Se ha observado que varios botnets de denegación de servicio distribuido (DDoS) están aprovechando una falla crítica en dispositivos Zyxel que salió a la luz en abril de 2023 para obtener control remoto de sistemas vulnerables.

> *«Mediante la captura del tráfico de explotación, se pudo identificar la dirección IP del atacante, y se determinó que los ataques estaban ocurriendo en múltiples regiones, incluyendo América Central, América del Norte, Asia Oriental y Asia del Sur»*, señaló Cara Lin, investigadora de Fortinet FortiGuard Labs.

La vulnerabilidad, identificada como CVE-2023-28771 (puntuación CVSS: 9.8), es una falla de inyección de comandos que afecta a múltiples modelos de firewall y que podría permitir a un actor no autorizado ejecutar código arbitrario enviando un paquete especialmente diseñado al dispositivo objetivo.

El mes pasado, la Fundación Shadowserver advirtió que la falla estaba siendo *«activamente explotada para construir un botnet similar a Mirai»*, al menos desde el 26 de mayo de 2023, lo que indica cómo está aumentando el abuso de servidores que ejecutan software sin parches.

Los últimos descubrimientos de Fortinet indican que la vulnerabilidad está siendo oportunamente aprovechada por múltiples actores para infiltrarse en hosts susceptibles y agruparlos en un botnet capaz de lanzar ataques de denegación de servicio distribuido (DDoS) contra otros objetivos.

Esto incluye variantes del botnet Mirai, como Dark.IoT, y otro botnet apodado Katana por su autor, que tiene la capacidad de llevar a cabo ataques DDoS utilizando protocolos TCP y UDP.

> *«Se pudo identificar la dirección IP del atacante a través de la captura del tráfico de explotación, y se determinó que los ataques estaban ocurriendo en múltiples regiones, incluyendo América Central, América del Norte, Asia Oriental y Asia del*

> *Sur»,* señaló Cara Lin, investigadora de Fortinet FortiGuard Labs.

La falla, rastreada como CVE-2023-28771 (puntuación CVSS: 9.8), es una vulnerabilidad de inyección de comandos que afecta a varios modelos de firewall y que podría permitir a un actor no autorizado ejecutar código arbitrario enviando un paquete especialmente diseñado al dispositivo objetivo.

El mes pasado, la Fundación Shadowserver advirtió que la vulnerabilidad estaba siendo *«activamente explotada para construir un botnet similar a Mirai»*, al menos desde el 26 de mayo de 2023, lo que indica cómo está aumentando el abuso de servidores que ejecutan software sin parches.

Los más recientes descubrimientos de Fortinet sugieren que diversas entidades están aprovechando de manera oportunista la debilidad para vulnerar sistemas susceptibles y agruparlos en una botnet capaz de lanzar ataques DDoS contra otros objetivos.

Esta situación incluye variantes del botnet Mirai, como Dark.IoT, y otra botnet denominada Katana por su autor, la cual cuenta con capacidades para llevar a cabo ataques DDoS utilizando protocolos TCP y UDP.

> *«Es evidente que esta campaña utilizó múltiples servidores para llevar a cabo los ataques y se actualizó en tan solo unos días para maximizar la explotación de los dispositivos Zyxel»,* afirmó Lin.

La revelación se da en un contexto en el cual Cloudflare reportó un *«alarmante aumento en la sofisticación de los ataques DDoS»* durante el segundo trimestre de 2023, con actores de amenazas desarrollando formas novedosas de evadir la detección al *«imitar de manera hábil el comportamiento de un navegador»* y manteniendo bajas sus tasas de ataques por segundo.

A esto se suma la complejidad del uso de ataques de lavado de DNS para ocultar el tráfico malicioso a través de resolutores DNS recursivos de confianza y botnets de máquinas virtuales para llevar a cabo ataques DDoS de gran volumen.

> *«En un ataque de lavado de DNS, el actor de amenazas realiza consultas a subdominios de un dominio que es administrado por el servidor DNS de la víctima. El prefijo que define el subdominio es aleatorio y nunca se utiliza más de una o dos veces en este tipo de ataque»,* explicó Cloudflare.

> *«Debido al elemento de aleatoriedad, los servidores DNS recursivos nunca tendrán una respuesta almacenada en caché y deberán reenviar la consulta al servidor DNS autoritativo de la víctima. El servidor DNS autoritativo se ve entonces bombardeado por tantas consultas que no puede atender las consultas legítimas o incluso colapsa completamente».*

Otro factor relevante que contribuye al aumento de las ofensivas DDoS es la aparición de grupos hacktivistas pro-rusos como KillNet, REvil y Anonymous Sudan (también conocido como Storm-1359) que han dirigido sus ataques principalmente hacia objetivos en Estados Unidos y Europa. No existen evidencias que vinculen a REvil con el conocido grupo de ransomware.

> *«La continua creación y absorción de nuevos grupos por parte de KillNet es, al menos en parte, un intento de mantener la atención de los medios occidentales y mejorar el componente de influencia de sus operaciones. El enfoque del grupo ha estado consistentemente alineado con las prioridades geopolíticas establecidas y emergentes de Rusia»,* afirmó Mandiant en un nuevo análisis,

> *«La estructura, el liderazgo y las capacidades de KillNet han experimentado varios cambios observables en los últimos 18 meses, avanzando hacia un modelo que incluye nuevos grupos afiliados de mayor notoriedad, destinados a destacar sus marcas individuales además de la marca global de KillNet»,* agregó.