Publicado en Madrid el 12/11/2024

El malware más buscado de octubre de 2024: los infostealers aumentan a medida que los ciberdelincuentes aprovechan nuevos vectores de ataque

El Índice Global de Amenazas de Check Point Software revela un aumento significativo de infostealers como Lumma Stealer, mientras que el malware para móviles como Necro sigue representando una amenaza importante

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 octubre de 2024. El informe destaca una tendencia en el panorama de la ciberseguridad: el aumento de los infostealers y la sofisticación de los métodos de ataque empleados por los ciberdelincuentes.

Este mes, los investigadores han descubierto una cadena de infección en la que se utilizan páginas CAPTCHA falsas para distribuir el malware Lumma Stealer, que ha alcanzado el cuarto lugar en el ranking mensual de los malwares más activos. Esta campaña destaca por su alcance global, ya que afecta a varios países a través de dos vectores de infección principales: uno que involucra URLs de descarga de juegos maliciosos y otro a través de emails de phishing dirigidos a usuarios de GitHub, como un nuevo formato de vector de ataque. El proceso de infección engaña a las víctimas para que ejecuten un script malicioso que se copia en su portapapeles.

En el ámbito del malware móvil, la nueva versión de Necro ha surgido como una amenaza importante y ocupa ya el segundo lugar entre los malwares móviles. Necro ha infectado varias aplicaciones populares, incluidas modificaciones de juegos disponibles en Google Play, con una audiencia acumulada de más de 11 millones de dispositivos Android. Este malware emplea técnicas de confusión para evadir su detección y utiliza esteganografía, que es la práctica de ocultar información dentro de otro mensaje u objeto físico para camuflar sus cargas maliciosas. Una vez activado, puede mostrar anuncios en ventanas invisibles, interactuar con ellos e incluso suscribir a las víctimas a servicios de pago, lo que subraya la evolución de las tácticas que los atacantes utilizan para monetizar sus operaciones.

"El aumento de los infostealers sofisticados subraya una realidad en crecimiento. Los ciberdelincuentes están evolucionando sus métodos y aprovechando vectores de ataque innovadores. Las empresas deben ir más allá de las defensas tradicionales, adoptando medidas de seguridad proactivas y adaptativas que anticipen amenazas emergentes para contrarrestar estos desafíos persistentes de manera efectiva", 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 7% en organizaciones de todo el mundo, seguido de Androxgh0st, con un impacto global del 5% y Lumma, con un impacto global del 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.
? 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% de las compañías españolas.
? Lumma – Lumma, también conocido como LummaC2, es un malware de robo de información vinculado a Rusia que opera como plataforma de Malware-as-a-Service (MaaS) desde 2022. Este malware, descubierto a mediados de 2022, está en continua evolución y se distribuye activamente en foros en ruso. Como típico ladrón de información, LummaC2 se centra en recopilar diversos datos de los sistemas infectados, incluidas las credenciales del navegador y la información de las cuentas de criptomonedas. Este malware ha impactado en un 3% de los negocios en España.

Vulnerabilidades más explotadas

? 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.
? 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 de esta vulnerabilidad permitiría a atacantes remotos ejecutar comandos arbitrarios en el sistema afectado.

Los tres malware móviles más usados en octubre

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

? 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.
? Necro - es un troyano dropper de Android. Es capaz de descargar otro malware, mostrar anuncios intrusivos y robar dinero mediante el cobro de suscripciones de pago.
? Anubis – es un 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.

Los sectores más atacados en España
El mes pasado, Gobierno/Militar se mantuvieron en el primer puesto de los sectores más atacados a escala mundial, seguido de Servicios Públicos y Medios de Comunicación.

Gobierno/Militar.
Servicios Públicos.
Medios de 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 17% de los ataques publicados, seguido de Play con un 10% y Meow 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 – 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.

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.

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 Digital Actualidad Empresarial