Publicado en Madrid el 15/10/2024

# El malware "top ventas" de septiembre sigue siendo RansomHub, que vuelve a liderar el RaaS

## El Índice Global de Amenazas de Check Point Software pone de relieve cómo la inteligencia artificial sigue siendo una herramienta que se utiliza para crear malware con mayor facilidad

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 septiembre de 2024. El informe destaca una tendencia en el panorama de la ciberseguridad, en particular la aparición de malware impulsado por inteligencia artificial.

Este mes, los investigadores han descubierto que los ciberdelincuentes han utilizado la IA para desarrollar un script que distribuye el malware AsyncRAT, que ahora ocupa el décimo lugar en la lista de malware más prevalente. El método implica el contrabando de HTML, donde se envía un archivo ZIP protegido por contraseña que contiene código malicioso en VBScript que inicia una cadena de infección en el dispositivo de la víctima. Una vez ejecutado, AsyncRAT se instala, lo que permite al atacante registrar pulsaciones de teclas, controlar remotamente el dispositivo infectado y desplegar malware adicional. Este descubrimiento resalta una tendencia creciente: los ciberdelincuentes con habilidades técnicas limitadas usan IA para crear malware con mayor facilidad.

Por otra parte, Joker continúa siendo el malware móvil más prevalente, mientras que RansomHub sigue siendo el grupo de ransomware líder, ambos mantienen sus posiciones desde el mes anterior.

"El hecho de que los ciberdelincuentes hayan comenzado a utilizar IA generativa como parte de su infraestructura de ataque resalta la continua evolución de las tácticas de ciberataques. Los atacantes están aprovechando cada vez más las tecnologías disponibles para mejorar sus operaciones, lo que hace esencial que las empresas implementen estrategias de seguridad proactivas, incluidos métodos avanzados de prevención y una capacitación integral para sus equipos", 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 6,9% en organizaciones de todo el mundo, seguido de Androxgh0st, con un impacto global del 5,7% y Formbook, con un impacto global del 3,8%

? 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 6,9% 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 5,7% de las empresas en España.

? Formbook – Infostealer (ladrón de información) que tiene como objetivo el sistema operativo de Windows y fue el primero detectado en 2016. Se comercializa como 'malware como servicio' en foros de hacking clandestinos debido a sus sólidas técnicas de evasión y a su precio relativamente bajo. FormBook recopila credenciales de varios buscadores webs, realiza capturas de pantallas, supervisa y registra las pulsaciones del teclado, y puede descargar y ejecutar archivos según las órdenes de su centro de control. Este infostealer ha impactado en un 3,8% de las 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.

? 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 travesía de directorios en diferentes servidores web. La vulnerabilidad se debe a un error de validación de entrada en un servidor web que no desinfecta correctamente la URI para los patrones de travesía de directorios. La explotación exitosa permite a atacantes remotos no autenticados revelar o acceder a archivos arbitrarios en el servidor vulnerable.

? HTTP Headers Remote Code Execution (CVE-2020-10826, CVE-2020-10827, CVE-2020-10828, CVE-2020-1375) – Los encabezados HTTP permiten que el cliente y el servidor pasen información adicional con una solicitud HTTP. Un atacante remoto puede utilizar un encabezado HTTP vulnerable para ejecutar código arbitrario en la máquina víctima.

Los tres malware móviles más usados en septiembre

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

? 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.
? Hiddad - Hiddad es un malware para Android que re empaqueta aplicaciones legítimas y las coloca en la tienda de un tercero. Su función principal es mostrar anuncios, pero también puede obtener acceso a detalles de seguridad clave integrados en el sistema operativo.

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.

Gobierno/Militar.
Medios de comunicación.
Consultoría.

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 17% de los ataques publicados, seguido de Play con un 10% y Qilin con un 5%.

RansomHub - es una operación de ransomware como servicio (RaaS) que surgió como una versión renovada de 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.
Play Ransomware -también conocido como PlayCrypt, es un grupo de ransomware que surgió por primera vez en junio de 2022. Se ha dirigido un amplio espectro de empresas e infraestructuras críticas en América del Norte, América del Sur y Europa y ha afectado aproximadamente a 300 entidades para octubre de 2023. Play Ransomware suele obtener acceso a redes a través de cuentas válidas comprometidas o mediante la explotación de vulnerabilidades no parcheadas, como las de los Fortinet SSL VPN. Una vez dentro, emplea técnicas como el uso de binarios de "living-off-the-land" (LOLBins) para tareas como la exfiltración de datos y el robo de credenciales.
Qilin - Qilin, también conocido como Agenda, es una operación criminal de Ransomware-as-a-Service que colabora con afiliados para cifrar y filtrar datos de empresas comprometidas, exigiendo posteriormente un rescate. Esta variante de ransomware se detectó por primera vez en julio de 2022 y está desarrollada en Golang. La agenda es conocida por dirigirse a grandes empresas y compañías de alto valor, con un enfoque en los sectores de la salud y la educación. Qilin suele infiltrarse en las víctimas a través de correos electrónicos de phishing que contienen enlaces maliciosos para establecer el acceso a sus redes y extraer información sensible. Una vez dentro, Qilin suele moverse lateralmente por la infraestructura de la víctima en busca de datos críticos que cifrar.

**Datos de contacto:**
EverythinkPR
EverythinkPR

91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Inteligencia Artificial y Robótica Comunicación Software Ciberseguridad Dispositivos móviles Innovación Tecnológica Consultoría Actualidad Empresarial