Publicado en España el 20/09/2023

El FBI arremete contra QBot y ChromeLoader vuelve para propagar extensiones de navegador maliciosas

Qbot se mantiene como el malware más utilizado por los ciberdelincuentes en nuestro país: ha afectado al 7% de las empresas españolas durante el mes de agosto. El sector de las comunicaciones es la segunda industria más afectada por los ciberataques a nivel mundial, alcanzando el tercer puesto en España

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 agosto. Los investigadores de Check Point Research han informado sobre una nueva variante del malware ChromeLoader, que ha estado dirigido a usuarios del navegador Chrome con anuncios falsos con extensiones maliciosas. Por otra parte, el sector de las comunicaciones es la segunda industria más afectada a nivel mundial, desplazando a la sanidad de la lista por primera vez este año.

También durante este mes, el FBI anunció una victoria significativa en su operación global contra el Qbot (también conocido como Qakbot). En la "Operación Duck Hunt", el FBI tomó el control de la botnet, eliminó el malware de los dispositivos infectados e identificó un número sustancial de dispositivos afectados. Qbot se convirtió en un servicio de distribución de malware utilizado para diversas actividades ciberdelincuentes, incluidos ataques de ransomware. Aunque se mantuvo como el malware más prevalente en agosto, Check Point Software ha observado una disminución significativa en su impacto después de la operación.

"La desarticulación de QBot es un avance significativo en la lucha contra el cibercrimen, pero no se puede confiar porque cuando uno cae, otro ocupa su lugar", explica Maya Horowitz, vicepresidenta de investigación de Check Point Software. "Hay que permanecer alerta, trabajar juntos y llevar unas buenas prácticas de seguridad en todos los vectores de ataque".

Los 3 malware más buscados en España en agosto
*Las flechas se refieren al cambio de rango en comparación con el mes anterior.

? Qbot – AKA Qakbot es un troyano bancario que apareció por primera vez en 2008. Fue diseñado para robar las credenciales bancarias y las pulsaciones de teclas. A menudo distribuido a través del correo electrónico no deseado, Qbot emplea varias técnicas anti-VM, anti-depuración y anti-sandbox para dificultar el análisis y evadir la detección. Este troyano ha aumentado su incidencia en las empresas españolas hasta el 7%.
? Fakeupdates – Fakeupdates (AKA SocGholish) es un downloader 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. El downloader impactó en 3,8% de las compañías españolas.

? Nanocore – NanoCore es un troyano de acceso remoto que se dirige a usuarios de sistemas operativos Windows y fue observado por primera vez en estado salvaje en 2013. Todas las versiones de la RAT contienen plugins básicos y funcionalidades como captura de pantalla, minería de criptomonedas, control remoto del escritorio y robo de sesiones de webcam. Este malware ha afectado al 3,7% de las empresas en España.

Las tres industrias más atacadas a nivel mundial
El mes pasado, la educación/investigación continuó siendo la industria más atacada a nivel mundial, seguida por comunicaciones y gobierno/militar.

Educación/investigación
Comunicaciones
Gobierno/militar

A nivel local, las industrias más atacadas en España fueron el sector sanidad, seguido de finanzas/banca y comunicaciones.

Las tres vulnerabilidades más explotadas en agosto
Por otra parte, Check Point Research señala la "Ejecución Remota de Código a través de Encabezados HTTP" fue la vulnerabilidad más explotada y afectó al 40% de las empresas en todo el mundo, seguida de la "Inyección de Comandos a través de HTTP", con un 38%. La tercera vulnerabilidad más utilizada fue la "Ejecución Remota de Código en MVPower CCTV DVR", con un impacto global del 35%.

? Ejecución Remota de Código a través de Encabezados HTTP – Los encabezados HTTP permiten que el cliente y el servidor transmitan información adicional con una solicitud HTTP. Un atacante remoto puede usar un encabezado HTTP vulnerable para ejecutar código arbitrario en el equipo de la víctima.
? Inyección de Comandos a través de HTTP (CVE-2021-44228) – 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. La explotación exitosa permite a un atacante ejecutar código arbitrario en el dispositivo objetivo.
? Ejecución Remota de Código en MVPower CCTV DVR (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756) – Existe una vulnerabilidad de ejecución remota de código en MVPower CCTV DVR. La explotación exitosa de esta vulnerabilidad permite ejecutar código arbitrario en el sistema atacado.

Los tres malwares móviles más usados en agosto

Anubis – Malware troyano bancario diseñado para teléfonos móviles Android. Desde que se detectó

inicialmente ha ganado funciones adicionales que incluyen 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.

SpinOk – Es un módulo de software para Android que funciona como spyware. Recopila información sobre los archivos almacenados en los dispositivos y es capaz de transferirla a los ciberdelincuentes. El módulo malicioso se ha encontrado presente en más de 100 aplicaciones Android y se ha descargado más de 421.000.000 veces a fecha de mayo de 2023.

El Índice Global de Impacto de Amenazas de Check Point Software y su mapa ThreatCloud están impulsados por la inteligencia ThreatCloud de Check Point Software. ThreatCloud proporciona inteligencia de amenazas en tiempo real derivada de cientos de millones de sensores en todo el mundo, sobre redes, endpoints y móviles. La inteligencia se enriquece con motores basados en IA y datos de investigación exclusivos de Check Point Research, la rama de inteligencia e investigación de Check Point Software Technologies.

Datos de contacto:
Eduardo Malo Roldán
Check Point Software
91 551 98 91

Nota de prensa publicada en: España

Categorías: Internacional Nacional Programación Software Ciberseguridad Dispositivos móviles