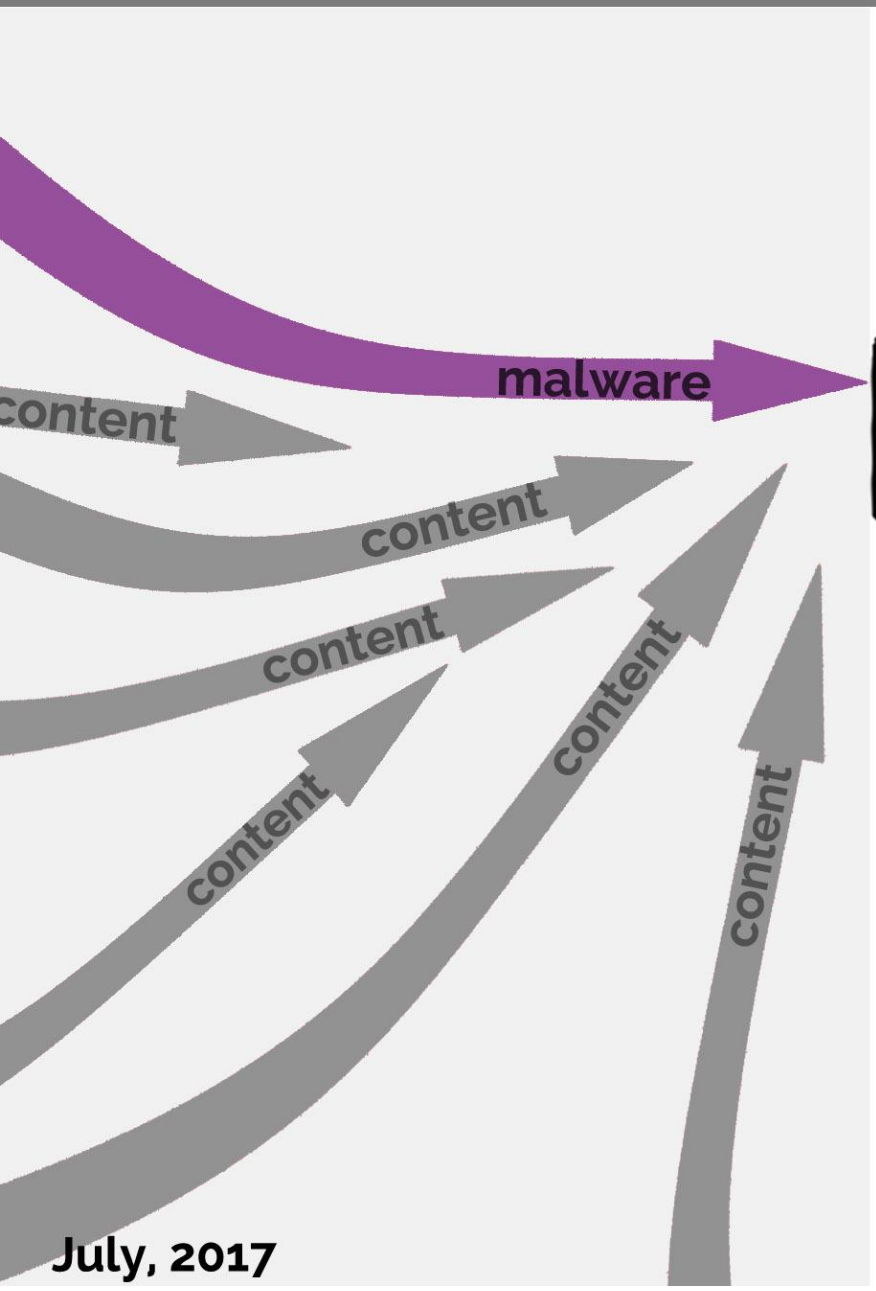
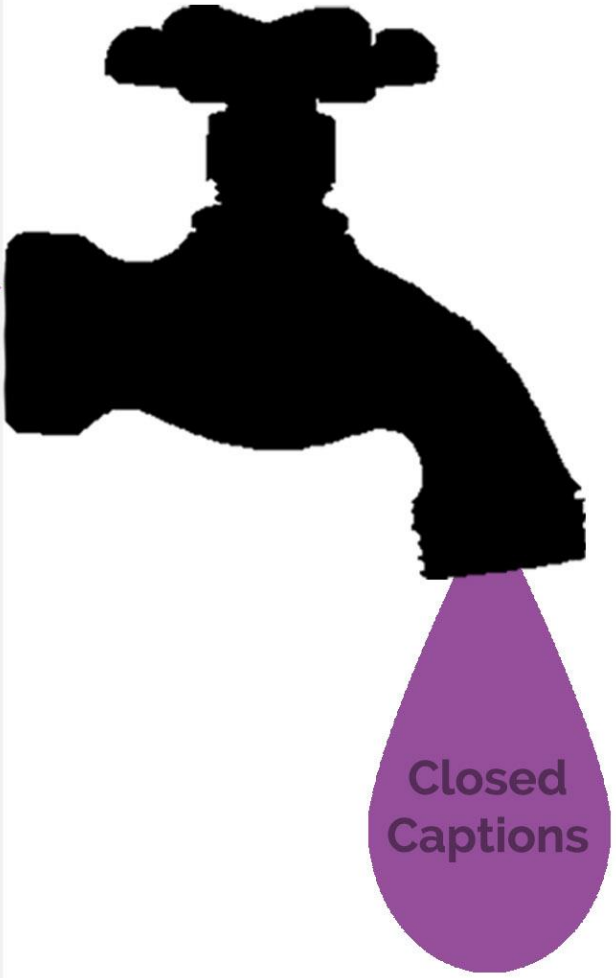
Digital Citizens Alliance Alert

Close Captioned for the Security Impaired

How the leaky system of illicit streaming devices poses a malware threat to consumers.





July, 2017

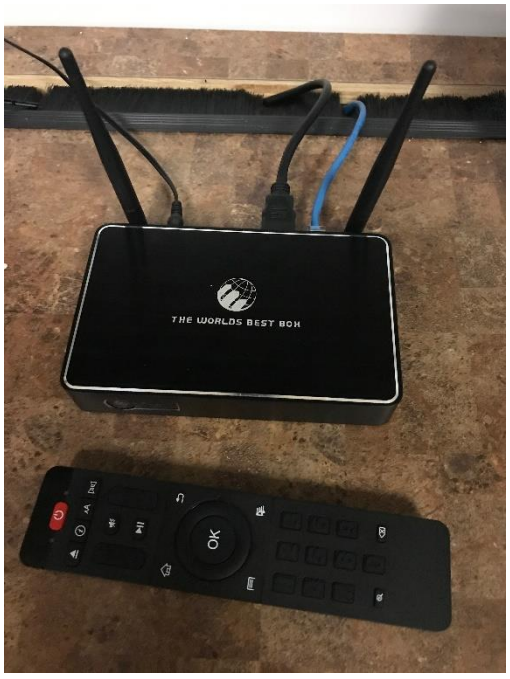
digitalcitizens alliance

DIGITAL CITIZENS ALLIANCE ALERT

BUYER BEWARE: "KODI BOXES" ARE CLOSED CAPTIONED FOR THE SECURITY IMPAIRED

HOW THE LEAKY SYSTEM OF ILLICIT STREAMING DEVICES POSES A MALWARE THREAT TO CONSUMERS

RAISING PUBLIC AWARENESS VITAL STEP TO COMBATTING HACKERS AND BAD ACTORS PREYING ON CONSUMERS



July, 2017

As consumers, we love new digital gadgets. Devices such as the iPhone or Galaxy or iPad not only excite us, they often change the way we behave. In recent years, one of the most exciting developments has been the introduction of devices that enable consumers to stream Internet-based content via a device that isn't associated with a traditional cable or satellite provider.

When new streaming devices, such as the Amazon Firestick and Apple TV, were first introduced, many were intrigued by the ease by which they could watch "over the top" content from the Internet, such as Netflix or Hulu on their living room televisions.

Since then, there has been a proliferation of other devices – many with an open-source media player known as "Kodi," which enables viewers to watch a wide range of movies and television shows from illegal sources through software add-ons. These devices are now generally identified as illicit streaming devices (ISDs) or nicknamed "Kodi boxes." They are often sold "pre-loaded" with add-on apps that provide the access to large-scale pirate sites and enable a user to easily stream live channels and on demand material from content theft websites.

But consumers need to be aware that these customized devices with add-ons for watching pirated content are as illegal as large-scale piracy sites. Kodi is working to distance itself from content thieves, discouraging piracy add-ons and praising Facebook for new policies prohibiting selling pre-loaded boxes that offer pirated content. Similarly, Amazon and eBay have banned sales of ISDs.

But many of these devices also have serious security issues. Digital Citizens Alliance warns consumers to be wary of these illicit streaming devices – or you may get more than just free content. Security experts have warned how hackers can exploit these devices to infect consumers' computers and other devices.

Recently, the security firm Check Point issued a warning that hackers were exploiting these devices to hack users. "We estimate there are approximately 200 million video players and streamers that currently run the vulnerable software, making this one of the most widespread, easily accessed and zero-resistance vulnerabilities reported in recent years," said a Check Point spokesperson, adding that Media Players VLC, Popcorn Time, and Stremio are also vulnerable to hacking.

Here's how this particular vulnerability works: As part of streaming movies and television content, pre-loaded "Kodi" boxes allow the user to search for subtitles that may be downloaded when the user wants to watch a movie in a foreign language.

Hackers have seized on this to create the vulnerability. By generating their own tampered language files and adding it to the un-curated directory of subtitle files, they are able to install malware on a user's system making it accessible to the hacker.

And the malware is unlikely to be discovered by the software because the file format of most caption files is typically viewed as non-threatening, and therefore, not analyzed as closely.

"These subtitles repositories are, in practice, treated as a trusted source by the user or media player," reported Check Point. "Our research also reveals that those repositories can be manipulated and be made to award the attacker's malicious subtitles a high score, which results in those specific subtitles being served to the user."

When news of this vulnerability became public, software makers updated the source code to prevent such vulnerabilities from happening via their own software. However, unlike devices manufactured by the major players, there is no mechanism by which to widely update the software in existing streaming devices. Also, many users may not be aware of the security update and therefore may be unaware of the vulnerability to their system.

The biggest challenge is that none of the players in the illicit streaming device ecosystem makes their users' security or privacy a priority. Participants in this underground industry typically point fingers at each other and have not yet stepped up to protect the safety and security of the consumer. That is vastly different than established providers such as Verizon or Apple who have a vested interest in a user's trust, and continued business.

And this is not the first security challenge for these devices. According to Android PC Review, in 2015 a security firm found that certain software was vulnerable to "man in the middle" attacks where a hacker seizes on a lack of security on how updates to software are handled to change code and install viruses onto a system.

The ISD community has been flippant when it comes to security. When posed with the issue of security, a United Kingdom-based developer responded:

"Whilst I fully understand what a malicious add-on could do, you cannot police people's stupidity and naïvety. It's up to the user to decide whether or not to install something and no matter how many warnings you give and how many hoops you make them jump through to do it, they will still install it. You can't have freedom of choice in a closed eco-system. Kodi offers a lot of freedom to do with it as you want and I personally don't want that to change because of a minority of idiots."

The worry for consumers is they may not even realize that illicit streaming devices pre-loaded with pirated content, or those that stream pirated content, are illegal. And that, in part, is the problem: we have gotten used to trusting our devices because they were associated with well-known brands. Unfortunately, disreputable actors are exploiting that trust to offer devices that can harm unknowing consumers.

The future of content on pre-loaded or illicit streaming devices is uncertain. In recent weeks several illegal add-ons have abruptly shut down. Given the security issues and add-on shutdowns, it's clear that consumers who spent

money on the devices may be getting malware and risk along with their "free content" – not what they expected.

Buyer Beware – Key Developments Consumers Should Be Aware of:

- Be careful from whom you make purchases. For years, Digital Citizens has warned consumers about making retail purchases from obscure online websites because they often don't have the same guarantees as well-known retailers. But recently, a growing number of websites have added bells and whistles to make themselves look legitimate. Consumers should not be fooled by slick looking sites or deceptive marketing telling you these pre-loaded boxes are "legal." Reputable online retailers such as Amazon and Facebook, for example, are taking steps to prevent the sale of these devices on their platforms.

- The add-ons market is in flux: Just last month, popular add-on providers and some popular add-ons have shut down without notice. The exit of some vendors who purposely and accidently allowed for dangerous activity opens the door to others who want to jump in the market. The illegal streaming market is ripe for opportunists looking to make a quick buck. While we'd say it's always dangerous to engage in this activity, it is particularly dangerous now.

- Law Enforcement is getting tough on those using Kodi illegally: Bad actors count on consumers being unaware of the dangers contained in some ISDs, but law enforcement agencies around the world are starting to focus on the problem. British authorities are aggressively going after individuals selling "fully-loaded" devices – or those that come "pre-loaded with third party plug-ins and add-ons that allow users to stream pirated content to their TV."[1] Several people have been arrested and police are committed to catching up with more.

Given the disperse nature of these devices and intended uses that are often unlawful, raising public awareness – both about specific vulnerabilities and the overall risks that occur when using unverified or untrusted devices or

[1] http://www.cornwalllive.com/kodi-boxese-this-is-what-official-piracy-experts-say-about-what-s-legal-and-what-s-not/story-30132149-detail/story.html

providers – is the first line of defense. There are many organizations that can help raise awareness:

- Consumer-focused groups should put out alerts to let their community know about the risks from illicit streaming devices.
- The Federal Trade Commission has both a wide reach and a wide range of tools to let consumers know about the threat and risks.
- State attorneys general, who often serve as the consumer protection function within their states, can play an important role in educating their citizens.

Hackers and bad actors rely on consumer confusion and lack of knowledge to be successful. That is why all those who care about protecting consumers must play a leading role in giving them their best defense: knowledge about online risks so they can steer clear.