## WATCHGUARD THREAT LAB INFORMA DE QUE EL VOLUMEN DE *RANSOMWARE* YA HA DUPLICADO EL TOTAL DE 2021 A FINALES DEL PRIMER TRIMESTRE DE 2022

WatchGuard® Technologies, líder global en seguridad e inteligencia de red avanzada, protección *endpoint* avanzada, autenticación multifactor (MFA) y Wi-Fi seguro, ha anunciado los resultados de su reciente Informe Trimestral de Seguridad en Internet, en el que se detallan las principales tendencias de *malware* y amenazas de seguridad de red analizadas por los investigadores de WatchGuard Threat Lab. Los principales hallazgos de la investigación revelan que las detecciones de *ransomware* en el primer trimestre de este año duplicaron el volumen total reportado para 2021, la botnet Emotet ha regresado con fuerza, la perversa vulnerabilidad Log4Shell ha triplicado sus esfuerzos de ataque, así como la actividad de criptominería maliciosa, y mucho más.

*"Basándonos en el pico temprano de ransomware de este año y en los datos de los trimestres anteriores, predecimos que 2022 romperá nuestro récord de detecciones anuales de ransomware"*, señala Corey Nachreiner, director de seguridad de WatchGuard. "*Seguimos instando a las empresas a que no solo se comprometan a implementar medidas sencillas, pero de importancia crítica, sino que adopten un verdadero enfoque de seguridad unificado que pueda adaptarse rápida y eficazmente a las amenazas crecientes y en evolución".*

Otras conclusiones clave de este Informe de Seguridad en Internet, que analiza los datos del Q1 de 2022, son las siguientes:

- El *ransomware* se vuelve nuclear - Aunque los resultados del Informe de Seguridad en Internet del Q4 de 2021 del Threat Lab revelaban que los ataques de ransomware han tenido una tendencia a la baja año tras año, todo cambió en Q1 de 2022 con una explosión masiva de detecciones de ransomware. Sorprendentemente, el número de ataques de ransomware detectados en Q1 ya ha duplicado el número total de detecciones de todo el año 2021.

- LAPSUS$ surge tras la caída de REvil - En Q4 de 2021 se produjo la caída del tristemente célebre grupo cibernético REvil, que, en retrospectiva, abrió la puerta a la aparición de otro grupo: LAPSUS$. El análisis del Q1 de WatchGuard sugiere que el grupo de extorsión LAPSUS$, junto con muchas nuevas variantes de ransomware como BlackCat, el primer ransomware conocido escrito en lenguaje de programación Rust, podrían ser factores que contribuyen a un panorama de amenazas de *ransomware* y *ciberextorsión* en constante aumento.

- Log4Shell hace su debut en la lista Top 10 de ataques de red - Divulgada públicamente a principios de diciembre de 2021, la perversa vulnerabilidad Apache Log4j2, también conocida como Log4Shell, debutó en el top 10 de principales ataques de red a finales de este trimestre. En comparación con las detecciones de IPS totales en el Q4 de 2021, la firma de Log4Shell casi se triplicó en Q1 de este año. Destacado como el principal incidente de seguridad en el último Informe de Seguridad en Internet de WatchGuard, Log4Shell atrajo la atención por obtener una puntuación perfecta de 10,0 en CVSS, la máxima criticidad posible para una vulnerabilidad, y por su uso generalizado en programas Java y el nivel de facilidad en la ejecución de código arbitrario.

- Emotet regresa de nuevo- A pesar de los esfuerzos para interrumpirlo por parte de las fuerzas de seguridad a principios de 2021, Emotet representa 3 de las 10 principales detecciones y el *malware* más extendido este trimestre tras su resurgimiento en el Q4 de 2021. Las detecciones de Trojan.Vita, que se dirigió en gran medida a Japón y también apareció en la lista de los cinco primeros *malware* cifrados, y Trojan. Valyria utilizan ambos *exploits* en Microsoft Office para descargar el botnet Emotet. La tercera muestra de *malware* relacionada con Emotet, MSIL.Mensa.4, puede propagarse a través de dispositivos de almacenamiento conectados y se dirige principalmente a redes de Estados Unidos. Los datos del Threat Lab indican que Emotet actúa como *dropper*, descargando e instalando el archivo desde un servidor de entrega de malware.

- Los scripts de PowerShell lideran el aumento de los ataques a *endpoints* - Las detecciones generales de *endpoints* en Q1 aumentaron un 38 % respecto al trimestre anterior. Los *scripts*, concretamente los de PowerShell, fueron el vector de ataque dominante. Con el 88 % de todas las detecciones, los *scripts* superaron por sí solos el número de detecciones totales de *endpoints* que se habían registrado en el trimestre anterior. Los *scripts* de PowerShell fueron responsables del 99,6 % de las detecciones de *scripts* en Q1, lo que demuestra que los atacantes están pasando a los ataques sin archivos y a los que viven de las herramientas legítimas. Aunque estos *scripts* son la clara elección de los atacantes, los datos de WatchGuard revelan que no hay que pasar por alto otras fuentes de origen del *malware*.

- Operaciones legítimas de minería de criptomonedas asociadas a actividades maliciosas - Las tres nuevas incorporaciones a la lista de los principales dominios de *malware* en Q1 estaban relacionadas con Nanopool. Esta popular plataforma agrega la actividad de la minería de criptomonedas para permitir un rendimiento constante. Estos dominios son técnicamente legítimos y están asociados a una organización legítima. Sin embargo, las conexiones a estos *pools* de minería casi siempre se originan en una red empresarial o educativa a partir de infecciones de *malware* en lugar de operaciones de minería legítimas.

- Las empresas todavía se enfrentan a una amplia gama de ataques de red únicos - Mientras que las 10 principales firmas de IPS representaron el 87 % de todos los ataques de red; las detecciones únicas alcanzaron su mayor recuento desde el Q1 de 2019. Este aumento indica que los ataques automatizados se están centrando en un subconjunto más pequeño de potenciales *exploits* en lugar de probarlo todo. Sin embargo, las empresas siguen experimentando una amplia variedad de detecciones.

- EMEA continúa siendo un punto de acceso para las amenazas de *malware* – Las detecciones regionales generales de malware básico y evasivo muestran que los Firebox en Europa, Oriente Medio y África (EMEA) se vieron más afectados que los de América del Norte, Central y del Sur (AMER) en 57 % y 22 %, respectivamente, seguida por Asia-Pacífico (APAC) con 21 %.

Los informes de investigación trimestrales de WatchGuard se basan en datos anónimos proporcionados por Firebox Feed de los Fireboxes de WatchGuard activos cuyos propietarios han optado por compartir datos en apoyo directo de los esfuerzos de investigación de Threat Lab. En el primer trimestre, WatchGuard bloqueó un total de más de 21,5 millones de variantes de *malware* (274 por dispositivo) y casi 4,7 millones de amenazas de red (60 por dispositivo). El informe completo incluye detalles sobre *malware* adicional y tendencias de red del Q1 de 2022, estrategias de seguridad recomendadas y consejos de defensa críticos para empresas de todos los tamaños y en cualquier sector, y mucha más información.