Publicado en Madrid el 11/09/2024

# El malware más buscado de agosto de 2024: RansomHub lidera el RaaS, mientras que Meow aumenta su popularidad

**El Índice Global de Amenazas de Check Point Software pone de relieve un cambio en el panorama del ransomware como servicio (RaaS). Los investigadores han identificado el ascenso de Meow con tácticas novedosas y un impacto significativo**

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 agosto de 2024. El ransomware se ha mantenido como fuerza dominante, con RansomHub como el principal grupo. Esta operación RaaS se ha expandido rápidamente desde su cambio de marca del ransomware Knight, que ha atacado a más de 210 víctimas en todo el mundo. Mientras tanto, ha surgido una nueva amenaza llamada Meow, otro ciberataque de ransomware que ha pasado del cifrado a la venta de datos robados en mercados de filtración.

El mes pasado, RansomHub consolidó su posición como la principal amenaza de ransomware, como se detalla en un aviso conjunto del FBI, CISA, MS-ISAC y HHS. Esta organización RaaS ha atacado de forma agresiva sistemas Windows, macOS, Linux y, especialmente, entornos VMware ESXi, mediante técnicas sofisticadas de cifrado.

"La aparición de RansomHub como la principal amenaza de ransomware en agosto subraya la creciente sofisticación de las operaciones de Ransomware-as-a-Service", afirma Maya Horowitz, VP de Investigación de Check Point Software. "El auge de Meow pone de relieve el cambio hacia el mercado de filtración de datos, lo que indica un nuevo método de monetización para los operadores de ransomware, donde cada vez más la información robada se vende a terceros, en lugar de simplemente publicarse online. A medida que evolucionan estas amenazas, las empresas deben mantenerse alerta, adoptar medidas de seguridad proactivas y mejorar continuamente sus defensas contra ataques cada vez más sofisticados".

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 7% en organizaciones de todo el mundo, seguido de Qbot, con un impacto global del 5,3%, y Androxgh0st, con un impacto global del 5,3%.

? FakeUpdates (AKA SocGholish) – 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 7%

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 instalar 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 5,3% de empresas españolas.

? 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 5,3% de las empresas en España.

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.

Los tres malware móviles más usados en agosto

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

? 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.

? Hydra - Troyano bancario diseñado para robar credenciales bancarias solicitando a las víctimas que habiliten permisos y accesos peligrosos cada vez que entran en cualquier aplicación bancaria.

Los sectores más atacados en España

El mes pasado, los medios de comunicación se mantuvieron en el primer puesto de los sectores más atacados a escala mundial, seguido de gobierno/militar y servicios públicos.

Medios de comunicación.
Gobierno/militar.
Servicios públicos.

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 15% de los ataques publicados, seguido de Meow con un 9% y LockBit con un 8%.

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.
Meow - Meow Ransomware es una variante basada en el ransomware Conti, conocida por cifrar una amplia gama de archivos en sistemas comprometidos y añadirles la extensión «.MEOW». Deja una nota de rescate llamada «readme.txt», que indica a las víctimas que se pongan en contacto con los atacantes por correo electrónico o Telegram para negociar el pago del rescate. El ransomware Meow se propaga a través de varios vectores, incluyendo configuraciones RDP desprotegidas, spam de correo electrónico y descargas maliciosas, y utiliza el algoritmo de cifrado ChaCha20 para bloquear archivos, excluyendo «.exe» y archivos de texto.
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.

**Datos de contacto:**
EverythinkPR
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Telecomunicaciones Comunicación Programación Madrid Ciberseguridad Dispositivos móviles Otras Industrias Actualidad Empresarial