Publicado en Madrid el 14/05/2024

El malware más buscado en abril de 2024: aumento de ataques de Androxgh0st y declive de LockBit3

Check point Research ha identificado un aumento en los ataques de Androxgh0st, un troyano que afecta plataformas Windows, Mac y Linux, lo que le ha permitido ascender al segundo lugar en la lista de malware más destacado.

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 abril de 2024. El mes pasado, los investigadores revelaron un aumento significativo en el uso de ataques Androxgh0st, con el malware utilizado como herramienta para robar información confidencial mediante botnets. A pesar de una caída del 55% en su tasa de detección desde principios de año, LockBit3 se mantuvo como el grupo de ransomware más prevalente en abril, lo que ha reducido su impacto mundial del 20% al 9%.

Los investigadores han monitorizado las actividades de Androxgh0st desde su aparición en diciembre de 2022. Los atacantes, que aprovechan vulnerabilidades como CVE-2021-3129 y CVE-2024-1709, despliegan web shells para el control remoto mientras se centran en construir botnets para el robo de credenciales. Así se señala en un aviso conjunto sobre ciberseguridad publicado por el FBI y el CISA. En particular, este operador de malware se ha asociado con la distribución del ransomware Adhublika. Los actores de Androxgh0st han demostrado una preferencia por explotar vulnerabilidades en aplicaciones Laravel para robar credenciales de servicios en la nube como AWS, SendGrid y Twilio.

Mientras tanto, Check Point Software destaca en su lista los "shame sites" -gestionados por grupos de ransomware de doble extorsión- que publican información sobre las víctimas para presionar a los objetivos que no pagan. LockBit3 encabeza de nuevo la clasificación con un 9% de los ataques, seguido de Play, con un 7%, y 8Base, con un 6%. 8Base, que vuelve a estar entre los tres primeros, afirmó recientemente que se había infiltrado en los sistemas informáticos de las Naciones Unidas y había filtrado información sobre recursos humanos y adquisiciones. Aunque LockBit3 sigue en primer lugar, el grupo ha sufrido varios reveses. En febrero, el sitio de filtración de datos fue incautado en el marco de una campaña interinstitucional denominada Operación Cronos, mientras que este mes, los mismos organismos internacionales encargados de la aplicación de la ley publicaron nuevos detalles, identificando a 194 afiliados que utilizaban LockBit3 junto con el desenmascaramiento y sanción del líder del grupo.

"Nuestra investigación ha demostrado que los esfuerzos internacionales colectivos para desactivar LockBit3 parecen haber tenido éxito puesto que se ha reducido su impacto en más del 50% desde el inicio de 2024", señala Maya Horowitz, vicepresidenta de investigación de Check Point Software. "Las empresas deben seguir priorizando su ciberseguridad siendo proactivas y reforzando la red, los endpoints y el correo electrónico. Implementar defensas multicapa y establecer copias de seguridad robustas, procedimientos de recuperación y planes de respuesta a incidentes sigue siendo clave para impulsar la ciberresiliencia.

El mes pasado, las vulnerabilidades más explotadas a nivel mundial fueron "Command Injection Over HTTP" y "Web Servers Malicious URL Directory Traversal", que afectaron al 52% de las empresas. Les siguió la " HTTP Headers Remote Code Execution", con un impacto global del 45%.

Los tres malware más buscados en España en abril
*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 1% de los ataques malware desde marzo. 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 6% de las empresas en España.
? Androxgh0st – Androxgh0st es un botnet que afecta a plataformas Windows, Mac y Linux. Para la infección inicial, Androxgh0st explota múltiples vulnerabilidades, específicamente dirigidas al PHPUnit, el Marco de Trabajo de Laravel y el Servidor Web Apache. El malware roba información sensible como cuentas de Twilio, credenciales SMTP, llave AWS, etc. Utiliza archivos de Laravel para recolectar la información requerida. Tiene diferentes variantes que escanean para diferente información. Este botnet ha impactado al 4% de las empresas en España.
? 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 3% de empresas españolas.

Las tres industrias más atacadas en España en abril
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 abril
Por otra parte, Check Point Software señala que el mes pasado las vulnerabilidades más explotadas fueron "Command Injection Over HTTP" y "Web Servers Malicious URL Directory Traversal", impactando en un 52% de las empresas de todo el mundo, seguida de "HTTP Headers Remote Code Execution" con un 45%.

? 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.

? 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.

? 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 abril

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

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.

Hiddad – Hiddad es un malware para Android que re empaqueta aplicaciones legítimas y las coloca en la tienda de un tercero. Su función principal es mostrar anuncios, pero también puede obtener acceso a detalles de seguridad clave integrados en el sistema operativo.

Los tres grupos ransomware más destacados en abril

Esta sección se basa en información recibida de más de 200 "shame sites" ejecutados 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 9% de los ataques realizados, seguido de Play con un 7% y 8Base con un 6%.

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.

8base – Esta banda de ransomware ha estado activa desde marzo de 2022. Ganó notoriedad a mediados de 2023 con un notable aumento de su actividad. Este grupo usa diversas variantes de ransomware, siendo Phobos un elemento común. 8Base opera con gran nivel de sofisticación y técnicas avanzadas. Sus métodos de ataque incluyen tácticas de doble extorsión.

La lista completa de las diez principales familias de malware en abril 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 Software Ciberseguridad Dispositivos móviles Innovación Tecnológica Digital Actualidad Empresarial