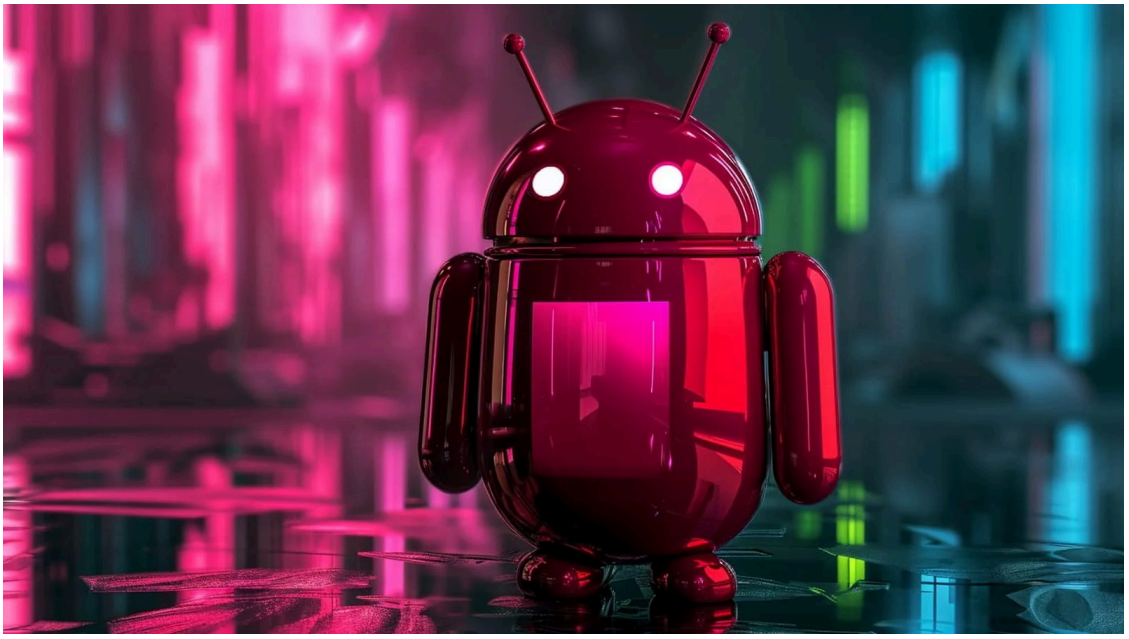
Germany blocks BadBox malware loaded on 30,000 Android devices

By Bill Toulas

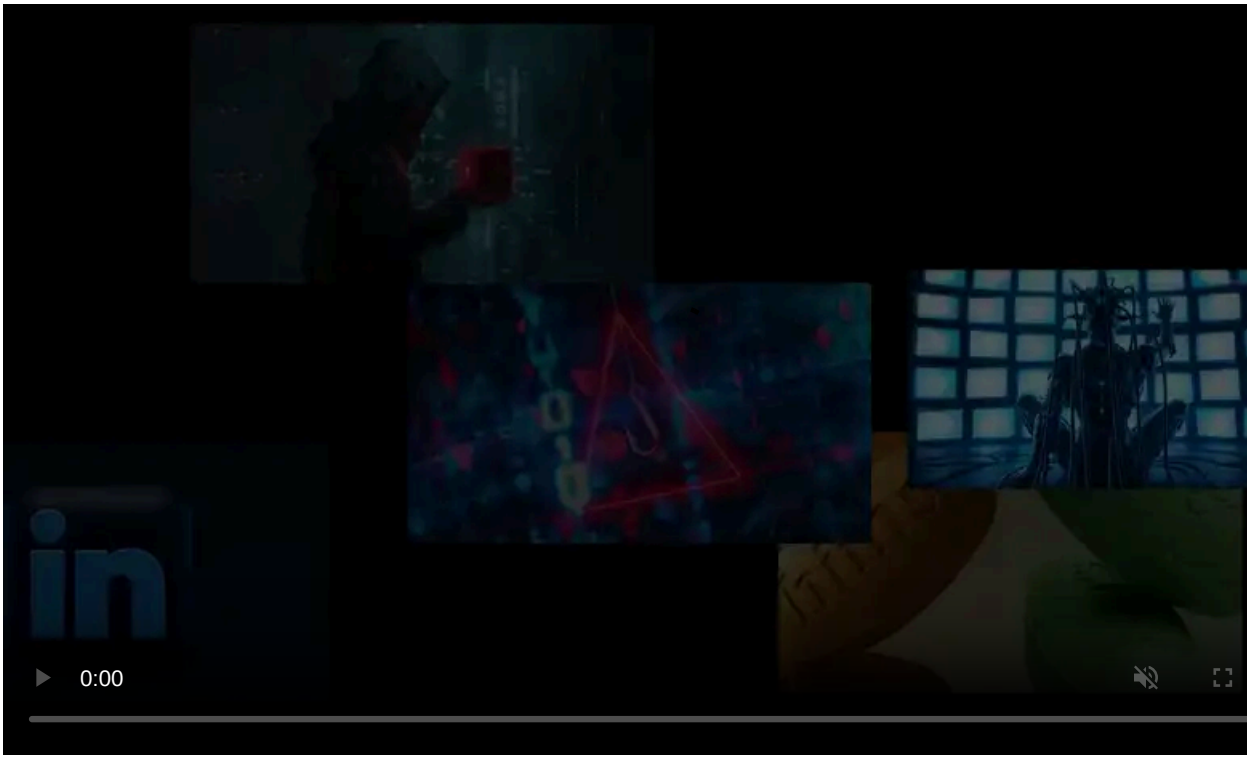
Published: 2024-12-13 · Archived: 2026-04-05 18:48:27 UTC



Germany's Federal Office for Information Security (BSI) has disrupted the BadBox malware operation pre-loaded in over 30,000 Android IoT devices sold in the country.

The types of impacted devices include digital picture frames, media players and streamers, and potentially smartphones and tablets.

BadBox is an Android malware that comes pre-installed in an internet-connected device's firmware that is used to steal data, install additional malware, or for the threat actors to remotely gain access to the network where the device is located.


0:00

When an infected device is first connected to the internet, the malware will attempt to contact a remote command and control server run by the threat actors. This remote server will tell the BadBox malware what malicious services should be run on the device and will also receive data stolen from the network.

BSI says the malware can steal two-factor authentication codes, install further malware, and create email and messaging platform accounts to spread fake news. It can also engage in ad fraud by loading and clicking on ads in the background, generating revenue for fraud rings.

Finally, BadBox can be set up to act as a proxy, allowing other people to use the device's internet bandwidth and hardware to route their own traffic. This tactic, known as residential proxying, often involves illegal operations that implicate the user's IP address.

Germany's cybersecurity agency says it blocked communication between the BadBox malware devices and their command and control (C2) infrastructure by sinkholing DNS queries so that the malware communicates with police-controlled servers rather than the attacker's command and control servers.

Sinkholing prevents the malware from sending stolen data to the attackers and receiving new commands to execute on the infected device, effectively preventing the malware from working.

"The BSI is currently redirecting the communication of affected devices to the perpetrators' control servers as part of a sinkholing measure pursuant to Section 7c of the BSI Act (BSIG)," reads BSI's announcement.

"This affects providers who have over 100,000 customers (More about sinkholing). There is no acute danger for these devices as long as the BSI maintains the sinkholing measure."

Infected device owners to be notified

Device owners who are impacted by this sinkholing operation will be notified by their internet service providers based on their IP address.

The agency says that anyone who receives a notification should immediately disconnect the device from their network or stop using it. Unfortunately, as the malware came pre-installed with firmware, other firmware from the device's manufacturer should not be trusted and the device should be returned or discarded.

BSI notes that all of the impacted devices were running outdated Android versions and old firmware, so even if they were secured against BadBox, they remain vulnerable to other botnet malware for as long as they are exposed online.

"Malware on internet-enabled products is unfortunately not a rare phenomenon. Outdated firmware versions in particular pose a huge risk," warned BSI President Claudia Plattner. "We all have a duty here: manufacturers and retailers have a responsibility to ensure that such devices do not come onto the market. But consumers can also do something: cyber security should be an important criterion when purchasing!"

Moreover, the announcement mentions that, due to the vast variance in Android IoT manufacturers and device iterations, it's very likely that many more devices infected by BadBox or similar malware exist in the country, which BSI could not pinpoint this time.

This may include smartphones and tablets, smart speakers, security cameras, smart TVs, streaming boxes, and various internet-connected appliances that follow an obscure route from manufacturing to resell networks.

Signs that your device is infected by botnet malware include overheating when seemingly idle, random performance drops, unexpected settings changes, atypical activity, and connections to unknown external servers.

To mitigate the risk of outdated Android IoTs, install a firmware image from a trustworthy vendor, turn off unnecessary connectivity features, and keep the device isolated from critical networks.

Generally, it is recommended that you buy smart devices only from reputable manufacturers and look for products offering long-term security support.

Update 12/14 - Google has sent BleepingComputer the below statement:

> "These off-brand devices discovered to be infected were not Play Protect certified Android devices. If a device isn't Play Protect certified, Google doesn't have a record of security and compatibility test results.
>
> Play Protect certified Android devices undergo extensive testing to ensure quality and user safety. To help you confirm whether or not a device is built with Android TV OS and Play Protect certified, our Android TV website provides the most up-to-date list of partners. You can also take these steps to check if your device is Play Protect certified." - A Google spokesperson

---

Source: https://www.bleepingcomputer.com/news/security/germany-blocks-badbox-malware-loaded-on-30-000-android-devices/