Se ha identificado una nueva campaña de malware que apunta a dispositivos perimetrales de Cisco, ASUS, QNAP y Synology, con el propósito de integrarlos en una botnet denominada PolarEdge desde finales de 2023.

La firma francesa de ciberseguridad Sekoia ha detectado a actores maliciosos desconocidos explotando la vulnerabilidad CVE-2023-20118 (calificación CVSS: 6.5), una brecha de seguridad grave que afecta a los routers Cisco Small Business RV016, RV042, RV042G, RV082, RV320 y RV325, permitiendo la ejecución arbitraria de comandos en los dispositivos comprometidos.

Dado que estos routers han alcanzado el fin de su ciclo de vida (EoL), no recibirán actualizaciones de seguridad. Como contramedida, Cisco recomendó en 2023 desactivar la administración remota y restringir el acceso a los puertos 443 y 60443.

En un ataque captado por los honeypots de Sekoia, la vulnerabilidad se utilizó para instalar un implante hasta ahora desconocido: un backdoor basado en TLS, capaz de escuchar conexiones entrantes y ejecutar instrucciones de manera remota.

Este backdoor se despliega a través de un script de shell denominado `"q"`, el cual se descarga mediante FTP y se ejecuta tras una explotación exitosa. Sus funciones incluyen:

- Eliminar registros del sistema
- Finalizar procesos sospechosos
- Descargar un archivo malicioso llamado «t.tar» desde 119.8.186[.]227
- Ejecutar un binario denominado «cipher_log» extraído del paquete
- Garantizar persistencia mediante la modificación del archivo `"/etc/flash/etc/cipher.sh"`, de manera que el binario `"cipher_log"` se ejecute continuamente
- Iniciar «cipher_log», el backdoor TLS

Bajo el nombre PolarEdge, el malware entra en un ciclo ininterrumpido donde establece una sesión TLS y crea un subproceso para gestionar solicitudes y ejecutar instrucciones utilizando

`exec_command`.

> *«El código malicioso notifica al servidor C2 cuando ha comprometido un nuevo sistema. El malware envía estos datos al servidor de monitoreo, permitiendo a los atacantes identificar los dispositivos infectados a través de su dirección IP y puerto asociado»,* explicaron los investigadores de Sekoia, Jeremy Scion y Félix Aimé.

Investigaciones adicionales han revelado que variantes de PolarEdge han sido empleadas contra dispositivos ASUS, QNAP y Synology. Todos los archivos maliciosos fueron cargados en VirusTotal por usuarios ubicados en Taiwán. Las cargas se propagan por FTP, utilizando la dirección IP 119.8.186[.]227, registrada bajo Huawei Cloud.

Se estima que la botnet ha comprometido al menos 2,017 direcciones IP únicas a nivel mundial, con la mayor cantidad de infecciones detectadas en Estados Unidos, Taiwán, Rusia, India, Brasil, Australia y Argentina.

> *«Todavía no se ha determinado el propósito exacto de esta botnet. Uno de los posibles objetivos de PolarEdge podría ser controlar dispositivos perimetrales infectados, convirtiéndolos en nodos de retransmisión para la ejecución de ataques cibernéticos ofensivos»*, indicaron los expertos.
>
> *«La botnet aprovecha diversas vulnerabilidades en múltiples dispositivos, lo que demuestra su capacidad de adaptarse a distintos entornos. La sofisticación del código malicioso sugiere que es una operación bien organizada, llevada a cabo por individuos con altos conocimientos técnicos. Esto posiciona a PolarEdge como una amenaza cibernética significativa y altamente coordinada».*

Botnet masiva ataca cuentas de Microsoft 365

Mientras tanto, la empresa SecurityScorecard ha identificado una botnet con más de 130,000 dispositivos comprometidos, utilizada para ejecutar ataques masivos de password-spraying contra cuentas de Microsoft 365 (M365).

Los ciberdelincuentes están explotando autenticaciones no interactivas mediante credenciales en texto plano, un método utilizado por protocolos heredados como POP, IMAP y SMTP, que en muchos casos no requiere autenticación multifactor (MFA).

Se cree que esta actividad está vinculada a un grupo de origen chino, dado que la infraestructura utilizada está asociada a CDS Global Cloud y UCLOUD HK. Los atacantes emplean credenciales obtenidas de logs de infostealers para acceder a cuentas de M365 y extraer información confidencial.

> «Este método elude las protecciones de seguridad modernas y omite la verificación en dos pasos, dejando una brecha crítica para los equipos de defensa. Los atacantes emplean credenciales robadas para comprometer cuentas de manera masiva», advirtió SecurityScorecard.
>
> *«Estos ataques aparecen en los registros de inicios de sesión no interactivos, los cuales rara vez son monitoreados por los equipos de seguridad. Los criminales se aprovechan de esta omisión para realizar ataques de password-spraying a gran escala sin ser detectados. Se ha observado este patrón en numerosos entornos de M365, lo que indica una amenaza continua y en expansión«.*