Android TV box on Amazon came pre-installed with malware

By Bill Toulas

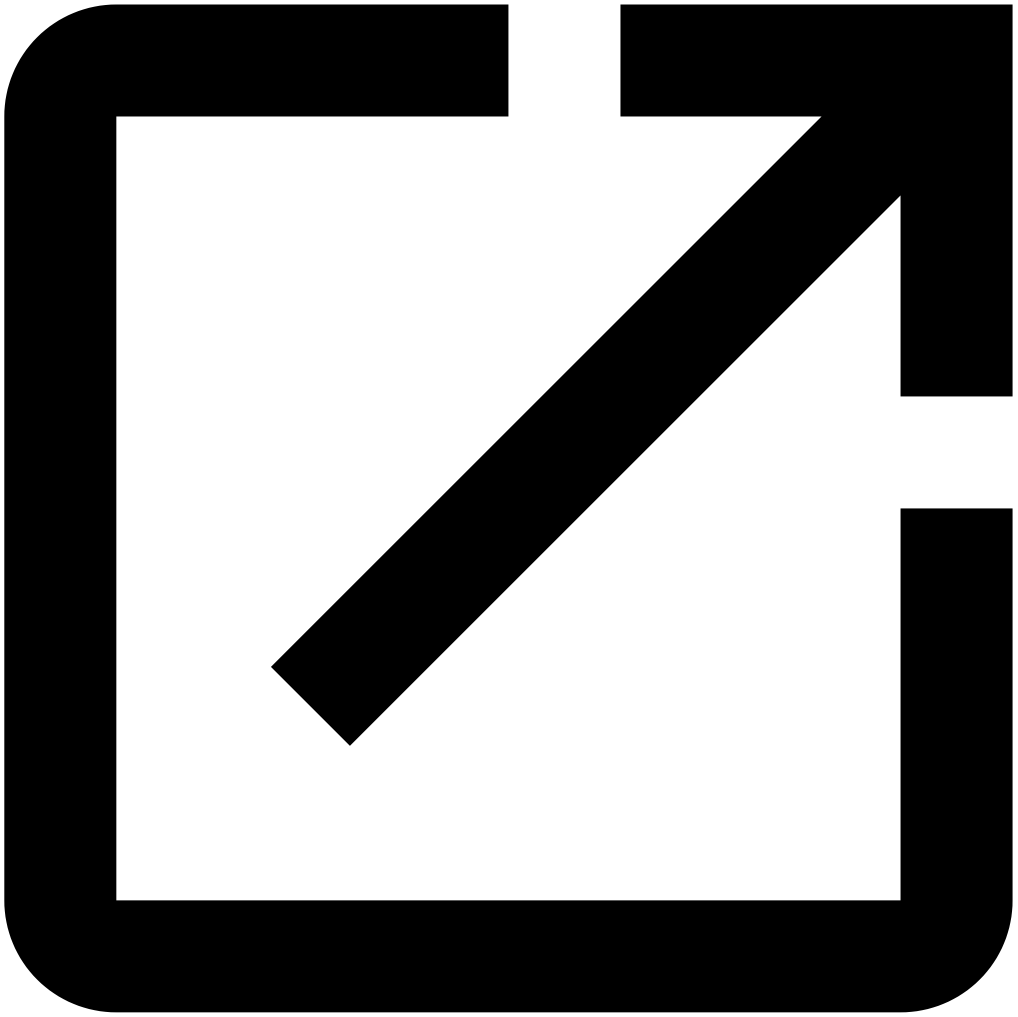
Published: 2023-01-12 · Archived: 2026-04-05 13:11:34 UTC

A Canadian systems security consultant discovered that an Android TV box purchased from Amazon was pre-loaded with persistent, sophisticated malware baked into its firmware.

The malware was discovered by Daniel Milisic, who created a script and instructions to help users nullify the payload and stop its communication with the C2 (command and control) server.

The device in question is the T95 Android TV box with an AllWinner T616 processor, widely available through Amazon, AliExpress, and other big e-commerce platforms.


DIE LINKE.
0:00



It is unclear if this single device was affected or if all devices from this model or brand include the malicious component.

Malware on the TV streaming box

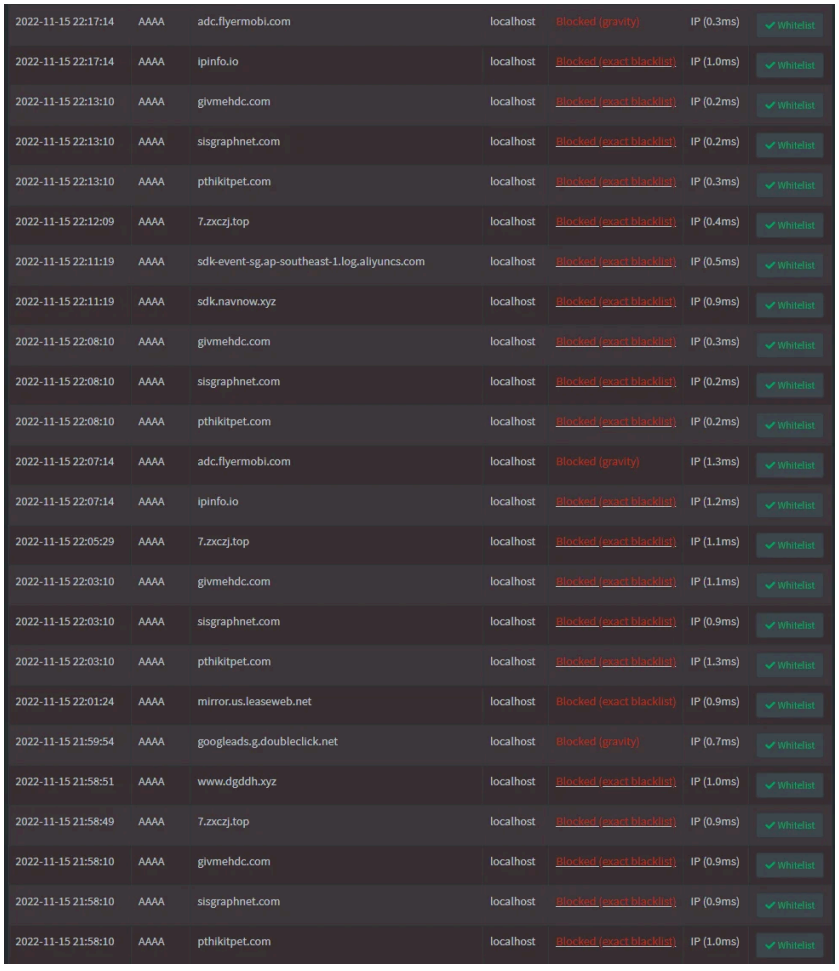
The T95 streaming device uses an Android 10-based ROM signed with test keys and the ADB (Android Debug Bridge) open over Ethernet and WiFi.

This is a suspicious configuration as ADB can be used to connect to devices for unrestricted filesystem access, command execution, software installation, data modification, and remote control.

However, as most consumer streaming devices sit behind a firewall, threat actors will likely be unable to connect to ADB remotely.

Milisic says he initially bought this device to run the Pi-hole DNS sinkhole, which protects devices from unwanted content, advertisements, and malicious sites without installing software.

While analyzing the DNS request in Pi-hole, Milisic discovered that the device was attempting to connect to several IP addresses associated with active malware.



2022-11-15 22:17:14	AAAA	adc.flyermobi.com	localhost	Blocked (gravity)	IP (0.3ms)	Whitelist
2022-11-15 22:17:14	AAAA	ipinfo.io	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist
2022-11-15 22:13:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:13:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:13:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (0.3ms)	Whitelist
2022-11-15 22:12:09	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (0.4ms)	Whitelist
2022-11-15 22:11:19	AAAA	sdk-event-sg.ap-southeast-1.log.aliyuncs.com	localhost	Blocked (exact blacklist)	IP (0.5ms)	Whitelist
2022-11-15 22:11:19	AAAA	sdk.navnow.xyz	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 22:08:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.3ms)	Whitelist
2022-11-15 22:08:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:08:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (0.2ms)	Whitelist
2022-11-15 22:07:14	AAAA	adc.flyermobi.com	localhost	Blocked (gravity)	IP (1.3ms)	Whitelist
2022-11-15 22:07:14	AAAA	ipinfo.io	localhost	Blocked (exact blacklist)	IP (1.2ms)	Whitelist
2022-11-15 22:05:29	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (1.1ms)	Whitelist
2022-11-15 22:03:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (1.1ms)	Whitelist
2022-11-15 22:03:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 22:03:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (1.3ms)	Whitelist
2022-11-15 22:01:24	AAAA	mirror.us.leaseweb.net	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:59:54	AAAA	googleads.g.doubleclick.net	localhost	Blocked (gravity)	IP (0.7ms)	Whitelist
2022-11-15 21:58:51	AAAA	www.dgddh.xyz	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist
2022-11-15 21:58:49	AAAA	7.zxczj.top	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	givmehdc.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	sisgraphnet.com	localhost	Blocked (exact blacklist)	IP (0.9ms)	Whitelist
2022-11-15 21:58:10	AAAA	pthikitpet.com	localhost	Blocked (exact blacklist)	IP (1.0ms)	Whitelist

List of malicious domains T95 attempts to connect to *(GitHub)*

Milisic believes the malware installed on the device is a strain that resembles 'CopyCat,' a sophisticated Android malware first discovered by Check Point in 2017. This malware was previously seen in an adware campaign where it infected 14 million Android devices to make its operators over $1,500,000 in profits.

The analyst tested the stage-1 malware sample on VirusTotal, where it returns only 13 detections out of 61 AV engine scans, classified with the generic term of an Android trojan downloader.

"I found layers on top of layers of malware using 'tcpflow' and 'nethogs' to monitor traffic and traced it back to the offending process/APK, which I then removed from the ROM," explains the analyst in a GitHub post.

"The final bit of malware I could not track down injects the 'system_server' process and looks to be deeply baked into the ROM."

The analyst observed that the malware attempted to fetch additional payloads from 'ycxrl.com,' 'cbphe.com,' and 'cbpheback.com.'

Because finding a clean ROM to replace the malicious is just as challenging, Milisic resorted to changing the DNS of the C2 to route the requests via the Pi-hole web server, making it possible to block them.

Users of T95 are recommended to follow these two simple steps to clean their device and nullify the malware that runs on it:

1. Reboot into recovery mode or perform “Factory Reset” from the settings menu.
2. Upon reboot, connect to ADB via USB or WiFi-Ethernet and run this script.

To confirm that the malware has been rendered harmless, run “ `adb logcat | grep Corejava` ” and verify that the `chmod` command failed to execute.

However, as these devices are fairly inexpensive on Amazon, it may be wiser to discontinue using them if you can afford to do so.

An ambiguous electronics market

Unfortunately, these inexpensive Android-based TV box devices follow an obscure route from manufacturing in China to global market availability.

In many cases, these devices are sold under multiple brands and device names, with no clear indication of where they originate.

Furthermore, as the devices commonly flow through many hands, vendors and re-sellers have several opportunities to load custom ROMs on the devices, potentially malicious ones.

Even if most e-commerce sites have policies to prevent selling devices pre-loaded with malware, enforcing these rules by scrutinizing all electronics and confirming they're free of sophisticated malware is practically impossible.

To avoid such risks, you can pick streaming devices from reputable vendors like Google Chromecast, Apple TV, NVIDIA Shield, Amazon Fire TV, and Roku Stick.

BleepingComputer attempted to contact the listed seller on Amazon but could not find any website or email address associated with the brand.

Update 1/13 - Daniel Milisic shared more information about the discovered malware with BleepingComputer, leading to minor corrections and additions in the article.
