The Infamous Mirai Trojan Evolves: New “Pandora” Variant Targets Android TVs

deform.co/the-infamous-mirai-trojan-evolves-new-pandora-variant-targets-android-tvs/

September 7, 2023

Doctor Web has found a series of **Android.Pandora** trojans that target Android devices, especially during firmware updates or when users install apps to watch pirated videos. These trojans possess advanced DDoS-attack capabilities, stemming from the **Linux.Mirai** trojan lineage.

Several users reported unexpected changes in the /system directory. The research identified specific files in the system, including **/system/bin/pandoraspearrk** and **/system/bin/supervisord**, among others. The malware's installation script modifies system services with executable code in .sh files to ensure the trojan runs after the device restarts.

A file, **pandoraspearrk**, stood out. After examination, it was categorized as Android.Pandora.2 backdoor, designed to use the compromised device in a botnet for DDoS attacks. The **supervisord** file supervises the status of the **pandoraspearrk** and reactivates the backdoor if shut down. It uses s.conf for its settings. Other files like **busybox** and curl are genuine command-line tools incorporated to manage networking and file operations.

The malware particularly targets cheaper Android TV devices, with Tanix TX6 TV Box, MX10 Pro 6K, H96 MAX X3, among others, being susceptible.

The trojan is a revised version of the Android.Pandora.10 backdoor that was originally part of a malicious firmware update in December 2015 for the MTX HTV BOX HTV3 Android box. This update, likely found on multiple websites, is authenticated with open Android Open Source Project test keys. The backdoor is incorporated in **boot.img**, showing its malicious launch from the **init.amlogic.board.rc** file.

Another infection route is through apps streaming pirated content from domains targeting Spanish speakers, such as youcine and magistv. Once such an app is initiated, the GoMediaService starts stealthily. On the first app launch, this service begins automatically upon device startup, triggering the **gomediad.so** program. This program deploys multiple files, including an executable detected as **Tool.AppProcessShell.1**, which malicious apps on the device can then communicate with.

The Android.Pandora.2 backdoor, once launched, connects to a control server to replace the original system file, update itself, and await further commands.

Attackers can control the compromised device to conduct DDoS attacks, start a reverse shell, or edit Android TV system partitions. These functionalities are derived from the **Linux.Mirai** code, known for its attacks on major sites like GitHub and Netflix since 2016.