Thousands of Android devices come with unkillable backdoor preinstalled

gremlin via Getty Images

reader comments

161 with

When you buy a TV streaming box, there are certain things you wouldn’t expect it to do. It shouldn’t secretly be laced with malware or start communicating with servers in China when it’s powered up. It definitely should not be acting as a node in an organized crime scheme making millions of dollars through fraud. However, that’s been the reality for thousands of unknowing people who own cheap Android TV devices.

In January, security researcher Daniel Milisic discovered that a cheap Android TV streaming box called the T95 was infected with malware right out of the box, with multiple other researchers confirming the findings. But it was just the tip of the iceberg. This week, cybersecurity firm Human Security is revealing new details about the scope of the infected devices and the hidden, interconnected web of fraud schemes linked to the streaming boxes.

Human Security researchers found seven Android TV boxes and one tablet with the backdoors installed, and they’ve seen signs of 200 different models of Android devices that may be

impacted, according to a report shared exclusively with WIRED. The devices are in homes, businesses, and schools across the US. Meanwhile, Human Security says it has also taken down advertising fraud linked to the scheme, which likely helped pay for the operation.

Advertisement

“They’re like a Swiss Army knife of doing bad things on the Internet,” says Gavin Reid, the CISO at Human Security who leads the company’s Satori Threat Intelligence and Research team. “This is a truly distributed way of doing fraud.” Reid says the company has shared details of facilities where the devices may have been manufactured with law enforcement agencies.

Human Security’s research is divided into two areas: Badbox, which involves the compromised Android devices and the ways they are involved in fraud and cybercrime. And the second, dubbed Peachpit, is a related ad fraud operation involving at least 39 Android and iOS apps. Google says it has removed the apps following Human Security’s research, while Apple says it has found issues in several of the apps reported to it.

First, Badbox. Cheap Android streaming boxes, usually costing less than $50, are sold online and in brick-and-mortar shops. These set-top boxes often are unbranded or sold under different names, partly obscuring their source. In the second half of 2022, Human Security says in its report, its researchers spotted an Android app that appeared to be linked to inauthentic traffic and connected to the domain flyermobi.com. When Milisic posted his initial findings about the T95 Android box in January, the research also pointed to the flyermobi domain. The team at Human purchased the box and multiple others, and started diving in.

In total the researchers confirmed eight devices with backdoors installed—seven TV boxes, the T95, T95Z, T95MAX, X88, Q9, X12PLUS, and MXQ Pro 5G, and a tablet J5-W. (Some of

these have also been identified by other security researchers looking into the issue in recent months). The company’s report, which has data scientist Marion Habiby as its lead author, says Human Security spotted at least 74,000 Android devices showing signs of a Badbox infection around the world—including some in schools across the US.

https://arstechnica.com/?p=1974179