Report

Malware in Content Streaming Hardware

How hackers are targeting popular content streaming hardware for distributing malwares and cryptominers

Office of Special Inspector General of Police, Maharashtra Cyber
As piracy shifts from websites and downloads to devices and apps, hackers are adapting and finding new ways to exploit consumers. They are tapping into a growing consumer trend, the use of illicit devices and apps to access pirated movies, TV shows and live programming, to spread malware, cryptomining campaigns and exploit unsuspecting users.

According to the Digital Citizens Alliance, a lot of people use a hardware device for pirating content. One such popular device is called a "Kodi box," which is sold for between $70 to $100 on grey markets. Once purchased, users are encouraged to add new piracy apps that offer access to an ever-widening range of pirated content, including the latest movies in theaters or live events such as pay-per-view boxing matches or elite soccer games.
It was found that such pirating hardwares enabling free streaming of copyright-protected content, comes packed with malicious malwares. The devices give criminals easy access to router settings, can plant malware on shared network devices and are often leveraged to steal user credentials.

By plugging the device into a home network, (users) are enabling hackers to bypass the security (such as a router’s firewall) designed to protect their system. If apps on the box or that are later downloaded have malware, the user has helped the hacker past network security.

In a review of hardware and pirating apps, such as FreeNetflix, researchers said they found malware piggybacking on illegal apps and preloaded with content. For example, when researchers installed a live sports streaming app called Mobdro, the app forwarded the researcher’s Wi-Fi network name and password to a server in Indonesia.

In one instance, 1.5 terabytes of data was uploaded from a device that shared the same network of the Kodi box. And, in yet another instance, researchers uncovered a clever scheme that enabled criminals to pose as well-known streaming sites, such as Netflix, to facilitate illegal access to a legitimate subscription of an actual Netflix subscriber.

Cybersecurity firm Kaspersky released a detailed report in early April 2019 that revealed that many of the torrent sites offering the most pirated TV shows of 2018 contained malware, adware and Trojans capable of hijacking computers. Kaspersky particularly focused on HBO’s Game of Thrones, with the security firm finding 9,986 individual malware-laced threats among torrents of the series that attempted 129,819 attacks.
How it works

The moment a user plugs in a fully loaded piracy device and uses a piracy app – like Mobdro, FreeNetflix, Exodus, or Krypton – the app is now behind the firewall on the trusted network, effectively bypassing network security.

Once launched, the app will immediately and automatically update. These updates are forced – the user has no option to block the changes that are coming. All this may happen while the user scans through the thousands of content options – which effectively lull users into a false sense of security. Everything seems to be working as planned, but the threat actor is also getting what he or she wants – access to the device and potentially devices and networks beyond it. While the user thinks he or she is getting movie functionality, in fact, the user's device is being weaponized. Cybersecurity practitioners refer to this as “augmented functionality.”

The reason that Kodi boxes are particularly vulnerable to being hacked is twofold. First, the boxes get around the security measures included in the router because they are escorted around those measures and hooked into the home network. Second, when configuring these boxes, normal security protections are typically not installed or are disabled to accommodate piracy streaming apps.

Kodi Media Player and Crypto Mining Malware

Kodi is an open-source media player designed for televisions and developed by the XBMC Foundation. The popular media player software does not provide any content itself, but users can extend the software’s functionality by installing various add-ons, found both in the official Kodi repository and in numerous third-party repositories. It’s widely known for its support of a bevy of copyright-infringing apps that offer free access
to premium content from Netflix, Amazon Prime, Hulu, sports networks and paid subscription music services.

According to a research, the malware found in the XvMBC repository was first added to the popular third-party add-on repositories Bubbles and Gaia (a fork of Bubbles), in December 2017 and January 2018, respectively. From these two sources, and through update routines of unsuspecting owners of other third-party add-on repositories and ready-made Kodi builds, the malware spread further across the Kodi ecosystem. The malware has a multi-stage architecture and employs measures to ensure that its final payload – the cryptominer – cannot be easily traced back to the malicious add-on. The cryptominer runs on Windows and Linux and mines the cryptocurrency Monero (XMR).

Victims of this crypto mining malware campaign end up running the illicit crypto miners in one of three ways:

1. They add the URL of a malicious repository to their Kodi installation so as to download some add-ons. The malicious add-on is then installed whenever they update their Kodi add-ons.
2. They install a ready-made Kodi build that includes the URL of a malicious repository. The malicious add-on is then installed whenever they update their Kodi add-ons.
3. They install a ready-made Kodi build that contains a malicious add-on but no link to a repository for updates. They are initially compromised, though receive no further updates to the malicious add-on. However, if the cryptominer is installed, it will persist and receive updates.

The top five countries affected by this threat, according to ESET’s telemetry, are the United States, Israel, Greece, the United Kingdom and the Netherlands.

Office of Special Inspector General of Police, Maharashtra Cyber
Technical analysis

After victims add the malicious repository to their Kodi installation, the malicious repository serves an add-on named `script.module.simplejson` – a name matching that of a legitimate add-on used by many other add-ons. However, while other repositories only have the `script.module.simplejson` add-on at version 3.4.0, the malicious repository serves this add-on with version number 3.4.1.

Since Kodi relies on version numbers for update detection, all users with the Auto Update feature enabled (which is a common default setting) will automatically receive `script.module.simplejson` version 3.4.1 from the malicious repository.

The only part of `script.module.simplejson` version 3.4.1 that is modified relative to version 3.4.0 is its metadata – the file `addon.xml` contains an additional `<requires>` line. This tells Kodi to download and install an add-on named `script.module.python.requests`, at version 2.16.0 or above. The `script.module.python.requests` add-on is served by the malicious repository only. It is a modification of the legitimate add-on `script.module.requests`, containing additional, malicious Python code.

That Python code downloads, as appropriate, a Windows or Linux binary, and executes it. This executable is a downloader that fetches and executes the final payload, an executable cryptominer. If the installation of the cryptominer is successful, the malicious Python code proceeds to a self-removal phase and deletes itself.
Conclusion

According to a major independent research, there are around 12-million active users of such illicit devices in North America alone. Such users offer hackers a new avenue to exploit consumers and a path to reach other devices on a home network. These findings are a wake-up call for all stakeholders - the consumers, the technology community, e-marketplaces and law-makers to take the threat seriously.

References: