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

5 August 2026

Advisory 182: BADBOX 2.0 Botnet Infections Detected on Consumer Internet-Connected Devices in Vanuatu

Release Date: 20th July 2026
Impact: HIGH
TLP: CLEAR

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

This alert is relevant to Internet Service Providers, Organizations and System/Network administrators operating networks in Vanuatu. This alert is intended to be understood by technical users and systems administrators. A separate non-technical public notification has been issued alongside this advisory.

What is it?

A botnet built from compromised Internet of Things (IoT) and Android-based consumer devices, used to provide criminal residential proxy services.

BADBOX 2.0 infects devices in two ways: some are shipped with backdoor malware already installed before purchase, and others are infected during set-up when the user is prompted to install applications from unofficial marketplaces. Once connected to a home or office network, the device joins the botnet and is enrolled into residential proxy services that allow criminals to route their traffic through the victim's internet connection.

The botnet succeeded the original BADBOX campaign, identified in 2023 and disrupted in 2024, and is assessed to consist of millions of devices worldwide. It has been the subject of international alerts and law enforcement action since 2023, summarised below.

CERTVU notes that no new international alert on BADBOX 2.0 has been issued since the FBI Public Service Announcement, which remains the current standing warning. Despite the threat having been publicly known for more than a year, infected devices remain active in Vanuatu.

What are the systems affected?

Generic Android-based television streaming boxes and set-top boxes, digital projectors with built-in Android, aftermarket vehicle infotainment systems, digital picture frames, and other low-cost IoT devices from unrecognised brands that are not Google Play Protect certified. Most affected devices are manufactured in China.

Devices sold through official channels by recognised manufacturers, and Android devices that are Play Protect certified, are substantially less likely to be affected. This is not a software flaw in a specific product version, so no patch resolves it. The device itself is the compromised component.

What does this mean?

Confirmed local infections:

CERTVU analysis of Shadowserver Foundation sinkhole HTTP data for Vanuatu, covering a single day on 20 July 2026, identified 27 BADBOX 2.0 events classified at critical severity, from 8 distinct source addresses within Vanuatu comprising 4 IPv4 and 4 IPv6 addresses. The affected addresses were distributed across three separate networks serving Vanuatu, indicating that the problem is not confined to the subscribers of any single provider. In the interest of responsible disclosure, CERTVU does not identify individual operators or subscribers in this advisory; affected providers are notified directly and confidentially.

The recorded user-agent strings confirm the device category directly, identifying Android 10 devices with build names including android_tv_box, TV BOX and MBOX. These are generic television streaming boxes rather than branded consumer electronics, most likely purchased through informal retail channels or online marketplaces.

Detections were observed on both urban and non-urban connectivity, which is significant for Vanuatu. Services that extend internet access to islands and communities outside the main centres reach areas where technical support is limited and where low-cost imported streaming devices are common, so infections there are less likely to be detected or remediated locally.

The consequences for an affected subscriber are practical. Their IP address may be used to commit offences, which can result in that address being blacklisted by online services, in the subscriber being unable to reach banking or government services, or in the subscriber being associated with criminal activity they did not commit. The compromised device also sits inside the local network alongside phones, laptops and business systems.

The same sinkhole data for 20 July 2026 also recorded bondat, avalanche-andromeda, expiro and m0yv activity in Vanuatu. These are addressed separately through CERTVU's routine sinkhole reporting to Internet Service Providers.

Indicators of Compromise

The following indicators were observed in Vanuatu sinkhole data:

• **Command-and-control domains:** tinder.holadns.com, 10.17ce.holadns.com, ycxrl.com, goologer.com

• **HTTP request patterns:** POST /terminal/client/register, POST /terminal/client/eventinfo, and GET /CLogin?key= followed by a long base64-encoded value

• **User-agent strings:**

- Dalvik/2.1.0 (Linux; U; Android 10; android_tv_box Build/QP1A.191105.004)
- Dalvik/2.1.0 (Linux; U; Android 10.0; TV BOX Build/QP1A.191105.004)
- Dalvik/2.1.0 (Linux; U; Android 10; MBOX Build/QP1A.191105.004)
- Lingjiang

• **Behavioral indicators identified by the FBI:**

- The device requires applications to be installed from unofficial marketplaces
- Set-up instructions require Google Play Protect to be disabled
- The device is advertised as unlocked or as providing free access to paid streaming content
- The device is from an unrecognized brand and is not Play Protect certified
- Unexplained or unusual internet traffic from the device

Mitigation process

CERTVU recommends the following:

• **Notify affected subscribers:** Internet Service Providers should request their own BADBOX 2.0 detection data from Shadowserver. CERTVU provides this data confidentially to each operator for its own network only.

• **Audit and remove affected devices:**

- Audit networks for generic Android streaming boxes and similar IoT devices, including those connected to guest and staff wireless networks.
- Where an affected device is identified, disconnect it from the network. Because the malware may reside in the device firmware, a factory reset may not remove it, and CERTVU recommends the device be permanently removed from service rather than reconnected.
- Segregate IoT and entertainment devices onto a separate or guest network so they cannot reach business systems, file shares or management interfaces.

• **Procurement and user guidance:**

- Purchase devices only from recognized manufacturers and authorized retailers, and avoid devices advertised as offering free paid content.

- Do not install applications from unofficial marketplaces, and never disable Google Play Protect at the instruction of a seller or set-up screen.
- Keep operating systems, applications and firmware up to date on all devices that receive vendor support.

• **Report:** Report suspected infections to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.fbi.gov/investigate/cyber/alerts/2025/home-internet-connected-devices-facilitate-criminal-activity
2. https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/
3. https://www.shadowserver.org/