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

Pratima Pradhan, BtCIRT GovTech Agency

What is the threat of BADBOX

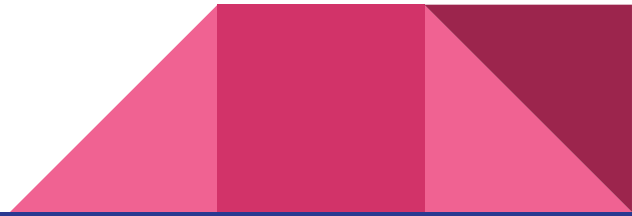
BadBox is not simply malware.

It is a:

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

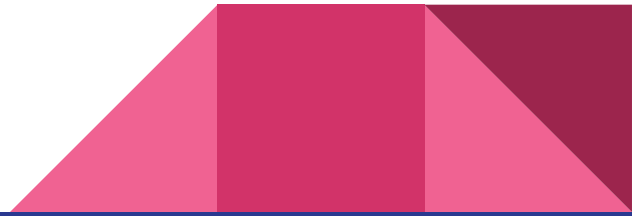
Evolution of Badbox

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



Infection Vectors

Vector 1 – Preinstalled Supply-Chain Malware
Vector 2 – First-Boot Network Infection
Vector 3 – Malicious Apps (Third-Party):



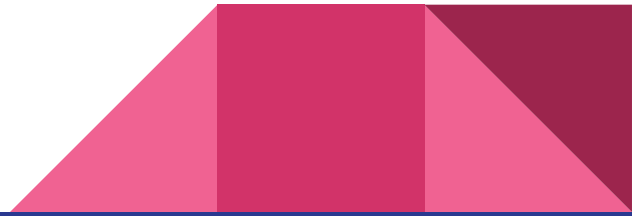
Why South Asia Should Care?

Common conditions

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

Potentially affected devices include:

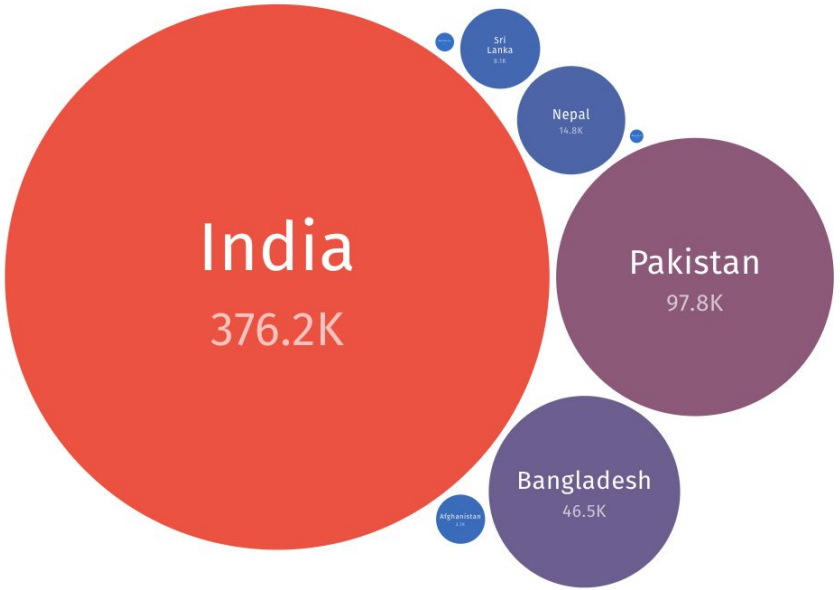
- Android TV boxes
- Streaming devices
- Smart TVs
- Projectors
- Tablets



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



Bhutan Case Study

Threat Intel Feeds through IoCs: All ASes in Bhutan are infected with Badbox at least 2 % of their network.

Actions: Not much action taken, but it is todo list.

Issues: At the national level, the badbox lies at the

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.

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 (summing up from [12] and [23]).

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 35

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.

Detection Framework for Operators (work to do..)

- ISPs Level
  - DNS sinkholing
  - Threat intelligence feeds
  - Abuse notification workflows
- CERT Level
  - Public advisories
  - Consumer awareness
  - Importer engagement
- Regulators

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

Human and Awareness Measures:

- Public Awareness Campaign
- Technical training for IT staffs
- Incident Reporting Mechanism
- Developer and Student Outreach
- Continuous Evaluation
- SANOG collaboration

References

https://research.cgu.edu/icdc/2025/07/19/badbox-2-0-case-study

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