El malware más buscado de marzo 2024: los hackers descubren un nuevo método de cadena de infección para distribuir Remcos

Los investigadores han descubierto un nuevo método de despliegue del troyano de acceso remoto (RAT) Remcos, que elude las medidas de seguridad habituales para obtener acceso no autorizado a los dispositivos de las víctimas. Mientras tanto, Blackbasta entró en el top tres de los grupos de ransomware más buscados y Comunicaciones saltó al tercer puesto de los sectores más explotados

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder de plataformas de ciberseguridad en la nube basadas en IA, ha publicado su Índice Global de Amenazas para marzo de 2024. El mes pasado, los investigadores revelaron que los hackers estaban utilizando archivos de disco duro virtual (VHD) para desplegar Remcos, un troyano de acceso remoto (RAT). Mientras tanto, Lockbit3 siguió siendo el grupo de ransomware más prevalente en marzo a pesar del desmantelamiento de las fuerzas de seguridad en febrero, aunque su frecuencia en los 200 "sitios de la vergüenza" de ransomware monitorizados por Check Point se redujo del 20% al 12%.

Remcos es un malware conocido que se ha visto en la naturaleza desde 2016. Esta última campaña elude las medidas de seguridad habituales para dar a los ciberdelincuentes acceso no autorizado a los dispositivos de las víctimas. A pesar de sus orígenes legales para administrar remotamente sistemas Windows, los ciberdelincuentes pronto comenzaron a capitalizar la capacidad de la herramienta para infectar dispositivos, capturar capturas de pantalla, registrar pulsaciones de teclas y transmitir los datos recopilados a servidores host designados. Además, el Remote Access Trojan RAT tiene una función de correo masivo que puede promulgar campañas de distribución y, en general, sus diversas funciones pueden utilizarse para crear botnets. El mes pasado, ascendió a la cuarta posición de la lista de principales programas maliciosos desde el sexto puesto que ocupaba en febrero.

"La evolución de las tácticas de ataque pone de manifiesto el incesante avance de las estrategias de los ciberdelincuentes", señala Maya Horowitz, vicepresidenta de Investigación de Check Point Software. "Esto subraya la necesidad de que las organizaciones den prioridad a las medidas proactivas. Permaneciendo vigilantes, desplegando una protección robusta de los endpoints y fomentando una cultura de concienciación sobre la ciberseguridad, podemos fortificar colectivamente nuestras defensas contra las ciberamenazas en evolución."

El Índice de ransomware de Check Point destaca los "sitios de la vergüenza" de ransomware gestionados por grupos de ransomware de doble extorsión que publicaron información sobre las víctimas. Lockbit3 encabeza de nuevo la clasificación con un 12% de los ataques publicados, seguido de Play, con un 10%, y Blackbasta, con un 9%. Blackbasta, que entra por primera vez entre los tres

primeros, reivindicó la autoría de un reciente ciberataque contra Scullion Law, un bufete de abogados escocés.

El mes pasado, la vulnerabilidad más explotada fue "Web Servers Malicious URL Directory Traversal", que afectó al 50% de las organizaciones de todo el mundo, seguida de cerca por "Command Injection Over HTTP", con un 48%, y "HTTP Headers Remote Code Execution", con un 43%.

Principales familias de malware

**Las flechas se refieren al cambio de rango con respecto al mes anterior.*

FakeUpdates fue el malware más extendido el mes pasado, con un impacto del **6%** en organizaciones de todo el mundo, seguido de **Qbot**, con **un 3%**, y **Formbook**, con **un 2%.**

1. ↔ **FakeUpdates** - FakeUpdates (AKA SocGholish) es un descargador escrito en JavaScript. Escribe las cargas útiles en el disco antes de lanzarlas. FakeUpdates condujo a un mayor compromiso a través de muchos programas maliciosos adicionales, incluyendo GootLoader, Dridex, NetSupport, DoppelPaymer, y AZORult.

2. ↔ **Qbot -** Qbot AKA Qakbot es un malware multipropósito que apareció por primera vez en 2008. Fue diseñado para robar las credenciales del usuario, registrar las pulsaciones de teclado, robar cookies de los navegadores, espiar las actividades bancarias y desplegar malware adicional. Qbot, que suele distribuirse a través de correo electrónico no deseado, emplea varias técnicas anti-VM, anti-depuración y anti-sandbox para dificultar el análisis y eludir la detección. A partir de 2022, se convirtió en uno de los troyanos más frecuentes.

3. ↔ **Formbook** - Formbook es un Infostealer dirigido al sistema operativo Windows y fue detectado por primera vez en 2016. Se comercializa como Malware as a Service (MaaS) en foros clandestinos de hacking por sus potentes técnicas de evasión y su precio relativamente bajo. Formbook obtiene credenciales de varios navegadores web, recopila capturas de pantalla, monitoriza y registra las pulsaciones de teclado, y puede descargar y ejecutar archivos según las órdenes de su C&C.

Principales vulnerabilidades explotadas

El mes pasado, "**Web Servers Malicious URL Directory Traversal**" seguía siendo la vulnerabilidad más explotada, afectando al **50% de las** organizaciones en todo el mundo. Le siguieron la "**Inyección de comandos a través de HTTP",** con **un 48%**, y la **"Ejecución remota de código de encabezados HTTP"**, con **un 43%**.

1. ↔ **Web Servers Malicious URL Directory Traversal (CVE-2010-4598,CVE-2011-2474,CVE-2014-0130,CVE-2014-0780,CVE-2015-0666,CVE-2015-4068,CVE-2015-7254,CVE-2016-4523,CVE-2016-8530,CVE-2017-11512,CVE-2018-3948,CVE-2018-3949,CVE-2019-18952,CVE-2020-5410,CVE-2020-8260) -** Existe una vulnerabilidad de directory traversal en diferentes servidores web. La vulnerabilidad se debe a un error de validación de entrada en un servidor web que no sanea correctamente el URI para los patrones de directory traversal. Una explotación exitosa

permite a atacantes remotos no autenticados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

2. ↔ Inyección de comandos a través de HTTP **(CVE-2021-43936, CVE-2022-24086)** - Se ha informado de una vulnerabilidad de inyección de comandos a través de HTTP. Un atacante remoto puede explotar este problema enviando una solicitud especialmente diseñada a la víctima. Una explotación exitosa permitiría a un atacante ejecutar código arbitrario en la máquina objetivo.

3. **↑ Ejecución remota de código en cabeceras HTTP (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-1375) - Las cabeceras HTTP** permiten al cliente y al servidor pasar información adicional con una petición HTTP. Un atacante remoto puede utilizar una cabecera HTTP vulnerable para ejecutar código arbitrario en la máquina víctima**.**

Principales programas maliciosos para móviles

El mes pasado, **Anubis ocupó** el primer puesto como malware para móviles más extendido, seguido de **AhMyth** y **Cerberus**.

1. ↔ **Anubis** - Anubis es un troyano bancario diseñado para teléfonos móviles Android. Desde que se detectó inicialmente, ha ganado funciones adicionales, incluyendo la funcionalidad de troyano de acceso remoto (RAT), keylogger, capacidades de grabación de audio y varias características de ransomware. Se ha detectado en cientos de aplicaciones diferentes disponibles en Google Store.

2. ↔ **AhMyth** - AhMyth es un troyano de acceso remoto (RAT) descubierto en 2017. Se distribuye a través de aplicaciones Android que se pueden encontrar en tiendas de aplicaciones y en varios sitios web. Cuando un usuario instala una de estas apps infectadas, el malware puede recopilar información sensible del dispositivo y realizar acciones como keylogging, tomar capturas de pantalla, enviar mensajes SMS y activar la cámara, que suele utilizarse para robar información sensible.

3. **↑ Cerberus** - Visto por primera vez en estado salvaje en junio de 2019, Cerberus es un troyano de acceso remoto (RAT) con funciones específicas de superposición de pantalla bancaria para dispositivos Android. Cerberus opera en un modelo de Malware como Servicio (MaaS), ocupando el lugar de banqueros descontinuados como Anubis y Exobot. Sus funciones incluyen control de SMS, key-logging, grabación de audio, rastreador de localización, etc.

Industrias más atacadas en todo el mundo

El mes pasado, Educación/Investigación se mantuvo en el primer puesto de los sectores más atacados a escala mundial, seguido de Gobierno/Militar y Comunicaciones.

1. Educación/Investigación
2. Gobierno/Militar
3. Comunicaciones

Principales grupos de ransomware

Esta sección presenta información procedente de "sitios de la vergüenza" de ransomware operados por grupos de ransomware de doble extorsión que publicaron los nombres y la información de las víctimas. Los datos de estos sitios de la vergüenza tienen sus propios sesgos, pero aún así proporcionan información valiosa sobre el ecosistema del ransomware.

Lockbit3 fue el grupo de ransomware más prevalente el mes pasado, responsable del **12% de** los ataques publicados, seguido de **Play** con el **10%** y **Blackbasta** con **el 9%**.

1. **LockBit3** - LockBit3 es un ransomware, que opera en un modelo RaaS, reportado por primera vez en septiembre de 2019. LockBit se dirige a grandes empresas y entidades gubernamentales de varios países y no se dirige a individuos en Rusia o la Comunidad de Estados Independientes. A pesar de experimentar importantes interrupciones en febrero de 2024 debido a la acción de las fuerzas de seguridad, LockBit3 ha reanudado la publicación de información sobre sus víctimas.
2. **Play -** Play Ransomware, también conocido como PlayCrypt, es un grupo de ransomware que surgió por primera vez en junio de 2022. Este ransomware se ha dirigido a un amplio espectro de empresas e infraestructuras críticas en Norteamérica, Sudamérica y Europa, afectando a aproximadamente 300 entidades en octubre de 2023. El ransomware Play suele acceder a las redes a través de cuentas válidas comprometidas o aprovechando vulnerabilidades no parcheadas, como las de las VPN SSL de Fortinet. Una vez dentro, emplea técnicas como el uso de binarios "living-off-the-land" (LOLBins) para tareas como la exfiltración de datos y el robo de credenciales.
3. Blackbasta - El ransomware BlackBasta se observó por primera vez en 2022 y funciona como ransomware como servicio (RaaS). Los autores de la amenaza se dirigen principalmente a organizaciones y particulares aprovechando vulnerabilidades RDP y correos electrónicos de phishing para distribuir el ransomware.

Siga a Check Point a través de:
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies
X: https://www.twitter.com/checkpointsw
Facebook: https://www.facebook.com/checkpointsoftware
Blog: https://blog.checkpoint.com
YouTube: https://www.youtube.com/user/CPGlobal

Acerca de Check Point Research
Check Point Research proporciona inteligencia líder sobre ciberamenazas a los clientes de Check Point Software y a la comunidad de inteligencia en general. El equipo de investigación recopila y analiza datos de ciberataques globales almacenados en ThreatCloud para mantener a raya a los hackers, al tiempo que garantiza que todos los productos de Check Point estén actualizados con las últimas protecciones. El equipo de investigación está formado por más de 100 analistas e investigadores que cooperan con otros proveedores de seguridad, fuerzas de seguridad y varios CERT.

Acerca de Check Point Software Technologies Ltd.
Check Point Software Technologies Ltd. () (www.checkpoint.com) es un proveedor líder de plataformas de ciberseguridad en la nube basadas en IA que protege a más de 100.000 organizaciones en todo el mundo. Check Point aprovecha el poder de la IA en todas partes para mejorar la eficiencia y precisión de la ciberseguridad a través de su Plataforma Infinity, con tasas de captura líderes en la industria que permiten la anticipación proactiva de amenazas y tiempos de respuesta más inteligentes y rápidos. La plataforma integral incluye tecnologías en la nube que consisten en Check Point Harmony para asegurar el espacio de trabajo, Check Point CloudGuard para asegurar la nube, Check Point Quantum para asegurar la red y Check Point Infinity Core Services para operaciones y servicios de seguridad colaborativos.

CONTACTO CON LOS MEDIOS DE COMUNICACIÓN
Marcela Ernst

Cel: 54 9 11 6 870 0368
Brand Partners
marcela@brand-partners.com.ar

