Más de una semana después de que Microsoft lanzara una herramienta de mitigación de un solo clic, para protegerse de los ataques cibernéticos dirigidos a los servidores Exchange locales, la compañía reveló que se han aplicado parches al 92% de los servidores conectados a Internet afectados por las vulnerabilidades de ProxyLogon.

Con esto, se pone fin a las campañas de espionaje y malware que afectaron a miles de empresas en todo el mundo, con hasta 10 grupos de amenazas persistentes avanzadas (APT) que se movieron rápidamente de forma oportunista para explotar los errores.

Según los datos de telemetría de RiskIQ, existen aproximadamente 29.966 instancias de servidores de Microsoft Exchange aún expuestos a ataques, frente a los 92,072 del 10 de marzo.

Aunque los servidores de Exchange fueron atacados por múltiples grupos de hacking estatales vinculados a China antes del parche de Microsoft el 2 de marzo, el lanzamiento de exploits de prueba de concepto públicos hizo que las infecciones crecieran considerablemente, abriendo la puerta a ataques cada vez mayores como ransomware y el secuestro de shells web instalados en servidores de Microsoft Exchange sin parches para entregar criptomineros y demás malware.

> *«Para empeorar las cosas, los scripts de ataque automatizados de prueba de concepto se están poniendo a disposición del público, lo que hace posible que incluso los atacantes no calificados obtengan rápidamente el control remoto de un servidor Microsot Exchange vulnerable»*, dijo la compañía de seguridad, F-Secure.

En las semanas transcurridas desde que Microsoft lanzó por primera vez sus parches, se descubrieron al menos dos cepas diferentes de ransomware que aprovechan las fallas para instalar DearCry y Black Kingdom.

El análisis de la compañía de seguridad cibernética Sophos, sobre Black Kingdom describe el ransomware como *«algo rudimentario y amateur en su composición»,* y los atacantes abusan de la falla de ProxyLogon para implementar un web shell, utilizándolo para emitir un comando de PowerShell que descarga la carga útil del ransomware, que encripta los archivos y exige un rescate en Bitcoin a cambio de la clave privada.

> *«El ransomware Black Kingdom dirigido a servidores Exchange sin parches tiene todas las características de haber sido creado por un script-kiddie motivado. Las herramientas y técnicas de cifrado son imperfectas, pero el rescate de $10,000 dólares en bitcoins es lo suficientemente bajo como para tener éxito. Todas las amenazas deben tomarse en serio, incluso las aparentemente bajas en calidad»,* dijo Mark Loman, director de ingeniería de Sophos.

El volumen de ataques aún antes de la divulgación pública de ProxyLogon ha llevado a los expertos a investigar si el exploit fue compartido o vendido en la Dark Web, o un socio de Microsoft, con quien la compañía compartió información sobre las vulnerabilidades por medio de su Programa de Protección Activa de Microsoft (MAPP), ya sea accidental o intencionalmente.