Publicado en Madrid el 13/06/2022

Snake Keylogger vuelve al Top Ten tras una larga ausencia que se ha propagado a través de archivos PDF

Check Point Research informa que mientras Emotet sigue siendo el malware número uno, Snake Keylogger vuelve al índice en el octavo lugar tras meses fuera del ranking

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 mayo de 2022. Los investigadores informan de que Emotet, un troyano avanzado, autopropagable y modular, sigue siendo el más prevalente como resultado de múltiples campañas generalizadas. Sin embargo, este mes, Snake Keylogger ha saltado al octavo puesto tras una larga ausencia en el índice. La principal funcionalidad de Snake es registrar las pulsaciones de los usuarios y transmitir los datos recogidos a los ciberdelincuentes.

Snake Keylogger suele propagarse a través de emails que incluyen archivos adjuntos docx o xlsx con macros maliciosas, sin embargo, este mes los investigadores informaron que SnakeKey Logger también se ha propagado a través de archivos PDF. Esto podría deberse en parte a que Microsoft bloquea por defecto las macros de Internet en Office, lo que significa que los ciberdelincuentes han tenido que ser más creativos, explorando nuevos tipos de documentos. Esta rara forma de propagar el malware está resultando bastante eficaz, ya que algunas personas perciben los PDF como intrínsecamente más seguros que otros archivos.

Emotet, está afectando al 8% de las organizaciones de todo el mundo, un ligero aumento con respecto al mes pasado. Este malware es tan ágil que resulta rentable gracias a su capacidad para pasar desapercibido. Su persistencia también hace que sea difícil de eliminar una vez que un dispositivo ha sido infectado, lo que lo convierte en la herramienta perfecta en el arsenal de un ciberdelincuente. Originalmente un troyano bancario, suele distribuirse a través de correos electrónicos de phishing y tiene la capacidad de incorporar otros malwares, lo que aumenta su habilidad para causar daños generalizados.

“Como se ha puesto de manifiesto con las recientes campañas de Snake Keylogger, todo lo que se hace online supone un riesgo de ciberataque, y abrir un documento PDF no es una excepción”, afirma Eusebio Nieva, director técnico de Check Point Software para España y Portugal. “Los virus y el código ejecutable malicioso pueden estar al acecho en el contenido multimedia y en los enlaces, con un ataque de malware, en este caso Snake Keylogger, listo para atacar una vez que el usuario lo abre. Por lo tanto, al igual que se cuestiona la legitimidad de un archivo adjunto de un email docx o xlsx, se debe tener la misma precaución con los PDF. En el panorama actual, nunca ha sido tan importante para las empresas contar con una sólida solución de seguridad para el correo electrónico que ponga en cuarentena e inspeccione los archivos adjuntos, impidiendo que cualquier documento malicioso entre en la red desde el principio”, concluye Nieva.

“Servidores web URL maliciosos Directory Traversal” ha sido la vulnerabilidad más explotada y común - ha afectado al 46% de las empresas de todo el mundo-, seguida muy de cerca por “Apache Log4j Remote Code Execution” que ha impactado en el 46% de las compañías a nivel mundial. “La revelación de información del servidor web Git" se sitúa en el tercer lugar del índice llegando a un 45% de las organizaciones. En abril el sector de la Educación/Investigación continúa siendo el más atacado a nivel mundial.

Los 3 malware más buscados en España en mayo:

*Las flechas muestran el cambio de posición en el ranking en comparación con el mes anterior.

? 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 a un 8,01% de las empresas en España.
? Formbook – Detectado por primera vez en 2016, FormBook es un Stealer que apunta al sistema operativo Windows. Se comercializa como MaaS en los foros de hacking underground por sus fuertes técnicas de evasión y su precio relativamente bajo. FormBook roba credenciales de varios navegadores web, recoge capturas de pantalla, monitoriza y registra las secuencias de teclas, pudiendo descargar y ejecutar archivos según las órdenes de su C&C. Este Stealer ha atacado al 3,12% de las empresas en nuestro país.
? XMRig – Cryptojacker utilizado para minar ilegalmente la criptomoneda Monero. Este malware fue descubierto por primera vez en mayo de 2017. Ha impactado en un 1,90% de las organizaciones en España.

Los sectores más atacados a nivel mundial:

Este mes, la Educación/Investigación es la industria más atacada a nivel mundial, seguida de las Gobierno/Militar y ISP/MSP.

Educación/Investigación
Gobierno/Militar
ISP/MSP

Top 3 vulnerabilidades más explotadas en mayo:

? Web Servers Malicious URL Directory Traversal (CVE-2010-4598, CVE-2011-2474, CVE-2014-0130, CVE-2014-0780, CVE-2015-0666, CVE-2015-4068, CVE-2015-7254,

CVE-2016-4523, CVE-2016-8530, CVE-2017-11512, CVE-2018-3948, CVE-2018-3949, CVE-2019-18952, CVE-2020-5410, CVE-2020-8260) - 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 adecuadamente el URI para los patrones de recorrido de directorios. Una explotación exitosa le permite a los atacantes remotos no autentificados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

? Ejecución remota de código en Apache Log4j (CVE-2021- 44228) – Existe una vulnerabilidad de ejecución remota de código en Apache Log4j que, si se explota de forma favorable, podría admitir un atacante remoto ejecutar código arbitrario en el sistema afectado.

? Filtración de información del repositorio Git–La vulnerabilidad en la exposición de información en el repositorio Git está reportada. La explotación exitosa de esta vulnerabilidad podría permitir la divulgación involuntaria de información de la cuenta.

Top 3 del malware móvil mundial en mayo:

AlienBot – Esta familia es un Malware-as-a-Service (MaaS) para dispositivos Android que permite a un atacante remoto, como primer paso, inyectar código malicioso en aplicaciones financieras legítimas. El ciberdelincuente obtiene acceso a las cuentas de las víctimas, y finalmente controla completamente su dispositivo.

FluBot – FluBot es un malware botnet para Android que se distribuye a través de SMS de phishing, la mayoría de las veces haciéndose pasar por marcas de reparto de logística. Una vez que el usuario hace clic en el enlace dentro del mensaje, FluBot se instala y obtiene acceso a toda la información sensible del teléfono.

xHelper – Aplicación Android maliciosa que fue descubierta por primera vez en marzo de 2019. Se utiliza para descargar otras aplicaciones maliciosas y mostrar anuncios. Es capaz de esquivar los antivirus móviles, así como reinstalarse por sí misma en caso de que el usuario la elimine.

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 las 10 familias principales de malware en mayo está disponible en el blog de Check Point Software.

Datos de contacto:
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid