Los enrutadores TP-Link Archer sin parches se han convertido en el objetivo de una nueva campaña de botnets denominada Ballista, según hallazgos recientes del equipo Cato CTRL.

> *«La botnet explota una vulnerabilidad de ejecución remota de código (RCE) en los enrutadores TP-Link Archer (CVE-2023-1389) para propagarse automáticamente por Internet»*, explicaron los investigadores de seguridad Ofek Vardi y Matan Mittelman en un informe técnico.

La vulnerabilidad CVE-2023-1389 es un fallo de alta gravedad que afecta a los enrutadores TP-Link Archer AX-21, permitiendo la inyección de comandos que pueden derivar en la ejecución remota de código.

Las primeras pruebas de explotación activa de esta falla datan de abril de 2023, cuando actores de amenazas no identificados la utilizaron para distribuir malware asociado a la botnet Mirai. Desde entonces, también ha sido aprovechada para propagar otras familias de malware, como Condi y AndroxGh0st.

El equipo de Cato CTRL detectó la campaña Ballista el 10 de enero de 2025, y el intento más reciente de explotación se registró el 17 de febrero.

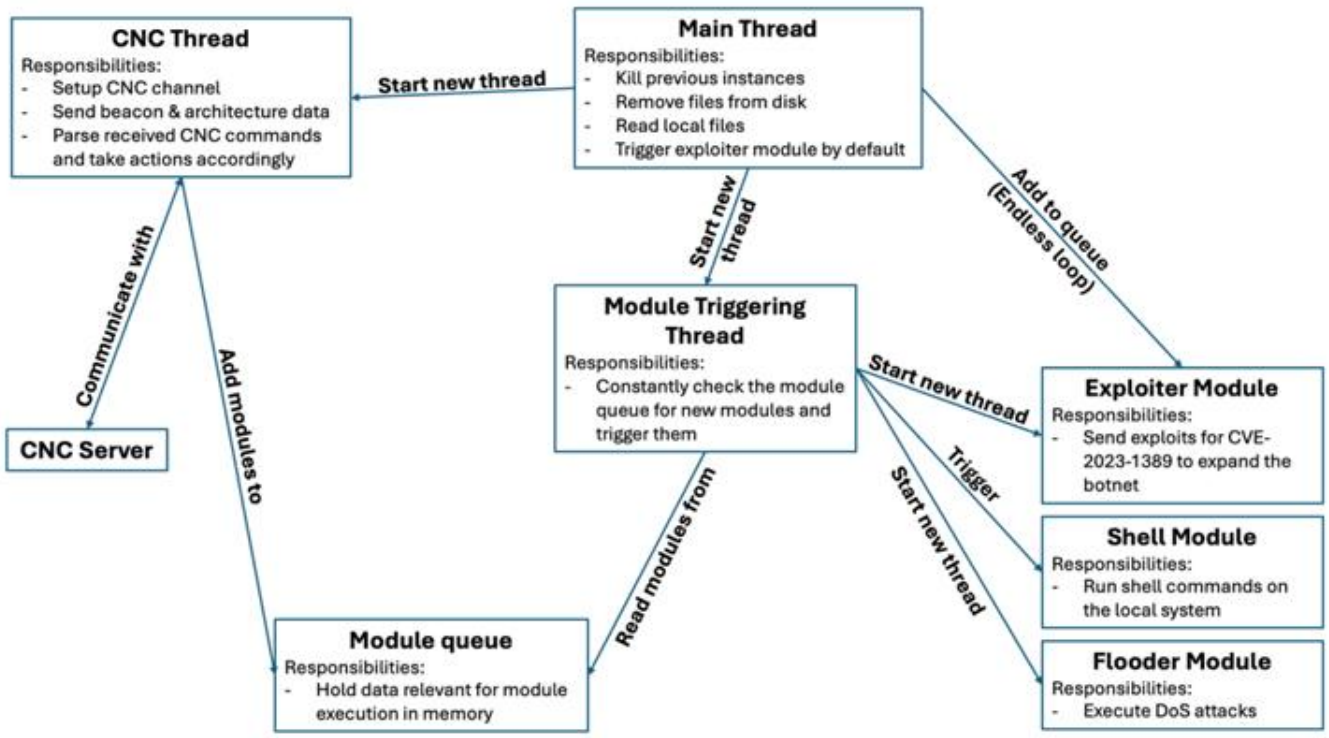
Mecanismo del ataque

El ataque utiliza un *dropper* de malware, un script de shell llamado `"dropbpb.sh"`, diseñado para descargar y ejecutar un binario en el sistema objetivo. Este binario es compatible con múltiples arquitecturas de sistema, incluyendo mips, mipsel, armv5l, armv7l y x86_64.

Una vez ejecutado, el malware establece un canal de comando y control (C2) cifrado en el puerto 82, permitiendo a los atacantes tomar el control del dispositivo.

> *«Esto permite ejecutar comandos en la terminal para realizar más ataques de*

> *ejecución remota de código (RCE) y de denegación de servicio (DoS). Además, el malware intenta acceder a archivos sensibles en el sistema local»,* explicaron los investigadores.



Comandos soportados

Entre los comandos que el malware puede ejecutar se incluyen:

- flooder: Inicia un ataque de inundación (*flood attack*).
- exploiter: Explota la vulnerabilidad CVE-2023-1389.
- start: Parámetro opcional para activar el módulo de explotación.
- close: Detiene el módulo activo.
- shell: Ejecuta comandos en la terminal de Linux.
- killall: Finaliza procesos en ejecución.

Además, el malware puede eliminar instancias previas de sí mismo y borrar sus huellas una vez que comienza su ejecución. También está diseñado para propagarse a otros enrutadores explotando la misma vulnerabilidad.

Origen del ataque y expansión

El uso de una dirección IP (2.237.57[.]70) en el servidor de C2 y la presencia de cadenas de texto en italiano dentro del código del malware sugieren que un actor de amenazas de origen italiano podría estar involucrado, según la empresa de ciberseguridad.

No obstante, el malware sigue en desarrollo, ya que la dirección IP utilizada previamente ya no está operativa y existe una nueva variante del *dropper* que emplea dominios de la red TOR en lugar de una dirección IP fija.

Un análisis en la plataforma de gestión de superficie de ataque Censys reveló que más de 6,000 dispositivos están infectados con Ballista, con infecciones concentradas en Brasil, Polonia, Reino Unido, Bulgaria y Turquía.

Las principales víctimas incluyen organizaciones de los sectores manufacturero, médico/salud, servicios y tecnología en países como Estados Unidos, Australia, China y México.

> *«Aunque esta muestra de malware comparte similitudes con otras botnets, sigue siendo distinta de botnets ampliamente utilizadas como Mirai y Mozi«,* señalaron los investigadores.