Una botnet basada en Linux llamada Enemybot, amplió sus capacidades para incluir vulnerabilidades de seguridad recientemente reveladas en su arsenal para apuntar a servidores web, dispositivos Android y sistemas de administración de contenido (CMS).

> *«El malware está adoptando rápidamente vulnerabilidades de un día como parte de sus capacidades de explotación. Se están apuntando a servicios como VMware Workspace ONE, Adobe ColdFusion, WordPress, PHP Scriptcase y más, así como a dispositivos IoT y Android»,* dijo AT&T Alien Labs.

Revelado por primera vez por Securonix en marzo y luego por Fortinet, Enemybot fue vinculado a un actor de amenazas rastreado como Keksec (también conocido como Kek Security, Necro y FreakOut), con ataques tempranos dirigidos a enrutadores de Seowon Intech, D-Link e iRZ.

Enemybot, que es capaz de realizar ataques DDoS, tiene su origen en varias otras botnets como Mirai, Qbot, Zbot, Gafgyt y LolFMe. Un análisis de última variante revela que se compone de cuatro componentes distintos:

- Un módulo de Python para descargar dependencias y compilar el malware para diferentes arquitecturas de sistemas operativos
- La sección central de botnets
- Un segmento de ofuscación diseñado para codificar y decodificar las cadenas del malware
- Una funcionalidad de comando y control para recibir comandos de ataque y obtener cargas útiles adicionales

> *«En caso de que un dispositivo Android esté conectado a través de USB, o un emulador de Android ejecutándose en la máquina, EnemyBot intentará infectarlo ejecutando un comando de shell»*, dijeron los investigadores, señalando una nueva función «adb_infect».

ADB se refiere a Android Debug Bridge, una utilidad de línea de comandos utilizada para comunicarse con un dispositivo Android.

También se incorpora una nueva función de escáner que está diseñada para buscar direcciones IP aleatorias asociadas con activos públicos en busca de posibles vulnerabilidades, al mismo tiempo que tiene en cuenta nuevos errores a los pocos días de su divulgación pública.

Además, de las vulnerabilidades de Log4Shell que salieron a la luz en diciembre de 2021, esto incluye fallas recientemente parcheadas en los routers Razer Sila (sin CVE), VMware Workspace ONE Access (CVE-2022-22954) y F5 BIG-IP (CVE-2022-1388) así como debilidades en complementos de WordPress o Video Synchro PDF.

Otras deficiencias de seguridad armadas son las siguientes:

- CVE-2022-22947 (puntaje CVSS: 10): Una vulnerabilidad de inyección de código en Spring Cloud Gateway
- CVE-2021-4039 (puntaje CVSS: 9.8): Una vulnerabilidad de inyección de comandos en la interfaz web de Zyxel
- CVE-2022-25075 (puntaje CVSS:9.8): Una vulnerabilidad de inyección de comando en el enrutador inalámbrico TOTOLink A3000RU
- CVE-2021-36356 (puntaje CVSS: 9.8): Una vulnerabilidad de escalada de privilegios y ejecución de comandos en Kramer VIAWare
- CVE-2020-7961 (puntaje CVSS: 9.8): Una vulnerabilidad de ejecución remota de código en Liferay Portal

Además, el código fuente de la botnet se compartió en GitHub, lo que lo hace ampliamente

disponible para otros actores de amenazas.

«No asumo ninguna responsabilidad por los daños causados por este programa. Esto se publica bajo licencia Apache y también se considera arte», dice el archivo Leeme del proyecto.

> *«Enemybot de Keksec parece estar comenzando a propagarse, sin embargo, debido a las rápidas actualizaciones de los autores, esta botnet tiene el potencial de convertirse en una gran amenaza para los dispositivos IoT y los servidores web»,* dijeron los investigadores.

> *«Esto indica que el grupo Keksec cuenta con buenos recursos y que ha desarrollado el malware para aprovechar las vulnerabilidades antes de que se parcheen, aumentando así la velocidad y la escala a la que se puede propagar».*