a través de «spear phishing», a empresas de infraestructuras críticas de Estados Unidos de alto perfil, incluidos los principales puertos de mar y aeropuertos de entrada, sistemas de transporte, empresas de servicios públicos y empresas de petróleo y gas. Estos ataques, que a menudo se realizaban mediante «spear phishing», se extendieron hasta mediados de 2022. Los objetivos coinciden directamente con los sectores de Teherán que han culpado a los Estados Unidos e Israel de los ataques a Irán y probablemente proporcionaron a Irán opciones para tomar represalias. El ataque de objetivos casi idénticos proporcionaría una oportunidad para frenar estos ataques en el futuro, a la vez que trataría de evitar que se escalaran al indicar la causa de los ataques sin admitir la culpa.

Reaparición de los ataques a infraestructuras iraníes



Los ataques iraníes a infraestructuras críticas llegaron a los niveles más altos observados desde finales de 2018 hasta principios de 2019. Utilizamos la Directiva Política Presidencial de Estados Unidos 21 (PPD-21) para determinar si una empresa se ajustaba a los criterios de infraestructuras críticas. (De julio de 2021 a junio de 2022).

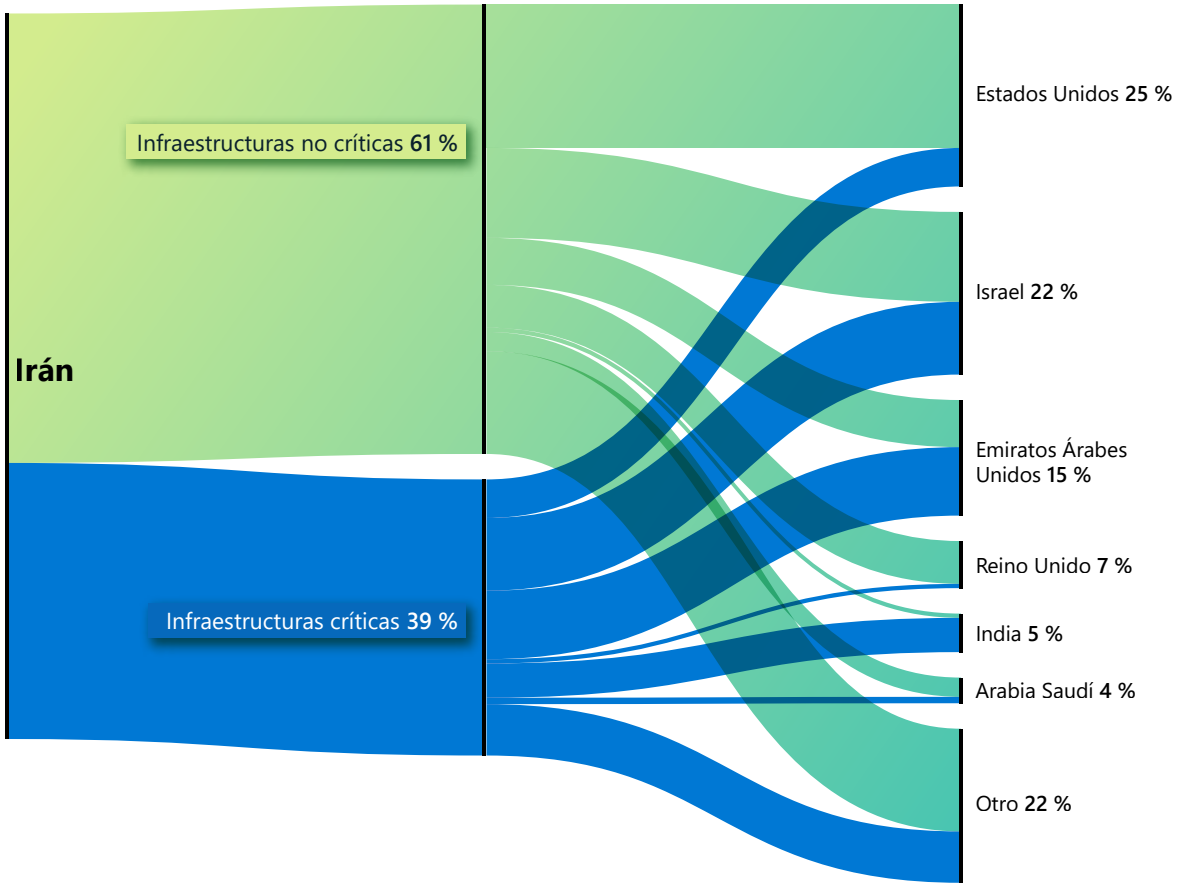
Irán acrecienta sus amenazas tras el cambio de poder

Continuación

En Israel, DEV-0198 atacó a ferrocarriles, empresas logísticas, proveedores de software de empresas logísticas y empresas de combustible israelíes y especialmente a las gasolineras. A principios de 2022, el grupo perpetró un ataque destructivo en la red de una importante empresa logística israelí, que obligó a la empresa a apagar sus ordenadores y detener algunas de sus operaciones para contenerlo. En otro caso, observamos el intento del grupo de acceder a la red de un importante proveedor de transporte israelí a través de credenciales robadas o reutilizadas. Mientras tanto, otro agente iraní, DEV-0343, cuyos ataques dirigidos a empresas de defensa, transporte marítimo e imágenes por satélite sugiere que estaba relacionado con los IRGC, atacó cuentas de entidades israelíes relacionadas con el transporte y los puertos a principios de 2021.

Es probable que los grupos de amenazas iraníes sigan siendo una amenaza para las empresas de transporte y energía de EE. UU. e Israel, particularmente mientras sigan los esfuerzos diplomáticos para reactivar el acuerdo nuclear iraní y Washington, Tel Aviv y Teherán busquen medios coercitivos alternativos para garantizar las concesiones.

Ataques iraníes a infraestructuras críticas por país



Los ataques iraníes a infraestructuras críticas se produjeron sobre todo contra organizaciones de Israel, los Emiratos y EE. UU.

Es probable que los agentes iranís sigan siendo una amenaza para las empresas de transporte y energía de EE. UU. e Israel el próximo año.

Los grupos iraníes han expandido los ataques de ransomware más allá de los adversarios regionales y los están dirigiendo a infraestructuras críticas de EE. UU. e Israel de alto perfil.

Conocimientos prácticos

1. Mejora la higiene cibernética general de tu organización habilitando soluciones sin contraseñas como MFA y aplicando su uso a todas las conexiones remotas para mitigar cualquier ataque potencial a credenciales.
2. Evalúa la autenticidad de todo el tráfico de correo electrónico entrante para asegurarte de que la dirección del remitente sea legítima.
3. Aplica parches lo antes posible y a menudo.[34]
4. Revisa y audita cada una de las relaciones de tus partners con los proveedores de servicios para minimizar los permisos innecesarios entre tu organización y los proveedores. Microsoft recomienda retirar el acceso a todas las relaciones con partners que parezcan desconocidas o que aún no se hayan auditado.[35]

Enlaces a información adicional (pueden estar en inglés)

- Aumento de los ataques iraníes al sector de TI | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft (DSU)
- Defensa de los ataques DEV-0343 vinculados con Irán, GIS y sectores marítimos | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft (DSU)

Grupo establecido en el Líbano vinculado a los ataques de Irán a Israel

Microsoft supervisa las actividades de ciberamenazas independientemente de la plataforma, las víctimas objetivo o la región geográfica. Mantenemos la visibilidad y la búsqueda activa de amenazas en todo el mundo para crear mejores medidas de detección para nuestros clientes.

Aunque las amenazas de Rusia, China, Irán y Corea del Norte representan la mayor parte de la actividad de los agentes de los estados nación observados, también rastreamos y comunicamos las amenazas de los países miembros de la OTAN de las naciones democráticas. El año pasado, publicamos la actividad de un agente emplazado en Turquía (SILICON) y un agente emplazado en Vietnam (BISMUTH). Este año, vamos a ampliar los detalles de un grupo con sede en el Líbano que ya dimos a conocer públicamente.[36]

Microsoft descubrió a un grupo con sede en el Líbano previamente desconocido que creemos con confianza moderada que operó en coordinación con agentes afiliados al Ministerio de Inteligencia y Seguridad de Irán (MOIS, por sus siglas en inglés). Tal colaboración o dirección de Teherán concordaría con las revelaciones de finales de 2020 de que el gobierno de Irán estaba utilizando a terceros para llevar a cabo operaciones cibernéticas, lo que probablemente justificaría la negación de la culpabilidad de Irán.

En la actividad observada, POLONIUM atacó a decenas de organizaciones con sede en Israel y a una IGO con operaciones en Líbano entre febrero y mayo de 2022, antes de que Microsoft cerrara y revelara públicamente su actividad. Casi la mitad de las organizaciones israelíes formaban parte del sector de defensa de Israel o tenían vínculos con empresas de defensa israelíes, lo que indica que el grupo tiene un conjunto de intereses similares a los de Irán en la obtención de inteligencia de Israel o directamente su lucha contra Israel.[37]

Los vínculos evaluados de POLONIUM con los grupos del MOIS se basan en la coincidencia de víctimas y en el uso de las mismas herramientas y técnicas.

- Solapamiento de víctimas: un grupo del Estado iraní vinculado al MOIS de Irán, que Microsoft rastrea como MERCURY, atacó previamente a varias víctimas de POLONIUM, lo que indica una convergencia de los requisitos de la misión o un posible «traspaso» de víctimas entre los grupos.
- Herramientas y técnicas comunes: de forma similar a POLONIUM, el MSTIC observó cómo DEV-0588 (también denominado CopyKittens) utiliza habitualmente AirVPN para las operaciones y DEV-0133 (también conocido como Lyceum[38]) utiliza OneDrive para C2 y la filtración. Al igual que los agentes del estado iraní, POLONIUM usó un proveedor de servicios en el cloud para atacar a una empresa de aviación y un bufete de abogados israelíes.[39]

POLONIUM desplegó una serie de implantes personalizados utilizando servicios en el cloud para C2 y filtración de datos, especialmente OneDrive y DropBox. POLONIUM, a menudo, creaba aplicaciones de OneDrive únicas para los objetivos, probablemente para eludir la detección.

En junio de 2022, Microsoft suspendió más de 20 aplicaciones de OneDrive creadas por POLONIUM, notificó a las organizaciones afectadas e implementó una serie de actualizaciones de inteligencia de seguridad para poner en cuarentena las herramientas desarrolladas por POLONIUM.

Microsoft fue capaz de detectar y desactivar el uso de POLONIUM de OneDrive como C2.

Conocimientos prácticos

1. Actualiza las herramientas antivirus[40] y asegúrate de que la protección del cloud[41] esté activada para detectar los indicadores relacionados.
2. Los clientes con relaciones con proveedores de servicios deben asegurarse de revisar y auditar todas las relaciones con los partners para minimizar los permisos innecesarios entre la organización y los proveedores.[42] Retira inmediatamente el acceso a las relaciones de partners que parezcan desconocidas o que no se hayan auditado.

Enlaces a información adicional (pueden estar en inglés)

- Exposición de la actividad y la infraestructura de POLONIUM para atacar organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft (DSU)
- MERCURY aprovecha las vulnerabilidades Log4j 2 en sistemas sin parches para atacar a organizaciones israelíes | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Equipo de investigación de Microsoft 365 Defender, Inteligencia sobre amenazas de Microsoft Defender

Capacidades cibernéticas norcoreanas empleadas para lograr los tres principales objetivos del régimen

Las prioridades cibernéticas de Corea del Norte durante el año pasado reflejaban las prioridades generales del gobierno. Kim Jong Un hizo hincapié en las tres prioridades de crear capacidad de defensa, mejorar la difícil situación económica del país y garantizar la estabilidad interna en varias direcciones clave.[43] Las medidas adoptadas por los agentes del estado de Corea del Norte muestran claramente que se estás utilizando los ciberataques para lograr estos tres objetivos.

Agentes de Corea del Norte utilizaron una serie de tácticas para intentar penetrar en empresas aeroespaciales de todo el mundo.

Los grupos de amenazas de Corea del Norte, principalmente CERIUM y ZINC, utilizaron una serie de tácticas para intentar penetrar en redes de empresas de defensa y aeroespaciales de todo el mundo. Cuando Corea del Norte se embarcó en el que ha sido su período más agresivo de pruebas de misiles en la primera mitad de 2022, utilizó el ciberespionaje para ayudar a los investigadores norcoreanos a obtener una ventaja en el desarrollo de sistemas de defensa autóctonos y contramedidas para los avances realizados por sus adversarios.

Hemos observado cómo COPERNICIUM atacaba a una serie de empresas relacionadas con criptomonedas en todo el mundo, a menudo con éxito, para ayudar a apoyar la difícil situación económica de Corea del Norte. Aunque no podemos confirmar si el grupo fue capaz de obtener dinero después de un ataque, sí observamos que COPERNICIUM infectó a decenas de máquinas enviando documentos malintencionados enmascarados como propuestas de otras empresas de criptomonedas.

Por último, un grupo que Microsoft rastrea como DEV-0215 trabajó para mantener la estabilidad y la lealtad en Corea del Norte atacando a organizaciones de noticias que informan sobre asuntos de Corea del Norte. Estos canales de noticias tienen fuentes tanto en Corea del Norte como dentro de las comunidades de disidentes, que Pyongyang considera una amenaza existencial. Asimismo, el grupo trabajó para obtener acceso a redes de grupos cristianos de habla coreana, que suelen oponerse a Corea del Norte y que trabajan activamente con los disidentes norcoreanos.

Ataques a empresas aeroespaciales y de defensa

Agentes de Corea del Norte liderados por CERIUM y SES hicieron un esfuerzo considerable en el desarrollo de tácticas destinadas a penetrar en empresas de defensa y aeroespaciales. CERIUM sondeó repetidamente redes privadas virtuales (VPN) surcoreanas descargando clientes y buscando puntos débiles. También descargó aplicaciones comunes utilizadas por clientes del ejército y de la administración surcoreanos, probablemente en busca de vulnerabilidades. El grupo siguió de cerca los acontecimientos actuales y escribió nuevos documentos señuelo que utilizaban temas de gran repercusión mediática como cebo para animar a los objetivos a hacer clic en sus archivos ejecutables y enlaces de malware.

Tanto ZINC como CERIUM usaron las redes sociales y la ingeniería social en las campañas. ZINC fue particularmente hábil en crear perfiles falsos en LinkedIn y otros sitios de redes sociales profesionales, donde sus operadores se hacían pasar por reclutadores de importantes empresas aeroespaciales y de defensa. Mediante estos perfiles, enviaron enlaces o archivos adjuntos maliciosos a posibles víctimas utilizando mensajes directos en redes sociales o correo electrónico.

Además de a los empleados de corporaciones, CERIUM también dirigió muchos de sus ataques a los miembros del ejército surcoreano, mostrando un especial interés tanto en las academias militares surcoreanas como en los miembros militares que trabajan en la enseñanza.

Ataques a las criptomonedas para equilibrar las pérdidas

Desde que se impusieron las sanciones de la ONU en 2016, la economía de Corea del Norte sigue contrayéndose, agravada por desastres naturales como inundaciones[44] y sequías[45], así como un bloqueo casi total de fronteras a las importaciones desde el inicio de la pandemia de la COVID-19 a principios de 2020.[46] Aunque Corea del Norte abrió sus fronteras comerciales con China brevemente a principios de 2022, pronto se cerraron de nuevo.[47] A mediados de mayo, Corea del Norte registró su primer caso nacional de COVID-19.[48] Desde entonces ha aplicado una estrategia de «COVID cero» al estilo chino de confinamientos masivos para combatir el virus que ha afectado negativamente a la economía ya frágil de Corea del Norte.

El grupo norcoreano COPERNICIUM trató de compensar parte de los ingresos perdidos robando dinero, normalmente en forma de criptomonedas, a cualquier empresa en cuyas redes pudieran penetrar. Hemos visto decenas de máquinas atacadas pertenecientes a empresas relacionadas con criptomonedas en Estados Unidos, Canadá, Europa y en toda Asia. COPERNICIUM atacó incluso máquinas pertenecientes a empresas relacionadas con criptomonedas del mayor aliado de Corea del Norte, China, tanto en el continente como en Hong Kong. El grupo usó ampliamente las redes sociales para su reconocimiento inicial y su enfoque a los objetivos. Los agentes creaban perfiles que simulaban ser desarrolladores o agentes sénior de empresas relacionadas con las criptomonedas. A continuación, establecían relaciones con agentes del sector, enviando enlaces o archivos maliciosos una vez que habían creado una relación.

Capacidades cibernéticas norcoreanas empleadas para lograr los tres principales objetivos del régimen

Continuación

Un grupo relacionado con PLUTONIUM desarrolla e implementa ransomware

Un grupo de agentes procedentes de Corea del Norte que Microsoft rastrea como DEV-0530 comenzó a desarrollar y utilizar ransomware en ataques en junio de 2021. Este grupo, que se denominaba H0lyGh0st, utilizó una carga útil de ransomware con el mismo nombre para sus campañas y atacó con éxito a pequeñas empresas de varios países en septiembre de 2021.

Microsoft cree que DEV-0530 tenía conexiones con otro grupo establecido en Corea del Norte rastreado como PLUTONIUM (también denominado DarkSeoul o Andariel). Aunque el uso del ransomware H0lyGh0st en las campañas es exclusivo de DEV-0530, el MSTIC observó comunicaciones entre los dos grupos y vio que DEV-0530 utilizaba herramientas creadas exclusivamente por PLUTONIUM.

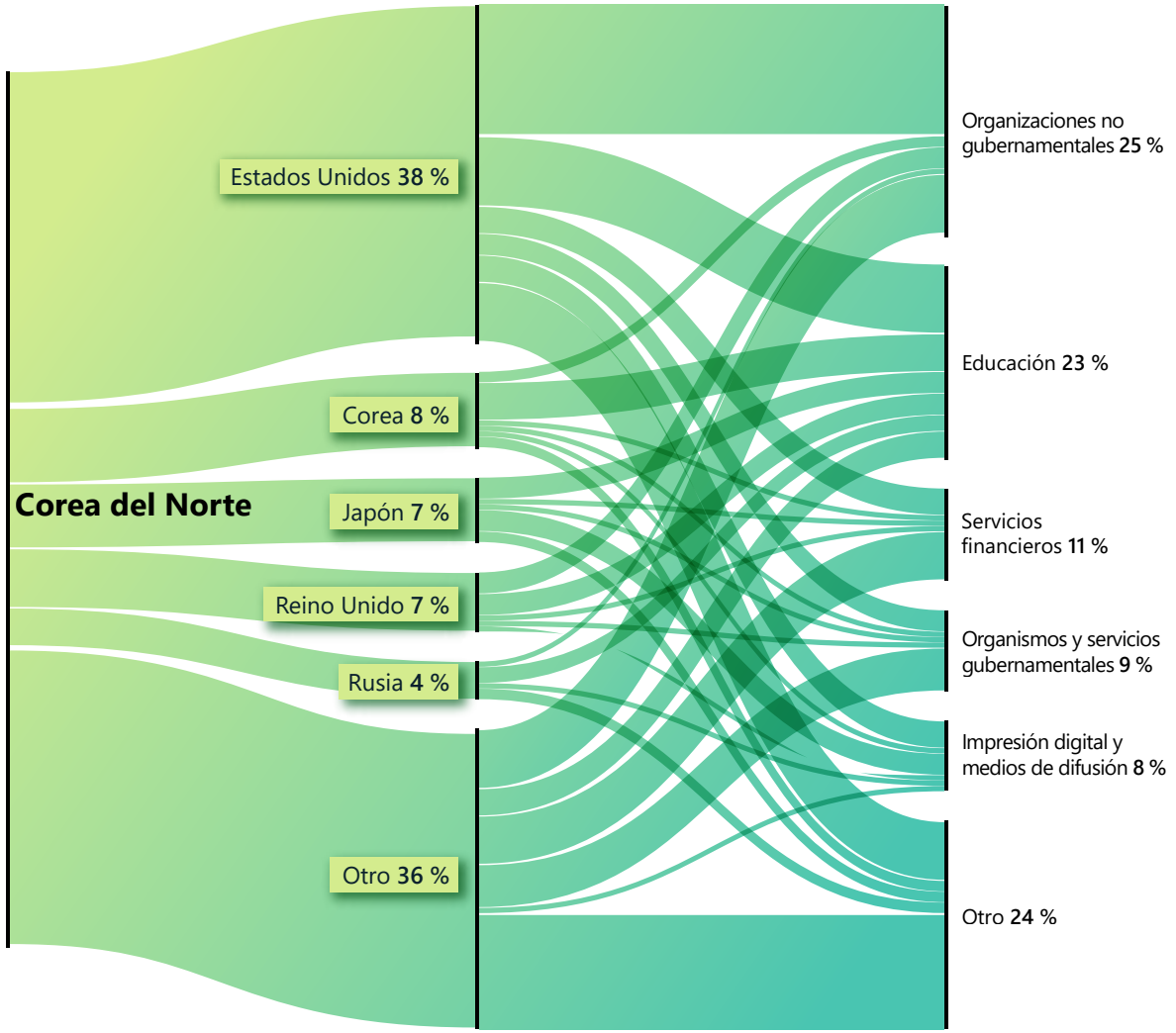
No es seguro que la actividad de DEV-0530 esté patrocinada por el gobierno. Aunque el gobierno podría haber ordenado ataques de ransomware por la misma razón por la que patrocina el robo de empresas de criptomonedas, también es posible que los agentes que se esconden detrás de DEV-0530 actuaran de forma independiente para ganar dinero para su propio beneficio. Si fueran hackers norcoreanos que operaban de forma independiente, eso explicaría por qué no se trataba de una actividad generalizada en comparación con las operaciones de robo patrocinadas por el gobierno contra empresas de criptomonedas.

Ataque a redacciones de noticias, disidentes, grupos religiosos y organizaciones de ayuda norcoreanos

El año pasado, el líder supremo Kim Jong Un hizo público su mayor interés por la seguridad interna y la lealtad que por los misiles y las armas nucleares. Al menos dos grupos del estado de Corea del Norte se centraron en aspectos que el régimen veía como amenazas internas, lo que refleja esta preocupación por los asuntos internos.

El primero fue un grupo que Microsoft rastrea como DEV-0215, con ataques dirigidos a organizaciones de medios de comunicación que siguen de cerca las noticias norcoreanas. Un motivo probable de este ataque es que estos medios de comunicación obtienen las noticias de los disidentes norcoreanos, de ciudadanos chinos que trabajan estrechamente con Corea del Norte e incluso de algunos ciudadanos norcoreanos dentro del país, utilizando diversos métodos para comunicarse con el mundo exterior. El gobierno norcoreano considera a estos grupos una amenaza existencial a su supervivencia, especialmente a los ciudadanos dentro de Corea del Norte que se consideran traidores y espías. DEV-0215 probablemente trató de identificar las fuentes de estos canales de noticias para neutralizar posibles filtraciones de información.

Corea del Norte: los cinco principales países y sectores de la industria objetivo de los ataques



Para Corea del Norte sus principales enemigos son Estados Unidos, Corea del Sur y Japón. Pese a que Rusia es un aliado desde hace mucho tiempo, los actores de amenazas norcoreanos han atacado a think tanks, académicos y funcionarios diplomáticos rusos para obtener inteligencia de las opiniones de los rusos sobre los asuntos mundiales.

Capacidades cibernéticas norcoreanas empleadas para lograr los tres principales objetivos del régimen

Continuación

Microsoft también vio pruebas de cómo DEV-0215 atacaba a las comunidades cristianas de habla coreana. Las iglesias evangelistas surcoreanas suelen ser críticas con los gobiernos de Corea del Norte y Corea del Sur que están a favor de mantener relaciones con Corea del Norte. Es probable que estas iglesias realicen campañas de divulgación de los disidentes y que algunas participen en labores humanitarias con Corea del Norte. Corea del Norte las considera una amenaza porque, aunque el flujo de deserciones procedentes de Corea del Norte prácticamente se frenó en seco durante la pandemia,[49] estos grupos cristianos a menudo desempeñan un papel crítico en la ayuda a los desertores. DEV-0215 ha generado documentos falsos sobre conferencias cristianas de ponentes coreanos como señuelos para atacar al grupo y descubrir quién está ayudando a organizar las deserciones.

Por último, el grupo de estado OSMIUM mostró un interés continuo en las organizaciones de ayuda internacional durante todo el año, incluidas las organizaciones que han ayudado a Corea del Norte en el pasado. Aunque Corea del Norte ha rechazado por lo general las ofertas de ayuda de fuera del país, especialmente desde el estallido de la COVID-19,[50], es posible que esté considerando aceptar estos ofrecimientos de ayuda, pero se muestra cautelosa por las ramificaciones de seguridad que implica permitir que los trabajadores de ayuda extranjeros entren en el país. Corea del Norte puede estar penetrando en las redes de organizaciones de ayuda en todo el mundo para determinar si permite esa ayuda en su propio país.

Conocimientos prácticos

1. Los agentes del Estado norcoreano son competentes, implacables y creativos, pero las organizaciones pueden defenderse de ellos.
2. La mayoría de los ataques que llegan a término se pueden detener con una higiene cibernética básica, como la autenticación de dos factores o abstenerse de abrir archivos adjuntos de personas desconocidas en un entorno virtual.

Enlaces a información adicional (pueden estar en inglés)

- El actor de amenazas norcoreano ataca a pequeñas y medianas empresas con ataques de ransomware H0lyGh0st | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Unidad de seguridad digital de Microsoft (DSU)

Los expertos de Corea del Norte llevan mucho tiempo debatiendo sobre si el gobierno norcoreano se toma en serio sus declaraciones públicas o si es un mero «postureo». La correspondencia de los ciberataques con las prioridades anunciadas por Corea del Norte valida la creencia de que Corea del Norte se cree lo que dice cuando habla públicamente sobre sus objetivos.

Los cibermercenarios amenazan la estabilidad del ciberespacio

Hay un sector creciente de empresas privadas que desarrollan y venden herramientas, técnicas y servicios que permiten a sus clientes, a menudo administraciones públicas, irrumpir en las redes, ordenadores, teléfonos y dispositivos conectados a Internet. Estas entidades, un activo para los agentes de los estados nación, suelen poner en peligro a disidentes, defensores de los derechos humanos, periodistas, defensores de la sociedad civil y otros ciudadanos privados. Nos referimos a ellos como cibermercenarios o agentes ofensivos del sector privado.

Un mundo donde las empresas del sector privado crean y venden ciberamenazas es más peligroso para los consumidores, las empresas de todos los tamaños y las administraciones públicas. Estas herramientas ofensivas se pueden utilizar de maneras que contravengan las normas y los valores democráticos y de buen gobierno. Microsoft cree que la protección de los derechos humanos es una obligación fundamental y algo que nos tomamos muy en serio restringiendo la «vigilancia como servicio» en todo el mundo.

Microsoft ha visto cómo algunos agentes estatales de regímenes democráticos y autoritarios subcontratan el desarrollo o el uso de tecnología de «vigilancia como servicio». Así es como evitan la rendición de cuentas y la supervisión, y como adquieren capacidades que serían difíciles de desarrollar de forma nativa.

> Estas armas cibernéticas proporcionan a los Estado nación capacidades de vigilancia que no habrían podido desarrollar ellos mismos.

El mercado en el que operan los cibermercenarios es opaco. Sin embargo, seguimos observando cómo estos grupos utilizan ataques de día cero e incluso ataques de clic cero que no requieren ninguna interacción de las víctimas, lo que permite la vigilancia como servicio.

Microsoft anunció recientemente la existencia de un agente del sector privado europeo denominado KNOTWEED, un PSOA con sede en Austria llamado DSIRF. Varios informes de noticias han vinculado a la empresa con el desarrollo e intento de vender un conjunto de herramientas de malware llamado Subzero.[51] Entre las víctimas se incluyen bufetes de abogados, bancos y consultorías estratégicas en países como Austria, Reino Unido y Panamá.[52]

Debido a que estas capacidades de vigilancia de amenazas ya no son capacidades altamente confidenciales creadas por las agencias de defensa e inteligencia, sino más bien productos comerciales que se ofrecen ahora a las empresas y los particulares, cualquier régimen normativo para las armas cibernéticas tiene que ir más allá del control de las exportaciones. El impacto de estas armas cibernéticas puede ser devastador.

Cuando un cibermercenario aprovecha una vulnerabilidad de un producto o servicio, pone en peligro todo el ecosistema informático. Cuando las vulnerabilidades se identifican públicamente, las empresas emprenden una carrera contrarreloj para publicar medidas de seguridad antes de que sobrevenga un ataque más amplio (véase el análisis anterior sobre la explotación de vulnerabilidades). Este es un ciclo peligroso y difícil tanto para los proveedores de software (que deben desarrollar los parches con rapidez) como para los consumidores de los productos (que deben implementar los parches inmediatamente).

Como miembro fundador del Cybersecurity Tech Accord[53]— una importante alianza que aúna a más de 150 empresas tecnológicas— Microsoft se ha comprometido a no participar en operaciones ofensivas online. Nos atenemos a ese compromiso y a nuestras responsabilidades en materia de derechos humanos. Hemos participado en desmantelamientos técnicos e impugnaciones legales para poner de relieve el impacto negativo causado por los servicios prestados por los cibermercenarios y seguiremos protegiendo a nuestros clientes cuando veamos abusos.

> Los cibermercenarios crean y proporcionan capacidades de «vigilancia como servicio» tecnológicamente sofisticadas y ampliamente disponibles, incluido malware avanzado y una serie de técnicas.

Conocimientos prácticos para los gobiernos

1. Implementa requisitos de transparencia y supervisión de vigilancia como servicio, particularmente en las adquisiciones, incluida la prohibición de comprar a estos actores de amenazas, como ha hecho Estados Unidos con el listado de empresas del Departamento de Comercio en la Entity List (Lista de entidades).
2. Establece restricciones para los exempleados de este sector.
3. Procura implantar las obligaciones de «conoce a tu cliente» y animar a las empresas a mantener sus compromisos de derechos humanos.

Enlaces a información adicional (pueden estar en inglés)

- Desentrañando a KNOTWEED: un actor de amenazas del sector privado europeo que usa ataques de día 0 | Centro de inteligencia sobre amenazas de Microsoft (MSTIC), Centro de respuesta de seguridad de Microsoft (MSRC), RiskIQ (Inteligencia sobre amenazas de Microsoft Defender)
- Continuando con la lucha contra las ciberamenazas del sector privado | Microsoft On the Issues

Aplicación de normas de ciberseguridad para disfrutar de tranquilidad y seguridad en el ciberespacio

Necesitamos urgentemente un marco global coherente que priorice los derechos humanos y proteja a las personas del comportamiento online irresponsable de los países. En ninguna otra parte resulta más evidente esto que en la guerra de Ucrania. Además de un esfuerzo estratégico global, los gobiernos pueden actuar ahora para causar un impacto positivo inmediato.

Hace cinco años, Microsoft organizó una «Convención de Ginebra Digital» para promover responsabilidades y obligaciones entre los sectores para defender la paz y la seguridad online. El ciberespacio estaba surgiendo como un dominio singular y volátil de conflicto y competencia entre estados, y los ataques eran cada vez más habituales, incluso en tiempos de paz.

Hoy en día, sigue habiendo una necesidad clara de este tipo de marco de trabajo, evidenciado por los ciberataques rusos contra Ucrania como parte de la invasión rusa. Esta guerra ha creado una nueva primera línea de combate que es radicalmente diferente de la que conocíamos.

Aportar estabilidad al ciberespacio exigirá fortalecer y rediseñar las instituciones de gobierno globales para adecuarlas a tal fin. El ciberespacio es radicalmente diferente a otros dominios: no tiene límites, es sintético y se mantiene en gran medida gracias al sector privado. Esto implica pedir a la industria tecnológica que asuma una mayor responsabilidad tanto en la seguridad de los productos y servicios como del ecosistema digital más amplio. Aunque se han realizado progresos notables en todos los frentes, los desafíos han aumentado drásticamente.

Debemos redoblar los esfuerzos colectivos para defender la seguridad del ciberespacio. No podemos dar por hecho los derechos y libertades online. Mientras luchamos por abordar los desafíos, los agentes malintencionados están planificando cómo y dónde atacar mediante la IA, aprovechando la desinformación y encontrando formas de socavar el incipiente metaverso. Los defensores de los derechos humanos, la industria tecnológica y los gobiernos que respetan los derechos deben trabajar juntos para obtener una visión positiva de un mundo online seguro y fiable. El camino que nos espera es largo, pero hay cosas que los gobiernos pueden hacer hoy mismo para mejorar inmediatamente el ecosistema de ciberseguridad:

- Citar normas, leyes y consecuencias en las atribuciones. Una mejora importante de los últimos cinco años ha sido la velocidad y coordinación de las atribuciones gubernamentales de los ciberataques. Además de simplemente nombrar y culpar, estas declaraciones deben resaltar qué leyes o normas internacionales se infringen y qué tipo de consecuencias se impondrán para ayudar a fortalecer el reconocimiento de las expectativas internacionales.
- Aclarar la interpretación del derecho internacional online. Aunque los gobiernos están de acuerdo en que el derecho internacional se aplica en Internet, todavía no está claro cómo se aplica en situaciones específicas. Esto es especialmente pertinente en las consecuencias de la invasión de Ucrania. Los gobiernos pueden avanzar mucho en la definición de las expectativas, en evitar los malentendidos y en generar confianza explicando cómo entienden sus obligaciones en derecho internacional.
- Consultar a otras partes interesadas. Mientras los foros internacionales continúan descubriendo las mejores maneras de incluir de forma sistemática la multilateralidad, los gobiernos pueden respaldar el diálogo informado consultando a las comunidades formadas por distintas partes interesadas, en particular al sector tecnológico, para garantizar que el diálogo se beneficie de aquellas personas con conocimientos indispensables.
- Formar un organismo permanente que apoye el comportamiento responsable de los estados en el ciberespacio. El trabajo de los foros internacionales para promover el comportamiento responsable de los estados online nunca ha sido tan importante. Es evidente que se necesita un mecanismo de la ONU permanente para abordar el ciberespacio como un dominio de conflicto.
- Definir nuevas normas para las amenazas en evolución. Las amenazas al ciberespacio evolucionan constantemente junto con las innovaciones en tecnología. Aunque las normas internacionales deben ser neutrales en cuanto a la tecnología, tendrán que actualizarse y atenuarse en función de los cambios que se produzcan en el panorama de amenazas y en la forma en que usamos la tecnología. Incluso hoy en día, vemos que se está abusando de las deficiencias del marco internacional existente. Los estados deben comprometerse a proteger expresamente los procesos básicos que sustentan el ecosistema digital que actualmente no están protegidos, como el proceso de actualización de software. Además, hay áreas específicas que merecen protecciones adicionales. Por ejemplo, como hemos aprendido a raíz de la pandemia, las normas para proteger la atención sanitaria son esenciales.

El volumen y la sofisticación de los agentes y los ataques de los estados nación están aumentando, lo que está creando una situación insostenible.

La acción inmediata es imprescindible: existen medidas que las administraciones pueden emprender ahora mismo para mejorar inmediatamente el ecosistema de ciberseguridad, incluida la implementación de normas y reglas acordadas sobre el comportamiento de los estados en el ciberespacio y trabajar con la comunidad mutisectorial más amplia para abordar las brechas emergentes.

Las instituciones multilaterales deben replantarse cómo hacer frente al desafío apremiante de los ciberataques a los estados nación.

Enlaces a información adicional (pueden estar en inglés)

- Un momento para el ajuste de cuentas: la necesidad de una respuesta de ciberseguridad firme y global | Microsoft On the Issues
- Los ciberataques dirigidos a la atención sanitaria deben parar | Microsoft On the Issues
- Se vislumbra el siguiente capítulo de la diplomacia cibernética en las Naciones Unidas | Microsoft On the Issues

Notas al pie

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. Las infraestructuras críticas de este capítulo se definen de acuerdo con la Directiva Política Presidencial 21 (PPD-21), Critical Infrastructure Security and Resilience (febrero de 2013).
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

Continuación de las notas al pie

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. En concreto, aplicar parches a los servidores de Exchange para las vulnerabilidades ProxyShell (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 y CVE-2021-27065, CVE-2021-34473). Además, asegúrate de aplicar parches a los dispositivos VPN SSL de Fortinet FortiOS en busca de vulnerabilidades.
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein, In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin, FOCUS Online, (2022), https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy, We unveil the «Subzero» state trojan from Austria, Europe-cities (2021), https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister, We unveil the state Trojan «Subzero» from Austria, Netzpolitik.org (2022), https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich.
52. Como se indica en nuestro blog técnico, la identificación de objetivos en un país no significa necesariamente que un cliente de DSIRF resida en el mismo país, ya que los ataques internacionales son habituales.
53. Página de inicio | Cybersecurity Tech Accord (cybertechaccord.org)

Dispositivos e infraestructura

Con la aceleración de la transformación digital, la seguridad de la infraestructura digital es más importante que nunca.

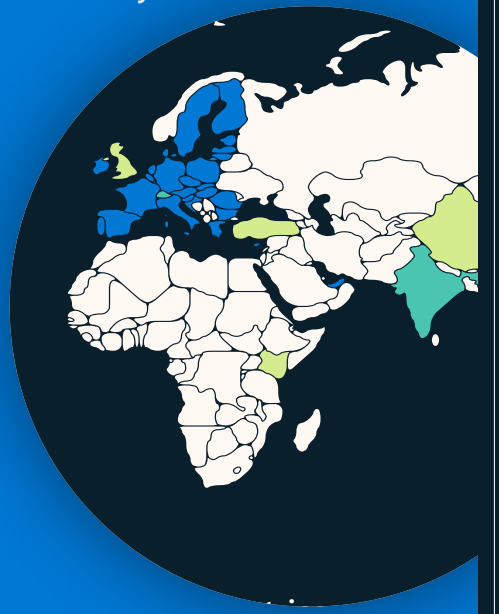
Información general sobre los

dispositivos y la infraestructura

La pandemia, junto con la rápida adopción de dispositivos con acceso a Internet de todo tipo como una forma de acelerar la transformación digital, ha aumentado enormemente la superficie de ataque del mundo digital.

Los ciberdelincuentes y los Estados nación están aprovechando rápidamente las ventajas. Aunque la seguridad del hardware y el software de TI se ha reforzado en los últimos años, la seguridad de los dispositivos del Internet de las cosas (IoT) y tecnología de las operaciones (OT) no ha seguido el mismo ritmo. Los actores de amenazas están atacando estos dispositivos para acceder a las redes y permitir el movimiento lateral, para establecer un punto de apoyo en una cadena de suministro o para interrumpir las operaciones de OT de la organización objetivo.

Gobiernos de todo el mundo están actuando para proteger las infraestructuras críticas mejorando la seguridad de IoT y OT.



Más información en la página 59

Se necesitan políticas de seguridad coherentes e interoperables a escala para garantizar una adopción generalizada.

Más información en la página 59

El malware como servicio se ha movido a grandes operaciones contra el IoT y OT expuestos en infraestructuras y servicios públicos, así como en redes corporativas.

Más información en la página 63

Los ataques contra dispositivos de administración remota están aumentando, con más de 100 millones de ataques observados en mayo de 2022, cinco veces más que el año pasado.

Más información en la página 62

Los atacantes aprovechan cada vez más las vulnerabilidades del firmware de los dispositivos de IoT para infiltrarse en las redes corporativas y perpetrar ataques devastadores.

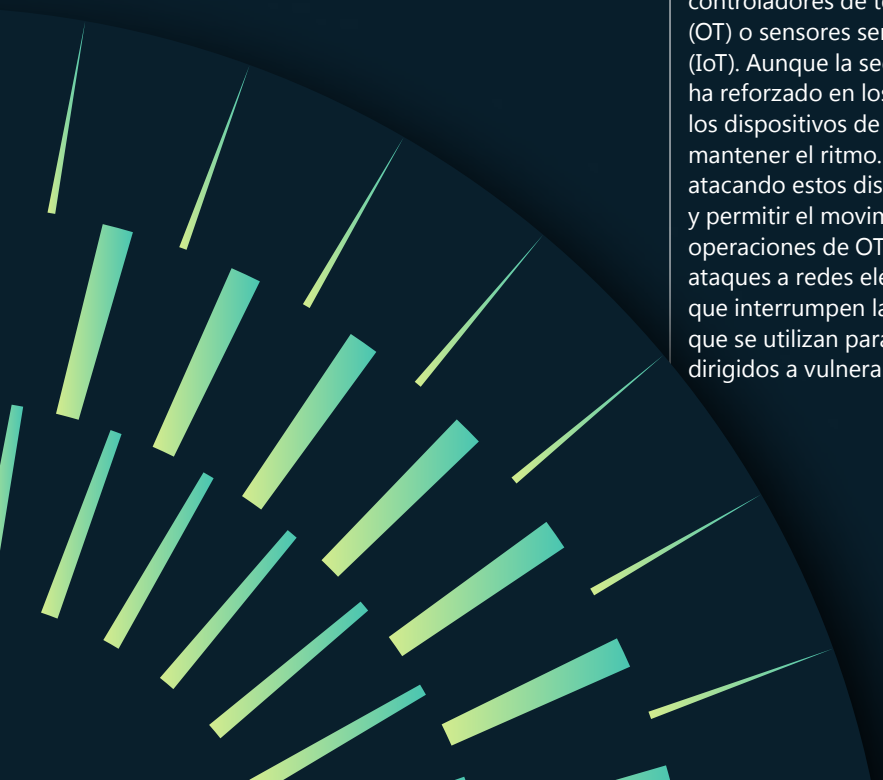
Más información en la página 65

El 32 % de las imágenes de firmware analizadas contenía al menos 10 vulnerabilidades críticas conocidas.

Más información en la página 66

Introducción

La aceleración de la transformación digital ha aumentado el riesgo de ciberseguridad para la las infraestructuras críticas y los sistemas cibernéticos y físicos.



En los últimos años, se han observado cambios sin precedentes en el mundo digital. Las organizaciones están evolucionando para aprovechar los avances en capacidad informática tanto del cloud inteligente como del perímetro inteligente. Como resultado de la pandemia, que obligó a las entidades a digitalizarse para sobrevivir, y del ritmo al que sectores de todo el mundo están adoptando dispositivos con conexión a Internet, la superficie de ataque del mundo digital está aumentando exponencialmente.

Esta rápida migración ha superado la capacidad de la comunidad de seguridad de seguir el ritmo. Durante el último año, hemos observado amenazas dirigidas a dispositivos de todas las partes de la organización, desde equipos informáticos tradicionales hasta controladores de tecnología de las operaciones (OT) o sensores sencillos del Internet de las cosas (IoT). Aunque la seguridad de los equipos de TI se ha reforzado en los últimos años, la seguridad de los dispositivos de IoT y OT no ha sido capaz de mantener el ritmo. Los actores de amenazas están atacando estos dispositivos para acceder a las redes y permitir el movimiento lateral o para interrumpir las operaciones de OT de las organizaciones. Hemos visto ataques a redes eléctricas, ataques de ransomware que interrumpen las operaciones de OT, routers de IoT que se utilizan para aumentar la persistencia y ataques dirigidos a vulnerabilidades del firmware.

Aunque la prevalencia de las vulnerabilidades de IoT y TO es un desafío para todas las organizaciones, las infraestructuras críticas corre un mayor riesgo debido a que los actores de amenazas se han dado cuenta de que deshabilitar los servicios críticos es un arma poderosa. El ataque de ransomware de 2021 al Oleoducto Colonial es una demostración de cómo los delincuentes pueden interrumpir un servicio crítico para aumentar las probabilidades de que se pague un rescate. Y los ciberataques de Rusia contra Ucrania demuestran que algunos estados nación consideran los ciberataques contra infraestructuras críticas un sabotaje aceptable para lograr sus objetivos militares.

Sin embargo, hay esperanza en el horizonte. Los legisladores y los defensores de las redes actúan para mejorar la ciberseguridad de las infraestructuras críticas, incluidos los dispositivos IoT y OT en los que confían. Los legisladores están acelerando el desarrollo de leyes y normativas para generar confianza pública en la seguridad cibernética de dispositivos e infraestructuras críticas.

Microsoft colabora con gobiernos de todo el mundo para aprovechar esta oportunidad de mejorar la ciberseguridad y estamos dispuestos a ampliar nuestra implicación. Sin embargo, nos preocupa que requisitos incoherentes, diseñados a medida o complejos puedan tener efectos no deseados, incluida la disminución de la seguridad en algunos casos al invertir recursos de seguridad escasos en el cumplimiento de múltiples certificaciones redundantes.

Desde el punto de vista de las operaciones de seguridad, los defensores de las redes deben adoptar varios enfoques para mejorar la posición de seguridad de IoT/OT de su organización. Un enfoque es implementar la supervisión continua de los dispositivos IoT y OT. Otro es el denominado «shift-left», es decir, exigir e implementar mejores prácticas de ciberseguridad para los propios dispositivos IoT y OT. Un tercer enfoque es implementar una solución de supervisión de seguridad que abarque redes de TI y OT. Este enfoque integral tiene el importante beneficio adicional de contribuir a los procesos organizativos críticos, como «descomponer los silos» entre OT y TI, lo que a su vez permite a la organización adoptar un enfoque de seguridad mejorado mientras satisface los objetivos del negocio.

Michal Braverman-Blumenstyk
Vicepresidente corporativo, director de tecnología, cloud y seguridad de IA

Actuación de los gobiernos para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Gobiernos de todo el mundo están desarrollando políticas para gestionar los riesgos críticos de ciberseguridad en las infraestructuras. Muchos también están promulgando políticas para mejorar la seguridad de los dispositivos IoT y OT. La creciente ola mundial de iniciativas políticas está creando una enorme oportunidad para mejorar la ciberseguridad, pero también plantea desafíos a las partes interesadas de todo el ecosistema.

Desarrollar una visión integral para gestionar el riesgo cibernético de las infraestructuras críticas es esencial, pero complejo, especialmente si tenemos en cuenta el grado de interconexión entre las tecnologías y los proveedores globales, el abanico de usos de la tecnología y los riesgos asociados, y la necesidad de invertir en estrategias tanto a corto como a largo plazo. Las políticas bien enfocadas que impulsan el aprendizaje iterativo y las mejoras, y respaldan la interoperabilidad global y sectorial, pueden ayudar a gestionar la complejidad y permitir una transformación digital más centrada en la seguridad. Sin embargo, un enfoque fragmentado de la legislación podría dar lugar a requisitos normativos solapados e incoherentes. Esto podría afectar a los recursos y, en última instancia, socavar los objetivos de seguridad. Por ejemplo, las organizaciones podrían desviar recursos de la innovación y la seguridad a ejercicios de cumplimiento formalistas.

Microsoft pretende asociarse con gobiernos de todo el mundo en la búsqueda de políticas de ciberseguridad eficaces para las infraestructuras críticas, con el fin de conocer mejor los desafíos y oportunidades y de respaldar las iniciativas para mejorar la postura de riesgo colectivo.

Desarrollos de políticas para la gestión de riesgos de ciberseguridad de infraestructuras críticas

Durante el último año, varias jurisdicciones, incluidas las de Australia, Chile, la Unión Europea (UE), Japón, Singapur, el Reino Unido (UK) y los Estados Unidos, han desarrollado, actualizado o implementado requisitos de ciberseguridad multisectoriales o específicos del sector.[1] Muchos de estos gobiernos, y otros como India[2] y Suiza[3], ya han publicado o están desarrollando requisitos de divulgación de incidentes de ciberseguridad para infraestructuras críticas y proveedores de servicios esenciales.[4]

Durante el último año se produjeron algunos desarrollos políticos notables en Australia, la UE, Indonesia y los Estados Unidos. Australia promulgó dos leyes para ayudar a gestionar los riesgos de ciberseguridad en infraestructuras críticas multisectoriales. Las leyes, entre otras cosas, designan nuevos sectores de infraestructuras críticas, requieren el desarrollo de planes de gestión de riesgos, exigen informes de incidentes de ciberseguridad y permiten al gobierno intervenir si determina que un operador de una infraestructura crítica no está dispuesto o no puede responder adecuadamente a un incidente.

La UE ha trabajado para actualizar su directiva NIS de 2016, que proporciona un marco para que los estados miembro de la UE regulen los servicios y productos tecnológicos que se consideren críticos para su economía y el funcionamiento de la sociedad. El NIS 2 propuesto incluye revisiones que crearán una nueva categoría de infraestructura digital crítica, aumentarán los requisitos para la divulgación de ciberataques e impondrán requisitos adicionales de gestión de riesgos de ciberseguridad. La UE también desarrolló una propuesta de actualización de su Ley de Resiliencia Operativa Digital (DORA, por sus siglas en inglés), que impone nuevos requisitos para las tecnologías de comunicación de la información utilizadas en el sector de los servicios financieros.

En mayo, Indonesia emitió un reglamento presidencial sobre la protección de infraestructura de información esencial («IIV», por sus siglas en inglés), que entrará en vigor en mayo de 2024 y abarcará sectores como la energía, el transporte, las finanzas y la salud, entre otros. El objetivo de Indonesia con el reglamento es proteger la continuidad de la implementación de IIV, prevenir los ciberataques y aumentar el grado de preparación para la gestión de incidentes cibernéticos. Los proveedores de IIV serán responsables de llevar a cabo una protección segura y fiable, de implementar una gestión eficaz de los riesgos cibernéticos y de informar de los resultados de los riesgos cibernéticos a los organismos gubernamentales pertinentes. El reglamento incluye el requisito de informar de los ciberataques en un plazo de 24 horas.

Actuación de los gobiernos para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Continuación

El Congreso de EE. UU. aprobó una ley que autoriza a la Agencia de Ciberseguridad e Infraestructura de Seguridad (CISA) a publicar normativas para exigir la divulgación de ciberataques de operadores de infraestructuras críticas, y la Administración de Seguridad del Transporte (TSA) de Estados Unidos publicó nuevos requisitos de ciberseguridad específicos del sector del transporte. En 2021, TSA publicó dos directivas de seguridad para los operadores de líquidos peligros y gaseoductos de gas natural en respuesta al ataque de ransomware al Oleoducto Colonial:

- La primera directiva exige a los operadores que designen un coordinador de ciberseguridad, informen de los ciberataques en un plazo de 12 horas y realicen una evaluación de vulnerabilidades de sus sistemas.
- La segunda directiva, que TSA revisó en 2022, les exige implementar medidas de mitigación específicas para proteger de los ataques de ransomware y otras amenazas conocidas a los sistemas de TI y OT, desarrollar e implementar un plan de contingencias y respuestas de ciberseguridad en un plazo de 30 días y someterse a una revisión anual del diseño de la arquitectura de ciberseguridad.

Basándose en sus reglamentos para los oleoductos, TSA publicó dos directivas de seguridad adicionales más adelante en 2021 que promulgan requisitos de ciberseguridad para el transporte ferroviario de mercancías, el transporte ferroviario de pasajeros o los sistemas de transporte ferroviario. Las directivas exigen que los operadores implicados designen a un coordinador de ciberseguridad, informen de los incidentes de ciberseguridad en el plazo de 24 horas, desarrollen e implementen un plan de respuesta a incidentes de ciberseguridad y realicen una evaluación de vulnerabilidades de ciberseguridad. TSA anunció simultáneamente que actualizaba también sus programas de seguridad para la aviación para exigir a los operadores de aeropuertos y aerolíneas que implementaran las dos primeras disposiciones: designar a un coordinador e informar de los incidentes en el plazo de 24 horas.

Desarrollo de políticas de seguridad de dispositivos IoT y OT

En decenas de países, los gobiernos están desarrollando activamente requisitos para mejorar la ciberseguridad de los productos y servicios de tecnología de la información y la comunicación (TIC), incluidos los dispositivos de IoT y OT. En el contexto de los productos y servicios TIC, las mayores preocupaciones son la seguridad de la cadena de suministro de software y la seguridad del IoT.

- La Comisión Europea propuso la Ley de Resiliencia Cibernética, que establece requisitos de ciberseguridad para el software independiente y los dispositivos conectados y servicios auxiliares.[5] Las prácticas relevantes para los proveedores de software incluyen usar un ciclo de vida de desarrollo de software seguro[6] y proporcionar una lista de materiales de software.[7] Se aplicarán nuevos requisitos de seguridad a los dispositivos conectados y todos los fabricantes tendrán la tarea de gestionar procesos coordinados de divulgación de vulnerabilidades[8] para los productos publicados.

Los legisladores también han centrado su atención en la proliferación continua de dispositivos de IoT y dispositivos de OT conectados en red.

- En el Reino Unido, el proyecto de ley Lista de Seguridad de Productos e Infraestructura de Telecomunicaciones exigirá a los fabricantes de productos de consumo conectables, como los televisores inteligentes, que dejen de usar contraseñas predeterminadas, que son un objetivo fácil para los ciberdelincuentes, establezcan una política de divulgación de vulnerabilidades (como un medio de recibir avisos de fallos de seguridad) y proporcionen transparencia sobre la cantidad mínima de tiempo durante la que proporcionarán actualizaciones de seguridad.[9]
- En la UE, se están implantando nuevas normas o requisitos de seguridad a través de varios instrumentos legislativos, incluido un acto delegado a la Directiva de Equipos de Radio que se aplica a los dispositivos inalámbricos y que pretende mejorar la resiliencia de la red, proteger la privacidad de los consumidores y reducir el riesgo de fraude monetario.[10] Además, podría ser necesario utilizar un plan de certificación en el cloud,[11] actualmente en desarrollo, como resultado de la Ley de Ciberseguridad de la UE de 2019[12].

La necesidad de coherencia

En muchos casos, las actividades analizadas abarcan regiones, sectores, tecnologías y áreas de gestión de riesgos operativos, lo que da lugar a posibles solapamientos o incoherencias en el alcance y los requisitos, y añade complejidad para las organizaciones que desean usar directrices o demostrar el cumplimiento. Sin una definición universalmente aceptada de IoT, la delimitación del alcance resulta especialmente difícil para las regulaciones de dispositivos IoT y OT. Los ejemplos anteriores se aplican potencialmente a «productos conectados y servicios auxiliares», «productos de consumo conectables» y «dispositivos inalámbricos». Al mismo tiempo, muchos gobiernos pretenden implantar regímenes de evaluación más robustos para saber si las organizaciones y los productos cumplen los requisitos actuales, emergentes y en evolución. La complejidad aumentará cuando estas tendencias converjan. Resulta alentador que las preguntas planteadas durante la consulta sobre el Ley de Resiliencia Cibernética de la UE indagaran en cómo la nueva normativa podría interferir potencialmente en la normativa de ciberseguridad existente, lo que indica la intención de evitar requisitos de ciberseguridad contradictorios.

Los enfoques iterativos basados en el riesgo y orientados a los resultados o los procesos (en lugar de ser específicos de la implementación) podrían fomentar una mejor ciberseguridad y una mejora continua. Del mismo modo, dirigir el punto de atención a la interoperabilidad de sectores, regiones y áreas políticas podría mejorar sistemáticamente la ciberseguridad en las cadenas de suministro globales interconectadas.

Actuación de los gobiernos para mejorar la seguridad y la resiliencia de las infraestructuras críticas

Continuación

Se están desarrollando políticas de ciberseguridad de infraestructuras críticas cada vez más complejas en distintas regiones, sectores y áreas temáticas. Esta actividad ofrece grandes oportunidades y entraña desafíos importantes. La forma de proceder de los gobiernos será crucial para el futuro de la transformación digital y la seguridad en todo el ecosistema.

Acelerar las inversiones de todo el ecosistema en seguridad de la cadena de suministro de software y arquitectura de Confianza cero

El decreto presidencial de EE. UU. 14028 sobre la mejora de la ciberseguridad ha sido un catalizador para acelerar las iniciativas continuas de Microsoft de invertir en la seguridad de nuestra propia cadena de suministro en todo el ecosistema y para permitir a nuestros clientes cumplir los objetivos de Confianza cero.

Hace mucho tiempo que creemos que para mejorar la cadena de suministro de software es necesario compartir las lecciones aprendidas y las prácticas recomendadas, empezando por el lanzamiento público del Ciclo de Vida de Desarrollo de Seguridad de Microsoft hace unos 15 años.

Además, nos hemos asociado estrechamente con el Centro Nacional de Excelencia de Ciberseguridad para demostrar enfoques de arquitectura de Confianza cero aplicada a la tecnología on-premises y en el cloud, y establecer nuevas funcionalidades de productos, incluida la capacidad de aplicar la autenticación resiliente al phishing para entornos híbridos y multicloud.

Actualmente, queremos ir más allá de los requisitos del decreto presidencial, y demostrar el cumplimiento con los requisitos de seguridad de la cadena de suministro de software y proporcionar información de la lista de materiales de software (SBOM) de dos maneras:

1. En primer lugar, vamos a compartir una versión de código abierto de nuestra herramienta SBOM, que hemos creado para que se integre fácilmente con las canalizaciones CI/CD que admiten compilaciones en plataformas Windows, Linux, Mac, iOS y Android.[13]
2. En segundo lugar, vamos a contribuir al desarrollo de estándares del sector para la integridad, transparencia y confianza de la cadena de suministro (SCITT). Esto permitirá el intercambio automatizado de información de la cadena de suministro verificable, incluidos artefactos que demuestren el cumplimiento de requisitos como los resultantes de las directrices de la cadena de suministro de software del decreto presidencial.

Conocimientos prácticos

1. Las instituciones multilaterales deben replantarse cómo hacer frente al desafío apremiante de los ciberataques a los estados nación.
2. Desarrolla políticas de ciberseguridad coherentes e interoperables en distintas regiones, sectores y ámbitos.

Enlaces a información adicional (pueden estar en inglés)

- Inversiones continuas en seguridad de la cadena de suministro en apoyo del decreto presidencial ciberseguridad | Microsoft Tech Community
- El gobierno de EE. UU. adopta la estrategia y los requisitos de la arquitectura de Confianza cero | Blog de seguridad de Microsoft
- Decreto presidencial sobre ciberseguridad | Microsoft Federal
- Integridad, transparencia y confianza de la cadena de suministro | github.com
- Implementación de una arquitectura de Confianza cero | NCCoE (nist.gov)

IoT y OT expuestos: tendencias y ataques

El mundo digital, cada vez más conectado, significa que los dispositivos se están conectando rápidamente a Internet, comunicándose con sistemas más grandes, recopilando datos y creando visibilidad en espacios anteriormente opacos. Esto ofrece oportunidades a las organizaciones y a los actores de amenazas por igual, ya que el negocio de la ciberdelincuencia se está convirtiendo tanto en un sector multimillonario como en un riesgo.

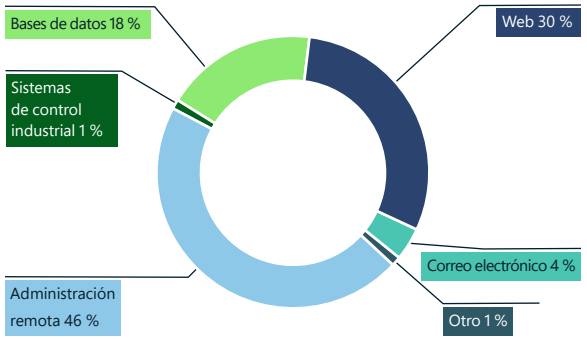
Los dispositivos del IoT, que incluyen todo tipo de dispositivos, desde impresoras hasta cámaras web, dispositivos de control de la temperatura y controles de acceso a los edificios, plantean riesgos de seguridad únicos para las personas, las organizaciones y las redes. Aunque son fundamentales para las operaciones de muchas organizaciones, pueden convertirse rápidamente en un riesgo de responsabilidad y seguridad. La rápida adopción de soluciones de IoT en casi todos los sectores ha aumentado el número de vectores de ataque y el riesgo de exposición de las organizaciones.

El malware como servicio se ha trasladado a operaciones a gran escala contra infraestructuras y servicios públicos (incluidos hospitales, petróleo y gas, redes eléctricas, servicios de transporte y otras infraestructuras críticas), así como redes corporativas. Los actores de amenazas requieren grandes esfuerzos de investigación para descubrir y explotar la configuración de entornos operativos y dispositivos del IoT y OT integrados.

Los dispositivos del IoT plantean riesgos de seguridad únicos como puntos de entrada y pivote en la red. Millones de dispositivos del IoT no tienen parches o están expuestos.

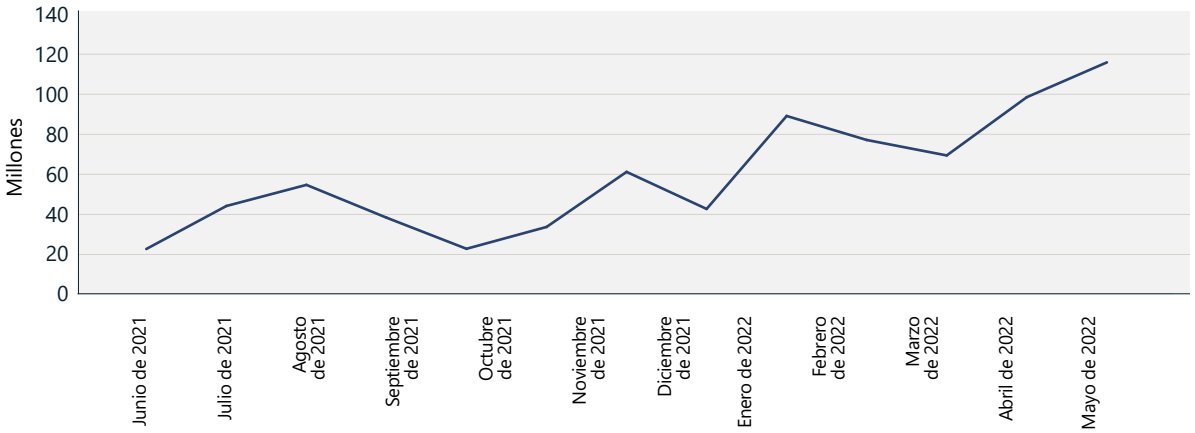
Los dispositivos expuestos se pueden detectar a través de herramientas de búsqueda en Internet identificando los servicios que escuchan en puertos de red abiertos. Estos puertos se utilizan habitualmente para la administración remota de dispositivos. Si no está protegido correctamente, un dispositivo del IoT expuesto se puede utilizar como punto de pivote en otra capa de la red empresarial, ya que los usuarios no autorizados pueden acceder a los puertos de forma remota. Hemos observado cómo distintos actores de amenazas intentan aprovechar las vulnerabilidades de los dispositivos expuestos a Internet, desde cámaras hasta enrutadores o termostatos. Sin embargo, a pesar del riesgo, millones de dispositivos permanecen sin parches o siguen expuestos.

Resumen de tipos de ataques a IoT/OT



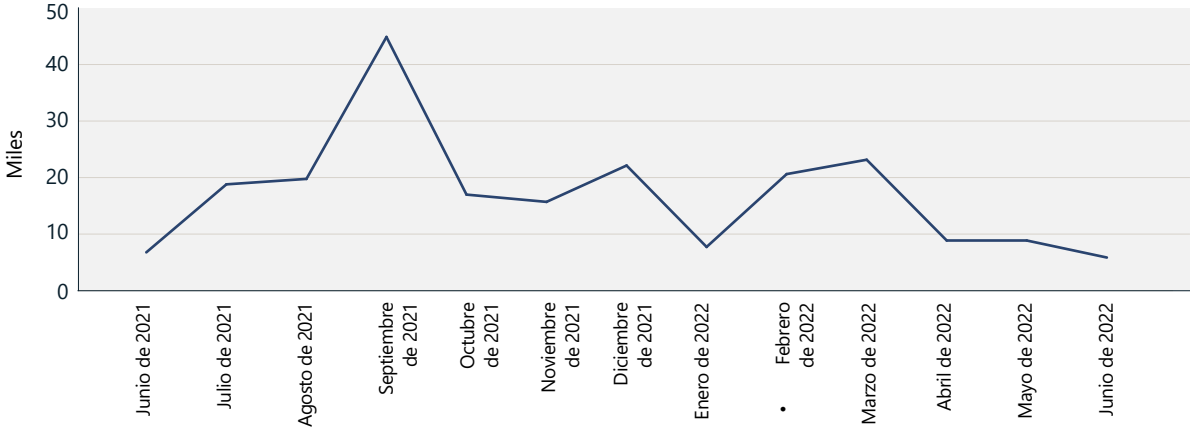
Tipos de ataques observados a través de la red de sensores del MSTIC. Los más prevalentes fueron los ataques contra dispositivos de administración remota, los ataques a través de Internet y los ataques a bases de datos (de fuerza bruta o exploits).

Ataques contra dispositivos de administración remota



Aumento de los ataques a los puertos de administración remota a lo largo del tiempo, de acuerdo con la red de sensores del MSTIC.

Ataques web contra IoT y OT



Volumen de ataques web a lo largo del tiempo, de acuerdo con la red de sensores del MSTIC. Conforme vaya disminuyendo el número de dispositivos conectados directamente a la Web, posiblemente los atacantes estén menos dispuestos a investigarlos.

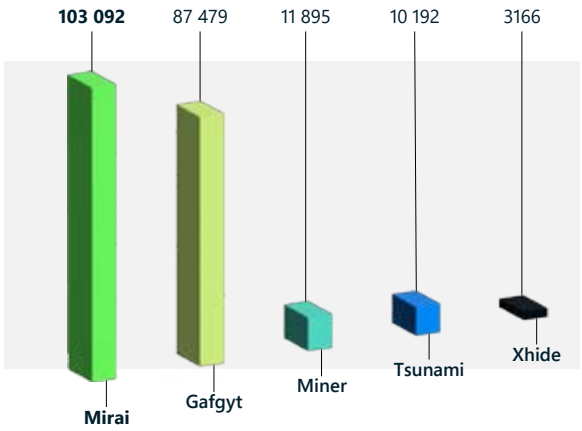
IoT y OT expuestos: tendencias y ataques

Continuación

Utilidad renovada del malware

Los grupos de ciberdelincuentes evolucionan al mismo ritmo que su implementación del malware y la elección de objetivos. El año pasado, observamos que los ataques contra protocolos comunes del IoT, como Telnet, se redujeron considerablemente, en algunos casos hasta en un 60 por ciento. Al mismo tiempo, los grupos de ciberdelincuentes y los agentes de los estados nación están dando un nuevo uso a las botnets. La persistencia del malware, como Mirai, pone de relieve la modularidad de estos ataques y la capacidad de adaptación de las amenazas existentes.

Principal malware del IoT detectado en el mundo real



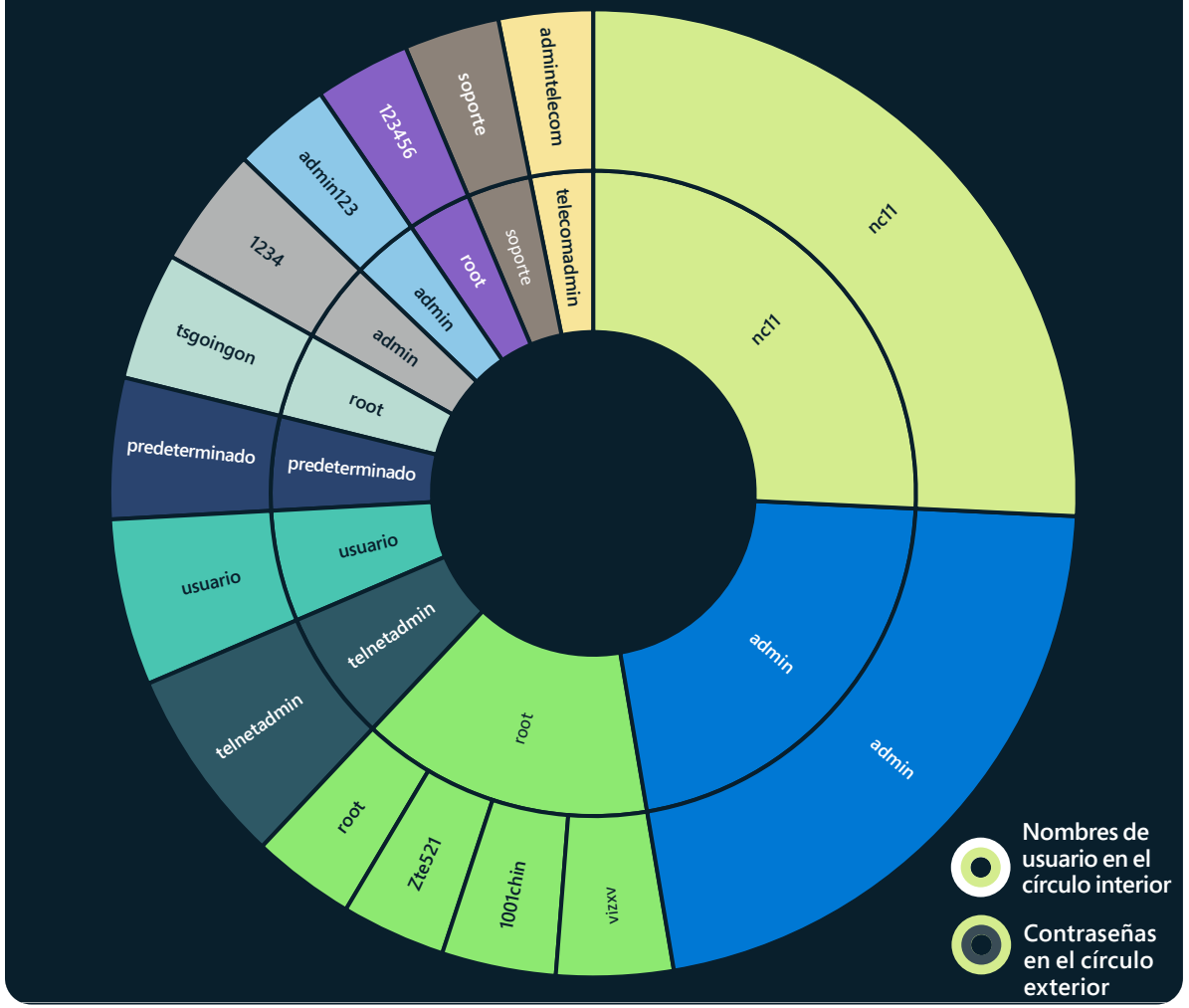
Mirai evolucionó para infectar a un amplio conjunto de dispositivos del IoT, incluidas cámaras de Protocolo de Internet, grabadoras de vídeo digitales de cámaras de seguridad y routers. El vector de ataque elude los controles de seguridad heredados y plantea un riesgo para los puntos de conexión dentro de la red al aprovechar vulnerabilidades adicionales y moverse lateralmente. Mirai se ha rediseñado varias veces, con variantes que se adaptan a diferentes arquitecturas y aprovechan las vulnerabilidades conocidas y de día cero para explotar nuevos vectores de ataque.

El uso de Mirai aumentó en las arquitecturas de CPU x86 de 32 y 64 bits en el último año, y al malware se le dieron nuevas capacidades que fueron rápidamente adoptadas por los grupos delictivos y de estados nación. Los ataques de los estados nación aprovechan ahora nuevas variantes de botnets existentes en ataques distribuidos de denegación de servicio (DDoS) contra adversarios extranjeros.

A medida que los ingresos de los ataques contra dispositivos del IoT disminuyeron en 2022, observamos cómo varios grupos de actores de amenazas utilizaban vulnerabilidades, como Log4j y Spring4Shell, para distribuir una carga malintencionada a dispositivos como servidores, infectándolos e incorporándolos en grandes botnets que perpetran ataques DDoS. La nueva utilidad de malware diseñada para atacar dispositivos del IoT vulnerables tiene graves implicaciones tanto para las organizaciones como para las naciones, ya que el movimiento lateral puede exponer puertas traseras a cargas útiles adicionales y otros dispositivos en las redes.

Muchos protocolos de sistemas de control industrial no están monitorizados y, por lo tanto, son vulnerables a ataques específicos de OT. Esto puede implicar un mayor riesgo para las infraestructuras críticas.

Prevalencia relativa de parejas de nombres de usuario y contraseñas observada en los dispositivos del IoT/OT en 45 días de señales de los sensores



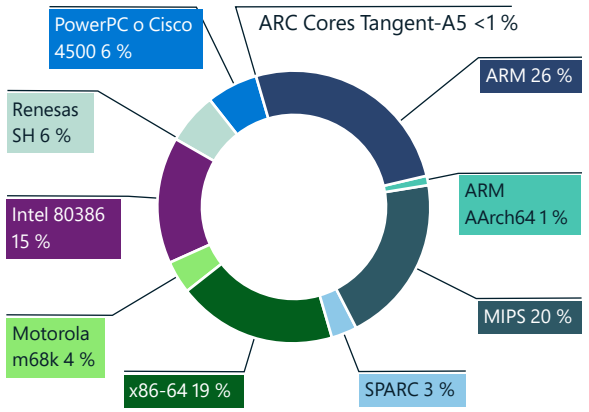
El uso de parejas comunes de nombre de usuario y contraseña aumenta el riesgo de sufrir un ataque. De acuerdo con un tamaño de muestra de más de 39 millones de dispositivos del IoT y OT, aquellos que utilizan nombres de usuario y contraseñas idénticos representan alrededor del 20 por ciento.

IoT y OT expuestos: tendencias y ataques

Continuación

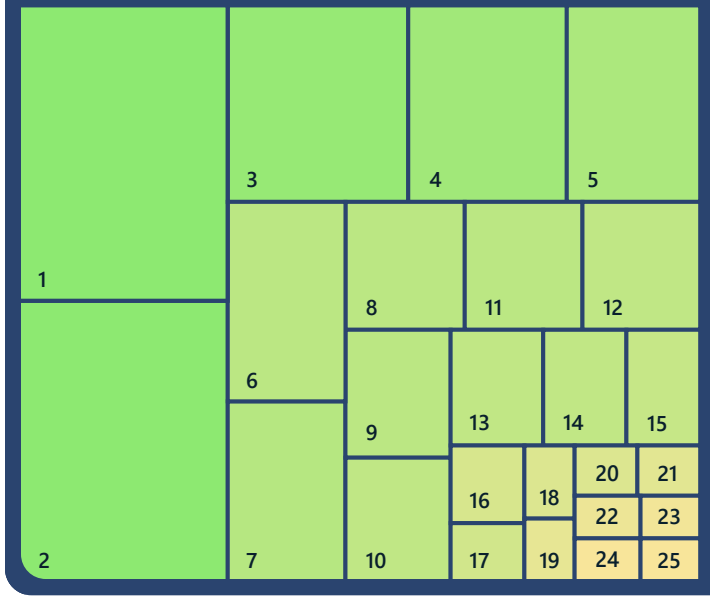
Aunque las configuraciones débiles y las credenciales predeterminadas siguen entrañando un riesgo para las redes, Microsoft observó que muchos ataques basados en web utilizaban HTTP. Hemos observado este aumento de los ataques a servicios basados en web mediante botnets heredadas. Mientras tanto, hubo una disminución en el número de puertos abiertos en Internet, un signo positivo para la seguridad de la red, ya que las botnets que presentaban un riesgo histórico para los dispositivos están perdiendo relevancia.
A pesar de esta disminución de puertos telnet abiertos seguimos observando botnets persistentes en las redes de sensores.

Distribución del malware de IoT por arquitectura de CPU



Microsoft observó que los dispositivos del IoT que se ejecutan en ARM son los que más ataques de malware sufren, seguidos de las CPU MIPS, X86-64 e Intel 80386.

Prevalencia del protocolo de sistemas de control industrial



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. Deltav
17. GSM
18. DNP3
19. AMS
20. SRTP
21. Twincat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

Vulnerabilidades del protocolo de sistemas de control industrial

Hemos analizado los datos de OT de nuestros sensores conectados al cloud y hemos revelado los protocolos más comunes de sistemas de control industrial (CIS). Estos protocolos proporcionan conocimientos sobre la naturaleza de estos dispositivos y su superficie de ataque. Esto es especialmente relevante para la seguridad de las infraestructuras críticas. Algunas conclusiones clave son:

1. La mayoría de los protocolos representados son propietarios, por lo que las herramientas de supervisión de TI estándar no tienen visibilidad suficiente de la seguridad de estos dispositivos y protocolos. Por consiguiente, las redes no están supervisadas y, por lo tanto, son más vulnerables a ataques específicos de OT.
2. Hay una gran variedad de protocolos específicos del proveedor. Esto significa que las soluciones de seguridad específicas del proveedor no son capaces de cubrir adecuadamente toda la red. Microsoft da prioridad a un enfoque independiente del proveedor para proporcionar cobertura de seguridad para la amplia variedad de dispositivos diferentes.
3. Las organizaciones deben asegurarse de que estos protocolos no se expongan directamente a Internet desde sus redes. Esta exposición podría suponer un riesgo de seguridad importante debido a las vulnerabilidades y a la naturaleza poco segura de estos protocolos.

El malware como Mirai persiste mediante el desarrollo de nuevas capacidades y está siendo adoptado por grupos de ciberdelincuentes y actores estado nación, aprovechando nuevas variantes de botnets existentes en ataques DDoS contra adversarios extranjeros.

Conocimientos prácticos

1. Asegúrate de que los dispositivos sean robustos aplicando parches y cambiando las contraseñas predeterminadas y los puertos SSH predeterminados.
2. Reduce la superficie de ataque eliminando las conexiones a Internet y los puertos abiertos innecesarios, restringiendo el acceso remoto mediante el bloqueo de puertos, la denegación del acceso remoto y el uso de servicios de VPN.
3. Utiliza una solución de detección y respuesta de redes compatible con IoT/OT y una solución de administración de eventos e información de seguridad (SIEM)/orquestación y respuesta de seguridad (SOAR) para supervisar los dispositivos en busca de comportamientos anómalos o no autorizados, como la comunicación con hosts desconocidos.
4. Segmenta las redes para limitar la capacidad de un atacante de moverse lateralmente y atacar los activos después de la intrusión inicial. Los dispositivos del IoT y las redes de TO deben aislarse de las redes corporativas de TI mediante firewalls.
5. Asegúrate de que los protocolos ICS no se expongan directamente a Internet.

La cadena de suministro y hacking de firmware

Casi todos los dispositivos conectados a Internet tienen firmware, que es software integrado en el hardware o la placa de circuito del dispositivo. En los últimos años, hemos visto cómo el firmware se convertía cada vez más en un objetivo para perpetrar ataques devastadores. Como es probable que el firmware siga siendo un objetivo valioso para los actores de amenazas, las organizaciones deben protegerse contra el hacking del firmware.

El firmware es responsable de las funciones principales de un dispositivo, como conectarse a una red o almacenar datos. El firmware se encuentra en routers, cámaras, televisores y otros dispositivos utilizados en las empresas (IoT), junto con los equipos de control industrial (OT) utilizados en infraestructuras críticas. Tradicionalmente, el firmware se ha escrito con código no seguro, lo que crea vulnerabilidades importantes que se pueden aprovechar para tomar el control del dispositivo o inyectar código malintencionado en el firmware.

Este riesgo se agrava cuando hablamos de la cadena de suministro. La mayoría de los dispositivos se construyen utilizando componentes de software y hardware de numerosos fabricantes, así como bibliotecas de código abierto. En muchos casos, los operadores de dispositivos no tienen visibilidad de la lista de materiales de hardware y software (H/SBOM) para evaluar el riesgo de la cadena de suministro de los dispositivos de su red. En junio de 2020, se revelaron vulnerabilidades en una pila de red utilizada por muchos fabricantes diferentes que afectó a cientos de millones de dispositivos del IoT en el ámbito de equipos industriales y de consumo.[14] En algunos casos, otros proveedores cambiaron la marca de la pila de red y no había ninguna indicación de que un dispositivo fuera vulnerable. Vemos una amenaza cada vez mayor de agentes malintencionados que atacan esta cadena de suministro de software y hardware de dispositivos del IoT/OT para poner en peligro a las organizaciones.

El proceso de actualización del firmware varía considerablemente en función del dispositivo, y la complejidad y el desafío logístico de aplicarlo afectan a la frecuencia de actualización. No siempre es posible determinar si un dispositivo está ejecutando el firmware más reciente, por lo que a los profesionales de seguridad les resulta difícil supervisar y garantizar la posición de seguridad de sus dispositivos del IoT y OT. Además, algunos dispositivos tienen firmware que no está firmado criptográficamente, lo que les permite actualizarse sin verificación del usuario. Estos puntos débiles exponen aún más los dispositivos a los ataques de la cadena de suministro en toda la cadena de producción y distribución.

Para hacer frente a estas amenazas, Microsoft ha realizado una importante inversión en garantizar la seguridad y la integridad del firmware a medida que se mueve por las distintas etapas de la cadena de suministro y en certificar en cualquier momento que no ha sido manipulado durante su incorporación o a lo largo del proceso. Esto nos permitirá validar la confianza entre cada segmento de la canalización y proporcionar una cadena de custodia de extremo a extremo certificada y demostrable para cada componente que enviamos a los clientes. Trabajamos con nuestros partners para llevar esta seguridad desde el chip hasta el cloud a todos los dispositivos de la red empresarial y de OT.

«Los proveedores de infraestructuras TIC son cada vez más objetivos de los ataques, ya que permiten la replicación generalizada de un solo ataque. Al mismo tiempo, la legislación y los reglamentos globales y la demanda de los clientes de seguridad y resiliencia de la cadena de suministro están aumentando y, a menudo, sus requisitos son diferentes.

La solución es la colaboración. Junto con proveedores y gobiernos de todo el mundo, Microsoft se compromete a abordar la seguridad en todo nuestro ecosistema de la cadena de suministro, satisfaciendo con creces las exigencias de los clientes y los reguladores. Para ello, estamos trabajando en un enfoque integral de seguridad y resiliencia operativa que se pueda implementar de manera flexible en toda la cadena de suministro.

Mejorar la integridad del firmware desde el diseño hasta el funcionamiento del dispositivo es clave para nuestro enfoque conjunto. Garantizar los procesos de SDL de los proveedores e implementar las innovaciones de raíz de confianza del hardware son ejemplos de cómo podemos mejorar la integridad de la cadena de suministro.

Nuestra comunidad está aprovechando la investigación y el desarrollo conjuntos que abarcan nuevas técnicas antimanipulación y mecanismos criptográficos, combinados con la supervisión continua y la detección de anomalías. Juntos, estamos progresando en reducir el atractivo de la cadena de suministro como superficie de ataque».

Edna Conway,
Vicepresidenta responsable de seguridad y riesgos, infraestructura en el cloud

Aspectos destacados de las vulnerabilidades del firmware

Los atacantes aprovechan cada vez más las vulnerabilidades del firmware de los dispositivos del IoT para infiltrarse en las redes corporativas. A diferencia de los puntos de conexión de TI tradicionales que utilizan agentes XDR para identificar puntos débiles, la identificación de vulnerabilidades dentro de los dispositivos del IoT/OT es mucho más difícil.

Una encuesta reciente realizada por Microsoft y Ponemon Institute pone de manifiesto la oportunidad y el desafío de seguridad de los dispositivos del IoT/OT en una empresa.[15] Mientras que el 68 por ciento de los encuestados cree que la adopción de IoT/OT es fundamental para su transformación digital estratégica, el 60 por ciento reconoce que la seguridad del IoT/OT es uno de los aspectos menos seguros de la infraestructura de TI y OT.

Un ejemplo de atacantes que utilizan vulnerabilidades en el firmware de un dispositivo del IoT para infiltrarse en una red es el troyano Trickbot, que aprovechó las contraseñas predeterminadas y las vulnerabilidades de los enrutadores Mikrotik[16] para eludir los sistemas de defensa corporativos. El problema fundamental del firmware de los dispositivos del IoT es la falta de visibilidad de la posición de seguridad y las vulnerabilidades de los dispositivos.

Aunque hay soluciones disponibles para crear dispositivos seguros, hay miles de millones de dispositivos que ya están en el mercado e implementados en las empresas. Estos dispositivos reciben el nombre de dispositivos «brownfield». En 2021, Microsoft adquirió ReFirm Labs para arrojar luz sobre la seguridad de los dispositivos «brownfield» y permitir a los desarrolladores de dispositivos mejorar la seguridad de sus productos. ReFirm Labs analiza la imagen binaria del firmware de un dispositivo y produce un informe detallado sobre posibles puntos débiles de seguridad.[17] Esta tecnología se va a incorporar a una futura versión de Microsoft Defender para IoT.

El año pasado, examinamos los resultados acumulados del firmware único analizado por nuestros clientes. Aunque no todos los puntos débiles descubiertos podrían ser aprovechables, estos resultados subrayan el desafío fundamental que supone la seguridad del firmware de los dispositivos.

Téngase en cuenta que los tipos de puntos débiles que existen en los dispositivos del IoT/OT nunca serían aceptables en puntos de conexión tradicionales de Windows o Linux.

- Contraseñas poco seguras: el 27 por ciento de las imágenes del firmware analizadas contiene cuentas con contraseñas codificadas mediante algoritmos poco seguros (MD5/DES), que los atacantes pueden descifrar fácilmente.

Puntos débiles de seguridad en las imágenes de firmware analizadas

- Vulnerabilidades conocidas: al igual que otros sistemas, el firmware de los dispositivos del IoT/OT aprovechó ampliamente las bibliotecas de código abierto. Sin embargo, los dispositivos se distribuyen sin versiones actualizadas de estos componentes. En nuestro análisis, el 32 % de las imágenes contenía al menos 10 vulnerabilidades conocidas (CVE) valoradas como críticas (9,0 o superior). El 4 por ciento contenía al menos 10 vulnerabilidades críticas con más de seis años de antigüedad.
- Certificados caducados: los certificados se utilizan para autenticar conexiones e identidades, así como para proteger los datos confidenciales, pero el 13 % de las imágenes analizadas contenía al menos 10 certificados que caducaron hace más de tres años.
- Componentes de software: el 36 por ciento de las imágenes contiene componentes de software que Microsoft recomienda excluir en dispositivos del IoT, como las herramientas de captura de paquetes (tcpdump, libpcap), que se pueden utilizar para el reconocimiento de la red como parte de una cadena de ataque.

Ataques de firmware en el mundo real

Viasat: uso de una vulnerabilidad del firmware para atacar las comunicaciones por satélite

En febrero de 2022, un incidente de una red por satélite desconectó una red de comunicación estratégica cuyo impacto se sintió en toda Europa. El sistema KA-SAT de Viasat recibió una gran cantidad de tráfico que desconectó muchos módems y se inició un ataque de denegación de servicio contra la red. Cuando se interrumpió la banda ancha fija, miles de aerogeneradores quedaron inaccesibles de forma remota para los operadores y se implementó malware «wiper» malintencionado para los dispositivos móviles afectados. La interrupción afectó a más de 30 000 terminales de satélite utilizados por empresas y organizaciones para la comunicación.

Cyclops Blink: uso de un ataque a la cadena de suministro del firmware dirigido a puertas de enlace de firewall

Para los atacantes, el desarrollo y la expansión de la infraestructura de mando y control (C2) y de ataques es un componente crucial del éxito. Conforme ha aumentado la necesidad de una infraestructura C2 estable, los routers se han convertido en un vector de ataque deseable debido a que no se les aplican parches frecuentemente y a la falta de soluciones de seguridad integrales.

Microsoft se ha asociado con organizaciones gubernamentales y con el sector de la tecnología de análisis de firmware para obtener mayor visibilidad de la seguridad de los dispositivos y proporcionar seguridad del ciclo de vida completo para los desarrolladores y operadores de dispositivos.

Desde junio de 2019, un grupo de amenazas avanzadas persistentes (APT) afiliado a un estado nación utilizó el malware modular Cyclops Blink para atacar dispositivos de firewall vulnerables WatchGuard y routers ASUS mediante la ejecución de actualizaciones de firmware malintencionadas y su reclutamiento en una gran botnet. El malware infecta con éxito los dispositivos aprovechando una vulnerabilidad conocida que permite el escalado de privilegios, con lo que los actores de amenazas pueden administrar el dispositivo. Una vez infectado, el malware permite instalar más módulos y elude las actualizaciones del firmware. Se ha observado que los dispositivos atacados se conectan a servidores C2 alojados en otros dispositivos WatchGuard. Emitiendo muchos certificados SSL para su C2 en varios puertos TCP, los operadores de Cyclops Blink con privilegios obtuvieron acceso remoto a las redes mediante la ejecución de actualizaciones de firmware malintencionadas y eludiendo los métodos de seguridad tradicionales como el escaneado.

Cómo Microsoft está mejorando la seguridad de la cadena de suministro

Microsoft se ha asociado con las organizaciones gubernamentales y con el sector para abordar estos desafíos de seguridad de dispositivos del IoT y OT (véase la explicación de la página 66). Nuestra contribución incluirá el uso de tecnología de análisis del firmware para proporcionar a los operadores de dispositivos visibilidad de la posición de seguridad de los dispositivos de su red. Esto permitirá a los clientes identificar y priorizar los dispositivos que necesiten protecciones adicionales y actualizaciones o deban ser sustituidos e impulsará la exigencia de que los desarrolladores de dispositivos inviertan en seguridad de los dispositivos. Al mismo tiempo, respaldamos a los fabricantes con soluciones completas para diseñar dispositivos seguros y adoptar ciclos de vida de desarrollo seguros.

Otro componente clave es proporcionar a los fabricantes y operadores una infraestructura robusta que permita que el firmware del dispositivo se actualice a medida que se detectan y resuelven los problemas de seguridad. Microsoft está reuniendo el análisis del firmware y Defender para IoT con Device Update para IoT Hub para proporcionar una solución que aborde el ciclo de vida completo de la seguridad de los dispositivos del IoT y OT. Estos son pasos importantes para materializar nuestra visión de que los clientes protejan la infraestructura mediante la adopción de dispositivos que admitan un enfoque de Confianza cero para sus soluciones del IoT y OT.[18]

Los atacantes aprovechan cada vez más las vulnerabilidades del firmware de los dispositivos de IoT para infiltrarse en las redes corporativas.

Conocimientos prácticos

1. Obtén visibilidad más detallada de los dispositivos del IoT/OT de tu red y clasifícalos según el riesgo que entrañan para la empresa si sufrieran un ataque.
2. Utiliza herramientas de análisis del firmware para conocer los posibles puntos débiles de seguridad y trabaja con proveedores para identificar cómo mitigar los riesgos de los dispositivos de alto riesgo.
3. Influye positivamente en la seguridad de los dispositivos del IoT/OT exigiendo a tus proveedores la adopción de prácticas recomendadas seguras para el ciclo de vida de desarrollo.

Enlaces a información adicional (pueden estar en inglés)

- Evaluación de las cadenas de suministro críticas para el sector de tecnologías de la información y comunicaciones en EE. UU.

Ataques OT basados en reconocimiento

Las cadenas de suministro complejas utilizan información de diseño específica para planificar el sistema real. De la multitud de activos que componen esta información de diseño, el más sensible es el archivo del proyecto, que define el entorno y sus activos. Este archivo es un objetivo estratégico crucial para los atacantes que buscan obtener acceso y perpetrar un ataque totalmente adaptado al entorno.

El ataque a sistemas industriales para interrumpir los procesos operativos consta de dos pasos.

1. En primer lugar, el atacante debe acceder a la red de OT. Para ello, puede entrar a través de dispositivos del IoT en el lado empresarial de la red (nivel 4 del modelo Purdue) y cruzar el límite de TI-OT, tradicionalmente separados por firewalls y equipos de red, en los niveles de operación y control.
2. En segundo lugar, se deben identificar los dispositivos de red. Los sistemas industriales utilizan dispositivos y componentes estándar en arquitecturas personalizadas diseñadas específicamente para sus entornos. Uno de estos dispositivos estándar es el controlador lógico programable (PLC). Cada fabricante desarrolla interfaces y funciones únicas para sus PLC, que son un componente crucial de los sistemas industriales, y estos dispositivos se configuran después con esquemas personalizados diseñados específicamente para los entornos del cliente.

La configuración única de cada PLC se describe en el archivo del proyecto, que contiene la definición del entorno y sus activos, el lenguaje «ladder» y otro contenido.

En la mayoría de los entornos que muestran pruebas de un ataque, el análisis constata que la línea cronológica anterior al ataque supera con creces la duración del propio ataque. Los atacantes suelen dedicar meses a simular el entorno y sus activos de forma remota, realizando muchos intentos de construir un modelo y preparar su ataque dirigido. Conforme los entornos cambian y van integrando nuevos dispositivos, se crean vulnerabilidades específicamente en torno a los datos de los archivos del proyecto y de configuración. El robo de un archivo del proyecto puede hacer avanzar un ataque en semanas o meses y permitir a los atacantes modelar el entorno de destino de forma rápida y precisa, lo que aumenta la dificultad para detectar la actividad malintencionada.

Industroyer e Incontroller

Hemos observado un aumento de los ataques contra organizaciones, infraestructuras críticas y objetivos gubernamentales por parte de agentes de los estados nación que utilizan marcos modulares de malware y ataque. Los nuevos intentos de interferir en operaciones críticas de Ucrania subrayan la creciente amenaza de ataques de OT basados en reconocimiento que están sumamente adaptados a sus entornos objetivo. Las extensas fases de reconocimiento e investigación llevadas a cabo por los actores de amenazas de los estados nación apuntan a una estrategia de uso de la guerra cibernética para paralizar la infraestructura de forma remota con objeto de cumplir objetivos estratégicos u operativos específicos en operaciones cibercinéticas y estrategia política combinadas.

Hemos observado una creciente amenaza de ataques OT basados en reconocimiento que están sumamente adaptados a sus entornos objetivo.

Ataques OT basados en reconocimiento

Continuación

A principios de 2022, se identificaron dos ataques de OT críticos adaptables. Un ataque ciberfísico contra subestaciones eléctricas y relés de protección en Ucrania se llevó a cabo con malware personalizado, incluida una variante de Industroyer, un malware que se sabe que ha causado apagones en Ucrania después de su implementación en 2016.

Industroyer2 es la primera reimplementación conocida del malware de ataque de OT malintencionado en un nuevo objetivo. Utilizó el plugin de protocolo IEC104 (protocolo estándar para la supervisión y el control de sistemas de alimentación) desarrollado para Industroyer y atacó sobre todo unidades de terminal remotas tipo PLC con el número de modelo ABB RTU540/560. El autor de este malware utilizó el conocimiento del entorno de la víctima para enviar comandos repetidamente a los resultados predeterminados, de forma que no se pudiera desactivar manualmente. Esto garantizaba interrupciones del suministro eléctrico más prolongadas y un impacto más dañino.

Incontroller, un marco de ataque modular identificado durante el mismo período, es un kit de herramientas modular que reduce considerablemente el tiempo de penetración y ataque de dispositivos de OT, eludiendo las soluciones de seguridad antiguas. El kit de herramientas de uso general tiene capacidades de recopilación de datos, reconocimiento y ataque que son sumamente personalizables para diferentes entornos y que pueden afectar considerablemente a la fase de investigación de un ataque de OT, al reducir el tiempo necesario para realizar el reconocimiento y permitir la simulación de entornos mediante la extracción de información sobre dispositivos y sus configuraciones.

El marco Incontroller admite protocolos para los PLC de Schneider Electric y Omron, y recopila información, como la versión del firmware, el tipo de modelo y los dispositivos conectados. El kit de herramientas puede emitir comandos para cambiar las configuraciones y activar y desactivar los resultados. Una vez que se accede a un entorno, la plataforma permite implantar puertas traseras en dispositivos para la distribución de más cargas útiles, exponer vulnerabilidades para aumentar los puntos de acceso, cargar lenguaje «ladder» y la capacidad de iniciar ataques DoS. La naturaleza genérica del kit de herramientas permite a un actor de amenazas atacar un entorno rápidamente sin necesidad de crear nuevos ataques para cada PLC o ubicación. Esto permite al atacante interactuar fácilmente con diferentes tipos de máquinas, potencialmente en muchos sectores de la industria.

Conocimientos prácticos

1. Evita transferir archivos que contengan definiciones del sistema a través de canales poco seguros o a personal no esencial.
2. Cuando la transferencia de dichos archivos sea inevitable, asegúrate de supervisar la actividad en la red y de garantizar que los activos sean seguros.
3. Protege las estaciones de ingeniería mediante la supervisión con soluciones de EDR.
4. Aplica de forma proactiva la respuesta a incidentes para las redes de OT.
5. Implementa la supervisión continua, como Defender para IoT.

Notas al pie

1. Véase, por ejemplo, Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe's digital future (europa.eu); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1; Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au); Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance; Japan passes economic security bill to guard sensitive technology | The Japan Times; Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg); Proposal for legislation to improve the UK's cyber resilience—GOV.UK (www.gov.uk); Telecommunications (Security) Act 2021 (legislation.gov.uk); Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In: página de inicio
3. Inicio de la consulta sobre la introducción de la obligación de divulgar los ciberataques (admin.ch)
4. Véase, por ejemplo, sin título (house.gov)
5. Ley de Resiliencia Cibernética | Dando forma al futuro digital de Europa (europa.eu)
6. Véase, por ejemplo, Ciclo de vida de desarrollo de seguridad de Microsoft
7. Véase, por ejemplo, Generación de listas de materiales de software (SBOM) con SPDX en Microsoft: Engineering@Microsoft; véase también, por ejemplo, Los elementos mínimos de una lista de materiales de softwares (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. Véase, por ejemplo, https://www.microsoft.com/en-us/msrc/cvd
9. Lista de infraestructura de telecomunicaciones y seguridad de los productos (PSTI) (ficha técnica de seguridad de los productos): GOV.UK (www.gov.uk)
10. La Comisión refuerza la ciberseguridad de los dispositivos y productos inalámbricos (europa.eu)
11. Plan de certificación en el cloud: creación de servicios en el cloud de confianza en toda Europa: ENISA (europa.eu)
12. Certificación: ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool« GitHub - microsoft/sbom-tool: la herramienta SBOM es una herramienta altamente escalable y preparada para la empresa para crear SBOM compatibles con SPDX 2.2 para cualquier tipo de artefactos.
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. La innovación en IoT/OT es crítica, pero entraña riesgos importantes (diciembre de 2021): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. Uso de dispositivos del IoT por parte de Trickbot en infraestructura C2 (marzo de 2022): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. Episodio de IoT Show en Channel 9 sobre análisis del firmware del IoT (mayo de 2022): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. Cómo aplicar un enfoque de Confianza cero a tus soluciones del IoT (mayo de 2021): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

Operaciones de ciberinfluencia

Las operaciones actuales de influencia extranjera utilizan nuevos métodos y tecnologías, lo que aumenta la eficacia de sus campañas diseñadas para erosionar la confianza.

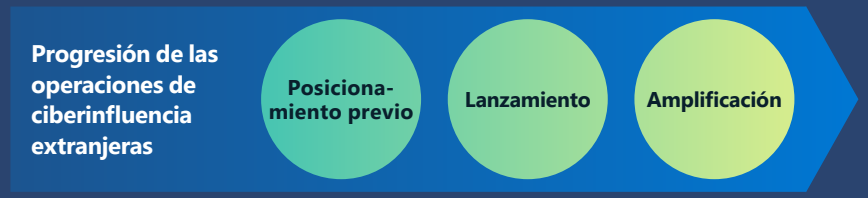
Información general sobre las

operaciones de ciberinfluencia

Las operaciones actuales de influencia extranjera utilizan nuevos métodos y tecnologías, lo que aumenta la eficacia de sus campañas diseñadas para erosionar la confianza.

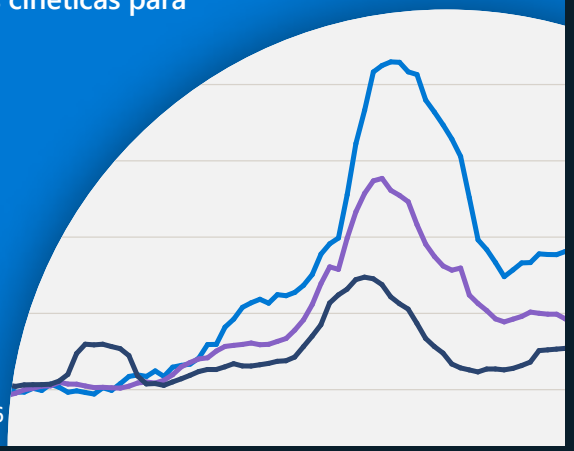
Los Estado nación utilizan cada vez más operaciones de influencia sofisticadas para distribuir propaganda e influir en la opinión pública tanto nacional como internacionalmente. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos. Los agentes, expertos manipuladores y concienzudos, utilizan los medios tradicionales junto con Internet y las redes sociales para aumentar enormemente el alcance, la escala y la eficiencia de sus campañas, y su influencia desmedida en el ecosistema de la información global. En el último año, hemos visto cómo estas operaciones se utilizaban como parte de la guerra híbrida de Rusia en Ucrania, pero también hemos visto a Rusia y otras naciones, como China e Irán, desplegar cada vez más operaciones propagandísticas en las redes sociales para ampliar su influencia global.

Las operaciones de ciberinfluencia son cada vez más sofisticadas a medida que más gobiernos y Estado nación utilizan estas operaciones para modelar la opinión, desacreditar a los adversarios y promover las desavenencias.



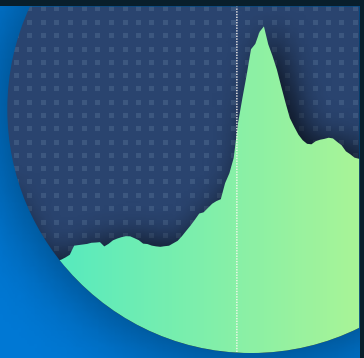
Más información en la página 74

La invasión rusa de Ucrania demuestra que las operaciones de ciberinfluencia se han integrado con ciberataques más tradicionales y operaciones militares cinéticas para maximizar el impacto.



Más información en la página 76

Rusia, Irán y China emplearon campañas propagandísticas y de influencia durante toda la pandemia de COVID-19 a menudo como un instrumento estratégico para lograr objetivos políticos más amplios.



Más información en la página 76

Los medios sintéticos son cada vez más frecuentes debido a la proliferación de herramientas que crean y difunden fácilmente imágenes artificiales, vídeos y audio muy realistas. La tecnología de procedencia digital que certifica el origen de activos multimedia promete combatir el uso indebido.

Más información en la página 80

Un enfoque integral para protegerse de las operaciones de ciberinfluencia

Microsoft emplea su infraestructura de inteligencia sobre ciberamenazas ya madura para combatir las operaciones de ciberinfluencia. Nuestra estrategia es detectar, interrumpir y frenar las campañas propagandísticas de agresores extranjeros, así como defendernos de ellas.

Más información en la página 83

Introducción

La democracia necesita información fiable para prosperar. Un ámbito de interés clave para Microsoft son las operaciones de influencia que desarrollan y perpetúan los estados nación. Estas campañas erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos.

Las operaciones de influencia extranjera siempre han sido una amenaza para el ecosistema de la información. Sin embargo, lo que es diferente en la era de Internet y las redes sociales es el enorme aumento del alcance, la escala y la eficiencia de las campañas, y el inmenso impacto que pueden tener en la salud del ecosistema global de la información.

Ahora, los datos corroboran el antiguo dicho de que «una mentira puede recorrer medio mundo mientras la verdad aún está poniéndose los zapatos». Un estudio del Instituto de Tecnología de Massachusetts (MIT)[1] constató que las falsedades tienen un 70 por ciento más de probabilidades de ser retuiteadas que la verdad y llegan a las primeras 1500 personas seis veces más rápido. El ecosistema de la información se ha vuelto cada vez más turbio a medida que las campañas propagandísticas prosperan en Internet y las redes sociales y socavan la confianza en las noticias tradicionales. En un estudio de 2021,[2] solo el 7 por ciento de los adultos estadounidenses afirmó que «confiaba mucho» en los periódicos y las noticias de la televisión y la radio, mientras que el 34 por ciento afirmó que «no confiaba nada».

Microsoft ha trabajado para identificar a los principales agentes, amenazas y tácticas en el espacio de influencia cibernética extranjero y para compartir las lecciones aprendidas. En junio de este año, publicamos un informe exhaustivo sobre las lecciones aprendidas de Ucrania, que contenía un análisis detallado de las operaciones de ciberinfluencia rusas.[3]

También estamos estudiando cómo las tecnologías avanzadas como los «deep fakes» pueden usarse como armas y socavar la credibilidad de los periodistas. Y estamos trabajando con la industria, el gobierno y el mundo académico para desarrollar mejores formas de detectar medios sintéticos y restaurar la confianza, como los sistemas de inteligencia artificial (IA) que pueden detectar las noticias falsas.

La naturaleza en rápido cambio del ecosistema de información y la propaganda online de los estados nación, incluida la fusión de los ciberataques tradicionales con las operaciones de influencia y la interferencia en las elecciones democráticas, requiere un enfoque que abarque a toda la sociedad para mitigar las amenazas tanto online como sin conexión a la democracia.

Microsoft tiene la misión de respaldar un ecosistema de información saludable en el que prosperen las noticias y la información fiables. Estamos desarrollando herramientas y funciones de detección de amenazas para combatir el riesgo cambiante y creciente de las operaciones de influencia basadas en los estados nación. Para facilitar este trabajo, recientemente adquirimos Miburo Solutions, nos hemos asociado con validadores externos como el Global Disinformation Index y NewsGuard, y participamos y, en ocasiones, lideramos asociaciones multilaterales, incluida la Coalition for Content Provenance and Authenticity (C2PA). Solo trabajando juntos, podremos enfrentarnos a aquellos que quieren socavar los procesos y las instituciones democráticos.

Teresa Hutson

Vicepresidenta, tecnología y responsabilidad corporativa

Tendencias en las operaciones de ciberinfluencia

Las operaciones de ciberinfluencia se vuelven cada vez más sofisticadas a medida que evoluciona la tecnología. Estamos viendo una superposición y expansión de las herramientas utilizadas en los ciberataques tradicionales que se aplican a las operaciones de ciberinfluencia. Asimismo, estamos viendo una mayor coordinación y amplificación entre los estados nación.

Microsoft invirtió en combatir las operaciones de influencia extranjera este año mediante la adquisición de Miburo Solutions, una empresa especializada en el análisis de operaciones de influencia extranjera. Reuniendo a estos analistas con los analistas del contexto de amenazas de Microsoft, Microsoft formó el Centro de análisis de amenazas digitales (DTAC). El DTAC analiza las amenazas de los estados nación e informa de ellas, incluidos los ciberataques y las operaciones de influencia, combinando información e inteligencia sobre amenazas con análisis geopolíticos para proporcionar conocimientos y proponer una respuesta y medidas de protección eficaces.

Más de tres cuartas partes de las personas de todo el mundo afirmaron que les preocupa el uso de información como un arma,[4] y nuestros datos respaldan estas preocupaciones. Microsoft y sus partners han realizado un seguimiento de cómo los agentes de los estados nación están utilizando las operaciones de influencia para lograr sus objetivos estratégicos y políticos. Además de los ciberataques destructivos y los esfuerzos de espionaje cibernético, los regímenes autoritarios utilizan cada vez más las operaciones de ciberinfluencia para modelar la opinión, desacreditar a los adversarios, incitar el miedo, promover la discordia y distorsionar la realidad.

Estas operaciones de ciberinfluencia extranjeras suelen tener tres etapas:

Posicionamiento previo

Al igual que el posicionamiento previo del malware dentro de la red informática de una organización, las operaciones de ciberinfluencia extranjeras publican relatos falsos preparatorios en el dominio público en Internet. La táctica de posicionamiento previo ha ayudado durante mucho tiempo a actividades cibernéticas más tradicionales, especialmente si los administradores de TI analizan su actividad de red más reciente. El malware que está latente durante un tiempo prolongado en una red puede hacer que su uso posterior sea más eficaz. Los relatos falsos que pasan inadvertidos en Internet pueden hacer que las referencias posteriores parezcan más creíbles.

Lanzamiento

A menudo, en el momento más beneficioso para lograr los objetivos del agente, se lanza una campaña coordinada para propagar relatos a través de los medios de comunicación y canales de redes sociales influidos y respaldados por los gobiernos.

Amplificación

Por último, los medios y proxies controlados por los estados nación amplifican los relatos para audiencias específicas. A menudo, habilitadores tecnológicos involuntarios amplían el alcance de los relatos. Por ejemplo, la publicidad online puede ayudar a las actividades financieras y los sistemas de entrega de contenido coordinados pueden inundar los motores de búsqueda.

Este enfoque de tres pasos se aplicó a finales de 2021 para respaldar el falso relato ruso sobre supuestas armas y laboratorios biológicos en Ucrania. Este relato se publicó por primera vez en YouTube el 29 de noviembre de 2021 como parte de un programa habitual en habla inglesa de un expatriado estadounidense con sede en Moscú que afirmó que los laboratorios biológicos financiados por Estados Unidos en Ucrania estaban vinculados a las armas biológicas. El relato pasó desapercibido durante meses. El 24 de febrero de 2022, justo cuando los tanques rusos cruzaban la frontera, el relato llegó al campo de batalla. Un equipo de análisis de datos de Microsoft identificó 10 sitios de noticias controlados o influidos por Rusia que publicaron simultáneamente informes el 24 de febrero refiriéndose al «informe del año pasado» y tratando de darle crédito. Asimismo, funcionarios del Ministerio de Asuntos Exteriores ruso realizaron conferencias de prensa que sembraron noticias falsas sobre laboratorios biológicos estadounidenses en el entorno de la información. Los equipos patrocinados por Rusia trabajaron entonces para amplificar el relato en las redes sociales y en sitios de Internet para que tuviera mayor difusión.

Estamos viendo que regímenes autoritarios de todo el mundo trabajan juntos para contaminar el ecosistema de la información en beneficio mutuo. Por ejemplo, durante toda la pandemia de COVID-19, Irán y China emplearon operaciones propagandísticas y de influencia usando una combinación de métodos de difusión abiertos, semiencubiertos y cubiertos para atacar las democracias y otros objetivos geopolíticos (que se analizan más adelante en la página 76). Los tres regímenes formaban parte de los ecosistemas de mensajería e información de los otros para promocionar sus relatos preferidos. Gran parte de esta cobertura consistió en críticas o teorías conspiratorias sobre Estados Unidos y sus aliados promulgadas por figuras gubernamentales en declaraciones oficiales mientras promocionaban sus propias vacunas y respuestas a la COVID-19 como superiores a las de los Estados Unidos y otras democracias. Al amplificar los relatos unos a otros, los medios de comunicación operados por los estados crearon un ecosistema en el que la cobertura negativa de las democracias (o la cobertura positiva de Rusia, Irán y China) producida por un medio de comunicación estatal era corroborada por los otros.

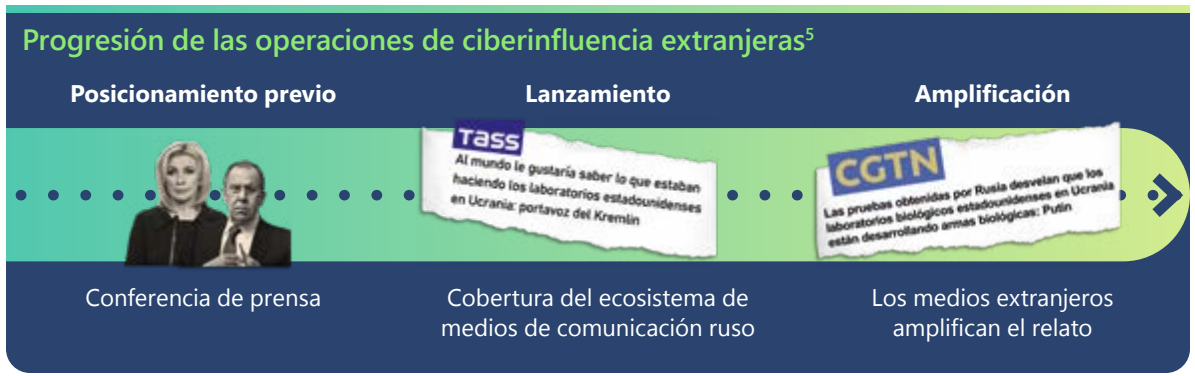


Ilustración de cómo los relatos sobre laboratorios biológicos y armas biológicas de Estados Unidos se propagaban a través de las tres grandes fases de muchas operaciones de influencia extranjera: posicionamiento previo, lanzamiento y amplificación.

Tendencias en las operaciones de ciberinfluencia

Continuación

A este desafío se suma el hecho de que las entidades tecnológicas del sector privado podrían permitir sin querer estas campañas. Los habilitadores pueden incluir empresas que registran dominios de Internet, alojan sitios web, promueven material en redes sociales y sitios de búsqueda, canalizan el tráfico y ayudan a pagar estas actividades con publicidad digital. Las organizaciones deben conocer las herramientas y métodos empleados por los regímenes autoritarios para las operaciones de ciberinfluencia para poder detectar y evitar la propagación de las campañas. También existe una creciente necesidad de ayudar a los consumidores a desarrollar mayor capacidad para identificar las operaciones de influencia extranjera y limitar su implicación en los relatos o contenidos.

Las operaciones de ciberinfluencia, incluida la propaganda de los regímenes autoritarios, son una amenaza a las democracias en todo el mundo, ya que erosionan la confianza, aumentan la polarización y amenazan los procesos democráticos.

Se necesita una mayor coordinación e intercambio de información entre los gobiernos, el sector privado y la sociedad civil para aumentar la transparencia y divulgar e interrumpir estas campañas de influencia.

En todo el mundo, a más de las tres cuartas partes de los ciudadanos les preocupa que esta información se utilice como un arma.

Aspectos destacados de las operaciones de influencia durante la pandemia de la COVID-19 y la invasión rusa de Ucrania

Los estados nación que buscaban controlar el entorno de información a lo largo de la pandemia y durante la invasión rusa de Ucrania proporcionan ejemplos contundentes de cómo los regímenes autoritarios combinan las operaciones cibernéticas y de información.

Propaganda de la COVID-19

Rusia, Irán y China emplearon campañas propagandísticas y de influencia durante la pandemia de COVID-19. El tema de la COVID-19 ocupaba un lugar central en estas campañas de dos maneras:

1. Representaciones de la propia pandemia.
2. Campañas que utilizaron la COVID-19 como un medio estratégico de lograr objetivos políticos más amplios.

El objetivo general de este tipo de campañas es doble: en primer lugar, socavar las democracias, las instituciones democráticas y la imagen de los Estados Unidos y sus aliados en la etapa global; y en segundo lugar, reforzar su propia posición nacional e internacional.

Se puede ver un ejemplo de esto en los mensajes enviados por cuentas y organizaciones de medios de comunicación rusos dirigidos a lectores de habla inglesa que versaban sobre cómo el gobierno ruso se comunicaba con sus ciudadanos en relación con las vacunas y la gravedad de la COVID-19.

Temas cubiertos por las 10 noticias de coronavirus más vistas en RT.com
(octubre de 2021-abril de 2022)

La propaganda antivacunas se dirige a lectores no rusos

Ruso (traducido abajo al español)	Inglés (traducido al español)
«Los confinamientos y las dosis de refuerzo impiden la transmisión»	«Las vacunas son incapaces de frenar la transmisión y no son eficaces contra las nuevas cepas»
«Figuras públicas rusas están dando positivo»	«La vacuna de Pfizer tiene efectos secundarios peligrosos»
«Los casos y las muertes aumentan en Rusia»	«La vacunación masiva tiene motivaciones políticas»
«La vacuna Sputnik V es sumamente eficaz»	«Pfizer y Moderna realizan ensayos no regulados»
«Se necesita un certificado de vacunación en el transporte público»	

Los mensajes rusos sobre la COVID-19 difieren en función del idioma.

Las campañas que trataron de ocultar el origen del virus COVID-19 constituyen otro ejemplo. Desde el inicio de la pandemia, la propaganda rusa, iraní y china sobre la COVID-19 aumentó su cobertura con respecto a las de los demás países para amplificar estos temas centrales. Gran parte de esta cobertura consistió en realizar críticas o divulgar teorías conspiratorias acerca de los Estados Unidos. Al amplificar periódicamente los relatos unos a otros, los medios de comunicación operados por los estados desarrollaron un ecosistema en el que la cobertura negativa de las democracias (o la cobertura positiva de Rusia, Irán y China) producida por un medio de comunicación estatal era corroborada por los otros.

Un ejemplo de ello es la insinuación a principios de la pandemia por parte de los medios estatales rusos e iraníes de que la COVID-19 podría ser un arma biológica creada por Estados Unidos. Esta afirmación circuló por sitios web conspiratorios radicales al principio de la pandemia después de una entrevista con un profesor de derecho que afirmó que creía que la COVID-19 se creó como un arma.[6] Después de que la entrevista se publicara en algunos sitios web con un alcance limitado, medios de comunicación estatales se hicieron eco de la noticia. PressTV, un canal de noticias de habla inglesa y francesa patrocinado por el gobierno iraní,[7] publicó una noticia en lengua inglesa en febrero de 2020 titulada «¿Es el coronavirus un arma biológica de EE. UU. como cree Francis Boyle?». El artículo sugería que los Estados Unidos estaban detrás del brote de COVID-19 y añadía: «En todas las guerras de EE. UU., se utilizan armas radiológicas, químicas, biológicas y otras armas prohibidas, que causan un efecto devastador en las personas de determinadas zonas».[8] Medios de comunicación del estado ruso y cuentas gubernamentales chinas divulgaron esta insinuación. Russia Today (RT), un canal de noticias propiedad del estado conocido por su papel en la difusión propagandística del Kremlin,[9] publicó al menos un artículo que dio pie a que altos ejecutivos iraníes afirmaran que la COVID-19 podría ser un «producto del ataque biológico de EE. UU. dirigido a Irán y China»[10], que tuvo mucha repercusión en las redes sociales. Por ejemplo, un tweet de RT del 27 de febrero de 2020 decía: «Que levanten la mano aquellos que no se sorprenderían si se revelara que el #coronavirus es un arma biológica».[11]

La guerra en Ucrania: la propaganda como arma de guerra

La invasión rusa de Ucrania ofrece un ejemplo elocuente de cómo las operaciones de ciberinfluencia se pueden combinar con ciberataques más tradicionales y operaciones militares sobre el terreno para maximizar su impacto.

En el período inmediatamente anterior a la invasión de Ucrania, analistas de inteligencia sobre amenazas de Microsoft vieron al menos cómo seis agentes afiliados a Rusia lanzaban más de 237 ciberataques contra Ucrania. Estas campañas pretendían degradar los servicios y las instituciones, interrumpir el acceso de los ucranianos a información fiable y sembrar dudas sobre el liderazgo del país.

Aspectos destacados de las operaciones de influencia durante la pandemia de la COVID-19 y la invasión rusa de Ucrania

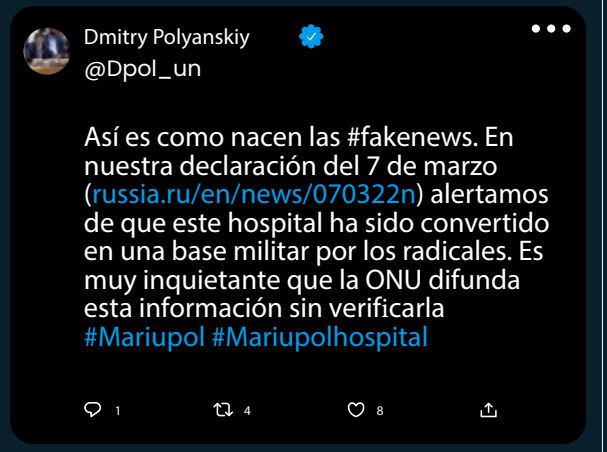
Continuación

En un informe de Microsoft publicado en abril de 2022, mostramos cómo, en un intento aparente de controlar el entorno de información de Kiev, Rusia lanzó un ataque con misiles contra una torre de televisión de Kiev el mismo día que lanzó un malware destructivo contra una importante empresa de medios de comunicación ucraniana.[12]

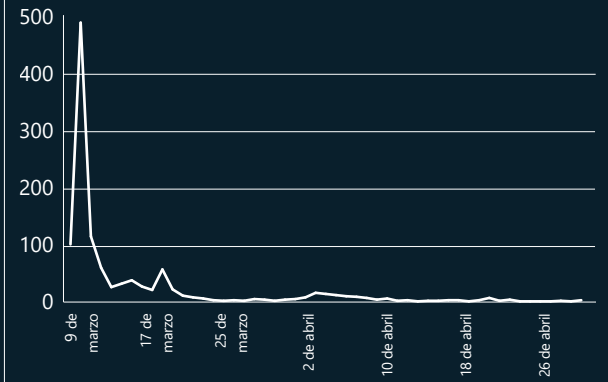
Un actor de amenazas ruso envió a ciudadanos ucranianos correos electrónicos que decían proceder de residentes de Mariupol en los que se culpaba al gobierno ucraniano de la escalada de la guerra y pedían a los compatriotas que lucharan contra el gobierno, lo que constituye otro ejemplo de cómo convergen los ciberataques y las operaciones de influencia. Estos correos electrónicos se dirigieron a los destinatarios por su nombre, lo que indica que posiblemente se robó su información en un ciberataque anterior relacionado con el espionaje. No se incluyeron enlaces malintencionados, lo que sugiere que su intención era únicamente llevar a cabo una operación de influencia.

Una táctica frecuente que utilizan los agentes rusos en las operaciones de influencia es emplear material supuestamente pirateado o filtrado o de carácter confidencial. Durante la guerra de Ucrania, los canales sociales prorrusos han promocionado materiales que, según ellos, han sido filtrados de fuentes ucranianas. Los canales sociales y los medios de comunicación prorrusos utilizan materiales filtrados o de carácter confidencial como parte de una estrategia de influencia mayor para minar la confianza en las instituciones y poner en duda los relatos dominantes. Esta información puede manipularse para crear ataques propagandísticos contra Ucrania y los países occidentales, minar la confianza en la seguridad digital y erosionar el apoyo de la ayuda occidental a Ucrania.

Rusia ha usado otros ataques de información para modelar la opinión pública después de ataques sobre el terreno con el fin de ocultar o desvirtuar los hechos. Por ejemplo, el 7 de marzo, Rusia lanzó un relato preparatorio a través de una comunicación dirigida a la Organización de las Naciones Unidas (ONU) en el que se explicaba que un hospital de maternidad de Mariupol, Ucrania, había sido vaciado y estaba siendo utilizado como base militar. El 9 de marzo, Rusia bombardeaba el hospital. Después de la noticia del bombardeo, el representante ruso de la ONU, Dmitry Polyanskiy, tuiteó que la cobertura del ataque era una noticia falsa y mencionó las declaraciones anteriores rusas sobre su supuesto uso como base militar. A continuación, Rusia difundió este relato por sitios web controlados por Rusia durante dos semanas después del ataque al hospital.

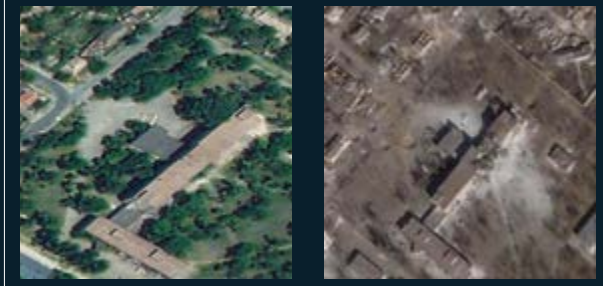


Dominios con tráfico
(9 de marzo de 2022-30 de abril de 2022)



Sitios web propagandísticos publican noticas sobre el hospital de maternidad durante aproximadamente dos semanas recuperando una noticia del 1 de abril de 2022. Fuente: Microsoft IA for Good Lab.

Imágenes por satélite de un hospital perinatal de Mariupol en febrero y marzo de 2022



Imágenes por satélite de Microsoft demostraron que el hospital perinatal había sido bombardeado. La primera foto es del 24 de febrero de 2022 y la segunda es del 24 de marzo de 2022. Fuente de la foto: Planet Labs.

El blanqueamiento de las atrocidades rusas ha continuado a lo largo de la guerra. Por ejemplo, a finales de junio de 2022, medios de comunicación e «influencers» rusos interpretaron el bombardeo de un centro comercial como algo justificado y necesario, afirmando falsamente que no se utilizaba como centro comercial, sino más bien como un arsenal de las fuerzas de defensa territorial ucranianas.[13] Varios blogueros afines al Kremlin de Telegram publicaron y amplificaron el contenido reforzando el relato de «bandera falsa», con blogueros que señalaban supuestos indicadores de fabricación de armas, incluida la presencia de personas con uniforme militar en las imágenes de la escena[14] y la ausencia de mujeres en las imágenes.[15] Rusia lanzó las campañas gracias a un sistema integrado de mensajeros y medios de comunicación propagandísticos.
La amplificación de estos relatos online proporciona a Rusia la capacidad de eludir su responsabilidad en el escenario internacional y evitar tener que rendir cuentas.

Estados nación como Rusia conocen el valor de usar la información obtenida de fuentes cerradas para influir en la opinión pública, utilizando campañas «hack and leak» para contrarrestar los relatos y sembrar la desconfianza.

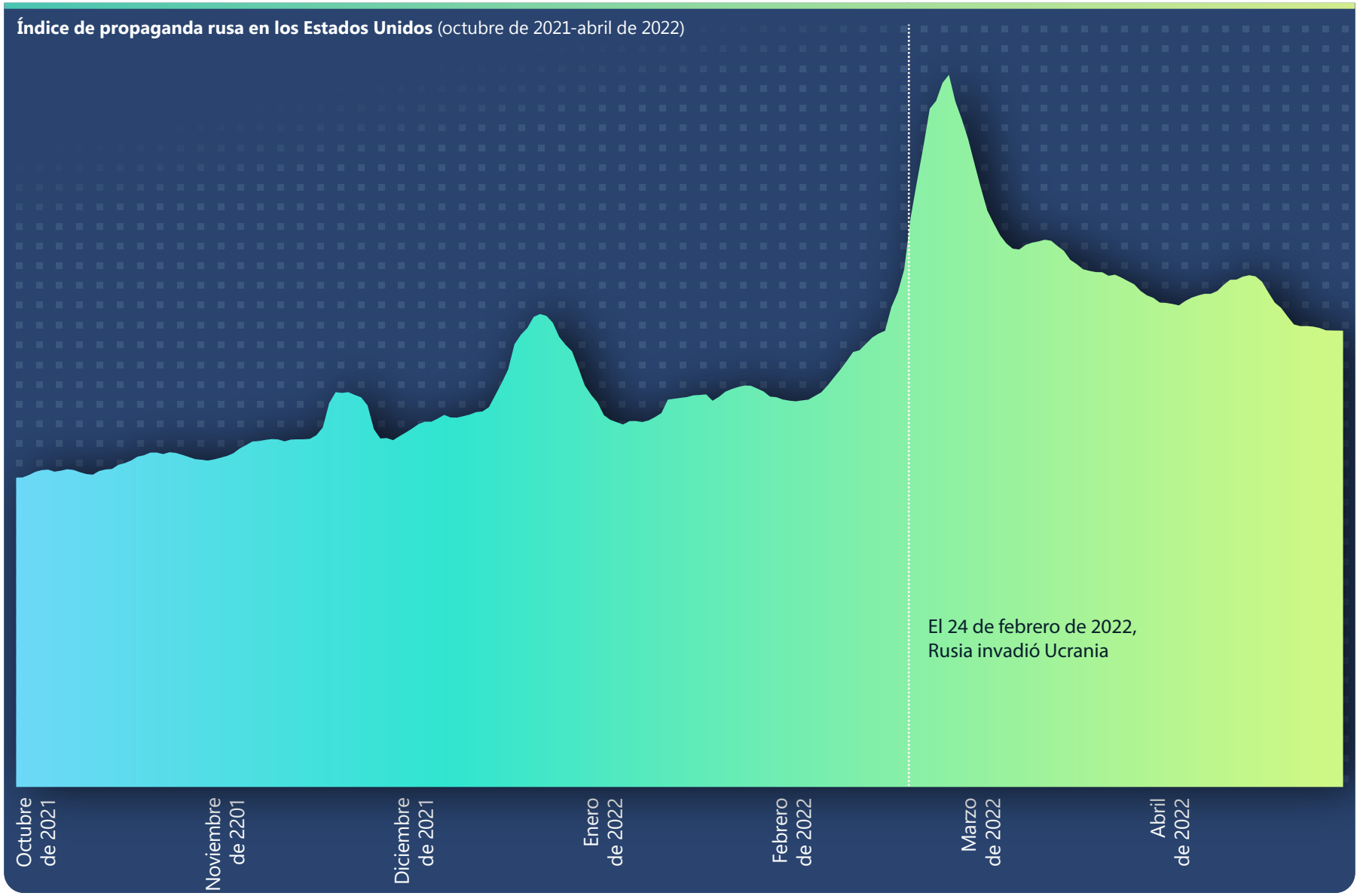
Enlaces a información adicional (pueden estar en inglés)

- Defensa de Ucrania: lecciones tempranas de la guerra cibernética | Microsoft On the Issues
- Información general de la actividad de ciberataques de Rusia en Ucrania | Informe especial de Microsoft
- Desmantelamiento de ciberataques dirigidos a Ucrania | Microsoft On the Issues

Seguimiento del programa de propaganda ruso

En enero de 2022, casi mil sitios web estadounidenses hablaban de tráfico a sitios web propagandísticos rusos. Los temas más habituales de los sitios web propagandísticos rusos dirigidos a un público estadounidense fueron la guerra de Ucrania, la política interior de Estados Unidos (tanto a favor de Trump como a favor de Biden) y relatos relacionados con la COVID-19 y las vacunas.

El Índice de propaganda rusa (RPI, por sus siglas en inglés) supervisa el flujo de noticias de los canales de comunicación y amplificadores controlados y patrocinados por el estado ruso como una proporción del tráfico general de noticias en Internet. El RPI se puede utilizar para cartografiar el consumo de propaganda rusa a través de Internet y en diferentes zonas geográficas en una línea cronológica precisa. Microsoft señala, sin embargo, que solo podemos observar la propaganda rusa publicada en sitios web previamente identificados. No tenemos información sobre la propaganda en otros tipos de sitios web, incluidos sitios de noticias autorizados, sitios web no identificados y grupos de redes sociales.



Seguimiento del programa de propaganda ruso

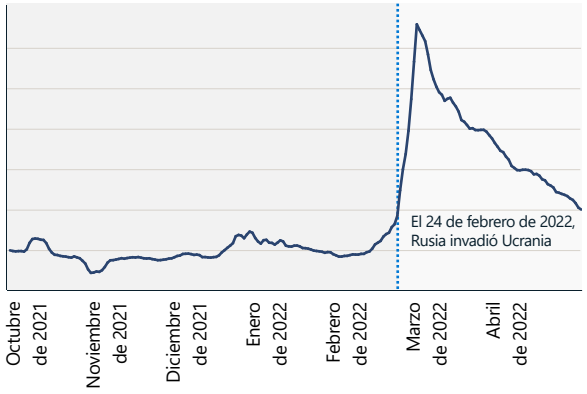
Continuación

Índice de propaganda rusa: Ucrania

Cuando comenzó la guerra de Ucrania, vimos un aumento del 216 por ciento en la propaganda rusa, alcanzando su punto máximo el 2 de marzo. En la siguiente tabla se muestra cómo este aumento repentino coincide con la invasión. Los dos gráficos muestran cómo la propaganda rusa empezó poco después de que comenzara la invasión.

RPI, Ucrania

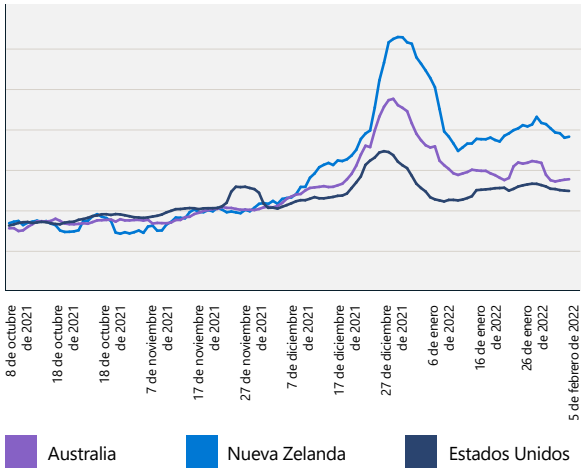
(7 de octubre de 2021-30 de abril de 2022)



Índice de propaganda rusa: Nueva Zelanda frente a Australia y Estados Unidos

Una evaluación del RPI en Nueva Zelanda mostró un aumento a finales de 2021 relacionado con la propaganda de la COVID-19. Este aumento del consumo de propaganda rusa en Nueva Zelanda precedió a un aumento de las protestas públicas a principios de 2022 en Wellington. Un segundo pico estaba claramente relacionado con la invasión rusa de Ucrania y superó los RPI de Australia y los Estados Unidos.

RPI, Nueva Zelanda frente a Australia y Estados Unidos



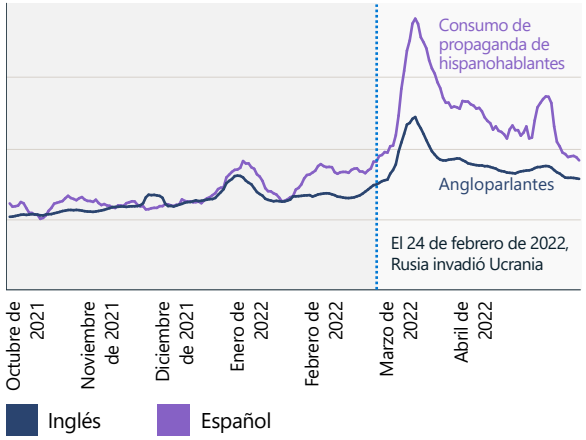
El consumo de propaganda rusa en Nueva Zelanda es similar al de Australia hasta la primera semana de diciembre de 2021. Después de diciembre, el consumo de propaganda rusa en Nueva Zelanda aumentó en más de un 30 por ciento con respecto al consumo en Australia y los Estados Unidos.

Índice de propaganda rusa en los Estados Unidos: inglés y español

El RPI también rastrea la propaganda en otros idiomas. Varios canales de noticias, incluidos RT y Sputnik News, están disponibles en más de 20 idiomas. Estos incluyen inglés, español, alemán, francés, griego, italiano, checo, polaco, serbio, letón, lituano, moldavo, bielorruso, armenio, osetio, georgiano, azerbaiyano, árabe, turco, persa y dari.

El siguiente gráfico muestra que el RPI para las noticias en español en Estados Unidos es mucho mayor que el de las noticias en inglés.

El consumo de propaganda rusa es dos veces mayor entre los hispanohablantes



El consumo de propaganda rusa en Estados Unidos es dos veces mayor entre los hispanohablantes.

La propaganda rusa es alta en Latinoamérica

RT en español es el canal de noticias internacionales con el mayor número de visitas a páginas y seguidores de Facebook.

Fuente: Microsoft AI for Good Research Lab

Medios sintéticos

Hemos entrado en la edad de oro de la creación y manipulación de contenido multimedia a través de la IA. Los analistas de Microsoft señalan que esto se debe a dos tendencias clave: la proliferación de herramientas y servicios fáciles de usar para crear artificialmente imágenes, vídeos, audio y texto sintéticos muy realistas y la capacidad de difundir rápidamente contenido optimizado para audiencias específicas.

Ninguno de estos desarrollos es problemático de por sí. La tecnología basada en IA se puede utilizar para crear contenido digital divertido y atractivo, ya sea creando un producto puramente sintético o mejorando el material existente. Estas herramientas están siendo ampliamente utilizadas por empresas para la publicidad y las comunicaciones, y por particulares para crear contenido atractivo para sus seguidores. Sin embargo, los medios sintéticos, cuando se crean y distribuyen con la intención de hacer daño, tienen el potencial de causar daños graves a las personas, las empresas, las instituciones y la sociedad. Microsoft ha sido una fuerza impulsora en el desarrollo de tecnologías y prácticas, tanto internamente como en todo el ecosistema general de contenido multimedia, para limitar este daño.

En este apartado se exploran los conocimientos del análisis de Microsoft sobre el estado actual de la tecnología de vanguardia para la creación de contenido sintético dañino, los daños que pueden surgir si este contenido se difunde ampliamente y las mitigaciones técnicas que pueden defender contra las ciberamenazas basadas en medios sintéticos.

Creación de medios sintéticos

El campo de texto y contenido multimedia sintéticos avanza a pasos agigantados, debido a que las técnicas que antes eran solo posibles con los inmensos recursos informáticos de los grandes estudios cinematográficos ahora están integradas en las aplicaciones para el teléfono. Al mismo tiempo, las herramientas son cada vez más fáciles de usar y pueden generar contenido con un nivel de realismo capaz de engañar incluso a los especialistas de contenido multimedia forenses. Estamos muy cerca de llegar al punto en el que cualquiera pueda crear un vídeo sintético de una persona diciendo o haciendo cualquier cosa. No es descabellado pensar que estamos entrando en una época en la que una cantidad importante del contenido que vemos online se ha sintetizado total o parcialmente con técnicas de IA.

> Gracias a la disponibilidad de herramientas más sofisticadas, fáciles de usar y ampliamente disponibles, la creación de contenido sintético no hace otra cosa que crecer y pronto será indistinguible de la realidad.

Hay muchas herramientas de edición de audio, vídeo y imágenes comerciales y gratuitas de alta calidad. Estas herramientas se pueden utilizar para realizar cambios sencillos pero potencialmente dañinos en el contenido digital, como añadir texto engañoso, intercambiar rostros y eliminar o alterar el contexto. Estas «cheap fakes» se utilizan ampliamente para difundir contenido malicioso, promover ideologías políticas y dañar la reputación. Un ejemplo conocido es el vídeo de 2019[16] de la portavoz de la Cámara de EE. UU., Nancy Pelosi, hablando con balbuceos, lo que daba la impresión de que estaba borracha. Aunque pronto se determinó que el vídeo se había ralentizado para crear el efecto, la «cheap fake» se difundió por todas partes antes de que se dieran a conocer el vídeo y el contexto originales.

Entre los enfoques más sofisticados para modificar el contenido multimedia se incluye la aplicación de técnicas avanzadas de IA para (a) crear medios puramente sintéticos y (b) realizar ediciones más sofisticadas del contenido multimedia existente. El término «deepfake» se utiliza a menudo para definir los medios sintéticos que se han creado utilizando técnicas de IA de vanguardia (el nombre proviene de las redes neuronales profundas («deep») que se utilizan a veces). Estas tecnologías se están desarrollando como aplicaciones, herramientas y servicios independientes e integradas en herramientas de edición comerciales y de código abierto establecidas.

Estas tecnologías las utilizan los agentes dañinos como armas con la intención de dañar a particulares e instituciones. Algunos ejemplos de técnicas de «deepfake» son:

- **Intercambio de rostros (vídeo, imágenes):** reemplazar una cara en un vídeo por otra. Esta técnica se puede utilizar para intentar chantajear a una persona, empresa o institución, o para colocar a las personas en lugares o situaciones embarazosas.
- **«Puppeteering» (vídeo, imágenes)**: usar un vídeo para animar una imagen fija o un segundo vídeo. Esto puede hacer que parezca que una persona ha dicho algo embarazoso o engañoso.
- **Redes generativas antagónicas (vídeo, imágenes)**. un grupo de técnicas para generar imágenes fotorrealistas.
- **Modelos de transformadores (vídeo, imágenes, texto):** crear imágenes multimedia a partir de descripciones de texto.

Estas técnicas avanzadas basadas en IA aún no se utilizan de manera generalizada en las campañas de ciberinfluencia de hoy en día, pero esperamos que el problema crezca a medida que las herramientas sean más fáciles de usar y estén más disponibles.

El impacto de la manipulación de medios sintéticos

El uso de las operaciones de información para causar daños o expandir la influencia no es nuevo. Sin embargo, la velocidad a la que se puede propagar la información y nuestra incapacidad para distinguir rápidamente los hechos de la ficción significan que el impacto y el daño causados por las falsificaciones y otros medios maliciosos generados de forma sintética pueden ser mucho mayores, como demuestra el ejemplo de Pelosi.

Clasificamos los daños en varios grupos: manipulación del mercado, fraude de pagos, «vishing», suplantaciones, daños a la marca, daños a la reputación y botnets. Hemos visto un gran número de ejemplos reales de muchos de estos grupos, capaces de socavar nuestra capacidad de separar los hechos de la ficción.

Esto supone una amenaza a largo plazo y más insidiosa a nuestra capacidad de dilucidar lo que es cierto si ya no podemos confiar en lo que vemos y escuchamos. Debido a esto, puede desestimarse la falsedad de cualquier imagen, audio o vídeo comprometedor de una figura pública o privada, un resultado conocido como El beneficio del mentiroso.[17] Las investigaciones recientes[18] muestran que este abuso de la tecnología ya se está utilizando para atacar los sistemas financieros, aunque muchos otros escenarios de abuso son plausibles.

Medios sintéticos

Continuación

Detección de medios sintéticos

Se están realizando esfuerzos en la industria, la administración y el mundo académico para desarrollar mejores formas de detectar y mitigar los medios sintéticos y restaurar la confianza. Hay varios caminos prometedores que se pueden seguir, así como obstáculos que deben ser considerados.

Un enfoque es crear sistemas basados en IA que puedan identificar información falsa, básicamente, sistemas de IA «defensivos» para contrarrestar los sistemas de IA ofensivos. Esta es un área de investigación activa en la que los sistemas actuales para crear audio y vídeo sintéticos dejan artefactos delatores que pueden ser detectados por analistas forenses de contenido multimedia cualificados y herramientas automatizadas.

Lamentablemente, aunque las noticias falsas actuales tienen fallos, los artefactos precisos suelen ser específicos de una herramienta o algoritmo en concreto. Esto significa que el entrenamiento sobre falsas noticias conocidas no suele generalizarse a otros algoritmos, como se demostró en una competición abierta de 2020 para crear detectores de «deepfakes».[19] Puede parecer tentador aumentar la inversión en el desarrollo de detectores más avanzados, pero Microsoft no está muy convencida de que esto produzca mejoras significativas por dos razones:

En primer lugar, tenemos excelentes modelos físicos que reflejan el mundo real. Los creadores actuales de noticias falsas toman atajos, lo que produce artefactos detectables, pero los modelos más recientes son cada vez más realistas. No hay nada inherentemente especial en una escena del mundo real capturada por una cámara que no pueda modelar un ordenador.

En segundo lugar, los algoritmos avanzados de creación de noticias falsas utilizan una técnica denominada Redes generativas antagónicas (GAN, por sus siglas en inglés) como parte del proceso de creación. Una GAN utiliza dos sistemas de IA contrapuestos que constan de un generador para crear la información falsa y un discriminador para detectar imágenes falsas y entrenar el generador. Cualquier inversión en desarrollar un detector mejor solo permitirá que el generador mejore la calidad de la información falsa.

Medios sintéticos

Continuación

Procedencia de los activos digitales

Si la detección de información falsa no es fiable, ¿qué podemos hacer para protegernos de los usos dañinos de los medios sintéticos? Una tecnología emergente importante es la procedencia digital, un mecanismo que permite a los creadores de contenido multimedia digitales certificar un activo y ayudar a los consumidores a identificar si el activo digital ha sido manipulado o no. La procedencia digital es particularmente importante en el contexto de las redes sociales actuales dada la velocidad con la que el contenido puede viajar a través de Internet y la oportunidad de que los agentes dañinos manipulen fácilmente el contenido.

900 %

aumento año tras año de la proliferación de «deepfakes» desde 2019.[20]

La tecnología de procedencia digital es una versión moderna de la firma criptográfica de documentos, diseñada para capturar el origen, el historial de modificaciones y los metadatos de los objetos a medida que viajan por Internet. La idea y los métodos técnicos para permitir este tipo de certificación de contenido multimedia a prueba de manipulaciones fueron desarrollados por un equipo interdisciplinar de investigadores y científicos de Microsoft. Colaboramos en una asociación intersectorial destinada a dar vida a la tecnología de procedencia de contenido multimedia en Project Origin (fundada por Microsoft, la BBC, CBC/Radio-Canada y el New York Times) y participamos en la Content Authenticity Initiative (fundada por Adobe). Microsoft también ha trabajado con partners de servicios de tecnología y contenido multimedia para fundar la Coalition for Content Provenance and Authenticity (C2PA). C2PA es una organización de estándares que recientemente publicó la especificación de procedencia digital más avanzada para su uso con activos multimedia como imágenes, vídeos, audio y texto.

Un objeto habilitado para C2PA incorpora un manifiesto que protege el objeto y los metadatos de la manipulación, y el certificado que lo acompaña identifica al publicador.

Los medios sintéticos no se diseñaron originalmente para causar daños, pero agentes dañinos los están empleando como armas para socavar la confianza en las personas y las instituciones.

La procedencia digital es una tecnología emergente prometedora que tiene el potencial de ayudar a restaurar la confianza de las personas en el contenido multimedia online mediante la certificación del origen de un activo multimedia.

Las soluciones disponibles públicamente basadas en la especificación C2PA se incluyen como una nueva característica en los productos existentes o como nuevas aplicaciones y servicios independientes. Esperamos que la mayoría de las herramientas de captura, edición y creación usadas habitualmente sean compatibles con C2PA en pocos años. Esto representa una oportunidad para que las empresas determinen sus necesidades y usos para la procedencia digital en la actualidad y para exigir esta capa adicional de protección en las herramientas que utilizan en los flujos de trabajo existentes.

Conocimientos prácticos

1. Toma medidas proactivas para proteger tu organización de las amenazas de desinformación considerando de manera proactiva tus respuestas en las relaciones públicas y la comunicación.
2. Utiliza la tecnología de procedencia para proteger las comunicaciones oficiales.

Enlaces a información adicional (pueden estar en inglés)

- Un avance prometedor contra la desinformación | Microsoft On the Issues
- Un hito alcanzado, 31 de enero de 2022
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- Detalles técnicos del sistema que utiliza Project Origin para la autenticación de contenido multimedia | Microsoft ALT Innovation

Un enfoque integral para protegerse de las operaciones de ciberinfluencia

Microsoft se basa en su infraestructura de inteligencia sobre amenazas cibernéticas ya madura para desarrollar una visión más amplia e inclusiva de las operaciones de ciberinfluencia.

Utilizamos un marco de trabajo para las estrategias de respuesta y mitigación sugeridas para combatir la amenaza que plantean las operaciones, que se puede dividir en cuatro pilares clave: detectar, interrumpir, defender y disuadir.

Asimismo, Microsoft ha adoptado cuatro principios para afianzar nuestro trabajo en este ámbito. El primero es el compromiso de respetar la libertad de expresión y mantener la capacidad de nuestros clientes de crear, publicar y buscar información a través de nuestras plataformas, productos y servicios. En segundo lugar, trabajamos de forma proactiva para evitar que nuestras plataformas y productos se utilicen para amplificar sitios y contenido de ciberinfluencia extranjeros. En tercer lugar, no nos beneficiaremos económicamente de forma deliberada del contenido o de los agentes de ciberinfluencia extranjeros. Por último, priorizamos la divulgación de contenido para contrarrestar las operaciones de ciberinfluencia extranjeras utilizando datos internos y fiables de terceros en nuestros productos.

Detectar

Al igual que con la defensa cibernética, el primer paso para contrarrestar las operaciones de ciberinfluencia extranjeras es desarrollar la capacidad de detectarlas. Ninguna empresa u organización puede esperar por sí sola hacer los avances necesarios. Una nueva y más amplia colaboración entre el sector tecnológico será crucial, ya que los avances en el análisis y la divulgación de las operaciones de ciberinfluencia dependen en gran medida del papel de la sociedad civil, incluidas las instituciones académicas y organizaciones sin ánimo de lucro.

Una vez reconocido este papel, los investigadores Jake Shapiro y Alicia Wanless de la Universidad de Stanford y la Carnegie Endowment for International Peace, respectivamente, han elaborado planes para lanzar el nuevo «Institute for Research on the Information Environment» (IRIE). Con el apoyo de Microsoft, la Knight Foundation y Craig Newmark Philanthropies, la IRIE creará una institución de investigación multisectorial inclusiva inspirada en la Organización Europea para la Investigación Nuclear (CERN). Combinará conocimientos especializados en procesamiento y análisis de datos para acelerar y permitir nuevos descubrimientos en este ámbito. Las conclusiones se compartirán para mantener más informados a los legisladores, las empresas tecnológicas y los consumidores.

Defender

El segundo pilar estratégico es reforzar las defensas democráticas, una prioridad a largo plazo que necesita inversión e innovación. Debe tener en cuenta los desafíos que la tecnología ha planteado a la democracia y las oportunidades que la tecnología ha creado para defender a las sociedades democráticas de manera más eficaz.

El marco de estrategia de Microsoft tiene como objetivo ayudar a las partes interesadas multisectoriales a detectar, interrumpir, defenderse y disuadir de la propaganda, especialmente las campañas de agresores extranjeros.

Es conveniente comenzar con uno de los grandes desafíos tecnológicos de nuestra era: el impacto de Internet y la publicidad digital en el periodismo tradicional. Desde el siglo XVIII, la prensa libre e independiente ha desempeñado un papel especial en apoyar a todas las democracias del planeta, desvelando la corrupción, documentando las guerras y esclareciendo los mayores desafíos sociales de esta y otras épocas. Sin embargo, Internet ha destrozado el periodismo local al devorar los ingresos publicitarios y captar a los suscriptores de pago. Muchos periódicos locales han cerrado. Una de las numerosas conclusiones de nuestro trabajo reciente es que las poblaciones que carecen de un periódico están inadvertida e inevitablemente expuestas a un volumen mayor que la media de propaganda extranjera. Por estas razones, uno de los puntales defensivos críticos de la democracia debe fortalecer el periodismo tradicional y una prensa libre, especialmente a escala local. Esto requiere una inversión e innovación continuas que deben reflejar las necesidades locales de diferentes países y continentes. Estos problemas no son sencillos y requieren enfoques multilaterales, que Microsoft y otras empresas tecnológicas están respaldando cada vez más.

También necesitamos nuevas innovaciones en las políticas públicas, que deben ser una prioridad pública. Esto puede incluir leyes que permitan a los editores negociar los ingresos publicitarios colectivamente con las empresas de tecnología, y legislación que proporcione créditos fiscales para aliviar a las redacciones locales de una parte de los impuestos de los periodistas que trabajan en ellas. Los periodistas necesitan muchas otras herramientas para desempeñar su oficio, incluida la capacidad de dividir el contenido entre fuentes legítimas y fraudulentas.

También existe una necesidad cada vez mayor de ayudar a los consumidores a desarrollar mayor capacidad para identificar las operaciones de información basadas en los estados nación. Aunque esto pueda parecer desalentador, es similar al trabajo que el sector de la tecnología lleva mucho tiempo haciendo para combatir otras ciberamenazas. Se debe considerar la posibilidad de formar a los consumidores para que estén más atentos a las direcciones de correo electrónico con el fin de ayudar a detectar spam u otras comunicaciones fraudulentas. Iniciativas en los Estados Unidos, como el News Literacy Project y el Trusted Journalism.

Esto supone una amenaza a largo plazo y más insidiosa a nuestra capacidad de dilucidar lo que es cierto si ya no podemos confiar en lo que vemos y escuchamos.

Un enfoque integral para protegerse de las operaciones de ciberinfluencia

Continuación

Los programas están ayudando a crear consumidores mejor informados sobre noticias e información. En todo el mundo, las nuevas tecnologías, como el plugin de navegador de NewsGuard, pueden ayudar a hacer avanzar esta iniciativa mucho más rápido.

Esto también nos debe recordar que parte de los cimientos de la democracia es la educación de la sociedad civil. Como siempre, este esfuerzo debe comenzar en las escuelas. Pero vivimos en un mundo que requiere recibir educación cívica continua a lo largo de toda una vida. La nueva promesa de la educación cívica en el trabajo, liderada por el Centro de Estudios Estratégicos e Internacionales, y de la que Microsoft ha sido signataria inaugural, pretende revitalizar la alfabetización cívica en las comunidades corporativas. Es un buen ejemplo de la amplitud de oportunidades para fortalecer nuestras defensas democráticas.

Interrumpir

En los últimos años, la Unidad de delitos digitales (DCU) de Microsoft ha perfeccionado las tácticas y ha desarrollado herramientas para desestabilizar ciberamenazas que abarcan desde ransomware a botnets y ataques de los estados nación. Hemos aprendido muchas lecciones importantes, empezando por el papel de la disrupción activa en la lucha contra un amplio conjunto de ciberataques.

Cuando pensamos en contrarrestar las operaciones de ciberinfluencia, la disrupción podría desempeñar un papel aún más importante y el mejor enfoque para la disrupción es cada vez más evidente. El antídoto más eficaz contra el engaño generalizado es la transparencia. Es por eso por lo que Microsoft aumentó su capacidad de detectar e interrumpir las operaciones de influencia de los estados nación mediante la adquisición de Miburo Solutions, una empresa líder en análisis e investigación de amenazas cibernéticas especializada en la detección y respuesta a las operaciones de ciberinfluencia extranjeras.

Nuestra experiencia ha demostrado que los gobiernos, las empresas de tecnología y las ONG deben atribuir los ciberataques con sumo cuidado y con pruebas abundantes. Conocer el impacto de tal disrupción es vital y puede ser aún más útil para destruir la ciberinfluencia. Hemos sido testigos del intercambio de información por parte del gobierno de los Estados Unidos en el período previo de la invasión rusa de Ucrania, que se materializó en medidas efectivas, como la exposición de los planes rusos, incluidas campañas concretas como un complot para usar un vídeo gráfico falso.

Tal como se mostró en la publicación del verano pasado del CyberPeace Institute de Ginebra sobre los ciberataques en curso dentro y fuera de Ucrania, un conjunto más amplio de la sociedad civil y organizaciones del sector privado tienen la oportunidad de promover la transparencia en relación con las operaciones de ciberinfluencia. Los informes fiables sobre las operaciones recién descubiertas y bien documentadas pueden ayudar al público a evaluar mejor lo que lee, ve y escucha, especialmente en Internet. A tal efecto, Microsoft ampliará sus informes cibernéticos existentes y publicará nuevos informes, datos y actualizaciones relacionados con lo que descubramos sobre las operaciones de ciberinfluencia, incluida la designación de atribuciones cuando corresponda. Publicaremos un informe anual que utilizará un enfoque basado en datos para buscar en toda la empresa la prevalencia de las operaciones de información extranjera y los siguientes pasos para garantizar una mejora incremental. También consideraremos la posibilidad de añadir nuevas medidas que se basen en este tipo de transparencia.

El papel de la publicidad digital es especialmente importante, por ejemplo, ya que la publicidad puede ayudar a financiar operaciones extranjeras y a crear una apariencia de legitimidad para sitios propagandísticos patrocinados por naciones extranjeras. Serán necesarios nuevos esfuerzos para desmantelar estos flujos financieros.

Disuadir

Por último, no podemos esperar que las naciones cambien su comportamiento si no se las responsabiliza por incumplir las normas internacionales. Exigir esta rendición de cuentas es una responsabilidad exclusivamente gubernamental. Sin embargo, cada vez más, la acción multilateral está desempeñando un papel importante en el fortalecimiento y la ampliación de las normas internacionales. Más de 30 plataformas online, anunciantes y editores, incluido Microsoft, firmaron el código de práctica sobre desinformación de la Comisión Europea, recientemente actualizado, que establece un mayor compromiso para hacer frente a este creciente desafío. Al igual que el reciente Acuerdo de París, la Cumbre de Christchurch y la Declaración sobre el Futuro de Internet, la acción multilateral y multisectorial puede reunir a los gobiernos y al público de las naciones democráticas. Los gobiernos pueden basarse en estas normas y leyes para hacer avanzar la rendición de cuentas que las democracias del mundo necesitan y merecen.

A través de una transparencia rápida y radical, los gobiernos y las sociedades democráticos pueden amortiguar de manera eficaz las campañas de influencia atribuyendo la fuente de los ataques de estados nación, informando al público y generando confianza en las instituciones.

> Hemos aumentado la capacidad técnica para detectar y desmantelar las operaciones de influencia extranjera y tenemos el compromiso de informar de forma transparente sobre estas operaciones como hacemos en nuestros informes sobre ciberataques.

Conocimientos prácticos

1. Implementa prácticas de higiene digital robustas en toda la organización.
2. Piensa en formas de reducir la habilitación no intencionada de campañas de ciberinfluencia por parte de tus empleados o tus prácticas empresariales. Esto incluye la reducción de la oferta a sitios de propaganda extranjeros conocidos.
3. Apoya la alfabetización en información y las campañas de participación ciudadana como un componente clave para ayudar a las sociedades a defenderse de la propaganda y la influencia extranjera.
4. Trabaja directamente con grupos relevantes para tu sector encargados de abordar las operaciones de influencia.

Notas al pie

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. Defensa de Ucrania: lecciones tempranas de la guerra cibernética (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. La portavoz del Ministerio de Asuntos Exteriores ruso, Maria Zakharova: https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Afirmaciones rusas sobre Kremenchuk contrarias a las pruebas: bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Comprobación de hechos: El vídeo de Nancy Pelosi «borracha» se ha manipulado | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Resultados de la competición de detección de «deepfakes»: una iniciativa abierta para impulsar la IA (facebook.com)
20. Deepfakes 2020: The Tipping Point, Johannes Tammekänd, John Thomas y Kristjan Peterson, octubre de 2020

Ciberresiliencia

Conocer los riesgos y los beneficios de la modernización es crucial para un enfoque de resiliencia integral.

Información general sobre la

ciberresiliencia

La ciberseguridad es un factor clave del éxito tecnológico. La innovación y la mejora de la productividad solo se pueden lograr introduciendo medidas de seguridad que aumenten todo lo posible la resiliencia de las organizaciones a los ataques modernos.

La pandemia ha obligado a cambiar las prácticas y tecnologías de seguridad para proteger a los empleados de Microsoft dondequiera que trabajen. Durante este último año, los actores de amenazas continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido gestionar la prevalencia y complejidad de los diversos métodos de ataque y el aumento de la actividad de los estados nación.

La resiliencia cibernética eficaz requiere un enfoque holístico y adaptable para resistir las amenazas en evolución a los servicios e infraestructuras básicos.

Más información en la página 89

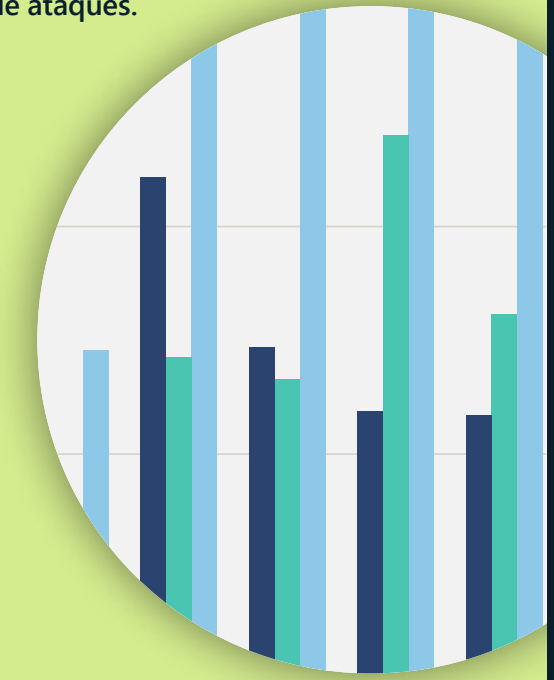
Los sistemas y la arquitectura modernizados son importantes para gestionar las amenazas en un mundo hiperconectado.

Más información en la página 90

La posición básica de seguridad es un factor determinante en la eficacia de las soluciones avanzadas

Más información en la página 92

Aunque los ataques basados en contraseñas siguen siendo la principal fuente de compromiso de identidad, están apareciendo otros tipos de ataques.



Más información en la página 93

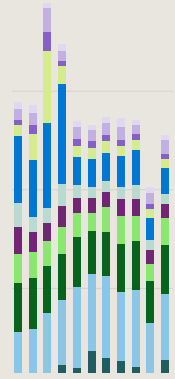
La dimensión humana de la resiliencia a las operaciones de ciberinfluencia es nuestra capacidad de colaborar y cooperar.

Más información en la página 102

La gran mayoría de los ciberataques que han tenido éxito podría haberse evitado con una higiene de seguridad básica.

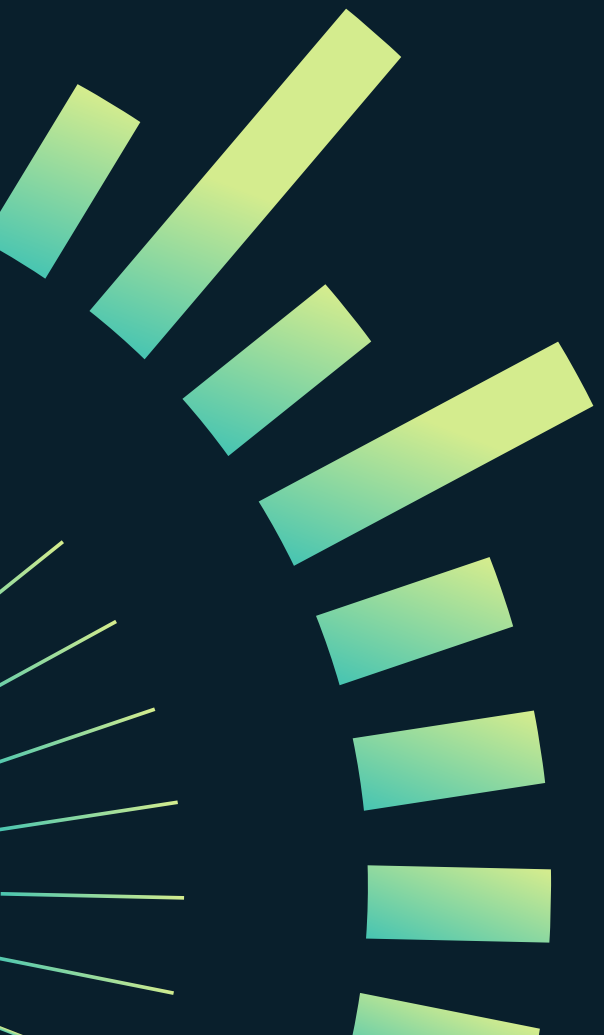
Más información en la página 108

Durante el año pasado, el mundo experimentó una actividad de DDoS sin precedentes en volumen, complejidad y frecuencia.



Más información en la página 98

Introducción



La pandemia ha obligado a cambiar las prácticas y tecnologías de seguridad para proteger a los empleados de Microsoft dondequiera que trabajen. Durante este último año, los actores de amenazas continuaron aprovechando las vulnerabilidades expuestas durante la pandemia y el cambio a un entorno de trabajo híbrido. Desde entonces, nuestro principal desafío ha sido gestionar la prevalencia y complejidad de los diversos métodos de ataque y el aumento de la actividad de los estados nación.

La actividad de amenazas digitales y el grado de sofisticación de las ciberamenazas aumentan cada día. Muchos de los ataques complejos de hoy en día se centran en poner en peligro las arquitecturas de identidad, las cadenas de suministro y terceros con distintos grados de controles de seguridad. En particular, hemos observado que los ataques de phishing de identidad son una amenaza clara y presente. Sin embargo, estos tipos de ataques no suelen tener éxito gracias a las buenas prácticas de administración de identidades, control de phishing y administración de puntos de conexión. Por tanto, debemos recordar lo básico: el 98 % de los ataques se puede detener con la implantación de medidas de higiene básicas. En Microsoft, administramos las identidades y los dispositivos como parte de nuestro enfoque de Confianza cero, que incluye el acceso con privilegios mínimos y credenciales resistentes al phishing para detener eficazmente a los atacantes y mantener nuestros datos protegidos.

Hoy en día, incluso los actores de amenazas que carecen de conocimientos técnicos sofisticados pueden lanzar ataques increíblemente destructivos, a medida que aumenta el acceso a tácticas, técnicas y procedimientos avanzados en la economía de la ciberdelincuencia. La guerra de Ucrania demostró cómo los agentes de los estados nación han escalado sus operaciones cibernéticas ofensivas mediante el aumento del uso de ransomware. El ransomware es ahora un sector sofisticado con actores de amenazas que utilizan tácticas de extorsión doble o triple para conseguir un pago y con desarrolladores que ofrecen ransomware como servicio (RaaS). Con RaaS, los atacantes utilizan una red afiliada para perpetrar los ataques, lo que reduce la barrera de entrada para los ciberdelincuentes menos cualificados y, en última instancia, amplía el grupo de atacantes.

Por ello, Microsoft ha diseñado un programa de eliminación de ransomware. El objetivo del programa es corregir las brechas de control y cobertura, contribuir a las mejoras de las características de los servicios y desarrollar manuales de recuperación para nuestro centro de operaciones de seguridad y equipos de ingeniería en caso de que se produzca un ataque de ransomware.

Los ataques recientes a la cadena de suministro y de proveedores externos indican un importante punto de inflexión en el sector. La disrupción que estos ataques causan a nuestros clientes, partners, gobiernos y Microsoft sigue aumentando, lo que ilustra la importancia de centrar la atención en la ciberresiliencia y la colaboración entre las partes interesadas de seguridad. Los adversarios también están atacando los sistemas on-premises, lo que refuerza la necesidad de que las organizaciones administren las vulnerabilidades que suponen los sistemas heredados mediante la modernización y la migración de la infraestructura al cloud, donde la seguridad es más robusta.

Vivimos en una época en la que la seguridad es un factor clave para el éxito tecnológico. La innovación y la mejora de la productividad solo se pueden lograr introduciendo medidas de seguridad que aumenten todo lo posible la resiliencia de las organizaciones a los ataques modernos. A medida que las amenazas digitales se incrementan y evolucionan, es crucial crear ciberresiliencia en el tejido de todas las organizaciones.

Bret Arsenault
Director de seguridad de la información

Ciberresiliencia: un aspecto fundamental de una sociedad conectada

La revolución de la tecnología digital ha hecho que las organizaciones se transformen para estar cada vez más conectadas tanto en la forma de operar como en los servicios que ofrecen. A medida que aumentan las amenazas en el panorama cibernético, la creación de ciberresiliencia en el tejido de la organización es tan crucial como la resiliencia financiera y operativa.

La transformación digital ha alterado para siempre la forma en que las organizaciones interactúan con los clientes, partners, empleados y otras partes interesadas. Las nuevas tecnologías ofrecen enormes oportunidades de interactuar con las personas, transformar los productos y optimizar las operaciones. La pandemia aceleró la transformación digital impulsando tecnologías innovadoras que permiten a las personas colaborar de nuevas formas y desde cualquier lugar.

A medida que las ciberamenazas se vuelven endémicas, evitar que pongan en peligro a una organización se vuelve más difícil en nuestro mundo «siempre conectado». La ciberresiliencia representa la capacidad de una organización para continuar las operaciones y mantener la aceleración del crecimiento a pesar del aluvión de ataques. La prevención debe equilibrarse con la capacidad de supervivencia y recuperación, y los gobiernos y las empresas están desarrollando modelos integrales que van más allá de la seguridad y la privacidad para proteger activos, datos y otros recursos como parte de la ciberresiliencia.

Desarrollar un enfoque de ciberresiliencia integral

La ciberresiliencia eficaz requiere un enfoque holístico, adaptable y global que pueda resistir las amenazas en evolución a los servicios e infraestructuras básicos, e incluye:

- Una higiene cibernética básica, tal como se describe en nuestra curva en campana de ciberresiliencia.
- Conocer y gestionar el equilibrio entre los riesgos y las recompensas de la transformación digital.
- Funcionalidades de respuesta en tiempo real que permitan la detección proactiva de amenazas y vulnerabilidades.
- La protección contra ataques conocidos y actividad preventiva contra vectores de ataque nuevos y esperados, incluida la capacidad de corrección automática.
- Reducción del impacto de los ataques y desastres mediante el aislamiento de errores y la segmentación.
- Recuperación y redundancia automatizadas en caso de interrupción.
- Priorizar las pruebas operativas para encontrar deficiencias y conocer las responsabilidades compartidas y las dependencias de los recursos externos, como las soluciones de seguridad basadas en el cloud.

Un programa efectivo de ciberresiliencia comienza con fundamentos de los recursos, como conocer los servicios disponibles y disponer de un catálogo fiable de recursos que se puedan recuperar en caso de disrupción. Sobre esa base, el programa debe ser capaz de evaluar su propia eficacia, medir el rendimiento de los servicios críticos y sus dependencias, probar y validar las capacidades en los servicios on-premises y en el cloud, y promover la mejora continua en todo el ciclo de vida digital de la organización.

Con el fin de ofrecer un enfoque integral, nos hemos asociado con organizaciones para identificar sus servicios on-premises y online más críticos, procesos de negocio, dependencias, personal, distribuidores y proveedores. También buscamos identificar los activos y recursos asociados con las expectativas del cliente y del mercado, las obligaciones normativas y contractuales y las operaciones internas. A medida que se identifican estos recursos críticos, se deben detectar y supervisar las amenazas, las disrupciones, los potenciales vectores de ataque y las vulnerabilidades del sistema y el proceso mediante esfuerzos paralelos. La capacidad de hacer esto ante la escasez actual de conocimientos exige rigurosidad en la definición de prioridades en función del riesgo global que representa para la organización.

Este tipo de enfoque integral debe ser adaptable en un telón de fondo donde las amenazas no paran de evolucionar, con el objetivo de impulsar una mejora del rendimiento cuantificable, un menor tiempo para detectar, responder y recuperarse, y un menor radio de impacto en caso de disrupción. El enfoque también debe reconocer la creciente conexión de las amenazas. Por ejemplo, un incidente de seguridad podría dar lugar a una filtración de datos con implicaciones para la privacidad, lo que requeriría que muchos equipos internos y externos trabajaran juntos para responder rápidamente y minimizar el impacto.

La ciberresiliencia es la capacidad de una empresa de seguir operando y de mantener la aceleración del crecimiento a pesar de las disrupciones, incluidos los ciberataques.

Conocimientos prácticos

1. Crea y administra sistemas tecnológicos que limiten el impacto de una infracción y puedan seguir funcionando de forma segura y eficaz, incluso si se produce una infracción. Céntrate en activos críticos comunes, soporte para la agilidad y arquitectura para la adaptabilidad (por ejemplo, entornos híbridos y multicloud multiplataforma), reduce las superficies de ataque (por ejemplo, elimina las aplicaciones no utilizadas y los derechos de acceso sobreaprovisionados), da por hecho que se va a producir un ataque a los recursos y da por sentado que los adversarios mejorarán sus tácticas.
2. Al planificar proyectos digitales, ten en cuenta las amenazas potenciales junto con las oportunidades y las responsabilidades compartidas de resiliencia en toda la cadena de suministro de la tecnología digital, incluidas las soluciones de seguridad basadas en el cloud.
3. Crea sistemas para integrar la seguridad por diseño y toma medidas para prever, detectar, resistir, adaptarte y responder a las amenazas en evolución futuras.
4. Asegúrate de que los directivos de la empresa trabajen con los equipos de seguridad según sea necesario para conocer los riesgos asociados con nuevos desarrollos. Del mismo modo, los equipos de seguridad deben tener en cuenta los objetivos empresariales y asesorar a los directivos sobre cómo perseguirlos de forma segura.
5. Garantiza la existencia de prácticas operativas y procedimientos claros para la resiliencia de la organización en caso de ciberataques.

La importancia de modernizar los sistemas y la arquitectura

A medida que desarrollamos nuevas capacidades para un mundo hiperconectado, debemos gestionar las amenazas que entrañan los sistemas y el software heredados.

Los sistemas heredados, es decir, los que se desarrollaron antes de que se generaliza el uso de las herramientas de conectividad modernas, como smartphones, tablets y servicios en el cloud, representan un riesgo para la organización que los sigue utilizando. Esta exposición al riesgo se ve reforzada por los hallazgos del equipo de Microsoft Security Services for Incident Response, un grupo de profesionales de seguridad que ayuda a los clientes a responder a los ataques y recuperarse de ellos.

El año pasado, los problemas detectados de los clientes que se recuperaban de ataques estaban relacionados con seis categorías, mostradas en la tabla de esta página. En la página siguiente se describen los pasos que se pueden tomar para mejorar la resiliencia.

Más del 80 por ciento de los incidentes de seguridad se pueden rastrear hasta la identificación de algunos elementos inexistentes, que se pueden abordar con enfoques de seguridad modernos.

Aspectos clave que afectan a la ciberresiliencia

En esta tabla se muestra el porcentaje de clientes afectados que carecían de controles de seguridad básicos, que son fundamentales para aumentar la ciberresiliencia de la organización. Los resultados se basan en las interacciones de Microsoft con los clientes en el último año.

«Los directivos deben considerar la ciberresiliencia una faceta crítica de la resiliencia empresarial. Deben planificar las disrupciones cibernéticas de la misma manera que lo hacen con los desastres naturales u otros sucesos imprevistos, y reunir a las partes interesadas internas, como operaciones, comunicaciones, departamento jurídico, etc., para elaborar estrategias. Esto ayudará a garantizar que las organizaciones vuelvan a poner en funcionamiento sus sistemas empresariales críticos lo antes posible para reanudar las operaciones normales del negocio.

Pero eso no es todo. Como muchas organizaciones confían en proveedores externos y proveedores de servicios, los directivos deben aplicar los planes de ciberresiliencia cibernética a toda su cadena de valor para garantizar aún más la continuidad del negocio y la resiliencia».

Ann Johnson,
Vicepresidenta corporativa de seguridad, cumplimiento, identidad y desarrollo empresarial de gestión

La importancia de modernizar los sistemas y la arquitectura

Continuación

Hay áreas claras que las organizaciones pueden abordar para modernizar su enfoque y protegerse de las amenazas:

Problema	Medidas
Configuración poco segura del proveedor de identidades La configuración errónea y la exposición de las plataformas de identidad y sus componentes son un vector común para obtener acceso no autorizado con privilegios elevados.	Sigue las referencias de configuración de seguridad y las prácticas recomendadas al implementar y mantener sistemas de identidad como la infraestructura de AD y Azure AD. Implementa restricciones de acceso aplicando la segregación de privilegios y el acceso con privilegios mínimos, y utilizando estaciones de trabajo de acceso con privilegios (PAW) para administrar sistemas de identidad.
Controles de acceso con privilegios y movimiento lateral insuficientes Los administradores tienen permisos excesivos en todo el entorno digital y suelen exponer las credenciales administrativas en estaciones de trabajo vulnerables a riesgos de Internet y de productividad.	Protege y limita el acceso administrativo para aumentar la resiliencia del entorno y limitar el alcance de un ataque. Emplea controles de administración de acceso con privilegios, como el acceso «just-in-time» y la administración «just enough».
Sin autenticación multifactor (MFA) Los atacantes actuales no entran empleando la fuerza: simplemente inician sesión.	MFA es un control de acceso de los usuarios fundamental y esencial que todas las organizaciones deben habilitar. Combinada con el acceso condicional, MFA puede ser de un valor incalculable en la lucha contra las ciberamenazas.
Operaciones de seguridad poco maduras La mayoría de las organizaciones afectadas utilizaban herramientas tradicionales de detección de amenazas y no tenían información relevante para la respuesta y la corrección oportunas.	Una estrategia integral de detección de amenazas requiere inversiones en la detección y respuesta extendidas (XDR) y en herramientas nativas del cloud modernas que empleen el machine learning para separar el ruido de las señales. Moderniza las herramientas de operaciones de seguridad incorporando XDR, que puede proporcionar amplios conocimientos de seguridad en todo el panorama digital.
Falta de control de protección de la información A las organizaciones le sigue resultando difícil crear controles integrales de protección de la información que tengan cobertura plena en todas las ubicaciones de datos, sigan siendo eficaces a lo largo del ciclo de vida de la información y concuerden con la importancia crítica de los datos para el negocio.	Identifica tus datos empresariales críticos y dónde se encuentran. Revisa los procesos del ciclo de vida de la información y aplica la protección de los datos garantizando al mismo tiempo la continuidad del negocio.
Adopción limitada de marcos de seguridad modernos La identidad es el nuevo perímetro de seguridad que permite el acceso a servicios digitales y entornos informáticos dispares. La integración de principios de Confianza cero, la seguridad de las aplicaciones y otros marcos cibernéticos modernos permiten a las organizaciones gestionar proactivamente los riesgos que, de no existir, no serían fácilmente identificables por las organizaciones.	Los marcos de Confianza cero imponen conceptos de privilegios mínimos, aplican la verificación explícita de todo el acceso y siempre presuponen que se va a producir un ataque. Las organizaciones también deben implementar controles y prácticas de seguridad en DevOps y en los procesos del ciclo de vida de las aplicaciones para obtener mayores garantías de sus sistemas empresariales.

La posición básica de seguridad es un factor determinante en la eficacia de las soluciones avanzadas

En nuestro análisis, descubrimos la prevalencia de puntos ciegos comunes en las defensas organizativas que permiten a los atacantes obtener acceso inicial, establecer un punto de apoyo y perpetrar un ataque, incluso en presencia de soluciones de seguridad avanzadas.

En muchos casos, el resultado de un ciberataque está determinado mucho antes de que comience. Los atacantes aprovechan los entornos vulnerables para obtener acceso inicial, realizar operaciones de vigilancia y hacer estragos a través del movimiento lateral y el cifrado o la filtración. Detener a un atacante en una etapa temprana aumenta enormemente la oportunidad de reducir el impacto general.

Microsoft ha estudiado configuraciones específicas en las posturas de seguridad para identificar las deficiencias más comunes en la práctica real en estos entornos. Esto nos ha permitido ver las vulnerabilidades más comunes atacadas durante ataques de ransomware operados por humanos que permitieron a los actores de amenazas obtener acceso y viajar a través de una red sin ser detectados.

Las configuraciones de seguridad básicas deben estar activadas

Los dispositivos de una organización que no están inscritos o están obsoletos (tanto en relación con las vulnerabilidades como con el estado de los agentes de seguridad) sirven como posibles puntos de entrada y rutas de establecimiento de acceso para los atacantes. Hemos descubierto que, aunque garantizar que los dispositivos de la organización estén integrados con una solución actualizada de detección y respuesta de puntos de conexión[1] (EDR) y una plataforma de protección de puntos de conexión[2] (EPP) es un paso importante, no está garantizado que se detenga el ransomware.

Las soluciones avanzadas como EDR y EPP son fundamentales para detectar a un atacante en las primeras etapas del flujo de ataque y para permitir la corrección y protección automáticas. Sin embargo, dado que estas soluciones avanzadas se basan en una capacidad fundamental para detectar un ataque, requieren que se activen las configuraciones de seguridad básicas. De hecho, hemos observado una prevalencia de escenarios con soluciones avanzadas implementadas que se vieron socavados por la ausencia de configuraciones de seguridad básicas.

Las prácticas recomendadas de configuraciones de seguridad son un mayor indicador de resiliencia que el tiempo de respuesta de los analistas del centro de operaciones de seguridad (SOC)

Hemos observado una reducción del 70 % en el tiempo que un analista del SOC tarda en ver y actuar ante una alerta relevante durante un período de seis meses en nuestra población de clientes y partners. Esta mayor capacidad de reacción es una buena señal. Sin embargo, aunque la visibilidad de la configuración de seguridad mejoró el rendimiento de los analistas del SOC, permitir la visibilidad de los productos mediante la incorporación y actualización de los dispositivos de la organización fue un mayor indicador del éxito de la prevención.

Riesgo introducido por los dispositivos desconocidos

A diferencia de las redes en el cloud, donde los clientes saben qué activos se ejecutan y en qué sistemas operativos, las redes on-premises pueden contener una amplia variedad de dispositivos como IoT, escritorios, servidores y dispositivos de red que no están supervisados ni administrados por la organización.

La red empresarial media tiene más de 3500 dispositivos conectados que no están protegidos por un agente de EDR y pueden tener acceso a recursos empresariales o incluso a activos de alto valor. Microsoft Defender para punto de conexión (MDE) utiliza la inspección de red para detectar dispositivos y proporcionar información sobre la clasificación de dispositivos para aquellos conectados a la red como el nombre del dispositivo, la distribución del sistema operativo y el tipo de dispositivo.

3500

número medio de dispositivos conectados en una empresa que no están protegidos por un agente de detección y respuesta de puntos de conexión.

En el caso de los dispositivos que no admiten un agente de EDR, al menos debes conocer su existencia y actuar para protegerlos evaluando las vulnerabilidades, así como restringiendo el acceso a la red.

Conocimientos prácticos

1. Incluso las soluciones avanzadas pueden dejar de ser eficaces si no existen configuraciones de seguridad básicas.
2. Invierte en prácticas recomendadas sobre configuraciones de posición de seguridad para protegerte de ataques futuros. Estos ajustes básicos producen un inmenso retorno de la inversión en cuanto a la capacidad de una organización para defenderse de los ataques.
3. Incorpora todos los dispositivos aplicables a una solución EDR.
4. Asegúrate de actualizar los agentes de seguridad y de garantizar la protección contra la manipulación para permitir una mayor visibilidad y obtener beneficios más completos de la protección de los productos.

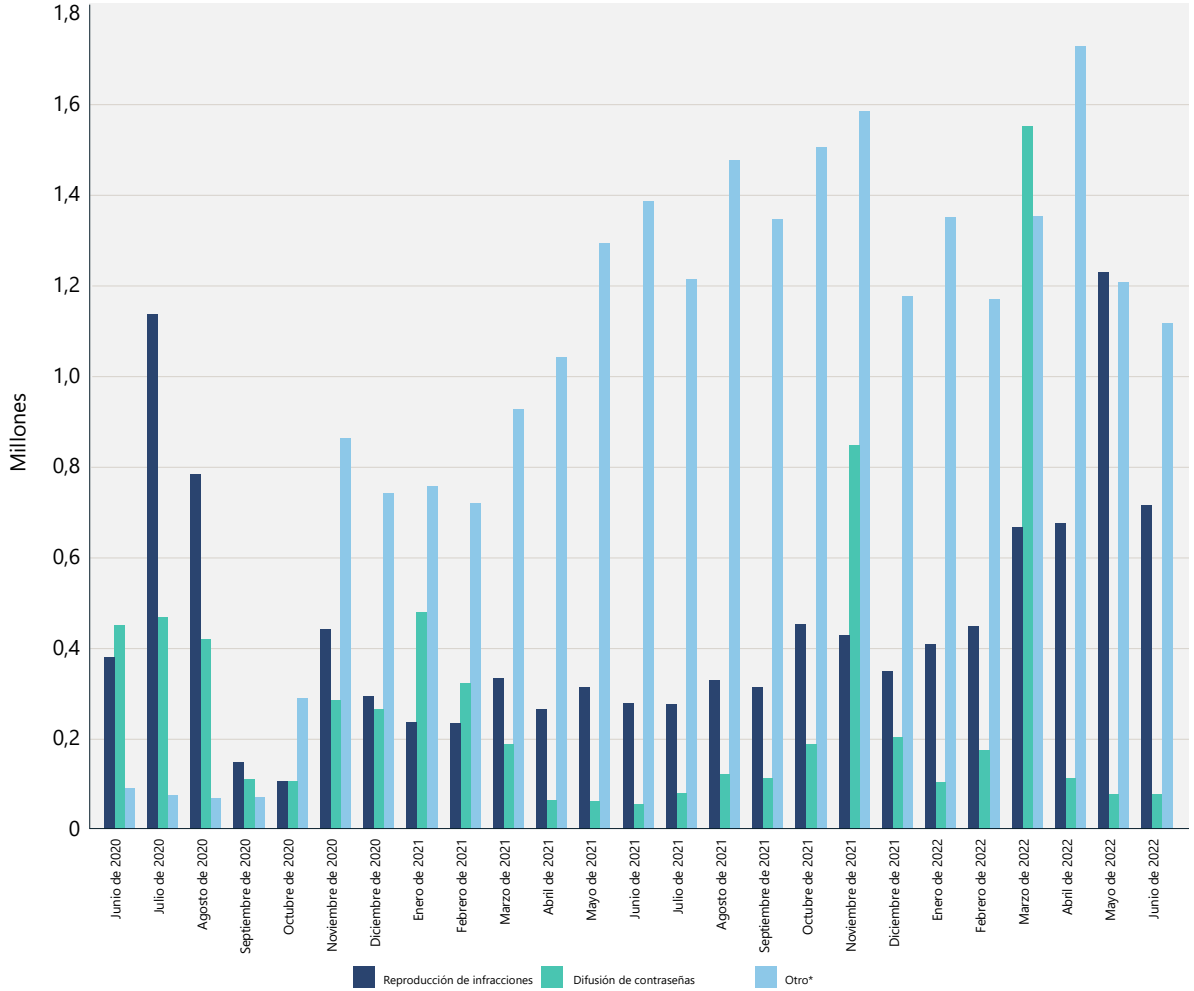
Mantener la salud de la identidad es fundamental para el bienestar de las organizaciones

Proteger la identidad es más importante que nunca. Aunque los ataques basados en contraseñas siguen siendo la principal fuente de ataques de identidad, están apareciendo otros tipos de ataques. El volumen de ataques sofisticados sigue aumentando con respecto a los ataques anteriores de «password spray» y reproducción de vulnerabilidades.

Los ataques basados en contraseñas siguen siendo habituales y más del 90 por ciento de las cuentas atacadas mediante estos métodos no están protegidas con una autenticación segura. La autenticación segura utiliza más de un factor de autenticación, como contraseña + SMS y claves de seguridad FIDO2.

Hemos visto un aumento de los ataques dirigidos de «password spray», con picos muy grandes en el volumen de tráfico de los atacantes repartidos por miles de direcciones IP.

Usuarios atacados por tipo de ataque



Usuarios atacados al mes por tipo de ataque. Los volúmenes de ataques de «password spray» fueron muy volátiles, como se observó en los picos de noviembre de 2021 y marzo de 2022. Estos picos representan miles de usuarios y miles de direcciones IP afectados. * «Otro» indica ataques diferentes a los de «password spray» y reproducción de vulneraciones, incluidos phishing, malware, «man-in-the-middle», ataques a los emisores de tokens on-premises y otros. Fuente: Azure AD Identity Protection.

4500

En el tiempo que se tarda en leer esta frase, nos hemos defendido de 4500 ataques de contraseñas.

Mantener la salud de la identidad es fundamental para el bienestar de las organizaciones

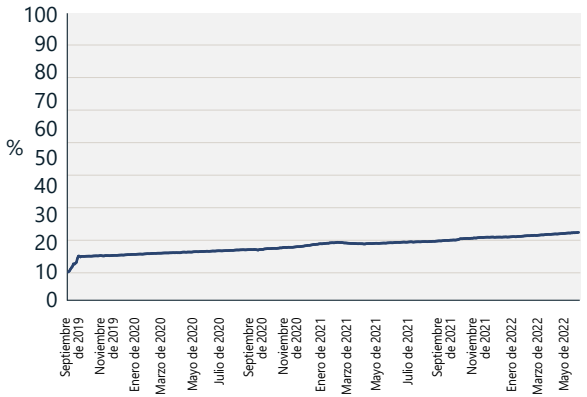
Continuación

Adopción de una autenticación segura

Como dato positivo, estamos observando un crecimiento constante en la adopción de una autenticación robusta entre la base de clientes empresariales de Azure Active Directory (Azure AD). En Azure AD, los usuarios activos mensuales (UAM) de autenticación segura crecieron del 19 al 26 por ciento el año pasado, mientras que los UAM de autenticación segura para cuentas administrativas crecieron del 30 al 33 por ciento aproximadamente.

Esta tendencia es positiva, pero aún se necesita crecer mucho para alcanzar una cobertura mayoritaria de autenticación segura; los clientes que no utilizan todavía la autenticación segura en sus entornos deben empezar a planificarla e implementarla para proteger a sus usuarios.[3] Al diseñar una implementación de autenticación segura, la autenticación sin contraseñas debe considerarse la experiencia más segura que se puede usar, ya que elimina el riesgo de ataques de contraseña.

Uso de la autenticación segura
(septiembre de 2019-mayo de 2022)

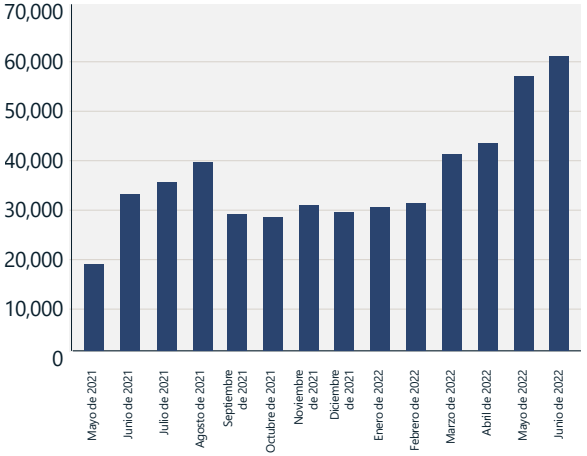


Aunque el uso de la autenticación segura se ha duplicado desde 2019, solo el 26 % de los usuarios y el 33 % de los administradores la utilizan. Fuente: Azure Active Directory.

Aumento constante de los ataques de reproducción de tokens

El porcentaje de otras formas de ataque aumentó en 2022. Hemos visto un aumento de los ataques dirigidos que eludían específicamente la autenticación basada en contraseñas para reducir las posibilidades de detección. Estos ataques aprovechan las cookies de inicio de sesión único (SSO) del navegador o los tokens de actualización obtenidos a través de malware, phishing y otros métodos. En algunos casos, los atacantes eligen una infraestructura en una ubicación cercana al lugar geográfico del usuario objetivo para reducir aún más las posibilidades de detección. Hemos visto un aumento constante de los ataques de reproducción de tokens, con más de 40 000 detecciones al mes en Azure AD Identity Protection. La reproducción de tokens es el uso de tokens emitidos a un usuario legítimo por un atacante que está en posesión de estos tokens. Normalmente, los tokens se obtienen mediante malware, por ejemplo, filtrando las cookies del navegador del usuario o mediante métodos de phishing avanzados.

Volumen de ataques de reproducción de tokens detectados



Ataques de reproducción de tokens detectados al mes. Fuente: Azure AD Identity Protection, sesiones únicas identificadas por la detección de tokens anómalos.

Mantener la salud de la identidad es fundamental para el bienestar de las organizaciones

Continuación

Extracción de tokens

Más que malware, los atacantes necesitan credenciales para lograr sus objetivos. De hecho, el 100 % de todos los ataques de ransomware operados por humanos incluye credenciales robadas. Muchas intrusiones sofisticadas incluyen credenciales compradas en la «dark web», robadas inicialmente con malware de robo de credenciales no sofisticado y ampliamente distribuido. Este tipo de malware ha evolucionado para robar tokens, incluida la información de la sesión y las notificaciones de MFA. Esto significa que las infecciones en los sistemas domésticos, en los que los usuarios inician sesión en activos corporativos, pueden provocar incidentes graves en las redes corporativas.

Los atacantes también pueden extraer tokens de los dispositivos de las víctimas a través de ataques «man-in-the-middle», en los que la víctima hace clic en un enlace malintencionado incluido en un correo electrónico de phishing o en un mensaje instantáneo y se dirige a un sitio web que simula la página de inicio de sesión legítima del proveedor de identidad. En realidad, es un servicio web desarrollado por el atacante que transmite e intercepta todo el tráfico entre el usuario y el proveedor de identidad. El atacante puede interceptar el nombre de usuario y la contraseña, y también reproducir las preguntas de acceso de MFA; los tokens resultantes emitidos por el proveedor de identidad e interceptados por el atacante pueden contener notificaciones de MFA que el atacante puede utilizar para satisfacer los requisitos de MFA.

Microsoft Defender for Cloud Apps ha detectado un promedio de 895 estos ataques al mes desde principios de 2022. Esta forma de ataque se puede evitar mediante factores resistentes al phishing de MFA, como la autenticación basada en certificados, Windows Hello para empresas o claves de seguridad FIDO2.

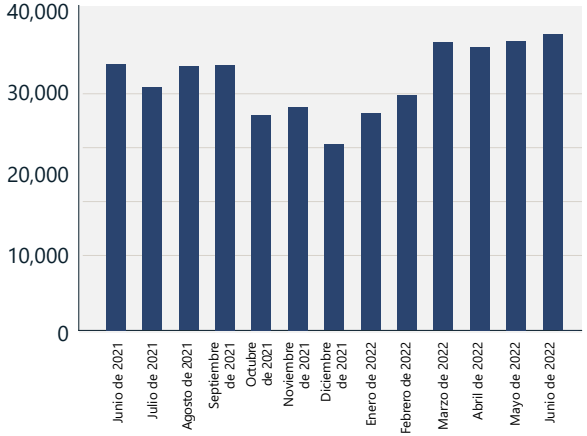
Los ataques basados en contraseñas son el método principal de ataque a las cuentas.

Fatiga de MFA

Usando el concepto de «fatiga de MFA», los atacantes generan múltiples solicitudes de MFA en el dispositivo de la víctima, con la esperanza de que la víctima acepte la solicitud involuntariamente o como resultado del agotamiento. Este ataque se puede prevenir mediante el uso de aplicaciones modernas de autenticación como Microsoft Authenticator, combinadas con características como la correspondencia numérica[4] y la habilitación de contexto adicional.[5] Azure AD Identity Protection calcula que hay 30 000 ataques por fatiga de MFA al mes.

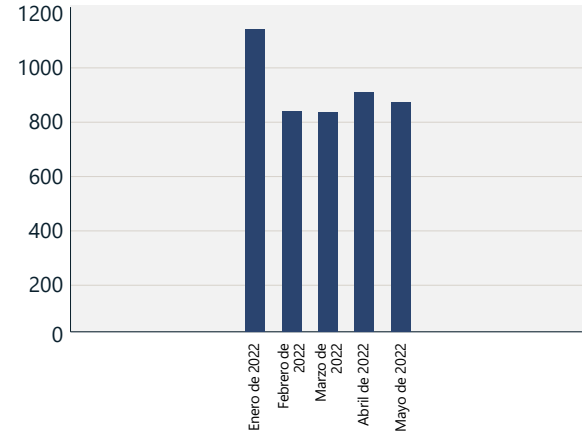
El porcentaje de ataques avanzados sigue aumentando, lo que subraya la necesidad de usar los factores resistentes al phishing de la autenticación multifactor.

Casos estimados de ataques por fatiga de MFA



Fuente: Azure AD Identity Protection.

Casos detectados de phishing seguidos de ataques «man-in-the-middle»



Fuente: Microsoft Defender for Cloud Apps.

Conocimientos prácticos

1. Asegúrate de que todas las cuentas de tu organización estén protegidas con medidas de autenticación robustas.
2. La autenticación sin contraseña ofrece la experiencia más segura y fácil de usar, ya que elimina el riesgo de ataques de contraseña.
3. Deshabilita la autenticación heredada en toda la organización.
4. Protege las cuentas administrativas y de alto valor con formas resistentes al phishing de autenticación segura.
5. Cambia de un proveedor de identidad on-premises a un proveedor de identidad en el cloud y conecta todas las aplicaciones con el proveedor de identidad basado en el cloud para disfrutar de una experiencia de usuario y una seguridad coherentes.

Enlaces a información adicional (pueden estar en inglés)

- En este Día Mundial de las Contraseñas, considera la posibilidad de abandonar por completo las contraseñas | Seguridad de Microsoft

Configuración de seguridad predeterminada del sistema operativo

Con el panorama de amenazas de seguridad en constante evolución, vemos una creciente necesidad de medidas de seguridad informática configuradas de forma predeterminada para mejorar la ciberresiliencia. Aunque la seguridad del sistema operativo es más urgente, compleja y esencial para el negocio que nunca, puede ser difícil gestionarla.

En el pasado, la seguridad informática y de los dispositivos incluía características de seguridad integradas que el cliente o profesional de TI tenía que configurar para conseguir el nivel de seguridad deseado. Este enfoque ya no es suficiente, debido a que los atacantes utilizan herramientas más avanzadas de automatización, infraestructura en el cloud y tecnologías de acceso remoto para lograr sus objetivos. Ahora es fundamental que todas las capas de seguridad, desde el chip hasta el cloud, estén configuradas de forma predeterminada. Microsoft ha evolucionado para configurar la seguridad del sistema operativo Windows de forma predeterminada.[6]

Los clientes que adoptan la defensa en profundidad, incluida una posición de seguridad por capas, nuevas características de seguridad, parches y actualizaciones periódicas y coherentes, así como formación y conocimientos de seguridad para informar del phishing y otras estafas, pueden esperar menos malware.

Para simplificar la defensa en profundidad, Windows 11 tiene protecciones de hardware y software integradas y activadas de forma predeterminada, incluida la integridad de memoria, el arranque seguro y Módulo de plataforma segura 2.0. Los usuarios de Windows 10 en hardware compatible también pueden activar estas características en la aplicación Configuración de Windows o en el menú de las BIOS.

En los dispositivos más antiguos, por lo general, no suele haber una armonización tan clara de las técnicas de seguridad de hardware y software. En los dispositivos en los que la seguridad no está habilitada de forma predeterminada debe configurase manualmente en los ajustes siempre que sea posible.[7]

En los dispositivos en los que la seguridad no está habilitada de forma predeterminada, Microsoft recomienda configurarla manualmente en los ajustes siempre que sea posible.

Adopta una actitud proactiva a la vez que aplicas actualizaciones continuas del sistema operativo y parches de seguridad, que ayudan a proporcionar protección a lo largo del ciclo de vida del hardware y el software.

Conocimientos prácticos

1. Usa una solución sin contraseñas que enlace las credenciales de inicio de sesión del Módulo de plataforma segura. Busca específicamente una solución sin contraseña que cumpla el estándar del sector Faster Identity Online (FIDO) Alliance[8].
2. Realiza una limpieza puntual de todos los ejecutables no utilizados y obsoletos que estén en los dispositivos de la organización.
3. Protégete de los ataques avanzados del firmware habilitando la integridad de la memoria, el arranque seguro y Módulo de plataforma segura 2.0, si no están habilitados de forma predeterminada, para reforzar la seguridad del arranque con las funciones integradas en las CPU modernas.
4. Activa el cifrado de datos y la protección de credenciales.
5. Habilita controles de aplicación y navegador para una mejor protección frente a aplicaciones que no son de confianza y otras protecciones contra vulnerabilidades de seguridad integradas.
6. Habilita la protección de acceso a la memoria para ayudarte a protegerte de ataques físicos ocasionales, como cuando alguien conecta un dispositivo malintencionado a puertos de acceso externo.

Enlaces a información adicional (pueden estar en inglés)

- Libro de seguridad de Windows | Comercial
- Las nuevas características de seguridad de Windows 11 ayudarán a proteger el trabajo híbrido | Blog de seguridad de Microsoft

Centralización de la cadena de suministro de software

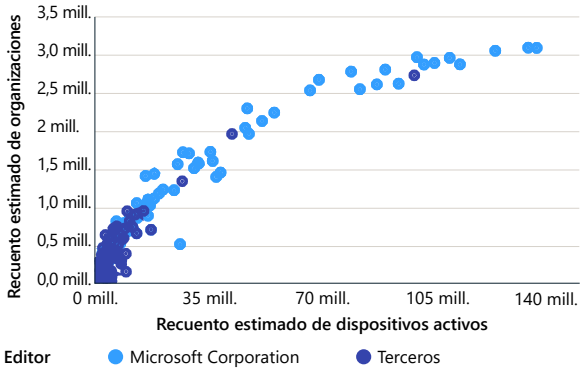
Los ataques a aplicaciones, complementos y extensiones de terceros pueden erosionar la confianza del cliente en los proveedores que desempeñan un papel central en el ecosistema de suministro. El uso de la teoría de redes para buscar la centralidad del software arroja luz sobre la importancia crítica de la aplicación de parches, especialmente para las aplicaciones centrales.

La Red de aplicaciones Windows cuenta con 18 millones de ejecutables de aplicaciones instalados y utilizados en cinco millones de organizaciones, lo que proporciona una perspectiva general de nuestro ecosistema de software. De las 100 000 aplicaciones más utilizadas, el 97 % las producen organizaciones de terceros quienes se encargan de mantener las actualizaciones y los parches de seguridad. Esto ilustra dos rasgos importantes de nuestro ecosistema de aplicaciones comerciales.

En primer lugar, el ecosistema de aplicaciones comerciales de Windows está centralizado. Solo las 100 000 aplicaciones principales (de los 18 millones) se utilizan en mil o más dispositivos. O dicho de otra forma, poco más de la mitad del 1 % de estas aplicaciones tienen este tipo de efecto de amplio alcance en el ecosistema de dispositivos.

En segundo lugar, existe diversidad en la capacidad de administración de esas aplicaciones, donde los 10 000 principales proveedores de aplicaciones administran las actualizaciones y los parches de seguridad de estas aplicaciones comerciales más utilizadas. Esto demuestra la interdependencia que tiene una empresa en un conjunto diverso de controles, cumplimiento y administración de la seguridad de los proveedores de software.

Penetración comercial de las aplicaciones más utilizadas



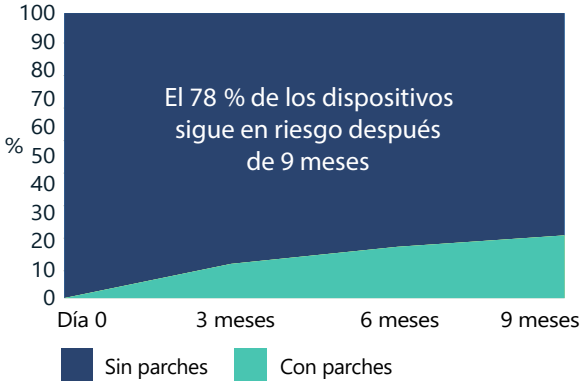
Millones de organizaciones y decenas de millones de dispositivos utilizan las aplicaciones principales. Debido a que son casi omnipresentes, los adversarios buscan constantemente aprovechar las vulnerabilidades de estas aplicaciones principales, lo que puede afectar a millones de dispositivos de la base de usuarios.

Observamos que millones de dispositivos comerciales siguen utilizando versiones de aplicaciones vulnerables muchos meses después de la publicación de parches o incluso años después del fin del soporte del producto. Por ejemplo, hay más de un millón de dispositivos comerciales Windows activos que ejecutan una versión de un lector de PDF que no recibe soporte desde 2017.

Las versiones antiguas de aplicaciones que no tienen soporte siguen usándose activamente en millones de dispositivos comerciales. Por consiguiente, las organizaciones corren el riesgo de tener vulnerabilidades no corregidas.

En el caso de las versiones de aplicaciones que reciben soporte, vemos un estancamiento de la velocidad de adopción de parches críticos, lo que contraviene la tendencia de aumentar la resiliencia. En lugar de ello, la curva debe mostrar una adopción exponencial de los parches mes tras mes para lograr la resiliencia necesaria.

Tasa de implementación de parches críticos



Tras examinar una vulnerabilidad crítica que afectó a 134 versiones de un conjunto de navegadores, descubrimos que el 78 por ciento, o millones de dispositivos, seguía utilizando una de las versiones afectadas nueve meses después de que se publicara el parche.

Utilizamos el kit de herramientas InterpretML[9] para identificar las características relacionadas con organizaciones que tienen más probabilidades de contar con dispositivos con versiones de aplicaciones más antiguas. Entre los indicadores más importantes se incluyen los siguientes: pocas horas de interacción en los dispositivos; áreas geográficas como Asia Pacífico y Latinoamérica; y sectores de la industria como la automoción, los productos químicos, las telecomunicaciones, el transporte y la logística, las mutuas (gestoras de siniestros) y los seguros.

El mantenimiento de la resiliencia del software debe incluir la desactivación o desinstalación periódica de las aplicaciones no utilizadas.

La seguridad y el cumplimiento de una organización dependen de sus propios esfuerzos y del de sus proveedores de software.

Conocimientos prácticos

1. Realiza actualizaciones puntuales en todas las aplicaciones y puntos de conexión de tu organización.
2. Realiza una limpieza puntual de todos los ejecutables no utilizados y obsoletos que estén en los dispositivos de la organización.

Enlaces a información adicional (pueden estar en inglés)

- Documentación de Microsoft Intune | Microsoft Docs
- Administrar aplicaciones | Microsoft Docs
- Microsoft Defender para punto de conexión | Seguridad de Microsoft
- Plataforma de cadena de suministro segura de OSS | Seguridad de Microsoft
- Marco de cadena de suministro segura de software de código abierto de Microsoft | Github

Aumentar la resiliencia a los ataques de DDoS, aplicaciones web y red emergentes

La transformación digital acelerada ha puesto fin al modelo tradicional de redes y perímetros de seguridad. La migración al cloud significa que las empresas deben adoptar la seguridad de red nativa del cloud para proteger los activos digitales.

La complejidad, la frecuencia y el volumen de los ataques continúan creciendo y ya no se limitan a las temporadas de vacaciones, lo que indica un cambio a ataques durante todo el año. Esto pone de relieve la importancia de una protección continua que abarque más que las temporadas de picos de tráfico tradicionales.

Ataques distribuidos de denegación de servicio (DDoS)

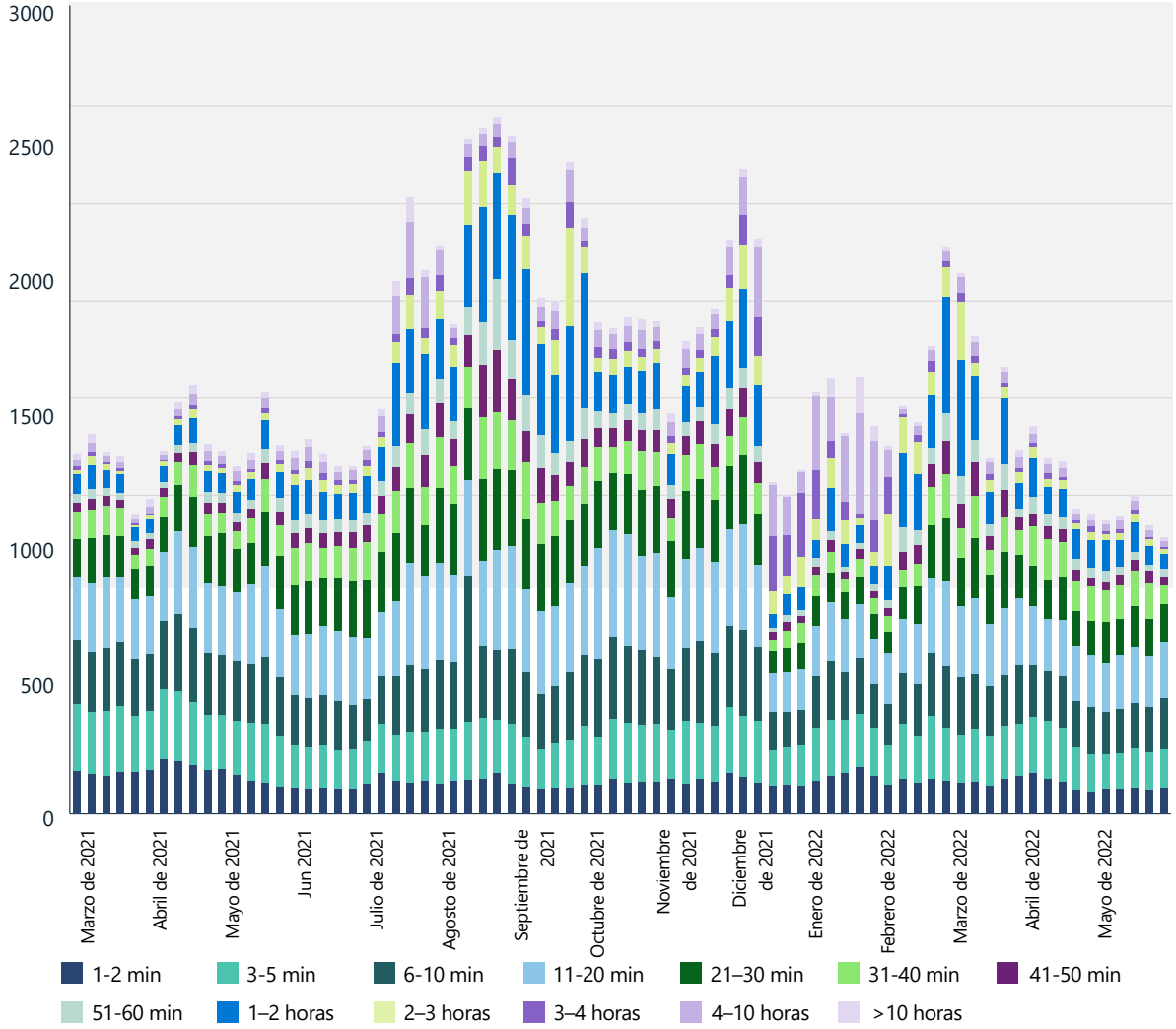
Durante el año pasado, el mundo experimentó una actividad de DDoS sin precedentes en volumen, complejidad y frecuencia. Esta explosión de DDoS vino impulsada por un aumento sustancial de los ataques de los estados nación y la proliferación continua de servicios DDoS por encargo de bajo coste. Microsoft mitigó una media de 1955 ataques al día, lo que supone un aumento del 40 % con respecto al año anterior. Anteriormente, el número máximo de ataques se produjo normalmente durante la temporada navideña de fin de año. Sin embargo, este año, el mayor número de ataques registrados en un día fue el 10 de agosto de 2021. Esto podría indicar un cambio a ataques durante todo el año y destaca la importancia de una protección continua que se extienda más allá de las temporadas de picos de tráfico tradicionales.

En noviembre de 2021, Microsoft frustró un ataque volumétrico de DDoS con una velocidad de 3,4 terabits por segundo (Tbps) de aproximadamente 10 000 fuentes de varios países. Ataques volumétricos similares superiores a 2 TBP se mitigaron en 2022, lo que indica que no solo es la complejidad y la frecuencia de los ataques lo que está aumentando, sino también el volumen (ancho de banda) de los ataques.

Duración de los ataques

La mayoría de los ataques observados en el último año fueron de corta duración. Aproximadamente el 28 % de los ataques duró menos de 10 minutos, el 26 % duró entre 10 y 30 minutos y el 14 % duró entre 31 y 60 minutos. El 32 % de los ataques tuvo más de una hora de duración.

Número de ataques de DDoS y distribución de la duración
(marzo de 2021-mayo de 2022)



La mayoría de los ataques del último año fueron de corta duración. Aproximadamente el 28 % de los ataques duró menos de 10 minutos.

Aumentar la resistencia a los ataques de DDoS, aplicaciones web y red emergentes

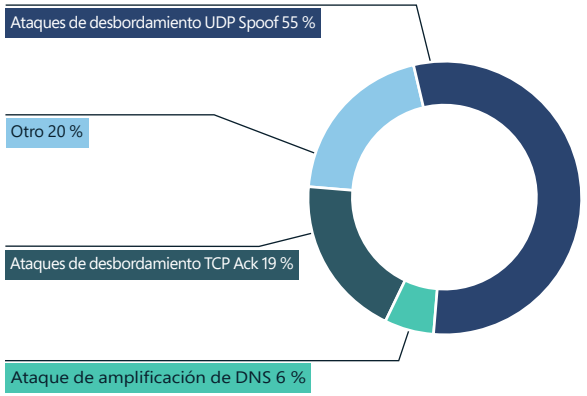
Continuación

Vectores de ataque DDoS

El año pasado, los vectores de ataque empleados habitualmente fueron una reflexión del Protocolo de datagramas de usuario (UDP) en el puerto 80 mediante el protocolo simple de detección de servicios (SSDP), el protocolo de acceso de directorio ligero sin conexión (CLDAP), el sistema de nombres de dominio (DNS) y el protocolo de tiempo de red (NTP) que comprenden un único pico. También vimos un aumento de los ataques DDoS de la capa de la aplicación dirigidos a sitios web, con 16,3 millones de RPS (solicitudes por segundo) máximas y 9,89 Tbps de tráfico máximo.

En 2022, Microsoft mitigó casi 2000 ataques de DDoS diarios y frustró el mayor ataque de DDoS registrado en la historia.

Vectores de ataque DDoS



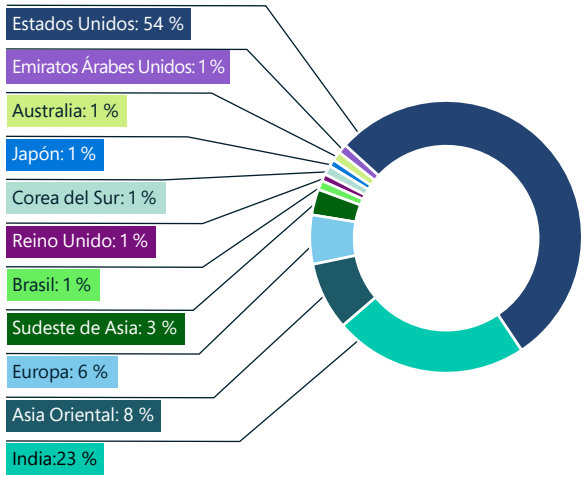
El ataque de desbordamiento UDP Spoof aumentó hasta convertirse en el vector más importante en la primera mitad de 2022, del 16 al 55 por ciento. El ataque de desbordamiento TCP Ack disminuyó del 54 al 19 por ciento.

El sector de los videojuegos sigue siendo el principal objetivo de los ataques DDoS, principalmente a partir de las mutaciones de la botnet Mirai y de los ataques al protocolo UDP de bajo volumen. Puesto que UDP se utiliza habitualmente en juegos y aplicaciones de streaming, una abrumadora mayoría de los vectores de ataque fueron desbordamientos de suplantación de UDP, mientras que una pequeña parte fueron ataques de reflexión y amplificación de UDP.

Regiones geográficas objetivo

De los ataques DDoS detectados durante el año pasado, el 54 % se llevó a cabo contra objetivos de los Estados Unidos, una tendencia que podría explicarse parcialmente por el hecho de que la mayoría de los clientes de Azure y Microsoft están en los Estados Unidos. También vimos un aumento brusco de los ataques contra India: de solo el 2 por ciento de todos los ataques en la segunda mitad de 2021 al 23 por ciento en la primera mitad de 2022. El este de Asia, en particular, Hong Kong, sigue siendo un objetivo popular, con un 8 por ciento. En Europa vimos concentraciones de ataques contra las regiones de Ámsterdam, Viena, París y Fráncfort.

Destino de los ataques DDoS

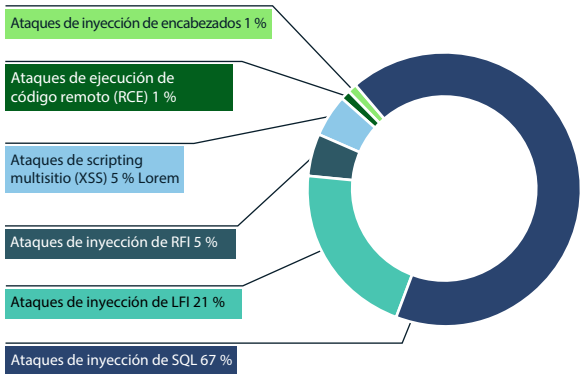


Atribuimos el gran volumen de ataques en Asia a la enorme huella de videojuegos de la región, especialmente en China, Japón, Corea del Sur e India. Esta huella continuará creciendo a medida que la creciente penetración de smartphones aumente la popularidad de los videojuegos para el móvil, lo que sugiere que este objetivo geográfico solo seguirá incrementándose.

Ataques a aplicaciones web

El firewall de aplicaciones web (WAF), en combinación con la protección DDoS, forma una parte integral de la estrategia de defensa en profundidad para proteger los activos de la interfaz de programación de aplicaciones (API) web. Microsoft observó más de 300 000 millones de reglas WAF activadas al mes a través de WAF de Azure.

Distribución de los tipos de ataque más prevalentes



El WAF de Azure detecta miles de millones de ataques Open Web Application Security Project (OWASP) Top 10[10] cada día. Según nuestras señales, los ataques más intentados fueron los de inyección de SQL seguidos de los ataques de inyección local de archivos y de inyección remota de archivos. Esto concuerda con la lista OWASP Top Ten, que muestra que los ataques de inyección son el tercer tipo más común de ataques web.

También ha habido un aumento de los ataques de bot contra aplicaciones web de Azure, con un promedio de 1700 millones de solicitudes de bot al mes, de las cuales el 4,6 por ciento procedían de bots maliciosos.

Aumentar la resiliencia a los ataques de DDoS, aplicaciones web y red emergentes

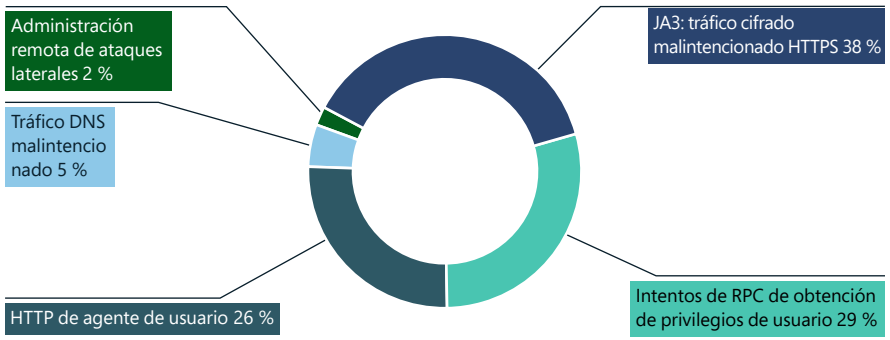
Continuación

Debido al creciente número de bots que realizan ataques de suplantación de credenciales, fraudes de tarjetas de crédito, campañas de ciberinfluencia y ataques a la cadena de suministro, esperamos ver un aumento constante de los ataques de bots contra aplicaciones web.

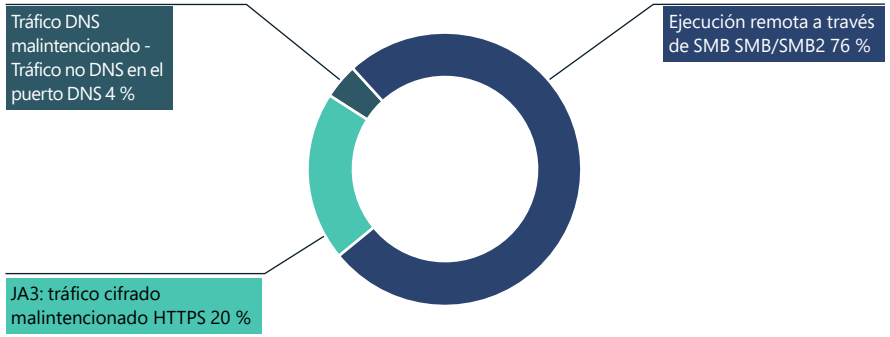
Intrusiones en la red: detección y prevención

En 2022, se observó un aumento importante de los ataques a la capa de red, especialmente el malware. El sistema de detección y prevención de intrusiones de Azure Firewall (IDPS) bloqueó más de 150 millones de conexiones solo en el mes de junio.

Motivo de tráfico de denegación de IDPS



Motivos de alertas de tráfico de IDPS



El análisis de las alertas de IDPS y de tráfico de denegación muestra los siguientes enfoques utilizados por los atacantes. En el tráfico de denegación, estamos viendo que los atacantes utilizan SSL para ocultar sus actividades y que los ataques de ejecución remota son cada vez más comunes. En el tráfico de alertas, estamos viendo cómo se utilizan los protocolos SMB/SMB2 para realizar ataques de ejecución remota.

Conocimientos prácticos

1. Inspecciona todo el tráfico entre los sistemas de un centro de datos o servicio en el cloud y el tráfico que busca acceder a ellos.
2. Desarrolla una estrategia de respuesta de seguridad de red robusta para todo el año.
3. Utiliza servicios de seguridad nativos del cloud para implementar una posición robusta de seguridad de red de confianza cero.

Enlaces a información adicional (pueden estar en inglés)

- Mejora tus defensas de seguridad contra ataques de ransomware con Azure Firewall | Blog y actualizaciones de Azure | Microsoft Azure
- Anatomía de un ataque de amplificación de DDoS | Blog de seguridad de Microsoft
- Protección inteligente de aplicaciones desde el perímetro hasta el cloud con Azure Web Application Firewall | Blog y actualizaciones de Azure | Microsoft Azure

Desarrollar un enfoque que equilibre la seguridad de los datos y la ciberresiliencia

La transformación digital ha traído consigo una amplia expansión de los activos de datos y un aumento de los riesgos de seguridad, cumplimiento y privacidad. Las organizaciones ciberresilientes deben equilibrar las inversiones en funciones de protección, cumplimiento y recuperación de datos e integrarlas en procesos de respuesta a las normativas especializados para abordar distintos tipos de vulneraciones.

La pregunta no es si se van a producir filtraciones de datos, sino cuándo se van a producir. Según el estudio «Cost of a Data Breach, 2021» de IBM y Ponemon Institute, una infracción de datos global media cuesta 4,24 millones de dólares (un 10 % más que en el año anterior) y 9,05 millones de dólares en Estados Unidos. Este informe constata que los fallos de cumplimiento son el principal factor amplificador de los costes. Por el contrario, las reducciones del coste de las infracciones se asociaron con prácticas recomendadas como la planificación de la respuesta a incidentes (IR), la madurez de la implementación de Confianza cero, la IA y la automatización de seguridad y el uso del cifrado.

Las filtraciones de datos son inevitables. Las organizaciones que adopten un enfoque de resiliencia equilibrado reducirán la frecuencia, el impacto y el coste de las infracciones.

El gobierno de los datos, la seguridad, el cumplimiento y la privacidad son interdependientes

Hemos visto que los datos han cobrado importancia en los últimos años y se han convertido en un motor crucial de creación de valor para las organizaciones. Al mismo tiempo, el aumento de las normativas de privacidad, que exigen tanto el gobierno de los datos como la seguridad, han difuminado las líneas entre las funciones de riesgo. Si bien los nuevos roles directivos, como el director de datos (CDO) o los directores de privacidad (CPO), tienen un interés especial en la seguridad y el cumplimiento, la implementación y puesta en marcha de la protección de datos, a menudo estas responsabilidades recaen en equipos dirigidos por los directores de informática (CIO) o el director de seguridad de la información (CISO). Esta no es una calle de un solo sentido, ya que las iniciativas de gobierno de los datos lideradas por los CDO también tienen beneficios para la seguridad. Como resultado de esta interconectividad, los equipos de TI, gobierno de los datos, seguridad, cumplimiento y privacidad deben trabajar cada vez más estrechamente para aumentar la eficiencia y gestionar el riesgo.

Las plataformas unificadas de gestión de riesgos de datos para el patrimonio de datos de toda la organización son el futuro

La alineación del proceso de TI, gobierno de los datos, seguridad, cumplimiento y administración de la privacidad es difícil en un entorno donde existen aplicaciones a medida para cada disciplina y una cobertura incoherente de la típica expansión de datos híbridos y multicloud de la organización. Creemos que las organizaciones necesitan un único panel para localizar y conocer sus datos, protegerlos, regular el acceso, el uso y el ciclo de vida de los datos y evitar la pérdida de datos en todo el patrimonio de datos.

Trabajar a partir de la misma información sobre el inventario y las actividades de los datos facilita los procesos entre los equipos, proporciona una imagen más completa de los riesgos y permite a las organizaciones preparar y optimizar mejor su respuesta a una filtración.

Este único panel debe actuar como un prisma. Los equipos interesados en la seguridad, el cumplimiento y la privacidad de los datos necesitan vistas diferentes pero coherentes del mismo inventario y actividad de datos para coordinarse y colaborar. La actividad de los datos incluye eventos de acceso, modificación y movimiento de datos, que son una parte valiosa de la ecuación de seguridad de los datos.

El gobierno de los datos, la seguridad, el cumplimiento y la privacidad eficaces son interdependientes y requieren la colaboración de los equipos.

Conocimientos prácticos

1. Equilibra la defensa con la recuperación y minimiza el impacto de las filtraciones de datos invirtiendo en funciones de cumplimiento, protección de datos y respuesta.
2. Desarrolla y adopta procesos y herramientas que reduzcan los silos de riesgo de datos y cubran todo el patrimonio de datos.

Enlaces a información adicional (pueden estar en inglés)

- Microsoft Purview: soluciones de protección de datos | Seguridad de Microsoft
- El futuro del cumplimiento y el gobierno de datos ya está aquí: Microsoft Purview | Blog de seguridad de Microsoft

Resiliencia ante las operaciones de ciberinfluencia: la dimensión humana

En los últimos cinco años, los avances en gráficos y machine learning han permitido crear herramientas fáciles de usar capaces de generar rápidamente contenido realista y de alta calidad que puede distribuirse ampliamente por Internet en cuestión de segundos.

En el caso de los eventos registrados a través de texto, audio y contenido visual, hemos llegado a un punto en el que ni los humanos ni los algoritmos pueden distinguir de forma fiable la realidad de la ficción. La proliferación de estas herramientas y sus resultados está generando dudas sobre la fiabilidad de todos los medios digitales, mermando nuestra comprensión de los acontecimientos locales y mundiales. Las nuevas formas de operaciones de influencia habilitadas por los avances tecnológicos tienen graves implicaciones para los procesos democráticos.[11]

Surgen preguntas sobre lo que podemos hacer para prepararnos para un futuro más resiliente contra estas operaciones de ciberinfluencia. La tecnología es solo una pieza del rompecabezas. Va a requerir muchos esfuerzos, incluida la educación dirigida a la alfabetización, la concienciación y la vigilancia de los medios de comunicación, las inversiones en periodismo de calidad —con dispositivos de confianza en la escena local, nacional e internacional—, redes de intercambio y alerta sobre las operaciones de influencia y nuevos tipos de normativas que penalicen a los agentes malintencionados que generen o manipulen medios digitales con el objetivo de engañar.

También reconocemos que restablecer la confianza en el contenido digital es un objetivo ambicioso que requerirá perspectivas diversas y un alto grado de participación. No hay una sola empresa, institución o gobierno que pueda resolver estas amenazas por sí solo. Nuestro superpoder como seres humanos es nuestra capacidad de colaborar y cooperar. Esto es especialmente importante ahora porque requerirá que todo el mundo —los gobiernos globales, los sectores de la industria, el mundo académico y, en especial, las organizaciones de noticias, redes sociales y medios de comunicación— colabore en pro de la mejora y la salud de nuestra sociedad.

Enlaces a información adicional (pueden estar en inglés)

- Aplicaciones de inteligencia artificial en las misiones cibernéticas del Departamento de Defensa | Microsoft On the Issues
- Inteligencia artificial y ciberseguridad: desafíos crecientes y directrices prometedoras. Audiencia sobre aplicaciones de la inteligencia artificial en operaciones en el ciberespacio ante el Subcomité de Ciberseguridad, del Comité de Servicios Armados del Senado, congreso 117º (3 de mayo de 2022; testimonio de Eric Horvitz)

Fortalecer el factor humano con conocimientos

Abordar el factor humano es un componente clave de cualquier estrategia de capacitación en ciberseguridad. Según el estudio de Kaspersky Human Factor in IT Security,[12] el 46 por ciento de los incidentes de ciberseguridad involucra a personal descuidado o desinformado que facilita involuntariamente el ataque.

El equipo de educación y concienciación de Microsoft en la organización de seguridad digital y resiliencia es responsable de fortalecer el factor humano de la ciberseguridad capacitando a los empleados para que protejan nuestros propios sistemas y datos y los de nuestros clientes. Nuestros objetivos son:

- Reducir el riesgo para Microsoft y nuestros clientes mediante la creación de un conjunto centralizado de competencias de seguridad básicas para toda la empresa entre la población de empleados.
- Reforzar los conocimientos de seguridad de los empleados mediante un enfoque de refuerzo de formación de varias fases para respaldar los resultados de comportamiento deseados.
- Fomentar el cambio cultural convirtiendo la mentalidad de seguridad en una parte intrínseca de la cultura de Microsoft a través de formación y eventos de seguridad anuales.
- Promover un recurso web centralizado para prácticas recomendadas, información de políticas empresariales e informes de incidentes para todo lo relacionado con la ciberseguridad

Todos los empleados de Microsoft deben realizar un programa de capacitación en ciberseguridad dirigido y centralizado al menos una vez al año. Las ofertas de formación están optimizadas para respaldar las iniciativas actuales de ciberseguridad y ofrecer resultados de comportamiento cuantificables. El Information Risk Management Council (IRMC) de Microsoft desempeña un papel clave en la identificación de los resultados importantes de cambio de comportamiento en ciberseguridad que deben abordarse en la formación.

Con todos nuestros programas de capacitación en ciberseguridad, medimos la eficiencia, la eficacia y los resultados de la solución siempre que es posible. Por ejemplo, nuestra oferta de capacitación sobre amenazas internas tiene un 95 por ciento de asistencia y una calificación de excepcional por parte de los alumnos, y ha dado lugar a un aumento importante de los directivos que informan de posibles casos de amenazas internas a través de la herramienta Report It Now de la empresa. El programa incluye:

Fundamentos de seguridad: formación centralizada en concienciación y cumplimiento de la ciberseguridad en toda la empresa, que aborda las prácticas básicas de seguridad y privacidad. Esta serie de cursos, que provocan gran expectación, emplea un modelo de formación para que el aprendizaje sobre ciberseguridad sea atractivo e interesante.

STRIKE: formación técnica de Microsoft necesaria para los ingenieros que crean y mantienen soluciones de línea de negocio. Este curso accesible solo por invitación aborda las áreas específicas y críticas de las prácticas recomendadas de higiene de ciberseguridad y utiliza un modelo de impartición híbrido en tiempo real adaptado a las necesidades del público.

Específicos del programa: los programas de formación dirigidos respaldan las iniciativas específicas de ciberseguridad, como Shadow IT, Insider Threat y Microsoft Federal. Estas ofertas se integran estrechamente en la estrategia general de participación de sus respectivas iniciativas de ciberseguridad a través del apoyo de la dirección e informes del cuadro de mando para evitar un enfoque de formación tipo test.

MSProtect: un recurso web centralizado de Microsoft que proporciona prácticas recomendadas, información de políticas empresariales e informes de incidentes para todo lo relacionado con la ciberseguridad Este recurso a petición es la herramienta de referencia para los empleados, además de las ofertas de formación formales.

La capacitación en seguridad no debe considerarse una actividad de cumplimiento normativo de relleno de formularios. En su lugar, debe centrarse en el cambio de comportamiento para permitir que los resultados se supervisen a través de comportamientos identificados y establecer sistemas de escucha para determinar el impacto de las ofertas.

Conocimientos prácticos

1. Proporciona formación y recursos de seguridad a los empleados cuando y donde los necesiten.
2. Desarrolla una estrategia centralizada de capacitación basada en las opiniones de las partes interesadas de toda la empresa.
3. Garantiza que se realice un seguimiento y análisis del impacto de la formación en busca de eficiencia (cantidad), eficacia (calidad) y resultados (impacto empresarial).

Enlaces a información adicional (pueden estar en inglés)

- Microsoft inicia la siguiente etapa de la iniciativa de capacitación después de ayudar a 30 millones de personas

Ideas extraídas de nuestro programa de eliminación de ransomware

Microsoft ha iniciado su propio proceso de Confianza cero[13] en los últimos cinco años para garantizar que las identidades y los dispositivos estén correctamente administrados y en buen estado. A medida que crece el riesgo de ransomware, hemos desarrollado una perspectiva detallada para respaldar nuestro enfoque dirigido a protegernos a nosotros mismos y a nuestros clientes.

Después de una evaluación interna en profundidad, creamos un programa de eliminación de ransomware para corregir las deficiencias en los controles y la cobertura, contribuir a las mejoras de características de servicios como Defender para punto de conexión, Azure y M365, y desarrollar cuadernos de estrategias para nuestros equipos de SOC y de ingeniería sobre cómo recuperarse en caso de un ataque de ransomware.

El primer paso fue conocer el alcance de nuestra protección contra un ataque de ransomware dirigido a Microsoft. Ya se estaba trabajando para implementar Defender para punto de conexión y garantizar que todos los dispositivos estuvieran administrados y cumplieran nuestras políticas de Confianza cero, pero necesitábamos encontrar una manera de conocer todas las facetas de la gran pregunta de si podríamos recuperarnos eficazmente de un ataque. Para obtener perspectiva, hemos evaluado el NIST 8374: Gestión de riesgos de ransomware: un perfil de Cybersecurity Framework (CSF),[14] que se adapta a nuestra política general empresarial con nuestra lista de controles conocidos. Este análisis identificó rápidamente las deficiencias de cobertura.

A continuación, priorizamos las deficiencias en las funciones Identificar, Proteger, Responder y Recuperarse del CSF. Encontramos una alineación estratégica con la Confianza cero y otros programas, y también descubrimos deficiencias que no tenían ningún flujo de trabajo existente. Después de haber evaluado la cantidad de trabajo y esfuerzo necesarios para corregir estas deficiencias, las dividimos en dos pilares:

- **Proteger a la empresa (PtE):** definir los elementos de trabajo que debemos emprender como empresa para protegernos y poder recuperarnos de un ataque, en caso de que uno llegue a término.
- **Proteger al cliente (PtC):** crear funciones en nuestras ofertas para proteger a nuestros clientes y a nuestro negocio.

Integración de las conclusiones en nuestra propia empresa

Para remediar los principales riesgos y proteger nuestros servicios críticos contra un ataque de ransomware, queremos centrar las inversiones en los próximos 6 o 12 meses en lograr los cinco escenarios siguientes como parte de un programa dedicado exclusivamente al ransomware. Una vez que consigamos cada uno de estos escenarios, ampliaremos gradualmente el alcance del programa para aplicarlos a todas las partes de la empresa.

Escenario 1: los miembros del equipo de seguridad conocen el riesgo general asociado a un ataque de ransomware y establecen un proceso que proporciona conocimientos a los directivos sobre las deficiencias de control y el estado de riesgo.

Escenario 2: los miembros del equipo de seguridad tienen acceso a cuadernos de trabajo diseñados para ayudarles a ellos y a otros equipos de Microsoft a responder a los servicios críticos y recuperarse de un ataque de ransomware.

Escenario 3: los miembros del equipo de resiliencia empresarial tienen un estándar que seguir para las copias de seguridad de los sistemas críticos. Para garantizar que los datos se puedan recuperar en caso de un ataque de ransomware, existen cuadernos de estrategias y se realizan ejercicios periódicos de copia de seguridad.

Escenario 4: los propietarios de los servicios conocen e implementan los controles y políticas operativos y de seguridad necesarios para proteger su servicio, los datos de los clientes, los puntos de conexión y los activos de red contra ataques de ransomware, centrándose especialmente en los servicios priorizados por Microsoft como servicios críticos.

Escenario 5: todos los empleados pueden acceder a recursos educativos y de formación que describen cómo reconocer un ataque de ransomware y cómo notificar al equipo de seguridad e iniciar la respuesta.

Conocimientos prácticos

1. Documenta y valida actividades integrales de recuperación y corrección relacionadas con ataques de ransomware contra servicios críticos.
2. Implica a las partes interesadas en la actualización de los cuadernos de trabajo de gestión de las crisis empresariales para incluir actividades específicas del ransomware, así como un proceso de decisión y orientación para determinar si o cuándo se debe pagar el rescate del ransomware.
3. Mejora la cobertura de detección y protección habilitando las funciones disponibles en tus productos de seguridad implementados (por ejemplo, reglas de reducción de la superficie de ataque de Defender para punto de conexión).
4. Trabaja con el equipo de normas de seguridad para definir una línea de referencia para la protección contra un ataque de ransomware y proporciona formación y documentación a los equipos de ingeniería sobre cómo protegerse contra un ataque de ransomware.
5. Pon en marcha la automatización para facilitar la implementación de políticas de seguridad y operaciones a los equipos de DevOps y asegurarte de que si un sistema se desvía del cumplimiento se identifica y corrige rápidamente.

Enlaces a información adicional (pueden estar en inglés)

- Cómo Microsoft protege frente a los ataques de ransomware | Microsoft Inside Track

Actuación inmediata ante las implicaciones de la seguridad cuántica

La presión está en gestionar la amenaza que plantea la computación cuántica a la criptografía actual y a todo lo que esta protege. El Memorando sobre la mejora de la ciberseguridad del Departamento de Defensa e Inteligencia de la Comunidad de Seguridad Nacional[15] recientemente publicado, basado en el decreto presidencial de EE. UU. 10428[16] para la mejora de la ciberseguridad de la nación, hace hincapié en proteger la cadena de suministro de software como un aspecto fundamental para abordar futuros ataques de los estados nación.

¿Qué son los ordenadores cuánticos?

Los ordenadores cuánticos son máquinas que utilizan las propiedades de la física cuántica para almacenar datos y realizar cálculos. Pueden ser extremadamente útiles para algunas tareas que pueden realizar muchísimo mejor que nuestros mejores superordenadores. La computación cuántica ya está abriendo nuevos horizontes para el cifrado y procesamiento de datos. Los estudios prevén que la computación cuántica se convierta en un sector cuántico de varios miles de millones de dólares (USD) tan pronto como en 2030.[17] De hecho, la computación cuántica y la comunicación cuántica están preparadas para tener un efecto transformador en multitud de sectores, desde la atención sanitaria y la energía hasta las finanzas y la seguridad.

La computación cuántica es una amenaza para la criptografía actual y para todo lo que protege.

La amenaza a la criptografía actual

Con el algoritmo de Shor de 1994 y un ordenador cuántico a escala industrial de más de unos pocos millones de cúbits físicos, todos nuestros algoritmos criptográficos de claves públicas actuales y ampliamente implementados podrían descomponerse fácilmente. Es fundamental considerar, evaluar y estandarizar sistemas criptográficos seguros frente la computación cuántica que sean eficientes, ágiles y seguros contra un ataque cuántico. La migración del software a la «criptografía poscuántica», es decir, algoritmos y protocolos clásicos existentes robustos a los ataques cuánticos, tardarán años, si no una década o más, en conseguirse.[18]

Esto significa que la presión recae en gestionar la amenaza que plantea la computación cuántica a la criptografía actual y a todo lo que esta protege. Los adversarios pueden grabar datos cifrados ahora y aprovecharlos más adelante una vez que un ordenador cuántico esté disponible. Si esperamos a que llegue la computación cuántica para abordar sus implicaciones criptográficas será demasiado tarde.

Como la criptografía se utiliza en todo el ecosistema cibernético, esto significa que nuestros servicios de seguridad basados en criptografía podrían estar en peligro. Esto incluye, por ejemplo, servicios de comunicaciones (TLS, IPSec), mensajería (correo electrónico, conferencias web), administración de identidad y acceso, navegación web, firma de código, transacciones de pago y otros servicios que dependen de la criptografía para su protección.

Cuando los ordenadores cuánticos se conviertan en una realidad, los componentes de software de terceros que contengan implementaciones de algoritmos y funciones criptográficas también requerirán un escrutinio adicional. Esto exige que todas las organizaciones a lo largo de la cadena de valor hagan lo que corresponda para garantizar que la cadena permanezca segura. La industria y los gobiernos están incrementando los esfuerzos para definir los requisitos de seguridad de la cadena de suministro de software y, en algunos casos, introduciendo nuevos mandatos para proteger la cadena. El Memorando de Seguridad Nacional NSM-8[19] establece los requisitos y los plazos para la implementación de la criptografía poscuántica en los sistemas de seguridad nacionales (NSS). Impone un calendario de 180 días para «la planificación de la modernización, el uso de cifrado no compatible, protocolos aprobados únicos para la misión, protocolos resistentes a la computación cuántica y planificación del uso de criptografía resistente a la computación cuántica cuando sea necesario».

La estandarización es una actividad a largo plazo en la transición a la criptografía cuánticamente segura. Los organismos de normalización que trabajan en estándares que utilizan criptografía de claves públicas deben comenzar a probar algoritmos poscuánticos y adaptarse ahora a estos algoritmos.

Los nuevos algoritmos de criptografía poscuántica (PQC) —algoritmos clásicos que se consideran robustos frente a los ataques cuánticos— se están revisando en el Proyecto de estandarización poscuántica de NIST.[20] Este trabajo influirá en las iniciativas globales de los organismos de normalización. Aunque habrá algún solapamiento en los algoritmos seleccionados por el gobierno de Estados Unidos, las diferentes opciones normativas o de los organismos nacionales para algoritmos compatibles podrían plantear desafíos internacionales. Esta fragmentación complicará a su vez el diseño de productos y servicios.

Los nuevos algoritmos de criptografía poscuántica se están revisando a través del programa de estandarización de criptografía poscuántica del NIST. Este trabajo influirá en los esfuerzos globales de los organismos de normalización.

Conocimientos prácticos

Junto con SAFECode y los socios, la industria debe emprender medidas inmediatas para prepararse para la transición a la PQC.[21] Entre ellas se incluyen:

1. Realizar un inventario de los productos/códigos que utilizan criptografía.
2. Implementar una estrategia de agilidad criptográfica en toda la organización que incluya minimizar la pérdida de código necesaria cuando cambie la criptografía.
3. Realizar pruebas piloto del uso de algoritmos seguros frente a la computación cuántica candidatos en los productos o servicios que utilizan criptografía.
4. Prepararse para utilizar diferentes algoritmos de clave pública para el cifrado, el intercambio de claves y las firmas.
5. Probar las aplicaciones para comprobar el impacto de las claves, cifrados y firmas muy grandes.

Enlaces a información adicional (pueden estar en inglés)

- Microsoft ha demostrado la física subyacente necesaria para crear un nuevo tipo de cúbit | Microsoft Research

Integración de negocio, seguridad y TI para aumentar la resiliencia

La resiliencia cibernética robusta depende de que los líderes empresariales trabajen con los equipos de seguridad para implementar medidas de seguridad. Según Microsoft, el liderazgo en seguridad es una disciplina compleja que requiere el apoyo de los líderes de la organización para proteger la organización de la manera más eficaz.

Los líderes de seguridad se enfrentan a una serie de desafíos dinámicos que abarcan temas relacionados con el riesgo, la tecnología, la economía, el proceso organizativo, los modelos de negocio, la transformación de la cultura, los intereses geopolíticos, el espionaje y el cumplimiento de sanciones internacionales. Cada uno de ellos tiene matices que deben conocerse y gestionarse.

Los líderes de seguridad también tienen la tarea de frustrar a los atacantes humanos inteligentes, con amplios recursos financieros y muy motivados, así como a los ciberdelincuentes poco cualificados pero eficaces. Sus equipos deben defender patrimonios técnicos complejos construidos a menudo durante 30 años o más cuando la seguridad era una prioridad baja o inexistente. Las decisiones tomadas hace años pueden suponer riesgos hoy en día hasta que paguemos la deuda técnica y abordemos las brechas de seguridad.

Los líderes de las organizaciones y los legisladores pueden tener un impacto positivo importante en la seguridad si apoyan activamente a los líderes de seguridad y les ayudan a tender un puente entre las medidas de seguridad integradas y el resto de la organización. Microsoft ha observado que los clientes que cuentan con este tipo de trabajo coordinado están construyendo una organización más resiliente y también mejorando su agilidad para adaptarse e innovar.

Los líderes de la organización pueden apoyar a los líderes de seguridad centrándose en tres áreas clave:

1. Crear seguridad por diseño

La seguridad a veces se considera un obstáculo o una idea de última hora en los procesos de negocio, y a menudo solo se tiene en cuenta en las decisiones cuando es demasiado tarde para evitar un riesgo o solucionarlo de forma barata y sencilla.

Los líderes de las organizaciones y los legisladores deben asegurarse de:

Incluir la seguridad en las primeras fases de las nuevas iniciativas. Las nuevas iniciativas digitales y la adopción del cloud deben priorizar la seguridad para garantizar que el riesgo de la organización no aumente con cada nueva aplicación o capacidad digital. Una vez que se haya incluido la seguridad de forma fiable, se pueden utilizar esos procesos para modernizar los sistemas heredados y disfrutar al mismo tiempo de ventajas de seguridad y productividad.

Normalizar el mantenimiento preventivo de la seguridad. Garantizar que el mantenimiento básico de la seguridad, como la aplicación de actualizaciones y parches de seguridad y configuraciones seguras, cuenta con todo el apoyo de la organización (incluidos presupuestos, tiempo de inactividad previsto, requisitos de adquisición para el soporte de productos del proveedor).

Lamentablemente, muchas organizaciones retrasan estas prácticas comunes o solo las aplican parcialmente. Esto ofrece a los atacantes grandes oportunidades de explotación. La necesidad de normalización de la seguridad se refleja en la norma NIST de EE. UU. 800-40.[22]

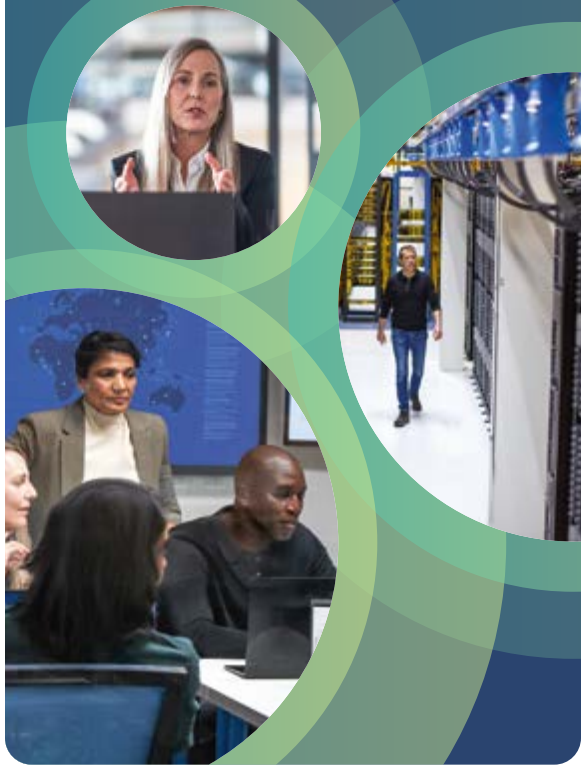
2. Participar en la seguridad

Los líderes de las organizaciones deben participar activamente en los procesos de seguridad clave y apoyarlos para garantizar la priorización de los recursos y la preparación ante los desastres de seguridad. Esto incluye participar en:

Identificar los activos empresariales críticos. Los líderes y los equipos de seguridad necesitan saber qué activos son esenciales para el negocio para centrar los recursos de seguridad en lo más importante. Este, a menudo, es un nuevo ejercicio que incluye plantearse nuevas preguntas que no se han abordado anteriormente.

Ejercicios de continuidad del negocio y recuperación ante desastres de ciberseguridad. Los ciberataques pueden convertirse en eventos importantes que interrumpan o detengan la mayoría o todas las operaciones empresariales. Garantizar que los equipos de toda la organización estén preparados para gestionar estas situaciones reducirá el tiempo para restaurar las operaciones del negocio, limitará los daños a la organización y ayudará a mantener la confianza de los clientes, ciudadanos y electores. Esto debe integrarse dentro de un proceso de continuidad del negocio y recuperación ante desastres existente.

Las decisiones sobre los riesgos de seguridad las toman mejor los propietarios de las empresas o de la misión, quienes tienen visibilidad completa de todos los riesgos y oportunidades.



Integración de negocio, seguridad y TI para aumentar la resiliencia

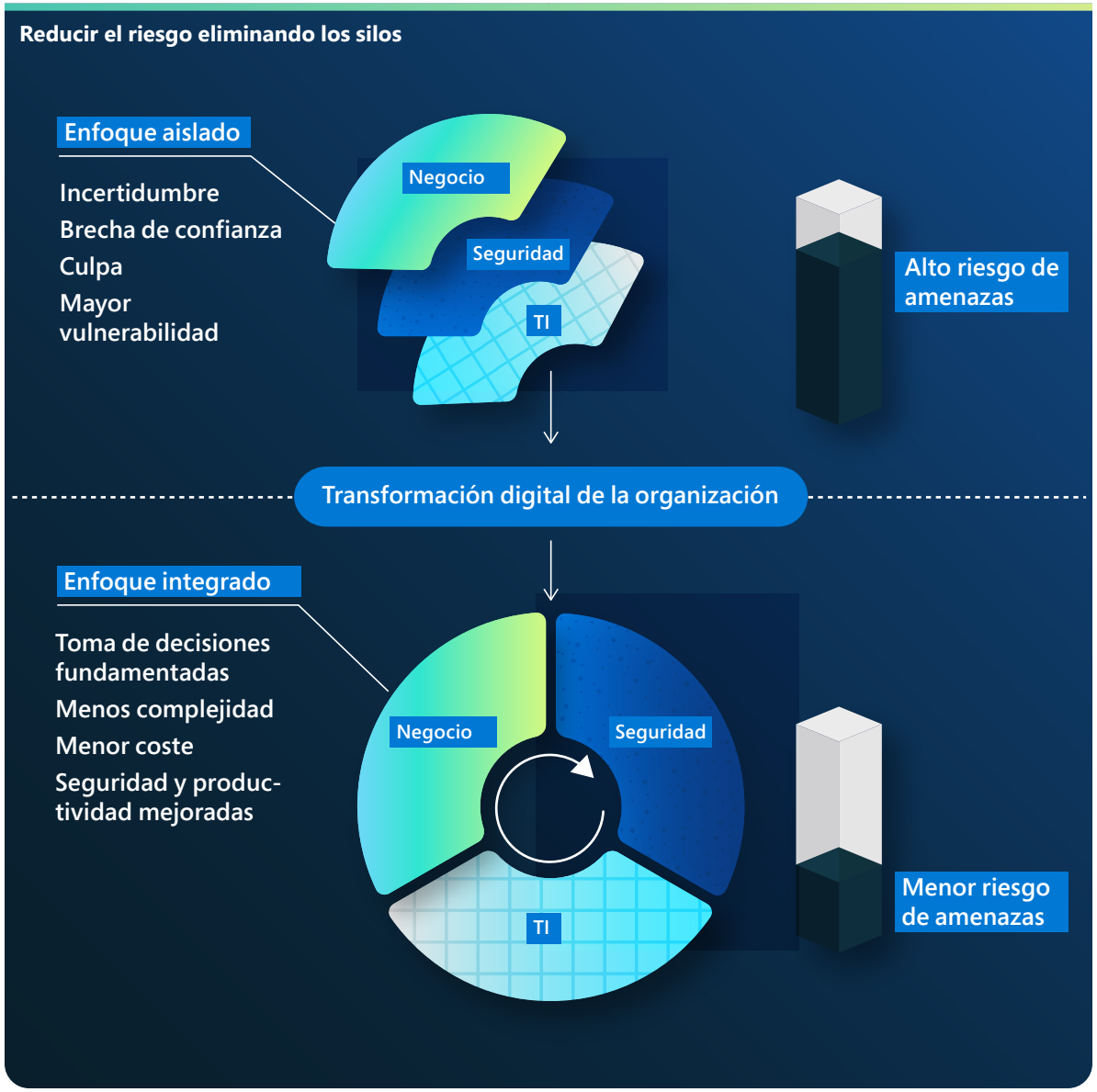
Continuación

3. Colocar la seguridad en el lugar que le corresponde

La forma en que las organizaciones estructuran la responsabilidad de los riesgos de seguridad a menudo impide tomar decisiones correctas sobre la seguridad. Las decisiones sobre los riesgos las toman mejor los propietarios de empresas o de la misión, quienes tienen visibilidad completa de todos los riesgos y oportunidades, pero las organizaciones a menudo asignan responsabilidades de riesgos de seguridad (implícita o explícitamente) a expertos en la materia del equipo de seguridad. Esto supone una sobrecarga para los equipos de seguridad que priva a los propietarios de las empresas de la visibilidad y el control sobre un riesgo clave para su negocio. Las organizaciones pueden solucionar esto:

Preparando a los propietarios de las empresas: formar a los propietarios de empresas sobre el riesgo de seguridad en general y cómo estas amenazas pueden afectar y afectarán a su negocio. La participación directa de los equipos de seguridad en esta iniciativa aumenta también la relación de colaboración con la seguridad y la agilidad empresarial general.

Asignando el riesgo de seguridad a los propietarios de las empresas: cuando los propietarios de las empresas dispongan de la información suficiente para entender y aceptar el riesgo de seguridad, la organización debe traspasarles la responsabilidad de los riesgos de seguridad, manteniendo la responsabilidad de los equipos de seguridad de gestionar ese riesgo y de proporcionar conocimientos especializados y orientación al propietario.



«La ciberresiliencia es un proceso gradual de la continuidad del negocio y recuperación ante desastres clásicas, que empieza por una buena copia de seguridad de los datos y se extiende hasta las funciones de recuperación de procesos, tecnología y sus dependencias (incluidas personas y terceros) y el cambio a servicios siempre disponibles de reparación automática, resiliencia para roles críticos y conmutación por error para terceros críticos. Las organizaciones más resilientes promueven la integración entre los directores de TI, los directivos de la empresa y los profesionales de seguridad. Una buena resiliencia incluye diseñar teniendo en cuenta la resiliencia desde el principio, la administración segura de los cambios y el aislamiento granular de los fallos. La ciberresiliencia es solo un escenario de un buen programa de planificación de todos los peligros. A medida que aumenten los riesgos cibernéticos y la intersección entre la ciberseguridad y la resiliencia cobre importancia, aumentará la conexión del director de seguridad de la información (CISO) con el programa de resiliencia empresarial. Cada año aumenta el número de directores de seguridad de la información responsables de proporcionar resiliencia a toda la empresa».

Lisa Reshaur
Directora general, gestión de riesgos, Microsoft

Enlaces a información adicional (pueden estar en inglés)

- De la resiliencia a la perseverancia digital: cómo las organizaciones están utilizando la tecnología digital para repuntar en tiempos sin precedentes | Blog oficial de Microsoft
- Cómo los equipos de TI y seguridad pueden trabajar juntos para mejorar la seguridad de los puntos de conexión | Seguridad de Microsoft

La curva en campana de la ciberresiliencia

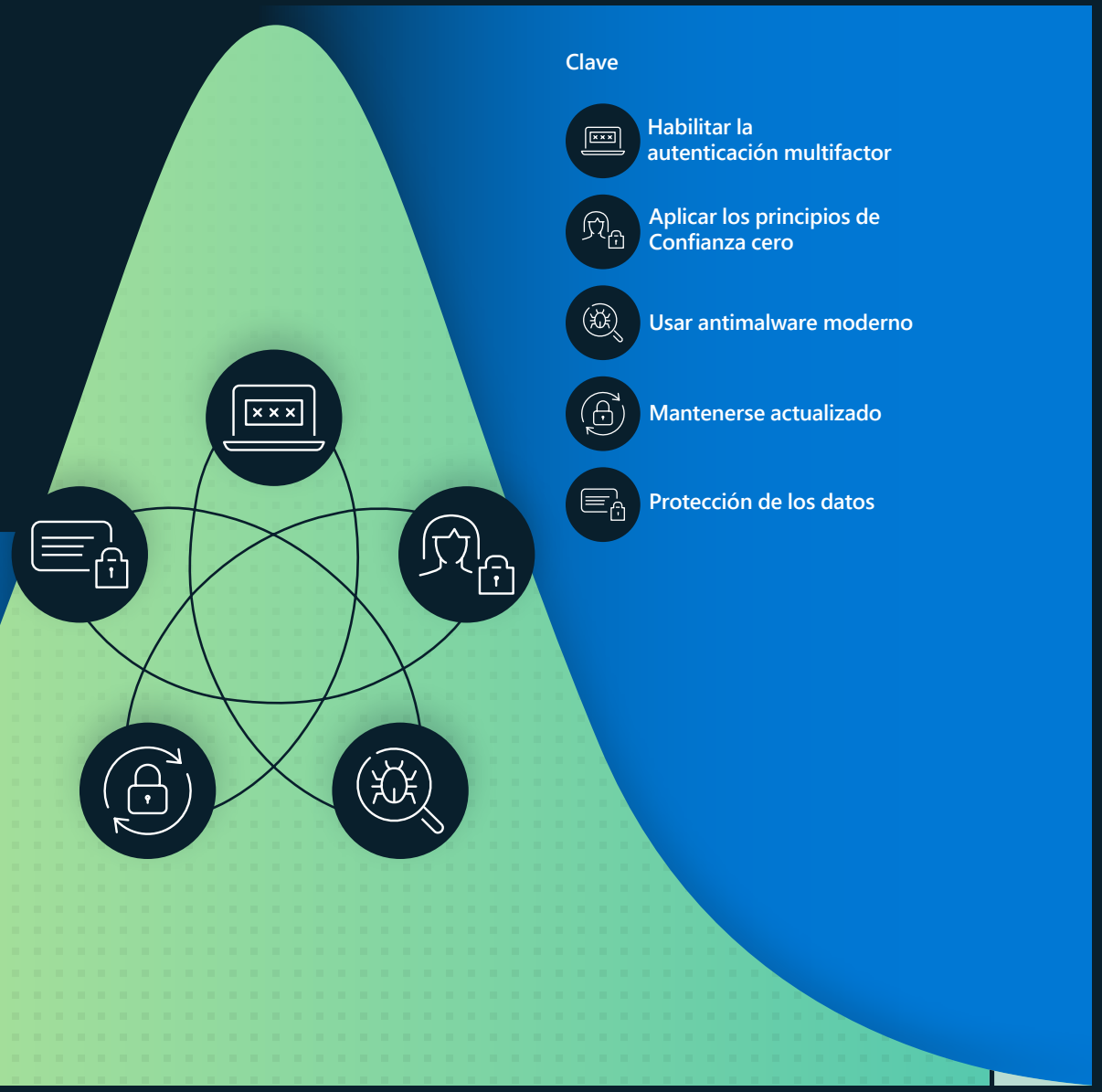
Factores de éxito de la resiliencia que todas las organizaciones deben adoptar

Como hemos visto, muchos ciberataques prosperan simplemente porque no se ha seguido una higiene de seguridad básica. Los estándares mínimos que debe adoptar cada organización son:

- **Habilitar la autenticación multifactor (MFA):** para protegerse de las contraseñas de usuario expuestas y ayudar a proporcionar resiliencia adicional a las identidades.
- **Aplicar principios de Confianza cero:** la piedra angular de cualquier plan de resiliencia que desee limitar el impacto en una organización. Estos principios son:
  1. – Verificar explícitamente: asegurarse de que los usuarios y los dispositivos estén en buen estado antes de permitir el acceso a los recursos.
  2. – Usar el acceso con privilegios mínimos: permitir solo los privilegios necesarios para acceder a un recurso y nada más.
  3. – Asumir que se va a producir un ataque: dar por hecho que se han vulnerado las defensas del sistema y que los sistemas podrían sufrir un ataque. Esto significa supervisar constantemente el entorno para un posible ataque.
- **Usar antimalware de detección y respuesta extendidas:** implementar software para detectar y bloquear ataques automáticamente y proporcionar información a las operaciones de seguridad. La supervisión de la información procedente de los sistemas de detección de amenazas es esencial para poder responder a las amenazas puntualmente.
- **Mantenerse al día:** los sistemas sin parches y desactualizados son uno de los principales motivos por los que muchas organizaciones son víctimas de un ataque. Asegúrate de que todos los sistemas se mantengan actualizados, incluido el firmware, el sistema operativo y las aplicaciones.
- **Proteger los datos:** conocer los datos importantes, dónde se encuentran y si se han implementado los sistemas adecuados es crucial para implementar la protección adecuada.

98 %

El 98 % de los ataques se pueden evitar con higiene de seguridad básica



Notas al pie

1. La detección y respuesta de puntos de conexión (EDR) es una plataforma de seguridad de puntos de conexión empresarial diseñada para ayudar a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas. Las funciones de detección y respuesta de puntos de conexión proporcionan detecciones avanzadas de ataques casi en tiempo real que ofrecen un plan de actuación. Los analistas de seguridad pueden priorizar las alertas eficazmente, obtener visibilidad del alcance completo de una vulneración y emprender medidas de respuesta para remediar las amenazas.
2. Una plataforma de protección de puntos de conexión (EPP) es una solución implementada en dispositivos de punto de conexión para evitar malware basado en archivos, detectar y bloquear la actividad malintencionada de aplicaciones fiables y no fiables, y proporcionar las funciones de investigación y corrección necesarias para responder dinámicamente a incidentes y alertas de seguridad.
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Libro de seguridad de Windows: comercial
7. Las nuevas características de seguridad de Windows 11 ayudarán a proteger el trabajo híbrido | Blog de seguridad de Microsoft
8. FIDO Alliance: estándares de autenticación abiertos más seguros que las contraseñas
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. Decreto presidencial 14028: mejorar la ciberseguridad de la nación
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. «El largo camino que nos espera para la transición a la criptografía poscuántica», https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

Equipos colaboradores

Equipos colaboradores

Los datos y las ideas de este informe los proporciona un grupo diverso de profesionales centrados en la seguridad que trabajan en muchos equipos de Microsoft diferentes. En conjunto, su objetivo es proteger a Microsoft, a sus clientes y al mundo en general de la amenaza de los ciberataques. Nos sentimos orgullosos de compartir estos conocimientos con un espíritu de transparencia, con el objetivo común de hacer del mundo un lugar más seguro para todos.

AI for Good Research Lab: aprovechar el poder de los datos y la IA para abordar muchos de los desafíos del mundo. El laboratorio colabora con organizaciones ajenas a Microsoft, aplicando la IA para mejorar las condiciones de vida y los entornos. Las áreas de interés incluyen la seguridad online (desinformación, ciberseguridad, seguridad infantil), la respuesta ante desastres, la sostenibilidad y la IA para la salud.

Azure Edge & Platform, Enterprise & OS Security: responsable de la seguridad básica del sistema operativo y la plataforma en Windows, Azure y otros productos de Microsoft. El equipo crea soluciones de seguridad y hardware líderes del sector en las plataformas de Microsoft para evitar el aprovechamiento de vulnerabilidades, los ataques de identidad y el malware desde el chip hasta el cloud. Creadores de la plataforma de núcleo seguro de Microsoft para PC, dispositivos perimetrales, servidores y el procesador de seguridad Microsoft Pluton, entre otras cosas.

Redes de Azure, base: un equipo de redes en el cloud centrado en la WAN de Microsoft, las redes de centro de datos y la infraestructura de red definida por software de Azure, incluida la plataforma DDoS, la plataforma perimetral de red y los productos de seguridad de red como Azure WAF, Azure Firewall y Azure DDoS Protection Standard.

Equipo de investigación de seguridad en el cloud: al proteger el cloud de Microsoft, crear características y productos de seguridad innovadores y realizar investigaciones, este equipo protege y permite a los clientes de Microsoft transformar de forma segura sus organizaciones.

Seguridad y confianza de los clientes (CST): un equipo que impulsa la mejora continua de la seguridad de los clientes en los productos y servicios online de Microsoft. Trabajando con los equipos de ingeniería y seguridad de toda la empresa, la misión de CST es garantizar el cumplimiento, mejorar la seguridad y proporcionar más transparencia para proteger a nuestros clientes y promover la confianza global en Microsoft.

Éxito del cliente: los equipos de seguridad del éxito del cliente trabajan directamente con los clientes para compartir prácticas recomendadas, lecciones aprendidas y directrices para acelerar la transformación y la modernización de la seguridad. Este equipo reúne y organiza las prácticas recomendadas y las lecciones aprendidas del proceso de Microsoft, y del de nuestros clientes, en estrategias de referencia, arquitecturas de referencia, planes de referencia, etc.

Centro de operaciones de ciberdefensa (CDOC): los servicios de ciberseguridad y defensa de Microsoft constituyen un centro de fusión que reúne a profesionales de la seguridad de toda la empresa para proteger nuestra infraestructura corporativa y la infraestructura en el cloud a la que tienen acceso los clientes. Los responsables de la respuesta a incidentes se reúnen con científicos de datos e ingenieros de seguridad de todos los grupos de servicios, productos y dispositivos de Microsoft con el objetivo de proteger de las amenazas, detectarlas y responder a ellas las 24 horas del día todos los días de la semana.

Democracy Forward Initiative: un equipo de Microsoft que trabaja en la conservación, protección y avance de los fundamentos de la democracia promoviendo un ecosistema de información saludable, protegiendo los procesos democráticos abiertos y seguros y abogando por la responsabilidad civil corporativa.

Unidad de delitos digitales (DCU): un equipo de abogados, investigadores, científicos de datos, ingenieros, analistas y profesionales empresariales dedicados a la lucha contra la ciberdelincuencia a escala global mediante tecnología, análisis forenses, acciones civiles, denuncias penales y asociaciones tanto públicas como privadas.

Diplomacia digital: un equipo internacional de exdiplomáticos, legisladores y expertos jurídicos que trabaja para desarrollar un ciberespacio pacífico, estable y seguro ante el creciente conflicto de los estados nación.

Seguridad digital y resiliencia (DSR): una organización dedicada a permitir que Microsoft cree los dispositivos y servicios más fiables y a mantener protegida nuestra empresa y los datos de nuestra empresa y de los clientes.

Unidad de seguridad digital (DSU): un equipo de abogados y analistas de ciberseguridad que proporcionan conocimientos legales, geopolíticos y técnicos para proteger a Microsoft y a sus clientes. DSU genera confianza en las defensas de seguridad empresariales de Microsoft frente a los ciberatacantes avanzados de todo el mundo.

Centro de análisis de amenazas digitales (DULT): un equipo de expertos que analizan y comunican las amenazas de los estados nación, incluidos los ciberataques y las operaciones de influencia. El equipo combina la información e inteligencia sobre amenazas cibernéticas con análisis geopolíticos para proporcionar conocimientos a nuestros clientes y a Microsoft con el fin de comunicar respuestas y medidas de protección eficaces.

Empresa y seguridad: un equipo centrado en proporcionar una plataforma moderna, segura y manejable para el cloud inteligente y el perímetro inteligente.

Movilidad empresarial: un equipo que ayuda a ofrecer un lugar de trabajo moderno y una administración moderna para mantener la seguridad de los datos, tanto en el cloud como on-premises. Endpoint Manager incluye los servicios y las herramientas que Microsoft y los clientes utilizan para administrar y supervisar los dispositivos móviles, los equipos de escritorio, las máquinas virtuales, los dispositivos incrustados y los servidores.

Equipos colaboradores

Continuación

Administración de riesgos empresariales: un equipo que trabaja en varias unidades de negocio para priorizar los debates sobre riesgos con los directivos sénior de Microsoft. ERM conecta varios equipos de riesgo operativo, administra el marco de riesgos empresariales de Microsoft y facilita la evaluación de seguridad interna de la empresa mediante el marco de ciberseguridad NIST.

Directiva de ciberseguridad global: un equipo que colabora con gobiernos, ONG y partners del sector para impulsar políticas públicas de ciberseguridad que permitan a los clientes reforzar su seguridad y resiliencia al adoptar y usar la tecnología de Microsoft.

Seguridad de acceso de identidad y red (IDNA): un equipo que trabaja para proteger a todos los clientes de Microsoft del acceso no autorizado y el fraude. IDNA Security es un equipo multidisciplinar de ingenieros, jefes de producto, científicos de datos e investigadores de seguridad.

Seguridad de M365: una organización que desarrolla soluciones de seguridad como Microsoft Defender para punto de conexión (MDE), Microsoft Defender for Identity (MDI) y otras, para proteger a los clientes empresariales.

IA y ética de Microsoft y su impacto en la ingeniería e investigación (AETHER): un consejo asesor de Microsoft cuyo objetivo es garantizar que las nuevas tecnologías se desarrollen y se desplieguen de una manera responsable.

Microsoft Bing Search y distribución: un equipo dedicado a proporcionar un motor de búsqueda en Internet de primera clase, que permita a usuarios de todo el mundo encontrar resultados de búsqueda e información fiables rápidamente, incluido el seguimiento de los temas y las tendencias relevantes, al tiempo que ofrece a los usuarios el control de su privacidad.

Soluciones para clientes y partners de Microsoft: la organización comercial unificada de Microsoft responsable de las funciones sobre el terreno, como los especialistas y asesores en seguridad y ventas técnicas.

Microsoft Defender Experts: la organización mundial más grande de Microsoft de investigadores de seguridad centrados en productos, científicos aplicados y analistas de inteligencia de amenazas. Defender Experts ofrece funciones innovadoras de detección y respuesta en los productos de seguridad de Microsoft 365 y servicios administrados de Microsoft Defender Experts.

Microsoft Defender para IoT: un equipo compuesto por investigadores expertos especializados en ingeniería inversa de malware, protocolos y firmware de IoT/OT. El equipo busca las amenazas del IoT/OT para descubrir tendencias y campañas malintencionadas.

Inteligencia sobre amenazas de Microsoft Defender (RiskIQ): un equipo que produce inteligencia táctica a través del análisis de la amplia colección de telemetría externa de Microsoft, cartografiando el panorama de amenazas a medida que evoluciona para descubrir una infraestructura de amenazas previamente desconocida y añadiendo contexto a los actores de amenazas y las campañas. El equipo publica periódicamente investigaciones puntuales y específicas para ofrecer inteligencia táctica crucial a los defensores.

Equipo de desarrollo empresarial de seguridad de Microsoft: un equipo que lidera la estrategia de crecimiento de ciberseguridad, las asociaciones y las inversiones estratégicas de Microsoft.

Centro de respuesta de seguridad de Microsoft (MSRC): un equipo que trabaja con investigadores de seguridad para proteger el ecosistema de clientes y partners de Microsoft. Como parte integrante del Centro de operaciones de ciberdefensa de Microsoft (CDOC), el MSRC reúne a expertos en respuesta de seguridad para proteger de las amenazas y responder a ellas en tiempo real.

Servicios de seguridad de Microsoft para la respuesta a incidentes: un equipo de expertos en ciberseguridad que ayuda a los clientes durante todo un ciberataque, desde la investigación hasta las actividades de contención y recuperación relacionadas. Los servicios se ofrecen a través de dos equipos estrechamente integrados, el equipo de detección y respuesta (DART), centrado en la investigación y las bases para la recuperación, y la práctica de seguridad de recuperación de riesgos (CRSP), que se centra en los aspectos de contención y recuperación.

Centro de inteligencia sobre amenazas de Microsoft (MSTIC): un equipo dedicado a identificar, rastrear y recopilar inteligencia relativa a los adversarios más avanzados que afectan a los clientes de Microsoft, incluidas las amenazas de los estados-nación, el malware y el phishing.

One Engineering System (1ES): un equipo con la misión de ofrecer herramientas de primera clase para ayudar a los desarrolladores de Microsoft a ser lo más productivos y seguros posibles. El equipo lidera la estrategia central para proteger la cadena de suministro de software completa de Microsoft.

Centro de inteligencia sobre amenazas operativas (OpTIC): el equipo responsable de administrar y difundir la inteligencia sobre amenazas cibernéticas que respalda la misión del Centro de operaciones de ciberdefensa de Microsoft (CDOC) para proteger a Microsoft y a nuestros clientes.

Microsoft

Aportar luz al panorama de amenazas y permitir una defensa digital.

- Obtén más información: **https://microsoft.com/mddr**
- Conoce los detalles: **https://blogs.microsoft.com/on-the-issues/**
- Mantente conectado: **@msftissues and @msftsecurity**