Publicado en Madrid el 13/03/2024

Check Point Software descubre una nueva campaña de FakeUpdates que ataca las páginas web hechas con Wordpress

España continúa experimentando una disminución de los ataques, esta vez del 7%. Debido a su nueva campaña, FakeUpdates se posiciona como principal malware en España y arrebata el puesto a Qbot

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder de soluciones de ciberseguridad a nivel mundial, ha publicado su Índice Global de Amenazas del mes de febrero de 2024. El mes pasado, se descubrió una nueva campaña de FakeUpdates que comprometía sitios web de Wordpress que se infectaron usando cuentas de administrador wp-admin vulneradas y ediciones alteradas de plugins de WordPress, engañando así a los usuarios para que descargaran troyanos de acceso remoto. Por otro lado, Lockbit3 continúa siendo el principal ransomware, responsable del 20% de los ataques publicados, y la educación continúa siendo la industria más afectada a nivel internacional.

FakeUpdates, también conocido como SocGholish, ha estado operativo desde 2017, siendo el malware más prevalente en el Índice de Amenazas. Utiliza malware JavaScript para atacar páginas web, especialmente aquellos con sistemas de gestión de contenido, con el objetivo de que los usuarios descarguen un software malicioso. Esta variante de malware ha estado asociada previamente con el grupo Evil Corp, que se encarga de monetizarlo con la venta del acceso a los sistemas que infecta.

"Las páginas web son el escaparate del mundo digital, esenciales para la comunicación, el comercio y las conexiones", dijo Maya Horowitz, VP de investigación en Check Point Software. "Defenderlas de las ciberamenazas es fundamental para proteger la presencia online y también a las empresas, ya que este tipo de malware ponen en riesgo su dinero y su reputación. Es vital implementar medidas preventivas y adoptar una cultura de tolerancia cero para garantizar una protección absoluta contra las amenazas".

El índice de amenazas de Check Point Research también incluye información de alrededor de 200 sitios web de contenido sospechoso dirigidos por grupos ransomware de doble extorsión, 68 de los cuales publicaron información de sus víctimas este año para presionarles cuando no querían pagar. Lockbit3 continúa siendo el ransomware más significativo, con un 20% de incidentes detectados, seguido por Play con un 8% y 8base con un 7%.

CPR también ha revelado que "Web Servers Malicious URL Directory Traversal" ha sido la vulnerabilidad más explotada, afectando a un 51% de las empresas, seguida de "Command Injection Over HTTP" y "Zyxel ZyWALL Command Injection" con un 50% ambas.

Los tres malware más buscados en España en febrero

*Las flechas indican el cambio en el ranking en comparación con el mes pasado.

España ha experimentado una disminución del 7% de los ataques. 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 11,9% 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 5,2% de empresas españolas.
? Pandora – El ransomware Pandora fue identificado por primera vez a principios de 2023. Pandora se propaga a través de correos electrónicos de phishing, descargas maliciosas o vulnerabilidades en la seguridad de la red. Es conocido por dirigirse tanto a usuarios particulares como a empresas y causa importantes pérdidas de datos y daños económicos. Ha hecho impacto en el 3,1% de las empresas en España.

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

Sanidad
Gobierno/Militar
Finanzas/Banca

Las tres vulnerabilidades más explotadas en febrero
Por otra parte, Check Point Software señala que el mes pasado la vulnerabilidad más explotada fue "Web Servers Malicious URL Directory Traversal" impactando en un 51% de las empresas de todo el mundo, seguida de "Command Injection Over HTTP" y "Zyxel ZyWALL Command Injection" con un impacto global del 50% ambas.

? 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.

? 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 engañar a la víctima.

? Zyxel ZyWALL Command Injection (CVE-2023-28771) – Existe una vulnerabilidad de inyección de comandos en Zyxel ZyWALL. La explotación de esta vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios de forma remota en el sistema operativo del dispositivo afectado.

Los tres malware móviles más usados en febrero

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 febrero

Esta sección se basa en información recibida de más de 200 "shame sites" ejecutadas por grupos ransomware de doble extorsión. Los ciberdelincuentes utilizan estas páginas para presionar a las víctimas a que paguen el rescate de forma inmediata. Estas páginas aportan información importante para comprender el sistema ransomware, siendo este en la actualidad el mayor ciberriesgo para las empresas.

En el último mes, LockBit3 ha sido el ransomware más destacado, responsable del 20% de los ataques realizados, seguido de Play con un 8% y 8base con un 7%.

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 Commonwealth.

Play – Se trata de un malware que encripta datos y pide rescates para poder recuperarlos.

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 febrero 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 Inteligencia Artificial y Robótica Programación Madrid Software Ciberseguridad Dispositivos móviles Otras Industrias Innovación Tecnológica Digital