Investigadores en ciberseguridad han revelado que un actor malicioso identificado como ViciousTrap ha comprometido cerca de 5,300 dispositivos de borde de red únicos en 84 países, convirtiéndolos en una especie de red tipo *honeypot*.

Este actor de amenazas ha sido visto aprovechando una vulnerabilidad crítica de seguridad que afecta a los routers Cisco Small Business modelos RV016, RV042, RV042G, RV082, RV320 y RV325 (identificada como CVE-2023-20118) para agrupar estos dispositivos comprometidos en una red de honeypots a gran escala. La mayoría de los dispositivos afectados se encuentra en Macao, donde se han detectado 850 equipos comprometidos.

> "La cadena de infección implica la ejecución de un script de shell, denominado *NetGhost*, que redirige el tráfico entrante desde puertos específicos del router comprometido hacia una infraestructura tipo honeypot controlada por el atacante, lo que les permite interceptar los flujos de red", señaló Sekoia en un análisis publicado el jueves.

Cabe destacar que la explotación de la vulnerabilidad CVE-2023-20118 ya había sido previamente atribuida por la empresa francesa de ciberseguridad a otra botnet llamada PolarEdge.

Aunque no se ha encontrado evidencia directa que vincule ambas actividades, se sospecha que el actor de amenazas responsable de ViciousTrap está construyendo una infraestructura tipo honeypot al comprometer una amplia variedad de dispositivos expuestos a Internet. Entre ellos se incluyen routers SOHO, VPNs SSL, grabadores de video (DVRs) y controladores BMC de más de 50 marcas distintas, como Araknis Networks, ASUS, D-Link, Linksys y QNAP.

sekoia | Devices and brands monitored by ViciousTrap infrastructure

SOHO routers and Switches

FRITZ!Box
GPON Home Gateway
D-LINK DIR-850L
D-LINK DNR-312L
D-LINK DIR-853/ET
Cisco RV042
Cisco RV042G
Ikuai8 router
MoviStar router
TP-link AC2100
TP-link TL-WR841N
TP-link Archer C12000
Netonix WISP switch
Robustel LTE router
TotoLink router
VSOL SOHO Router
iGate GW040-H
Trendnet N300 and Tew-711br
Ruijie Networks-EWEB
Ruijie RG-EG5210-JP
LinkSys Smart WiFi
Mitrastar
ZyXEL VMG3625-T20A
ZyXEL XMG3927-B50A
ZyXEL Speedlink 5501
ARRIS router
ASUS DSL

Network security appliances

Stormshield SSLVPN
Ivanti Connect Secure 9.1.18
Fortinet
Citrix Netscaler
Cisco ASA
Check Point Quantum Spark Gateway
Check Point Quantum Security Gateway
Guardo 1.0 資安管理系統

DVR / IP Camera

Honeywell Security Camera
Avtech
Axis
Amcrest
DahuaSecurity camera
Panasonic BB-ST162
Panasonic BL-VT164
Panasonic WV-SC385
Panasonic BB-ST165
Rifatron IDSS
Speco
Xiongmai Technology
ICCTV
Samsung
Tiandy Net
QNO
D-link DCS

Network storage systems

QNAP QTS
Linkstation™ ls220d – buffalo
Motorola-mobility bms
Buffalo TeraStation

Other devices & softwares

Ruckus wireless Zonedirector
Supermicro Intelligent Management (IPMI)
VOS3000
PestPac Control Software
TP-link deco system
Unifi network ubiquiti
Ubiquiti AirOs
Canon GX7000 Printer
Etrafficers, inc. server
Cisco Catalyst SD-WAN
Cambium cnPilot e400
Asus AI Cloud

> "*Esta configuración permitiría al actor observar intentos de explotación en distintos entornos y, posiblemente, recopilar exploits no públicos o de tipo zero-day, además de reutilizar accesos obtenidos por otros grupos maliciosos*", añadieron.

La cadena de ataque comienza con la explotación de la vulnerabilidad CVE-2023-20118, que

permite descargar y ejecutar un script Bash utilizando `ftpget`. Este script inicial se conecta luego a un servidor externo para obtener el binario de `wget`. A continuación, se vuelve a explotar la misma vulnerabilidad de Cisco para ejecutar un segundo script descargado mediante el `wget` previamente instalado.

Este script de segunda etapa, conocido internamente como NetGhost, está diseñado para redirigir el tráfico de red del sistema comprometido hacia una infraestructura externa bajo el control del atacante. Esto facilita ataques del tipo adversario-en-el-medio (AitM). Además, el script incluye funciones para autoborrarse del host comprometido, reduciendo así las huellas forenses.

Según Sekoia, todos los intentos de explotación han sido rastreados hasta una única dirección IP: «101.99.91[.]151», con actividad inicial registrada desde marzo de 2025. Un mes después, se observó un evento significativo: los operadores de ViciousTrap reutilizaron una *web shell* no documentada previamente usada en los ataques de la botnet PolarEdge.

> *"Esta hipótesis concuerda con el uso de NetGhost por parte del atacante. El mecanismo de redirección posiciona al actor como un observador silencioso, capaz de recopilar intentos de explotación y, potencialmente, accesos a web shells en tránsito",* explicaron los investigadores de seguridad Felix Aimé y Jeremy Scion.

Incluso durante este mes, los esfuerzos de explotación también han apuntado a routers ASUS, aunque desde otra dirección IP («101.99.91[.]239»). Sin embargo, en estos casos no se ha detectado la creación de honeypots en los dispositivos comprometidos. Todas las direcciones IP utilizadas en esta campaña se encuentran en Malasia, asociadas al Sistema Autónomo AS45839, gestionado por el proveedor de hosting Shinjiru.

Se cree que el actor detrás de estas operaciones es de origen chino-hablante, basándose en una leve coincidencia con la infraestructura usada por GobRAT y en el hecho de que el tráfico es redirigido hacia numerosos recursos ubicados en Taiwán y Estados Unidos.

> *"El objetivo final de ViciousTrap sigue sin estar claro, aunque evaluamos con alta confianza que se trata de una red con comportamiento de honeypot"*, concluyó Sekoia.