Publicado en Madrid el 19/01/2023

Qbot desplaza a Emotet y se coloca en el primer puesto del malware más presente en diciembre

Check Point Research informa que Glupteba ha regresado a la lista de los diez primeros por primera vez desde julio de 2022. Qbot superó a Emotet como el malware más frecuente en diciembre, mientras que el malware para Android Hiddad regresa

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 de diciembre de 2022. Glupteba Malware, una ambiciosa botnet troyana habilitada para blockchain, vuelve al octavo puesto de la lista top 10, después de estar fuera de esta clasificación desde julio de 2022. Qbot, un sofisticado troyano que roba credenciales bancarias y pulsaciones de teclas, superó a Emotet como el malware más frecuente, y ha afectado a un7% de las organizaciones en todo el mundo. Mientras tanto, el malware para Android Hiddad hizo una reaparición.

Aunque Google ha logrado causar una interrupción importante en las operaciones de Glupteba en diciembre de 2021, ha vuelto a la acción. Como una variante de malware modular, Glupteba puede lograr varios objetivos en un ordenador infectado. La botnet se utiliza a menudo como descargador y gotero para otro malware. Esto significa que su infección podría provocar un ataque de ransomware, violación de datos u otros incidentes de seguridad. Glupteba también está diseñado para robar credenciales de usuario y cookies de sesión de dispositivos infectados. Estos datos de autenticación se pueden usar para obtener acceso a las cuentas online de un usuario u otros sistemas, lo que permite al atacante robar datos confidenciales o realizar otras acciones utilizando estas cuentas comprometidas. El malware se usa con frecuencia para implementar funciones de criptominería que drenan los recursos del ordenador al extraer bloques.

En diciembre, Hiddad también llegó a la lista de los tres principales malware móvil por primera vez en 2022. Este malware de distribución de anuncios está dirigido a dispositivos Android. Bloquea aplicaciones legítimas y luego las libera en una tienda de terceros. Su función principal es mostrar anuncios, pero también puede obtener acceso a detalles clave de seguridad integrados en el sistema operativo.

"La última investigación muestra cómo el malware a menudo se disfraza de software legítimo que permite a los ciberdelincuentes acceder por la puerta trasera a los dispositivos sin levantar sospechas. Por ello es importante extremar precauciones al descargar cualquier software y aplicaciones o hacer clic en enlaces, independientemente de cuán genuinos se vean", afirma Eusebio Nieva, director técnico de Check Point Software para España y Portugal.

Los 3 malware más buscados en España en diciembre:
*Las flechas muestran el cambio de posición en el ranking en comparación con el mes anterior.

? Qbot – Qbot AKA Qakbot es un troyano bancario que apareció por primera vez en 2008. A menudo distribuido a través de correo electrónico de spam, Qbot emplea varias técnicas anti-VM, anti-depuración y anti-sandbox para dificultar el análisis y evadir la detección. Ha sido responsable del 7,5% de ataques en España.

? 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 bajado su incidencia hasta el 4,1%.

? 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 2,8% de las empresas españolas.

Los sectores más atacados a nivel mundial:
Este mes el sector Educación/Investigación continuó en primer lugar como la industria más atacada a nivel mundial, seguido del Gobierno/Militar y la Sanidad.

Educación/Investigación
Gobierno/Militar
Sanidad

Top 3 vulnerabilidades más explotadas en diciembre:

? Web Server Exposed Git Repository Information Disclosure - Es una vulnerabilidad de divulgación de información en Git Repository. Si se aprovecha correctamente, esta vulnerabilidad permite divulgar de forma involuntaria de la información de la cuenta.

? Cruce de directorios de URL malintencionadas de servidores web (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 correctamente el URI para los patrones de recorrido de directorios. Permite a los atacantes remotos no autenticados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

? Command Injection Over HTTP (CVE-2021-43936,CVE-2022-24086) - Un atacante remoto puede aprovechar este problema enviando una solicitud especialmente diseñada a la víctima. La explotación exitosa facilita al atacante ejecutar código arbitrario en el equipo de destino.

Top 3 del malware móvil mundial en octubre:

Anubis – Anubis es un malware troyano bancario diseñado para teléfonos móviles Android. Desde que se detectó inicialmente, ha sumado funcionalidad de troyano de acceso remoto (RAT), keylogger y capacidades de grabación de audio, así como varias características de ransomware adicionales. Se ha detectado en cientos de aplicaciones diferentes disponibles en Google Store.

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

AlienBot – AlienBot es un troyano bancario para Android, vendido clandestinamente como Malware-as-a-Service (MaaS). Admite registro de teclas, superposiciones dinámicas para el robo de credenciales y recolección de SMS para la omisión de 2FA. Ofrece capacidades adicionales de control remoto conun módulo de TeamViewer.

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 diciembre está disponible en el blog de Check Point Software.

Datos de contacto:
Everythink PR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Software Ciberseguridad Dispositivos móviles