Publicado en Madrid el 16/10/2023

Top malware septiembre: Remcos siembra el caos en Colombia y Formbook ocupa el primer lugar tras la desactivación de Qbot

Formbook se convierte en el malware predominante tras el colapso de Qbot en agosto. Check Point Research identifica una nueva campaña de phishing a gran escala dirigida a más de 40 empresas en Colombia

Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, ha publicado su Índice Global de Amenazas del mes de septiembre 2023. Los investigadores han encontrado una nueva y sigilosa campaña de phishing dirigida a empresas colombianas y diseñada para distribuir de manera discreta al Troyano de Acceso Remoto (TAR) Remcos. Mientras tanto, Formbook se ha convertido en el malware más utilizado tras el colapso de Qbot, y la educación continua siendo el sector más atacado.

En septiembre, Check Point Research ha descubierto una importante campaña de phishing que se dirigía a más de 40 compañías de múltiples industrias en Colombia. El objetivo era instalar con sigilo el TAR Remcos en los ordenadores de las víctimas. Remcos, que era el segundo malware dominante este mes, es un sofisticado TAR tipo "navaja suiza" que otorga control total sobre el ordenador infectado y puede emplearse en gran variedad de ataques. Algunas consecuencias habituales de Remcos son el robo de datos, las infecciones posteriores y la toma de control de cuentas.

El mes pasado vimos también cómo Qbot desaparecía de la lista de malware principales después de que el FBI tomara control de la botnet en agosto. Esto marcó el final de una larga carrera del malware más importante, que había encabezado la lista durante la mayor parte de 2023.

"La campaña que descubrimos en Colombia muestra la complejidad de las técnicas de evasión que emplean los atacantes. Es también una buena ilustración sobre lo invasivas que son estas técnicas y por qué necesitamos emplear resiliencia cibernética para protegernos contra la gran variedad de tipos de ataques", explica Maya Horowitz, VP de Investigación de Check Point Software.

CPR también ha revelado que "Web Servers Malicious URL Directory Traversal" ha sido la vulnerabilidad más explotada en septiembre y que ha afectado al 47% de las empresas a nivel global, seguido de "Inyección de comandos a través de HTTP" con el 42% e "Inyección de comandos por Zyxel zyWALL" con el 39%.

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

?Formbook - Formbook es un 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 aumentado su incidencia en las empresas españolas hasta el 3,1%.

?Remcos – Remcos es un RAT que apareció primero en estado salvaje en 2016. Este malware se distribuye a través de documentos de Microsoft Office maliciosos que están adjuntos en emails de SPAM, y está diseñado para eludir la seguridad del UAC (Control de Cuentas de Usuario) de Microsoft y ejecutar malware con altos privilegios. Este RAT ha impactado en el 2,9% de las empresas en España.

?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. El troyano ha alcanzado al 2,4% de las compañías españolas.

Las tres industrias más atacadas a nivel mundial en septiembre

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

Las tres vulnerabilidades más explotadas en septiembre

Por otra parte, Check Point Software señala que el mes pasado la vulnerabilidad más utilizada fue la de "Web Servers Malicious URL Directory Traversal", impactando en un 47% de las empresas en todo el mundo, seguido de "Inyección de comandos a través de HTTP" con un 42 % e "Inyección del comando Zyxel ZyWALL" con un 39%.

? Web Servers Malicious URL Directory Traversal – Esta vulnerabilidad se debe a un error de validación de la entrada en servidores web que no ha desinfectado adecuadamente la URL para los patrones de cruce de directorios. Una explotación exitosa permite a los atacantes remotos sin autentificar revelar o acceder a cualquier archivo del servidor atacado.

? 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 al atacante ejecutar un código arbitrario en el dispositivo objetivo.

? Inyección del comando Zyxel ZyWALL (CVE-2023-28771) – La explotación exitosa de esta vulnerabilidad permitiría a los atacantes remotos ejecutar comandos arbitrarios del sistema operativo en el dispositivo afectado.

Los tres malware móviles más usados en septiembre

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, lo que se suele usar para robar información sensible.

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 encontró presente en más de 100 aplicaciones Android y llegó a descargar 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.

La lista completa de los diez malware más buscados en septiembre se puede encontrar en el blog de Check Point Software.

Datos de contacto:
Everythink PR
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Telecomunicaciones Programación Software Ciberseguridad