Publicado en Madrid el 15/04/2024

Los ciberdelincuentes descubren un nuevo método de infección en cadena para distribuir Remcos

Check Point Research destaca que España ha experimentado una disminución del 2% de los ataques malware desde febrero. FakeUpdates es, por segundo mes consecutivo, el principal malware en nuestro país

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder en soluciones de ciberseguridad en la nube basadas en IA, publica su Índice Global de Amenazas del mes de marzo de 2024 donde se recoge el uso archivos de Disco Duro Virtual (VHD) para desplegar el troyano de acceso remoto (RAT) Remcos. Mientras tanto, Lockbit3 se mantiene como el grupo de ransomware más prevalente a pesar de la intervención policial en febrero, aunque su frecuencia en los "shame sites" de ransomware monitorizado por Check Point Software se redujo del 20% al 12%.

Remcos es un malware que ha estado en circulando libremente desde 2016. Esta última campaña ha logrado eludir las medidas de seguridad y dar a los ciberdelincuentes acceso no autorizado a los dispositivos de las víctimas. A pesar de sus orígenes legítimos para administrar de forma remota sistemas Windows, los atacantes pronto comenzaron a infectar dispositivos, hacer capturas de pantalla, registrar pulsaciones de teclas y transmitir los datos recopilados a servidores host. Además, el troyano de acceso remoto RAT tiene la función de envío masivo de correos electrónicos que puede poner en marcha campañas de distribución y, en general, sus diversas funciones pueden usarse para crear botnets. El mes pasado, ascendió al cuarto lugar en la lista de malware principal y consigue ascender dos puestos desde febrero.

"En la evolución de las tácticas de ataque destaca el avance en las estrategias de los ciberdelincuentes", comenta Maya Horowitz, VP de Investigación de Check Point Software. "Esto subraya la necesidad de que las empresas prioricen medidas proactivas. Manteniéndonos alerta, desplegando una protección de endpoint sólida y fomentando una cultura de conciencia de ciberseguridad, se puede fortalecer en conjunto las defensas contra los ciberataques en evolución".

El índice de amenazas de Check Point Research también incluye información de alrededor de 200 páginas web de contenido sospechoso dirigidos por grupos ransomware de doble extorsión, 68 de las cuales publicaron información de sus víctimas este año para presionarles cuando no querían pagar. Lockbit3 continúa siendo el ransomware más significativo, con un 12% de incidentes detectados, seguido por 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 a Scullion Law, una firma legal escocesa.

CPR también ha revelado que "Web Servers Malicious URL Directory Traversal " ha sido la vulnerabilidad más explotada, afectando a un 50% de las empresas, seguida de "Inyección de comandos sobre HTTP" con un 48%, y "Ejecución de código remoto a través de cabeceras HTTP", con un 43%.

Los tres malware más buscados en España en marzo
*Las flechas indican el cambio en el ranking en comparación con el mes pasado.

Check Point Research destaca que España ha experimentado una disminución del 2% de los ataques malware desde febrero. Estos son los tres malware más buscados en el país:

? FakeUpdates – Downloader escrito en JavaScript. Escribe las payloads en el disco antes de lanzarlas. Fakeupdates ha llevado a muchos otros programas maliciosos, como GootLoader, Dridex, NetSupport, DoppelPaymer y AZORult. Este downloader ha impactado en el 9.37% de las empresas en España.
? Remcos – Remcos es un RAT que apareció por primera vez en la naturaleza en 2016. Remcos se distribuye a través de documentos maliciosos de Microsoft Office que se adjuntan a correos electrónicos no deseados y está diseñado para eludir la seguridad de Control de Cuentas de Usuario (UAC) de Microsoft Windows y ejecutar malware con privilegios de alto nivel. El malware ha afectado al 6.42% de compañías españolas.
? Qbot – Qbot es un malware multifunción que apareció por primera vez en 2008. Fue diseñado para robar las credenciales de los usuarios, registrar pulsaciones de teclas, sustraer las cookies de los navegadores, espiar actividades bancarias e implementar malware adicional. A menudo se distribuye a través de correos electrónicos no deseados, y emplea diversas técnicas anti-VM, anti-debuggin y anti-sandbox para obstaculizar el análisis y eludir la detección. Desde 2022, se ha posicionado como uno de los troyanos predominantes. El malware ha vuelto a afectar al 4.08% de empresas españolas.

Las tres industrias más atacadas en Europa en marzo
El mes pasado, Educación/Investigación se situó como la industria más atacada en España, seguida de Gobierno/Militar y Sanidad.

Educación/Investigación
Gobierno/Militar
Sanidad

Las tres vulnerabilidades más explotadas en marzo
Por otra parte, Check Point Software señala que el mes pasado la vulnerabilidad más explotada fue "Travesía de directorios de URL maliciosas en servidores web" impactando en un 50% de las empresas de todo el mundo, seguida de "Inyección de comandos sobre HTTP" con un 48% y "Ejecución remota de código a través de encabezados HTTP" con un 43%.

? 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 travesía de directorios en diferentes servidores web. La vulnerabilidad se debe a un error de validación de entrada

en un servidor web que no desinfecta correctamente la URI para los patrones de travesía de directorios. La explotación exitosa permite a atacantes remotos no autenticados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

? Command Injection Over HTTP (CVE-2021-43936, CVE-2022-24086) – Se ha informado de una vulnerabilidad de inyección de comandos sobre HTTP. Un atacante remoto puede explotar este problema enviando una solicitud especialmente diseñada a la víctima. La explotación exitosa permitiría a un atacante ejecutar código arbitrario en la máquina objetivo.

? HTTP Headers Remote Code Execution (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-1375) – Los encabezados HTTP permiten que el cliente y el servidor pasen información adicional con una solicitud HTTP. Un atacante remoto puede utilizar un encabezado HTTP vulnerable para ejecutar código arbitrario en la máquina víctima.

Los tres malware móviles más usados en marzo

El mes pasado Anubis se mantuvo en el primer lugar como el malware móvil más usado, seguido de AhMyth y Cerberus.

Anubis – Malware troyano bancario diseñado para teléfonos móviles Android. Desde que se detectó ha ido sumando funciones adicionales como capacidades de troyano de acceso remoto (RAT), keylogger, grabación de audio y varias características de ransomware. Se ha detectado en cientos de aplicaciones diferentes disponibles en Google Store.

AhMyth – Troyano de acceso remoto (RAT) descubierto en 2017. Se distribuye a través de aplicaciones de Android que se pueden encontrar en tiendas de aplicaciones y varios sitios web. Cuando un usuario instala una de estas aplicaciones infectadas, el malware puede recopilar información confidencial del dispositivo y realizar acciones como el registro de teclas, capturas de pantalla, el envío de mensajes SMS y la activación de la cámara, lo que se suele usar para robar información sensible.

Cerberus – Visto por primera vez en la naturaleza 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 características incluyen control de SMS, keylogging, grabación de audio, rastreador de ubicación, y más.

Los tres grupos ransomware más destacados en marzo

Esta sección se basa en información recibida de más de 200 "shame sites" ejecutadas por grupos ransomware de doble extorsión que publicaron los nombres e información de las víctimas. Los datos de estos sitios tienen sus propios sesgos, pero aun así proporcionan información valiosa sobre el ecosistema del ransomware.

En el último mes, LockBit3 ha sido el ransomware más destacado, responsable del 12% de los ataques realizados, seguido de Play con un 10% y Blackbasta con un 9%.

LockBit3 - LockBit3 es un ransomware que opera en un modelo de RaaS, reportado por primera vez en septiembre de 2019. LockBit tiene como objetivo a grandes empresas y entidades gubernamentales

de varios países y no apunta a individuos en Rusia o la Comunidad de Estados Independientes. A pesar de experimentar interrupciones significativas en febrero de 2024 debido a la acción de las fuerzas del orden, LockBit3 ha reanudado la publicación de información sobre sus víctimas.

Play - Play Ransomware, también conocido como PlayCrypt, es un grupo de ransomware que surgió por primera vez en junio de 2022. Este ransomware ha dirigido un amplio espectro de empresas e infraestructuras críticas en América del Norte, América del Sur y Europa, afectando aproximadamente a 300 entidades para octubre de 2023. Play Ransomware suele obtener acceso a redes a través de cuentas válidas comprometidas o mediante la explotación de vulnerabilidades no parcheadas, como las de los Fortinet SSL VPN. Una vez dentro, emplea técnicas como el uso de binarios de "living-off-the-land" (LOLBins) para tareas como la exfiltración de datos y el robo de credenciales.

Blackbasta - El ransomware BlackBasta se observó por primera vez en 2022 y opera como ransomware como servicio (RaaS). Los actores de amenazas detrás de él principalmente tienen como objetivo a organizaciones e individuos mediante la explotación de vulnerabilidades de RDP y correos electrónicos de phishing para entregar el ransomware.

La lista completa de las diez principales familias de malware en marzo puede consultarse en el blog de Check Point Software.

Datos de contacto:
EverythinkPR
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Inteligencia Artificial y Robótica Madrid Emprendedores Software Ciberseguridad Dispositivos móviles Innovación Tecnológica Digital