GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

12 August 2026

Advisory 187: Kimwolf v7 Android and IoT Botnet Malware

Release Date: 11th August 2026
Impact: MEDIUM
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

Kimwolf v7 (also tracked as AISURU) is the latest version of an Android and IoT botnet family, discovered by Palo Alto Networks Unit 42 in February 2026. It has been active since mid-2024, originally targeting Linux IoT devices under the AISURU name before adding Android TV boxes as a second propagation target from August 2025.
Version 7 adds an HTTP/2-based DDoS flood that constructs complete browser fingerprints, making malicious traffic harder to distinguish from legitimate browsing, along with a more resilient command-and-control (C2) design using Ethereum Name Service (ENS) domain lookups, a hard-coded Tor hidden service, and a local proxy for routing between clearnet and Tor. This advisory is issued for general threat awareness rather than a specific vulnerability, as no CVE has been assigned.

What are the systems affected?

Affected systems are consumer and small-business devices with weak or default remote-access configurations, most commonly reached over residential broadband connections rather than government or enterprise networks directly.

Android TV boxes with Android Debug Bridge (ADB) enabled on port 5555 – (Affected)
Linux-based IoT devices (via the AISURU codebase) – (Affected)
Devices reached via residential proxy services abused by the operators – (At risk)

Households and businesses using inexpensive or unbranded Android TV boxes are at particular risk, as these commonly ship with ADB enabled and are widely used across Vanuatu households connected via Vodafone Vanuatu and Digicel Vanuatu residential broadband.

What does this mean?

Kimwolf v7 operates as a self-propagating DDoS-for-hire botnet: once a device is compromised, it is silently conscripted to attack third parties and relay malicious traffic, without necessarily disrupting the device owner's own use of it - meaning infections can go unnoticed for long periods.

Step 1 - Initial Access
The operators use residential proxy services and scanning (via an external loader, separate from the core Kimwolf payload) to locate Android TV boxes with ADB exposed on port 5555, or vulnerable Linux IoT devices, and deliver a malicious APK or ELF payload.

Step 2 - Concealment
Distributed APK packages masquerade as a system service (e.g. "SystemService"), probe for root access, and execute a bundled payload that disguises itself as a legitimate Android process such as "netd_service" to avoid detection.

Step 3 - Resilient Command and Control
The bot resolves its C2 address via Ethereum Name Service (ENS) lookups against legitimate public Ethereum RPC services, with a hard-coded Tor .onion address as a fallback, routed through a local proxy on the device. This tiered design makes the botnet significantly harder to disrupt through conventional domain or IP takedowns.

Step 4 - DDoS and Proxy Abuse
On command, the bot launches HTTP/2 floods with forged browser fingerprints and high-performance UDP floods against third-party targets, and can also relay other malicious traffic through the infected device, exposing the device owner's IP address and broadband connection to abuse-related complaints or blocklisting.

Mitigation process

CERTVU recommends the following:

1. **Disable ADB and Segment Android TV Devices**

On Android TV boxes, disable ADB entirely, or restrict it to USB-only access rather than leaving it reachable over the network on port 5555 - this removes the primary propagation vector for this botnet. Treat Android TV boxes and similar cheap streaming devices as untrusted, and place them on a separate network segment or guest Wi-Fi rather than the same network as business systems or sensitive data.

Unit 42: Kimwolf v7 - An Evolution of the Kimwolf Botnet

2. **ISP-Level Detection and Subscriber Notification**

ISPs in Vanuatu are encouraged to monitor for anomalous outbound DDoS-pattern traffic (high-volume HTTP/2 or UDP floods) from residential connections, and to notify affected subscribers so infected Android TV boxes and IoT devices can be remediated, consistent with CERTVU's existing ISP sinkhole and malware feed reporting process.

Reference

1. https://thehackernews.com/2026/08/kimwolf-v7-android-botnet-makes-http2.html
2. https://unit42.paloaltonetworks.com/kimwolf-v7-botnet-malware/

.