Publicado en España el 13/07/2023

Qbot es el malware más prevalente en 2023 y el troyano para móviles SpinOk hace su debut en más de 100 aplicaciones Android con 421 millones de descargas

Check Point Research ha informado de que el troyano multipropósito Qbot ha sido el malware más prevalente durante la primera mitad de 2023, afectando al 8,5% de las empresas españolas durante el mes de junio. Emotet vuelve a los primeros puestos y es uno de los troyanos con más incidencia en las empresas españolas

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 junio. Los investigadores de Check Point Research han descubierto que el troyano Qbot es el malware más prevalente en lo que va de 2023, ocupando el primer puesto en cinco de los seis meses transcurridos hasta la fecha. Por su parte, el troyano para móviles SpinOk se ha situado por primera vez en lo más alto de la lista después de detectarse el mes pasado, y el ransomware ha saltado a los titulares a raíz de una vulnerabilidad de 'zero-day' en el software de intercambio de archivos MOVEIt.

Qbot, que surgió inicialmente en 2008 como troyano bancario, ha experimentado un desarrollo constante, y ha sumado funcionalidades adicionales para robar contraseñas, correos electrónicos y datos de tarjetas de crédito. Se propaga habitualmente a través de spam y emplea diversas técnicas: métodos anti-VM, anti-depuración y anti-sandbox, para impedir el análisis y evitar su detección. En la actualidad, su función principal es actuar como cargador de otro malware y consolidar su presencia en las empresas objetivo donde hace de trampolín para los operadores de grupos de ransomware.

Los investigadores han detectado un prolífico malware para móviles que ha acumulado hasta la fecha 421 millones de descargas. El mes pasado, por primera vez, el kit de desarrollo de software (SDK) troyanizado SpinOk se abrió camino hasta la cima de las familias de malware para móviles. Se utiliza en numerosas aplicaciones populares para marketing y se ha infiltrado en aplicaciones y juegos muy populares, algunos de los cuales estaban disponibles en Google Play Store. Capaz de robar información sensible de los dispositivos y de vigilar las actividades del portapapeles, SpinOk supone una grave amenaza para la privacidad y la seguridad de los usuarios.

El mes pasado también se produjo el lanzamiento de una campaña de ransomware a gran escala que afectó a empresas de todo el mundo. En mayo de 2023, Progress Software Corporation reveló una vulnerabilidad en MOVEit Transfer y MOVEit Cloud (CVE-2023-34362) que daba acceso no autorizado al entorno. A pesar de que se parcheó en 48 horas, los ciberdelincuentes asociados con el grupo de ransomware Clop, afiliado a Rusia, explotaron la vulnerabilidad y lanzaron un ataque a la cadena de suministro contra los usuarios de MOVEit. Hasta la fecha, 108 empresas -entre ellas siete universidades estadounidenses- están incluidas en la lista pública tras el incidente, con cientos y miles de registros obtenidos.

"El exploit MOVEit demuestra que 2023 ya se está convirtiendo en un año trascendental para el ransomware. Grupos como Clop no están operando tácticamente para infectar a un único objetivo, sino que hacen sus operaciones más eficientes aprovechándose de los softwares que se utilizan habitualmente en entornos corporativos. Este enfoque supone alcanzar a cientos de víctimas en un solo ataque", explica Maya Horowitz, VP de Investigación de Check Point Software. "Este patrón de ataque enfatiza la importancia de que las empresas implementen una estrategia de ciberseguridad de múltiples capas y prioricen la aplicación de parches rápidamente cuando se revelan vulnerabilidades".

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

? 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. Este troyano ha aumentado su incidencia en las empresas españolas hasta el 8,5%.
? 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 impactado en el 3,2% de las empresas en España.
? 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 2,6% de las compañías españolas.

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
Gobierno/militar
Sanidad

Las tres vulnerabilidades más explotadas en junio
Por otra parte, Check Point Research señala que "Web Servers Malicious URL Directory Traversal" es la vulnerabilidad más explotada que afectó al 51% de las empresas a nivel mundial, seguida de

"Apache Log4j Remote Code Execution" (46%) 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

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 ha encontrado presente en más de 100 aplicaciones Android y se ha descargado más de 421.000.000 veces hasta el 23 de 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.

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: Internacional Nacional Programación Ciberseguridad Dispositivos móviles