An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

# Android BadBox 2.0 Malware

18 July 2025

STATUS: **TLP:CLEAR**

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

Please treat this document in accordance with the TLP assigned.

**ncsc.gov.ie**

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

# Executive Summary

The NCSC has recently observed a significant increase in compromised devices within Ireland, infected with Android BadBox 2.0 malware. **BADBOX 2.0** is an Android malware which is embedded in device firmware affecting many comsumer grade products. Infected devices immediately connect to a Command and Control (C2) server and enable the attacker to access the local network (proxy), intercept two-factor authentication secrets and to install additional malware on the device.

The NCSC's Computer Security Incident Response Team (CSIRT-IE) is currently receiving telemetry from trusted partners who are operating a sinkhole for IPs geolocated to Ireland. Sinkholing is a technique whereby a resource used by malicious actors to control malware is taken over and redirected to a benign listener that can (to a varying degree) understand connections coming from infected devices.

This report aims to explain the scale and capabilities of those infections and outline how Ireland is affected by these malware infections.

# What is Badbox 2.0?

Badbox 2.0 is a large scale Android malware supply chain operation which involves the **pre-infection of consumer devices.** Low cost Android devices such as Android tablets, connected TV (CTV) devices, digital photo frames, phones etc. are often targeted, usually by rogue firmware images installed during manufacturing or distribution.

These devices typically come from low-cost manufacturers using third-party firmware providers, with poor supply chain security.

The malware is embedded in the system image or signed with privileged certificates making removal of the malware considerably more difficult. A factory reset or flashing of the device often does not mitigate the infection. For added persistence, some variants install hidden launchers, system apps or downloaders, which will re-install the malware after removal.

Badbox 2.0 is not a single piece of malware it is a modular eco system built by collaborating threat actors. Infected devices become part of a botnet and subsequently have the capacity to conduct several attacks including:

Ad Fraud Module:

- Opens and clicks on ads in the background without user consent.
- Utilizes hidden WebViews or emulated user interactions.
- Capable of simulating thousands of ad impressions per day per device.
- Generates revenue for attackers via fake ad traffic.

App Installation & Ranking Fraud:

- Silently downloads and installs specific apps without user permission.
- Inflates app install counts and manipulates app store rankings.
- Often runs the installed apps silently in the background to simulate user engagement.

Residential Proxy Services, turns infected devices into proxy exit nodes to facilitate the following attacks:

- Account Takeover (ATO)
- Fake Account Creation

- Distributed Denial of Service (DDoS)
- Malware Distribution
- One-Time Password (OTP) Theft

Data Harvesting Module, collects sensitive user and device information, including:

- Installed apps
- IP and MAC addresses
- Geolocation data
- Device ID, IMEI, Android version, and more

# What to do?

BadBox 2.0 represents a serious supply chain threat, affecting millions of Android-based home devices globally that are often unknowingly compromised before reaching users.

- For consumers, this means exercising caution when purchasing low-cost smart devices and seeking products from trusted vendors, users should ensure Google Play Protect, Android's malware protection is enabled.
- Internet service providers and network administrators are encouraged to monitor for unusual traffic patterns, engage with national early warning services, and act on sinkhole data to identify and assist affected users.
- Maintain awareness and monitor internet traffic of home networks.
- Assess all IoT devices connected to networks for suspicious activity.
- Avoid downloading/sideloading applications from unofficial marketplaces advertising free streaming content.
- Keep all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps to minimise its exposure to cybersecurity threats. Prioritise patching firewall vulnerabilities and known exploited vulnerabilities in internet-facing systems.

Coordinated awareness and remediation efforts across all levels - individual, commercial, and national - are essential to limit the reach and impact of persistent and evolving malware ecosystems.

BadBox 2.0 is one of many malware campaigns currently being sinkholed—alongside others such as Vo1d[1], Tinba[2] and Nymaim/GozNym[3] variants and proxy botnets—underscoring the need for continued collaboration between industry, government, and threat intelligence partners to contain these evolving threats.

# Irish IP Addresses Communicating with Sinkholes

The NCSC receives intelligence from several trusted partner organisations regarding a range of emerging cyber threats. We are actively monitoring devices in the Irish IP address space that appear to be infected and are communicating with known sinkhole and honeypot infrastructure.

---

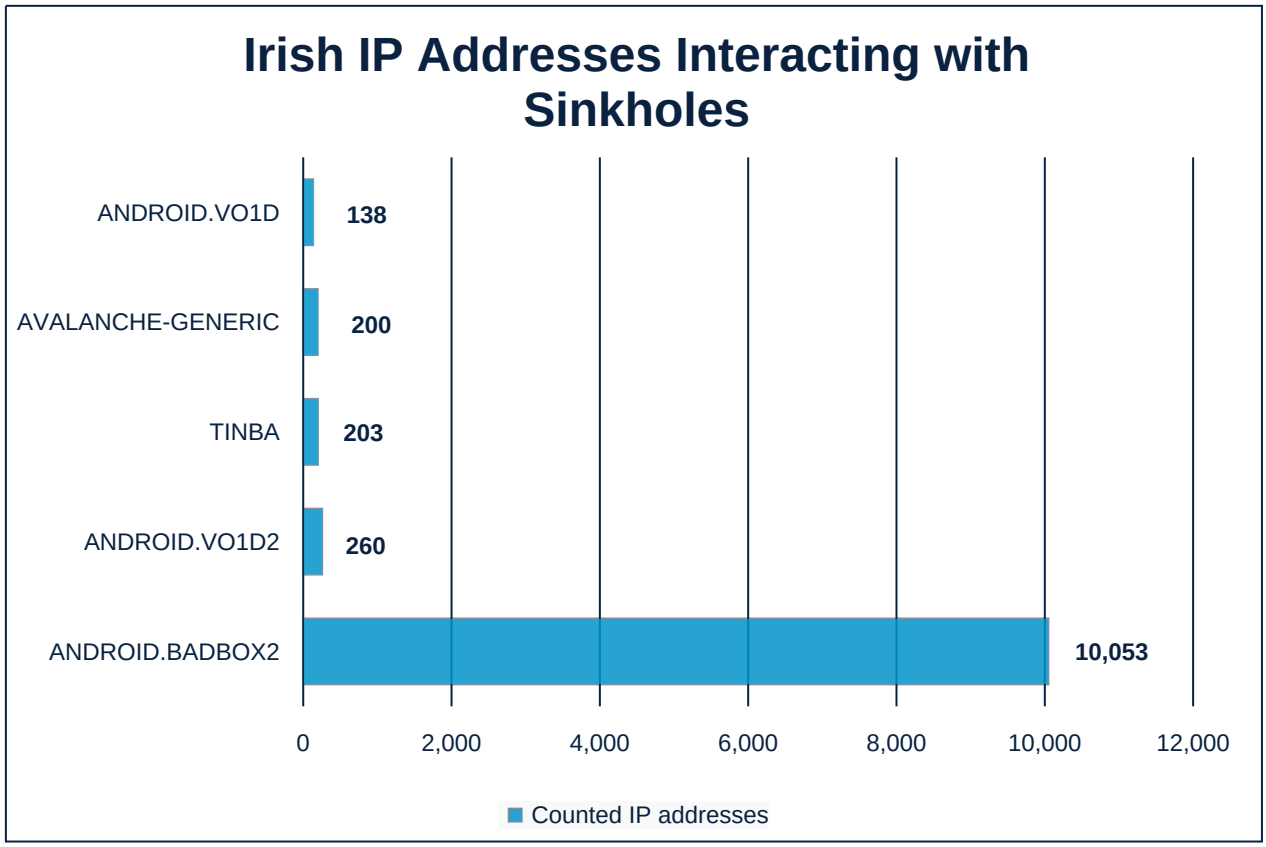
[1] https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Vo1d/Vo1d.html

[2] https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Botnetz-Avalanche/Malware/Tinba/TinyBanker_Tinba.html

[3] https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Botnetz-Avalanche/Malware/Nymaim/Nymaim.html

One of our key partners in this effort is **The Shadowserver Foundation**, a leading non-governmental organisation dedicated to internet security and threat intelligence. Supported by the Irish NCSC, Shadowserver is recognised globally for its work in uncovering vulnerabilities, tracking malicious activity, and assisting in victim remediation.

Shadowserver are coordinating the sinkhole for Badbox 2.0 malware and have shared details with CSIRT-IE of Irish IP addresses interacting with these Sinkholes. Below is a summary of sinkholed botnets currently observing traffic originating from Irish IP addresses:




As part of the NCSC's effort to protect the Irish IP address space, the National Cyber Defence Services unit within the NCSC operate an Early Warning Service (EWS). The EWS helps to protect internet users across the country by alerting internet service providers when devices on their networks may be compromised by malware, part of a botnet, or exposing security vulnerabilities.

# References

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

www.ic3.gov/PSA/2025/PSA250605

https://www.shadowserver.org/what-we-do/network-reporting/sinkhole-events-report/