Una grave vulnerabilidad de seguridad, ya corregida, en el servidor Wazuh está siendo explotada por actores maliciosos para desplegar dos variantes distintas de la botnet Mirai y llevar a cabo ataques de denegación de servicio distribuido (DDoS).

Akamai, que identificó los primeros intentos de explotación a finales de marzo de 2025, indicó que la campaña maliciosa se dirige a la vulnerabilidad CVE-2025-24016 (puntaje CVSS: 9.9), una falla de deserialización insegura que permite la ejecución remota de código en servidores Wazuh.

El defecto, presente en todas las versiones del software del servidor desde la versión 4.4.0, fue corregido en febrero de 2025 con la publicación de la versión 4.9.1. Un exploit como prueba de concepto (PoC) fue revelado públicamente aproximadamente al mismo tiempo que se liberaron los parches.

El problema radica en la API de Wazuh, donde los parámetros del DistributedAPI son serializados en formato JSON y luego deserializados utilizando la función `"as_wazuh_object"` en el archivo `framework/wazuh/core/cluster/common.py`. Un atacante podría aprovechar esta debilidad inyectando cargas útiles JSON maliciosas para ejecutar código Python arbitrario de forma remota.

La empresa de infraestructura web señaló que detectó intentos de dos botnets distintas de explotar la CVE-2025-24016 tan solo semanas después de que se divulgara públicamente la vulnerabilidad y se hiciera disponible el PoC. Los ataques se registraron entre principios de marzo y mayo de 2025.

> *«Este es el ejemplo más reciente de cómo los operadores de botnets han reducido drásticamente el tiempo que tardan en explotar nuevas CVEs»,* afirmaron los investigadores Kyle Lefton y Daniel Messing en un informe.

En el primer caso, una explotación exitosa permite la ejecución de un script en shell que actúa como descargador del payload de Mirai desde un servidor externo («176.65.134[.]62»)

para diversas arquitecturas. Se ha determinado que las muestras del malware corresponden a variantes de LZRD Mirai, activas desde 2023.

Cabe señalar que LZRD también ha sido utilizado recientemente en ataques dirigidos a dispositivos IoT de GeoVision que han alcanzado su fin de vida (EoL). Sin embargo, Akamai declaró que no hay evidencia de que ambos grupos de actividad estén relacionados, ya que LZRD es empleado por numerosos operadores de botnets.

El análisis de la infraestructura relacionada con «176.65.134[.]62» y sus dominios asociados ha permitido identificar otras versiones de la botnet Mirai, incluidas variantes de LZRD denominadas «neon» y «vision«, así como una versión actualizada de V3G4.

Algunas de las otras vulnerabilidades aprovechadas por estas botnets incluyen fallas en Hadoop YARN, TP-Link Archer AX21 (CVE-2023-1389), y una vulnerabilidad de ejecución remota de código en routers ZTE ZXV10 H108L.

La segunda botnet que explota la CVE-2025-24016 emplea una estrategia similar, utilizando un script malicioso en shell para distribuir otra variante de Mirai, conocida como Resbot (también llamada *Resentual*).

> *«Una de las cosas interesantes que notamos sobre esta botnet fue el lenguaje asociado. Utilizaba una variedad de dominios con nomenclatura italiana para propagar el malware. Estas convenciones lingüísticas podrían sugerir una campaña dirigida a dispositivos operados por usuarios de habla italiana»*, indicaron los investigadores.

Además de propagarse mediante FTP por el puerto 21 y escaneos vía Telnet, esta botnet ha sido detectada explotando múltiples vulnerabilidades, como las que afectan a los routers Huawei HG532 (CVE-2017-17215), al SDK de Realtek (CVE-2014-8361), y al router TrueOnline ZyXEL P660HN-T v1 (CVE-2017-18368).

> *«La propagación de Mirai continúa sin mayores obstáculos, ya que es relativamente sencillo reutilizar su código fuente para crear nuevas botnets. Y muchos operadores obtienen resultados simplemente explotando vulnerabilidades recién publicadas»,* dijeron los investigadores.

La CVE-2025-24016 no es la única vulnerabilidad explotada por variantes de Mirai. En ataques recientes, los atacantes también han aprovechado la CVE-2024-3721, una vulnerabilidad de inyección de comandos de severidad media que afecta a los dispositivos DVR TBK DVR-4104 y DVR-4216, con el objetivo de integrarlos a la botnet.

Esta falla se utiliza para iniciar la ejecución de un script que descarga Mirai desde un servidor remoto («42.112.26[.]36») y lo ejecuta, aunque primero verifica si el sistema está operando dentro de una máquina virtual o en un entorno QEMU.

La empresa de ciberseguridad rusa Kaspersky señaló que las infecciones se concentran principalmente en China, India, Egipto, Ucrania, Rusia, Turquía y Brasil, y añadió que ha identificado más de 50,000 dispositivos DVR expuestos en internet.

> «La explotación de vulnerabilidades conocidas en dispositivos IoT y servidores sin parches, junto con el uso masivo de malware enfocado en sistemas Linux, provoca que haya miles de bots escaneando la red en busca de objetivos», explicó el investigador Anderson Leite.

La revelación coincide con datos que muestran que China, India, Taiwán, Singapur, Japón, Malasia, Hong Kong, Indonesia, Corea del Sur y Bangladés fueron los países más atacados en la región APAC durante el primer trimestre de 2025, según cifras compartidas por StormWall.

> *«Los ataques del tipo 'API flood' y 'carpet bombing' están creciendo más rápido que los ataques volumétricos tradicionales TCP/UDP, obligando a las empresas a*

> *adoptar defensas más inteligentes y adaptables. Al mismo tiempo, las tensiones geopolíticas están impulsando un aumento de ataques contra sistemas gubernamentales y Taiwán, reflejando una mayor actividad por parte de hacktivistas y actores estatales»,* señaló la compañía.

Esto también se produce tras una advertencia del Buró Federal de Investigaciones (FBI) de EE. UU., sobre la botnet BADBOX 2.0, que ha comprometido millones de dispositivos conectados a internet —en su mayoría fabricados en China— para convertirlos en proxies residenciales usados en actividades delictivas.

> *«Los ciberdelincuentes obtienen acceso no autorizado a redes domésticas al configurar los productos con software malicioso antes de que el usuario los adquiera, o infectando los dispositivos cuando estos descargan aplicaciones con puertas traseras, generalmente durante el proceso de instalación»,* explicó el FBI.
>
> *«La botnet BADBOX 2.0 incluye millones de dispositivos infectados y mantiene numerosos accesos ocultos a servicios de proxy que los actores criminales explotan vendiéndolos o facilitando su uso gratuito para diversas actividades ilegales.»*