IMPORTANT CYBERSECURITY NEWS: BADBOX 2.0 BOTNET DISRUPTED AGAIN AFTER INFECTING OVER 1 MILLION ANDROID DEVICES

Vairav Cyber Security News Report

Date: March 06, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

In collaboration with Google, Trend Micro, and Shadowserver, HUMAN Security's Satori Threat Intelligence team has successfully disrupted the BADBOX 2.0 botnet, which has infected over 1 million Android devices worldwide. The malware, embedded in 24 deceptive applications, primarily targeted low-cost Android-based devices such as TV streaming boxes, tablets, smart TVs, and smartphones. These malicious apps either came pre-installed by manufacturers or were downloaded by unsuspecting users. BADBOX malware converted infected devices into residential proxies, facilitated ad fraud, redirected users to fraudulent websites, and enabled credential stuffing attacks. Despite previous takedown attempts, BADBOX operations have been resilient, with its largest impact seen in Brazil, the U.S., Mexico, and Argentina.

INCIDENT ANALYSIS

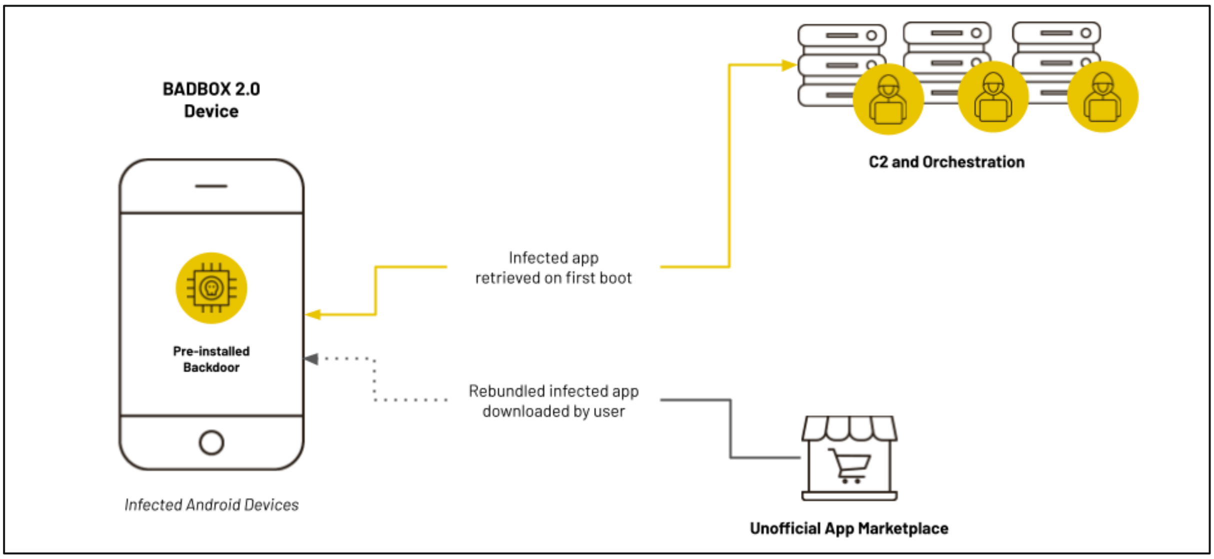


Figure 1: Backdoor delivering mechanism for BadBox 2.0

Malware Deployment & Functionality

The attack involves a backdoor named BB2DOOR, which is embedded in malicious apps disguised as legitimate software. These “evil twin” apps mimic legitimate ones, deceiving users and generating fraudulent ad traffic by requesting billions of fake ad bids weekly. The backdoor exploits a malicious libanl.so library, which downloads additional payloads to maintain contact with command-and-control (C2) servers. It exploited infected devices to:

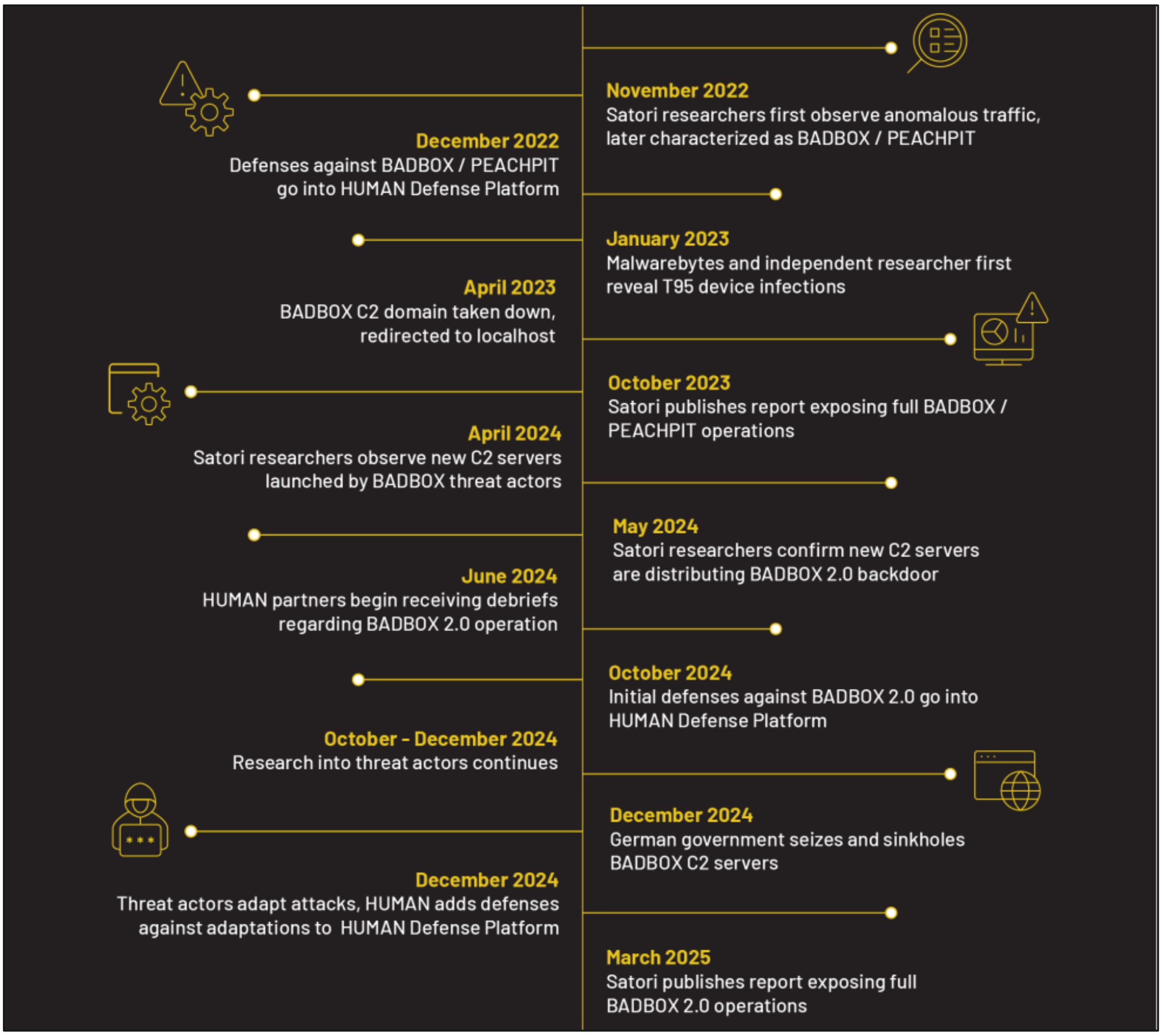
- Act as residential proxies for cybercriminals.

- Generate fraudulent ad impressions and traffic redirection schemes.
- Conduct credential stuffing and fake account creation attacks.

Threat Actor Groups Involved

Researchers identified four interconnected cybercrime groups responsible for deploying BADBOX 2.0: **SalesTracker Group, MoYu Group, Lemon Group,** and **LongTV**.

Attack Timeline



November 2022
Satori researchers first observe anomalous traffic, later characterized as BADBOX / PEACHPIT

December 2022
Defenses against BADBOX / PEACHPIT go into HUMAN Defense Platform

January 2023
Malwarebytes and independent researcher first reveal T95 device infections

April 2023
BADBOX C2 domain taken down, redirected to localhost

October 2023
Satori publishes report exposing full BADBOX / PEACHPIT operations

April 2024
Satori researchers observe new C2 servers launched by BADBOX threat actors

May 2024
Satori researchers confirm new C2 servers are distributing BADBOX 2.0 backdoor

June 2024
HUMAN partners begin receiving debriefs regarding BADBOX 2.0 operation

October 2024
Initial defenses against BADBOX 2.0 go into HUMAN Defense Platform

October - December 2024
Research into threat actors continues

December 2024
German government seizes and sinkholes BADBOX C2 servers

December 2024
Threat actors adapt attacks, HUMAN adds defenses against adaptations to HUMAN Defense Platform

March 2025
Satori publishes report exposing full BADBOX 2.0 operations

Figure 2: Attack timeline of BadBox/BadBox 2.0

Affected Devices & Global Reach

BADBOX 2.0 primarily targets uncertified Android Open-Source Project (AOSP) devices produced in China and distributed globally. These devices lack Google Play Protect certification, making them vulnerable to backdoor infections. It originally disrupted in

December 2024 by German authorities, quickly resurfaced and grew to over 1 million infections across 222 countries. Brazil (37.6%), United States (18.2%), Mexico (6.3%), and Argentina (5.3%) saw the highest infection rates. The malware affects smart TVs and TV boxes, digital projectors, tablets, and infotainment systems. The device models known to be impacted by the BadBox malware are provided below:

Device Models			
TV98	X96Q_Max_P	Q96L2	X96Q2
X96mini	S168	ums512_1h10_Natv	X96_S400
X96mini_RP	TX3mini	HY-001	MX10PRO
X96mini_Plus1	LongTV_GN7501E	Xtv77	NETBOX_B68
X96Q_PR01	AV-M9	ADT-3	OCBN
X96MATE_PLUS	KM1	X96Q_PRO	Projector_T6P
X96QPRO-TM	sp7731e_1h10_native	M8SPROW	TV008
X96Mini_5G	Q96MAX	Orbsmart_TR43	Z6
TVBOX	Smart	KM9PRO	A15
Transpeed	KM7	iSinbox	I96
SMART_TV	Fujicom-SmartTV	MXQ9PRO	MBOX
X96Q	isinbox	Mbox	R11
GameBox	KM6	X96Max_Plus2	TV007
Q9 Stick	SP7731E	H6	X88
TV98	X96Q_Max_P	Q96L2	X96Q2
X98K	TXCZ		

The BADBOX 2.0 takedown marks a significant step in combating Android malware. However, its resilience highlights the need for continuous security vigilance. While Google and cybersecurity firms are actively dismantling this botnet, users and enterprises must take proactive measures to secure their devices and networks against future threats.

RECOMMENDED ACTIONS

- Users should check if their Android device is Google Play Protect certified via Play Store settings.
- Ensure real-time threat scanning is active to block malicious app installations.
- Only download apps from official sources like Google Play to reduce infection risk.
- Unusual network traffic or high resource consumption may indicate an infection.
- Keep firmware and applications updated to mitigate potential vulnerabilities.
- Organizations using Android-based devices should implement network monitoring and mobile threat detection (MTD) solutions to detect anomalous behavior.

RESOURCES

https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/

https://cybersecuritynews.com/badbox-from-google-play-hacked-50000-android-devices/

https://www.bleepingcomputer.com/news/security/badbox-malware-disrupted-on-500k-infected-android-devices/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com