Internet Crime Complaint Center (IC3)

Published: 2025-06-05 · Archived: 2026-04-05 17:05:34 UTC

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 compromise and consider disconnecting suspicious devices from their networks. The FBI has identified potential indicators that may assist in detecting malicious devices. An indicator alone does not accurately determine malicious cyber activity or a crime. The following suspicious activities/indicators do not relate to any individual, group, or business and should be observed in context.

Possible indicators of BADBOX 2.0 botnet activity include:

- The presence of suspicious marketplaces where apps are downloaded.
- Requiring Google Play protect settings to be disabled.
- Generic TV streaming devices advertised as unlocked or capable of accessing free content.
- IoT devices advertised from unrecognizable brands.
- Android devices that are not Play Protect certified.
- Unexplained or suspicious Internet traffic.

Mitigations

The following mitigation strategies can be effective steps to minimize exposure to unauthorized residential proxy networks.

- Maintaining awareness and monitor Internet traffic of home networks.
- Assess all IoT devices connected to home networks for suspicious activity.
- Avoid downloading apps from unofficial marketplaces advertising free streaming content.
- Keeping all operating systems, software, and firmware up to date. Timely patching is one of the most efficient and cost-effective steps to minimize its exposure to cybersecurity threats. Prioritize patching firewall vulnerabilities and known exploited vulnerabilities in internet-facing systems.

Acknowledgements

Google, Human Security, Trend Micro, and the Shadowserver Foundation contributed to this product.

Victim Reporting

If you believe you have been a victim of an intrusion, please file a report with the FBI's Internet Crime Complaint Center (IC3) at www.ic3.gov.
