Los expertos en ciberseguridad han alertado sobre un incremento en actividades maliciosas que involucran la integración de routers D-Link vulnerables en dos redes de bots diferentes: una variante de Mirai llamada FICORA y una variante de Kaiten (también conocida como Tsunami) denominada CAPSAICIN.

> *«Estas botnets suelen propagarse explotando vulnerabilidades conocidas en routers D-Link, las cuales permiten a atacantes remotos ejecutar comandos maliciosos a través de la acción GetDeviceSettings en la interfaz HNAP (Protocolo de Administración de Red Doméstica)»,* explicó Vincent Li, investigador de Fortinet FortiGuard Labs, en un informe publicado el jueves.
>
> *«Esta falla en HNAP fue revelada por primera vez hace casi diez años y afecta a múltiples dispositivos, asociados a diversos números de CVE, como CVE-2015-2051, CVE-2019-10891, CVE-2022-37056 y CVE-2024-33112«.*

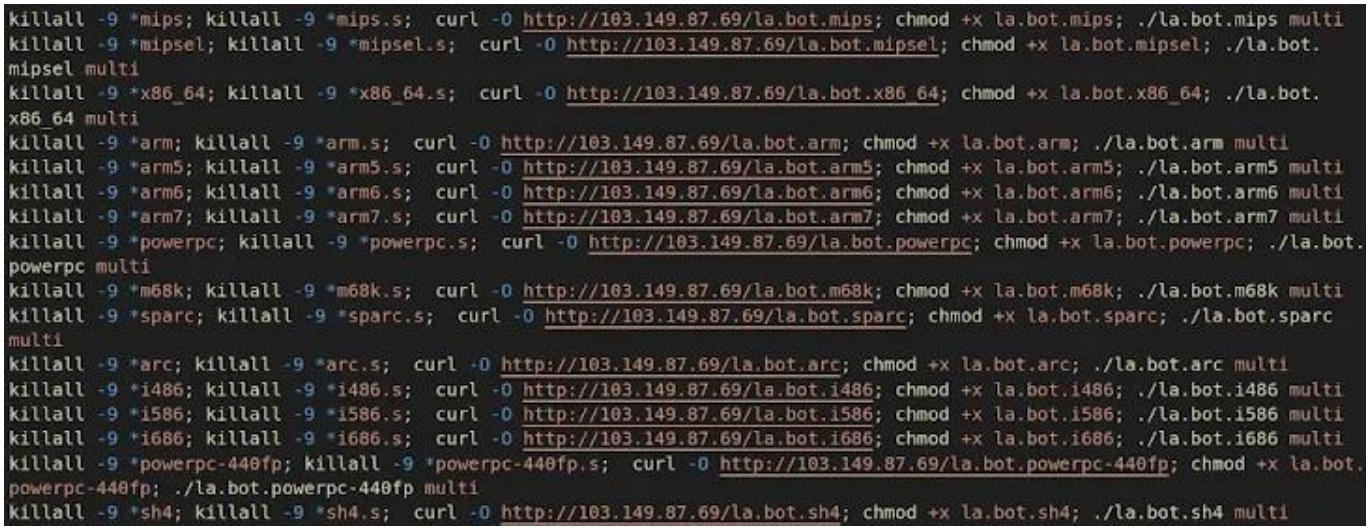
Según los datos de telemetría de la empresa de ciberseguridad, los ataques relacionados con FICORA se han dirigido a varios países en todo el mundo, mientras que los vinculados a CAPSAICIN se han concentrado principalmente en regiones de Asia Oriental, como Japón y Taiwán. Asimismo, se ha informado que la actividad de CAPSAICIN fue especialmente intensa entre el 21 y 22 de octubre de 2024.

Los ataques del botnet FICORA incluyen la ejecución de un script shell descargador («multi») desde un servidor remoto («103.149.87[.]69»), que posteriormente obtiene la carga útil principal para diferentes arquitecturas de Linux mediante los comandos wget, ftpget, curl y tftp.

El malware de esta botnet incorpora una funcionalidad para ataques de fuerza bruta, utilizando una lista predefinida de nombres de usuario y contraseñas. Además, la variante de Mirai está diseñada para llevar a cabo ataques distribuidos de denegación de servicio (DDoS) empleando protocolos UDP, TCP y DNS.

Por otro lado, el script descargador («bins.sh») de CAPSAICIN utiliza una dirección IP distinta («87.10.220[.]221») y sigue un enfoque similar para descargar el botnet en múltiples arquitecturas de Linux, optimizando su compatibilidad.

> *«El malware elimina procesos asociados a otras botnets para garantizar que es la única ejecutándose en el sistema comprometido. CAPSAICIN establece un canal de comunicación con su servidor de comando y control (C2), '192.110.247[.]46', y envía información sobre el sistema operativo del dispositivo víctima, así como el apodo asignado por el malware, al servidor C2»*, señaló Li.



A partir de ahí, CAPSAICIN espera órdenes adicionales que puede ejecutar en los dispositivos comprometidos, como las siguientes:

- GETIP: Obtener la dirección IP de una interfaz.
- CLEARHISTORY: Borrar el historial de comandos.
- FASTFLUX: Configurar un proxy hacia otro puerto o IP desde una interfaz.
- RNDNICK: Asignar un apodo aleatorio al dispositivo víctima.
- NICK: Modificar el apodo del dispositivo víctima.

- SERVER: Cambiar el servidor de comando y control.
- ENABLE: Activar el bot.
- KILL: Finalizar la sesión.
- GET: Descargar un archivo.
- VERSION: Solicitar la versión del dispositivo víctima.
- IRC: Enviar un mensaje al servidor.
- SH: Ejecutar comandos en el shell.
- ISH: Interactuar con el shell del dispositivo víctima.
- SHD: Ejecutar comandos en el shell ignorando señales.
- INSTALL: Descargar e instalar un binario en «/var/bin».
- BASH: Ejecutar comandos utilizando bash.
- BINUPDATE: Actualizar un binario en «/var/bin» mediante get.
- LOCKUP: Finalizar el backdoor de Telnet y ejecutar el malware.
- HELP: Mostrar información sobre las funciones del malware.
- STD: Ataque de inundación con cadenas aleatorias para un puerto y objetivo determinados.
- UNKNOWN: Ataque de inundación UDP con caracteres aleatorios para un puerto y objetivo específicos.
- HTTP: Ataque de inundación HTTP.
- HOLD: Ataque de inundación por conexiones TCP.
- JUNK: Ataque de inundación TCP.
- BLACKNURSE: Ataque basado en la inundación de paquetes ICMP.
- DNS: Ataque de amplificación DNS.
- KILLALL: Detener todos los ataques DDoS en curso.
- KILLMYEYEPEEUSINGHOIC: Terminar el malware original.

> *«A pesar de que estas vulnerabilidades fueron identificadas y corregidas hace casi una década, los ataques basados en ellas han seguido siendo frecuentes en todo el mundo. Es esencial que las organizaciones mantengan actualizados los núcleos de sus dispositivos y establezcan mecanismos robustos de monitoreo»,* concluyó Li.