Supply-Chain Malware at Scale: Mapping BadBox Exposure in Bhutan and South Asia

Pratima Pradhan, BtCIRT GovTech Agency

BADBOX starts with consumer devices

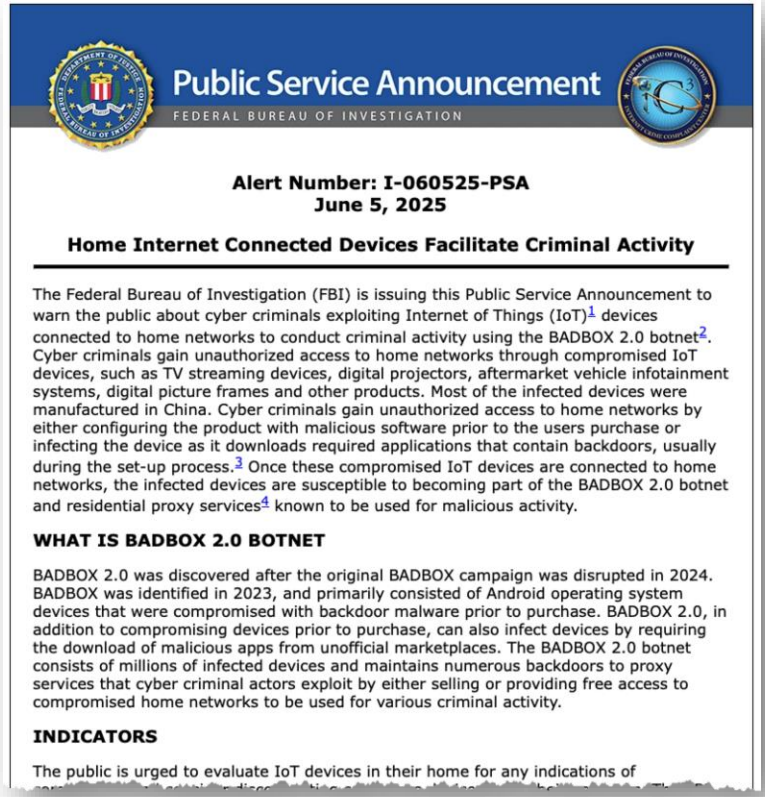
Visual generated with Microsoft Copilot. Device categories based on FBI IC3, BitSight and HUMAN Security reporting.

What is the threat of BADBOX

BadBox is not simply malware. It

is a:

- Supply-chain security issue
- Consumer IoT problem
- ISP abuse issue
- Residential proxy network
- Ad fraud infrastructure
- National cyber resilience challenge



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-060525-PSA
June 5, 2025

Home Internet Connected Devices Facilitate Criminal Activity

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement to warn the public about cyber criminals exploiting Internet of Things (IoT)[1] devices connected to home networks to conduct criminal activity using the BADBOX 2.0 botnet[2]. Cyber criminals gain unauthorized access to home networks through compromised IoT devices, such as TV streaming devices, digital projectors, aftermarket vehicle infotainment systems, digital picture frames and other products. Most of the infected devices were manufactured in China. Cyber criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to the users purchase or infecting the device as it downloads required applications that contain backdoors, usually during the set-up process.[3] Once these compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of the BADBOX 2.0 botnet and residential proxy services[4] known to be used for malicious activity.

WHAT IS BADBOX 2.0 BOTNET

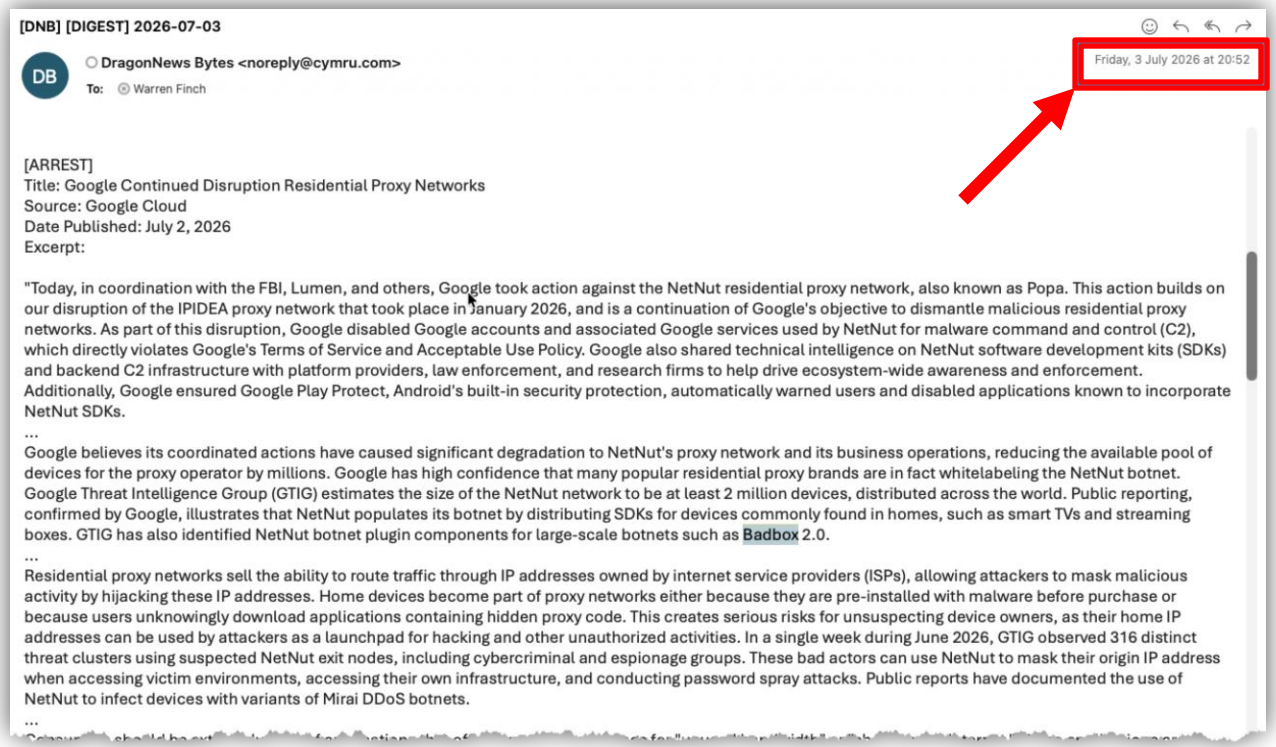
BADBOX 2.0 was discovered after the original BADBOX campaign was disrupted in 2024. BADBOX was identified in 2023, and primarily consisted of Android operating system devices that were compromised with backdoor malware prior to purchase. BADBOX 2.0, in addition to compromising devices prior to purchase, can also infect devices by requiring the download of malicious apps from unofficial marketplaces. The BADBOX 2.0 botnet consists of millions of infected devices and maintains numerous backdoors to proxy services that cyber criminal actors exploit by either selling or providing free access to compromised home networks to be used for various criminal activity.

INDICATORS

The public is urged to evaluate IoT devices in their home for any indications of

https://www.ic3.gov/PSA/2025/PSA250605

What is the threat of BADBOX



[DNB] [DIGEST] 2026-07-03

DB

DragonNews Bytes <noreply@cymru.com>

To: Warren Finch

Friday, 3 July 2026 at 20:52

[ARREST]
Title: Google Continued Disruption Residential Proxy Networks
Source: Google Cloud
Date Published: July 2, 2026
Excerpt:

"Today, in coordination with the FBI, Lumen, and others, Google took action against the NetNut residential proxy network, also known as Popa. This action builds on our disruption of the IPIDEA proxy network that took place in January 2026, and is a continuation of Google's objective to dismantle malicious residential proxy networks. As part of this disruption, Google disabled Google accounts and associated Google services used by NetNut for malware command and control (C2), which directly violates Google's Terms of Service and Acceptable Use Policy. Google also shared technical intelligence on NetNut software development kits (SDKs) and backend C2 infrastructure with platform providers, law enforcement, and research firms to help drive ecosystem-wide awareness and enforcement. Additionally, Google ensured Google Play Protect, Android's built-in security protection, automatically warned users and disabled applications known to incorporate NetNut SDKs.

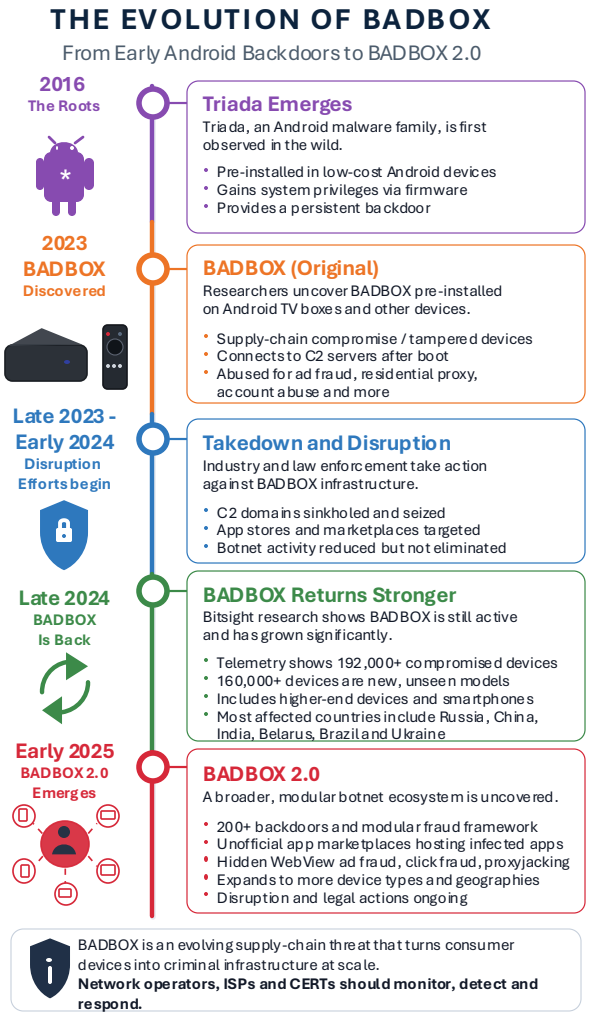
...

Google believes its coordinated actions have caused significant degradation to NetNut's proxy network and its business operations, reducing the available pool of devices for the proxy operator by millions. Google has high confidence that many popular residential proxy brands are in fact whitelabeling the NetNut botnet. Google Threat Intelligence Group (GTIG) estimates the size of the NetNut network to be at least 2 million devices, distributed across the world. Public reporting, confirmed by Google, illustrates that NetNut populates its botnet by distributing SDKs for devices commonly found in homes, such as smart TVs and streaming boxes. GTIG has also identified NetNut botnet plugin components for large-scale botnets such as Badbox 2.0.

...

Residential proxy networks sell the ability to route traffic through IP addresses owned by internet service providers (ISPs), allowing attackers to mask malicious activity by hijacking these IP addresses. Home devices become part of proxy networks either because they are pre-installed with malware before purchase or because users unknowingly download applications containing hidden proxy code. This creates serious risks for unsuspecting device owners, as their home IP addresses can be used by attackers as a launchpad for hacking and other unauthorized activities. In a single week during June 2026, GTIG observed 316 distinct threat clusters using suspected NetNut exit nodes, including cybercriminal and espionage groups. These bad actors can use NetNut to mask their origin IP address when accessing victim environments, accessing their own infrastructure, and conducting password spray attacks. Public reports have documented the use of NetNut to infect devices with variants of Mirai DDoS botnets.

...



Evolution of Badbox

- Original BadBox (2023)
- BadBox 2.0
- Global growth
- Supply-chain compromise model

https://www.bitsight.com/blog/badbox-botnet-back

Infection Vectors

Vector 1
Preinstalled Supply-Chain Malware

Compromise before use

Malware or loader capability may be present before the customer receives the device.

Operator framing:

- Customer may not have installed anything.
- Factory reset may not be sufficient.
- Supply chain is part of the risk.

Vector 2
First-Boot Network Infection

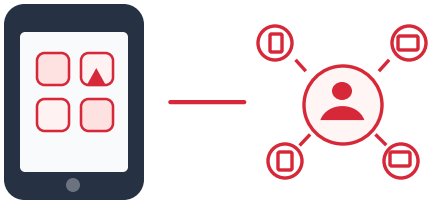
Compromise during setup

A device may contact setup infrastructure and retrieve a backdoor, loader or unauthorised app.

Operator framing:

- Look for repeated suspicious DNS or HTTP(S).
- Correlate DHCP, NAT and flow records.
- Do not treat one connection as proof.

Vector 3
Malicious Apps (Third-Party)



Compromise through apps

Malicious or rebundled applications may be installed from unofficial app marketplaces.

Operator framing:

- Customer education matters.
- Avoid unofficial app marketplaces.
- Use passive enrichment and CERT channels.

Use passive telemetry, customer context, CERT coordination and source-backed indicators before making an assessment.

Why South Asia Should Care?

Common conditions

- Large imports of low-cost Android devices
- Informal electronics markets
- Limited certification verification
- Increasing smart-TV adoption

Potentially affected devices include:

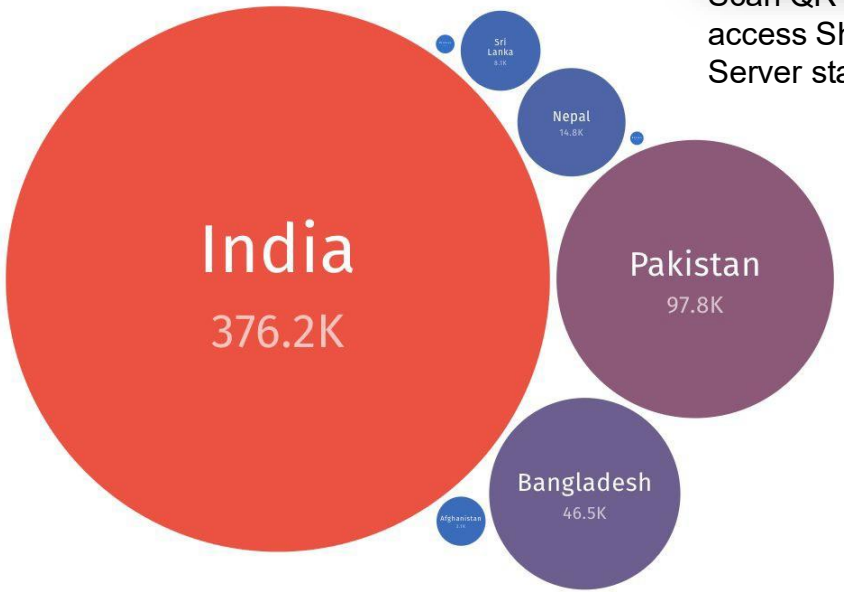
- Android TV boxes
- Streaming devices
- Smart TVs
- Projectors
- Tablets

Badbox infection (Data from: 1st May 2026 - 1st June 2026) -ShadowServer Foundation

SHADOWSERVER

Country	Counted IP addresses
India	376,152
Pakistan	97,786
Bangladesh	46,472
Nepal	14,847
Sri Lanka	8,095
Afghanistan	3,052
Maldives	441
Bhutan	228

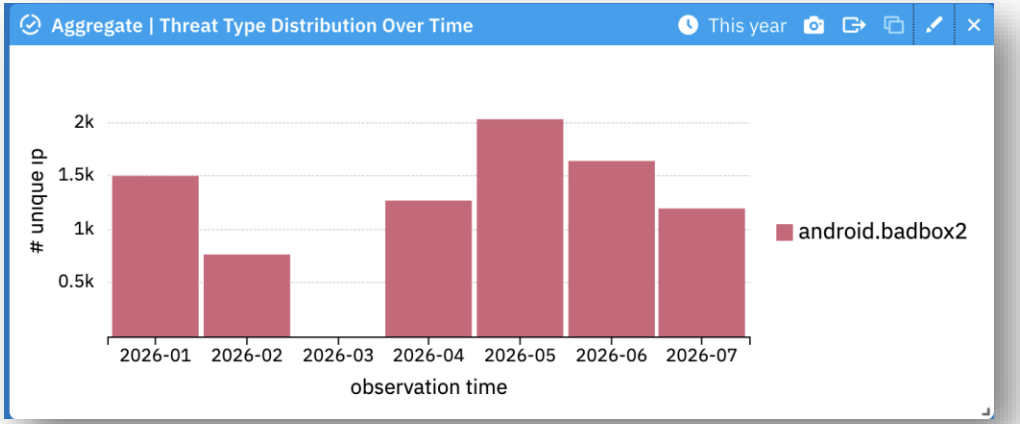
Scan QR Code to access Shadow Server stats



Bhutan Case Study

Security monitoring shows that every internet provider in Bhutan has devices affected by the Badbox malware. This affects at least 2% of each provider's network.

Actions: Little has been done so far. This is still a work in progress.



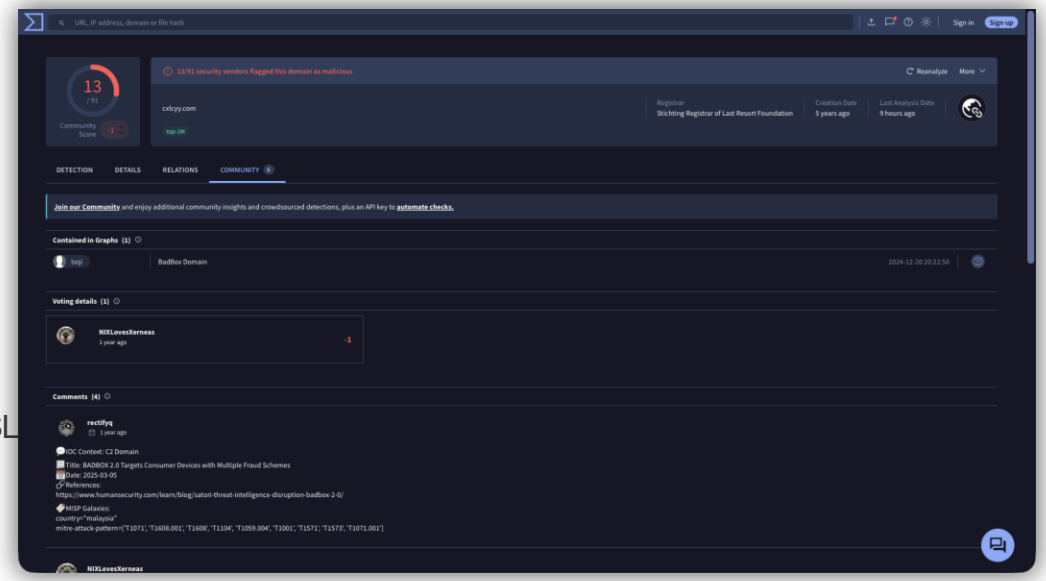
Technical Indicators and TTPs

C2 Infrastructure: Known command-and-control domain names include coslogdydy[.]in, yydsmr[.]com, logcer.com

Bitsight's analysis found dozens of related domains (e.g. cxlcyy.com, goo loger.com, yydsmr[.]com, etc.) that share naming patterns or SSL certificates

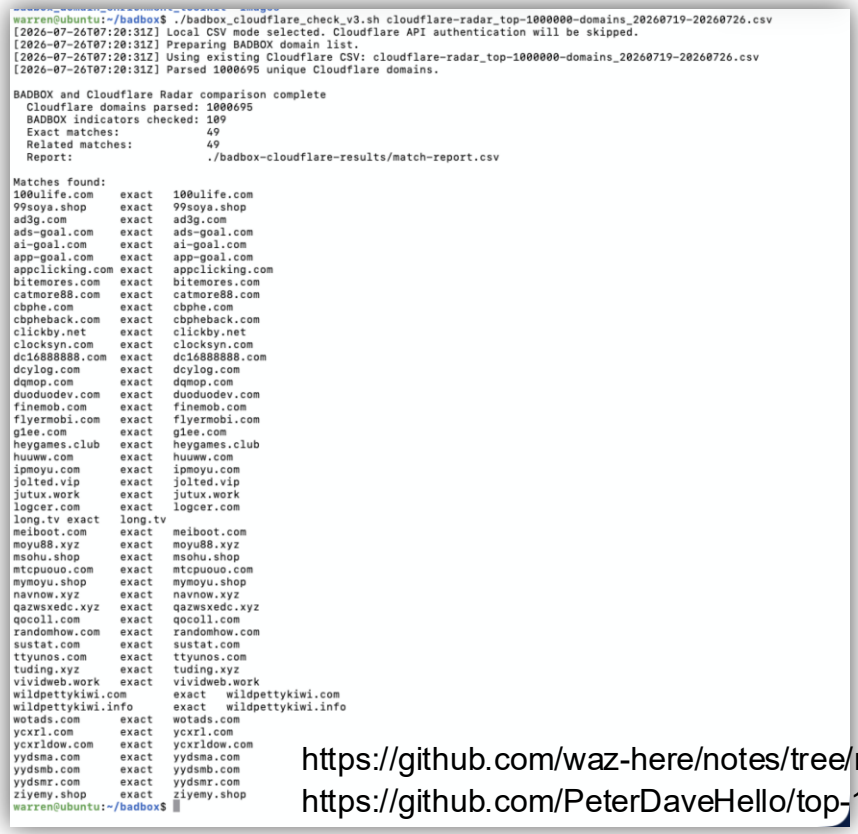
These domains often serve backdoor payloads (e.g. /uploads/apk/...) or respond with encrypted commands

Monitoring DNS queries for these domains (or their SSL fingerprints) is a key technical control.



https://www.virustotal.com/gui/domain/cxlcyy.com

Technical Indicators and TTPs



```
warren@ubuntu:~/badbox$ ./badbox_cloudflare_check_v3.sh cloudflare-radar_top-1000000-domains_20260719-20260726.csv
[2026-07-26T07:20:31Z] Local CSV mode selected. Cloudflare API authentication will be skipped.
[2026-07-26T07:20:31Z] Preparing BADBOX domain list.
[2026-07-26T07:20:31Z] Using existing Cloudflare CSV: cloudflare-radar_top-1000000-domains_20260719-20260726.csv
[2026-07-26T07:20:31Z] Parsed 1000695 unique Cloudflare domains.

BADBOX and Cloudflare Radar comparison complete
  Cloudflare domains parsed: 1000695
  BADBOX indicators checked: 109
  Exact matches:             49
  Related matches:           49
  Report:                    ./badbox-cloudflare-results/match-report.csv

Matches found:
100ulife.com      exact   100ulife.com
99soya.shop       exact   99soya.shop
ad3g.com          exact   ad3g.com
ads-goal.com      exact   ads-goal.com
ai-goal.com       exact   ai-goal.com
app-goal.com      exact   app-goal.com
appclicking.com   exact   appclicking.com
bitemores.com     exact   bitemores.com
catmore88.com     exact   catmore88.com
cbphe.com         exact   cbphe.com
cbpheback.com     exact   cbpheback.com
clickby.net       exact   clickby.net
clocksyn.com      exact   clocksyn.com
dc16888888.com    exact   dc16888888.com
dcylog.com        exact   dcylog.com
dqmop.com         exact   dqmop.com
duoduodev.com     exact   duoduodev.com
finemob.com       exact   finemob.com
flyermobi.com     exact   flyermobi.com
g1ee.com          exact   glee.com
heygames.club     exact   heygames.club
huuww.com         exact   huuww.com
ipmoyu.com        exact   ipmoyu.com
jolted.vip        exact   jolted.vip
jutux.work        exact   jutux.work
logcer.com        exact   logcer.com
long.tv exact     long.tv
meiboot.com       exact   meiboot.com
moyu88.xyz        exact   moyu88.xyz
msohu.shop        exact   msohu.shop
mtcpuouo.com      exact   mtcpuouo.com
mymoyu.shop       exact   mymoyu.shop
navnow.xyz        exact   navnow.xyz
qazwsxedc.xyz     exact   qazwsxedc.xyz
qocoll.com        exact   qocoll.com
randomhow.com     exact   randomhow.com
sustat.com        exact   sustat.com
ttyunos.com       exact   ttyunos.com
tuding.xyz        exact   tuding.xyz
vividweb.work     exact   vividweb.work
wildpettykiwi.com         exact   wildpettykiwi.com
wildpettykiwi.info        exact   wildpettykiwi.info
wotads.com        exact   wotads.com
ycxrl.com         exact   ycxrl.com
ycxrldow.com      exact   ycxrldow.com
yydsma.com        exact   yydsma.com
yydsmb.com        exact   yydsmb.com
yydsmr.com        exact   yydsmr.com
ziyemy.shop       exact   ziyemy.shop
warren@ubuntu:~/badbox$
```

badbox_cloudflare_check_v3.sh

Compares the current Cloudflare Radar Top 1 Million domain dataset against the list of known BADBOX 2.0 domains.

The script can either:

- download the latest Cloudflare dataset using the Radar API, or
- analyse an existing CSV that has already been downloaded.
- No DNS lookups are performed and no Internet scanning occurs.

https://github.com/waz-here/notes/tree/main/malware_research/badbox
https://github.com/PeterDaveHello/top-1m-domains

Technical Indicators and TTPs

BADBOX Domain Enrichment Report

Generated: 2026-07-26T14:12:03.607478Z

Provider names are heuristic inferences based on RDAP organisation and network names. They are not authoritative attribution.

Summary

Domain	A / AAAA	ASN	Country	Provider inference	VT malicious	URLhaus	ThreatFox	CT records
100ulife.com	178.162.202.96, 178.162.202.97, 46.165.199.7, 46.165.199.9, …	28753, 60781, 6939	64.62.128.0/17, DE, NL	Leaseweb	11	no_results	no_result	43
99soya.shop	178.162.202.96, 178.162.202.97, 46.165.199.7, 46.165.199.9, …	28753, 60781, 6939	64.62.128.0/17, DE, NL	Leaseweb	15	no_results	no_result	
ad3g.com	178.162.202.96, 178.162.202.97, 46.165.199.7, 46.165.199.9, …	28753, 60781	DE, NL	Leaseweb	10	no_results	no_result	
ads-goal.com	178.162.202.96, 178.162.202.97, 46.165.199.7, 46.165.199.9, …	28753, 60781, 6939	64.62.128.0/17, DE, NL	Leaseweb	10	no_results	no_result	

run_badbox_enrichment.sh

```
warren@ubuntu:~/badbox/badbox_domain_enrichment_toolkit$ ls
badbox-enrichment-results  readme.md          run_badbox_enrichment.sh
enrich_badbox_domains.py   requirements.txt
warren@ubuntu:~/badbox/badbox_domain_enrichment_toolkit$ ./run_badbox_enrichment.sh ../badbox-cloudflare-results/exact-matche
s.txt --limit 4 --workers 1
[2026-07-26T14:09:10Z] Installing or updating Python dependencies.
[2026-07-26T14:09:11Z] Starting BADBOX domain enrichment.
Loaded 4 domains from ../badbox-cloudflare-results/exact-matches.txt
[1/4] 100ulife.com: A=10 AAAA=0 VT=found URLhaus=queried ThreatFox=queried
[2/4] 99soya.shop: A=10 AAAA=0 VT=found URLhaus=queried ThreatFox=queried
[3/4] ad3g.com: A=10 AAAA=0 VT=found URLhaus=queried ThreatFox=queried
[4/4] ads-goal.com: A=10 AAAA=0 VT=found URLhaus=queried ThreatFox=queried

Results written to: badbox-enrichment-results
  CSV:      badbox-enrichment-results/enriched_domains.csv
  JSON:     badbox-enrichment-results/enriched_domains.json
  Markdown: badbox-enrichment-results/enriched_domains.md
warren@ubuntu:~/badbox/badbox_domain_enrichment_toolkit$ tree
-bash: tree: command not found
warren@ubuntu:~/badbox/badbox_domain_enrichment_toolkit$ tree
.
├── badbox-enrichment-results
│   ├── enriched_domains.csv
│   ├── enriched_domains.json
│   ├── enriched_domains.md
│   ├── errors.log
│   ├── raw
│   │   ├── 100ulife.com.json
│   │   ├── 99soya.shop.json
│   │   ├── ad3g.com.json
│   │   └── ads-goal.com.json
│   └── run_metadata.json
├── enrich_badbox_domains.py
├── readme.md
├── requirements.txt
└── run_badbox_enrichment.sh

3 directories, 13 files
warren@ubuntu:~/badbox/badbox_domain_enrichment_toolkit$
```

https://github.com/waz-here/notes/tree/main/malware_research/badbox

Technical Indicators and TTPs

```
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ls
badbox-domains.txt   calculate-ipv6-stats.sh  extract-cctld.sh       generate-report.sh  resolve-domains-parallel.sh  team-cymru-asn.sh
badbox-resolved.csv  discover-subdomains.sh   extract-unique-ips.sh  readme.md           resolve-domains.sh           top-asns.sh
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ./resolve-domains.sh badbox-domains.txt
Creating: badbox-resolved.csv
[109/109] zxcvbnmasdfghjkl.xyz
Finished.
DNS records collected: 1015
Output: badbox-resolved.csv
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ./calculate-ipv6-stats.sh badbox-resolved.csv
IPv6 Summary
============

Input file: badbox-resolved.csv

Domains analysed: 109
Domains with IPv4: 109
Domains with IPv6: 1
IPv6 adoption rate: 0.92%

IPv4 records observed: 1014
IPv6 records observed: 1

Output written to: badbox-ipv6-summary.txt
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ./extract-unique-ips.sh badbox-resolved.csv
Input file: badbox-resolved.csv
Output file: badbox-ips.txt

Unique IP addresses: 23
IPv4 addresses: 23
IPv6 addresses: 0
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ./team-cymru-asn.sh badbox-ips.txt
Input file: badbox-ips.txt
Unique IP addresses: 23
Querying Team Cymru bulk IP-to-ASN service...

Output written to: badbox-asn.txt

First few results:
Bulk mode; whois.cymru.com [2026-07-26 16:25:04 +0000]
13335   | 104.21.19.212    | 104.21.16.0/20      | US | arin     | 2014-03-28 | CLOUDFLARENET - Cloudflare, Inc., US
13335   | 104.21.26.221    | 104.21.16.0/20      | US | arin     | 2014-03-28 | CLOUDFLARENET - Cloudflare, Inc., US
134963  | 170.33.12.185    | 170.33.12.0/24      | SG | apnic    | 1994-02-03 | ASEPL-AS-AP - Alibaba Cloud (Singapore) Private Limited, SG
63949   | 172.236.104.157  | 172.236.96.0/19     | US | arin     | 2013-03-15 | AKAMAI-LINODE-AP - Akamai Connected Cloud, SG
63949   | 172.236.104.43   | 172.236.96.0/19     | US | arin     | 2013-03-15 | AKAMAI-LINODE-AP - Akamai Connected Cloud, SG
63949   | 172.238.172.122  | 172.238.160.0/19    | US | arin     | 2013-03-15 | AKAMAI-LINODE-AP - Akamai Connected Cloud, SG
13335   | 172.67.139.118   | 172.67.128.0/20     | US | arin     | 2015-02-25 | CLOUDFLARENET - Cloudflare, Inc., US
13335   | 172.67.190.55    | 172.67.176.0/20     | US | arin     | 2015-02-25 | CLOUDFLARENET - Cloudflare, Inc., US
28753   | 178.162.202.96   | 178.162.192.0/18    | DE | ripencc  | 2010-02-05 | LEASEWEB-DE-FRA-10 - Leaseweb Deutschland GmbH, DE
warren@ubuntu:~/ccTLD-domain-analysis/scripts$
```

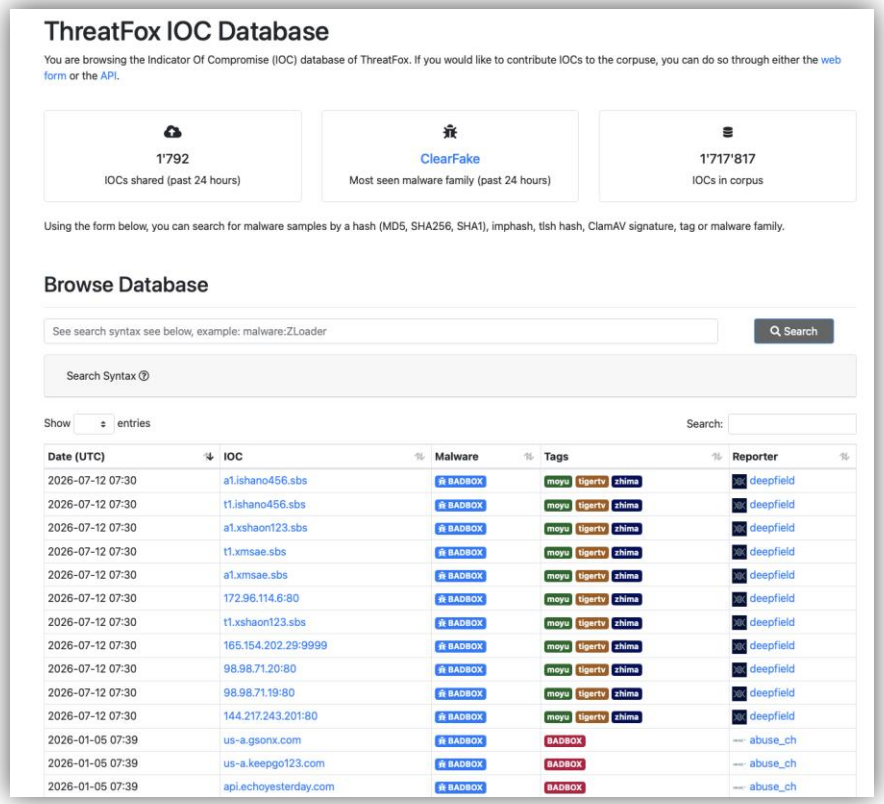
```
warren@ubuntu:~/ccTLD-domain-analysis/scripts$ ./top-asns.sh badbox-asn.txt
Top ASN report written to: badbox-top-asns.txt

Top 20 ASNs:

Count    ASN       Organisation
-----    ---       ------------
4        AS13335   CLOUDFLARENET - Cloudflare
4        AS28753   LEASEWEB-DE-FRA-10 - Leaseweb Deutschland GmbH
4        AS60781   LEASEWEB-NL-AMS-01 - LeaseWeb Netherlands B.V.
3        AS63949   AKAMAI-LINODE-AP - Akamai Connected Cloud
2        AS6939    HURRICANE - Hurricane Electric LLC
1        AS134963  ASEPL-AS-AP - Alibaba Cloud (Singapore) Private Limited
1        AS174     COGENT-174 - Cogent Communications
1        AS30058   FDCSERVERS - FDCservers.net
1        AS396982  GOOGLE-CLOUD-PLATFORM - Google LLC
1        AS6724    STRATO - Strato GmbH
1        ASError: no ASN or IP match on line 25.
warren@ubuntu:~/ccTLD-domain-analysis/scripts$
```

https://github.com/waz-here/ccTLD-domain-analysis/tree/main

Technical Indicators and TTPs



ThreatFox IOC Database

You are browsing the Indicator Of Compromise (IOC) database of ThreatFox. If you would like to contribute IOCs to the corpuse, you can do so through either the web form or the API.

1'792	ClearFake	1'717'817
IOCs shared (past 24 hours)	Most seen malware family (past 24 hours)	IOCs in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

Browse Database

See search syntax see below, example: malware:ZLoader — Search

Search Syntax

Show entries — Search:

Date (UTC)	IOC	Malware	Tags	Reporter
2026-07-12 07:30	a1.ishano456.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	t1.ishano456.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	a1.xshaon123.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	t1.xmsae.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	a1.xmsae.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	172.96.114.6:80	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	t1.xshaon123.sbs	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	165.154.202.29:9999	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	98.98.71.20:80	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	98.98.71.19:80	BADBOX	moyu tigertv zhima	deepfield
2026-07-12 07:30	144.217.243.201:80	BADBOX	moyu tigertv zhima	deepfield
2026-01-05 07:39	us-a.gsonx.com	BADBOX	BADBOX	abuse_ch
2026-01-05 07:39	us-a.keepgo123.com	BADBOX	BADBOX	abuse_ch
2026-01-05 07:39	api.echoyesterday.com	BADBOX	BADBOX	abuse_ch

https://threatfox.abuse.ch/browse.php?search=malware%3Abadbox

Technical Indicators and TTPs (cont)

Malicious APKs: The botnet uses specially crafted Android apps. Malwarebytes identified app packages (e.g. com.yandex[.]tv[.]home, com[.]instwall[.]launch , etc.) linked to BadBox .

Google/Trend Micro discovered “decoy twin” apps: benign app listings in Play versus identical malware outside

Malicious publishers include “Seekiny Studio” and others . Signature-based defenses can block known bad APKs.

Technical Indicators and TTPs (cont)

Traffic Patterns: Infected devices frequently make hidden HTTP(S) requests.
Researchers note
“hidden WebViews” loading hundreds of ad-heavy HTML5 game sites C2 check-ins use unique URI paths (e.g. /terminal/client/ , /ota/api/tasks/v2 with device-specific
query parameters)

Large spikes of DNS resolution (millions for yydsmr[.]com) indicate botnet scale Network

defenses can flag such abnormal volumes.

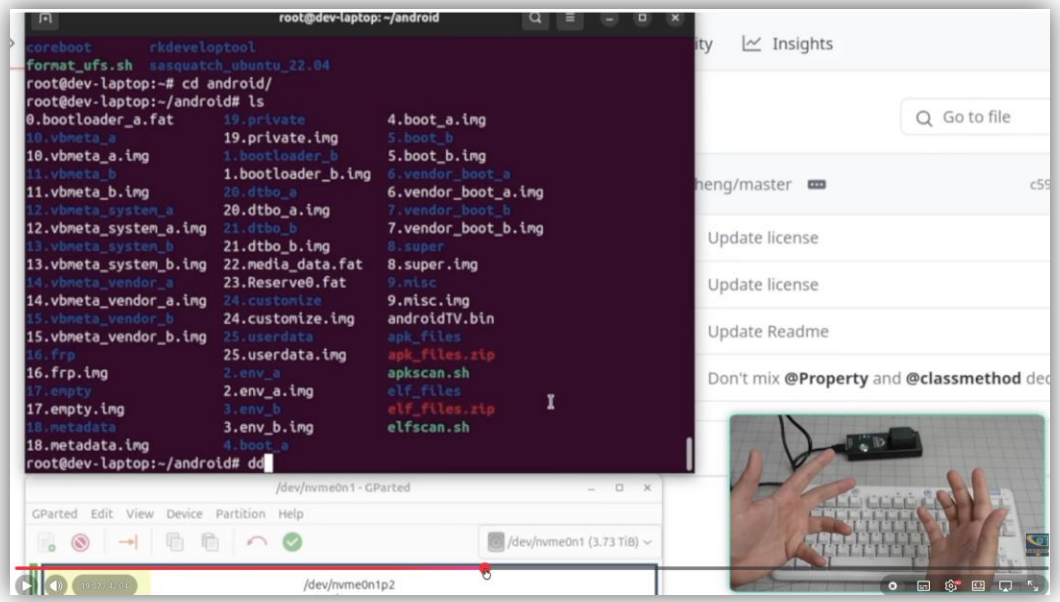
Technical Indicators and TTPs (cont)

Device Indicators: The FBI bulletin lists user-facing signs requiring Play Protect be disabled, use of unrecognized apps or marketplaces, sudden ad pop-ups, and unexplained network traffic .

Forensics on a suspect device may reveal hidden Android processes or unauthorized device admin apps.

Finding Malware in an Android TV Box

Matt Brown

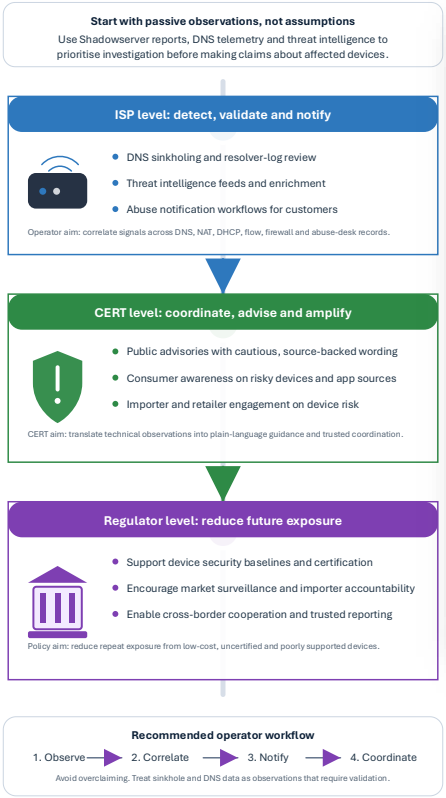


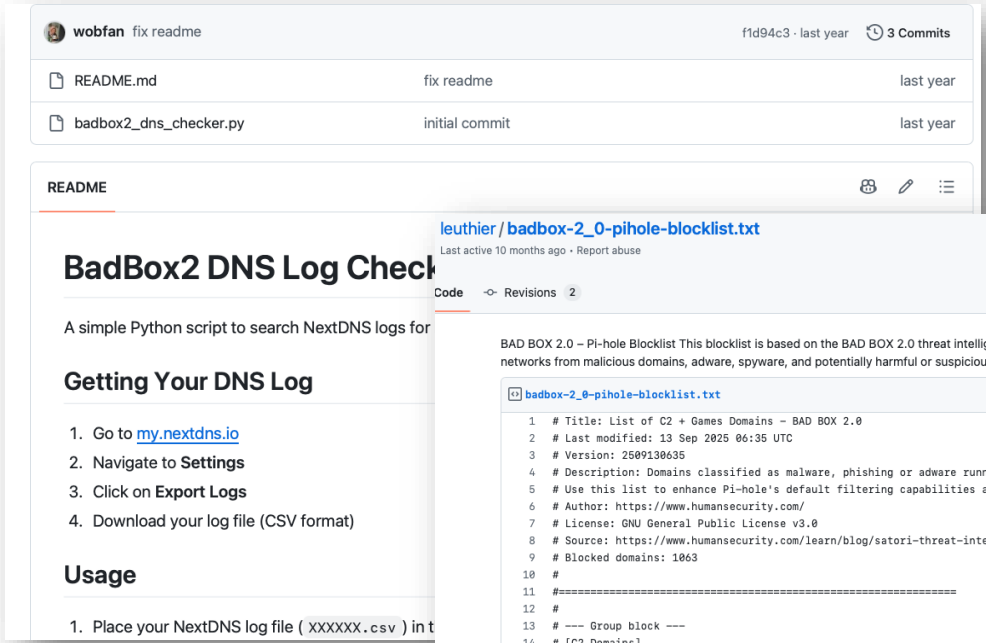
Technically unsure

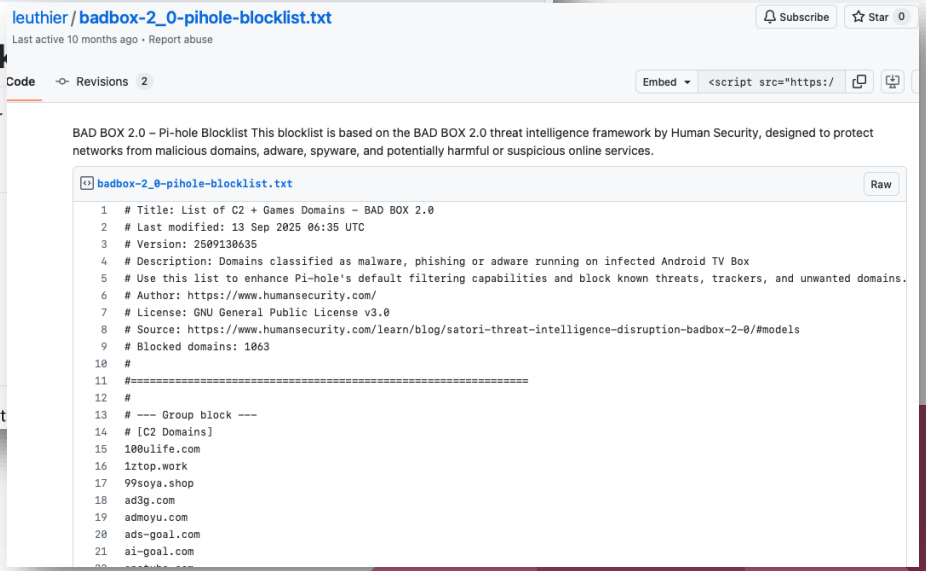
https://youtu.be/vIuT7rJgc8w

https://www.youtube.com/results?search_query=badbox+2.0+malware+investigation

Detection Framework for Operators







Recommendation for South Asia

Share

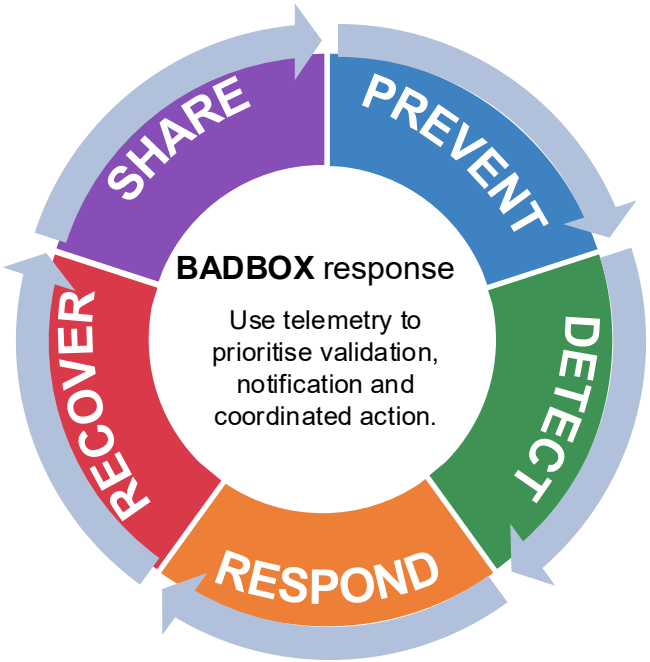
1. CERT coordination
2. Indicators of compromise
3. NOG collaboration

Recover

1. Remove insecure devices
2. Validate remediation
3. Track lessons learned

Respond

1. Customer notification
2. Abuse handling
3. CERT escalation



Prevent

1. Certified devices
2. Trusted suppliers
3. Approved app stores

Detect

1. DNS monitoring
2. Threat intelligence
3. Shadow Server reports

Recommendation for South Asia

Technical Measures:

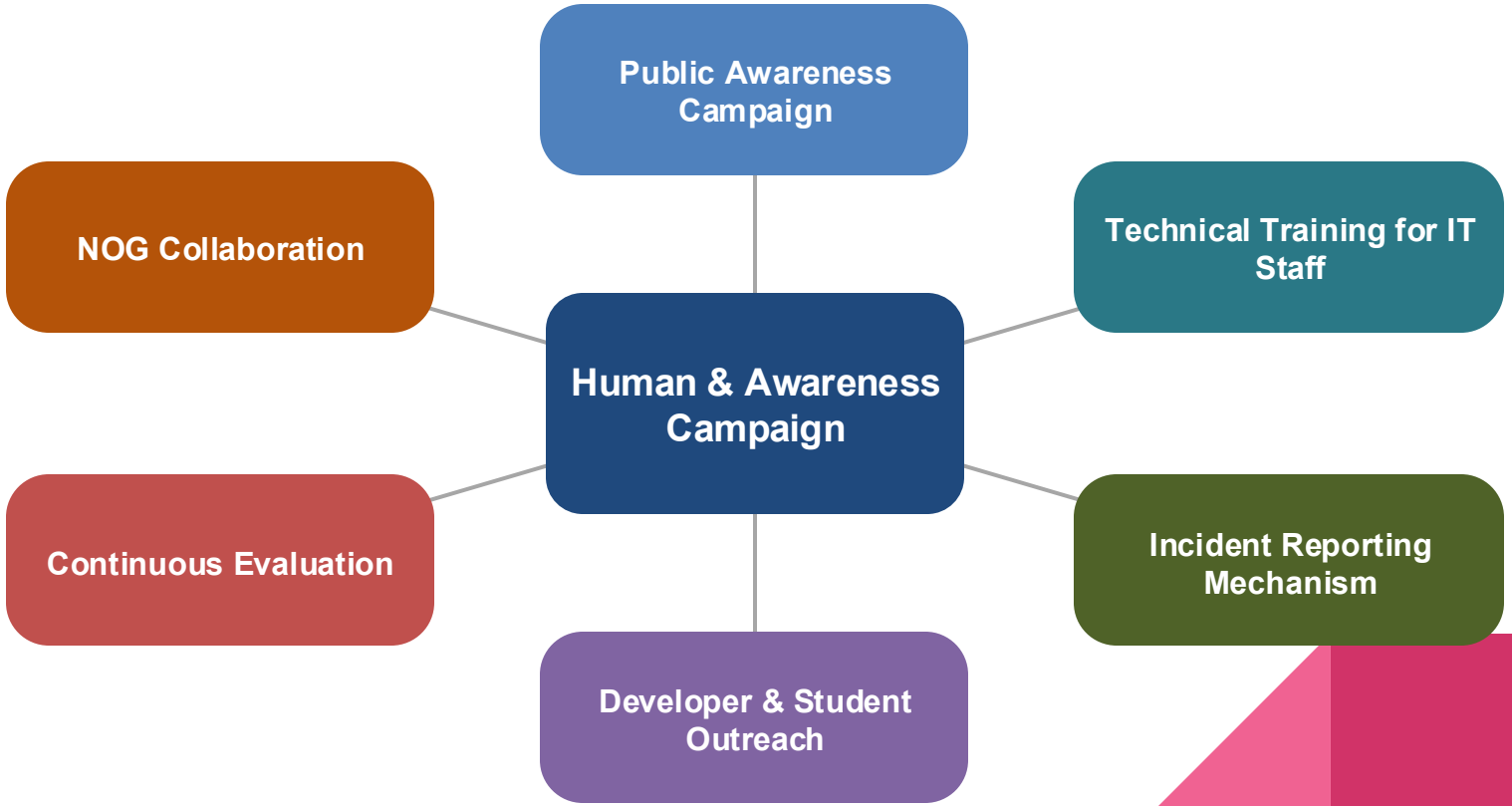
- Enforce Device Certification
- Harden App store
- Network Level Detection
- Firmware Integrity Checks
- IoT network Segmentations
- Regional threat-intelligence sharing

Recommendation for South Asia

Policy Recommendation:

- IoT/Device Security Standards (IoT security baselines)
- Market Surveillance and Certification
- Market place accountability
- Cross-border Cyber Cooperation
- Legal Enforcement

Recommendation for South Asia



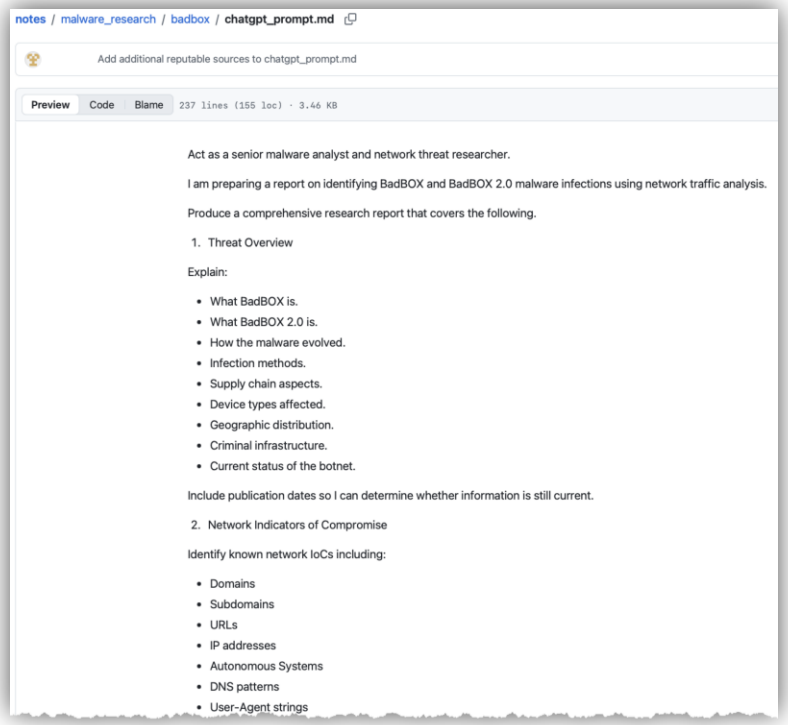
References

Title	Date	URL	Description
HUMAN Satori Threat Intelligence Disruption: BADBOX 2.0	5 Mar 2025	https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/	Primary technical investigation
FBI PSA I-060525-PSA	5 Jun 2025	https://www.fbi.gov/investigate/cyber/alerts/2025/home-internet-connected-devices-facilitate-criminal-activity	Official public warning
Google Legal Action Against BadBox 2.0	17 Jul 2025	https://blog.google/innovation-and-ai/technology/safety-security/google-taking-legal-action-against-the-badbox-20-botnet/	Google response and scale update
BADBOX 2.0 Case Study	19 Jul 2025	https://research.cgu.edu/icdc/2025/07/19/badbox-2-0-case-study/	Legal and operational analysis
Censys Unpacking the BADBOX Botnet	4 Feb 2025	https://www.censys.com/blog/unpacking-the-badbox-botnet	TLS and infrastructure analysis
Malwarebytes BadBOX Largely Disrupted	6 Mar 2025	https://www.malwarebytes.com/blog/news/2025/03/android-botnet-badbox-largely-disrupted	Follow-on analysis
HUMAN Reverse Engineering BADBOX 2.0	5 Mar 2025	https://www.humansecurity.com/learn/blog/satori-reverse-engineering-badbox-2/	Malware internals
The Hacker News BADBOX 2.0	18 Mar 2025	https://thehackernews.com/2025/03/badbox-20-botnet-infects-1-million.html	Industry summary

References

Title	Date	URL	Description
FBI IC3 PSA (I-060525-PSA)	5 Jun 2025	https://www.ic3.gov/PSA/2025/PSA250605	Official public warning
Bitsight BADBOX Botnet Is Back	17 Dec 2024	https://www.bitsight.com/blog/badbox-botnet-back	Botnet resurgence and scale
StealthMole Chen Daihai Case	4 Feb 2026	https://stealthmole-intelligence-hub.blogspot.com/2026/02/tracing-identity-exposure-around-badbox.html	Identity attribution investigation
BADBOX 2.0 Pi-hole Blocklist	13 Sep 2025	https://gist.github.com/leuthier/62fbfd86b003ca5888235e1c2e4e100d	Community C2 domain blocklist
BadBox2 DNS Log Checker	2024	https://github.com/wobfan/badbox2_dns_log_checker	DNS log detection tool
Hak5 Threat Wire: BADBOX	15 Jul 2026	https://youtu.be/j_rKXznEMvE?t=65	News video segment
BADBOX 2.0 Impacting Millions (talk)	22 Oct 2025	https://youtu.be/73jRP1hiVxQ	Conference presentation
BADBOX 2.0 Explainer Video	—	https://youtu.be/Epp-8n-_CWA	Video overview

Bonus – AI prompt



notes / malware_research / badbox / chatgpt_prompt.md

Add additional reputable sources to chatgpt_prompt.md

Preview | Code | Blame | 237 lines (155 loc) · 3.46 KB

Act as a senior malware analyst and network threat researcher.

I am preparing a report on identifying BadBOX and BadBOX 2.0 malware infections using network traffic analysis.

Produce a comprehensive research report that covers the following.

1. Threat Overview

Explain:

- What BadBOX is.
- What BadBOX 2.0 is.
- How the malware evolved.
- Infection methods.
- Supply chain aspects.
- Device types affected.
- Geographic distribution.
- Criminal infrastructure.
- Current status of the botnet.

Include publication dates so I can determine whether information is still current.

2. Network Indicators of Compromise

Identify known network IoCs including:

- Domains
- Subdomains
- URLs
- IP addresses
- Autonomous Systems
- DNS patterns
- User-Agent strings

Act as a senior malware analyst and network threat researcher.
I am preparing a report on identifying BadBOX and BadBOX 2.0 malware infections using network traffic analysis.

Produce a comprehensive research report that covers the following.
1.Threat Overview
Explain:
•What BadBOX is.
•What BadBOX 2.0 is.
•How the malware evolved.
•Infection methods.
•Supply chain aspects.
•Device types affected.
•Geographic distribution.
•Criminal infrastructure.
•Current status of the botnet.

Include publication dates so I can determine whether information is still current.

https://github.com/waz-here/notes/blob/main/malware_research/badbox/chatgpt_prompt.md