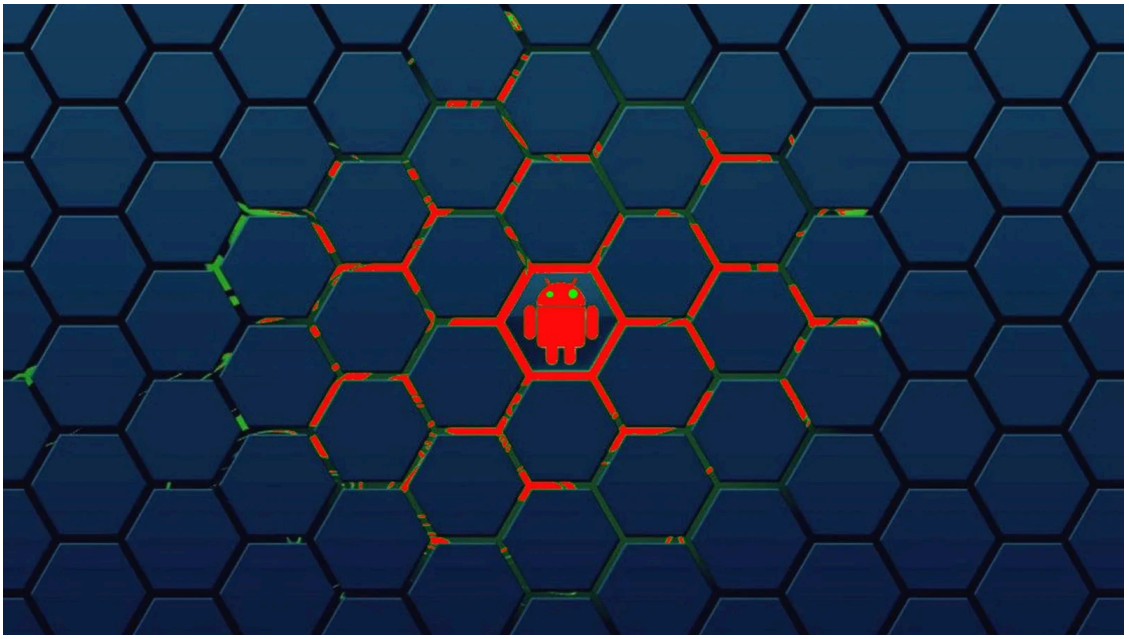
BadBox malware botnet infects 192,000 Android devices despite disruption

By Bill Toulas

Published: 2024-12-19 · Archived: 2026-04-05 21:28:58 UTC

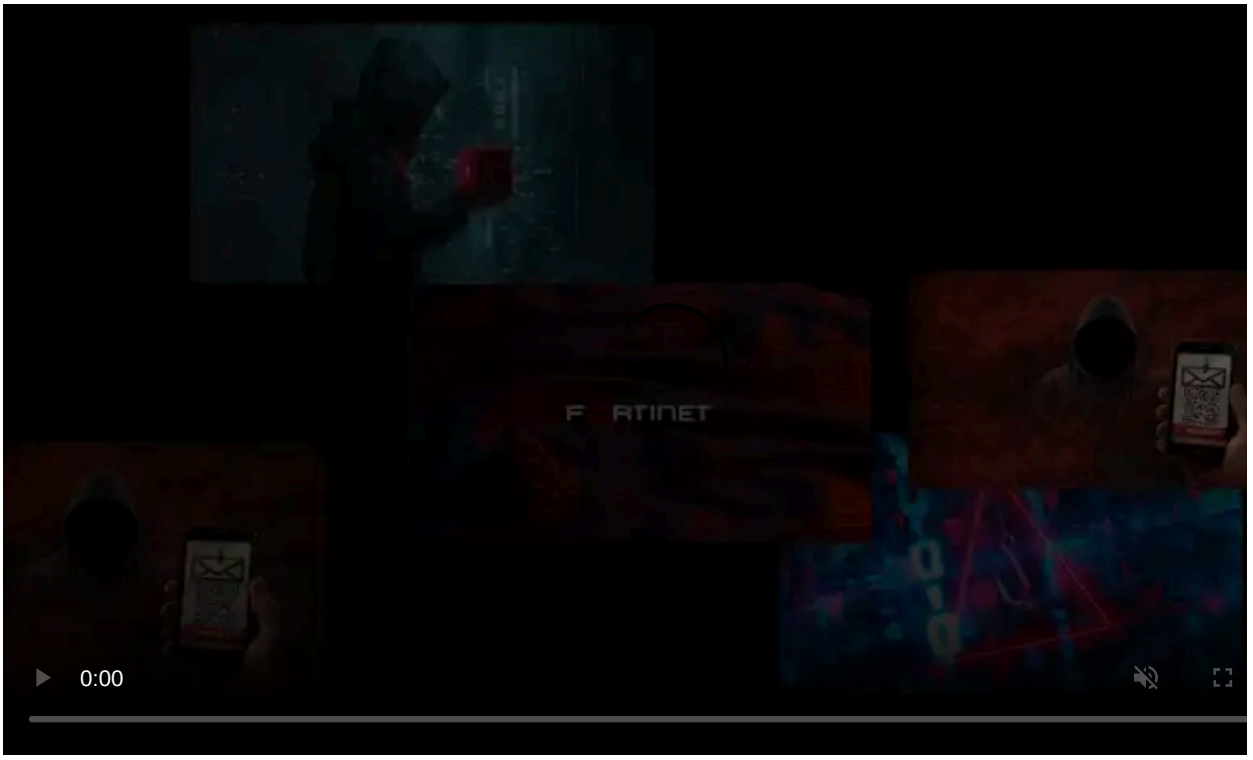


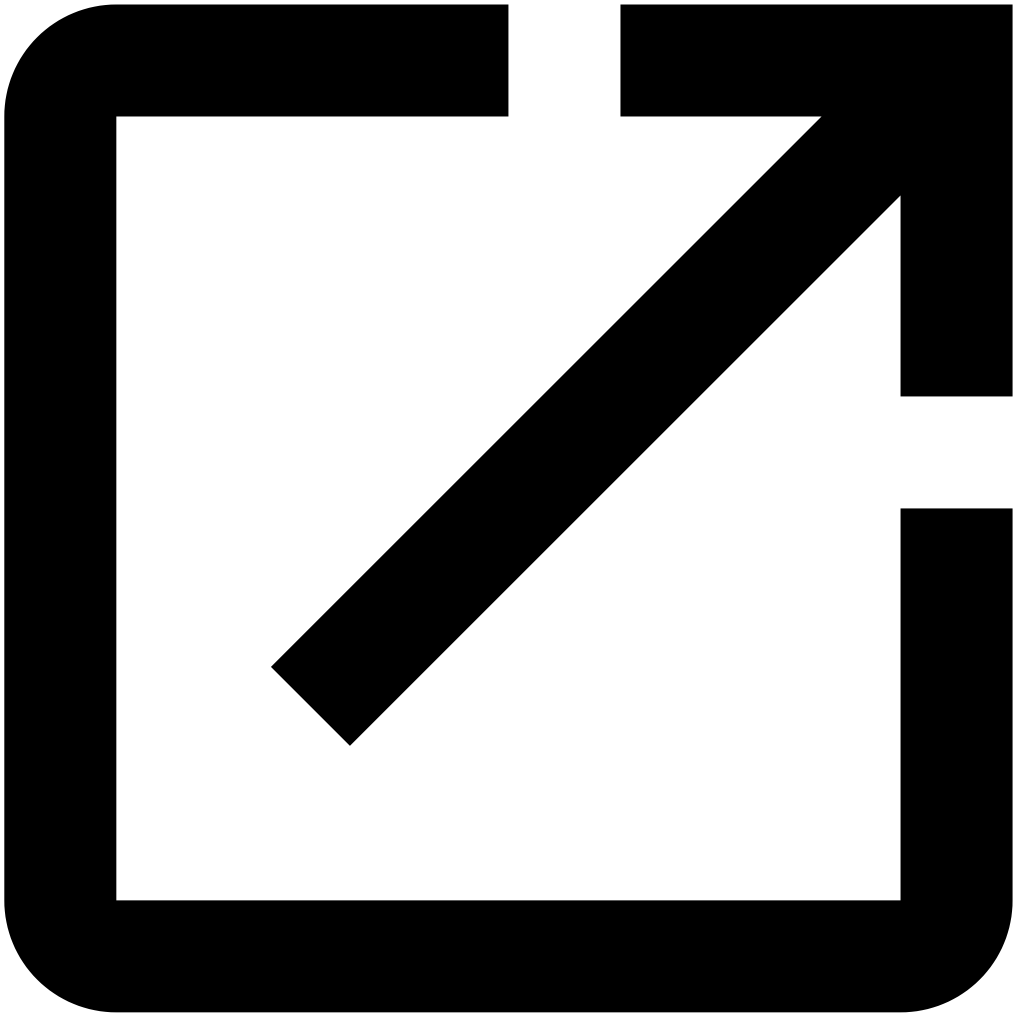
The BadBox Android malware botnet has grown to over 192,000 infected devices worldwide despite a recent sinkhole operation that attempted to disrupt the operation in Germany.

Researchers from BitSight warn that the malware appears to have expanded its targeting scope beyond no-name Chinese Android devices, now infecting more well-known and trusted brands like Yandex TVs and Hisense smartphones.

The BadBox malware botnet

BadBox is an Android malware thought to be based on the 'Triada' malware family, infecting devices made by obscure manufacturers either through supply chain attacks on their firmware, shady employees, or through injections taking place as they enter the product distribution phase.

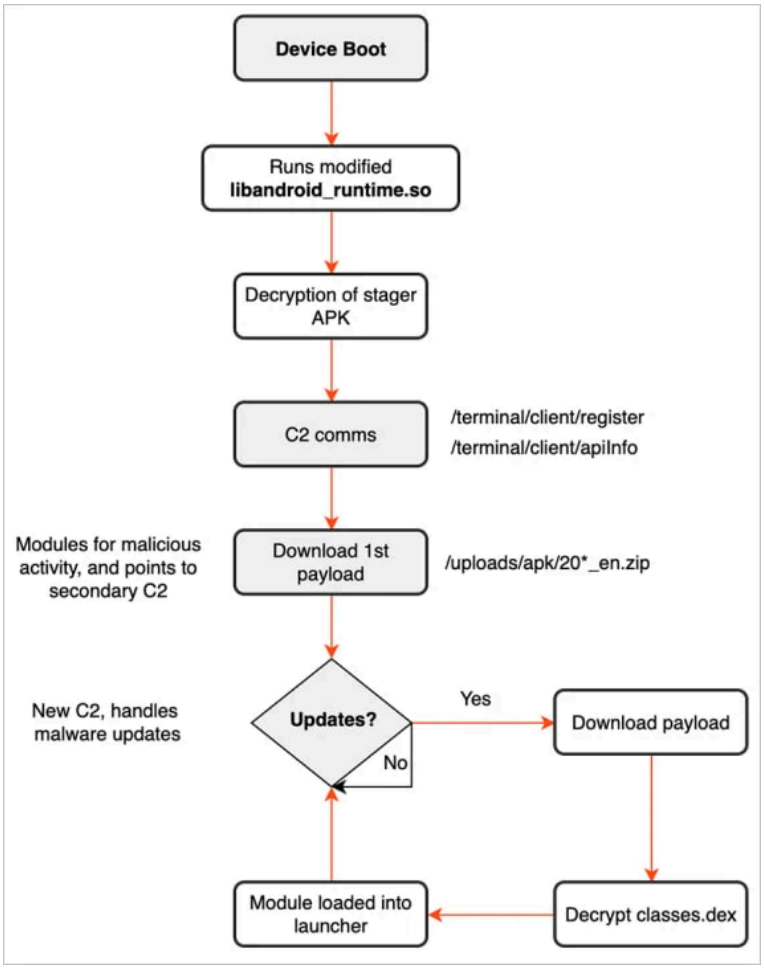

F RTINET
0:00



It was first discovered on a T95 Android TV box purchased from Amazon by Canadian security consultant Daniel Milisic in early 2023. Since then, the malware operation has expanded to other no-name products sold online.

The goal of the BadBox campaign is financial gain, which is achieved by turning the device into a residential proxy or using it to perform ad fraud. These residential proxies can then be rented to other users, in many cases cybercriminals, who use your device as a proxy to conduct attacks or other fraudulent activity.

Additionally, the BadBox malware can be used to install additional malicious payloads onto Android devices, enabling more dangerous operations.



Malware activity flow
Source: BitSight

Last week, Germany's Federal Office for Information Security (BSI) announced they disrupted the BadBox malware operation in the country after it sinkholed one of the malware's command and control servers, cutting off communication for 30,000 Android devices.

These devices were primarily Android-based digital picture frames and media streaming boxes, but BSI warned that it's very likely that BadBox is present in more product categories.

BadBox continues to grow

The new report from BitSight confirms that the BadBox operation has continued to grow despite Germany's police action, with researchers finding the Android malware installed on 192,000 TVs and smartphones.

According to BitSight researcher Pedro Falé, the cybersecurity company was able to sinkhole one of the command and control servers used by the BadBox malware operation.

As the researchers now control the domain, they can see when devices attempt to connect to it, allowing them to see how many unique IP addresses are impacted.

"The reality is that BADBOX still seems to be very much alive and spreading," wrote Falé.

"This was evident when Bitsight managed to sinkhole a BADBOX domain, registering more than **160,000 unique IPs in a 24 hour period**. A number that has been steadily growing."

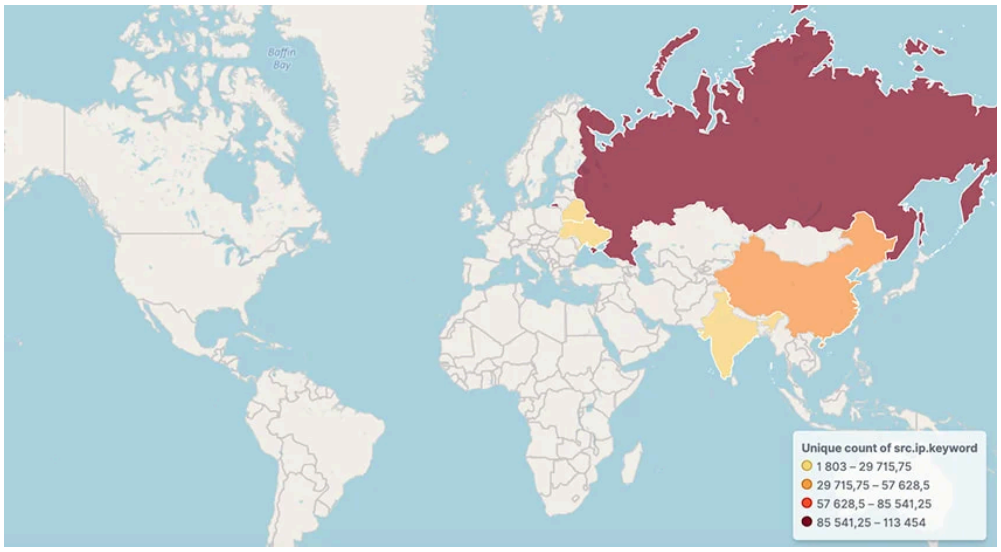
The number of detected devices is much higher than what was previously considered the peak for this botnet, at around 74,000 compromised devices.

Roughly 160,000 of the infected devices are the Yandex 4K QLED Smart TV, which is very popular in Russia, and the Hisense T963 smartphone.

"The [impacted] models ranging from YNDX-00091 to YNDX-000102 are 4K Smart TVs from a well-known brand, not cheap Android TV boxes," explains BitSight.

"It's the first time a major brand Smart TV is seen directly communicating at such volume with a BadBox command and control (C2) domain, broadening the scope of affected devices beyond Android TV boxes, tablets, and smartphones."

The devices detected by BitSight are primarily located in Russia, China, India, Belarus, Brazil, and Ukraine.



Location of devices communicating with the BadBox servers
Source: BitSight

BitSight also reports that BSI's recent operation did not impact its telemetry data, as the action was geographically limited, allowing the BadBox Android malware operation to continue unabated.

With BadBox expanding to more major brands, it's crucial for consumers to apply the latest firmware security updates, isolate their smart devices from more critical systems, and disconnect them from the internet when not in use.

However, if no security or firmware updates are available for your device, you are strongly advised to disconnect them from your network or turn them off altogether.

Signs of a BadBox botnet infection include overheating and performance drops from high processor usage, atypical network traffic, and changes in the device settings.

A Google spokesperson has sent BleepingComputer the following comment regarding the above story:

> "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/badbox-malware-botnet-infects-192-000-android-devices-despite-disruption/