Publicado en España el 17/08/2023

El malware no se va de vacaciones: el troyano bancario Anubis para móviles recupera la primera posición, mientras que Remcos recupera puestos, según Check Point Software

Qbot es el malware más utilizado por los ciberdelincuentes en España, afectando al 7,54% de las empresas durante el mes de julio. Remcos vuelve a los primeros puestos y es uno de los troyanos con más incidencia en las empresas de todo el mundo

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 julio. Los investigadores de Check Point Research han descubierto que los ciberdelincuentes creaban sitios web falsos para difundir una descarga maliciosa que contenía el malware Remcos. Además, el troyano bancario para móviles Anubis desbancó al relativamente recién llegado SpinOk para volver a ocupar el primer puesto de la lista de malware para móviles.

Remcos es un Troyano de Acceso Remoto (RAT) que apareció por primera vez en 2016 y se distribuye a través de documentos o descargas maliciosas de Microsoft. Recientemente se ha observado en una campaña relacionada con el malware Fruity. El objetivo era atraer a las víctimas para que lo descargaran, a través del cual se instalaran diferentes RAT como Remcos, conocido por su capacidad para obtener acceso remoto al sistema de la víctima, robar información confidencial y credenciales y llevar a cabo actividades maliciosas en el ordenador del usuario.

"Esta época del año es perfecta para los ciberdelincuentes. Mientras que muchos aprovechan la temporada de vacaciones, las empresas tienen menos personal y eso puede reducir su capacidad para monitorizar las amenazas y minimizar el riesgo", comparte Maya Horowitz, vicepresidenta de investigación de Check Point Software. "Introducir procesos de seguridad automatizados y consolidados puede ayudar a las compañías a mantener buenas prácticas durante los periodos vacacionales".

Los 3 malware más buscados en España en julio:
*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 de un usuario. A menudo distribuido a través de 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 7,54%.
? FormBook – FormBook es un infostealer dirigido al sistema operativo Windows y fue detectado por primera vez en 2016. Se comercializa en foros clandestinos de ciberdelincuencia como Malware as a

Service (MaaS) por sus potentes técnicas de evasión y su precio relativamente bajo. FormBook recopila credenciales de varios navegadores web, realiza capturas de pantalla, monitoriza y registra las pulsaciones de teclado, y puede descargar y ejecutar archivos según las órdenes de su C&C. El infostealer impactó en 3,59% de las compañías españolas.

? Emotet – Troyano avanzado, autopropagable y modular. Emotet funcionaba como un troyano bancario, pero ha evolucionado para distribuir otros programas o campañas maliciosas. Además, destaca por utilizar múltiples métodos y técnicas de evasión para evitar su detección. Puede difundirse a través de campañas de spam en archivos adjuntos o enlace maliciosos en correos electrónicos. Este malware ha afectado al 2,51% 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 gobierno/militar y sanidad.

Educación/investigación
Gobierno/militar
Sanidad

A nivel local, las industrias más atacadas en España fueron el sector Público, seguido de transportes y minorista/mayorista.

Las tres vulnerabilidades más explotadas en julio

Por otra parte, Check Point Research señala que "Web Servers Malicious URL Directory Traversal" fue la vulnerabilidad más explotada, afectando al 49% de las organizaciones a nivel mundial, seguida de "Apache Log4j Remote Code Execution" con un 45% y "HTTP Headers Remote Code Execution" con un impacto global del 42%.

? Web Servers Malicious URL Directory Traversal – Existe una vulnerabilidad de cruce de directorios en diferentes servidores web. La vulnerabilidad se debe a un error de validación de entrada en un servidor web que no sanea correctamente el URI. La explotación exitosa permite acceder a archivos arbitrarios en el servidor vulnerable.

? Ejecución remota de código Apache Log4j (CVE-2021-44228) – Se ha detectado una vulnerabilidad de ejecución remota de código en Apache Log4j que permite que un atacante remoto ejecute código arbitrario en el sistema afectado.

? Ejecución remota de código de encabezados HTTP (CVE-2020-10826,CVE-2020-10827,CVE-2020-10828,CVE-2020-13756) – Los encabezados HTTP permiten al cliente y al servidor pasar información adicional con una solicitud HTTP. Un atacante remoto puede usar un encabezado HTTP vulnerable para ejecutar código arbitrario en el equipo víctima.

Los tres malwares móviles más usados en julio

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.

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 mayo de 2023.

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.

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
91 551 98 91

Nota de prensa publicada en: España

Categorías: Internacional Nacional Programación Hardware Madrid Entretenimiento Software Ciberseguridad Dispositivos móviles Innovación Tecnológica