Los operadores del enigmático botnet Quad7 están evolucionando activamente al comprometer diversas marcas de routers SOHO y dispositivos VPN, explotando una combinación de vulnerabilidades de seguridad, tanto conocidas como desconocidas.

Entre los dispositivos afectados se encuentran productos de TP-LINK, Zyxel, Asus, Axentra, D-Link y NETGEAR, según un reciente informe de la empresa francesa de ciberseguridad Sekoia.

> *«Los operadores del botnet Quad7 parecen estar mejorando su arsenal, introduciendo una nueva puerta trasera y probando nuevos protocolos, con el fin de incrementar su capacidad de sigilo y evitar que se rastreen sus cajas de relevo operativas (ORBs)»,* explicaron los investigadores Félix Aimé, Pierre-Antoine D. y Charles M.

Quad7, también conocido como 7777, fue documentado públicamente por primera vez en octubre de 2023 por el investigador independiente Gi7w0rm, quien destacó el patrón de actividades del grupo, centrado en comprometer routers TP-Link y grabadoras de video digital (DVRs) Dahua para incorporarlos en un botnet.

Este botnet, que recibe su nombre porque abre el puerto TCP 7777 en los dispositivos comprometidos, ha sido observado lanzando ataques de fuerza bruta contra instancias de Microsoft 365 y Azure.

> *«También parece infectar otros sistemas, como MVPower, Zyxel NAS y GitLab, aunque en volúmenes muy bajos. El botnet no solo habilita un servicio en el puerto 7777, sino que también activa un servidor SOCKS5 en el puerto 11228″*, mencionó Jacob Baines de VulnCheck en enero.

Análisis posteriores de Sekoia y Team Cymru durante los últimos meses han revelado que el

botnet no solo ha comprometido routers TP-Link en Bulgaria, Rusia, Estados Unidos y Ucrania, sino que también ha ampliado su alcance para atacar routers ASUS que tienen los puertos TCP 63256 y 63260 abiertos.

Los descubrimientos más recientes indican que el botnet está compuesto por tres grupos adicionales:

- xlogin (también conocido como botnet 7777): Un botnet conformado por routers TP-Link comprometidos con los puertos TCP 7777 y 11288 abiertos.
- alogin (también conocido como botnet 63256): Un botnet compuesto por routers ASUS comprometidos con los puertos TCP 63256 y 63260 abiertos.
- rlogin: Un botnet compuesto por dispositivos Ruckus Wireless comprometidos que tienen abierto el puerto TCP 63210.
- axlogin: Un botnet que tiene la capacidad de atacar dispositivos NAS de Axentra (aunque aún no se ha detectado en la naturaleza).
- zylogin: Un botnet compuesto por dispositivos VPN Zyxel comprometidos que tienen abierto el puerto TCP 3256.

Sekoia informó que los países con más infecciones son Bulgaria (1,093), Estados Unidos (733) y Ucrania (697).

En otro indicio de evolución táctica, los actores maliciosos ahora están utilizando una nueva puerta trasera llamada UPDTAE, la cual establece una shell inversa basada en HTTP para tomar control remoto de los dispositivos infectados y ejecutar comandos desde un servidor de comando y control (C2).

Todavía no está claro cuál es el objetivo final del botnet ni quién lo controla, pero la empresa indicó que es probable que se trate de un actor de amenazas patrocinado por el gobierno chino.

> *«En cuanto al botnet 7777, solo observamos intentos de fuerza bruta contra*

> *cuentas de Microsoft 365. Para los otros botnets, aún no tenemos claro cómo son utilizados»*, comentó Aimé a la publicación.
>
> *«No obstante, tras intercambiar información con otros investigadores y realizar nuevos descubrimientos, estamos casi seguros de que los operadores son patrocinados por el estado chino, en lugar de simples cibercriminales involucrados en compromisos de correos electrónicos empresariales.»*
>
> *«Observamos que los actores maliciosos están buscando ser más sigilosos mediante el uso de nuevos malwares en los dispositivos comprometidos. El principal objetivo de esta estrategia es evitar el rastreo de los botnets afiliados.»*