Investigadores de ciberseguridad han *descubierto* una nueva versión de la botnet Kimwolf/AISURU para dispositivos Android e Internet de las Cosas (IoT), que incorpora mejoras significativas orientadas a aumentar su resistencia operativa y potenciar su capacidad para ejecutar ataques de denegación de servicio distribuido (DDoS).

La nueva variante, identificada como Kimwolf v7, fue detectada por *Palo Alto Networks Unit 42* en febrero de 2026.

«Kimwolf v7 incorpora un mecanismo de inundación DDoS basado en HTTP/2 que genera huellas digitales completas de navegadores», señalaron los investigadores Asher Davila, Chris Navarrete y Doel Santos. *«Esto dificulta diferenciar el tráfico malicioso del tráfico legítimo generado por usuarios reales.»*

La botnet también busca fortalecer su infraestructura de comando y control (C2) frente a intentos de desmantelamiento mediante un sistema escalonado que utiliza Ethereum Name Service (ENS) para obtener direcciones C2, un servicio oculto Tor .onion integrado en el malware y un proxy local encargado de enrutar comunicaciones entre la red convencional y Tor. Al mismo tiempo, elimina por completo las capacidades de escaneo, explotación y fuerza bruta presentes en versiones anteriores.

La desaparición de los módulos de escaneo y explotación sugiere que los operadores han separado el proceso de propagación del malware principal, delegando el acceso inicial a cargadores externos, mientras que el binario de Kimwolf se concentra exclusivamente en ataques DDoS y funciones de retransmisión de tráfico.

Evolución de Kimwolf

Desde agosto de 2025, Kimwolf se ha caracterizado por atacar dispositivos Android TV, mientras que su contraparte para Linux, AISURU, se enfoca principalmente en dispositivos IoT basados en este sistema operativo. La actividad de la botnet se remonta al menos a mediados de 2024.

Habitualmente, la amenaza aprovecha servicios de proxy residenciales para localizar dispositivos Android TV que mantienen habilitado Android Debug Bridge (ADB) en el puerto 5555 dentro de redes locales. Una vez identificados, instala malware capaz de lanzar ataques DDoS y actuar como intermediario para redirigir tráfico malicioso.

Tras ejecutarse, el malware intenta pasar desapercibido adoptando nombres similares a procesos legítimos del sistema Android, como «netd_service».

Entre las capacidades más destacadas observadas en esta versión se encuentran:

1. Ataques de inundación HTTP/2 avanzados que utilizan la biblioteca *nghttp2* y generan huellas digitales completas de navegador para imitar comportamientos legítimos tanto a nivel de protocolo como de encabezados.
2. Uso de servicios públicos Ethereum RPC para consultar registros ENS y resolver dinámicamente las direcciones de comando y control.
3. Mecanismo de respaldo para C2 mediante Tor, utilizando un servicio oculto *.onion* integrado directamente en el código malicioso.
4. Arquitectura de proxy local, que canaliza todo el tráfico de comando y control a través de la dirección 127.0.0.1:23075, independientemente de que el destino sea la red convencional o Tor.
5. Función de inundación UDP de alto rendimiento, optimizada específicamente para procesadores ARM presentes en dispositivos Android TV.
6. Simplificación de comandos DDoS, reduciendo los 43 métodos identificados en versiones anteriores a solo 15 métodos numerados.

Distribución mediante aplicaciones Android falsas

Los operadores de Kimwolf también han sido observados distribuyendo paquetes APK para Android que se hacen pasar por un servicio legítimo denominado SystemService. Estas aplicaciones buscan obtener privilegios de root y luego ejecutan una carga útil ELF integrada dentro del sistema.

Los investigadores identificaron ocho muestras de este tipo distribuidas entre octubre y diciembre de 2025.

«La muestra más antigua detectada, orientada a la arquitectura x86 y equipada con un exploit Dirty COW, indica que esta familia evolucionó desde técnicas tradicionales de explotación en Linux hacia el actual modelo de propagación basado en ADB para Android», explicó *Unit 42*. *«El cambio del nombre libn[redacted]kernel.so a la menos llamativa libdevice.so en noviembre de 2025, seguido de una reversión en diciembre, demuestra ajustes continuos en sus medidas de seguridad operativa.»*

Nuevas familias de botnets emergentes

La revelación coincide con la identificación reciente de varias *nuevas familias de malware tipo botnet*:

1. AryStinger
   Botnet que incorpora routers domésticos antiguos y vulnerables a una red utilizada para reconocimiento distribuido y servicios de proxy.
2. RustDuck
   Amenaza que compromete routers residenciales, cámaras IP, dispositivos Android y servidores mal protegidos para integrarlos en una infraestructura destinada a ataques DDoS.
3. NadMesh
   Plataforma automatizada que combina escaneo, explotación de vulnerabilidades y recolección de credenciales. Está diseñada para localizar instancias expuestas de Redis, Docker, MCP, Kubernetes, ComfyUI, Ollama, n8n, Open WebUI, Langflow y Gradio, además de desplegar puertas traseras SSH y obtener credenciales, variables de entorno, tokens de cuentas y configuraciones de AWS y Docker.
4. Tengu
   Malware IoT derivado de Mirai que emplea ataques de fuerza bruta mediante Telnet para comprometer dispositivos IoT. Una vez dentro, puede lanzar ataques DoS, recopilar información de red, establecer persistencia, exfiltrar datos del sistema,

ejecutar comandos, descargar cargas adicionales y convertir el dispositivo afectado en un proxy.

Recomendaciones de seguridad

«Kimwolf v7 representa una evolución especializada de una botnet que ya operaba a gran escala», indicó *Unit 42*. *«Las organizaciones deberían considerar los dispositivos Android TV como elementos no confiables y aislarlos de las redes corporativas. Deshabilitar ADB o limitar su uso exclusivamente a conexiones USB elimina el principal mecanismo de propagación de esta amenaza.»*

Medidas recomendadas

- Deshabilitar ADB en dispositivos Android TV cuando no sea necesario.
- Restringir el acceso ADB únicamente mediante conexión USB.
- Segmentar los dispositivos Android TV de las redes empresariales.
- Supervisar tráfico HTTP/2 inusual y conexiones hacia servicios Tor.
- Implementar monitoreo sobre dispositivos IoT para detectar actividad anómala.
- Mantener actualizados todos los dispositivos Android e IoT expuestos a la red.