Publicado en Madrid el 15/02/2024

El malware más buscado en enero de 2024: descubierta la operación de VexTrio y Lockbit3, que se sitúa como el ransomware más destacado

Se ha destapado un gran distribuidor de ciberataques conocido como VexTrio, un intermediario de tráfico para que los ciberdelincuentes distribuyan contenido malicioso. LockBit3 se sitúa en el primer puesto de ransomware activos después de una serie de ataques en enero

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder en soluciones de ciberseguridad en la nube basadas en IA, ha publicado su Índice Global de Amenazas del mes de enero de 2024. El mes pasado, se identificó un nuevo sistema de distribución de tráfico (TDS) llamado VexTrio, que ha ayudado a más de 60 afiliados a través de una red en la que hay más de 70 mil sitios webs comprometidos. Por otro lado, LockBit3 se ha posicionado como el principal ransomware y el sector de la educación ha continuado siendo el más afectado a nivel mundial.

VexTrio ha estado activo desde 2017 colaborando con docenas de asociados para difundir contenido malicioso a través de un sofisticado TDS. A Mediante un método semejante al de las plataformas de marketing legítimo, las actividades de VexTrio suelen ser difíciles de detectar y, a pesar de llevar más de seis años en activo, la magnitud de sus operaciones ha pasado prácticamente desapercibida. Dada su extensa red de propagación, la sofisticación de sus operaciones y el sigilo con el que actúa, se ha convertido en un riesgo considerable para la ciberseguridad.

"Los atacantes han pasado de ser simples ciberdelincuentes a convertirse en arquitectos del engaño. VexTrio es otro recordatorio del enfoque claramente comercial que está siendo el sector" dijo Maya Horowitz, VP de investigación en Check Point Software. "Las empresas deben priorizar las actualizaciones regulares de sus sistemas, emplear una protección endpoint eficaz y fomentar la prevención y la vigilancia de estos ciberataques. Si se informa, se puede fortalecer colectivamente las defensas contra los ciberriesgos en constante evolución".

Por primera vez, Check Point Research ha incluido una clasificación de los grupos ransomware predominantes, basándose en la actividad de más de 200 sitios web de contenido sospechoso. El último mes, LockBit3 fue el ransomware más significativo, responsable del 20% de los ciberataques.

CPR también ha revelado que "Command Injection Over HTTP" ha sido la vulnerabilidad más explotada, afectando a un 44% de las empresas, seguida de "Web Servers Malicious URL Directory Traversal" con un impacto del 41% y "HTTP Headers Remote Code Execution" con un impacto global del 40%.

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

España ha experimentado una disminución del 8% de los ataques, con un 37,9 de riesgo, y estos son los tres malware más buscados en el país:

? 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 afectado en el 4,3% de las empresas españolas.

? 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 4,2% de las empresas en España.

? Formbook – Infostealer (ladrón de información) que tiene como objetivo el sistema operativo de Windows y fue el primero detectado en 2016. Se comercializa como ‘Malware como servicio’ en foros de hacking clandestinos debido a sus sólidas técnicas de evasión y a su precio relativamente bajo. FormBook recopila credenciales de varios buscadores webs, realiza capturas de pantallas, supervisa y registra las pulsaciones del teclado, y puede descargar y ejecutar archivos según las órdenes de su centro de control. Este infostealer ha impactado en un 3,1% de las empresas españolas.

Las tres industrias más atacadas en España en enero

El mes pasado, Sanidad se situó como la industria más atacada en España, seguida de Gobierno/Militar y Finanzas/Banca.

Sanidad
Gobierno/Militar
Finanzas/Banca

Las tres vulnerabilidades más explotadas en enero

Por otra parte, Check Point Software señala que el mes pasado la vulnerabilidad más explotada fue "Command Injection Over HTTP", impactando en un 44% de las empresas de todo el mundo, seguida de "Web Servers Malicious URL Directory Traversal", con un impacto del 41% y "HTTP Headers Remote Code Execution" con un impacto global del 40%.

? Command Injection Over HTTP (CVE-2021-43936, CVE-2022-24086) – Se ha detectado una vulnerabilidad de inyección de comandos a través de HTPP. La explotación de esta vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios en el sistema objetivo a través del envío de solicitudes diseñadas específicamente para la víctima.

? 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. Esta vulnerabilidad se debe a un error de validación de la entrada en servidores web que no ha desinfectado adecuadamente la URL. Una explotación exitosa permite a los atacantes remotos sin autentificar revelar o acceder a cualquier archivo del servidor atacado.

? HTTP Headers Remote Code Execution – Esta vulnerabilidad permite que el cliente y el servidor intercambien información adicional con una solicitud HTTP. La explotación de esta vulnerabilidad puede permitir que un atacante remoto ejecute un código arbitrario en el dispositivo afectado.

Los tres malware móviles más usados en enero

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 recopila información confidencial del dispositivo y realiza acciones como el registro de teclado, 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 enero

Esta sección se basa en información recibida de más de 200 "shame sites", páginas webs de difamación ejecutadas por grupos ransomware de doble extorsión en los que han publicado nombres e información de las víctimas. Los ciberdelincuentes utilizan estas páginas para presionar a las víctimas a que paguen el rescate de forma inmediata. En el último mes, LockBit3 ha sido el ransomware más destacado, responsable del 20% de los ataques realizados, seguido de 8Base con un 10%, y Akira con un 9%.

LockBit3 – Se trata de un ransomware que opera bajo un modelo de RaaS, detectado por primera vez en septiembre de 2019. Sus principales objetivos son grandes empresas y entidades gubernamentales de diferentes países y no tiene como objetivo ni a Rusia ni a la Comunidad de Estados Independientes.

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.

Akira – Fue detectado por primera vez a principios de 2023, teniendo como objetivo los sistemas de Windows y Linux. Emplea cifrado simétrico con CryptGenRandom y Chacha 2008 para encriptar los archivos y es similar al ransomware Conti v2. Akira se distribuye a través de vías diferentes, incluyendo archivos infectados adjuntos en correos electrónicos y exploits en endpoints de VPN. Tras la infección,

encripta los datos y añade la extensión".akira" a los nombres de los archivos, luego presenta una nota de rescate exigiendo el pago para el descifrado.

La lista completa de las diez principales familias de malware en enero 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: Nacional Medicina Finanzas Inteligencia Artificial y Robótica Madrid Software Ciberseguridad Dispositivos móviles Otras Industrias Innovación Tecnológica