Publicado en Madrid el 11/07/2024

El malware más buscado de junio de 2024: RansomHub ocupa el primer puesto como grupo de ransomware más prevalente tras el descenso de LockBit3

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 BadSpace Windows backdoor propagada a través de falsas actualizaciones del navegador

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 junio de 2024. El mes pasado, los investigadores han observado un cambio en el panorama del Ransomware-as-a-Service (RaaS), con el relativamente recién llegado RansomHub que ha desbancado a LockBit3 para convertirse en el grupo más prevalente. Mientras tanto, se ha identificado una puerta trasera de Windows apodada BadSpace, que implica sitios web de WordPress infectados y falsas actualizaciones del navegador.

El mes pasado, RansomHub fue el grupo RaaS más prevalente después de que la acción de las fuerzas de seguridad contra LockBit3 en febrero le hiciera perder lealtad entre sus afiliados. Como resultado, LockBit3 ha informado de un mínimo histórico de solo 27 víctimas en abril, seguido de una cifra inexplicablemente alta en mayo de más de 170, y menos de 20 en junio, lo que indica su posible declive.

Muchos afiliados a LockBit3 utilizan ahora cifradores de otros grupos RaaS, lo que ha provocado un aumento de las denuncias de víctimas por parte de otros ciberdelincuentes. RansomHub, que apareció por primera vez en febrero de 2024 y, según se informa, es una reencarnación del ransomware Knight, ha experimentado un aumento significativo en junio, con casi 80 nuevas víctimas. Solo el 25% de sus víctimas publicadas procede de EE.UU., con un número significativo de Brasil, Italia, España y Reino Unido.

Por otra parte, los investigadores han destacado una reciente campaña de FakeUpdates (también conocida como SocGholish), que se ha situado como el malware más prevalente, y que ahora ofrece un nuevo backdoor llamado BadSpace. La proliferación de FakeUpdates se ha facilitado a través de una red de afiliados de terceros, que redirige el tráfico de los sitios web comprometidos a las páginas de destino de FakeUpdates. Estas invitan a los usuarios a descargar lo que parece ser una actualización del navegador. Sin embargo, contiene en realidad un cargador basado en JScript que posteriormente descarga y ejecuta la puerta trasera de BadSpace. BadSpace emplea sofisticadas técnicas de ofuscación y antisandbox para evitar su detección y mantiene su persistencia mediante tareas programadas. Su comunicación de mando y control está cifrada, lo que dificulta su interceptación.

"Parece que las acciones contra LockBit3 han tenido el impacto deseado. Sin embargo, como se sugirió anteriormente, su declive solo abre paso a otros grupos para tomar el control y continuar sus campañas de ransomware contra organizaciones a nivel mundial", afirma Maya Horowitz, VP de Investigación de Check Point Software.

Principales familias de malware
*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 6%, y AgentTesla, con un impacto global del 3%.

? 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 9,8% 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 6% de las empresas en España.
? AgentTesla - AgentTesla es un RAT avanzado que funciona como keylogger y ladrón de información, capaz de monitorizar y recopilar la entrada de teclado de la víctima, el teclado del sistema, tomar capturas de pantalla y exfiltrar credenciales a una variedad de software instalado en la máquina de la víctima (incluyendo Google Chrome, Mozilla Firefox y el cliente de correo electrónico Microsoft Outlook). Este RAT ha tenido impacto en el 4% de las empresas españolas.

Vulnerabilidades más explotadas
El mes pasado, ‘Check Point VPN Information Disclosure’ fue la vulnerabilidad más explotada, afectando al 51% de las organizaciones a nivel global, seguida de cerca por ‘Web Servers Malicious URL Directory Traversal’ con un 49% y ‘HTTP Headers Remote Code Execution’ con un impacto global del 44%.

? VPN Information Disclosure (CVE-2024-24919) - se descubrió una vulnerabilidad de revelación de información en Check Point VPN. Esta permite potencialmente a un atacante leer cierta información en Gateways conectados a Internet con VPN de acceso remoto o acceso móvil habilitado.
? 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,C VE-2017-11512,CVE-2018-3948,CVE-2018-3949,CVE-2019-18952,CVE-2020-5410,CVE-2020-8260): existe una vulnerabilidad de traspaso de directorios en diferentes servidores web. Esta se debe a un error de validación de entrada en un servidor web que no sanea correctamente el URI para los patrones de directory traversal. Una explotación exitosa permite a atacantes remotos no autenticados

divulgar 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) - 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 Sanidad.

Educación/Investigación.
Gobierno/Militar.
Sanidad.

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 21% de los ataques publicados, seguido de Play con un 8% y Akira con un 5%.

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.

Play - Play Ransomware, también conocido como PlayCrypt - Ransomware que apareció por primera vez en junio de 2022. Se ha dirigido a un amplio espectro de empresas e infraestructuras críticas en Norteamérica, Sudamérica y Europa, afectando a aproximadamente 300 entidades en octubre de 2023. El ransomware Play suele obtener acceso a las redes a través de cuentas válidas comprometidas o aprovechando vulnerabilidades no parcheadas, como las de las VPN SSL de Fortinet. Una vez dentro, emplea técnicas como el uso de binarios vivientes (LOLBins) para tareas como la exfiltración de datos y el robo de credenciales.

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:
Carolina Domínguez
Everythink PR Boutique
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Internacional Nacional Programación Hardware Madrid Software Ciberseguridad Dispositivos móviles Innovación Tecnológica Digital