Un botnet nunca antes visto llamado Goldoon ha sido detectado atacando routers D-Link con una vulnerabilidad crítica de casi una década de antigüedad, con el objetivo de utilizar los dispositivos comprometidos para realizar ataques adicionales.

La vulnerabilidad en cuestión es CVE-2015-2051 (puntuación CVSS: 9.8), la cual afecta a los routers D-Link DIR-645 y permite a los atacantes remotos ejecutar comandos arbitrarios mediante solicitudes HTTP especialmente diseñadas.

> Los investigadores de Fortinet FortiGuard Labs, Cara Lin y Vincent Li, explicaron: *«Si un dispositivo objetivo es comprometido, los atacantes pueden obtener control total, lo que les permite extraer información del sistema, establecer comunicación con un servidor C2 y luego utilizar estos dispositivos para lanzar más ataques, como ataques de denegación de servicio distribuido (DDoS)».*

Los datos de telemetría de la empresa de seguridad en redes indican un aumento en la actividad del botnet alrededor del 9 de abril de 2024.

Todo comienza con la explotación de CVE-2015-2051 para obtener un script de carga útil de un servidor remoto, el cual es responsable de descargar la carga útil de la siguiente etapa para diferentes arquitecturas de sistemas Linux, incluyendo aarch64, arm, i686, m68k, mips64, mipsel, powerpc, s390x, sparc64, x86-64, sh4, riscv64, DEC Alpha y PA-RISC.

Posteriormente, la carga útil es lanzada en el dispositivo comprometido y actúa como un descargador para el malware Goldoon desde un punto final remoto. Luego, el distribuidor elimina el archivo ejecutado y después se borra a sí mismo en un intento de ocultar el rastro y pasar desapercibido.

Cualquier intento de acceder directamente al punto final mediante un navegador web muestra el mensaje de error: *«Lo siento, eres un agente del FBI y no podemos ayudarte ¡Vete o te mataré :)»*

Además de configurar la persistencia en el host mediante varios métodos de autorun, Goldoon establece contacto con un servidor de comando y control (C2) para esperar órdenes para acciones de seguimiento.

Esto incluye *«asombrosamente 27 métodos diferentes»* para llevar a cabo ataques de inundación DDoS utilizando diversos protocolos como DNS, HTTP, ICMP, TCP y UDP.

> *«Si bien CVE-2015-2051 no es una vulnerabilidad nueva y presenta una baja complejidad de ataque, tiene un impacto de seguridad crítico que puede llevar a la ejecución remota de código»,* explicaron los investigadores.

Este desarrollo ocurre mientras los botnets continúan evolucionando y explotando tantos dispositivos como sea posible, incluso cuando tanto los cibercriminales como los actores de amenazas persistentes avanzadas han demostrado interés en los routers comprometidos para usarlos como una capa de anonimización.

> Según un informe de la empresa de ciberseguridad Trend Micro, *«Los cibercriminales alquilan routers comprometidos a otros criminales, y lo más probable es que también los pongan a disposición de proveedores comerciales de proxies residenciales».*
>
> *«Actores de amenazas estatales como Sandworm utilizaron sus propios botnets de proxy dedicados, mientras que el grupo APT Pawn Storm tenía acceso a un botnet de proxy criminal de Ubiquiti EdgeRouters».*

El objetivo de utilizar los routers hackeados como proxies es ocultar rastros de su presencia y dificultar la detección de actividades maliciosas al mezclar su actividad con el tráfico normal benigno.

A principios de febrero, el gobierno de EE. UU. dio pasos para desmantelar partes de un botnet llamado MooBot que, entre otros dispositivos expuestos a Internet como Raspberry Pi y servidores VPS, aprovechaba principalmente los Ubiquiti EdgeRouters.

Trend Micro dijo que observó que los routers se utilizaban para diferentes fines, como fuerza bruta de Secure Shell (SSH), spam farmacéutico, empleo de reflectores del protocolo de bloques de mensajes del servidor (SMB) en ataques de relevos de hash NTLMv2, proxy de credenciales robadas en sitios de phishing, proxy multifuncional, minería de criptomonedas y envío de correos electrónicos de spear phishing.

Los routers de Ubiquiti también han sido atacados por otro actor de amenazas que infecta estos dispositivos con un malware llamado Ngioweb, que luego se utilizan como nodos de salida en un botnet de proxy residencial disponible comercialmente.

Los hallazgos subrayan aún más el uso de diversas familias de malware para controlar los routers y convertirlos efectivamente en puestos de escucha encubiertos capaces de monitorear todo el tráfico de la red.

> *«Los routers de Internet siguen siendo un activo popular para que los actores de amenazas los comprometan, ya que a menudo tienen una monitorización de seguridad reducida, políticas de contraseña menos estrictas, no se actualizan con frecuencia y pueden usar sistemas operativos potentes que permiten la instalación de malware como mineros de criptomonedas, proxies, malware de denegación de servicio distribuido (DDoS), scripts maliciosos y servidores web»,* dijo Trend Micro.