

BtCIRT THREAT BRIEFING

Supply-Chain Malware at Scale

Mapping BADBOX Botnet Exposure in Bhutan

Pratima Pradhan (ICT ANALYST)

BtCIRT, GovTech Agency

Warren Finch

Internet Society

TV

IoT



What Is a Botnet?

A botnet is a network of internet-connected devices — PCs, routers, IoT devices, smart TVs — infected with malware and controlled remotely by an attacker (a “bot herder”) through command-and-control (C2) infrastructure, without the owner’s knowledge or consent.

- Scale — thousands to millions of devices
- Stealth — owners are unaware
- Persistence — survives reboot & reset
- Rentable — sold or leased as a service

1

Infect

Malware is planted via supply chain, downloads, or exploited vulnerabilities.

2

Connect

The device silently contacts a C2 server on boot or at intervals.

3

Command

The attacker issues instructions to some or all of the botnet.

4

Exploit

Bots act in unison: DDoS, ad fraud, proxying, spam, credential theft.

Why Botnets Threaten National Digital Infrastructure



ISP & Country IP Reputation

Infected ASNs get blacklisted, degrading email delivery and hosting reputation nationwide.



Bandwidth & Service Quality

Hidden background traffic consumes consumer and upstream bandwidth, raising costs and degrading QoS.



Springboard for Attacks

Nationally hosted bots become launch points for DDoS and fraud against others — legal and diplomatic exposure.



Financial System Risk

Residential proxies disguise fraud and account-takeover traffic as legitimate in-country users.



Erosion of Digital Trust

As e-Government, digital ID and mobile banking expand, compromised home networks become the weakest link.



Attribution & Response Burden

NAT masks device-level attribution, raising the cost and time of every CERT investigation.

BADBOX Starts With Consumer Devices

1

Android TV
Boxes

3

Smart TVs

5

Tablets

2

Streaming
Devices

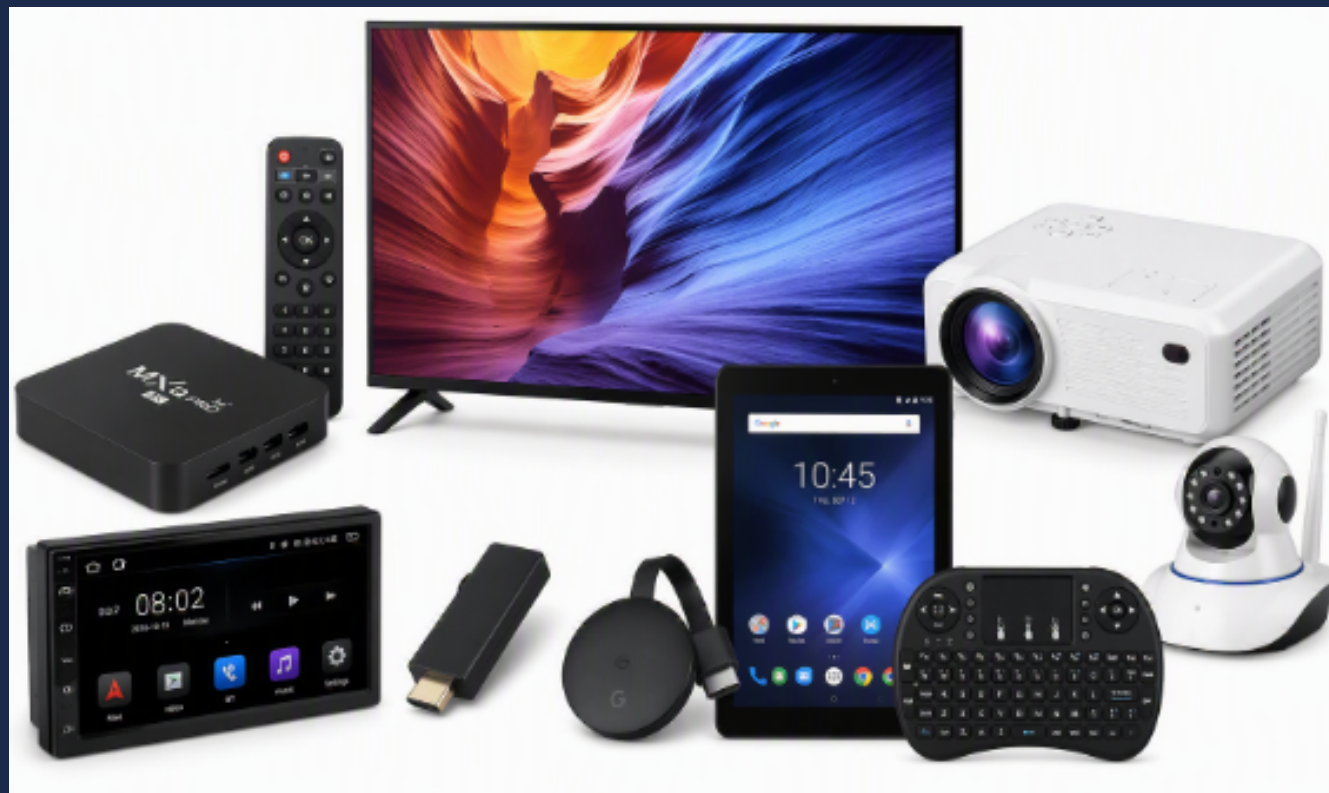
4

Projectors

6

Smartphones

Every category above has been confirmed as a BADBOX infection vector — compromised before the customer ever powers the device on.



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:

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 botnet². 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 services⁴ 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

The Evolution of BADBOX



BADBOX is an evolving supply-chain threat that turns consumer devices into criminal infrastructure at scale. Network operators, ISPs and CERTs should monitor, detect and respond.

Infection Vectors

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

2

First-Boot Network Infection

Compromise during setup. The device contacts setup infrastructure and retrieves a backdoor, loader or unauthorised app.

OPERATOR FRAMING

- Look for repeated suspicious DNS/HTTP(S)
- Correlate DHCP, NAT and flow records
- Don't treat one connection as proof

3

Malicious Apps (Third-Party)

Compromise through apps. Malicious or rebundled applications installed from unofficial marketplaces.

OPERATOR FRAMING

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

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

Why Should We Care?



Conditions in Bhutan

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

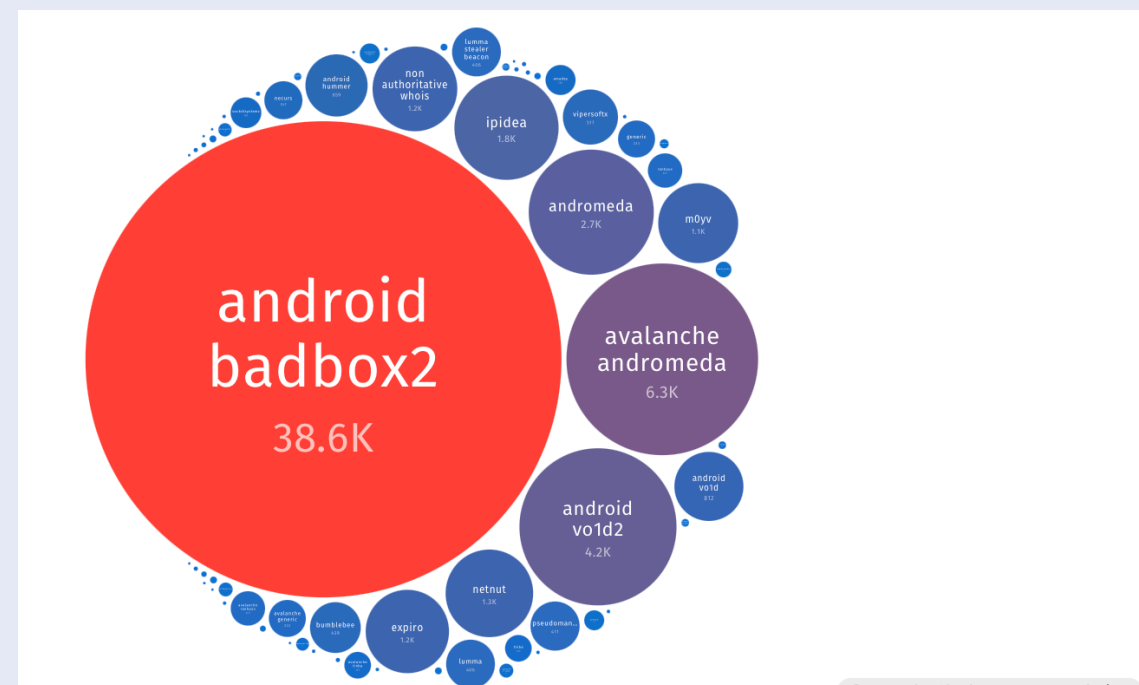
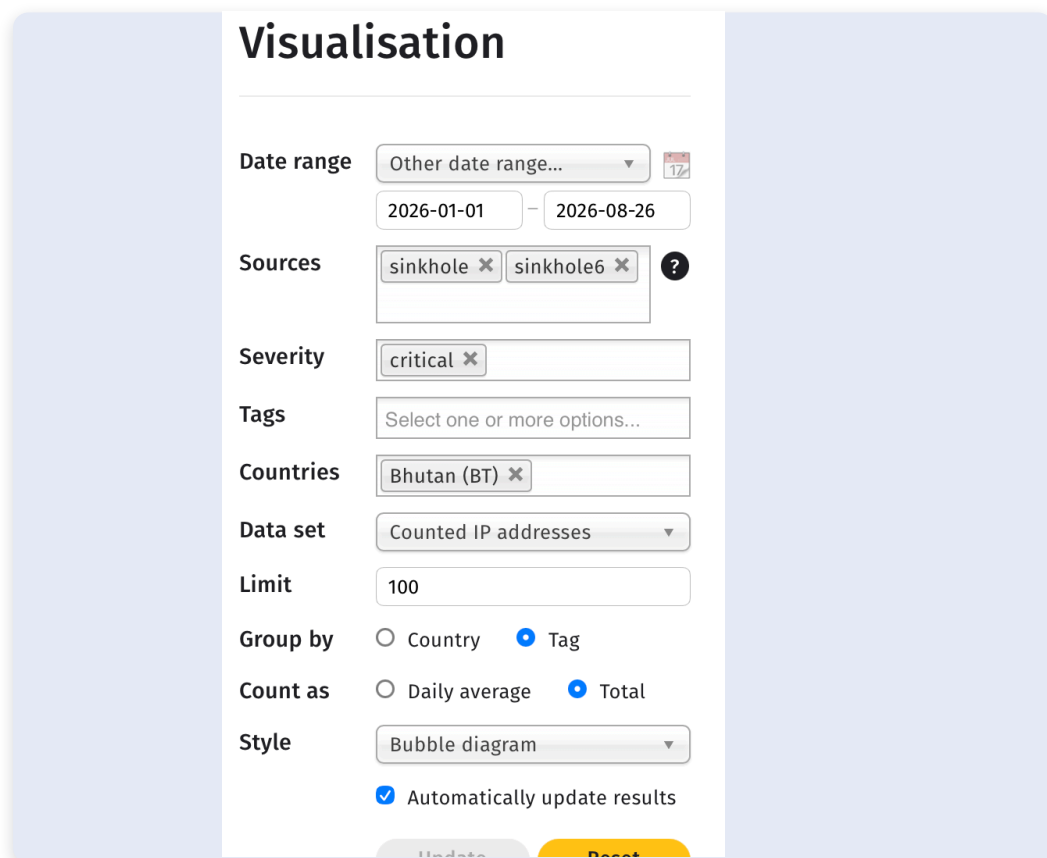


Potentially Affected Devices

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

Botnet Infections — Shadowserver Dashboard

Shadowserver's IoT-device and botnet dashboards track confirmed-infected unique IPs by country and ASN, refreshed daily. Bhutan is available as a filterable country.



Dashboard Link

Do We Know What Fraction of Imported Hardware Is Affected?

Short answer: No — globally or for Bhutan. Researchers report absolute infected-device counts (192,000+ globally per Bitsight; “millions” of devices for BADBOX 2.0 per FBI/IC3), not a share of shipped hardware.

1

No Stock Keeping Unit (SKU) -Level Registry

Manufacturers and importers don't track which production batches carry preinstalled malware.

2

NAT Undercounts Devices

Infected devices sit behind ISP Carrier Grade NAT — one public IP can hide many devices, so IP counts $\neq$ device counts.

3

No Import Denominator

The total in-country population of TV boxes, smart TVs and tablets isn't tracked against threat telemetry.

Bhutan Case Study



Findings

- Threat intelligence feeds identified BadBox-related infections associated with all known Autonomous Systems (ASs) in Bhutan.



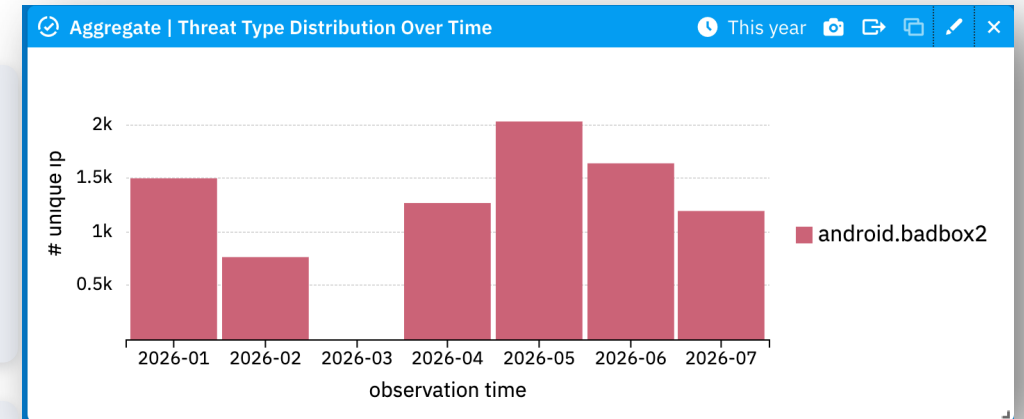
Actions

- Follow-up actions are being planned, including validation, notification, and coordination with ISPs and network operators.



Challenges

- BadBox-infected devices sit within customers' networks behind ISP-managed NAT. Tracing from a public IP to a specific customer device is difficult when multiple devices share one public IP.



Bhutan Traffic & Exposure Context

Confirmed today: BadBox-related infections are associated with all known AS in Bhutan (BtCIRT Commercial Tool). Granular figures below are not yet compiled — this is a ready-to-use data request.

Metric to compile	Source
Confirmed BadBox-infected unique IPs in Bhutan, trended over time	BtCIRT commercial tool / Shadowserver BT feed
Residential + mobile broadband subscriber base (denominator)	Perhaps: BICMA “Statistics at a Glance”, quarterly
Share of C2 check-in traffic from residential vs. enterprise/government ASNs	ISP flow data (BTL, TashiCell, Nano)
BadBox-related traffic volume vs. total ISP outbound traffic	ISP NetFlow telemetry

These four fields, once filled, directly answer “how does Bhutan’s BadBox traffic compare with overall and residential traffic?”

C2 Infrastructure



Known Command-and-Control Domains

- coslogdydy[.]in · yydsmr[.]com · logcer[.]com



Related Infrastructure

- Bitsight found dozens of related domains (e.g. cxlcyy.com, goologer.com) sharing naming patterns or SSL certificates
- These domains often serve backdoor payloads (e.g. / uploads/apk/...) or respond with encrypted commands



Key Control

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

virustotal.com

URL, IP address, domain or file hash

12/91

Community Score

-1

12/91 security vendors flagged this domain as malicious

Reanalyze

yydsmr....

Registrar

Stichting Registrar of Last Resort Foundation

Creation Date

3 years ago

Last Analysis Date

6 hours ago

top-100K

DETECTION

DETAILS

RELATIONS

COMMUNITY7

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks.](#)

Security vendors' analysis ⓘ

Do you want to auto

ADMINUSLabs	ⓘ Malicious	alphaMountain.ai	ⓘ Malicious
BitDefender	ⓘ Phishing	Chong Lua Dao	ⓘ Malicious
CyRadar	ⓘ Malware	Dr.Web	ⓘ Malicious
Forcepoint ThreatSeeker	ⓘ Malicious	Fortinet	ⓘ Malware
Kaspersky	ⓘ Malware	Lionic	ⓘ Malware
Sophos	ⓘ Malware	VIPRE	ⓘ Malware
ESET	ⓘ Suspicious	Gridinsoft	ⓘ Suspicious
Avast	ⓘ Clean	Avira	ⓘ Clean

C2 Infrastructure

badbox_cloudflare_check_v3.sh

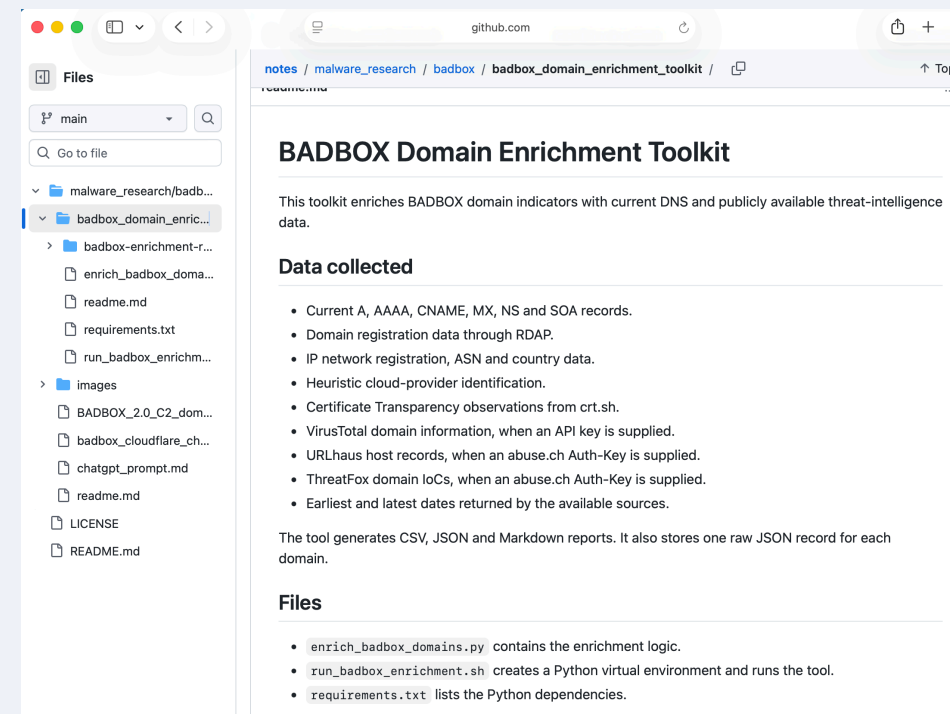
Compares the current Cloudflare Radar Top 1 Million domain dataset against the list of known BADBOX 2.0 domains.

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



Malicious APKs



Crafted Android Apps

- Malwarebytes identified packages (e.g. com.yandex.tv.home, com.instwall.launch) linked to BadBox



“Decoy Twin” Apps

- Google / Trend Micro discovered decoy twins: benign app listings in Play Store vs. identical malware distributed outside it



Publishers & Defenses

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

Traffic Patterns



Hidden Requests

- Infected devices make hidden HTTP(S) requests; “hidden WebViews” load hundreds of ad-heavy HTML5 game sites



C2 Check-Ins

- Unique URI paths (e.g. /terminal/client/, /ota/api/tasks/v2) with device-specific query parameters



Scale Indicator

- Large DNS resolution spikes (millions for yydsmr[.]com) indicate botnet scale — network defenses can flag such abnormal volumes

Device Indicators



User-Facing Signs (FBI Bulletin)

- Requirement to disable Google Play Protect
- Use of unrecognized apps or marketplaces
- Sudden ad pop-ups; unexplained network traffic



Forensic Signs

- Hidden Android processes or unauthorized device-admin apps on a suspect device

Detection Framework for Operators



Prevent

Certified devices, trusted suppliers, approved app stores.



Detect

DNS monitoring, threat intelligence, Shadowserver reports.



Respond

Customer notification, abuse handling, CERT escalation.



Recover

Remove insecure devices, validate remediation, track lessons.



Share

CERT coordination, indicators of compromise, NOG collaboration.

The next five slides break this down by who in Bhutan is responsible for what — BICMA, BtCIRT, ISPs and network/device owners.

Who Does What

Stakeholder	Prevent	Detect	Respond	Recover	Share
BICMA (Sector Regulator)	Device certification & import policy	—	Escalation support	—	Convene operators
BtCIRT (National CERT)	Consumer advisories	DNS & threat-intel monitoring	Coordinate & escalate	Track lessons learned	Monthly IOC bulletin
ISPs (BTL, TashiCell, DrukCom)	Source certified devices	Resolver-level DNS monitoring	Notify customers, abuse SLA	Validate remediation	Report findings to BtCIRT
Network & Device Owners	Buy certified devices	Watch device indicators	Report to ISP / BtCIRT	Replace infected device	—

The next four slides unpack each row in detail — the specific actions behind each cell above.

BICMA — Sector Regulator



What BICMA should do

- PREVENT** Require Play Protect–certified Android devices in any public procurement or resale guidance to consumers.
- PREVENT** Publish a consumer advisory listing red flags: unbranded “unlocked” TV boxes, “free streaming” marketing, no Play Protect certification.
- PREVENT** Explore HS-code import awareness with Customs for high-risk device categories — proposed next step, not yet in place.
- SHARE** Convene licensed ISPs and operators periodically to review compliance and BtCIRT’s IOC bulletins.

BtCIRT — National CERT



What BtCIRT should do

DETECT Operationalize Shadowserver's daily BadBox/IoT feed filtered to Bhutanese ASNs; auto-ingest into BtCIRT's ticketing system.

DETECT Run continuous DNS monitoring for known BADBOX C2 domains and related SSL-thumbprint infrastructure.

RESPOND Act as the central coordination point: validate hits, direct ISP notification, and escalate unresolved cases to regional/international CERT partners.

RECOVER Maintain a shared knowledge base of lessons learned per case to refine future detection rules.

SHARE Issue a monthly IOC bulletin to all licensed operators; represent Bhutan in BTNOG and regional CERT forums; feed validated indicators back to Shadowserver, Bitsight and HUMAN Security.

ISPs — BTL, TashiCell, DrukCom & Others



What ISPs should do

DETECT Correlate DHCP, NAT and flow logs so a public-IP hit maps to a customer session — essential given CGN.

DETECT Alert on abnormal per-subscriber DNS volume (a single device generating thousands of lookups/day).

RESPOND Follow a standard customer-notification script, and acknowledge BtCIRT notifications within a defined SLA — e.g. 5 business days.

RECOVER Validate remediation with a second DNS/telemetry check 7–14 days after notification — don't rely on customer self-report.

SHARE Report confirmed cases and any new indicators back to BtCIRT.

Network & Device Owners



What network & device owners should do

PREVENT Source only Play Protect–certified devices from trusted suppliers; avoid unofficial app marketplaces.

DETECT Watch for device indicators: forced Play Protect disable, unrecognized apps, sudden ad pop-ups, unexplained traffic.

RESPOND Report suspicious devices to your ISP or BtCIRT rather than just disconnecting quietly.

RECOVER Replace confirmed-infected devices — a factory reset alone is not sufficient if malware sits in firmware.

THE BOTTOM LINE — FOR EVERYONE ABOVE

Monitor DNS to known BADBOX C2 infrastructure, correlate a hit to a subscriber within 24 hours, notify within 5 business days — and never assume a factory reset alone has fixed an infected device.

References

- FBI IC3 — ic3.gov/PSA/2025/PSA250605
- Bitsight — bitsight.com/blog/badbox-botnet-back
- HUMAN Security — humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0
- StealthMole Intelligence Hub — stealthmole-intelligence-hub.blogspot.com
- gist.github.com/leuthier/62fbfd86b003ca5888235e1c2e4e100d
- github.com/wobfan/badbox2_dns_log_checker
- youtu.be/j_rKXznEMvE
- Shadowserver Foundation — dashboard.shadowserver.org
- BICMA — Statistics at a Glance — bicma.gov.bt

THANK YOU

Pratima Pradhan · BtCIRT, GovTech Agency

Warren Finch · Internet Society