Publicado en Madrid el 15/12/2023

# El malware más buscado de noviembre: una nueva campaña de AsyncRAT, y FakeUpdates vuelve al Top Ten tras un breve paréntesis

**Los investigadores han informado de una nueva campaña de AsyncRAT en la que se utilizan archivos HTML maliciosos para propagar el sigiloso malware. Por su parte, el programa de descargas FakeUpdates ha saltado directamente al segundo puesto tras una breve pausa en la lista de los diez primeros**

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 noviembre. El mes pasado, los investigadores descubrieron una nueva campaña de AsyncRAT en la que se utilizaban archivos HTML maliciosos para propagar el malware encubierto. Por su parte, FakeUpdates, un descargador de JavaScript, ha saltado directamente al segundo puesto tras un paréntesis de dos meses en la lista de los diez primeros, y una vez más el sector de la educación sigue siendo el más afectado en todo el mundo.

AsyncRAT es un troyano de acceso remoto (RAT) conocido por su capacidad para vigilar y controlar remotamente sistemas informáticos sin ser detectado. El malware, que ocupó el sexto lugar en la lista de los diez mejores del mes pasado, con una campaña en la que los destinatarios recibían un correo con un enlace incrustado que descargaba un archivo HTML malicioso, que permitía al malware camuflarse como una aplicación de confianza.

Mientras tanto, el programa de descarga FakeUpdates ha vuelto a entrar en la lista de los principales programas maliciosos tras una pausa de dos meses. Escrito en JavaScript, este marco de distribución de malware utiliza páginas web comprometidas para engañar a los usuarios y hacerles ejecutar falsas actualizaciones del navegador. Ha dado lugar a otros muchos programas maliciosos, como GootLoader, Dridex, NetSupport, DoppelPaymer y AZORult.

"Las ciberamenazas de noviembre demuestran cómo los ciberdelincuentes aprovechan métodos aparentemente inocuos para infiltrarse en las redes. El auge de la campaña AsyncRAT y el resurgir de FakeUpdates ponen de manifiesto una tendencia en la que los atacantes utilizan una simplicidad engañosa para eludir las defensas tradicionales. Es necesario que las empresas adopten un enfoque de seguridad en múltiples capas que no solo se base en el reconocimiento de las amenazas conocidas, sino que también tenga la capacidad de identificar, prevenir y responder a los nuevos vectores de ataque antes de que inflijan daño", dijo Maya Horowitz, VP de Investigación de Check Point Software.

CPR también ha revelado que "Inyección de comandos a través de HTTP" ha sido la vulnerabilidad más explotada en noviembre y que ha afectado al 45% de las empresas a nivel global, seguido de "Web Servers Malicious URL Directory Traversal" con el 42% e "Inyección de comandos por Zyxel zyWALL" con otro el 41%.

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

? Formbook - 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 2,6%.

? 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 1,9% de las empresas en España.

? 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 1,8% de las empresas en España.

Las tres industrias más atacadas a Europa en noviembre:
El mes pasado, la de Comunicaciones continuó siendo la industria más atacada a nivel mundial, seguida por Finanzas/banca y Sanidad.

Gobierno/militar.
Sanidad.
Educación/investigación.

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

? Inyección de comandos a través de HTTP – Un atacante remoto puede enviando una solicitud especialmente diseñada a la víctima y, si tiene éxito, le permite ejecutar un código arbitrario en el dispositivo objetivo.

? 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. Una explotación exitosa permite a los atacantes remotos sin autentificar, revelar o acceder a cualquier archivo del servidor atacado.

? Inyección del comando Zyxel ZyWALL (CVE-2023-28771) – La explotación de esta vulnerabilidad permite a los atacantes ejecutar comandos arbitrarios de forma remota en el sistema operativo en el

dispositivo afectado.

Los tres malware móviles más usados en octubre

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.
SpinOk – Módulo de software para Android que funciona como spyware. Recopila información sobre los archivos almacenados en los dispositivos y puede transferirla a ciberdelincuentes. El módulo malicioso se ha encontrado presente en más de 100 aplicaciones Android y se descargó más de 421.000.000 veces hasta 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:**
Everythink PR
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

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