November 14, 2023

The Honorable Lina Khan, Chair
The Honorable Rebecca Slaughter, Commissioner
The Honorable Alvaro Bedoya, Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

**Re: Complaint Regarding the Resale of Known Compromised Devices to Consumers by Amazon, AliExpress & Others**

Dear Commissioners,

Recent reports have revealed various models of Android TV set-top boxes and mobile devices that are being sold by resellers Amazon, AliExpress, and other smaller vendors to include malware before the point of sale.[1] These include malware included in devices by Chinese manufacturers AllWinner and RockChip. We call on the FTC to use its power under section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) to sanction resellers of devices widely known to include harmful malware.

As this also constitutes a supply-chain attack on consumer-based Internet of Things (IoT) devices, we are also sending a copy of this letter to the Cybersecurity and Infrastructure Security Agency Director Jen Easterly.

*Malware Specifics*

These devices, when first powered on and connected to the internet, will immediately begin communicating with botnet command and control (C2) servers.[2] From there, these devices connect to a vast click-fraud network which a report by HUMAN Security recently dubbed BADBOX.[3] All this operates in the background of the device, unbeknownst to the buyer. Even if the buyer does manage to learn about their device having malware, there is little they can do to remediate the situation to take back control of their devices without extensive technical knowledge.[4]

As the HUMAN report illustrates, the malware is a variant of the Triada trojan which is installed between the time when a Chinese manufacturer produces the device and when they are provided to resellers.

---

[1] EFF, *Android TV Boxes Sold on Amazon Come Pre-Loaded with Malware* (Last modified May 10, 2023), https://www.eff.org/deeplinks/2023/05/android-tv-boxes-sold-amazon-come-pre-loaded-malware.
[2] Wikipedia, *Botnet* (Accessed Nov 3, 2023), https://en.wikipedia.org/wiki/Botnet#Command_and_control.
[3] HUMAN Security, *Trojans All the Way Down: BADBOX and PEACHPIT* (Published Oct 4, 2023), https://www.humansecurity.com/hubfs/HUMAN_Report_BADBOX-and-PEACHPIT.pdf.
[4] Malwarebytes, *Analyzing and remediating a malware infested T95 TV box from Amazon* (Published Jan 30, 2023), https://www.malwarebytes.com/blog/news/2023/01/preinstalled-malware-infested-t95-tv-box-from-amazon.

Despite widespread reporting on these compromised devices in outlets as widely circulated as Wired, and attempts to raise this with Amazon directly, the devices continue to be sold as of the writing of this letter on Amazon, AliExpress, and other smaller vendors.[5] We note that this is over 10 months after initial reports.[6]

*Reseller Inaction*

We believe the resellers of these devices bear some responsibility for the broad scope of this attack and for failing to create a reliable pathway for researchers to notify them of these issues. In our correspondence with security researcher Daniel Milisic, who deeply researched and published his findings on the malware included in these devices, he mentioned finding it difficult (if not impossible) to reach out to Amazon and report the issue.[7] EFF itself reached out to Amazon and, as of this writing, the products are still available. While it would be impractical for resellers to run comprehensive security audits on every device they make available, they should pull these devices from the market once they are revealed and confirmed to include harmful malware. A reseller as large as Amazon should especially have systems in place.

*Risks for Consumers*

These devices put buyers at risk not only by the click-fraud they routinely take part in, but also the fact that they facilitate using the buyers' internet connections as proxies for the malware manufacturers or those they sell access to. This means that any nefarious deeds done using this proxy will look as though they were originating from the buyers' internet connection, possibly exposing them to significant legal risk. This can result in real harm to buyers of these devices, presenting an unacceptable risk which must be addressed.

*Section 5 Liability*

As noted above, we believe that these facts justify action by the FTC under section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) to sanction resellers of devices widely known to include harmful malware. We believe that the sale of these devices presents a clear instance of deceptive conduct: the devices are advertised without disclosure of the harms they present. They also expose the buyers to an unfair risk which starts after simply powering the device on and connecting it to the internet. This is not a case where freely modifiable set-top box hardware or software raise a mere possibility of a third party installing harmful malware. Freely modifiable video devices are not inherently harmful to consumers. Here, where products are sold containing real malware at the point of sale, issuing sanctions to the resellers will provide a powerful incentive for them to pull these products from the market and protect their customers.

---

[5] Wired, *Your Cheap Android TV Streaming Box May Have a Dangerous Backdoor* (Published Oct 4, 2023), https://www.wired.com/story/android-tv-streaming-boxes-china-backdoor/.
[6] BleepingComputer, *Android TV box on Amazon came pre-installed with malware* (Published Jan 12, 2023) https://www.bleepingcomputer.com/news/security/android-tv-box-on-amazon-came-pre-installed-with-malware/.
[7] DesktopECHO GitHub, *AllWinner H616/H618 & RockChip 3328 Android Malware Analysis · Cleanup* (Accessed Nov 3, 2023), https://github.com/DesktopECHO/T95-H616-Malware.

Additionally, we call on the FTC to use its regulatory power to make it easier for customers to report compromised devices either directly to the device vendors or to the commission itself, which can then in turn inform the vendor and ensure it takes remedial action. We hope you will consider your avenues for action with the seriousness that this issue deserves.

Sincerely,
Electronic Frontier Foundation

CC:

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane SW
Washington, D.C. 20528-0075