Microsoft

INFORME DE INTELIGENCIA SOBRE SEGURIDAD DE MICROSOFT

VOLUMEN 24
ENERO – DICIEMBRE 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
Defensa activa de Windows

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 a incidentes de seguridad

Matt Duncan
Ingeniería y análisis de datos de defensa activa de Windows

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. Le doy la bienvenida a la 24ª edición del Informe de inteligencia de seguridad de Microsoft (SIR). Como profesional y arquitecto de seguridad, leí informes como este con la esperanza de entender el panorama un poco mejor mediante consejos prácticos sobre cómo utilizar ese conocimiento para defender y proteger a las organizaciones de manera más eficaz.

El equipo de SIR incorpora el espíritu de la educación para mejorar la resiliencia cibernética a este informe y ha examinado un año de datos para extraer las lecciones más importantes.

Lo que está leyendo son ideas extraídas durante un año de análisis de datos de seguridad y lecciones prácticas aprendidas. Los datos analizados incluyen 6,5 billones de señales de amenaza que atraviesan la nube de Microsoft todos los días, y las experiencias de investigación y del mundo real de nuestros miles de investigadores y personal de seguridad inmediata en todo el mundo. En 2018, los atacantes utilizaron una variedad de trucos, tanto nuevos (minería de monedas) como viejos (phishing), en su búsqueda continua por robar datos y recursos de clientes y organizaciones. Los ataques híbridos, como la campaña de Ursnif, combinaron enfoques sociales y técnicos. A medida que los defensores actuaron de forma más inteligentes contra el ransomware, una forma agresiva y disruptiva de ataque, los delincuentes dieron un giro al ataque más "furtivo", pero aún rentable, de la minería de monedas.

Ese "giro" puede hacerlo sentir frustrado, como que los atacantes siempre están un paso por delante. Pero si se ve desde otra perspectiva, aquí la historia es positiva. Los defensores y profesionales de la ciberseguridad, como usted, implementaron técnicas de defensa que obligaron a los atacantes a cambiar sus cargas preferidas y alejarse del ransomware.

Otra área donde los ciberdelincuentes aumentaron su actividad fue la cadena de suministro. Uno de los más notables, el brote de minería de monedas de Dofoil, que golpeó el 6 de marzo de 2018, se puso en marcha con una aplicación de punto a punto contaminada. Las preocupaciones de la cadena de suministro fueron más allá de las aplicaciones y llegaron a la nube, e incluyeron extensiones de navegadores malintencionadas, repositorios de Linux comprometidos y varias instancias de módulos con "puertas traseras". Para abordar esta amenaza, las organizaciones están avanzando hacia un modelo de cadena de suministro transparente y confiable.

Los datos son geniales, pero a veces es útil descubrir lo que realmente sucedió en una organización. Es por eso que hemos incluido lecciones aprendidas en el campo de nuestro Equipo de detección y respuesta (DART). Entre estas se incluye cómo una gran empresa manufacturera pudo implementar controles para bloquear una campaña de phishing de varias etapas que los había atormentado durante meses, y organizaciones de servicios financieros que finalmente pudieron erradicar las amenazas de sus sistemas mediante herramientas avanzadas de investigación y supervisión de puntos de conexión.

Por último, pero no menos importante, los clics en ataques de phishing siguieron aumentando, pero los modelos de machine learning captan mejor las amenazas antes de que lleguen a los buzones de los usuarios y evitan el daño después del clic, si lo hacen. ¿Más buenas noticias? Cada vez más empresas están implementando soluciones multifactor para limitar el éxito de los correos electrónicos de phishing que buscan robar credenciales.

Los atacantes buscan oportunidades, por lo que cuanto más sepamos sobre sus técnicas y tácticas, mejor preparados estaremos para crear defensas y responder rápidamente. Pequeños pasos importantes pueden hacer una gran diferencia en el estado general de la ciberseguridad de una organización. Es por eso que en este informe, junto con conocimientos profundos sobre el cambio del paisaje de malware y ataques, encontrará pasos recomendados y otras recomendaciones prácticas. Porque cuando yo estaba a cargo eso era exactamente lo que necesitaba en mi lucha contra los tipos malos. Esperamos que sea lo que usted también necesita.

Diana Kelley
Directora de tecnología del área de ciberseguridad de Microsoft

P. D. Siempre estamos buscando mejorar SIR. Si tiene comentarios, póngase en contacto con nosotros y comparta su opinión.

SECCIÓN I

Ransomware, minería de criptomonedas y dinero

Las grandes historias de seguridad del año 2017 en su mayoría se trataban de ransomware. Ataques de alto perfil en todo el mundo de WannaCrypt y Petya impusieron el ransomware (un tipo de malware que bloquea o cifra los equipos, y a continuación, exige dinero para restaurar el acceso) en la conciencia general, y muchos especularon que el problema solo aumentaría en el futuro. En su lugar, las detecciones de ransomware disminuyeron significativamente en el año 2018.

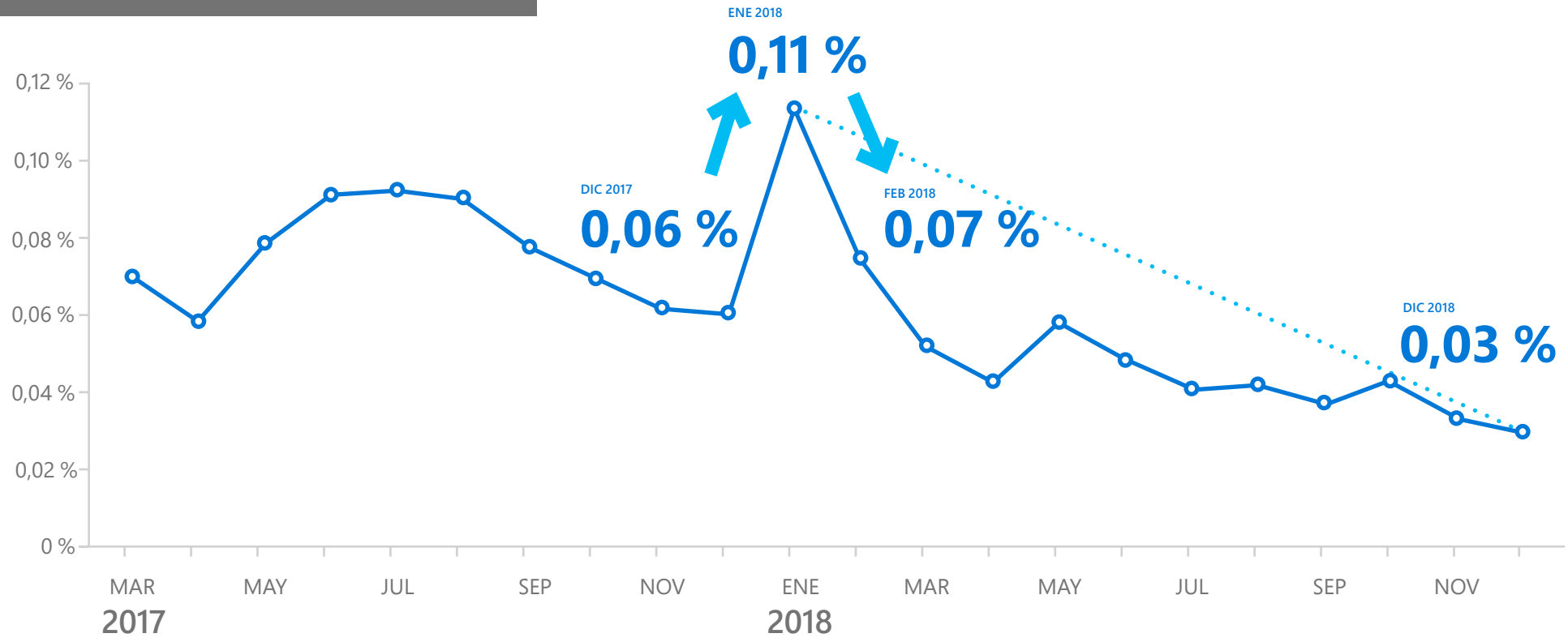
La disminución de las detecciones de ransomware se debió en parte a una mejor detección y educación que dificultaba que los atacantes se beneficiaran. Como resultado, los atacantes comenzaron a cambiar sus iniciativas para alejarse del ransomware y acercarse a enfoques como la minería de criptomonedas, que utiliza los recursos informáticos de las víctimas para crear dinero digital para los atacantes. El cambio demuestra la naturaleza fundamentalmente oportunista de la mayoría de los ciberdelincuentes orientados a los beneficios: suelen buscar el dinero más fácil posible, y cuando la economía de la ciberdelincuencia cambia, se apresuran a seguirla.

ATAQUES DE RANSOMWARE EN DESCENSO

Hace más de una década, los hackers y bromistas que dominaban el malware inicial clandestino fueron suplantados por el crimen organizado y otros intereses orientados a los beneficios. Mientras que los brotes de malware iniciales solían ser llamativos y obvios, el malware orientado a los beneficios era mucho más probable que funcionara sigilosamente y evitara atraer la atención con el fin de seguir cumpliendo su función: enviar spam, robar información confidencial, realizar ataques de denegación de servicio y otras actividades maliciosas, durante el mayor tiempo posible.

El ransomware se resistió a esta tendencia. En lugar de tratar de permanecer sin ser detectado, el ransomware abiertamente niega a las víctimas el acceso a sus equipos y archivos importantes hasta que pague el rescate (e incluso después; los atacantes a menudo no liberan el control de los equipos incluso después de que se paga el rescate). En 2017, cuando el ransomware alcanzaba su momento más álgido, parecía que este estilo de ataque representaría una nueva fase en las técnicas de los atacantes. Pero los datos más recientes sugieren que el ransomware podría estar en declive, con atacantes que vuelven cada vez más al modo más sigiloso de operación que han empleado hasta ahora, tratando de permanecer bajo el radar con el fin de llevar a cabo ataques más eficaces, como la minería de criptomonedas. Aunque ha habido una disminución en la tasa de detecciones de ransomware, esto no significa necesariamente que la severidad de los ataques haya disminuido.

Tasa de detecciones de ransomware



Las tasas de detecciones de ransomware disminuyeron aproximadamente en un 60 % entre marzo de 2017 y diciembre de 2018, con aumentos intermitentes a lo largo de ese período.

Probablemente, hay muchas causas para esta disminución general, aunque los investigadores de seguridad de Microsoft sospechan que un factor principal es que tanto los usuarios finales y las organizaciones son cada vez más conscientes de las amenazas ransomware y las abordan de manera más inteligente, incluido el tener mayor precaución y hacer copias de seguridad de archivos importantes para que puedan restaurarse si los cifran con ransomware. Además, como se describió anteriormente, los ciberdelincuentes son oportunistas.

FIGURA 1.

Detecciones de ransomware desde marzo de 2017 hasta diciembre de 2018

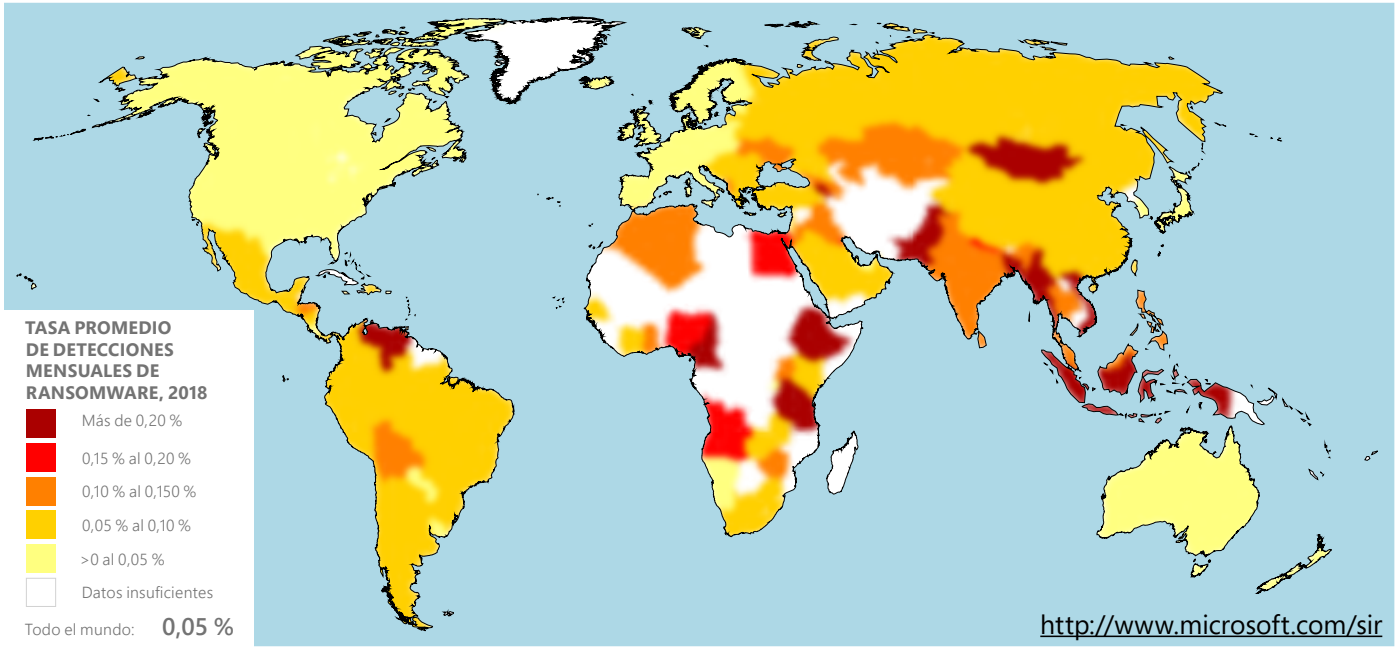
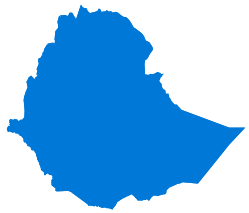


FIGURA 2.

Tasas promedio de detecciones mensuales de ransomware en todo el mundo por país/región en 2018

PAÍS MÁS AFECTADO POR RANSOMWARE: ETIOPÍA



Tasa promedio de detecciones mensuales: **0,77 %**

Los cinco países con las tasas promedio más altas de detecciones mensuales de ransomware en 2018 fueron Etiopía (tasa promedio de detecciones mensuales de ransomware de un 0,77 %), Mongolia (0,46 %), Camerún (0,41 %), Myanmar (0,33 %) y Venezuela (0,31 %), cada uno de los cuales presentó una tasa promedio mensual de detecciones de ransomware de 0,31 % o más durante el período.[1] Hace unos años, las detecciones de ransomware solían agruparse en los países y regiones de Europa y Norteamérica con más dinero, pero como el ransomware ha comenzado a desfavorecer a los atacantes el patrón de detecciones se asemeja más en total al de malware.

Las ubicaciones con las tasas más bajas de detecciones de ransomware en 2018 fueron Irlanda (0,01 %), Japón (0,01 %), Estados Unidos (0,02 %), Reino Unido (0,02 %) y Suecia (0,02 %), cada una de los cuales tuvo una tasa promedio mensual de detecciones de ransomware de 0,02 % o menos durante el mismo período. Las ubicaciones con bajas tasas de detecciones suelen tener infraestructuras de ciberseguridad sólidas y programas bien establecidos para proteger la infraestructura crítica y comunicarse con sus ciudadanos sobre la seguridad básica.

NOTAS AL PIE

[1] Tasa de detección es el porcentaje de equipos que ejecutan productos de seguridad en tiempo real de Microsoft que registran detecciones de malware. La detección de una amenaza no significa que el equipo haya sido infectado. Para el cálculo de las tasas de detección solo se tienen en cuenta los equipos cuyos usuarios eligieron proporcionar datos a Microsoft.

MINERÍA DE CRIPTOMONEDAS EN ASCENSO

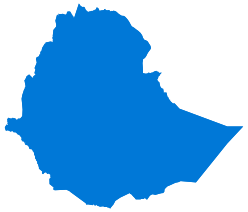
La criptomoneda es dinero virtual que se puede utilizar para comprar y vender anónimamente bienes y servicios, tanto en línea como en el mundo físico. Existen muchos tipos diferentes de criptomonedas, pero todas están basadas en la tecnología de blockchain, en la que cada transacción se registra en un libro de contabilidad distribuido que se mantiene en miles o millones de equipos en todo el mundo. Los equipos que realizan cálculos complejos que también verifican las transacciones de blockchain crean, o "minan", las nuevas monedas.

La minería de monedas puede ser muy lucrativa (en 2018, una sola moneda de bitcoin, la criptomoneda más antigua y popular, valía varios miles de dólares estadounidenses), pero realizar los cálculos necesarios puede exigir muchos recursos, lo que aumenta con cada moneda nueva que se mina. En el caso de las divisas populares, como bitcoin, minar monedas de forma rentable es casi imposible sin acceder a tremendos recursos informáticos que están absolutamente fuera del alcance de la mayoría de las personas y grupos pequeños. Por esta razón, los atacantes que buscan obtener ganancias ilícitas se están dedicando cada vez más al malware que les permite utilizar los equipos de las víctimas para minar criptomonedas. Este enfoque les permite aprovechar la potencia de procesamiento de cientos de miles de equipos en lugar de uno o dos. Incluso cuando se descubre una infección menor, la naturaleza anónima de la criptomoneda complica los esfuerzos para detectar a los responsables.

En 2018, la tasa de detección mensual promedio de minería de criptomonedas en todo el mundo fue de 0,12 %, en comparación apenas un 0,05 % de ransomware. Muchos factores contribuyen a la creciente popularidad de la minería como una carga útil para el malware. A diferencia del ransomware, la minería de criptomonedas no requiere la entrada del usuario: funciona en segundo plano, mientras el usuario está realizando otras tareas o está lejos del equipo, y puede que no se note en absoluto, a menos que perjudique lo suficiente el rendimiento del equipo. Como resultado, 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 disponibilidad de productos "listos" para la minería encubierta de muchas criptomonedas es otro factor que impulsa esta tendencia. La barrera para ingresar es baja debido a la amplia disponibilidad de software de minería de monedas, que los ciberdelincuentes convierten en malware para entregarlos a los equipos de usuarios desprevenidos. Los mineros malintencionados se distribuyen a las víctimas mediante muchas de las mismas técnicas que los atacantes utilizan para enviar otras amenazas, como la ingeniería social, vulneraciones y descargas ocultas. Después de instalar el software de minería, se ejecuta en segundo plano en los equipos de las víctimas para realizar los cálculos de blockchain, donde el atacante recibe las recompensas.

TASAS PROMEDIO MENSUALES DE DETECCIÓN DE LOS PAÍSES MÁS AFECTADOS POR LA MINERÍA DE CRIPTOMONEDAS



Etiopía: **5,58 %**

Tanzania: **1,83 %**

Pakistán: **1,47 %**

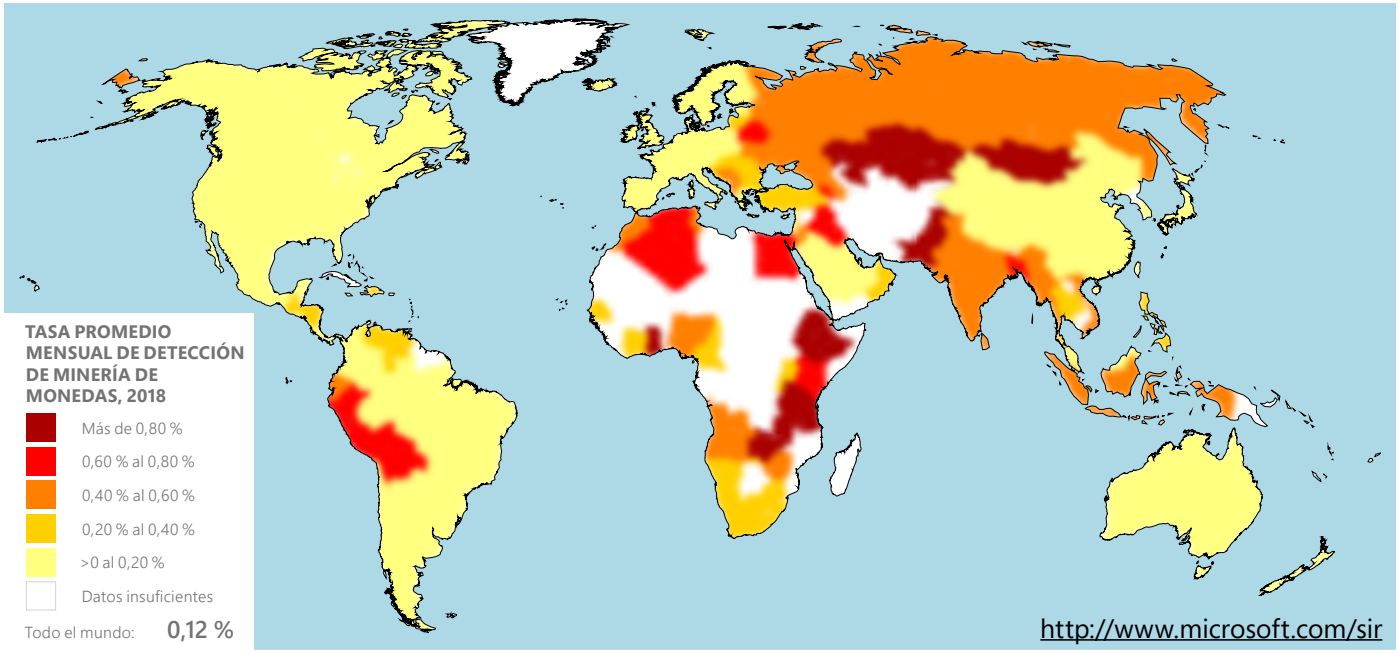


FIGURA 3.

Tasas promedio de detecciones mensuales de minería de monedas en todo el mundo por país/región en 2018

TASAS PROMEDIO MENSUALES DE DETECCIÓN DE LOS PAÍSES MENOS AFECTADOS POR LA MINERÍA DE CRIPTOMONEDAS

Irlanda: 0,02 %

Japón: 0,02 %

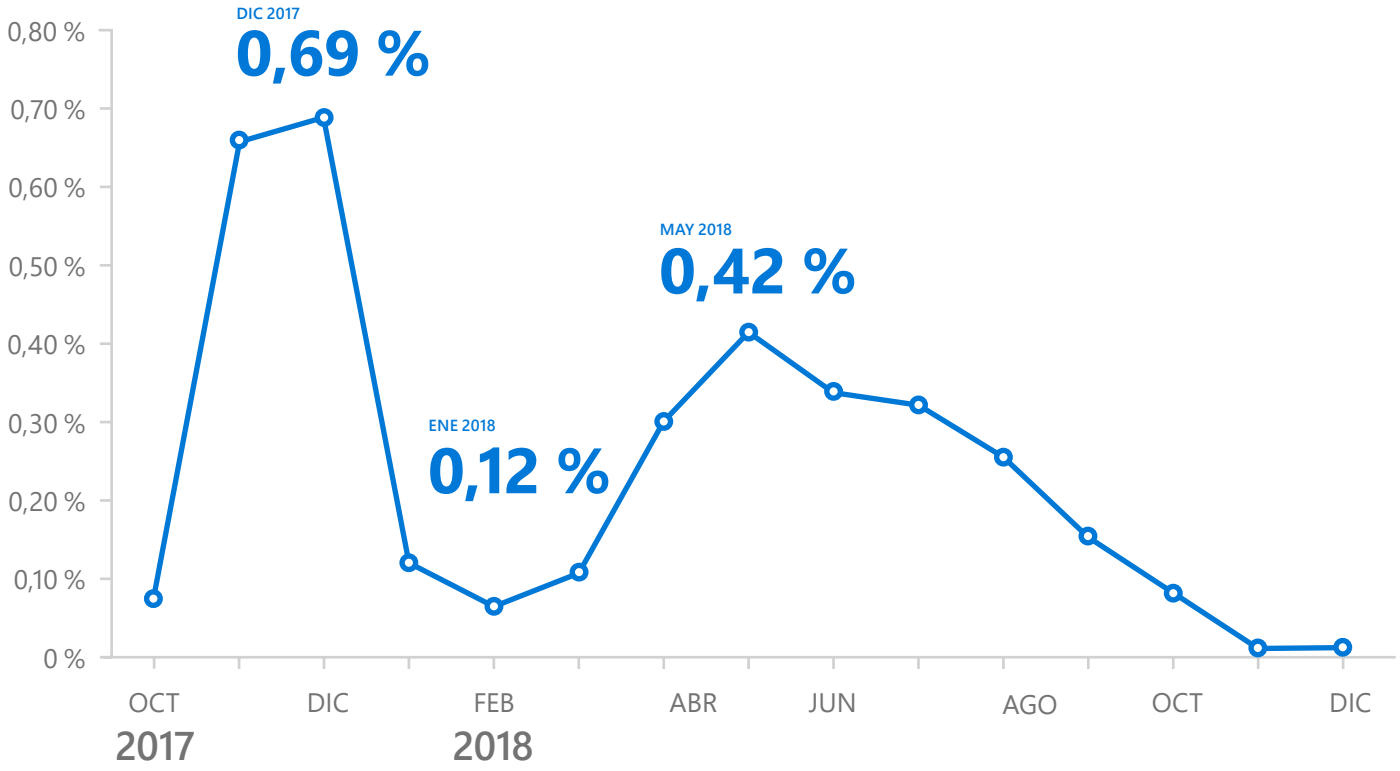
Estados Unidos: 0,02 %

Los cinco países con las tasas más altas de detección de minería de criptomonedas en 2018 fueron Etiopía (5,58 %), Tanzania (1,83 %), Pakistán (1,47 %), Kazajstán (1,24 %) y Zambia (1,13 %), cada uno de los cuales tenía una tasa promedio mensual de detección de minería de monedas de aproximadamente 1,13 % o más durante el período. Las ubicaciones con las tasas de detección de minería de monedas más bajas en 2018 fueron Irlanda, Japón, Estados Unidos y China, cada una de las cuales tenía una tasa promedio mensual de detección de minería de monedas de aproximadamente 0,02 % durante el período.

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

Las estadísticas presentadas en esta sección implican mineros de criptomonedas malintencionados que están diseñados para instalarse en los equipos de las víctimas como malware. Sin embargo, algunas de las amenazas de minería de criptomonedas más significativas se basan completamente en los navegadores web y no necesitan instalarse en absoluto. Muchos servicios anuncian la minería de criptomonedas basada en navegadores como una manera para los propietarios de sitios web de monetizar el tráfico a sus sitios sin depender de la publicidad. Los propietarios de sitios deben agregar código JavaScript a sus páginas que mina la criptomoneda en segundo plano mientras el usuario visita

Tasa de detección de Brocoiner



el sitio, donde los ingresos se dividen entre el propietario del sitio y el servicio. Por desgracia, los atacantes rápidamente han aprovechado estos servicios para minar criptomonedas sin obtener el consentimiento de los usuarios finales, a menudo al comprometer sitios web legítimos y de forma maliciosa insertar el código de minería en el código fuente. Estos mineros basados en navegadores no necesitan comprometer el equipo del usuario final en absoluto, y se ejecutan en cualquier plataforma con un navegador web compatible con JavaScript. Al igual que los troyanos mineros de criptomonedas, los mineros basados en navegadores pueden perjudicar significativamente el rendimiento del equipo y malgastar electricidad mientras el usuario visita una página web afectada.

FIGURA 4.

Tasa de detección de Brocoiner, el minero de criptomonedas basado en navegadores más extendido

EL IMPACTO DE LA MINERÍA DE CRIPTOMONEDAS NO SOLICITADA

La amenaza más obvia que enfrentan las víctimas de la minería malintencionada de criptomonedas es el consumo de recursos informáticos, que puede malgastar electricidad y perjudicar significativamente el rendimiento del equipo. Los usuarios y las organizaciones también enfrentan otros riesgos de la minería de monedas, entre los que se incluyen los siguientes:

- **Ganan un punto de ingreso para hacer un daño mayor en el futuro.**
  Al igual que otras formas de malware, la minería de criptomonedas puede ser un punto de entrada para los atacantes. Mientras que el equipo está minando criptomonedas en segundo plano, los ciberdelincuentes pueden aprender sobre el entorno y posiblemente descubrir brechas en la seguridad para utilizar con otros propósitos.

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

- **Daño a las máquinas.**
  El software de minería de criptomonedas que se ejecuta continuamente durante meses o más puede perjudicar el rendimiento, y el calor generado por el consumo excesivo de energía y el uso de la CPU puede dañar los equipos.

SECCIÓN II

Cadenas de suministro de software en riesgo

Durante años, Microsoft ha estado registrando los protagonistas de amenazas que usan los ataques de cadenas de suministro como punto de entrada para otros 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 un paquete de actualización que, después, se distribuye a los usuarios del software. A continuación, el código malicioso se ejecuta con la misma confianza y permisos que el software. El mayor número de ataques a cadenas de suministro de software en los últimos años se ha convertido en un tema clave en muchas conversaciones sobre ciberseguridad y es una fuente importante de preocupación en muchos departamentos de TI.

FIGURA 5.

Ataques de cadena de suministro de software en 2017 y 2018

ATAQUES MÁS IMPORTANTES DE CADENA DE SUMINISTRO DE SOFTWARE EN 2017

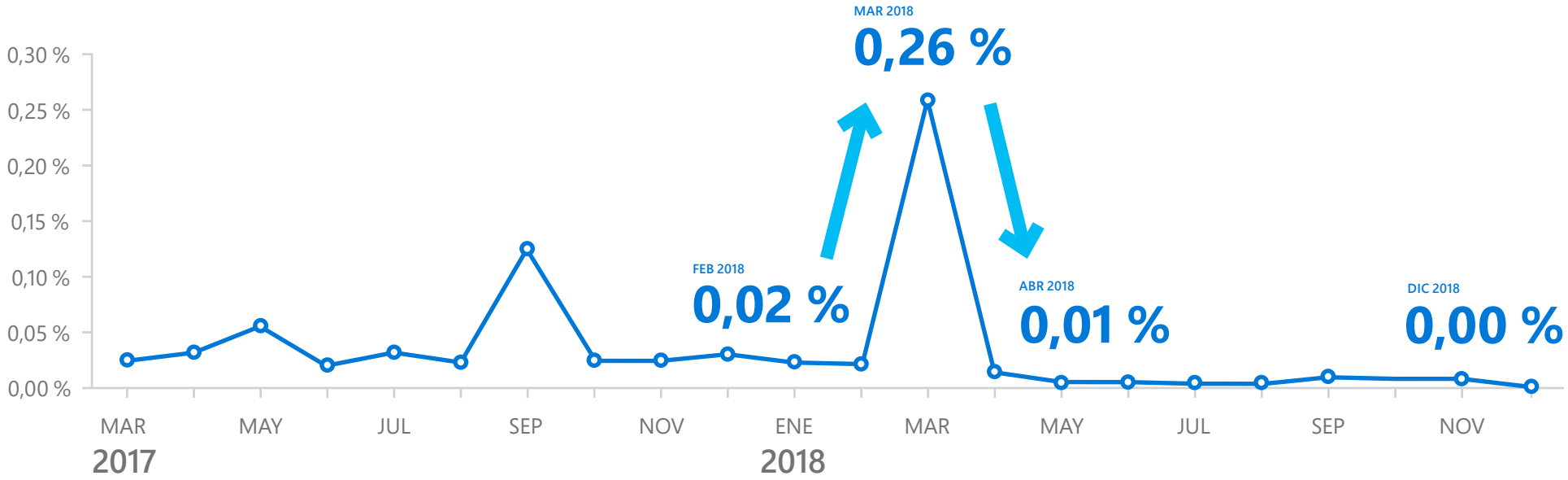
En 2017, los ataques de cadena de suministro fueron responsables de una serie de incidentes de alto perfil, donde el más importante fue el brote del ransomware Petya en junio, que se remontó a las infecciones iniciales de un proceso de actualización comprometido para una aplicación de contabilidad fiscal popular en Ucrania. En mayo, la Operación WilySupply comprometió un actualizador de software del editor de texto para instalar una puerta trasera en las organizaciones objetivo en los sectores financiero y de TI. En julio, una puerta trasera llamada ShadowPad se ocultó en un paquete de software de administración de servidores y permitió 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 CCleaner de software gratuito fue comprometida y una versión de puerta trasera se entregó a su base de usuarios.

El primer ataque grave a la cadena de suministro de software de 2018 se produjo el 6 de marzo, cuando ATP de Windows Defender bloqueó una campaña tremenda para enviar el troyano Dofoil (también conocido como Cargador de humo). La enorme campaña de malware se remontó a una aplicación de punto a punto contaminada. El paquete de actualización de la aplicación se reemplazó por uno malicioso que descargó el código comprometido, que más tarde instaló el malware Dofoil. El troyano sofisticado llevaba una carga de minería de monedas y demostró técnicas avanzadas de inyección de procesos cruzados, mecanismos de persistencia y métodos de evasión.

FIGURA 6.

La tendencia de detecciones de Dofoil (Cargador de humo) en 2018 muestra cómo aumentan las instancias bloqueadas en marzo

Tasa de detección de Dofoil



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

Se detectaron varios ataques más mediante cadenas de suministro de software comprometidas como mecanismos de entrega en 2018, incluidos los descritos en la siguiente tabla:

Período	Ataque	Descripción	Software afectado
Marzo de 2018	Campaña de minería de monedas Dofoil (registrado por Microsoft).	Los atacantes contaminaron el proceso de actualización de una aplicación de punto a punto para instalar Dofoil, que a su vez instaló el malware de minería de monedas.	Aplicación de 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 un proveedor de aplicaciones para editar PDF y uno de sus socios proveedores de software.	Aplicación de editor de PDF y proveedor de socio externo.
Agosto de 2018	Programa de soporte remoto comprometido (Operation Red Signature, registrado por Trend Micro e IssueMakersLab).	El servidor de actualización de un proveedor de soluciones de soporte remoto se comprometió para entregar una herramienta de acceso remoto llamada 9002 RAT.	Programa de soporte remoto.
Octubre de 2018	Solución de panel de control de hosting comprometido (registrado por ESET).	El script de instalación de una solución de panel de control de hosting se modificó para robar credenciales.	Solución de panel de control de hosting.

FIGURA 7.

Otros ataques de cadena de suministro de software en 2018

CONFIANZA EN RIESGO

Los ataques de cadenas 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 es a menudo firmado y certificado por el proveedor, y es posible que no presente ningún indicio de que algo está mal, lo que hace que sea significativamente más difícil detectar la infección. Pueden dañar la relación entre las cadenas de suministro y sus clientes, ya sean usuarios corporativos o domésticos. Al contaminar el software y socavar las infraestructuras de entrega o actualización, los ataques de cadenas de suministro pueden afectar la integridad y seguridad de los bienes y servicios que brindan las organizaciones.

Los ataques de cadenas de suministro han afectado a una amplia gama de software y se han orientado a organizaciones en diferentes sectores y ubicaciones geográficas. La amenaza de los ataques de cadenas de suministro es un problema de toda la industria que requiere atención de varias partes interesadas, incluidos los desarrolladores de software y los proveedores que escriben el código, los administradores del sistema que administran las instalaciones del software y la comunidad de seguridad de la información que detecta estos ataques y crea soluciones para proteger a las personas y al software de ellos.

MÁS ALLÁ DEL SOFTWARE: LA CADENA DE SUMINISTRO COMPROMETE MEDIANTE OBJETOS DE LA NUBE

La capacidad de los ataques de la cadena de suministro para socavar la confianza se agranda y complejiza todavía más en la nube. Varios incidentes de infraestructura, objetos y servicios en la nube comprometidos en 2018 destacan esta complejidad:

- Extensiones de Chrome contaminadas que instalaron malware de fraude por clic (registrado por ICEBRG)
- Diversos repositorios Linux comprometidos (registrados en algunos foros en línea)
- Complementos malintencionados de WordPress utilizados para distintas actividades malintencionadas, 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 cargarlo a la cuenta de Hub de Docker (registrado por Fortinet y Kromtech)
- Un paquete malintencionado de ocupación ilegal de error tipográfico en el repositorio oficial de Python. El paquete contenía un script malintencionado que descarga malware para secuestrar las direcciones de minería de monedas en el portapapeles (registrado en Medium)
- Script comprometido en StatCounter que permitía a los atacantes inyectar un script malintencionado en sitios web que usan StatCounter (registrado por ESET)
- Diversos incidentes de módulos npm de puerta trasera (El blog de npm, Medium) que, si se explotan, podrían dar lugar a situaciones donde, por ejemplo, un atacante ingrese código arbitrario en un servidor activo y lo ejecute.

Estos incidentes demuestran cómo el compromiso de la cadena de suministro puede ampliar inmensamente una superficie de ataque. Si no se protegen, los objetos en la nube pueden ser vectores de entrada inesperados. Por ejemplo, el incidente del Hub de Docker implicaba que una cuenta maliciosa cargara imágenes de Docker que contenían una puerta trasera oculta para la minería de monedas. Las imágenes de Docker se hospedaron en el Hub de Docker durante casi un año y se descargaron millones de veces. Además, las utilizaron administradores y usuarios desprevenidos.

Los riesgos de la cadena de suministro se extienden hasta el código en la nube, el open source, las bibliotecas web, los contenedores y otros objetos de la nube. Estos riesgos, junto con el alto grado de variación entre los incidentes de compromiso de la cadena de suministro de software y hardware que han salido a la luz, hacen que la cadena de suministro ataque una categoría amplia de amenazas. Si bien no existe una solución única para todo el espectro de estos tipos de ataques, las organizaciones tienen que crear una protección preventiva y una detección posterior a la infracción de los ataques de la cadena de suministro de proveedores de hardware y software comprometidos, proveedores y adquisiciones, proveedores de software open source, así como servicios en la nube y proveedores de infraestructura.

Investigación de incidentes cibernéticos con DART

El Equipo de detección y respuesta de Microsoft (DART) es un equipo global de expertos en ciberseguridad y personal de respuesta inmediata a incidentes que ayuda a las organizaciones con la detección, investigación y respuesta a incidentes de ciberseguridad. En esta sección, se destacan algunos de los casos de clientes que DART manejó en el último año. Ilustra las tendencias comunes de los atacantes y cómo Microsoft y los clientes pudieron frustrarlos.

UNA ORGANIZACIÓN DE SERVICIOS PROFESIONALES EXPERIMENTÓ UN ATAQUE AL ESTADO DE LA NACIÓN QUE FILTRÓ DATOS

Una organización de servicios profesionales se vio afectada por una sofisticada amenaza persistente avanzada (APT) patrocinada por el estado que obtuvo acceso a credenciales privilegiadas 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 débiles o ampliamente utilizadas (como "p@ssword" o "123456") para atacar a un gran número de cuentas de usuario y obtener credenciales administrativas de Office 365. (Los ataques de difusión de contraseñas se usan para evitar la detección ya que limitan la cantidad de intentos de inicio de sesión para cada cuenta). Después de infiltrarse en la red, la APT realizó una filtración automatizada y compleja de los datos de los buzones de los empleados. A pesar de los múltiples intentos internos de desalojarlos, los atacantes permanecieron en la red por más de 200 días. Como parte del ataque, el adversario aprovechó el software de la cadena de suministro de la organización y automatizó la filtración de datos.

Debido a que sospechaban de una infracción de los datos de sus clientes, la organización contrató al equipo de DART para investigar y ayudar a prevenir más daños. DART identificó búsquedas orientadas a buzones de correo de Office 365, cuentas comprometidas y canales de comando y control del atacante. Las lecciones clave del cliente de este incidente fueron implementar controles para proteger los servicios en la nube contra amenazas y atacantes basados en la identidad. La organización adoptó la autenticación multifactor (MFA), las directivas de acceso condicional para determinadas aplicaciones en la nube 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 de amenazas de punto final (EDR) para detectar atacantes que pueden estar intentando vulnerar su red. Además, hemos recomendado que esta organización designe un organismo de gobierno en la nube o un equipo de identidad global que administre y aplique las directivas adecuadas de autenticación de usuarios, de modo que la organización supervise su postura de seguridad y pueda mitigar de forma más eficaz el riesgo.

SECCIÓN III

El phishing aún prevalece

En 2018, los analistas de amenazas de Microsoft han evidenciado que los atacantes siguen usando el phishing como el método de ataque preferido. El phishing promete seguir siendo un problema en el futuro próximo porque involucra decisiones y juicios humanos ante los persistentes esfuerzos de los ciberdelincuentes para que las víctimas caigan con sus señuelos.

Las tasas de phishing siguen aumentando
Porcentaje de correos electrónicos entrantes totales que son correos electrónicos de phishing

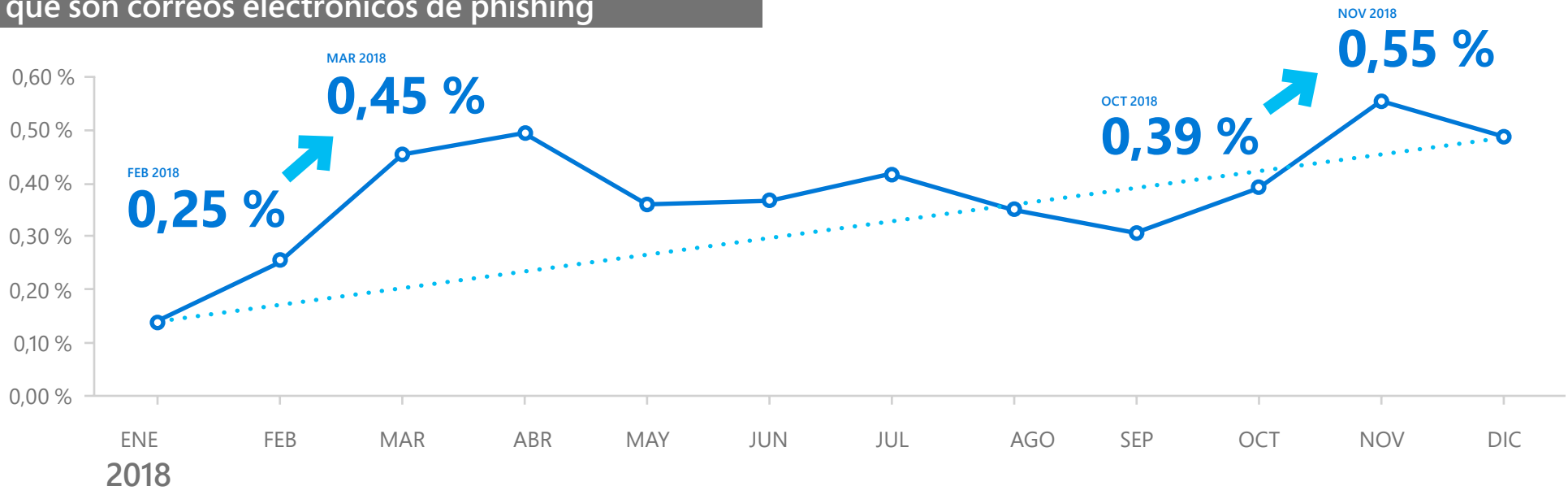


FIGURA 8.

Correos electrónicos de phishing en 2018

EL PHISHING SIGUE SIENDO UN VECTOR PREFERIDO DE ATAQUE EN 2018

Microsoft analiza y escanea en Office 365 más de 470.000 millones de mensajes de correo electrónico al mes en busca de phishing y malware, lo que proporciona a los analistas información considerable de las tendencias y técnicas de los atacantes. La proporción de correos electrónicos entrantes que fueron mensajes de phishing aumentó en un 250 % entre enero y diciembre de 2018. El phishing sigue siendo uno de los principales vectores de ataque utilizados para entregar cargas maliciosas de día cero a los usuarios, y Microsoft ha continuado consolidándose contra estos ataques con protección adicional, detección, investigación y capacidades de respuesta contra el phishing para ayudar a proteger a los usuarios.

Evolución de los métodos de ataques de phishing

A medida que las herramientas y técnicas utilizadas para proteger a las personas del phishing se vuelven más sofisticadas, los atacantes se ven obligados a adaptarse. Los ataques de phishing se han vuelto cada vez más polimórficos, lo que significa que los atacantes no utilizan una sola URL, dominio o dirección IP para enviar correos, sino que usan una infraestructura variada con múltiples puntos de ataque. La naturaleza de los ataques en sí también ha evolucionado, con campañas de phishing modernas que van desde ataques de corto alcance que están activos por solo minutos hasta campañas mucho más extensas de alto volumen. Otros son ataques de variantes seriales, en los que los atacantes envían un pequeño volumen de correo durante varios días sucesivos.

Además, Microsoft ha observado una tendencia hacia los atacantes que utilizan la infraestructura hospedada y otra infraestructura de nube pública, lo que hace que sea más fácil evitar la detección al ocultarse entre sitios y activos legítimos. Por ejemplo, los atacantes utilizan cada vez más sitios y servicios de colaboración y uso compartido de documentos para distribuir cargas maliciosas y formularios de inicio de sesión falsos que se usan para robar credenciales de usuarios. 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 phishing pueden ser orientadas a un objetivo o más amplias

Al igual que con la distribución de malware en general, las campañas de phishing pueden orientarse a un objetivo o ser ataques más genéricos. Aunque los ataques altamente sofisticados generan mayores ganancias monetarias por cada cuenta víctima de phishing, los ataques más genéricos producen menos dinero por cada cuenta comprometida, pero atacan a un conjunto más amplio de usuarios.

Un ejemplo de una campaña sofisticada y orientada es Ursnif, en la que los atacantes localizaron el nombre del archivo del documento para atacar específicamente una organización familiar o la industria del destino. Estos ataques son muy diferentes de las campañas amplias y parecen ser más legítimos y confiables.

Algunas de las campañas amplias en 2018 se relacionaron con el compromiso de correo electrónico empresarial (BEC) y la suplantación de marcas, dominios o usuarios conocidos dentro de las organizaciones de destino y sofisticadas campañas de simulación. La suplantación de dominios es una táctica de ataque común utilizada para atraer a las organizaciones con el fin de que crean que el correo electrónico es digno de confianza y debe abrirse.

Los señuelos del phishing tienen muchas formas

Los investigadores de Microsoft han descubierto que se usan diversos tipos diferentes de señuelos o cargas de phishing en las campañas, entre los que se incluyen los siguientes:

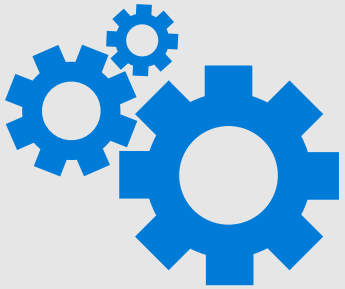
- **Simulación de dominios** (el dominio del mensaje del correo electrónico coincide exactamente con el nombre del dominio original)
- **Suplantación de dominios** (el dominio del mensaje de correo electrónico tiene un aspecto similar al nombre del dominio original)[2]
- **Suplantación de usuarios** (el mensaje de correo electrónico parece provenir de alguien de confianza)
- **Señuelos de texto** (el mensaje de texto parece provenir de una fuente legítima, como un banco, una agencia gubernamental u otra empresa para impartir legitimidad a sus reclamos y normalmente le pide a la víctima que proporcione información confidencial, como nombres de usuario, contraseñas o datos financieros confidenciales)
- **Vínculos de phishing de credenciales** (el mensaje de correo electrónico contiene un vínculo a una página que se asemeja a una página de inicio de sesión de un sitio legítimo, por lo que los usuarios ingresan sus credenciales de inicio de sesión)
- **Archivos adjuntos de phishing** (el mensaje de correo electrónico contiene un archivo adjunto malicioso que el remitente invita a la víctima a abrir)
- **Vínculos hacia ubicaciones falsas de almacenamiento en la nube** (el mensaje de correo electrónico parece provenir de una fuente legítima e invita al usuario a dar permiso y/o ingresar información personal, como credenciales, a cambio de acceso a una ubicación falsa de almacenamiento en la nube)

Esta variedad de señuelos que potencialmente podrían emplear los atacantes aumenta la complejidad de las amenazas de phishing con las que las organizaciones deben lidiar.

NOTAS AL PIE

[2] La suplantación de dominios puede parecerse a la simulación de dominios (coincide exactamente con el nombre del dominio original) en el caso excepcional donde el dominio aparece en el nombre del correo electrónico.

Investigación de incidentes cibernéticos con DART



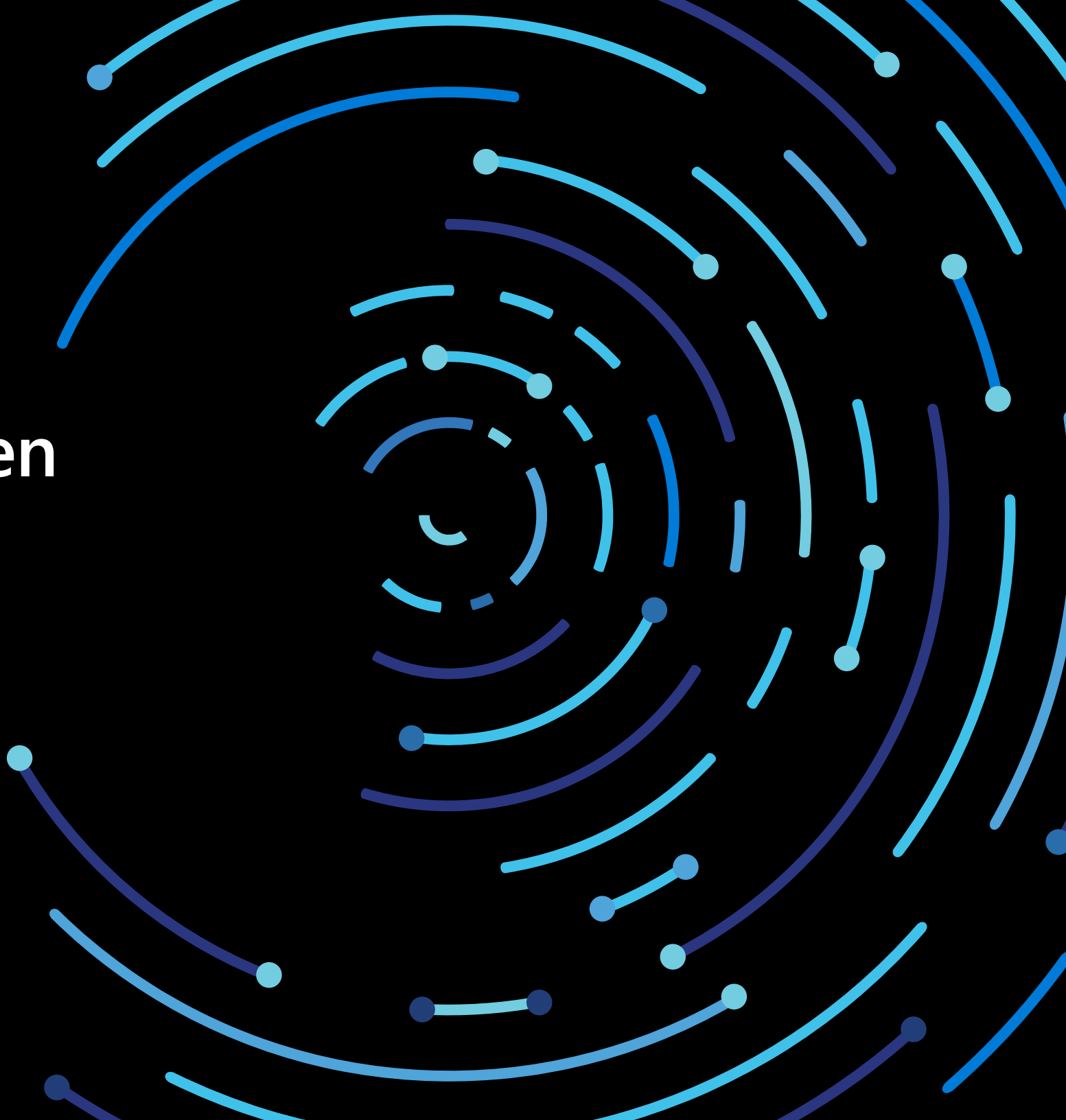
UNA IMPORTANTE ORGANIZACIÓN DE FABRICACIÓN ES GOLPEADA POR INCIDENTES DE PHISHING DIRIGIDOS

Una organización de fabricación enfrentó una campaña de phishing de varias etapas en un lapso de algunos meses. Este enfoque no es extraño. Durante la primera etapa, el atacante realiza el reconocimiento, y en la segunda etapa, se dirige a activos de alto valor. La primera etapa de esta campaña aprovechó una estafa de phishing bien conocida que se basaba en un vínculo a una página web incrustado en un correo electrónico enviado a un pequeño grupo de destino dentro de la organización. El correo electrónico indicaba que el objetivo tenía un documento electrónico importante que debía revisarse, y todo lo que el destinatario tenía que hacer era autenticarse con sus credenciales de dominio para obtener acceso. Esta página de aterrizaje falsa configurada para que el objetivo revisara el supuesto "documento importante" realmente recopiló las credenciales y permitió al atacante acceder a cuentas de 365 de Office desde cualquier parte del mundo. La segunda etapa de la campaña de phishing buscaba enviar correos electrónicos de phishing similares a activos de alto valor dentro de la organización de fabricación, con la esperanza de obtener acceso a datos más valiosos. Microsoft contrató a este cliente durante la segunda etapa de la campaña de phishing. Las lecciones clave que aprendió el cliente a partir de este incidente fueron que el phishing sigue siendo uno de los métodos de ataque más efectivos y que los usuarios siguen siendo el eslabón más débil. Capacitar a los usuarios para que sean cautelosos con las estafas de phishing, tener herramientas listas para identificar a los atacantes y actuar, e instalar parches periódicamente en los sistemas es importante. Si la organización no aborda incluso solo uno de estos factores, 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 cualquier tráfico al canal de comando y control mediante la solución de Microsoft Azure Log Analytics recién implementada. El equipo fue capaz de ayudar a resolver la situación en apenas tres horas. El acceso del atacante se bloqueó, y la organización pudo volcar su atención a la evaluación de daños y la recuperación. DART utilizó las herramientas de Azure Log Analytics para descubrir el comportamiento del atacante, lo que ayudó a detectar muchos desafíos de configuración de la organización. Por ejemplo, DART identificó brechas en la instalación de parches de servidores críticos, descubrió equipos en la red que se comunican con hosts dañinos conocidos en Internet, y también encontró varios servidores importantes sin protección contra malware.

SECCIÓN IV

Malware en el mundo



El malware plantea riesgos a organizaciones e individuos al deteriorar la capacidad de uso, extraer datos, robar propiedad intelectual, generar pérdidas monetarias, provocar angustia emocional e incluso poner en riesgo la vida humana. Microsoft utiliza una amplia gama de herramientas y técnicas para identificar, bloquear y erradicar las infecciones de malware dondequiera que se encuentren.

Las tasas de detección de malware oscilaron entre un 5 % hasta más del 7 % en 2017. A principios de 2018, se elevaron antes de disminuir durante la mayor parte del año a solo un poco más del 4 %. Algunas de las posibles razones de la disminución general de las tasas de detección de malware en el año 2018 son el aumento de la adopción de Windows 10 y el mayor uso de Windows Defender para la protección. La tasa de detección es el porcentaje de equipos que ejecutan el antivirus de Windows Defender que registró la detección de malware durante el mes, incluidos los intentos de infección que Defender bloqueó.

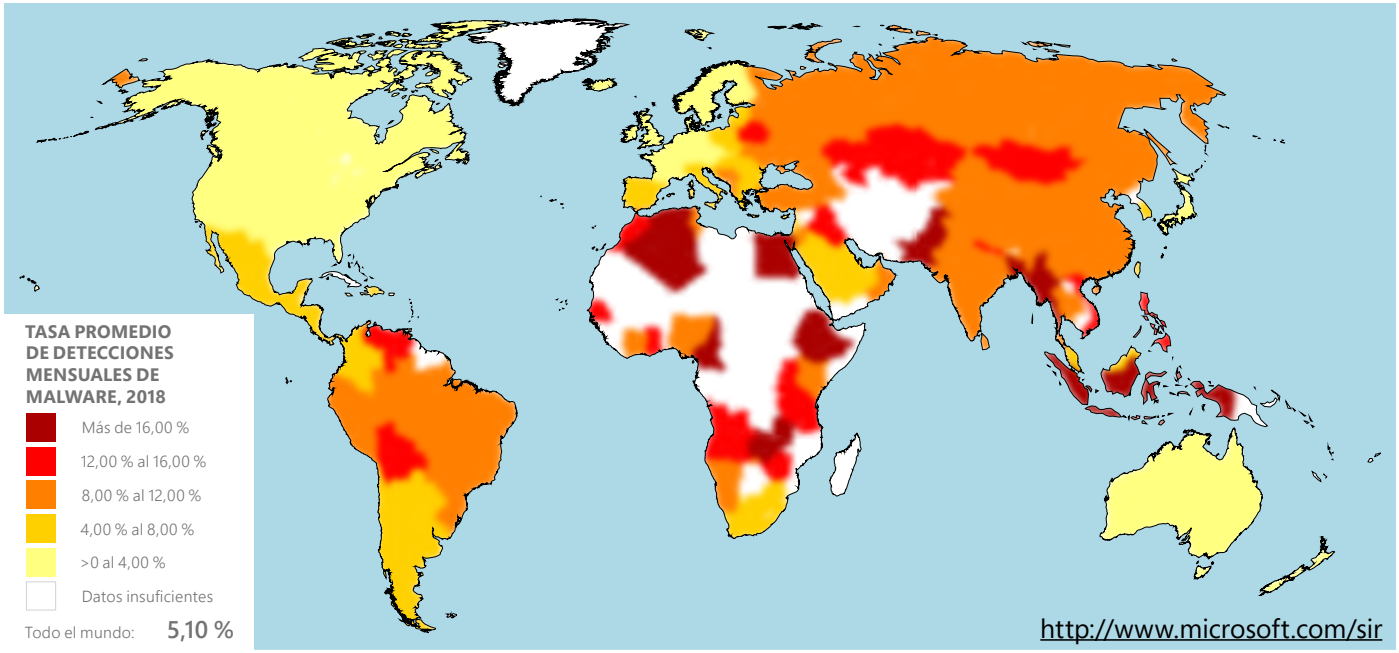


FIGURA 9.

Tasas promedio de detecciones mensuales de malware en todo el mundo por país/región en 2018

Las cinco ubicaciones con las mayores tasas de detección de malware durante el período comprendido entre enero y diciembre de 2018 fueron Etiopía (26,33 % de la tasa promedio de detecciones mensuales), Pakistán (18,94 %), los territorios palestinos (17,50 %), Bangladés (16,95 %) e Indonesia (16,59 %), todas las cuales tenían una tasa de detección mensual promedio de aproximadamente 16,59 % o más durante el período. Las tasas de infección suelen correlacionarse estrechamente con factores de desarrollo humano y la preparación tecnológica dentro de una sociedad. Todos los lugares con las tasas de detección más altas en 2018 se clasificaron en el 40 % inferior de los países y regiones del 2017 índice de tecnologías de información y comunicaciones (ICT), publicado por la Unión Internacional de Telecomunicaciones (ICT) de las Naciones Unidas.

Los cinco países con las tasas de detección de malware más bajas durante ese mismo período fueron Irlanda (1,26 %), Japón (1,51 %), Finlandia (1,74 %), Noruega (1,79 %) y los Países Bajos (1,82 %), todos los cuales tenían una tasa de detección mensual promedio de 1,82 % o menos durante el período. Estas ubicaciones suelen tener infraestructuras de ciberseguridad sólidas y programas bien establecidos para proteger la infraestructura crítica y comunicarse con sus ciudadanos sobre la seguridad básica.

TASAS PROMEDIO MENSUALES DE DETECCIÓN 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 EXPERIMENTARON ATAQUES AL ESTADO DE LA NACIÓN QUE INTERRUMPIERON LAS OPERACIONES

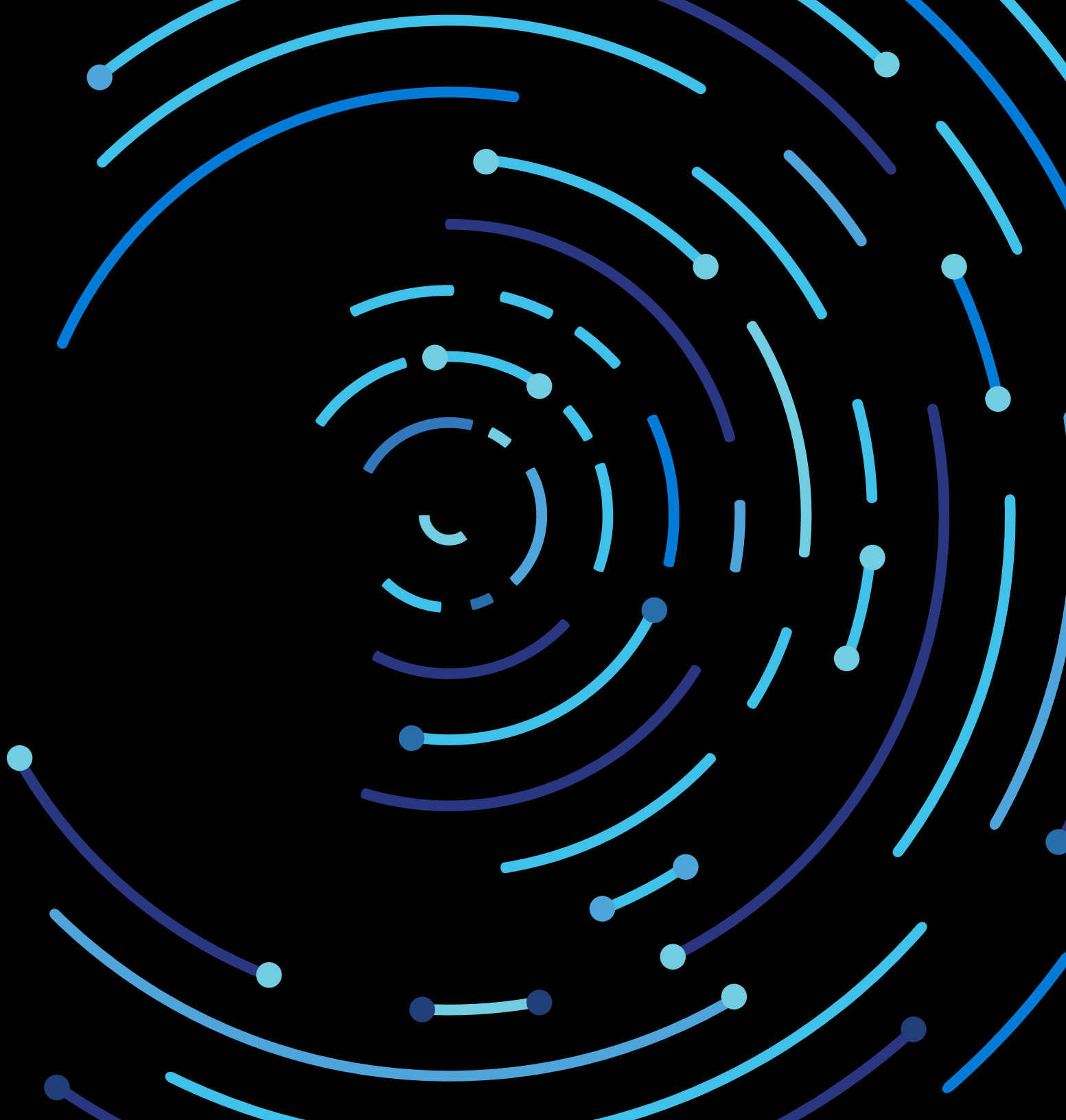
En uno de los incidentes más destructivos que DART ha visto, varias organizaciones de servicios financieros fueron el blanco de una APT patrocinada por el estado (un grupo diferente del que atacó a la organización de servicios profesionales a la que se hace referencia anteriormente) que se manifestó de forma semejante.

Esta APT obtuvo acceso administrativo después de infectar a una máquina paciente cero con un implante de puerta trasera altamente dirigido, confuso y que es posible que se haya entregado mediante un correo electrónico de phishing de objetivo definido. Posteriormente, la APT ejecutó diversas transacciones fraudulentas para transferir grandes sumas de dinero a cuentas bancarias extranjeras. En algunos casos, el atacante permaneció sin ser detectado durante más de 100 días. Cuando el atacante se dio cuenta de que lo habían detectado, desplegó rápidamente un ataque montado con anterioridad para entregar malware destructivo a más de la mitad de los sistemas en el entorno. Las operaciones de estos clientes se paralizaron durante varios días.

A partir de estos incidentes, se extrajeron algunas lecciones clave para el cliente. La primera fue que la administración del ciclo de vida del software es especialmente importante, lo que incluye garantizar que los sistemas se actualicen (sistemas operativos y seguridad), parchen y auditen periódicamente. En un caso, el entorno del sistema Linux de una organización que tenía un número excepcionalmente grande de cargas de trabajo ejecutándose estaba por completo sin administración, lo que lo dejaba frente a un riesgo notablemente alto de sufrir un 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 primarios. Otra lección fue que las soluciones antivirus tradicionales pueden no bastar si necesita conocer la actividad del adversario.

Volver al modo de funcionamiento normal era la prioridad más importante para estas organizaciones. DART ayudó a restaurar los servicios al investigar primero el impacto y luego al tomar las medidas de mitigación necesarias, como eliminar el malware de los sistemas afectados y dejarlos en un estado saludable. Además, el equipo entrenó a los clientes sobre cómo usar las herramientas de investigación de amenazas de Microsoft, incluidas las soluciones de EDR y otras, para que pudieran buscar comportamientos anómalos y actividad de atacantes en su red. DART enfatizó que la supervisión de los puntos de conexión es fundamental para defenderse contra ataques sofisticados y dirigidos que es posible que las soluciones antivirus tradicionales no detecten.

Guía



Guía

Crear resiliencia organizacional y reducir significativamente el riesgo requieren un enfoque de seguridad que incluya prevención, detección y respuesta. Hemos organizado los siguientes procedimientos y controles de seguridad recomendados en esas categorías.

PREVENCIÓN:

Los controles preventivos desempeñan un papel clave en la estrategia de defensa general, ya que las inversiones correctas pueden aumentar el costo de los ataques para los ciberdelincuentes y mantener esos costos de ataque más altos a lo largo del tiempo (sin necesitar que un analista experto supervise e interprete los resultados). Las inversiones de control preventivo deben dirigirse a las técnicas de menor costo para eliminar constantemente las técnicas de ataque baratas y efectivas.

Estos son cuatro aspectos que debe considerar para la prevención:

1. **La higiene de la seguridad es crítica. Como se ve en algunos de los incidentes cibernéticos compartidos en este informe, los problemas de higiene comunes pueden socavar las funcionalidades de seguridad avanzadas, por lo que seguir estos consejos puede ayudar a mitigar el riesgo:**

- Evite el uso de software libre y/o pirateado desconocido. Utilice únicamente software de fuentes de confianza.
- Mitigue el riesgo de robo de credenciales, incluida la protección de cuentas de administrador con privilegios. Para aprender cómo, lea este blog, que describe algunos principios y herramientas que Microsoft ha utilizado para guiar y mejorar nuestra propia postura de seguridad y algunas guías prescriptivas para ayudarle a planificar sus propias iniciativas.
- Aplique las líneas base de configuración segura proporcionadas por los proveedores del software.
- Mantenga las máquinas al día al aplicar rápidamente las actualizaciones más recientes en sus sistemas operativos y aplicaciones, e implemente de inmediato las actualizaciones de seguridad críticas para el sistema operativo, los navegadores y el correo electrónico. Aísle (o retire) máquinas que no se pueden actualizar o reparar.
- Implemente protecciones avanzadas de correo electrónico y navegador. Implemente un gateway de correo electrónico seguro que tenga funciones avanzadas de protección contra amenazas para defenderse contra las variantes modernas de phishing.
- Habilite el antimalware y las defensas de red del host para obtener respuestas de bloqueo casi en tiempo real de la nube (si está disponible en la solución).

2. **Implemente controles de acceso. Considere lo siguiente:**

- Aplique el principio de privilegio mínimo, que incluye implementar la segmentación de red, eliminar privilegios de administrador local de los usuarios finales y ejercer precaución al conceder permisos a las aplicaciones que se ejecutan en el equipo.
- Limite la descarga de aplicaciones solo a aquellas provenientes de fuentes confiables (una tienda de aplicaciones oficial).
- Implemente directivas sólidas de integridad de código, incluida la restricción de las aplicaciones que los usuarios pueden ejecutar. Si es posible, adopte una solución de seguridad que restrinja el código que se ejecuta en el núcleo del sistema (kernel) y que pueda bloquear scripts sin firmar y otras formas de código que no es de confianza. Utilice la lista blanca de aplicaciones.
- Para obtener información sobre los ataques de cadenas de suministro de software y cómo protegerse, lea este blog de investigadores de Microsoft.

3. **Mantenga copias de seguridad.**

- Cree copias de seguridad resistentes a la destrucción de sus sistemas y datos esenciales.
- Use servicios de almacenamiento en la nube para la copia de seguridad automática de datos en línea. En el caso de los datos que se encuentra en las instalaciones locales, realice copias periódicamente de los datos importantes con la regla 3-2-1. Mantenga tres copias de seguridad de sus datos, en dos tipos de almacenamiento diferentes y al menos una copia de seguridad fuera del sitio.

4. **Esté atento y actúe si sospecha algo.**

- Enseñe a los empleados a tener cuidado con las comunicaciones sospechosas que solicitan información confidencial y capacítelos para responder e informar al equipo de operaciones de seguridad de la organización de inmediato. La capacitación también puede ayudar a mitigar los ataques de ingeniería social y de phishing.
- Tenga cuidado al hacer clic en vínculos web. La práctica de hábitos de navegación web seguros 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 criptomonedas.
- Si un equipo funciona extraordinariamente lento, busque archivos sospechosos que se estén ejecutando y siéntase libre de enviar una muestra al proveedor del sistema operativo. Puede enviar archivos para el análisis de malware a Microsoft en https://www.microsoft.com/wdsi/filesubmission.

DETECCIÓN Y RESPUESTA:

La detección y la respuesta contribuyen a la resiliencia ya que limitan el tiempo durante el que un atacante tiene acceso a los recursos. Esto disminuye el ROI del atacante al aumentar sus costos (tiene que reintentarlo o modificar sus operaciones) y reducir el retorno (limita la probabilidad de alcanzar su objetivo).

La misma tecnología de nube que permite a las organizaciones empresariales satisfacer mejor las necesidades del mercado también puede ayudar a las operaciones de seguridad a luchar mejor contra los atacantes.

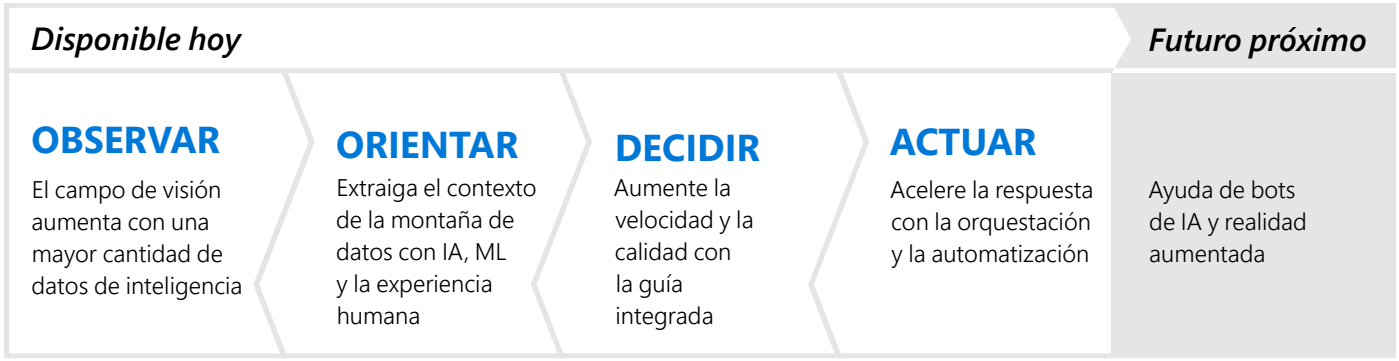


FIGURA 10.

Trayectoria de la evolución de los SOC

Cuando miramos 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" de Observar Orientar Decidir Actuar (OODA) que documentó el Coronel John Boyd de la USAF.[3]

OBSERVAR: los SOC pueden aprovechar una vasta inteligencia de seguridad disponible (de Microsoft y otras fuentes), lo que aumenta tremendamente su campo de visión dentro de la organización y el entorno externo.

ORIENTAR: a medida que estas nuevas fuentes de datos están disponibles para los SOC ya sobrecargados, machine learning (un subconjunto de inteligencia artificial) se convierte en una herramienta esencial para razonar sobre estos conjuntos de datos enormes e identificar anomalías que vale 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 los eventos individuales en incidentes integrales).

DECIDIR: debido a que el volumen y la complejidad de los ataques pueden sobrecargar rápidamente un SOC, los analistas y los equipos de intervención inmediata de incidentes necesitan tomar muchas decisiones y actuar rápidamente en respuesta a alertas y detecciones. Microsoft y otros proveedores han integrado funcionalidades de investigación automatizada, así como orientación para ayudar a los analistas a tomar buenas decisiones rápido (por ejemplo, para aislar los dispositivos potencialmente infectados o comprometidos). Por el momento, la automatización se enfoca en resolver rápidamente incidentes de baja prioridad para que las habilidades especializadas se puedan dedicar a problemas más complejos.

ACTUAR: responder requiere una ejecución rápida y precisa en muchas tecnologías y plataformas, que es lo que permiten las tecnologías de automatización de respuesta y organización de seguridad. Microsoft y muchos otros siguen invirtiendo en estas tecnologías, incluidas la detección moderna de amenazas y soluciones de respuesta automatizada.

NOTAS AL PIE

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

Estas son algunas otras tendencias que se aplican a un SOC moderno:

- **Calidad de feeds de alerta por sobre la cantidad:** a medida que las organizaciones cambian 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 impulsa una mayor necesidad de calidad en las alertas que requieren la participación de los analistas de nivel 1 y 2. Mientras que los feeds de datos adicionales siempre son útiles para las investigaciones y la detección proactiva, el SOC de TI corporativo de Microsoft mide la tasa positiva real de los feeds de alertas que requieren respuesta de los analistas (y, actualmente, requiere un 90 % o más de una tasa positiva real).

- Gravedad de los datos: el análisis de conjuntos de datos de gran tamaño (incluidos datos de seguridad) es difícil sin acceso a los datos subyacentes sin procesar. A medida que más datos de seguridad están disponibles, es más económico y práctico realizar los análisis de seguridad en la nube en lugar de llevar esos datos nuevamente a un sistema local. Esto probablemente conducirá a la evolución de las arquitecturas de SIEM y SOC que pueden incluir enfoques de SIEM híbridos o la adopción de SIEM de nube nativa como servicio.

- **Mucho contexto:** estos tipos de detecciones son mucho más útiles debido a su capacidad para correlacionar los conjuntos de datos de forma más eficaz. Aunque las detecciones tradicionales basadas en el tráfico de red todavía proporcionan cierto valor para la seguridad, el tráfico de red sin procesar suele carecer de contexto para diferenciar entre actividad legítima y actividad anómala. Vemos que los SOC obtienen mucho más valor de las detecciones ricas en contexto, como las siguientes:

  - **Soluciones de detección y respuesta en el punto de conexión (EDR)** que tienen un contexto profundo en la actividad del host
  - Detecciones basadas en identidades que incluyen información sobre los patrones normales de autenticación de usuarios (ubicaciones, horas, servicios a los que se accede, etc.) y aplican análisis de comportamiento

Es más difícil que los adversarios eludan estas detecciones ricas en contexto porque tienen que imitar una operación mucho más compleja (frente a algunos atributos técnicos del tráfico de IP).

Otra lección que hemos aprendido de las principales infracciones a los clientes fue la dificultad de responder con rapidez a los incidentes cuando las funciones de TI se externalizan parcial o totalmente. Le recomendamos que revise los contratos y los acuerdos de nivel de servicio (SLA) de externalización de TI, así como los proveedores de la cadena de suministro, para garantizar que sean compatibles con una respuesta de seguridad rápida. Para más hallazgos de nuestras investigaciones de incidentes de los clientes, consulte la Guía de consulta de respuestas 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 sobre seguridad de Microsoft a través de su oferta de una amplia gama de productos y servicios de Microsoft, 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 información sobre el panorama de amenazas de ciberseguridad en general. Estos datos incluyen análisis de las siguientes fuentes:[4]

- **Azure Security Center** es un servicio que ayuda a las organizaciones a prevenir, detectar y responder a las amenazas proporcionando una mayor visibilidad de la seguridad de las cargas de trabajo en la nube y utilizando análisis avanzados e inteligencia contra 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 buscar contenido malintencionado. Una vez detectado dicho contenido, Bing muestra advertencias a los usuarios para ayudar a prevenir la infección.

- **Exchange Online** es el servicio de productividad y correo electrónico hospedado por Microsoft. Los servicios antimalware y antispam de Exchange Online analizan miles de millones de mensajes cada año para identificar y bloquear el correo no deseado y el malware.

- La **herramienta de eliminación de software malintencionado** (MSRT) es una herramienta gratuita que Microsoft diseñó para ayudar a identificar y eliminar familias de malware prevalentes específicas de los equipos de clientes. La MSRT se lanza principalmente como una actualización importante a través de Windows Update, Microsoft Update y actualizaciones automáticas. Una versión de la herramienta también está disponible en el Centro de descargas de Microsoft. MSRT no reemplaza la solución antivirus actualizada en tiempo real.

- El **Examen de seguridad de Microsoft** es una herramienta de seguridad descargable gratuita que proporciona análisis a petición y ayuda a eliminar el malware y otros programas malintencionados. El Examen de seguridad de Microsoft no sustituye una solución antivirus actualizada, ya que no ofrece protección en tiempo real y no puede impedir que un equipo se infecte.

NOTAS AL PIE

[4]Es importante destacar que estos datos siempre pasan estrictos límites de privacidad y cumplimiento antes de utilizarse para la seguridad.

- **Microsoft Security Essentials** es un producto de protección en tiempo real, gratuito y fácil de descargar 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 contra malware y software no deseado para equipos de escritorio, equipos portátiles y sistemas operativos de servidor empresariales. Utiliza 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 usuarios individuales y organizaciones. Algunos planes de suscripción seleccionados incluyen acceso a Protección contra amenazas avanzada de Office 365.

- **Windows Security** en Windows 10 proporciona análisis en tiempo real y eliminación de malware y software no deseado. Además, la última versión de Windows aprovecha los datos contextuales enriquecidos, como la configuración de máquinas, el rendimiento y el estado del dispositivo, y otra información de este tipo para mejorar la seguridad de los clientes. Al mismo tiempo, facultamos a los clientes para que estén más informados sobre su privacidad en Windows 10. Lea este blog para obtener información sobre algunas de las formas en que Microsoft lo hace.

- La **Protección contra amenazas avanzada de Windows Defender** es un servicio integrado en la Actualización de aniversario de Windows 10 y versiones posteriores que permite a los clientes empresariales detectar, investigar y remediar las amenazas persistentes y las vulneraciones de datos avanzadas en sus redes.

- **Windows Defender Offline** es una herramienta descargable que se puede utilizar para crear un CD, DVD o unidad flash USB de arranque para escanear un equipo en busca de malware y otras amenazas. No ofrece protección en tiempo real y no sustituye una solución antimalware actualizada.

- **Windows Defender SmartScreen**, una característica de Microsoft Edge e Internet Explorer, ofrece protección a los usuarios contra sitios de phishing y sitios que alojan malware. Microsoft mantiene una base de datos de sitios de phishing y malware informados por los usuarios de Microsoft Edge, Internet Explorer y otros productos y servicios de Microsoft. Cuando un usuario intenta visitar un sitio que se encuentra en la base de datos y tiene el filtro activado, el navegador muestra una advertencia y bloquea la navegación a la página.