Los operadores detrás del malware AndroxGh0st están aprovechando un mayor número de fallos de seguridad en diversas aplicaciones expuestas a internet y, al mismo tiempo, están desplegando el malware Mozi en forma de botnet.

> *«Este botnet emplea métodos de ejecución remota de código y técnicas de robo de credenciales para mantener un acceso persistente, utilizando vulnerabilidades no parcheadas para infiltrarse en infraestructuras críticas»*, explicó CloudSEK en un informe reciente.

AndroxGh0st es una herramienta de ataque en la nube basada en Python, reconocida por su enfoque en aplicaciones Laravel con el fin de obtener datos sensibles de servicios como Amazon Web Services (AWS), SendGrid y Twilio.

Activo desde al menos 2022, este malware ha utilizado anteriormente vulnerabilidades en el servidor web Apache (CVE-2021-41773), el framework Laravel (CVE-2018-15133) y PHPUnit (CVE-2017-9841) para acceder inicialmente, elevar privilegios y establecer un control persistente en sistemas comprometidos.

En marzo, agencias de ciberseguridad e inteligencia de EE. UU. revelaron que los atacantes están usando AndroxGh0st para crear un botnet con el objetivo de *«identificar y explotar víctimas dentro de redes específicas».*

El análisis más reciente de CloudSEK muestra una ampliación estratégica en los objetivos del malware, ahora aprovechando diversas vulnerabilidades para obtener acceso inicial:

- CVE-2014-2120 (CVSS: 4.3) – Vulnerabilidad de XSS en la página de inicio de sesión de Cisco ASA WebVPN
- CVE-2018-10561 (CVSS: 9.8) – Vulnerabilidad de omisión de autenticación en Dasan GPON
- CVE-2018-10562 (CVSS: 9.8) – Vulnerabilidad de inyección de comandos en Dasan GPON

- CVE-2021-26086 (CVSS: 5.3) – Vulnerabilidad de recorrido de rutas en Atlassian Jira
- CVE-2021-41277 (CVSS: 7.5) – Vulnerabilidad de inclusión de archivos locales en mapas GeoJSON de Metabase
- CVE-2022-1040 (CVSS: 9.8) – Vulnerabilidad de omisión de autenticación en el firewall Sophos
- CVE-2022-21587 (CVSS: 9.8) – Vulnerabilidad de carga de archivos arbitraria sin autenticación en Oracle E-Business Suite (EBS)
- CVE-2023-1389 (CVSS: 8.8) – Vulnerabilidad de inyección de comandos en el firmware TP-Link Archer AX21
- CVE-2024-4577 (CVSS: 9.8) – Vulnerabilidad de inyección de argumentos en CGI de PHP
- CVE-2024-36401 (CVSS: 9.8) – Vulnerabilidad de ejecución de código remoto en GeoServer

> *«El botnet prueba nombres de usuario administrativos comunes y sigue un patrón de contraseña consistente. La URL redirige a /wp-admin/, el panel de administración backend de sitios WordPress. Si la autenticación es exitosa, obtiene acceso a configuraciones y controles clave del sitio web»,* mencionó la compañía.

Los ataques también están explotando fallos de ejecución de comandos no autenticados en dispositivos Netgear DGN y routers Dasan GPON para descargar un archivo llamado «Mozi.m» desde distintos servidores externos («200.124.241[.]140» y «117.215.206[.]216»).

Mozi es otro botnet ampliamente conocido, con un historial de comprometer dispositivos IoT para integrarlos en una red maliciosa y llevar a cabo ataques de denegación de servicio distribuido (DDoS).

Aunque los creadores del malware fueron arrestados por las autoridades chinas en septiembre de 2021, no se observó una caída significativa en la actividad de Mozi hasta agosto de 2023, cuando partes desconocidas emitieron un comando de desconexión para terminar con el malware. Se cree que la actualización para desmantelar la botnet podría haber sido distribuida tanto por sus creadores como por las autoridades chinas.

La incorporación de Mozi por parte de AndroxGh0st ha despertado la posibilidad de una alianza operativa, permitiéndole extenderse a un número de dispositivos sin precedentes.

> *«AndroxGh0st no solo colabora con Mozi, sino que también integra sus funcionalidades específicas (como los mecanismos de infección y propagación en dispositivos IoT) en su conjunto operativo estándar»,* señaló CloudSEK.
>
> *«Esto implica que AndroxGh0st ha ampliado su alcance, aprovechando el poder de propagación de Mozi para infectar más dispositivos IoT, utilizando las cargas útiles de Mozi para cumplir objetivos que, de otro modo, requerirían rutinas de infección independientes».*
>
> *«Si ambas botnets están usando la misma infraestructura de comando, sugiere un alto grado de integración operativa, lo que podría significar que tanto AndroxGh0st como Mozi están controladas por el mismo grupo cibercriminal. Esta infraestructura compartida permitiría una administración centralizada de una gama más amplia de*

> *dispositivos, mejorando tanto la eficacia como la eficiencia de sus operaciones conjuntas de botnets.»*