TransilienceAI

BADBOX 3.0 CTV ad-fraud/proxy operation

Threat Report · TLP:CLEAR

campaign · BADBOX 3.0

25 Nov 2026

Version 5 · 6 sources

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF . . . 3

- Bottom line . . . 3
- For the board . . . 3
- Are you exposed? . . . 3
- What to do . . . 3

TIMELINE . . . 4

WHAT THEY DID . . . 4

WHOM THEY TARGET . . . 4

MALWARE AND TOOLS . . . 5

ATTRIBUTION . . . 5

DISRUPTION, ADVISORIES AND LAW ENFORCEMENT . . . 5

ATT&CK; TECHNIQUES . . . 5

INDICATORS . . . 6

NOT KNOWN YET . . . 6

SOURCES . . . 6

ABOUT THIS REPORT . . . 6

Brief

ACTIVE
“BADBOX 3.0, an operation that turned inexpensive streaming boxes into hidden video ad players and residential proxies.” [1]

Bottom line

BADBOX 3.0 rebuilt on uncertified AOSP devices to run hidden video-ad fraud and rent residential IPs, peaking at ~40 billion bid requests/day; operators host modules in public repos and mirror delivery to resist takedowns. Check low-cost uncertified Android TV boxes, remove infections, and block known C2s and repos now. [1,2,3]

For the board

A large ad-fraud botnet (BADBOX 3.0) abused uncertified Android TV boxes to fake ad impressions and rent residential IPs; inventory and isolate such devices, block delivery infrastructure, and monitor for proxy/CTV anomalies now.

Are you exposed?

Targets	How to check
low-cost, uncertified Android Open Source Project TV/Android devices, off-brand AOSP boxes. [1,2,3]	Inspect inventories for off-brand AOSP Android TV boxes lacking Play Protect certification; watch hidden ad playback, unexpected bandwidth.

What to do

1. **Inventory and isolate uncertified Android TV/AOSP devices immediately.** [1,3]
   BADBOX 3.0 runs on low-cost, uncertified AOSP devices and abuses them for ad fraud and proxying.
2. **Block and hunt for the C2 domains, repo mirrors and GitHub proxy used to deliver modules.** [3,4]
   Operators host fraud modules on public repositories, mirrored CDN and a self-hosted GitHub proxy to resist takedowns.
3. **Check network egress for residential proxy-style traffic and abnormal bid-request patterns.** [1,2]
   Infected boxes enroll in 11 residential proxy networks and generated ~40 billion bid requests/day, skewing CTV traffic.

Also reported as Badbox · BADBOX 2.0 · PXYEDGE · XCPE.

Timeline

Date	Kind	What happened
2026-11-19 published	DISCLOSURE	Public disclosure by Satori (Human Security) of BADBOX 3.0 and its behavior. [1] *"BADBOX 3.0, an operation that turned inexpensive streaming boxes into hidden video ad players and residential proxies."* [1]
2026-11-19 published	DISCLOSURE	HUMAN reported peak volume (~40 billion bid requests/day) and CTV traffic share. [1] *"At its peak, the campaign generated roughly 40 billion bid requests per day, accounting for more than 4% of connected TV (CTV) traffic observed by HUMAN's platform."* [1]
2026-11-21 published	DISCLOSURE	BleepingComputer published Satori findings on BADBOX 3.0 returning with record 40 billion daily ad requests. [2] *"At its height, BADBOX 3.0 accounted for roughly 40 billion bid requests a day and more than 4% of all CTV traffic observed by the Human Defense Platform."* [2]
2026-11-23 published	RESPONSE	Human Security said it disrupted portions of BADBOX 3.0 and participated in Google-led disruption of XCPE. [4] *"Human said it was part of an operation to disrupt XCPE, a botnet linked to Badbot 3.0 by shared command-and-control (C2) domains."* [4]
2026-11-25 published	DISCOVERY	Kaspersky analysis places BADBOX among preinstalled firmware threats and notes capability to run proxies and ad fraud. [6] *"Other families of preinstalled malware exist, although they're less common than Triada and Keenadu. They include Dwphon, Vo1d, and BADBOX."* [6]

What they did

Count	Detail
40 billion bid requests/day	Botnet generated roughly 40 billion fraudulent advertising bid requests per day at peak. [1] *"At its peak, the campaign generated roughly 40 billion bid requests per day, accounting for more than 4% of connected TV (CTV) traffic observed by HUMAN's platform."* [1]
11 networks	Modules enrolled devices in 11 residential proxy networks and rented out home internet. [1] *"Proxy modules enrolled compromised devices in 11 residential proxy networks without the owners' consent."* [1]
—	Operators host module catalog on public repositories, mirrored across platforms and CDN. [3] *"The modules sit on public code repositories, with backups on a second code platform, an operator-controlled file server and, for some, a CDN mirror."* [3]

Whom they target

- Low-cost, off-brand Android Open Source Project (AOSP) streaming TV boxes and some cheap phones/tablets. [2]
  "The modus operandi remains the same: infecting cheap phones, tablets, and streaming TV boxes running the Android Open Source Project (AOSP) with malware that performs ad fraud and traffic proxying." [2]
- Global CTV ecosystem and advertisers (skewed ad metrics), plus owners of infected devices. [1]
  "For ad buyers, the case exposes a basic verification problem: neither a familiar app name nor a household IP address proves an ad reached a viewer." [1]

Malware and tools

- Fraud/ad modules that render hidden video ads and SSAI requests. [2]
  "The malware performs ad fraud by playing video ads in hidden windows while impersonating legitimate streaming apps to make the requests appear legitimate." [2]
- Open public code repositories, mirrored CDN, operator-controlled file server, self-hosted GitHub proxy. [3]
  "The operators also run their own GitHub proxy, so blocking the repositories at the network level does not stop the downloads." [3]

Attribution

- Satori links components to Chinese electronics manufacturer TXCZ through domains and device checks. [1]
  "Satori linked the module catalog to Chinese electronics manufacturer TXCZ through command infrastructure, manufacturer-specific device checks, and a company domain that served ad configurations." [1]
- Researchers assess PXYEDGE is IpMoYu, rebranded residential proxy from BADBOX 2.0 operators. [1]
  "Satori assessed that one network, PXYEDGE, succeeded IpMoYu, which researchers exposed during BADBOX 2.0." [1]

Disruption, advisories and law enforcement

- Google-led disruption took down XCPE domains and some C2 infrastructure; Human Security disrupted portions of BADBOX 3.0. [5]
  "Portions of BadBox 3.0, the cybersecurity firm says, were operated via command-and-control (C&C) domains that were disrupted when Google took down XCPE, a botnet of over 1.3 million Android set-top boxes." [5]
- One malware repository was taken down; Human now filters associated fraudulent advertising traffic. [2]
  "one of the malware repositories was taken down, while HUMAN says its systems now filter fraudulent advertising traffic associated with BADBOX 3.0." [2]

ATT&CK techniques

ID	Technique	Mapped from
T1105	**Ingress Tool Transfer** NAMED BY THE SOURCE	*"Compromised devices contacted a command-and-control server to learn which modules to load."* [1]
T1071.001	**Web Protocols** NAMED BY THE SOURCE	*"Proxy modules enrolled compromised devices in 11 residential proxy networks without the owners' consent."* [1]

T1104	**Multi-Stage Channels** NAMED BY THE SOURCE	*“Operators maintained those modules in public code repositories and kept backup copies elsewhere, so taking down one repository did not necessarily cut off delivery.”* [1]

Indicators

None published in the sources.

Not known yet

- exact number of infected BADBOX 3.0 devices
- full list of IOCs and C2 domains in machine-readable form
- definitive attribution beyond repository and device checks

Sources

#	Outlet	Article	Copy
1	**GBHackers** 19 Nov 2026	Hackers Hide Malware Inside Cheap TV Boxes to Steal Home Internet Bandwidth and Generate Fake Ads	archived copy
2	**BleepingComputer (Bluesky)** 21 Nov 2026	BADBOX 3.0 botnet returns with record-breaking 40 billion daily ad requests	archived copy
3	**Help Net Security** 23 Nov 2026	Infected TV boxes in BADBOX 3.0 rent out their owners' home internet - Help Net Security	archived copy
4	**Infosecurity Magazine** 23 Nov 2026	Badbox Returns to Spread Ad Fraud and Proxyjacking Payloads	archived copy
5	**SecurityWeek** 23 Nov 2026	BadBox 3.0 Ad Fraud Operation Generating 40 Billion Daily Bid Requests Disrupted	archived copy
6	**Kaspersky Securelist** 25 Nov 2026	Preinstalled Android malware: what businesses need to know	archived copy

About this report

Compiled by Transilience Newsroom from 6 public sources. Every quotation is checked against the article it cites; 4 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 5, written 25 November 2026, 09:17 UTC (threat-report-2026-09-25b). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/threat/mwnjzose6rcu