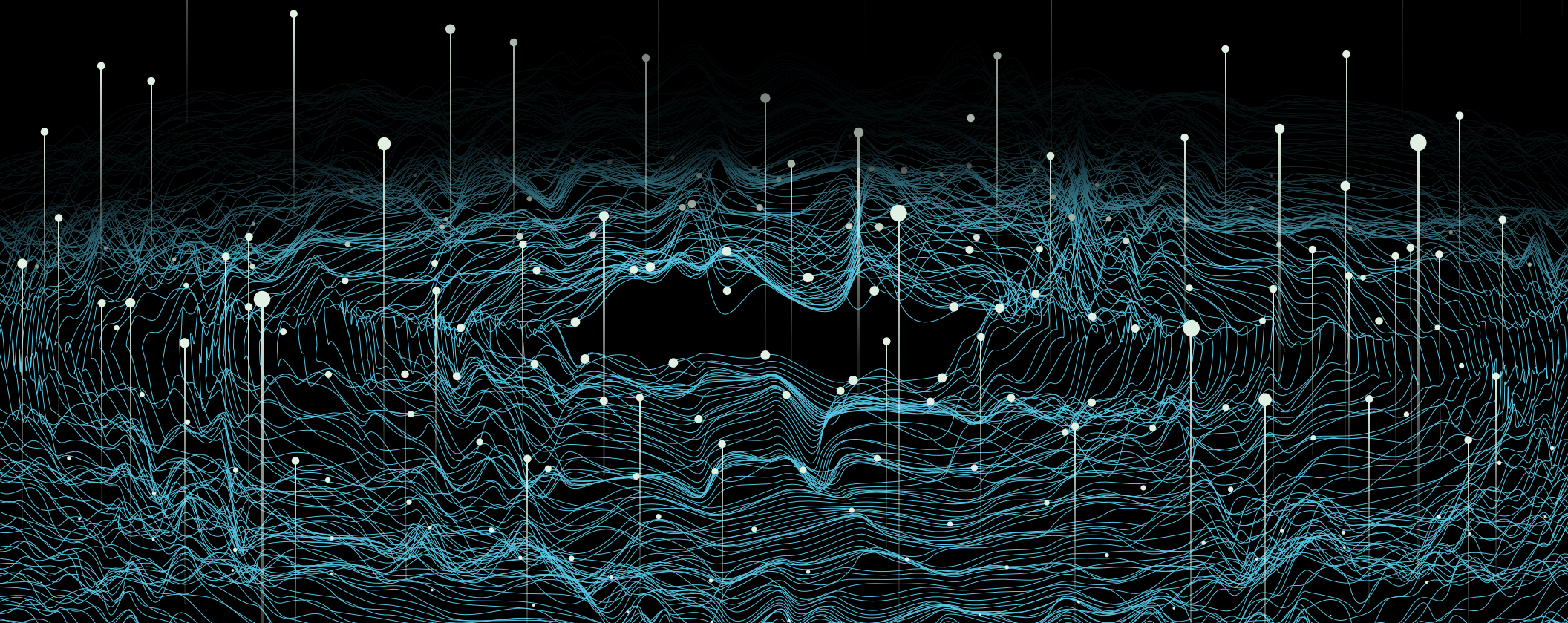
Microsoft

INFORME DE INTELIGENCIA DE SEGURIDAD DE MICROSOFT

VOLUMEN 24
ENERO A DICIEMBRE DE 2018



Índice

Autores y colaboradores

Abhishek Agrawal
Protección de la información

David Fantham
Protección de la información

Debraj Ghosh
Marketing de seguridad de Microsoft

Diana Kelley
Grupo de soluciones de ciberseguridad

Elia Florio
Windows Active Defense

Eric Avena
Equipo de investigación de Windows Defender

Eric Douglas
Equipo de investigación de Windows Defender

Francis Tan Seng
Equipo de investigación de Windows Defender

Jonathan Trull
Grupo de soluciones de ciberseguridad

Joram Borenstein
Grupo de soluciones de ciberseguridad

Karthik Selvaraj
Equipo de investigación de Windows Defender

Kasia Kaplinska
Marketing de seguridad de Microsoft

Kristina Laidler
Respuesta ante incidentes de seguridad

Matt Duncan
Ingeniería y análisis de datos de Windows Active Defense

Mark Simos
Grupo de soluciones de ciberseguridad

Paul Henry
Wadeware LLC

Pragya Pandey
Marketing de seguridad de Microsoft

Ram Pliskin
Azure Security

Ryan McGee
Marketing de seguridad de Microsoft

Seema Kathuria
Grupo de soluciones de ciberseguridad

Steve Wacker
Wadeware LLC

Tanmay Ganacharya
Equipo de investigación de Windows Defender

Volv Grebennikov
Bing

Yaniv Zohar
Azure Security

Prólogo

Hola y bienvenido a la 24.ª edición del Informe de inteligencia de seguridad de Microsoft (SIR). Como profesional y arquitecto de seguridad, leo informes como este con la esperanza de entender un poco mejor el panorama con la adopción de consejos prácticos sobre cómo usar ese conocimiento para defender y proteger a las organizaciones de manera más efectiva.

El equipo del SIR aporta a este informe el espíritu de la formación para mejorar la resistencia cibernética y ha examinado todo un año de datos para extraer las lecciones más importantes.

Lo que estás leyendo son los conocimientos extraídos de un año de análisis de datos de seguridad y lecciones prácticas aprendidas. Entre los datos analizados se incluyen los 6,5 billones de señales de amenazas que pasan por el cloud de Microsoft cada día, y la investigación y las experiencias reales de nuestros miles de investigadores de seguridad y equipos de intervención inmediata en todo el mundo. En 2018, los atacantes utilizaron diferentes artimañas, tanto nuevas (minería de moneda o coin-mining) como antiguas (suplantación de identidad o phishing), en su búsqueda continua de robar datos y recursos a clientes y organizaciones. Los ataques híbridos, como la campaña Ursnif, combinaban enfoques sociales y técnicos. A medida que los defensores actuaron de forma más inteligente contra el ransomware, una forma de ataque llamativa y perturbadora, los delincuentes se inclinaron por la más "sigilosa", pero rentable, minería de moneda.

Ese cambio puede resultar frustrante, como si los atacantes estuvieran siempre un paso por delante. Pero visto con otra perspectiva, la historia es positiva en este caso. Los defensores y los profesionales de la ciberseguridad como tú implementaron técnicas defensivas que obligaron a los atacantes a cambiar sus cargas útiles preferidas y a apartarse del ransomware.

Otra área en la que los ciberdelincuentes incrementaron su actividad es la cadena de suministro. Uno de los más destacados, el ataque de minería de moneda Dofoil, que se produjo el 6 de marzo de 2018, se inició mediante una aplicación punto a punto infectada. Los problemas de la cadena de suministro fueron más allá de las aplicaciones y se extendieron al cloud e incluyeron extensiones de navegador maliciosas, repositorios Linux comprometidos y varias instancias de módulos con puerta trasera. Para hacer frente a esta amenaza, las organizaciones están avanzando hacia un modelo de cadena de suministro transparente y fiable.

Los datos son excelentes, pero a veces ayudan a averiguar lo que realmente ha sucedido en una organización. Por ese motivo hemos incluido las lecciones aprendidas in situ de nuestro equipo de detección y respuesta (DART). Entre ellas se incluye cómo una gran empresa de fabricación pudo implementar controles para bloquear una campaña de suplantación de identidad (phishing) en varias fases que los había estado asediando durante meses, y las organizaciones de servicios financieros que finalmente pudieron erradicar los agentes de amenazas de sus sistemas mediante herramientas de investigación avanzadas y supervisión de puntos de conexión.

Por último, aunque no menos importante, los clics de suplantación de identidad (phishing) continuaron aumentando, pero los modelos de machine learning están mejorando la captura de la suplantación antes de que lleguen al usuario y la prevención de daños en caso de haber hecho clic. ¿Más buenas noticias? Cada vez son más las empresas que implementan soluciones multifactor para limitar el alcance del robo de credenciales en los correos electrónicos de suplantación de identidad (phishing).

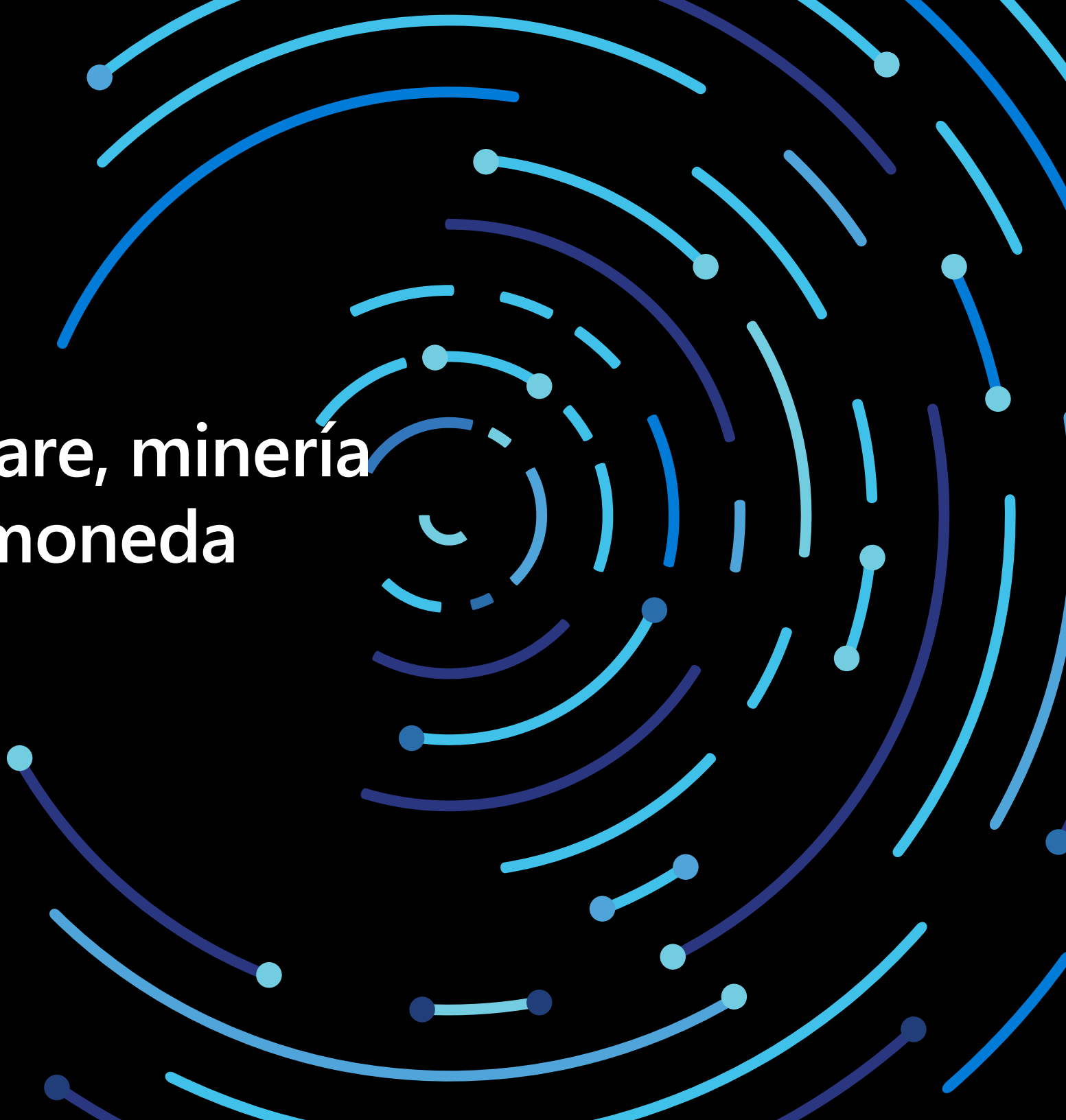
Los atacantes buscan oportunidades; por lo tanto, cuanto más sepamos sobre sus técnicas y oficio, mejor preparados estaremos para crear defensas y responder rápidamente. Los pequeños pasos importantes pueden suponer una gran diferencia en el estado general de la ciberseguridad de una organización. Por eso, junto con un profundo conocimiento del cambiante panorama del malware y los ataques, encontrarás pasos recomendados y otras guías de prácticas recomendadas en este informe, ya que es eso exactamente lo que necesitaba en mi lucha contra los delincuentes cuando era una especialista. Esperamos que sea lo que tú necesitas también.

Diana Kelley
Directora tecnológica de servicio in situ de ciberseguridad de Microsoft

P.D. Siempre queremos mejorar el SIR. Si tienes algún comentario, ponte en contacto con nosotros y danos tu opinión.

SECCIÓN I

Ransomware, minería de criptomoneda y dinero



El ransomware intervino en los casos de seguridad más importantes de 2017. Los ataques notables de WannaCrypt y Petya en todo el mundo impulsaron la sensibilización general del ransomware (un tipo de malware que bloquea o cifra los ordenadores y, después, exige dinero para devolver el acceso) y muchos especularon con que no dejaría de aumentar en el futuro. Por el contrario, los encuentros de ransomware disminuyeron considerablemente en 2018.

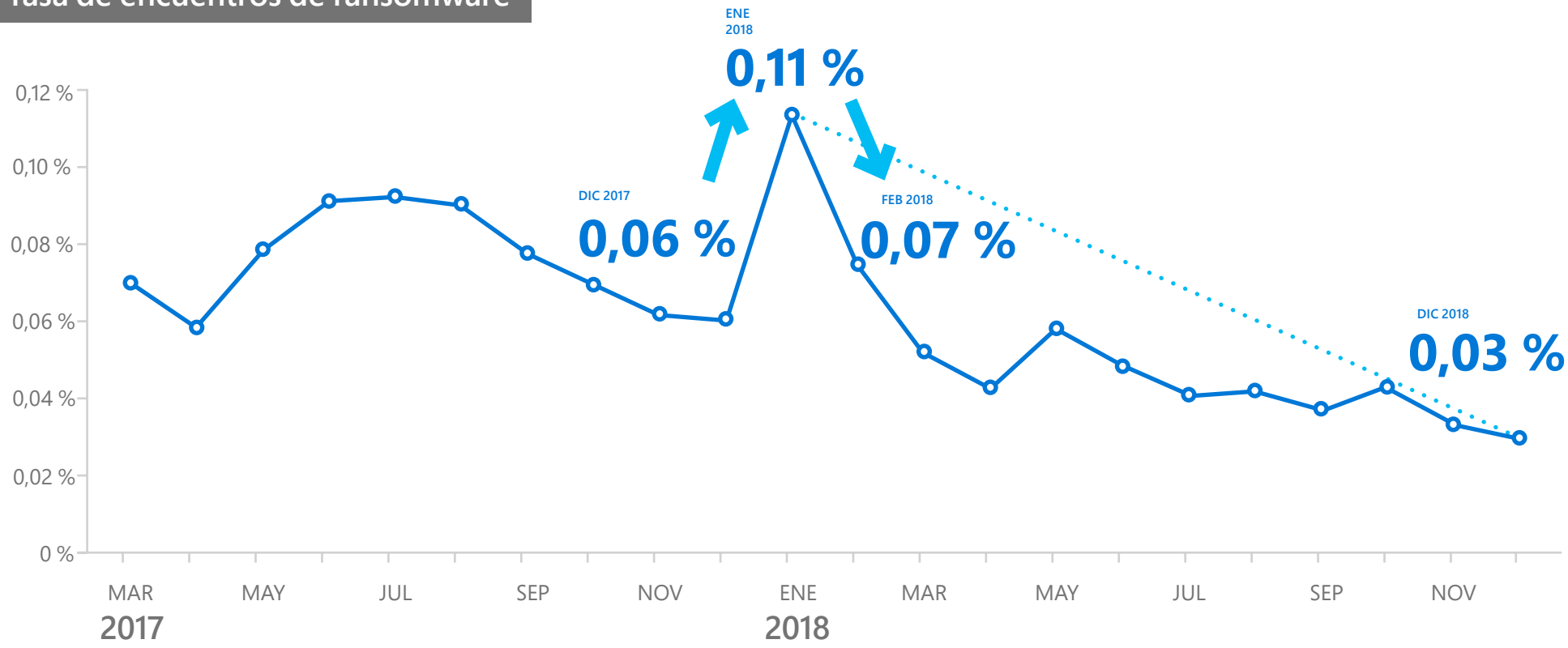
La disminución de los encuentros de ransomware se ha debido en parte a la mejora de la detección y la información, lo que dificultó que los atacantes obtuvieran provecho. Por consiguiente, los atacantes comenzaron a desplazar sus esfuerzos del ransomware a enfoques como la minería de criptomoneda, que utiliza los recursos informáticos de las víctimas con el fin de ganar dinero digital para los atacantes. Este cambio demuestra la naturaleza fundamentalmente oportunista de la mayoría de los ciberdelincuentes con fines de lucro: tienden a perseguir el dinero más fácil disponible y, cuando la economía del ciberdelito cambia, se apresuran a seguir adelante.

ATAQUES DE RANSOMWARE EN DECLIVE

Hace más de una década, los hackers y los bromistas que dominaban la clandestinidad del primer malware fueron suplantados por el crimen organizado y otros intereses con fines de lucro. Aunque los primeros ataques de malware solían ser llamativos y evidentes, el malware orientado a beneficios tenía muchas más probabilidades de funcionar de forma silenciosa y evitar llamar la atención, a fin de seguir desempeñando su función (enviar correo no deseado, robar información confidencial, llevar a cabo ataques de denegación de servicio y otras actividades maliciosas) el mayor tiempo posible.

El ransomware se resistió a esta tendencia. En lugar de intentar pasar desapercibido, el ransomware niega abiertamente a las víctimas el acceso a sus ordenadores y archivos importantes hasta que paguen el rescate (y a menudo incluso después; los atacantes no suelen liberar su control de los ordenadores incluso después de que se haya pagado el rescate). Cuando el ransomware alcanzaba su punto máximo en 2017, parecía que este estilo de ataque abierto podría representar una nueva fase en las técnicas de ataque. Pero los datos más recientes sugieren que el ransomware podría estar en declive, ya que los atacantes vuelven cada vez más al modo de operación más sigiloso que han empleado en el pasado, con la finalidad de pasar desapercibidos para llevar a cabo de forma más efectiva ataques como la minería de criptomoneda. Aunque ha habido un descenso en la tasa de encuentros de ransomware, esto no significa necesariamente que haya disminuido la gravedad de los ataques.

Tasa de encuentros de ransomware



Las tasas de encuentros de ransomware disminuyeron aproximadamente un 60 por ciento entre marzo de 2017 y diciembre de 2018, con aumentos intermitentes durante ese período.

Probablemente hay muchas causas para este declive general, aunque los investigadores de seguridad de Microsoft sospechan que un factor principal es que tanto los usuarios finales como las organizaciones están adquiriendo más consciencia y están tratando de forma más inteligente las amenazas de ransomware, incluido el ejercicio de una mayor cautela y la realización de copias de seguridad de los archivos importantes para que se puedan restaurar si se cifran mediante ransomware. Además, tal como se ha indicado antes, los ciberdelincuentes son oportunistas.

FIGURA 1.

Encuentros de ransomware de marzo de 2017 a diciembre de 2018

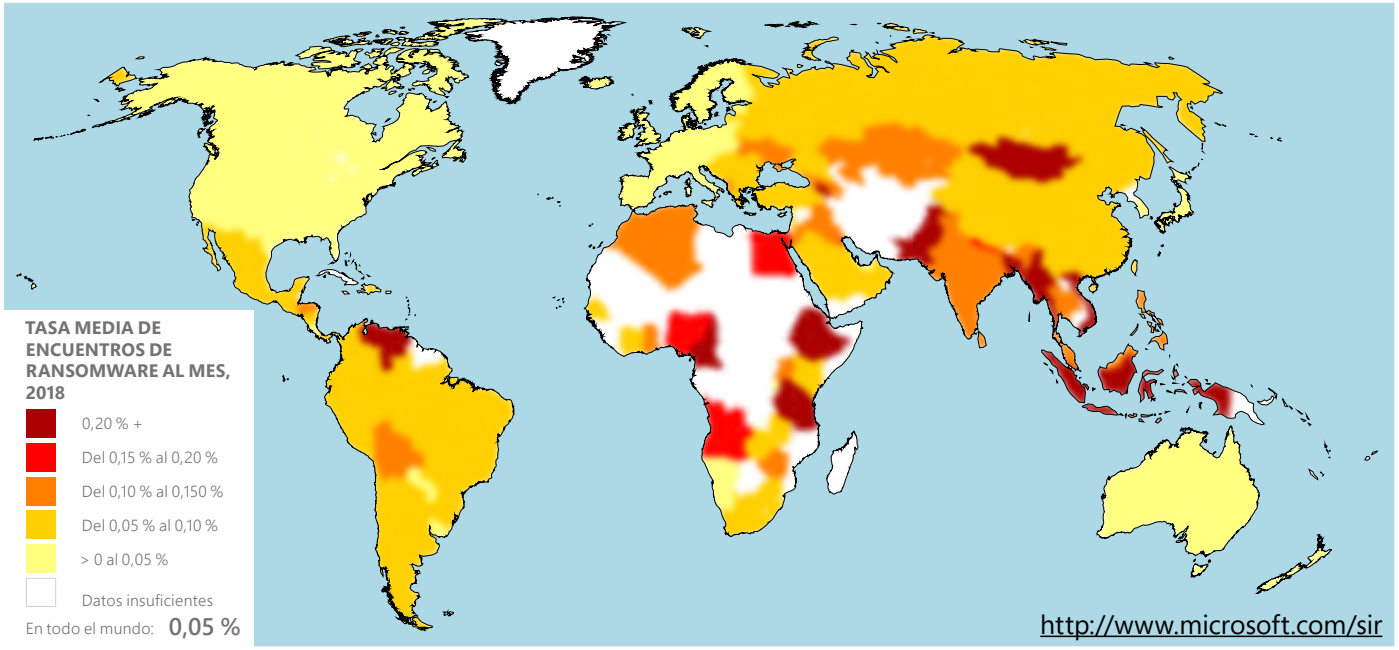
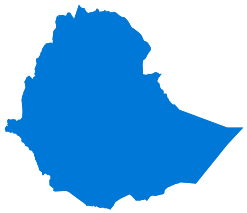


FIGURA 2.

Media mensual de tasas de encuentros de ransomware en todo el mundo, por país o región, en 2018

PAÍS MÁS AFECTADO POR RANSOMWARE: ETIOPÍA



Tasa media de encuentros al mes: **0,77 %**

Los cinco lugares con las tasas medias mensuales más altas de encuentros de ransomware en 2018 fueron Etiopía (0,77 por ciento), Mongolia (0,46), Camerún (0,41), Birmania (0,33) y Venezuela (0,31), cada uno de los cuales tuvo una tasa media mensual de encuentros de ransomware del 0,31 por ciento o más durante el período.1 Hace unos años, los encuentros de ransomware tendían a agruparse en países y regiones ricos de Europa y Norteamérica, pero, a medida que el ransomware ha empezado a perder el favor de los atacantes, el patrón de encuentros se ha ido pareciendo más al del malware en su conjunto.

Los lugares con las tasas más bajas de encuentros de ransomware en 2018 fueron Irlanda (0,01), Japón (0,01), Estados Unidos (0,02), Reino Unido (0,02) y Suecia (0,02 por ciento), cada uno de los cuales tuvo una tasa media mensual de encuentros de ransomware del 0,02 por ciento o menos durante el mismo período. Los lugares con tasas de encuentros bajas tienden a tener infraestructuras de ciberseguridad maduras y programas bien establecidos para proteger la infraestructura crítica y comunicarse con sus ciudadanos sobre la seguridad básica.

NOTAS AL PIE

[1] La tasa de encuentros es el porcentaje de ordenadores que ejecutan productos de seguridad en tiempo real de Microsoft que informan de un encuentro de malware. El encuentro de una amenaza no implica que el ordenador haya sido infectado. A la hora de calcular las tasas de encuentro, tan solo se tienen en cuenta los ordenadores cuyos usuarios hayan aceptado proporcionar datos a Microsoft.

MINERÍA DE CRIPTOMONEDA EN AUGE

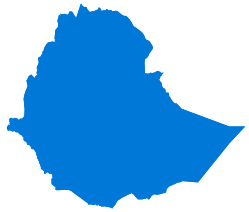
La criptomoneda es dinero virtual que se puede utilizar para comprar y vender bienes y servicios de forma anónima, tanto online como en el mundo físico. Existen muchos tipos diferentes de criptomonedas, pero todas se basan en la tecnología de blockchain, en la que cada transacción se registra en un libro mayor distribuido que mantienen miles o millones de ordenadores en todo el mundo. Las nuevas monedas se crean, o "extraen", mediante ordenadores que realizan cálculos complejos que también sirven para verificar las transacciones de blockchain.

La minería de moneda puede ser muy lucrativa (en 2018, un solo bitcóin, la criptomoneda más antigua y popular, valía varios miles de dólares estadounidenses), pero la realización de los cálculos necesarios puede requerir muchos recursos y aumentan a medida que se extrae cada nueva moneda. Para las monedas populares como el bitcóin, la minería de moneda rentable es casi imposible si no se accede a inmensos recursos informáticos que están fuera del alcance de la mayoría de los individuos y grupos pequeños. Por este motivo, los atacantes que buscan ganancias ilícitas han recurrido cada vez más al malware con el que pueden utilizar los ordenadores de las víctimas para ayudarlos a la minería de criptomoneda. Este enfoque les permite aprovechar la potencia de procesamiento de cientos de miles de ordenadores en lugar de uno o dos. Aunque se descubra una infección menor, la naturaleza anónima de la criptomoneda complica los esfuerzos para localizar a los responsables.

En 2018, la media mundial mensual de la tasa de encuentros de minería de criptomoneda fue del 0,12 por ciento, comparado con solo el 0,05 por ciento correspondiente al ransomware. Muchos factores contribuyen a la creciente popularidad de la minería como carga útil para el malware. A diferencia del ransomware, la minería de criptomoneda no requiere la intervención del usuario: trabaja en segundo plano, mientras el usuario realiza otras tareas o no está delante del ordenador y no se puede percibir en absoluto a menos que degrade lo suficiente el rendimiento del ordenador. En consecuencia, es menos probable que los usuarios tomen medidas para eliminar la amenaza y podría continuar con la minería en beneficio del atacante durante un período de tiempo prolongado.

La tendencia también se ve impulsada por la disponibilidad de productos "integrados" para la minería encubierta de muchas criptomonedas. La barrera de entrada es baja debido a la amplia disponibilidad de software para la minería de moneda, que los ciberdelincuentes reempaquetan como malware para distribuirlo a los ordenadores de los usuarios desprevenidos. Los mineros armados se distribuyen a las víctimas utilizando muchas de las técnicas que los atacantes utilizan para distribuir otras amenazas, como ingeniería social, vulnerabilidades de seguridad y descargas ocultas. Una vez instalado el software de minería, se ejecuta en segundo plano en los ordenadores de las víctimas para realizar los cálculos de blockchain y el atacante recoge la recompensa.

MEDIA DE TASAS MENSUALES DE ENCUENTROS DE LOS PAÍSES MÁS AFECTADOS POR LA MINERÍA DE CRIPTOMONEDA



Etiopía: **5,58 %**

Tanzania: **1,83 %**

Pakistán: **1,47 %**

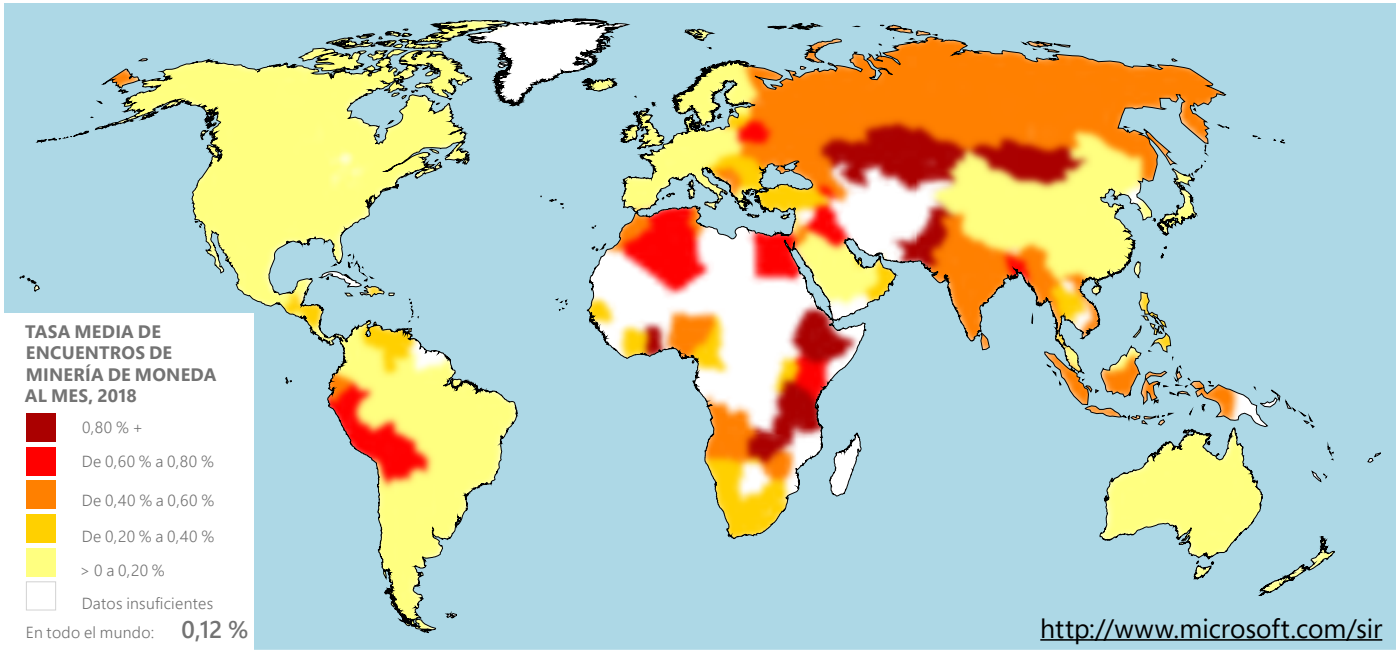


FIGURA 3.

Media mensual de tasas de encuentros de minería de moneda en todo el mundo, por país o región, en 2018

MEDIA MENSUAL DE TASAS DE ENCUENTROS DE LOS PAÍSES MENOS AFECTADOS POR LA MINERÍA DE CRIPTOMONEDA

Irlanda: 0,02 %

Japón: 0,02 %

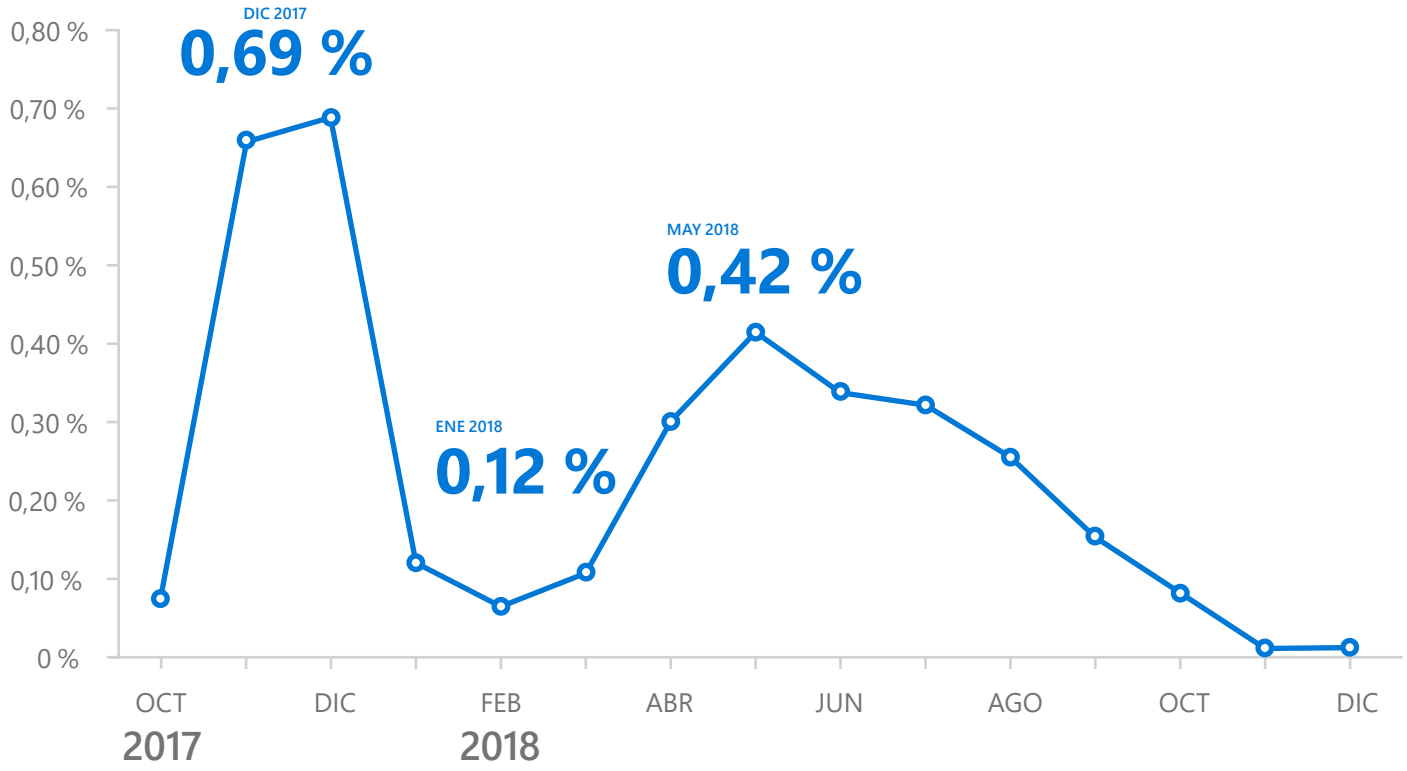
Estados Unidos: 0,02 %

Los cinco lugares con las mayores tasas de encuentros de minería de criptomoneda en 2018 fueron Etiopía (5,58), Tanzania (1,83), Pakistán (1,47), Kazajistán (1,24) y Zambia (1,13), cada uno de los cuales tuvo una tasa media mensual de encuentros de minería de moneda de aproximadamente el 1,13 por ciento o más durante el período. Los lugares con las tasas de encuentros de minería de moneda más bajas en 2018 fueron Irlanda, Japón, Estados Unidos y China, cada uno de los cuales tuvo una media de tasa mensual de encuentros de minería de moneda de aproximadamente 0,02 por ciento durante el período.

MINEROS DE CRIPTOMONEDA BASADOS EN NAVEGADORES: UN NUEVO TIPO DE AMENAZA

Las estadísticas presentadas en esta sección hacen referencia a mineros de criptomoneda maliciosos que están diseñados para instalarse en los ordenadores de las víctimas como malware. Pero algunas de las amenazas más significativas de minería de criptomoneda se basan completamente en navegadores web y no es necesario instalarlas. Una serie de servicios anuncian la minería de criptomoneda basada en navegador como una manera para que los propietarios de sitios web moneticen el tráfico a sus sitios sin depender de la publicidad. Los propietarios de los sitios deben añadir código JavaScript a sus páginas para realizar la minería de criptomoneda en segundo plano mientras

Tasa de encuentros de brocoiner



un usuario visita el sitio y las ganancias se dividen entre el propietario del sitio y el servicio. Lamentablemente, los atacantes se han apresurado a aprovecharse de estos servicios para efectuar la minería de criptomoneda sin obtener el consentimiento de los usuarios finales, a menudo comprometiendo sitios web legítimos e insertando maliciosamente el código de minería en su código fuente. Estos sistemas de minería basados en navegador no tienen que poner en peligro el ordenador del usuario final en absoluto y se ejecutan en cualquier plataforma con un navegador web compatible con JavaScript. Al igual que los troyanos de minería de criptomoneda, los sistemas de minería basados en navegador pueden degradar considerablemente el rendimiento del ordenador y desperdiciar electricidad mientras un usuario visita una página web afectada.

FIGURA 4.

Tasa de encuentros de Brocoiner, el sistema de minería de criptomoneda basado en navegador más frecuente

EL IMPACTO DE LA MINERÍA DE CRIPTOMONEDA NO SOLICITADA

La amenaza más obvia a la que se enfrentan las víctimas de la minería de criptomoneda maliciosa es el consumo de recursos informáticos, que puede desperdiciar electricidad y degradar significativamente el rendimiento de los ordenadores. Los usuarios y las organizaciones también se enfrentan a otros riesgos de la minería de moneda, entre los que se incluyen:

- **Obtener un punto de apoyo para hacer más daño en el futuro.** Al igual que otras formas de malware, la minería de criptomoneda puede ser un punto de entrada para los atacantes. Mientras el ordenador ejecuta la minería de criptomoneda en segundo plano, los ciberdelincuentes pueden obtener información del entorno y posiblemente descubrir brechas de seguridad para aprovecharlas con otros fines.

- **Los dispositivos conectados a Internet pueden verse comprometidos y convertirse en bots para la minería de criptomoneda.** Muchos de estos dispositivos carecen de seguridad incorporada, como la detección de amenazas de malware, lo que puede hacerlos objetivos deseables para los atacantes.

- **Perjudicar los equipos.** El software de minería de criptomoneda que se ejecuta continuamente durante meses o más puede perjudicar el rendimiento, y el calor generado por el consumo excesivo de energía y la utilización de la CPU puede dañar los ordenadores.

SECCIÓN II

Cadenas de suministro de software en peligro

Durante años, Microsoft ha estado rastreando a los atacantes que utilizan la cadena de suministro comprometida como punto de entrada para los ataques. En un ataque a la cadena de suministro, el atacante se concentra en comprometer el proceso de desarrollo o actualización de un editor de software legítimo.

Si tiene éxito, el atacante puede incorporar un componente comprometido en una aplicación legítima o en un paquete de actualización que después se distribuye a los usuarios del software. El código malicioso se ejecuta con la misma confianza y los mismos permisos que el software. El aumento del número de ataques a la cadena de suministro de software en los últimos años se ha convertido en un tema importante en muchas conversaciones sobre ciberseguridad y es un foco principal de preocupación en muchos departamentos de TI.

PRINCIPALES ATAQUES A LA CADENA DE SUMINISTRO DE SOFTWARE EN 2017

▲ **FIGURA 5.**

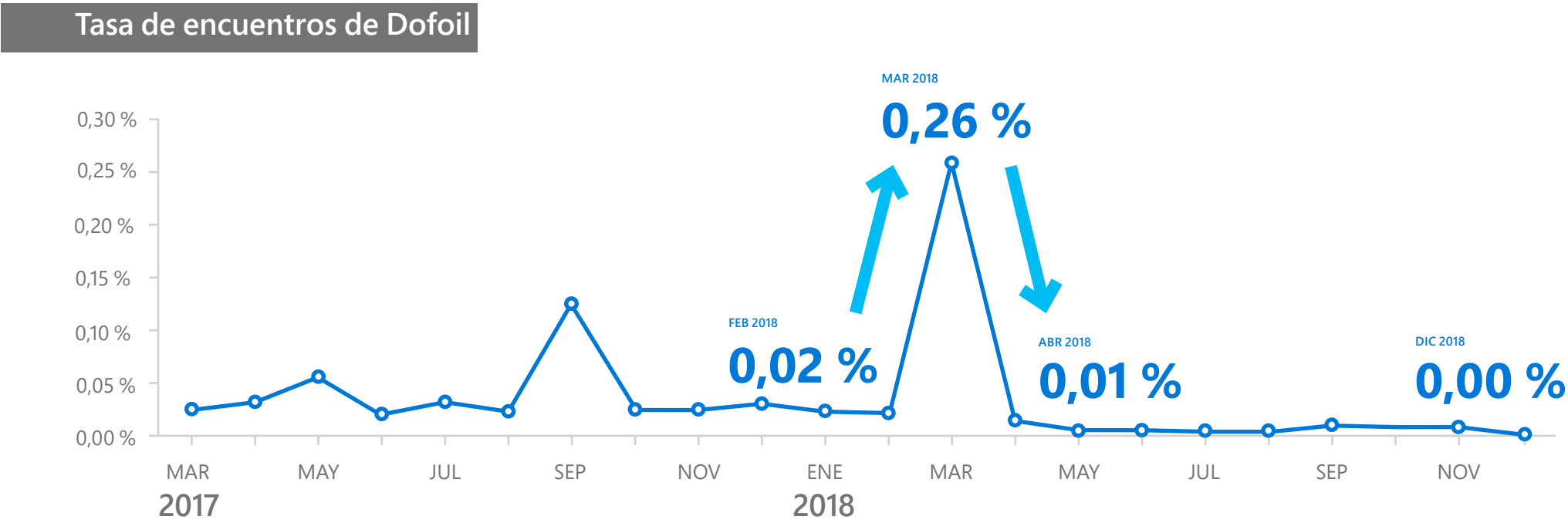
Ataques a la cadena de suministro de software en 2017 y 2018

En 2017, los ataques a la cadena de suministro fueron responsables de una serie de incidentes importantes, especialmente el ataque del ransomware Petya en junio, que se remonta a infecciones iniciales de un proceso de actualización comprometido de una aplicación de contabilidad fiscal popular en Ucrania. En mayo, Operation WilySupply comprometió la actualización del software de un editor de texto para instalar una puerta trasera en las organizaciones objetivo de los sectores financiero y de TI. En julio, una puerta trasera llamada ShadowPad estaba oculta en un paquete de software de administración de servidores y permitía a los atacantes instalar cargas de malware adicionales para el robo de datos y otras actividades maliciosas. En septiembre, la infraestructura de la popular herramienta freeware CCleaner se vio comprometida y se entregó una versión con puerta trasera a su base de usuarios.

El primer incidente importante en la cadena de suministro de software de 2018 sucedió el 6 de marzo, cuando Windows Defender ATP bloqueó una campaña masiva para entregar el troyano Dofoil (también conocido como Smoke Loader). Se rastreó la campaña masiva de malware hasta una aplicación punto a punto envenenada. El paquete de actualización de la aplicación se reemplazó por uno malicioso que descargaba código comprometido, el cual instaló el malware Dofoil. El sofisticado troyano llevaba una carga para la minería de moneda y presentaba técnicas avanzadas de inserción de procesos cruzados, mecanismos de persistencia y métodos de evasión.

FIGURA 6.

La tendencia de los encuentros de Dofoil (Smoke Loader) en 2018 muestra un pico de casos bloqueados en marzo



En las primeras 12 horas de la campaña, el antivirus de Windows Defender bloqueó más de 400.000 intentos de infección en todo el mundo. Rusia representó el 73 % de los encuentros mundiales, mientras que Turquía y Ucrania registraron el 18 % y el 4 %, respectivamente.

Se detectaron varios ataques más utilizando cadenas de suministro de software comprometidas como mecanismos de entrega en 2018, incluidos los que se describen en la siguiente tabla:

FIGURA 7.

Otros ataques a la cadena de suministro de software en 2018

Periodo	Ataque	Descripción	Software afectado
Marzo de 2018	Campaña de minería de moneda de Dofoil (registrado por Microsoft)	Los atacantes infectaron el proceso de actualización de una aplicación punto a punto para instalar Dofoil, que a su vez instaló malware de minería de moneda.	Aplicación punto a punto
Julio de 2018	Cadena de suministro comprometida dentro de una cadena de suministro (registrado por Microsoft)	Los atacantes comprometieron la infraestructura compartida entre el proveedor de una aplicación de editor PDF y uno de sus partners proveedores de software.	Aplicación de editor PDF y proveedor partner externo
Agosto de 2018	Programa de soporte remoto comprometido (Operation Red Signature, registrado por Trend Micro e IssueMakersLab)	El servidor de actualizaciones de un proveedor de soluciones de soporte remoto se vio comprometido al entregar una herramienta de acceso remoto llamada 9002 RAT.	Programa de soporte remoto
Octubre de 2018	Solución de panel de control de hosting comprometida (registrado por ESET)	Se modificó el script de instalación para una solución de panel de control de hosting para robar credenciales.	Solución de panel de control de hosting

CONFIANZA EN PELIGRO

Los ataques a la cadena de suministro son insidiosos porque se aprovechan de la confianza que los usuarios y los departamentos de TI depositan en el software que utilizan. El software comprometido a menudo está firmado y certificado por el proveedor, y puede no dar ninguna señal de que algo esté mal, lo que hace que sea considerablemente más difícil detectar la infección. Pueden dañar la relación entre las cadenas de suministro y sus clientes, ya sean empresas o usuarios domésticos. Al infectar el software y socavar las infraestructuras de entrega o actualización, los ataques a la cadena de suministro pueden afectar a la integridad y seguridad de los bienes y servicios que proporcionan las organizaciones.

Los ataques a la cadena de suministro han afectado a una amplia variedad de programas de software y organizaciones objetivo en diferentes sectores y ubicaciones geográficas. La amenaza de ataques a la cadena de suministro es un problema que afecta a todo el sector y que requiere la atención de múltiples partes interesadas, incluidos los desarrolladores y proveedores de software que escriben el código, los administradores de sistemas que administran las instalaciones de software y la comunidad de seguridad de la información que encuentra estos ataques y crea soluciones para proteger a las personas y al software de ellos.

MÁS ALLÁ DEL SOFTWARE: COMPROMETER LA CADENA DE SUMINISTRO A TRAVÉS DE OBJETOS EN EL CLOUD

La capacidad de los ataques a la cadena de suministro para socavar la confianza se amplifica y resulta más compleja en el cloud. Varios incidentes de objetos, servicios e infraestructura en el cloud comprometidos en 2018 ponen de manifiesto esta complejidad:

- Extensiones de Chrome infectadas que instalaron programas maliciosos para estafar a los usuarios (registrado por ICEBRG)
- Varios repositorios Linux comprometidos (registrado en algunos foros online)
- Complementos de WordPress maliciosos usados para varias actividades maliciosas, incluido permitir a los atacantes publicar contenido en sitios de WordPress (registrado por Wordfence)
- Imágenes de Docker maliciosas que contenían un script para descargar malware de minería de criptomonedas y se cargaban en la cuenta de Docker Hub (registrado por Fortinet y Kromtech)
- Un paquete "typosquatting" en el repositorio oficial de Python; el paquete contenía un script malicioso que descarga el malware utilizado para secuestrar direcciones de minería de moneda en el portapapeles (registrado en Medium)
- Script comprometido en StatCounter que permitía a los atacantes inyectar un script malicioso en los sitios web que utilizan StatCounter (registrado por ESET)
- Varios incidentes de módulos npm con puerta trasera (The npm Blog, Medium) que, si se aprovechan, pueden dar lugar a situaciones como, por ejemplo, que un atacante pueda introducir código arbitrario en un servidor en funcionamiento y ejecutarlo

Estos incidentes demuestran cómo la cadena de suministro comprometida puede ampliar enormemente una superficie de ataque. Si no están protegidos, los objetos en el cloud pueden ser vías de entrada inesperadas. Por ejemplo, en el incidente de Docker Hub intervino una cuenta maliciosa que subía imágenes de Docker con una puerta trasera oculta para la minería de moneda. Las imágenes de Docker estuvieron hospedadas en Docker Hub durante casi un año y se descargaron millones de veces y las utilizaron administradores y usuarios desprevenidos.

Los riesgos de la cadena de suministro se extienden al código en el cloud, código abierto, bibliotecas web, contenedores y otros objetos en el cloud. Estos riesgos, junto con el alto grado de variación entre los incidentes de cadena de suministro de software y hardware que han salido a la luz, convierten a este tipo de ataques en una categoría de amenaza amplia. Aunque no existe una solución única para todo el espectro de este tipo de ataques, las organizaciones necesitan crear una protección preventiva y una detección posterior a la infracción de los ataques a la cadena de suministro desde proveedores de hardware y software, proveedores y adquisiciones, proveedores de software de código abierto comprometidos, así como servicios de cloud y proveedores de infraestructura.

Investigación de incidentes cibernéticos con DART

El equipo de detección y respuesta (DART) de Microsoft es un equipo global de expertos en ciberseguridad y de respuesta a incidentes que ayuda a las organizaciones en la detección, investigación y respuesta a incidentes de ciberseguridad. En esta sección se destacan algunos de los casos prácticos de clientes que DART abordó el año pasado; ilustra las tendencias comunes de los atacantes y cómo Microsoft y los clientes pudieron frustrarlas.

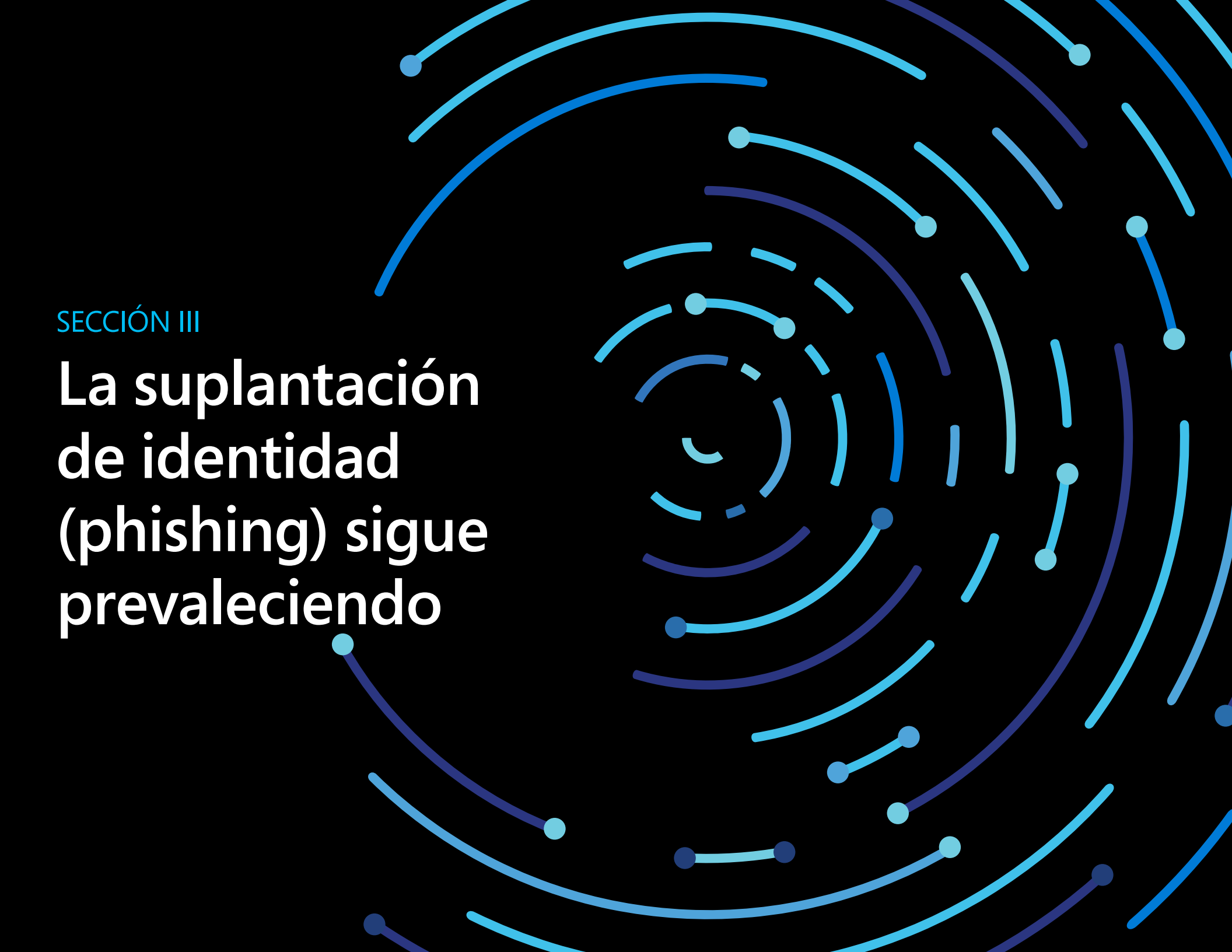
UNA ORGANIZACIÓN DE SERVICIOS PROFESIONALES SUFRIÓ UN ATAQUE DE ESTADO NACIONAL QUE EXTRAJO DATOS

Una organización de servicios profesionales se vio afectada por una sofisticada amenaza avanzada y persistente (APT) patrocinada por el estado que obtuvo acceso a las credenciales con privilegios de la organización. Los atacantes obtuvieron acceso a la red mediante un ataque de difusión de contraseñas, en el que utilizaron un pequeño número de contraseñas poco seguras o muy utilizadas (como "p@ssword" o "123456") para atacar un gran número de cuentas de usuario y obtener credenciales administrativas de Office 365 (los ataques de difusión de contraseñas se utilizan para evitar la detección al limitar el número de intentos de inicio de sesión de cada cuenta). Después de infiltrarse en la red, APT llevó a cabo una compleja y automatizada extracción de datos de los buzones de correo de los empleados. A pesar de los múltiples intentos internos de expulsarlo, el adversario permaneció en la red durante más de 200 días. Como parte del ataque, el adversario aprovechó el software de la cadena de suministro de la organización y la extracción automatizada de los datos.

Debido a que sospechaban que había un ataque a los datos de sus clientes, la organización contrató al equipo de DART para que investigara y ayudara a prevenir daños adicionales. DART identificó búsquedas en los buzones de Office 365 atacados, cuentas comprometidas y canales de mando y control de atacantes. Las principales lecciones de cliente de este incidente fueron la implementación de controles para proteger los servicios en el cloud de las amenazas basadas en identidad y de los atacantes. La organización adoptó la autenticación multifactor (MFA), políticas de acceso condicional para ciertas aplicaciones en el cloud y el registro de Office 365. Para protegerse aún más contra amenazas similares en el futuro, la organización también puede adoptar una solución de detección y respuesta a amenazas en el punto de conexión (EDR) para detectar a los atacantes que puedan intentar la vulneración de su red. Además, hemos recomendado que esta organización designe un órgano de gobierno del cloud o un equipo de identidad global que administre y aplique las políticas de autenticación de usuario adecuadas, de modo que la organización supervise su situación de seguridad y pueda mitigar el riesgo de forma más eficaz.

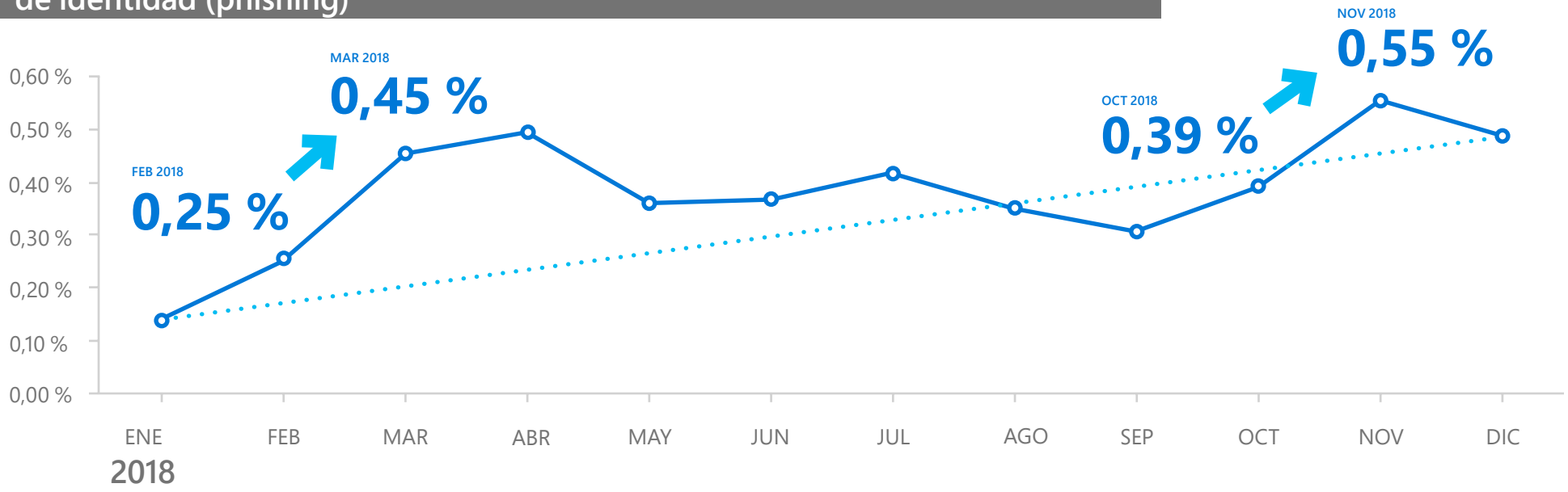
SECCIÓN III

La suplantación de identidad (phishing) sigue prevaleciendo



En 2018, los analistas de amenazas de Microsoft han podido constatar que los atacantes siguen utilizando la suplantación de identidad (phishing) como método de ataque preferido. La suplantación de identidad (phishing) promete seguir siendo un problema en un futuro previsible, ya que implica decisiones y juicios humanos ante los persistentes esfuerzos de los ciberdelincuentes por hacer que las víctimas caigan en su anzuelo.

Las tasas de suplantación de identidad (phishing) siguen en aumento
Porcentaje del total de correos electrónicos entrantes que son de suplantación de identidad (phishing)



LA SUPLANTACIÓN DE IDENTIDAD (PHISHING) SIGUE SIENDO LA VÍA DE ATAQUE PREFERIDA EN 2018

Microsoft analiza y examina en Office 365 más de 470 000 millones de mensajes de correo electrónico al mes en busca de ataques de suplantación de identidad (phishing) y malware, lo que proporciona a los analistas un conocimiento considerable de las tendencias y las técnicas de los atacantes. La proporción de correos electrónicos entrantes que eran mensajes de suplantación de identidad (phishing) aumentó un 250 por ciento entre enero y diciembre de 2018. La suplantación de identidad (phishing) sigue siendo una de las principales vías de ataque utilizadas para ofrecer cargas maliciosas de día cero a los usuarios y Microsoft ha seguido reforzándose contra estos ataques con funciones adicionales de protección, detección, investigación y respuesta contra la suplantación de identidad (phishing) para proteger a los usuarios.

▲ **FIGURA 8.**

Correos electrónicos de suplantación de identidad (phishing) en 2018

Evolución de los métodos de ataque de suplantación de identidad (phishing)

A medida que las herramientas y las técnicas utilizadas para proteger a las personas de la suplantación de identidad (phishing) son más sofisticadas, los atacantes se ven obligados a adaptarse. Los ataques de suplantación de identidad (phishing) son cada vez más polimórficos, lo que significa que los atacantes no utilizan una sola URL, dominio o dirección IP para enviar correo, sino que hacen uso de una infraestructura variada con múltiples puntos de ataque. La naturaleza de los ataques también ha evolucionado, con modernas campañas de suplantación de identidad (phishing) que van desde ataques de corta duración que están activos solo unos minutos hasta campañas de gran volumen mucho más duraderas. Otros son ataques de variantes en serie, en los que los atacantes envían un pequeño volumen de correo durante varios días sucesivos.

Además, Microsoft ha observado una tendencia en la que los atacantes utilizan la infraestructura hospedada y otra infraestructura de cloud público, lo que facilita evitar la detección escondiéndose entre sitios y activos legítimos. Por ejemplo, los atacantes utilizan cada vez más sitios y servicios populares de colaboración y uso compartido de documentos para distribuir cargas maliciosas y formularios de inicio de sesión falsos que se utilizan para robar las credenciales de usuario. También ha habido un aumento en el uso de cuentas comprometidas para distribuir más correos electrónicos maliciosos tanto dentro como fuera de una organización.

Las campañas de suplantación de identidad (phishing) varían desde campañas específicas hasta campañas de base amplia

Al igual que con la distribución de malware en general, las campañas de suplantación de identidad (phishing) varían desde ataques específicos hasta ataques genéricos de base amplia. Aunque los ataques muy sofisticados producen mayores ganancias económicas por cada cuenta suplantada, los ataques más genéricos producen menos dinero por cada cuenta comprometida, pero se dirigen a un conjunto más amplio de usuarios.

Un ejemplo de una campaña sofisticada y específica es Ursnif, en la que los atacantes localizaron el nombre del archivo del documento para que fuera específico de una organización familiar o del sector del objetivo. Dichos ataques son muy distintos de las campañas de base amplia y parecen ser más legítimos y fiables.

Algunas de las campañas de base amplia en 2018 estaban relacionadas con el correo electrónico empresarial (BEC) comprometido y la suplantación de marcas, dominios o usuarios conocidos en las organizaciones atacadas, así como con sofisticadas campañas de suplantación. La suplantación de dominio es una táctica de ataque común que se utiliza para hacer creer a las organizaciones que el correo electrónico es fiable y se debe abrir.

Los engaños de suplantación de identidad (phishing) se presentan de muchas maneras

Los investigadores de Microsoft han descubierto que en las campañas se emplean muchos tipos diferentes de engaños de suplantación de identidad (phishing) o cargas útiles, entre los que se incluyen:

- **Suplantación de dominios** (el dominio de los mensajes de correo electrónico coincide exactamente con el nombre de dominio original)
- **Simulación de dominios** (el dominio de los mensajes de correo electrónico es parecido al nombre de dominio original)[2]
- **Suplantación de usuario** (el mensaje de correo electrónico parece provenir de alguien en quien se confía)
- **Señuelos de texto** (el mensaje de texto parece provenir de una fuente legítima como un banco, una agencia gubernamental u otra empresa para dar legitimidad a sus reclamos y típicamente le pide a la víctima que proporcione información confidencial, como nombres de usuario, contraseñas o datos financieros confidenciales)
- **Enlaces de suplantación de credenciales** (el mensaje de correo electrónico contiene un enlace a una página que se parece a una página de inicio de sesión de un sitio legítimo, por lo que los usuarios introducen sus credenciales de inicio de sesión)
- **Archivos adjuntos de suplantación de identidad (phishing)** (el mensaje de correo electrónico contiene un archivo adjunto malicioso que el remitente invita a la víctima a abrirlo)
- **Enlaces a ubicaciones de almacenamiento en el cloud falsas** (el mensaje de correo electrónico parece provenir de una fuente legítima e incita al usuario a dar permiso o introducir información personal, como credenciales, a cambio de acceder a una ubicación de almacenamiento en el cloud falsa)

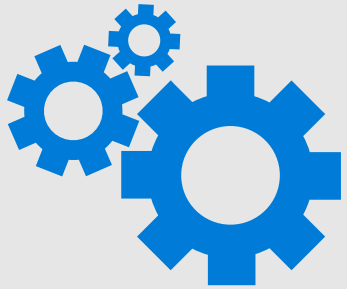
Esta variedad de señuelos que podrían utilizar los atacantes aumenta la complejidad de las amenazas de suplantación de identidad (phishing) a las que se deben enfrentar las organizaciones.

NOTAS AL PIE

[2] La simulación de dominios puede parecerse a la suplantación de dominios (coincidencia exacta con el nombre de dominio original) en el caso excepcional de que el dominio aparezca en el nombre del correo electrónico.

Investigación de incidentes cibernéticos con DART

ORGANIZACIÓN DE FABRICACIÓN GRANDE AFECTADA POR INCIDENTES DE SUPLANTACIÓN DE IDENTIDAD (PHISHING) ESPECÍFICOS



Una organización de fabricación experimentó una campaña de suplantación de identidad (phishing) en varias fases durante unos pocos meses. Este enfoque no es inusual. Durante la primera fase, el atacante realizará un reconocimiento y en la segunda se centrará en activos de alto valor. La primera fase de esta campaña aprovechó una conocida estafa de suplantación de identidad (phishing) que se basaba en un enlace de página web insertado en un correo electrónico enviado a un pequeño grupo objetivo en la organización. En el correo electrónico se afirmaba que el destinatario tenía un importante documento electrónico pendiente de revisión y lo único que tenía que hacer el destinatario era autenticarse con sus credenciales de dominio para obtener acceso. Esta página de destino falsa, creada para que el usuario atacado revisara el "documento importante", recopiló las credenciales y permitió al atacante acceder a las cuentas de Office 365 desde cualquier parte del mundo. La segunda fase de la campaña de suplantación de identidad (phishing) tenía por objeto enviar correos electrónicos de suplantación de identidad similares a activos de alto valor en la organización de fabricación atacada, con la esperanza de obtener acceso a datos más valiosos. Microsoft colaboró con este cliente durante la segunda fase de la campaña de suplantación de identidad (phishing). Las principales lecciones de cliente de este incidente son: la suplantación de identidad (phishing) sigue siendo uno de los métodos de ataque más eficaces y los usuarios siguen siendo el eslabón más débil. Capacitar a los usuarios para que desconfíen de las estafas de suplantación de identidad (phishing), disponer de herramientas para identificar a los atacantes y actuar, y aplicar parches periódicamente a los sistemas es importante; si la organización no se ocupa ni siquiera de uno de estos aspectos, puede ser vulnerable.

En este caso, la preocupación más importante del cliente era la necesidad inmediata de bloquear el acceso a las cuentas comprometidas. En asociación con los equipos de Azure Identity y Office 365, DART diseñó un plan para erradicar al atacante de la red y supervisar el tráfico al canal de mando y control mediante la solución Microsoft Azure Log Analytics implementada recientemente. El equipo pudo contribuir a resolver la situación en solo tres horas. Se bloqueó el acceso del atacante y la organización pudo centrar su atención en la evaluación de daños y la recuperación. DART utilizó las herramientas de Azure Log Analytics para buscar el comportamiento de los atacantes, lo que contribuyó a descubrir muchos desafíos de configuración para la organización. Por ejemplo, DART identificó lagunas en la aplicación de parches en servidores críticos, descubrió ordenadores en la red que se comunicaban con hosts de mala reputación en Internet y también encontró varios servidores importantes sin protección contra malware.

SECCIÓN IV

Malware en todo el mundo

El malware plantea riesgos para las organizaciones y los individuos que se traducen en deterioro de la usabilidad, pérdida de datos, robo de propiedad intelectual, pérdida de dinero, angustia emocional e incluso puede poner en peligro la vida. Microsoft utiliza un amplio conjunto de herramientas y técnicas para identificar, bloquear y erradicar las infecciones de malware dondequiera que se encuentren.

Las tasas de encuentros de malware oscilaron entre alrededor del 5 por ciento y más del 7 por ciento en 2017. A principios de 2018 se elevaron antes de disminuir durante la mayor parte del año a poco más del 4 por ciento. Algunos de los posibles motivos de la disminución general de las tasas de encuentros de malware en 2018 son el aumento de la adopción de Windows 10 y el mayor uso de Windows Defender como protección. La tasa de encuentros es el porcentaje de equipos que ejecutan el antivirus de Windows Defender que comunicaron haber encontrado malware durante el mes, incluidos los intentos de infección que bloqueó Defender.

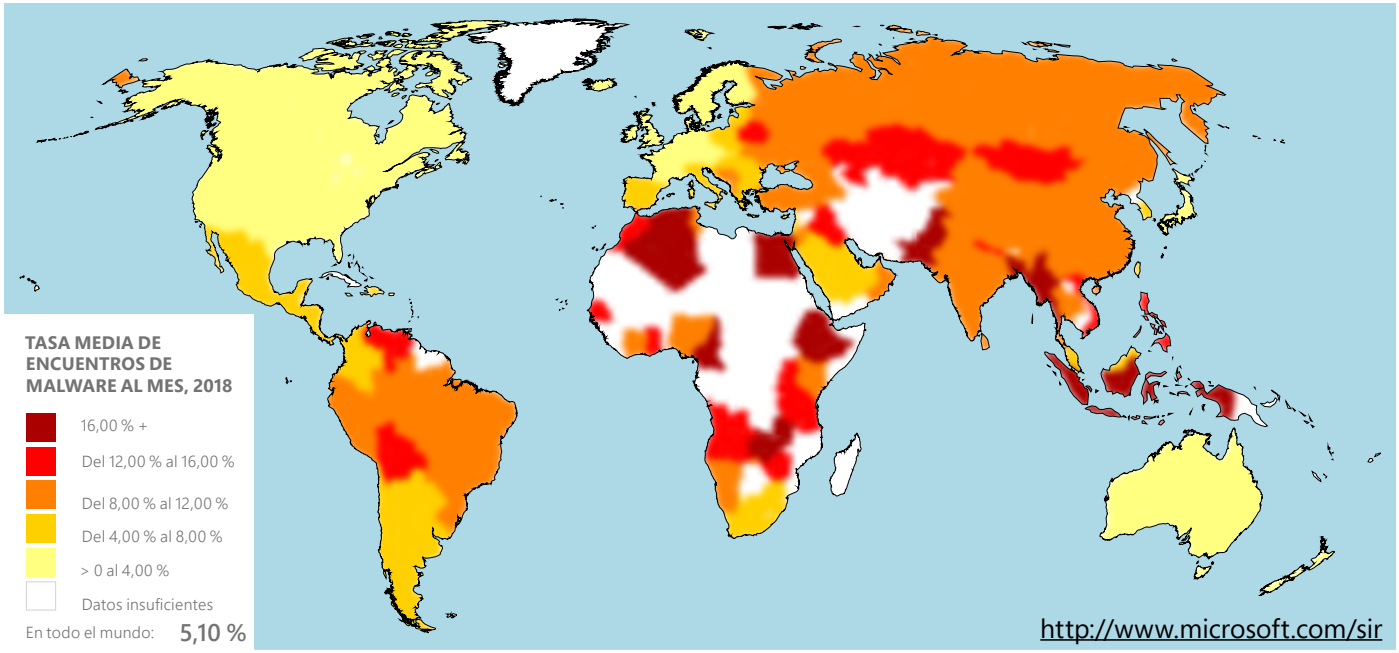


FIGURA 9.

Media mensual de tasas de encuentros de malware en todo el mundo, por país o región, en 2018

Los cinco lugares con las mayores tasas de encuentros de malware durante el periodo de enero a diciembre de 2018 fueron Etiopía (26,33 por ciento de tasa media de encuentros al mes), Pakistán (18,94), los territorios palestinos (17,50), Bangladesh (16,95) e Indonesia (16,59), todos los cuales tuvieron una tasa media mensual de encuentros de aproximadamente el 16,59 por ciento o más durante el periodo. Las tasas de infección suelen estar estrechamente relacionadas con los factores de desarrollo humano y la preparación tecnológica en una sociedad. Todos los lugares con las tasas de encuentros más altas en 2018 ocupaban el 40 por ciento inferior de los países y regiones en el Índice de Tecnologías de la Información y las Comunicaciones (TIC) de 2017, publicado por la Unión Internacional de Telecomunicaciones (UIT) de Naciones Unidas.

Los cinco lugares con las tasas más bajas de encuentros de malware durante el mismo periodo fueron Irlanda (1,26), Japón (1,51), Finlandia (1,74), Noruega (1,79) y Países Bajos (1,82), todos los cuales tuvieron una tasa media mensual de encuentros del 1,82 por ciento o menos durante el periodo. Estos lugares suelen tener infraestructuras de ciberseguridad maduras y programas bien establecidos para proteger la infraestructura crítica y comunicarse con sus ciudadanos sobre la seguridad básica.

MEDIA DE TASAS MENSUALES DE ENCUENTROS DE LOS PAÍSES MÁS AFECTADOS POR EL MALWARE

Etiopía: **26,33 %**

Pakistán: **18,94 %**

Territorios palestinos: **17,50 %**

Investigación de incidentes cibernéticos con DART

VARIAS ORGANIZACIONES DE SERVICIOS FINANCIEROS SUFRIERON ATAQUES DE ESTADO NACIONAL QUE INTERRUMPIERON LAS OPERACIONES

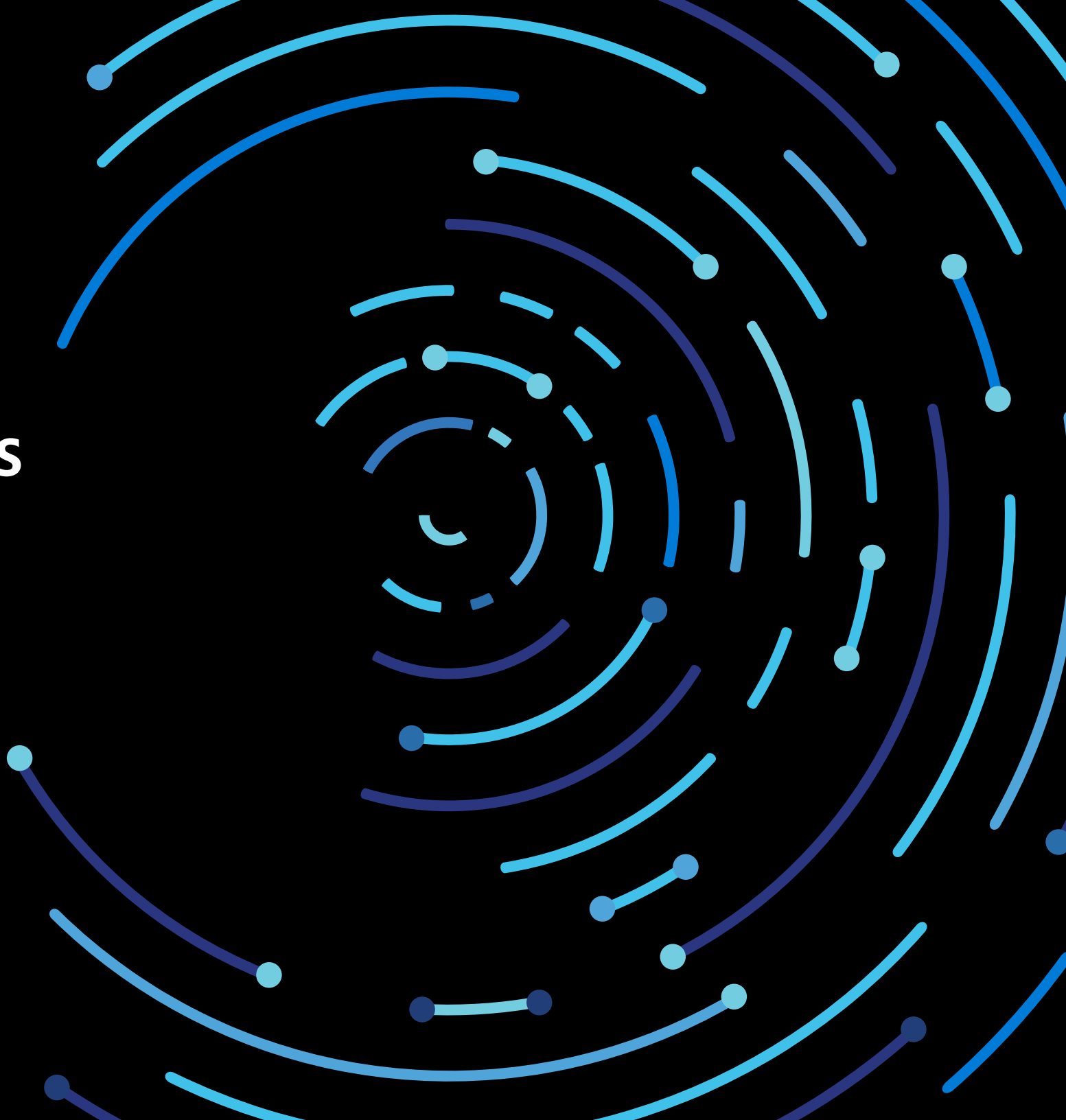
En uno de los incidentes más destructivos que ha visto DART, varias organizaciones de servicios financieros fueron blanco de una APT basada en estado (un grupo diferente del que se dirigía a la organización de servicios profesionales mencionada anteriormente) con evolución similar.

Esta APT obtuvo acceso administrativo después de infectar una máquina de paciente cero con una implantación de puerta trasera oculta y muy específica, posiblemente distribuida a través de un correo electrónico de suplantación de identidad (phishing) definido. Posteriormente, la APT ejecutó varias transacciones fraudulentas y transfirió grandes sumas de dinero en efectivo a cuentas bancarias extranjeras. En algunos casos, el atacante no fue detectado durante más de 100 días. Después de que el atacante se diera cuenta de que lo habían detectado, implementó rápidamente un ataque preestablecido con el envío de malware destructivo a más de la mitad de los sistemas del entorno; las operaciones de estos clientes se cerraron durante varios días.

Hubo algunas lecciones de cliente clave a partir de estos incidentes. La primera fue que la administración del ciclo de vida del software es muy importante, lo que incluye asegurarse de que los sistemas se actualizan periódicamente (sistemas operativos y seguridad), se les aplican parchen y se auditan. En un caso, el entorno de sistema Linux de una organización que tenía un número excepcionalmente grande de cargas de trabajo ejecutándose en él estaba sin administrar, lo que lo ponía en un riesgo considerablemente alto de ataque. La segunda lección fue que es importante mantener copias de seguridad de los datos del sistema en una ubicación sin conexión en caso de que se pierdan los datos principales. Otra lección fue que las soluciones antivirus tradicionales pueden no ser suficientes si se necesita obtener información sobre la actividad maliciosa.

El retorno al modo de funcionamiento normal fue la prioridad más alta para estas organizaciones. DART ayudó a restaurar los servicios investigando primero el impacto y, después, adoptando las medidas de mitigación necesarias, como eliminar el malware de los sistemas afectados y llevarlos a un estado correcto. El equipo también formó a los clientes sobre el uso de las herramientas de investigación de amenazas de Microsoft, incluida una EDR y de otro tipo, para que pudieran buscar comportamientos y actividad anómalos de los atacantes en su red. DART hizo hincapié en que la supervisión de los puntos de conexión es fundamental para defenderse de ataques sofisticados y selectivos que las soluciones antivirus tradicionales puedan pasar por alto.

Directrices



Directrices

El desarrollo de la resistencia organizativa y la reducción significativa de riesgos requieren un enfoque de seguridad que incluya la prevención, la detección y la respuesta. Hemos organizado las siguientes sugerencias de prácticas recomendadas y controles de seguridad en esas categorías.

PREVENCIÓN:

Los controles preventivos desempeñan un papel clave en una estrategia de defensa global, ya que las inversiones adecuadas pueden aumentar el coste de los ataques para los ciberdelincuentes y sostener el aumento de los costes de los ataques a lo largo del tiempo (sin necesidad de que un analista experto supervise e interprete los resultados). Las inversiones en control preventivo deben dirigirse a las técnicas de menor coste para eliminar de forma constante las técnicas de ataque baratas y eficaces.

Los cuatro aspectos que se deben tener en cuenta para la prevención son:

1. **La higiene de seguridad es crítica. Como se ha visto en algunos de los ciberincidentes presentados en este informe, los problemas de higiene comunes pueden socavar las funciones de seguridad avanzadas, por lo que seguir estos consejos puede contribuir a mitigar el riesgo:**

- Evita el uso de software libre o pirata desconocido. Usa solo software de fuentes de confianza.

- Mitiga el riesgo de robo de credenciales, incluida la seguridad de las cuentas de administrador con privilegios. Para saber cómo hacerlo, lee este blog, en el que se describen algunos principios y herramientas que Microsoft ha utilizado para orientar y mejorar nuestra propia postura de seguridad y algunas hojas de ruta prescriptivas para ayudarte a planificar tus propias iniciativas.

- Aplica las bases de referencia de configuración segura proporcionadas por los proveedores de software.

- Mantén los equipos actualizados aplicando rápidamente las últimas actualizaciones a tus sistemas operativos y aplicaciones, e implementa inmediatamente las actualizaciones de seguridad críticas para el sistema operativo, los navegadores y el correo electrónico. Aísla (o retira) los equipos que no se puedan actualizar o a los que no se puedan aplicar parches.

- Implementa protecciones avanzadas de correo electrónico y navegador. Implementa una puerta de enlace de correo electrónico segura que cuente con funciones avanzadas de protección contra amenazas para defenderte de las variantes modernas de suplantación de identidad (phishing).

- Habilita las defensas antimalware y de red del host para obtener respuestas de bloqueo del cloud casi en tiempo real (si están disponibles en tu solución).

2. **Implementa controles de acceso. Ten en cuenta lo siguiente:**

- Aplica el principio de privilegios mínimos, que incluye la implementación de la segmentación de red, la eliminación de los privilegios de administrador local de los usuarios finales y la precaución al conceder permisos a las aplicaciones que se ejecutan en el ordenador.
- Limita la descarga de aplicaciones solo a las que provengan de orígenes de confianza (una tienda de aplicaciones oficial).
- Implementa políticas de integridad de código sólidas, incluida la restricción de las aplicaciones que los usuarios pueden ejecutar. Si es posible, adopta una solución de seguridad que restrinja el código que se ejecuta en el núcleo del sistema (kernel) y que pueda bloquear los scripts no firmados y otras formas de código no fiable. Usa listas blancas de aplicaciones.
- Para obtener más información sobre los ataques a la cadena de suministro de software y cómo protegerte de ellos, lee este blog de investigadores de Microsoft.

3. **Mantén copias de seguridad.**

- Crea copias de seguridad resistentes a la destrucción de datos y sistemas críticos.
- Usa servicios de almacenamiento en el cloud para realizar copias de seguridad automáticas de los datos online. En el caso de los datos on-premises, realiza copias de seguridad periódicas de los datos importantes utilizando la regla 3-2-1. Mantén tres copias de seguridad de tus datos, en dos tipos de almacenamiento diferentes y al menos una copia de seguridad fuera de las instalaciones.

4. **Estate atento y actúa si sospechas algo.**

- Enseña a los empleados a desconfiar de las comunicaciones sospechosas que solicitan información confidencial e indícales cómo responder a ellas y comunicarlas al equipo de operaciones de seguridad de la organización de forma inmediata. La formación también puede ayudar a mitigar los ataques de ingeniería social y de suplantación de identidad (phishing) definida.
- Ten cuidado al hacer clic en los enlaces web. La práctica de hábitos de navegación segura en la web y el uso de soluciones que proporcionen advertencias o bloqueen el acceso a sitios no seguros pueden ayudar a reducir la probabilidad de encontrar sitios web asociados con la minería de criptomoneda.
- Si un ordenador se ejecuta de un modo excepcionalmente lento, busca cualquier archivo sospechoso que se esté ejecutando y no dudes en enviar una muestra al proveedor del sistema operativo. Puedes enviar archivos para el análisis de malware a Microsoft en esta dirección: https://www.microsoft.com/wdsi/filesubmission.

DETECCIÓN Y RESPUESTA:

La detección y la respuesta contribuyen a la resistencia al limitar el tiempo que un atacante tiene acceso a tus recursos. De este modo se reduce el ROI del atacante, tanto al aumentar el coste para él (tiene que volver a intentarlo o modificar sus operaciones) como al reducir la rentabilidad (limita la probabilidad de alcanzar su objetivo).

La misma tecnología de cloud con la que las organizaciones empresariales pueden satisfacer mejor las necesidades del mercado también puede contribuir a las operaciones de seguridad para combatir mejor a los atacantes.

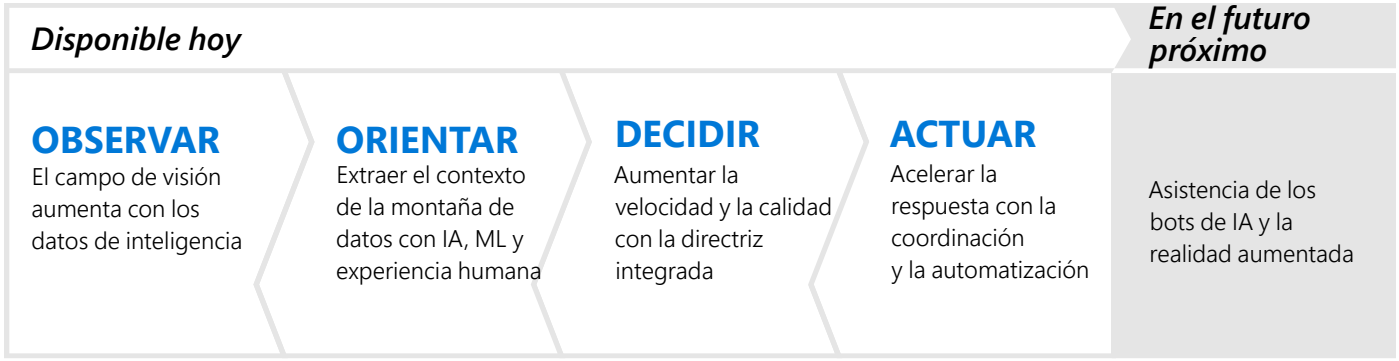


FIGURA 10.
Trayectoria de evolución de los SOC

Al observar la trayectoria de la evolución de los centros de operaciones de seguridad (SOC), vemos que la tecnología aumenta continuamente la velocidad y la calidad de las decisiones y acciones de los SOC. Muchas de estas innovaciones se pueden asignar a cada etapa del "bucle" Observar Orientar Decidir Actuar (OODA) que documentó el coronel John Boyd de la USAF.[3]

OBSERVAR: los SOC pueden aprovechar la vasta inteligencia de seguridad disponible (de Microsoft y otros orígenes), lo que aumenta drásticamente su campo de visión en la organización y en el entorno externo.

ORIENTAR: a medida que estos nuevos orígenes de datos están disponibles para los SOC ya sobrecargados, el machine learning (un subconjunto de inteligencia artificial) se convierte en una herramienta fundamental para razonar sobre estos conjuntos de datos masivos e identificar anomalías que merezca la pena investigar. Los proveedores de seguridad (incluido Microsoft) han adoptado la tecnología de machine learning para priorizar rápidamente los eventos (y ayudar a fusionar estos eventos individuales en incidentes globales).

DECIDIR: debido a que el volumen y la complejidad de los ataques pueden sobrecargar rápidamente un SOC, los analistas y los equipos de respuesta a incidentes necesitan tomar muchas decisiones y actuar con rapidez en respuesta a las alertas y las detecciones. Microsoft y otros proveedores han integrado funciones de investigación automatizada, así como orientación para ayudar a los analistas a tomar buenas decisiones rápidamente (por ejemplo, para aislar dispositivos potencialmente infectados o comprometidos). Por el momento, la automatización se centra en la resolución rápida de incidentes de baja prioridad para que se puedan aplicar conocimientos especializados a problemas más complejos.

ACTUAR: la respuesta requiere una ejecución rápida y precisa en muchas tecnologías y plataformas, que es lo que permiten las tecnologías coordinación de seguridad y automatización de respuestas. Microsoft y muchas otras empresas continúan invirtiendo en estas tecnologías, incluida las soluciones modernas de detección de amenazas y respuesta automatizada.

NOTAS AL PIE
[3] http://www.militaryhistoryveteran.com/colonel-john-boyd-ooda-loop/

Otras tendencias que se aplican a un SOC moderno son:

- **Calidad sobre cantidad de fuentes de alertas**: a medida que las organizaciones pasan de administrar "información insuficiente" a administrar "demasiada información", el tiempo y la atención de los analistas de SOC altamente especializados son cada vez más valiosos. Esto aumenta la necesidad de calidad en las alertas que requieren la participación de analistas de nivel 1 y 2. Aunque las fuentes de datos adicionales son siempre útiles para las investigaciones y la búsqueda proactiva, el SOC de TI corporativo de Microsoft mide la verdadera tasa positiva de las fuentes de alertas que requieren la respuesta de los analistas (y que actualmente requieren una tasa positiva real del 90 % o superior).

- Gravedad de los datos: el análisis de grandes conjuntos de datos (incluidos los datos de seguridad) es difícil de realizar sin acceder a los datos sin procesar subyacentes. A medida que hay disponibles más datos de seguridad, resulta más económico y práctico realizar los análisis de seguridad en el cloud en vez de transferir esos datos a un sistema on-premises. Esto probablemente impulsará la evolución de las arquitecturas SIEM y SOC, que pueden incluir enfoques SIEM híbridos o la adopción de SIEM de cloud nativo como servicio.

- **Elevado volumen de contexto**: estos tipos de detecciones son mucho más útiles debido a su capacidad de relacionar los conjuntos de datos de manera más efectiva. Mientras las detecciones tradicionales basadas en el tráfico de red siguen ofreciendo cierto valor de seguridad, el tráfico de red sin procesar normalmente carece de contexto para diferenciar entre actividad legítima y actividad anómala. Hemos observado que los SOC obtienen mucho más valor de las detecciones con mucho contexto como:

  - **Soluciones de detección y respuesta de los puntos de conexión (EDR)** que tienen un contexto exhaustivo de la actividad de host
  - Detecciones basadas en identidad que incluyen conocimientos sobre los patrones normales de la autenticación de usuario (ubicaciones, horas, servicios a los que se accede, etc.) y aplicar análisis de comportamiento

A los adversarios les resulta más difícil evadir estas detecciones con contexto exhaustivo porque tienen que imitar una operación mucho más compleja (frente a unos pocos atributos técnicos del tráfico IP).

Otra lección que hemos aprendido de los ataques importantes a los clientes es la dificultad de responder rápidamente a los incidentes cuando las funciones de TI se han subcontratado parcial o totalmente. Te recomendamos que revises tus contratos de subcontratación de TI y los acuerdos de nivel de servicio (SLA), así como los proveedores de la cadena de suministro, para asegurarte de que son compatibles con una respuesta de seguridad rápida. Para obtener más información sobre nuestras investigaciones de incidentes de los clientes, consulta la guía de referencia de respuesta a incidentes (IRRG) en https://aka.ms/IRRG.

Orígenes de datos

Orígenes de datos

Microsoft ha recopilado los datos incluidos en el informe de inteligencia de seguridad de Microsoft a través de la provisión de una amplia gama de productos y servicios de Microsoft, tal como se explica en la Declaración de privacidad de Microsoft. Estos datos nos proporcionan información valiosa sobre la seguridad y las operaciones de nuestros productos y servicios, así como conocimientos sobre el panorama de las amenazas a la ciberseguridad en general. Estos datos incluyen análisis de los siguientes orígenes:[4]

- **Azure Security Center** es un servicio que ayuda a las organizaciones a prevenir, detectar y responder ante amenazas al permitir una mayor visibilidad de la seguridad de las cargas de trabajo en el cloud y el uso de análisis avanzados e información sobre amenazas para detectar ataques.

- **Bing** es el motor de búsqueda y decisión que realiza miles de millones de análisis de páginas web al año para detectar contenido malintencionado. Después de detectar este contenido, Bing advierte a los usuarios para ayudar a prevenir la infección.

- **Exchange Online** es el servicio de correo electrónico y de productividad alojado de Microsoft. Los servicios antimalware y antispam de Exchange Online analizan miles de millones de mensajes cada año para identificar y bloquear spam y malware.

- La **herramienta de eliminación de software malintencionado** (MSRT) es una herramienta gratuita diseñada por Microsoft para ayudar a identificar y eliminar familias de malware prevalentes específicas en los ordenadores de los clientes. La MSRT se publica principalmente como una actualización importante a través de Windows Update, Microsoft Update y actualizaciones automáticas. También hay disponible una versión de la herramienta en el Centro de descarga de Microsoft. La MSRT no sustituye a una solución antivirus actualizada en tiempo real.

- El **Examen de seguridad de Microsoft** es una herramienta de seguridad que puede descargarse de manera gratuita y que ofrece análisis a petición y ayuda a eliminar malware y otros programas malintencionados. El Examen de seguridad de Microsoft no es un sustituto de una solución antivirus actualizada, ya que no ofrece protección en tiempo real y no puede evitar que un ordenador se infecte.

NOTAS AL PIE

[4]Es importante destacar que estos datos siempre pasan por límites estrictos de privacidad y conformidad antes de utilizarse por motivos de seguridad.

- **Microsoft Security Essentials** es un producto de protección en tiempo real gratuito y fácil de usar que proporciona protección antivirus y antispyware básica y eficaz para Windows Vista y Windows 7.

- **Microsoft System Center Endpoint Protection** (anteriormente Forefront Client Security y Forefront Endpoint Protection) es un producto unificado que proporciona protección frente a malware y software no deseado para ordenadores de escritorio empresariales, ordenadores portátiles y sistemas operativos de servidores. Utiliza el Microsoft Malware Protection Engine y la base de datos de firmas de antivirus de Microsoft para proporcionar protección en tiempo real, programada y a petición.

- **Office 365** es el servicio de suscripción de Microsoft Office para organizaciones y usuarios domésticos. Algunos planes de suscripción incluyen acceso a Advanced Threat Protection de Office 365.

- La **seguridad de Windows** en Windows 10 proporciona análisis en tiempo real y eliminación de malware y software no deseado. Además, la última versión de Windows aprovecha datos contextuales completos como la configuración del equipo, rendimiento y estado del dispositivo, así como información similar para mejorar la seguridad de los clientes. Al mismo tiempo, dotamos a los clientes de más información acerca de su privacidad en Windows 10. Lee este blog para conocer algunas de las formas en que Microsoft lo hace.

- **Advanced Threat Protection de Windows Defender** es un servicio integrado en la actualización de aniversario de Windows 10 y en versiones anteriores que concede a los clientes empresariales la capacidad de detectar, investigar y corregir amenazas persistentes avanzadas y vulneraciones de datos en sus redes.

- **Windows Defender sin Conexión** es una herramienta descargable que puede usarse para crear un CD, un DVD o una unidad flash USB de arranque con el fin de analizar un ordenador en búsqueda de malware y otras amenazas. No ofrece protección en tiempo real y no es un sustituto de una solución antimalware actualizada.

- **SmartScreen de Windows Defender** es una característica de Microsoft Edge e Internet Explorer que ofrece a los usuarios protección frente a sitios de suplantación de identidad (phishing) y sitios que hospedan malware. Microsoft mantiene una base de datos de sitios de phishing y malware notificados por usuarios de Microsoft Edge, Internet Explorer y otros productos y servicios de Microsoft. Cuando un usuario intenta visitar un sitio que figura en la base de datos y el filtro está activado, el navegador muestra una advertencia y bloquea el acceso a la página.