Publicado en España el 13/06/2023

Mayo "descarga" una nueva versión de Guloader: Check Point Software detecta una entrega de cargas cifradas basadas en la nube

Guloader vuelve al cuarto puesto con una nueva versión de su downloader, con cargas totalmente cifradas y técnicas anti-análisis que le permiten almacenarse sin ser detectado en los servicios de cloud pública

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 mayo. Los investigadores informan sobre una nueva versión de GuLoader, un downloader con base shellcode que se ha convertido en el cuarto malware más prevalente. Con cargas totalmente cifradas y técnicas anti-análisis, la última versión se almacena sin detección en servicios de cloud pública, incluido Google Drive. Mientras tanto, Qbot y Anubis ocupan el primer puesto mientras que Educación/Investigación repitió como el sector más vulnerado.

Los ciberdelincuentes utilizan con mucha frecuencia el malware GuLoader para eludir los antivirus. La última iteración emplea una sofisticada técnica de sustitución de código en un proceso legítimo, lo que facilita su evasión. Las cargas están totalmente cifradas y se almacenan sin que los servicios de cloud pública lo puedan detectar. Esta combinación única de cifrado, formato binario sin procesar, y separación del loader, hace que las cargas sean invisibles para los programas antivirus, lo que supone una importante amenaza para usuarios y empresas de todo el mundo.

Por otra parte, tanto Qbot como Anubis ocuparon los primeros puestos de sus respectivas listas. A pesar de los esfuerzos por ralentizar la distribución de malware bloqueando las macros de los archivos de Office, los operadores de Qbot no han tardado en adaptar su distribución y entrega. Recientemente se le ha visto explotar un fallo de secuestro de la biblioteca de vínculos dinámicos (DLL) en el programa WordPad de Windows 10 para infectar ordenadores.

"Los ciberdelincuentes aprovechan cada vez más las herramientas y servicios públicos para distribuir y almacenar malware. La fiabilidad de una fuente ya no garantiza una seguridad completa", afirma Maya Horowitz, vicepresidenta de Investigación de Check Point Software. "La formación es una necesidad urgente para identificar actividades sospechosas. Es muy importante no revelar información personal ni descargar archivos adjuntos a menos que se haya confirmado la autenticidad y la naturaleza benigna de la solicitud. Además, es crucial contar con soluciones de seguridad avanzadas como Check Point Horizon XDR/XPR que pueden identificar eficazmente si un comportamiento supuestamente legítimo es en realidad malicioso, proporcionando una capa adicional de protección contra amenazas sofisticadas".

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

? GuLoader – un downloader muy utilizado desde diciembre de 2019. Cuando apareció por primera vez, GuLoader se utilizaba para descargar Parallax RAT, pero se ha aplicado a otros troyanos de acceso remoto y ladrones de información como Netwire, FormBook y Agent Tesla.

? Qbot – 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.

? XMRig - XMRig es un software de minería de CPU de código abierto utilizado para minar la criptomoneda Monero. Los actores de amenazas a menudo abusan de este software de código abierto integrándolo en su malware para realizar minería ilegal en los dispositivos de las víctimas.

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
Sanidad Gobierno/militar
Sanidad

Las tres vulnerabilidades más explotadas en mayo

Por otra parte, Check Point Research señala que "Web Servers Malicious URL Directory Traversal" es la vulnerabilidad más explotada que afectó al 49% de las empresas a nivel mundial, seguida de "Apache Log4j Remote Code Execution" (45%) y "HTTP Headers Remote Code Execution" con un impacto del 44%.

? 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 mayo

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.

Hiddad - malware de Android que re empaqueta aplicaciones legítimas y luego las libera en una tienda de terceros. Su función principal es mostrar anuncios, pero también puede obtener acceso a detalles de seguridad integrados en el sistema operativo.

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: Nacional Software Ciberseguridad