Publicado en Madrid el 19/08/2024

El malware más buscado de julio de 2024: RansomHub lidera el RaaS, mientras que LockBit3 vuelve al ataque

El Índice Global de Amenazas de Check Point Software pone de relieve un cambio en el panorama del ransomware como servicio (RaaS). Los investigadores identificaron una campaña que distribuía el malware Remcos a raíz de un problema de actualización de CrowdStrike

Check Point® Software Technologies Ltd. (NASDAQ: CHKP), proveedor líder en soluciones de ciberseguridad en la nube basadas en IA, publica su Índice Global de Amenazas del mes de julio de 2024. A pesar de una caída significativa en junio, LockBit ha resurgido el mes pasado para convertirse en el segundo grupo de ransomware más prevalente, mientras que RansomHub ha conservado el primer puesto. Mientras tanto, los investigadores han identificado tanto una campaña que distribuía el malware Remcos a raíz de un problema de actualización de CrowdStrike, como una serie de nuevas tácticas de FakeUpdates, que han vuelto a ocupar el primer puesto este mes.

Un problema en el sensor CrowdStrike Falcon para Windows ha llevado a los ciberdelincuentes a distribuir un archivo ZIP malicioso llamado crowdstrike-hotfix.zip. Este archivo contenía HijackLoader, que posteriormente activaba el malware Remcos, clasificado como el séptimo malware más buscado en julio. La campaña se dirigía a empresas que utilizaban instrucciones en español e implicaba la creación de dominios falsos para ataques de phishing.

Mientras tanto, los investigadores han descubierto una serie de tácticas nuevas que empleaban FakeUpdates. Los usuarios que visitaban sitios web comprometidos se encontraban con falsos avisos de actualización del navegador, que conducían a la instalación de troyanos de acceso remoto (RAT) como AsyncRAT, que actualmente ocupa el noveno lugar en el índice de Check Point Software. Resulta alarmante que los ciberdelincuentes hayan empezado a explotar BOINC, una plataforma destinada a la informática voluntaria, para obtener el control remoto de los sistemas infectados.

"La continua persistencia y resurgimiento de grupos de ransomware como Lockbit y RansomHub subraya que los ciberdelincuentes siguen centrándose en el ransomware, un importante desafío para las empresas con implicaciones de gran alcance para su continuidad operativa y la seguridad de los datos. La reciente explotación de una actualización de software de seguridad para distribuir el malware Remcos pone aún más de relieve la naturaleza oportunista de los ciberdelincuentes, lo que compromete aún más las defensas de las empresas. Para contrarrestar estas amenazas, las compañías tendrán que adoptar una estrategia de seguridad multicapa que incluya una sólida protección de los endpoints, una monitorización continua y la educación de los usuarios para reducir el impacto de estos ciberataques cada vez más masivos", afirma Maya Horowitz, VP de Investigación de Check Point Software.

Principales familias de malware en España

*Las flechas se refieren al cambio de rango en comparación con el mes anterior.

FakeUpdates fue el malware más prevalente este mes, con un impacto del 9.45% en organizaciones de todo el mundo, seguido de Androxgh0st, con un impacto global del 5.87%, y Qbot, con un impacto global del 4.26%.

? FakeUpdates. Downloader hecho 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 9.45% de las empresas en España.
? Androxgh0st - Androxgh0st es un botnet que afecta a plataformas Windows, Mac y Linux. Para la infección inicial, Androxgh0st explota múltiples vulnerabilidades, específicamente dirigidas al PHPUnit, el Marco de Trabajo de Laravel y el Servidor Web Apache. El malware roba información sensible como cuentas de Twilio, credenciales SMTP, llave AWS, etc. Utiliza archivos de Laravel para recolectar la información requerida. Tiene diferentes variantes que escanean para diferente información. Este botnet ha impactado al 5.87% de las empresas en España.
? Qbot – Qbot es un malware multifunción que apareció por primera vez en 2008. Fue diseñado para robar las credenciales de los usuarios, registrar pulsaciones de teclas, sustraer las cookies de los navegadores, espiar actividades bancarias e implementar malware adicional. A menudo se distribuye a través de correos electrónicos no deseados, y emplea diversas técnicas anti-VM, anti-debuggin y anti-sandbox para obstaculizar el análisis y eludir la detección. Desde 2022, se ha posicionado como uno de los troyanos predominantes. El malware ha vuelto a afectar al 4.26% de empresas españolas.

Vulnerabilidades más explotadas

? Command Injection Over HTTP (CVE-2021-43936,CVE-2022-24086) - se descubrió una vulnerabilidad de 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 permitiría a un atacante ejecutar código arbitrario en la máquina objetivo.
? Zyxel ZyWALL Command Injection (CVE-2023-28771): existe una vulnerabilidad de inyección de comandos en Zyxel ZyWALL. La explotación exitosa permitiría a atacantes remotos ejecutar comandos arbitrarios en el sistema afectado.
? HTTP Headers Remote Code Execution (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-1375) - las cabeceras HTTP permiten al cliente y al servidor pasar información adicional con una petición HTTP. Un atacante remoto puede utilizar una cabecera HTTP vulnerable para ejecutar código arbitrario en la máquina víctima.

Principales programas maliciosos para móviles
El mes pasado, Joker ocupó el primer puesto como malware para móviles más extendido, seguido de Anubis y AhMyth.

? Joker - Un spyware Android en Google Play, diseñado para robar mensajes SMS, listas de contactos e información del dispositivo. Además, el malware registra a la víctima en silencio para servicios premium en páginas web de publicidad.

? 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 - Es un 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 apps infectadas, el malware puede recopilar información sensible del dispositivo y realizar acciones como keylogging, tomar capturas de pantalla, enviar mensajes SMS y activar la cámara, que suele utilizarse para robar información sensible.

Los sectores más atacados a escala mundial

El mes pasado, Educación/Investigación se mantuvo en el primer puesto de los sectores más atacados a escala mundial, seguido de Gobierno/Militar y Comunicación.

Educación/Investigación.
Gobierno/Militar.
Comunicación.

Principales grupos de ransomware

Los datos se basan en los "shame sites" de grupos de ransomware de doble extorsión que publicaron información sobre las víctimas. RansomHub fue el grupo de ransomware más prevalente el mes pasado, responsable del 11% de los ataques publicados, seguido de LockBit3 con un 8% y Akira con un 6%.

RansomHub - Es una operación de ransomware como servicio (RaaS) que surgió como una versión renovada del anteriormente conocido ransomware Knight. RansomHub, que apareció a principios de 2024 en foros clandestinos de ciberdelincuencia, ha ganado notoriedad rápidamente por sus agresivas campañas dirigidas a varios sistemas, como Windows, macOS, Linux y, en particular, entornos VMware ESXi. Este malware es conocido por emplear sofisticados métodos de cifrado.

LockBit3 - LockBit3 es un ransomware que opera en un modelo de RaaS, reportado por primera vez en septiembre de 2019. LockBit tiene como objetivo a grandes empresas y entidades gubernamentales de varios países y no apunta a individuos en Rusia o la Comunidad de Estados Independientes.

Akira – Se dio a conocer por primera vez a principios de 2023, se dirige tanto a sistemas Windows como Linux. Utiliza cifrado simétrico con CryptGenRandom y Chacha 2008 para cifrar archivos y es similar al ransomware Conti v2 filtrado. Akira se distribuye a través de varios medios, incluidos adjuntos de correo electrónico infectados y exploits en endpoints VPN. Una vez infectado, cifra los datos y añade la extensión "akira" a los nombres de los archivos, tras lo cual presenta una nota de rescate exigiendo el pago del descifrado.

Datos de contacto:

EverythinkPR
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Software Ciberseguridad Otras Industrias Actualidad Empresarial