Publicado en Madrid el 12/06/2024

La botnet Phorpiex desata un aluvión de phishing mientras LockBit3 vuelve a dominar el panorama del malware en mayo

Check Point Research destaca que España ha experimentado un aumento del 5% de los ataques de malware desde abril. Check Point Research ha descubierto una campaña con la botnet Phorpiex que se utilizaba para propagar ransomware a través de millones de correos electrónicos de phishing y Lockbit3 ha resurgido tras un breve paréntesis y representa un tercio de los ataques de ransomware

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 mayo de 2024. El mes pasado, los investigadores descubrieron una campaña de malspam dirigida por la botnet Phorpiex a través de millones de correos electrónicos de phishing que contenían LockBit Black, (una versión basada en LockBit3, pero no afiliada al grupo de ransomware). Por otro lado, el grupo LockBit3 de ransomware as a Service aumentó su incidencia, tras un breve paréntesis después de que las fuerzas de seguridad lo retiraran del mercado, y representó el 33% de los ataques de ransonware. Le siguieron Inc. Ransom con un 7% y Play con una tasa de detección del 5%. Inc. Ransom ha reivindicado recientemente la autoría de un grave incidente cibernético que interrumpió los servicios públicos del Ayuntamiento de Leicester, en el Reino Unido, donde supuestamente ha robado más de 3 terabytes de datos y ha provocado un apagón generalizado del sistema.

Los operadores originales de la red de bots Phorpiex cerraron y vendieron el código fuente en agosto de 2021. Sin embargo, en diciembre de 2021, Check Point Research descubrió que había resurgido como una nueva variante llamada «Twizt», que opera en un modelo peer-to-peer descentralizado. En abril de este año, la New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) encontró pruebas de que la botnet Phorpiex, que ocupaba el sexto lugar en el índice de amenazas de abril, se había utilizado para enviar millones de correos electrónicos de phishing como parte de una campaña del ransomware LockBit3. Estos correos llevaban ZIP adjuntos que, al ejecutar los archivos .doc.scr, desencadenaban el proceso de cifrado del ransomware. La campaña utilizó más de 1.500 direcciones IP únicas, principalmente de Kazajistán, Uzbekistán, Irán, Rusia y China.

"Aunque las fuerzas de seguridad han conseguido desarticular temporalmente al grupo de LockBit3 al desenmascarar a uno de sus líderes y afiliados, además de liberar más de 7.000 claves de descifrado de LockBit, no ha sido suficiente para acabar por completo con la amenaza, ya que se reagrupan y despliegan nuevas tácticas para continuar con su persecución", señala Maya Horowitz, vicepresidenta de investigación de Check Point Software. "El ransomware es uno de los métodos de ataque más disruptivos de los ciberdelincuentes. Una vez que se han infiltrado en la red y extraído la información, las opciones son limitadas y por ello. Las empresas deben estar alerta ante los riesgos y priorizar las medidas preventivas".

Los tres malware más buscados en España en mayo
*Las flechas indican el cambio en el ranking en comparación con el mes pasado.

Check Point Research destaca que España ha experimentado un aumento del 5% de los ataques malware desde abril. Estos son los tres malware más buscados en el país:

? FakeUpdates – Downloader escrito 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 10% 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 4% 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 3% de empresas españolas.

Las tres industrias más atacadas en mayo

El mes pasado, Educación/Investigación se situó como la industria más atacada a nivel mundial, seguida de Gobierno/Militar y Comunicación.

Educación/Investigación
Gobierno/Militar
Comunicación

Las tres vulnerabilidades más explotadas en mayo

Por otra parte, Check Point Software señala que el mes pasado las vulnerabilidades más explotadas "Command Injection Over HTTP", que impactó al 50% de las empresas, "Web Servers Malicious URL Directory Traversal", que afectó al 47%. Les siguió la "Apache Log4j Remote Code Execution", con un impacto global del 46%.

? Command Injection Over HTTP (CVE-2021-43936, CVE-2022-24086) – Se ha informado de una vulnerabilidad de inyección de comandos sobre 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 en la trayectoria 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.

?Apache Log4j Remote Code Execution (CVE-2021-44228) – La explotación de esta vulnerabilidad puede permitir que un atacante remoto ejecute un código arbitrario en el dispositivo afectado.

Los tres malware móviles más usados en mayo

El mes pasado, Anubis se mantuvo en el primer lugar como el malware móvil más usado, seguido de AhMyth y Hydra.

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 – 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 aplicaciones infectadas, el malware puede recopilar información confidencial del dispositivo y realizar acciones como el registro de teclas, capturas de pantalla, el envío de mensajes SMS y la activación de la cámara, lo que se suele usar para robar información sensible.

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 tres grupos ransomware más destacados en mayo

Esta sección se basa en información recibida de más de 200 "shame sites" ejecutados por grupos ransomware de doble extorsión que publicaron los nombres e información de las víctimas. Los datos de estos sitios tienen sus propios sesgos, pero aun así proporcionan información valiosa sobre el ecosistema del ransomware.

En el último mes, LockBit3 ha sido el ransomware más destacado, responsable del 33% de los ataques realizados, seguido de Inc. Ransom con un 7% y Play con un 5%.

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. A pesar de experimentar interrupciones significativas en febrero de 2024 debido a la acción de las fuerzas del orden, LockBit3 ha reanudado la publicación de información sobre sus víctimas.

Inc. Ransom - Inc. Ransom es una operación de extorsión de ransomware que surgió en julio de 2023, realizando ataques de spear-phishing y apuntando a servicios vulnerables. Los principales objetivos del grupo son empresas de Norteamérica y Europa de diversos sectores, como la sanidad, la educación y la administración pública. Las cargas útiles del ransomware de Inc. admiten varios argumentos de línea de comandos y utilizan cifrado parcial con un enfoque multiproceso.

Play - Play Ransomware, también conocido como PlayCrypt, es un grupo de ransomware que surgió por primera vez en junio de 2022. Este ransomware se ha dirigido a un amplio espectro de empresas e infraestructuras críticas en América del Norte, América del Sur y Europa, con aproximadamente 300 empresas afectadas en 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.

La lista completa de las diez principales familias de malware en mayo puede consultarse en el blog de Check Point Software.

Datos de contacto:
EverythinkPR
EverythinkPR
91 551 98 91

Nota de prensa publicada en: Madrid

Categorías: Inteligencia Artificial y Robótica Software Ciberseguridad Innovación Tecnológica