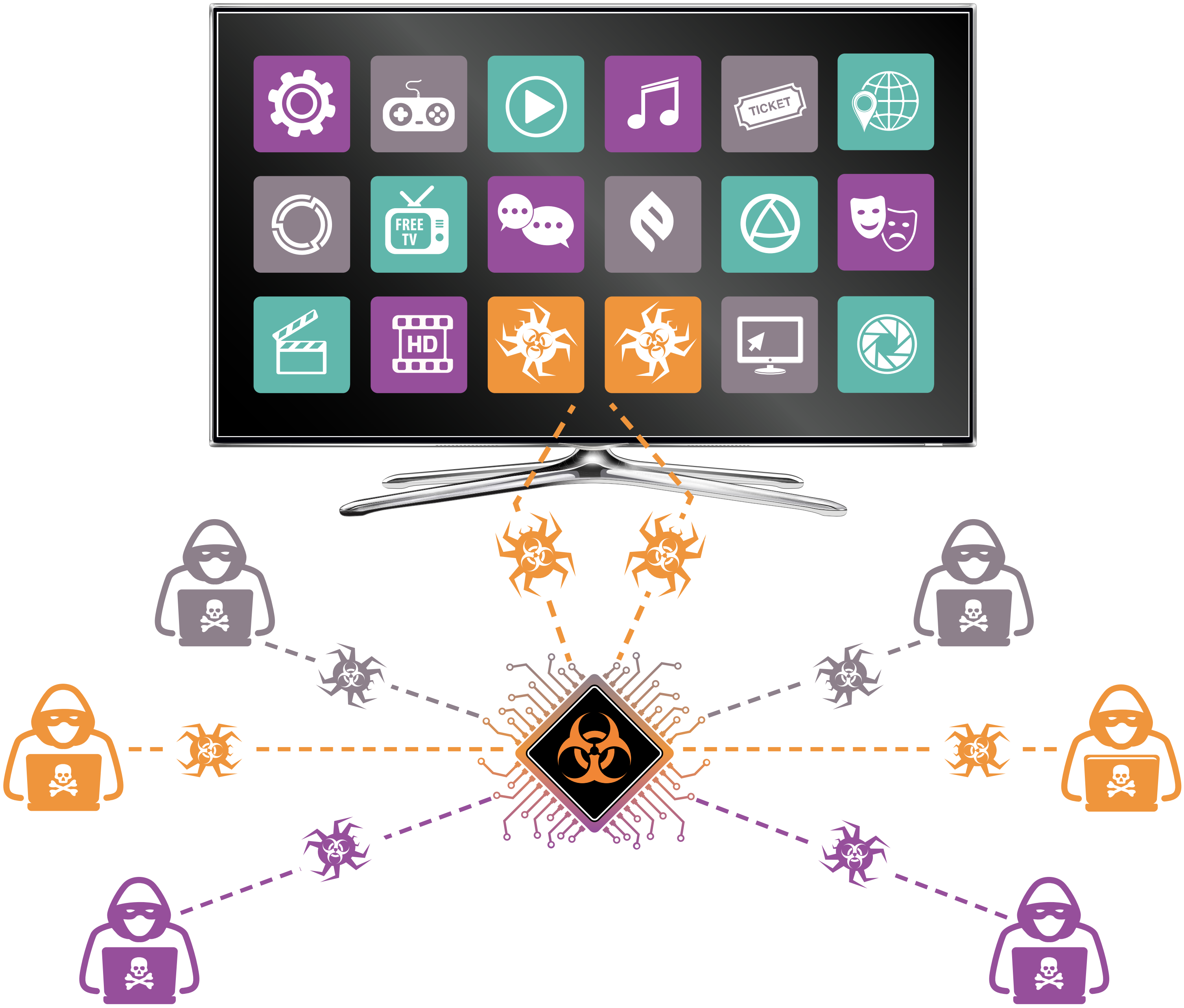
Fishing in the Piracy Stream: How the Dark Web of Entertainment is Exposing Consumers to Harm

Digital Citizens Investigation Finds Malware on Piracy Apps That Steal User Names and Passwords, Probe to Breach Networks, and Secretly Upload Data



APRIL 2019

digitalcitizens
alliance

Table of Contents

Executive Summary 3

The Streaming Piracy Ecosystem 7

Movies, Money, and Malware: How Piracy Apps Attack Companies and Consumers. 14

The Impact of Malware 17

Following a Pirate Playbook 19

Americans and Piracy Devices and Apps 22

Conclusion 23

Executive Summary

As consumers increasingly rely on streaming devices for their entertainment content, hackers are targeting the rogue market that offers illegal access to pirated movies and live programming to spread malware and exploit unsuspecting users, a Digital Citizens Alliance investigation has found.

During its probe, Digital Citizens' cybersecurity investigators observed malware from the piracy apps stealing user names and passwords, probing user networks and surreptitiously uploading data without consent. In addition, the investigation found an illegal scheme to monetize stolen Netflix accounts and ads for premium brands such as Amazon and Mini Cooper on pirate apps.

The 12 million active users of these illicit devices in North American homes present a tempting target because they offer hackers a new avenue to exploit consumers and a path to reach other devices on a home network. The findings should serve as a wake-up call for consumers, the technology community, and policymakers to take the threat seriously.

This cybersecurity threat is alarming because the users assist in the hack by "escorting" the hacker past vital network security. And it all starts so simply. A user purchases a device loaded with apps that offer free access, for example, to the latest movies in theaters or live broadcasts of Major League Baseball games. These devices – sometimes known as "Kodi boxes" or "jailbroken Fire TV Sticks" – look and behave like a Roku box, Apple TV or other legitimate device. But instead of accessing legitimate services like Netflix or Hulu, they link to pirate apps.

They are routinely purchased on online platforms such as Facebook Marketplace, Craigslist, or eBay for a one-time fee of $75 to $100. 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.

However, here's what most users don't know: by plugging the device into a home network, they 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. Like a trojan horse, the pirate apps are welcomed into the consumer's home because they purport to offer the gift of free content, only to use their position inside the walls to launch an attack – as evidenced by what Digital Citizens' researchers observed during 500 hours of laboratory testing.

Hackers benefit from the growing proliferation of these devices as well as consumers' lack of awareness of the risks. According to a Digital Citizens research survey of 2,073 Americans, 13 percent reported that they have a device that offers pirated content in their home. The majority of Americans (59 percent) said that "most consumers are probably unaware of the security risks that can occur when plugging one of these devices into a home network."

The lack of awareness about risks can have an impact. As part of its research survey, Digital Citizens asked Americans if they've had a problem with malware in the last 18 months. Of those who said they didn't have a piracy device in their home, 7 percent reported an issue with malware. Of those who said they did have a piracy device in their home, 44 percent reported an issue with malware. While there are multiple ways to get malware, this data suggests that engaging in risky behavior online, which includes plugging a rogue piracy device into a home network, substantially increases a person's digital security risk.

Of those who said they didn't have a piracy device in their home, 7 percent reported an issue with malware. Of those who said they did have a piracy device in their home, 44 percent reported an issue with malware.

The Digital Citizens investigation into so-called piracy apps on devices was conducted in conjunction with Dark Wolfe Consulting, a cybersecurity company that specializes in network and security, penetration testing, and targeted malware collection via honeynetting. The major findings of the investigation included the following:

- Researchers discovered malware on apps used to illegally watch movies, sports, and other content that came pre-loaded on devices.
- As soon as a researcher downloaded the ad-supported illicit movie and live sports streaming app "Mobdro," malware within the app forwarded the researcher's Wi-Fi network name and password to a server that appeared to be in Indonesia.
- Malware probed the researchers' network, searching for vulnerabilities that would enable it to access files and other devices. The malware uploaded, without permission, 1.5 terabytes of data from the researcher's device.
- Mobdro sought access to media content and other legitimate apps on the researcher's network.
- The 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.

- Compromised versions of streaming devices – including Amazon Fire TV Sticks and "Kodi boxes" – are being sold on mainstream digital marketplaces such as eBay, Craigslist, and Facebook Marketplace.
- Researchers found pirate apps supported by advertising, including ads for premium brands such as Amazon and Mini Cooper. The use of premium ads to both fund and legitimize criminal or rogue websites or apps is an ongoing cause of concern for the advertising industry as well as premium brands.

Digital Citizens also worked with cybersecurity firm GroupSense, which infiltrated Dark Web chatrooms where hackers discuss how to take advantage of vulnerabilities inherent in the pirate apps. The Dark Web discussions focused on using malware to exploit the computing power of the device (such as incorporate it into a botnet to later attack other computers or mine cryptocurrency) as well as how to access information that may be stored on the device, including photographs, passwords, and credit cards. Given that users rarely install anti-virus tools on such devices, the opportunities for exploitation are numerous.

While the threat is relatively new to illicit devices and pirate apps, the tactics follow a pattern that Digital Citizens found in prior piracy research: bait consumers with offers of free content, infect those that take the bait with malware, and steal vital personal information such as user names and passwords. In 2015, a Digital Citizens investigation found that 1 in 3 websites offering pirated content exposed consumers to malware that could steal personal and financial information and take over their computers to launch attacks.

Malware infecting piracy devices and apps is a serious problem because the service they provide is very popular. Canadian cybersecurity firm Sandvine found that almost 10 percent of the homes in North America are using a Kodi device.[1] This finding aligned with Digital Citizens polling that found 13 percent of U.S. respondents used an illicit streaming device.

Of the devices that Sandvine researched, almost 70 percent of Kodi boxes are re-purposed or "loaded" with add-ons configured to access unlicensed content. And the app repository "TV Addons" which runs on Kodi was reported to have roughly 12 million active users as of December 2018.[1]"

While piracy is obviously a concern for those who create entertainment content and those who distribute it legitimately, it is also a growing cybersecurity issue for consumers, government, and safety groups alike.

[1] https://www.tomsguide.com/us/amazon-fire-kodi-threat,news-27404.html

In June 2018, the tech website "tomsguide.com" reported that some 2,100 Amazon Fire TV sticks devices in the United States were "vulnerable because their owners have disabled basic security protections to install Kodi and other piracy-related streaming apps."[1]

That came on the heels of a 2017 alert from TV Addons (advocates of shady third-party piracy apps) that reported "there's a 99.99% chance that you have a huge security threat" if users were using a jailbroken Apple TV 2.[2] TV Addons also noted that the security flaw exposed users to "spam, DDoS, distribute malware or even something as disgusting as child pornography."

Also, 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.

Given the emerging cybersecurity risks of piracy, additional research into the potential impact of Kodi-enabled devices and piracy apps is needed. However, even given what we know already, steps should be taken to limit the risk. These include:

- Law enforcement should prioritize the investigation and prosecution of these criminal networks.
- Consumer protection agencies, both at the federal and state level, should warn consumers about the risks that illicit devices and piracy apps pose to their security and to their home devices.
- Government agencies and corporations should warn employees of the potential risks of using these devices over their networks, so they don't become a pathway to gain access to networks or steal sensitive information.
- Digital marketplaces such as eBay, Craigslist, and Facebook Marketplace should ban the sale of piracy devices.

Over the last decade, cybersecurity and consumer privacy have become national priorities. With millions of devices offering pirate apps in North America, the revelation that these devices are now a potential pathway for malware and other criminal schemes is deeply troubling. As tens of millions of new devices enter homes, steps must be taken to ensure that devices that can compromise both our security and our privacy don't slip in unnoticed.

[1] https://www.tomsguide.com/us/amazon-fire-kodi-threat,news-27404.html

[2] https://www.tvaddons.co/appletv2-jailbreak-threat/

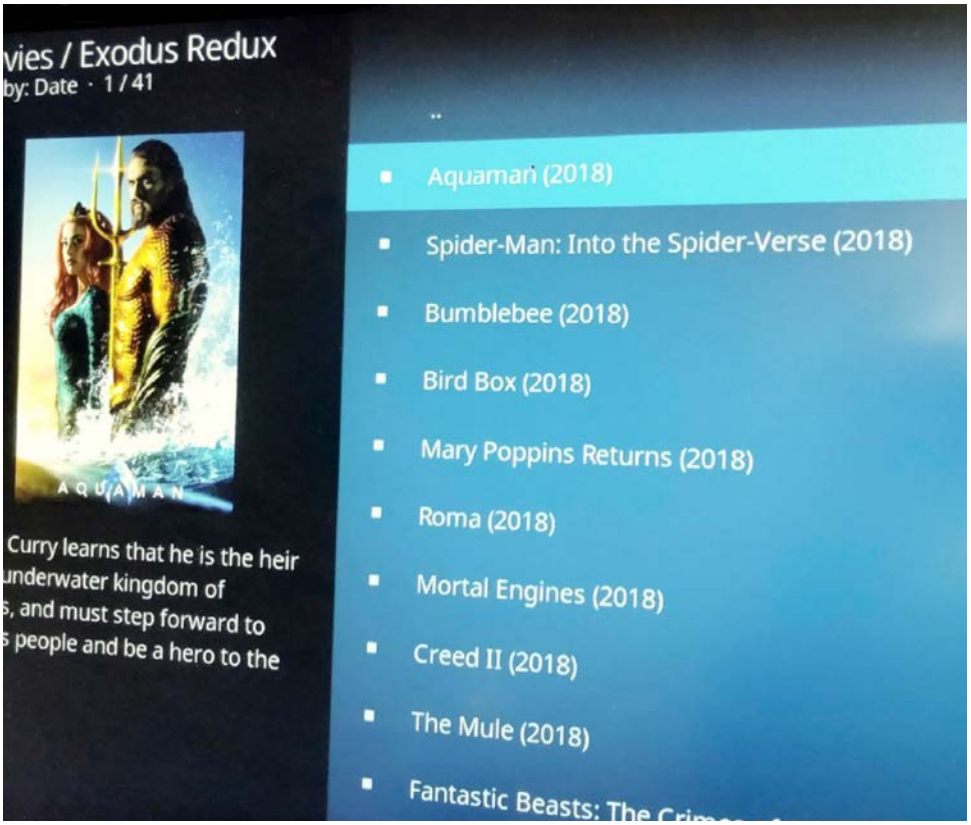
The Streaming Piracy Ecosystem

Seventy-five percent of Americans report that they stream entertainment at least several times per month. Most of that is done through reputable and well-known services such as Netflix, Amazon Prime Video, and Hulu. In less than a decade, roughly 250 million global subscribers have flocked to these services, and that number will jump when other major media companies introduce their own streaming services in the coming months. While no service is completely fool-proof, consumers have a justified expectation of safety with well-known brands.

Some consumers, however, take risky steps to go outside the mainstream app marketplaces to find their content. If you look at college dorm rooms, the man cave of a friend, or the bedroom of a teenager, you may find this underbelly of streaming: piracy devices like a jailbroken Amazon Fire TV stick or a so-called Kodi box, all powered by illicit apps.

In some cases, these piracy devices are set-top boxes – often imported from China – with little pre-installed software, which the device sellers load up with "Kodi" and apps that access the piracy ecosystem. In other cases, legitimate devices are "sideloaded" with software that allows illegal apps to be accessed as easily as legitimate apps like Netflix or Hulu. After loading the devices with the illegal apps (some of which are free and others require a subscription fee), the devices are sold to consumers at a substantial markup – often under some variation of the slogan: "Never pay for cable again."

However assembled, the devices are primarily used for one purpose: to illegally access pirated movies, TV shows, games, and even music. In some cases, they are used to gain access to movies that are still in theaters. Below is a screenshot of Aquaman from December 13, 2018, more than a week before it was released in the United States, on the app "Exodus Redux."



vies / Exodus Redux
by: Date · 1 / 41

..

- Aquaman (2018)
- Spider-Man: Into the Spider-Verse (2018)
- Bumblebee (2018)
- Bird Box (2018)
- Mary Poppins Returns (2018)
- Roma (2018)
- Mortal Engines (2018)
- Creed II (2018)
- The Mule (2018)
- Fantastic Beasts: The Crim

Curry learns that he is the heir
underwater kingdom of
s, and must step forward to
s people and be a hero to the

IMAGE 01
Exodus Redux

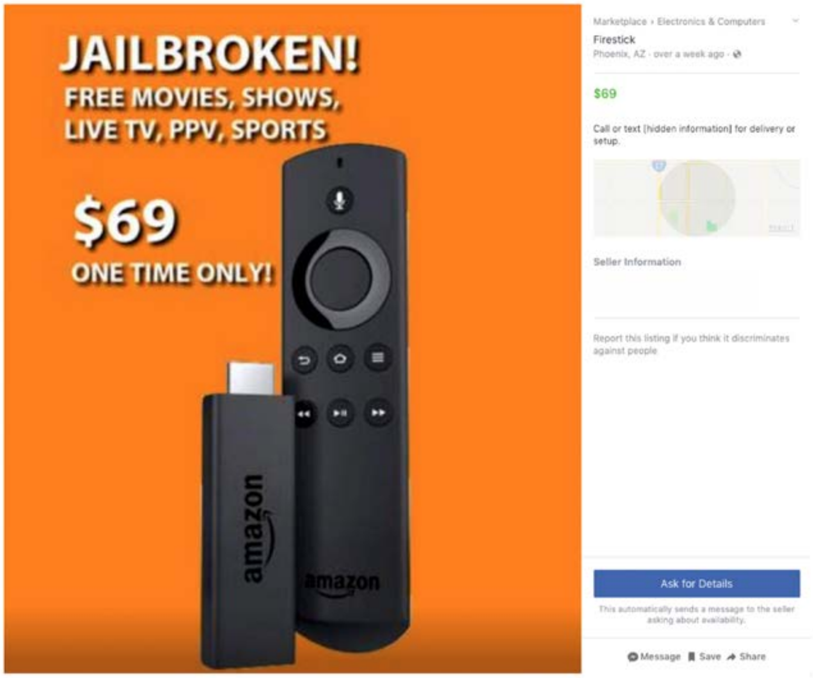
Piracy devices are not only a threat to the legitimate content ecosystem but also to cybersecurity overall. With millions of devices – from phones, tablets and entertainment devices to smart TVs, thermostats and doorbells – entering the home, the ability of hackers to infiltrate a home via these boxes is problematic.

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. For Android users, for example, disabling security features opens a specific port to the Internet that botnets routinely scan to find. Once detected, threat actors target the device for infection. Additionally, in order to use the apps, users often must give the app full administrator access, which includes permission to access the device's entire memory, along with its location and other security protections. Handing the keys to the device over to a creator of illegal apps exposes the user to a myriad of risks.

After initially ignoring complaints about how Kodi is susceptible to piracy, the XMBC Foundation, which oversees Kodi, denounced pirate add-ons because they give Kodi a bad name: “If you are selling a box on your website designed to trick users into thinking broken add-ons come from us and work perfectly, so you can make a buck, we’re going to do everything we can to stop you.”[3]

Given the rising concerns, Digital Citizens and Dark Wolfe launched an investigation. To explore the streaming piracy ecosystem, Dark Wolfe researchers acquired six streaming devices that use the Kodi platform. The sources of the purchases varied:

- Online purchases from sites found in searches on Google, Bing, and Dogpile.
- An ad on Craigslist that led Digital Citizens researchers to buy a device from a man who told them he was coming from the Department of Labor headquarters in Washington, D.C., to make the sale.
- A listing on Facebook Marketplace. The seller of that device, a Fire TV Stick, continued to reach out to the researcher after the sale, offering tips on how to access an upcoming UFC fight available on pay-per-view for no charge.



Marketplace › Electronics & Computers

Firestick

Phoenix, AZ · over a week ago ·

$69

Call or text [hidden information] for delivery or setup.

Seller Information

Report this listing if you think it discriminates against people

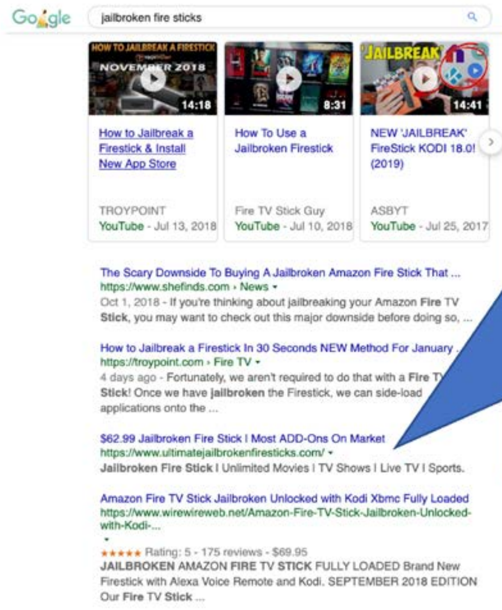
This automatically sends a message to the seller asking about availability.

IMAGE 02

A Jailbroken fire stick put up for sale on Facebook Marketplace

[3] Betzen, Nathan (February 14, 2016), The Piracy Box Sellers and YouTube Promoters Are Killing Kodi, Kodi News/Dev Journal

These devices are typically marketed as "pre-loaded" with apps that enable the user to access, for free or for a modest monthly subscription fee, on-demand movies (including those still in theatrical release) and television programs, as well as live real-time broadcast and cable entertainment, sports, and news channels from around the world. The apps, in turn, are often collected in pirate app repositories, called "repos," where users of illicit devices can "shop" for and download them.



jailbroken fire sticks

How to Jailbreak a Firestick & Install New App Store
TROYPOINT
YouTube - Jul 13, 2018

How To Use a Jailbroken Firestick
Fire TV Stick Guy
YouTube - Jul 10, 2018

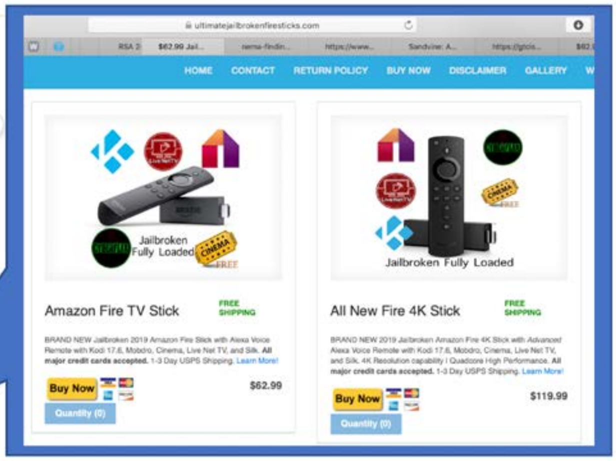
NEW 'JAILBREAK' FireStick KODI 18.0! (2019)
ASBYT
YouTube - Jul 25, 2017

The Scary Downside To Buying A Jailbroken Amazon Fire Stick That ...
https://www.shefinds.com › News ▾
Oct 1, 2018 - If you're thinking about jailbreaking your Amazon Fire TV Stick, you may want to check out this major downside before doing so, ...

How to Jailbreak a Firestick In 30 Seconds NEW Method For January ...
https://troypoint.com › Fire TV ▾
4 days ago - Fortunately, we aren't required to do that with a Fire TV Stick! Once we have jailbroken the Firestick, we can side-load applications onto the ...

$62.99 Jailbroken Fire Stick I Most ADD-Ons On Market
https://www.ultimatejailbrokenfiresticks.com/ ▾
Jailbroken Fire Stick I Unlimited Movies I TV Shows I Live TV I Sports.

Amazon Fire TV Stick Jailbroken Unlocked with Kodi Xbmc Fully Loaded
https://www.wirewireweb.net/Amazon-Fire-TV-Stick-Jailbroken-Unlocked-with-Kodi-...
▾
★★★★★ Rating: 5 - 175 reviews - $69.95
JAILBROKEN AMAZON FIRE TV STICK FULLY LOADED Brand New Firestick with Alexa Voice Remote and Kodi. SEPTEMBER 2018 EDITION Our Fire TV Stick ...



ultimatejailbrokenfiresticks.com

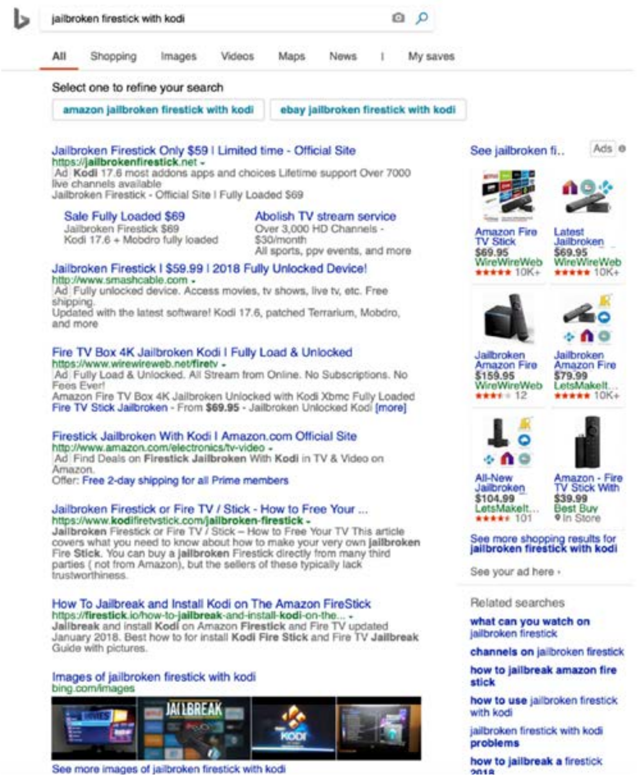
HOME CONTACT RETURN POLICY BUY NOW DISCLAIMER GALLERY

Amazon Fire TV Stick
FREE SHIPPING
BRAND NEW Jailbroken 2019 Amazon Fire Stick with Alexa Voice Remote with Kodi 17.6, Mobdro, Cinema, Live Net TV, and Silk. All major credit cards accepted. 1-3 Day USPS Shipping. Learn More!
$62.99

All New Fire 4K Stick
FREE SHIPPING
BRAND NEW 2019 Jailbroken Amazon Fire 4K Stick with Advanced Alexa Voice Remote with Kodi 17.6, Mobdro, Cinema, Live Net TV, and Silk. 4K Resolution capability I Quadcore High Performance. All major credit cards accepted. 1-3 Day USPS Shipping. Learn More!
$119.99

IMAGE 03

Searches for "jailbroken fire sticks" or "jailbroken fire sticks with kodi" revealed multiple websites pushing hacked firesticks.



jailbroken firestick with kodi

Select one to refine your search
amazon jailbroken firestick with kodi | ebay jailbroken firestick with kodi

Jailbroken Firestick Only $59 I Limited time - Official Site
https://jailbrokenfirestick.net ▾
Ad Kodi 17.6 most addons apps and choices Lifetime support Over 7000 live channels available
Jailbroken Firestick - Official Site I Fully Loaded $69

Sale Fully Loaded $69
Jailbroken Firestick $69
Kodi 17.6 + Mobdro fully loaded

Abolish TV stream service
Over 3,000 HD Channels - $30/month
All sports, ppv events, and more

Jailbroken Firestick I $59.99 I 2018 Fully Unlocked Device!
http://www.smashcable.com ▾
Ad Fully unlocked device. Access movies, tv shows, live tv, etc. Free shipping.
Updated with the latest software! Kodi 17.6, patched Terrarium, Mobdro, and more

Fire TV Box 4K Jailbroken Kodi I Fully Load & Unlocked
https://www.wirewireweb.net/firetv ▾
Ad Fully Load & Unlocked. All Stream from Online. No Subscriptions. No Fees Ever!
Amazon Fire TV Box 4K Jailbroken Unlocked with Kodi Xbmc Fully Loaded
Fire TV Stick Jailbroken - From $69.95 - Jailbroken Unlocked Kodi [more]

Firestick Jailbroken With Kodi I Amazon.com Official Site
http://www.amazon.com/electronics/tv-video ▾
Ad Find Deals on Firestick Jailbroken With Kodi in TV & Video on Amazon.
Offer: Free 2-day shipping for all Prime members

Jailbroken Firestick or Fire TV / Stick - How to Free Your ...
https://www.kodifiretvstick.com/jailbroken-firestick ▾
Jailbroken Firestick or Fire TV / Stick – How to Free Your TV This article covers what you need to know about how to make your very own jailbroken Fire Stick. You can buy a jailbroken Firestick directly from many third parties (not from Amazon), but the sellers of these typically lack trustworthiness.

How To Jailbreak and Install Kodi on The Amazon FireStick
https://firestick.io/how-to-jailbreak-and-install-kodi-on-the... ▾
Jailbreak and install Kodi on Amazon Firestick and Fire TV updated January 2018. Best how to for install Kodi Fire Stick and Fire TV Jailbreak Guide with pictures.

Images of jailbroken firestick with kodi
bing.com/images
See more images of jailbroken firestick with kodi

See jailbroken fi.. Ads

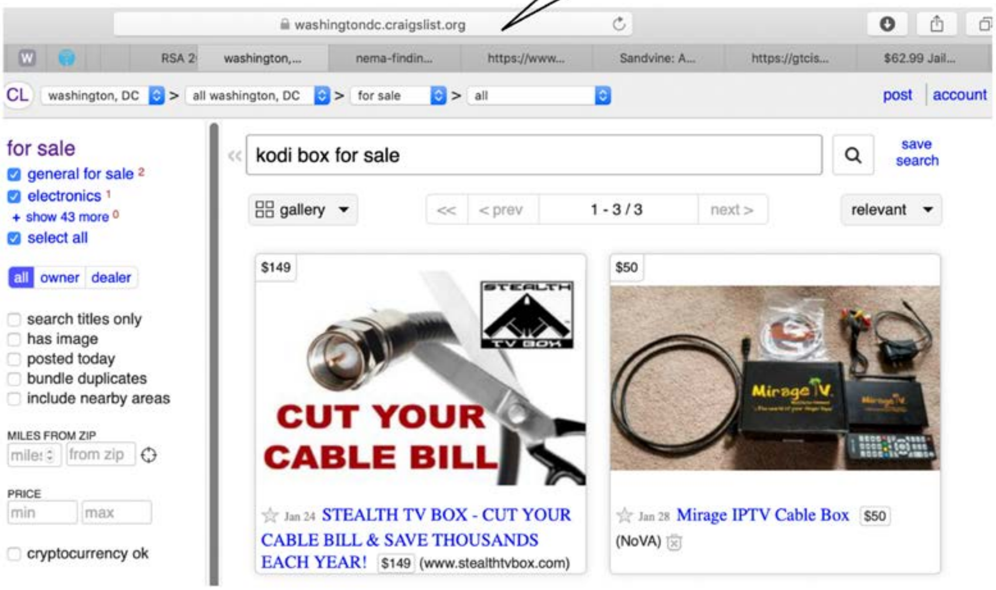
Amazon Fire TV Stick $69.95 WireWireWeb ★★★★★ 10K+	Latest Jailbroken $69.95 WireWireWeb ★★★★★ 10K+
Jailbroken Amazon Fire $159.95 WireWireWeb ★★★★ 12	Jailbroken Amazon Fire $79.99 LetsMakeIt... ★★★★★ 10K+
All-New Jailbroken $104.99 LetsMakeIt... ★★★★★ 101	Amazon - Fire TV Stick With $39.99 Best Buy In Store

See more shopping results for jailbroken firestick with kodi
See your ad here ›

Related searches
what can you watch on jailbroken firestick
channels on jailbroken firestick
how to jailbreak amazon fire stick
how to use jailbroken firestick with kodi
jailbroken firestick with kodi problems
how to jailbreak a firestick 2018

IMAGE 04

A listing on Craigslist led DCA researchers to a seller who said he worked at the Department of Labor. He met researchers on a street near the office, where the DCA researcher paid for the Amazon Firestick with cash.



washingtondc.craigslist.org

RSA 2 | washington,... | nema-findin... | https://www... | Sandvine: A... | https://gtcis... | $62.99 Jail...

CL washington, DC > all washington, DC > for sale > all — post | account

for sale

☑ general for sale 2
☑ electronics 1
+ show 43 more 0
☑ select all

all | owner | dealer

□ search titles only
□ has image
□ posted today
□ bundle duplicates
□ include nearby areas

MILES FROM ZIP: miles | from zip

PRICE: min | max

□ cryptocurrency ok

Search: kodi box for sale — save search

gallery | << | < prev | 1 - 3 / 3 | next > | relevant

$149 — ☆ Jan 24 STEALTH TV BOX - CUT YOUR CABLE BILL & SAVE THOUSANDS EACH YEAR! $149 (www.stealthtvbox.com)

$50 — ☆ Jan 28 Mirage IPTV Cable Box $50 (NoVA)

Below is an example of an ad for a device on eBay.

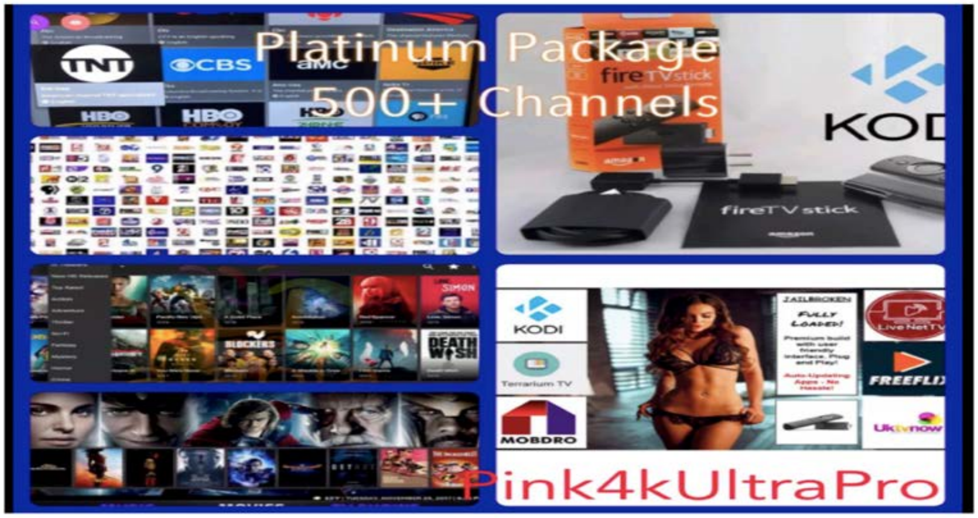
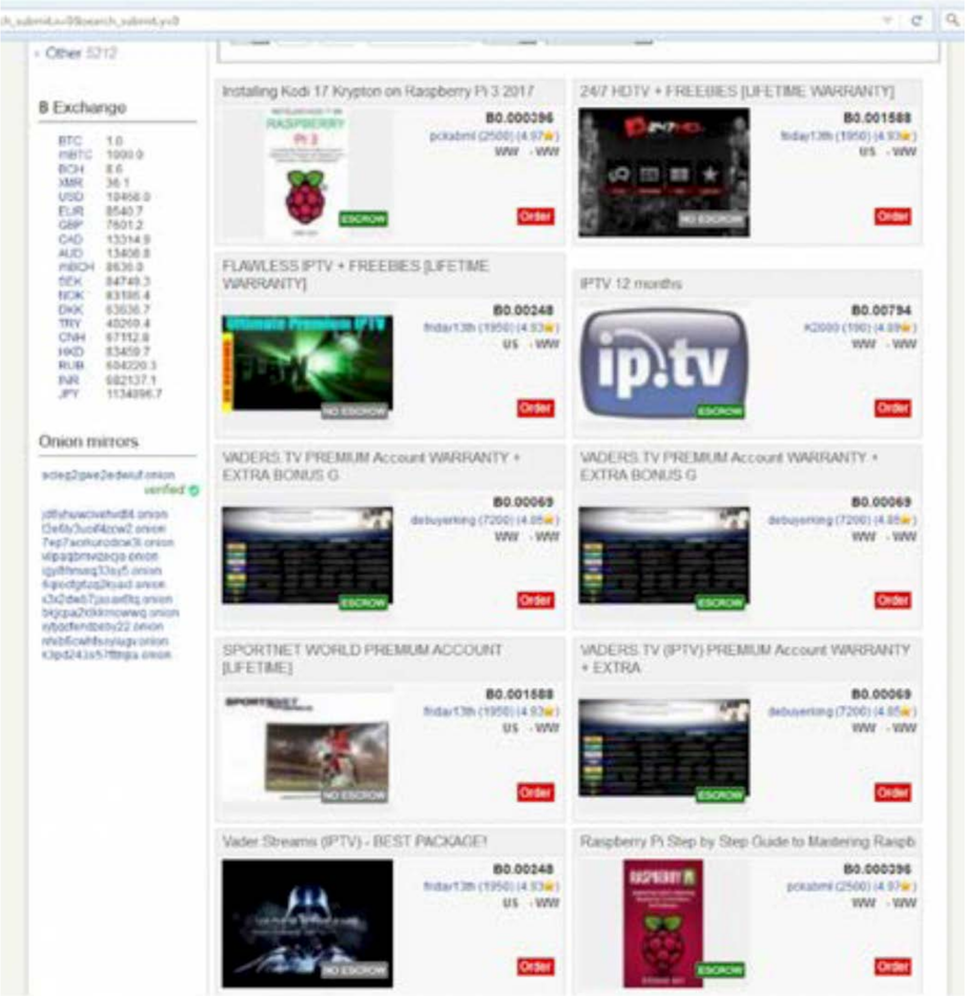


IMAGE 05

Jailbroken Fire Stick 2nd Gen.Fully Loaded With KODI 17.6 & much more!!!

These devices are also advertised (in a more straightforward manner) on Dark Web marketplaces. Sellers offer devices such as the “MXQ Pro fully loaded” that online reviewers forthrightly note come “with a complete set of Kodi builds that are considered illegal in most countries.”



Other 5212

B Exchange

BTC	1.0
mBTC	1000.0
BCH	8.6
XMR	36.1
USD	10468.0
EUR	8540.7
GBP	7601.2
CAD	13314.9
AUD	13406.8
mBCH	8636.0
SEK	84749.3
NOK	83186.4
DKK	63636.7
TRY	40269.4
CNH	67112.8
HKD	83459.7
RUB	604220.3
INR	682137.1
JPY	1134096.7

Onion mirrors

sdeg2gwe2edeiuf.onion verified

jdfshuwcivehvd84.onion
l3e6b3uof4zcw2.onion
7ep7acrkurodcie3l.onion
vlpaqbrwvzeqa.onion
igy8hnueq33uy5.onion
6qiodtgtzq2kuad.onion
x3x2dwb7jasawi8tq.onion
bkjcpa2rdkkmowwq.onion
iybodfendbeby22.onion
nhb6cwhfsylugv.onion
k3pd243s57ttnpa.onion

Installing Kodi 17 Krypton on Raspberry Pi 3 2017
B0.000396
pckabml (2500) (4.97★)
WW - WW
ESCROW
Order

24/7 HDTV + FREEBIES [LIFETIME WARRANTY]
B0.001588
friday13th (1950) (4.93★)
US - WW
NO ESCROW
Order

FLAWLESS IPTV + FREEBIES [LIFETIME WARRANTY]
B0.00248
friday13th (1950) (4.93★)
US - WW
NO ESCROW
Order

IPTV 12 months
B0.00794
K2000 (190) (4.89★)
WW - WW
ESCROW
Order

VADERS TV PREMIUM Account WARRANTY + EXTRA BONUS G
B0.00069
debuyerking (7200) (4.85★)
WW - WW
ESCROW
Order

VADERS TV PREMIUM Account WARRANTY + EXTRA BONUS G
B0.00069
debuyerking (7200) (4.85★)
WW - WW
ESCROW
Order

SPORTNET WORLD PREMIUM ACCOUNT [LIFETIME]
B0.001588
friday13th (1950) (4.93★)
US - WW
NO ESCROW
Order

VADERS TV (IPTV) PREMIUM Account WARRANTY + EXTRA
B0.00069
debuyerking (7200) (4.85★)
WW - WW
ESCROW
Order

Vader Streams (IPTV) - BEST PACKAGE!
B0.00248
friday13th (1950) (4.93★)
US - WW
NO ESCROW
Order

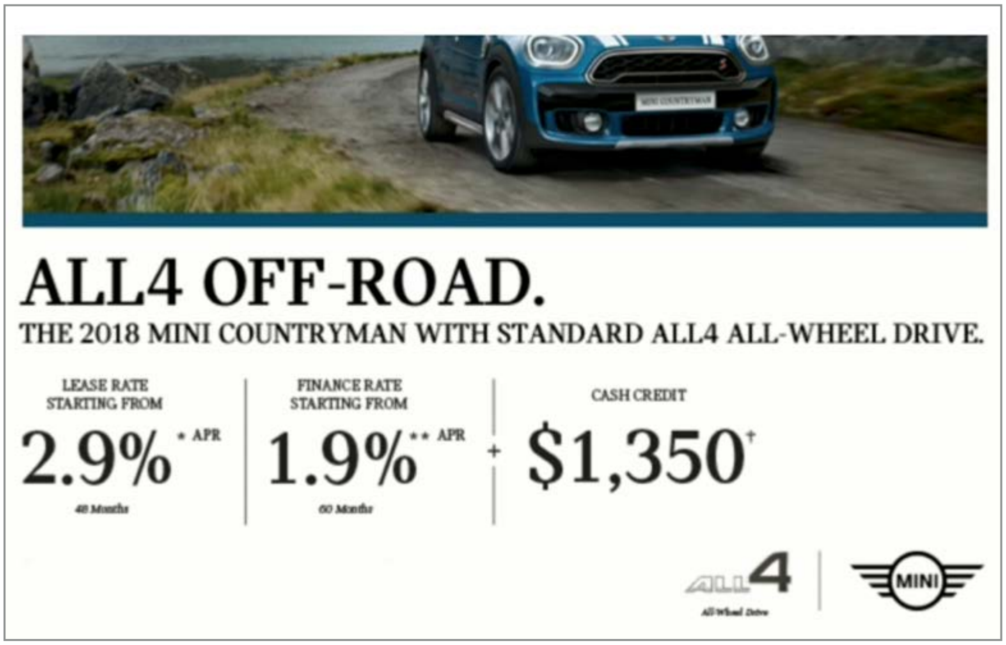
Raspberry Pi Step by Step Guide to Mastering Raspb
B0.000396
pckabml (2500) (4.97★)
WW - WW
ESCROW
Order

IMAGE 06

Dream Market and “rstforums,” well-established underground markets, have dozens of posts selling piracy devices. Dream Market is a Dark Web underground marketplace where a variety of illegal products are for sale – including drugs, counterfeit money, guns, and fake credit cards.

Another component of the piracy streaming ecosystem is advertising. As Digital Citizens found with piracy websites, bad actors incorporate mainstream advertising into their offerings. In doing so, they create a potential new revenue stream as well as create the impression that premium brands are comfortable being associated with their shady dealings.

Among the advertising researchers found on webpages offering illegal and/or illicit content were ads for Mini Cooper.



ALL4 OFF-ROAD.

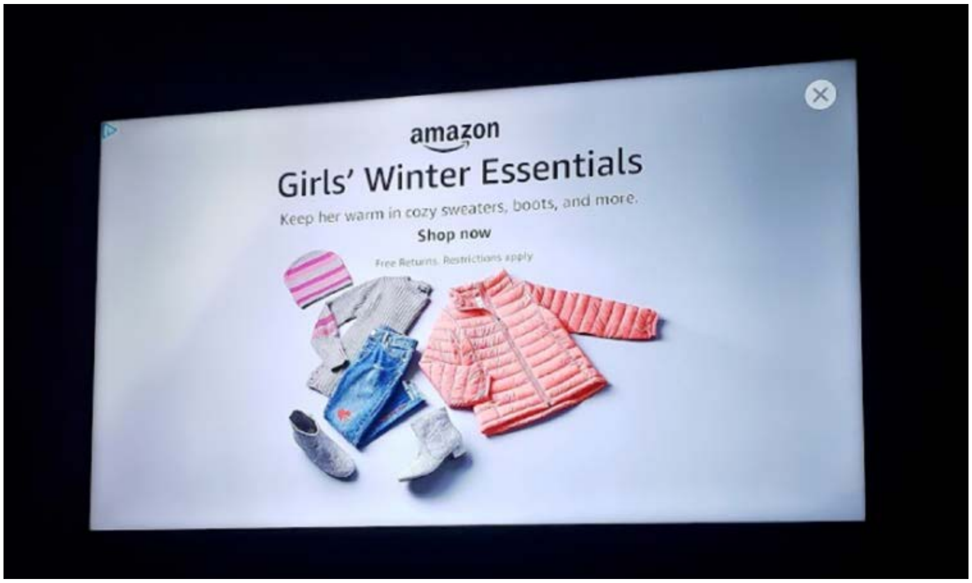
THE 2018 MINI COUNTRYMAN WITH STANDARD ALL4 ALL-WHEEL DRIVE.

LEASE RATE STARTING FROM 2.9%* APR 48 Months | FINANCE RATE STARTING FROM 1.9%** APR 60 Months + CASH CREDIT $1,350†

IMAGE 07

Researchers found this ad for Mini Coopers on Mobdro. Ads like this one show up when viewers are switching from one channel to another. The ads run for approximately 27 seconds and viewers can't skip them. Some adblockers may stop the ads, but Dark Wolfe researchers said, "they weren't always successful."

In addition, the following Amazon ad was found on multiple piracy apps.



amazon

Girls' Winter Essentials

Keep her warm in cozy sweaters, boots, and more.

Shop now

Free Returns. Restrictions apply

IMAGE 08

Dark Wolfe research found Amazon ads while using apps Mobdro and other pirate apps.

Dark Wolfe researchers noted that while some piracy advocates promote the "benefits" of free content – UFC fights, live sporting events, more movies – they do not warn users about the potential malware threat. That is disturbing given that this software is popular with threat actors because it allows them to deliver malware through the content.

Movies, Money, and Malware: How Piracy Apps Attack Companies and Consumers

The revelation that criminals are targeting these devices and pirate apps to install malware is a new breach in the effort to keep consumers safe. The Digital Citizens investigation found that rogue content theft apps downloaded to streaming devices expose users to a much higher risk of malware infestation on the home network. Access to these devices gives threat actors the chance to steal anything the device is linked to, including services such as Netflix and Amazon accounts.

The malware looks for a pathway to any connected device, putting an entire home network at risk. Expanding the infection vectors (the pathways from an attacker's computer into connected devices on a user's network - such as a child's tablet, a newer refrigerator or a computer) increases the likelihood of data theft.

The malware Dark Wolfe researchers identified came from apps that were either received infected, infected via updates, or infected via the stream. Once "in the network," malware will add any locally stored media it finds in a user's network of interconnected devices and make it part of its catalog of media, including the user's movies, pictures, images, and applications. Even if the illicit device is later removed from the home system, malware that has already infected adjacent systems will stay within the user's network.

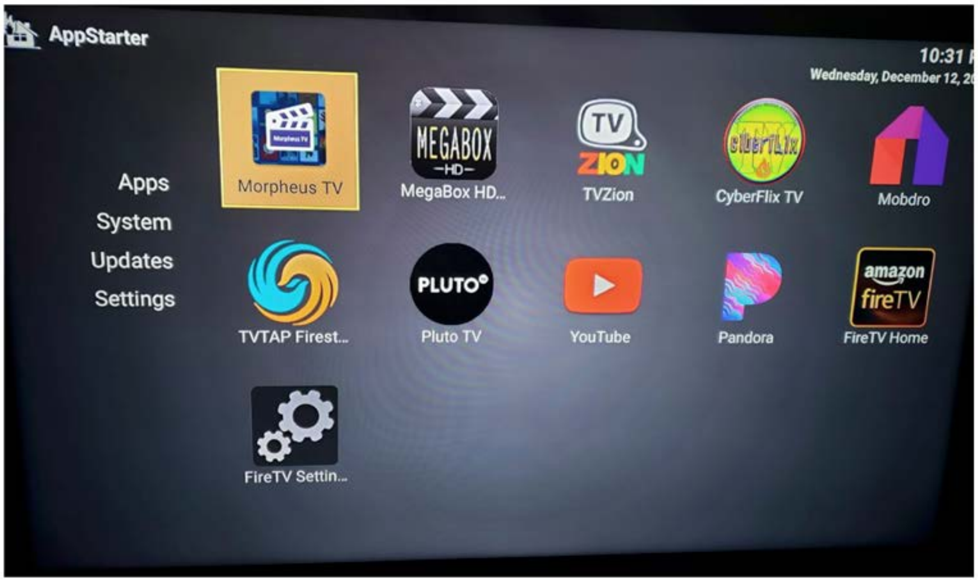


IMAGE 9

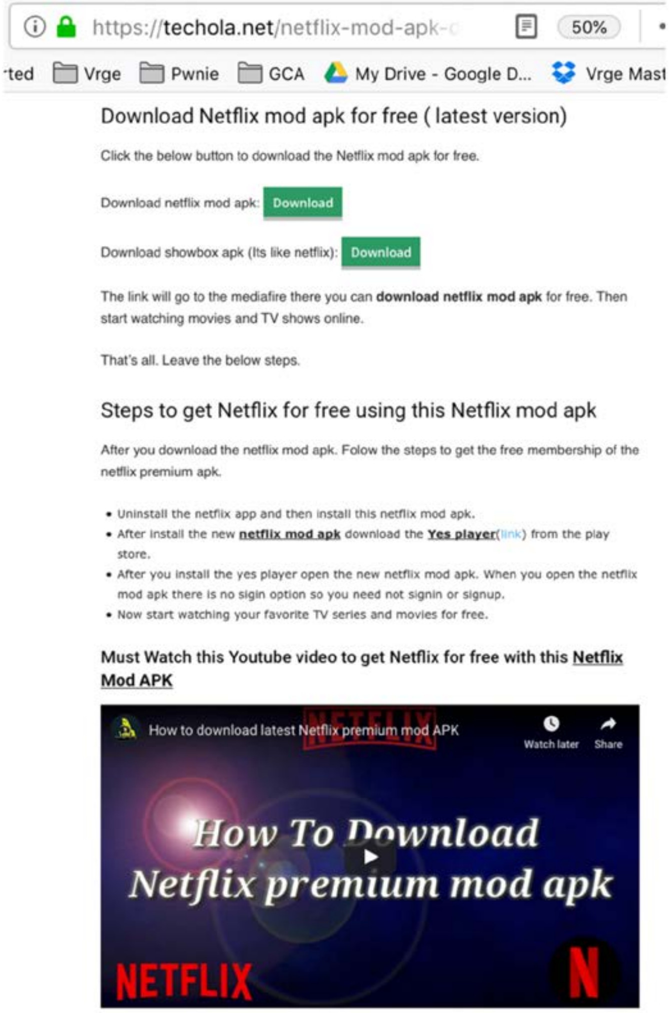
Above is the Kodi container with apps Dark Wolfe researchers downloaded from torrents and websites offering free movies. The researchers noticed unusual activity from the app Mobdro (top right corner) when it was launched and immediately updated with no permission granted from the user. The researchers noticed the app was receiving commands from the free movie streams, which could facilitate installing more malware, updating firmware, and installing more apps to Kodi – again with no permission from the user. Researchers found malware on their network as a result of Mobdro's malicious behavior.

Investigators identified two ways criminals can monetize the stolen credentials and pad their own pockets while taking money from law-abiding consumers and businesses. The first is by selling a legitimate user's credentials. Counterfeit Netflix apps, like "FreeNetflix," facilitate illegal access to a legitimate subscription, allowing a person shopping for unlicensed content to access a legitimate user's pirated subscription. Researchers observed FreeNetflix's operators offering the service for a one time, $10 payment that includes the app and one year's worth of updates. Updates in this case include more than just revisions to the app. When updated, the pirated credentials may also be rotated – meaning illegal users are switched from one legitimate subscription to another legitimate subscription.

Rotating credentials help rogue app operators prevent several possible problems, including the possible overuse of a single legitimate user's subscription by multiple illegitimate users at once. That avoids repeatedly interrupting the service of legitimate users, therefore reducing forced outages, password changes, and account lockouts.

IMAGE 10

Researchers found "FreeNetflix" offered on websites offering subscriptions, costing between $10-$20 dollars, for one year with free "updates." During the update, what engineers call "rotating credentials" takes place, meaning that criminal operators of the fake app swap one set of stolen credentials for another.



Download Netflix mod apk for free (latest version)

Click the below button to download the Netflix mod apk for free.

Download netflix mod apk: Download

Download showbox apk (Its like netflix): Download

The link will go to the mediafire there you can **download netflix mod apk** for free. Then start watching movies and TV shows online.

That's all. Leave the below steps.

Steps to get Netflix for free using this Netflix mod apk

After you download the netflix mod apk. Folow the steps to get the free membership of the netflix premium apk.

- Uninstall the netflix app and then install this netflix mod apk.
- After install the new **netflix mod apk** download the **Yes player**(link) from the play store.
- After you install the yes player open the new netflix mod apk. When you open the netflix mod apk there is no sigin option so you need not signin or signup.
- Now start watching your favorite TV series and movies for free.

Must Watch this Youtube video to get Netflix for free with this Netflix Mod APK

IMAGE 11

This is an example of a counterfeit Netflix advertisement with instructions.

Second, the content on these counterfeit Netflix apps included advertising, which likely created an additional stream of revenue for the criminal operators.

Counterfeit Netflix apps also augment the legitimate Netflix streams, providing additional content not found on Netflix's own app, including pirated streams of sporting events, music, games, and even some homegrown content, making them highly desirable and pulling business away from licensed streaming services.

Counterfeit Netflix apps also augment the legitimate Netflix streams, providing additional content not found on Netflix's own app, including pirated streams of sporting events, music, games, and even some homegrown content, making them highly desirable and pulling business away from licensed streaming services.

Other researchers have discovered that third-party add-ons for Kodi were used to distribute Linux and Windows cryptocurrency-mining malware. "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," reported security company ESET in a September 2018 report.

While the sources of the malware were defunct or no longer spreading malware, ESET warned that "unwitting victims" who had the cryptominer malware surreptitiously installed on their devices were likely still affected.

The Impact of Malware

Piracy devices are particularly vulnerable to malware because typical security protections are rarely installed or are disabled to enable piracy streaming apps. The devices have significantly more "attack vectors" than other connected devices, such as smart TVs or refrigerators, increasing the risk that hackers can access user names or passwords for anything that the device is connected to, such as Netflix accounts, Amazon accounts or anything else added to the system.

Here's how it typically 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."

For example, moments after a Dark Wolfe researcher downloaded the rogue movie and live sports streaming app Mobdro, it forwarded the researcher's Wi-Fi network name and password to a server that appeared to be in Indonesia. Researchers point out that the final destination is murky because the threat actors could be using a Virtual Private Network that shrouds their actual location. As soon as the app was launched, the researcher reported that the app forced an update. Then, Mobdro started to seek access to media content and other legitimate apps on the researcher's network.

One finding from Dark Wolfe is particularly troubling – after the initial update, the device accepted commands from a threat actor. Those commands may come from the app itself or from the movie streams. With each selection of content, the user opens the door to a new set of commands and malicious payloads from a threat actor to a device in use. This could include anything from commands to perform an update to pull down more malware, to participate in a DDoS attack, or to pull items stored on the device – like pictures, movies, documents - or any similar content available on devices connected to a network.

With these tools, the threat actor not only has full access to the unsecured data but can literally login into a user's device as if he or she were in front of it. The threat actor can navigate from that device to the Internet and pose as the user.

The commands in the apps or from the movie streams that Dark Wolfe found were either encrypted or encoded, making it difficult to analyze for infection. This demonstrates the threat actors have both sophistication and purpose.

The commands in the apps or from the movie streams that Dark Wolfe found were either encrypted or encoded, making it difficult to analyze for infection. This demonstrates the threat actors have both sophistication and purpose. This highly complex form of delivering malware into an ecosystem reflects criminal professionalism. Using updates and streamed content pulled from arbitrary sources could, potentially, be used to evade detection even from mainstream app marketplaces with highly developed security systems, like Apple's App Store and Google Play.

Once installed, the app checks or monitors for updates. Then, the malware from the apps detonates. Researchers observed that the app that sent the user's wireless name and password up to an external server in Indonesia then began probing the network and talking to any file-sharing services on the Local Area Network. It also "port knocked," a process to look for other active malware.

The app was also ingesting the stream data that was encoded or encrypted (depending on which app was under evaluation – both of these types of obfuscation were found). Streams could contain commands that enabled hackers to control the app remotely. If the app is running on a jailbroken device, the app could surreptitiously pull audio and video from a smart TV. The commands could also tell the app to update from another source, pulling down more malware functionality. This is an easy way for hackers to invade networks and evade security.

Digital Citizens researchers observed instances where unlicensed movies and TV shows are used as a lure, getting users to download applications that infect their devices. The research found that the content is not only a lure, but also used to control and manipulate devices connected to a user's network.

Following a Pirate Playbook

What researchers discovered reflects a common modus operandi used by hackers. In previous reports on ad-supported pirate websites, DCA and cybersecurity research firm RiskIQ reported on partnerships showing Dark Web discussions where pirate operators negotiate with threat actors on the price of malware installations. The research did not delve into how much the threat actors are profiting from both ads and infections, but it's clear that the networks both exist and can produce additional millions in revenue.

What hackers discuss on the Dark Web is often a leading indicator of the threats consumers will confront in the future. To understand what may be coming next, analysts from the cybersecurity firm GroupSense prowled the Dark Web to understand what threat actors are talking about as their next exploits.

Some of the discussion on the Dark Web focused on using the malware to exploit the computing power of the device (such as to attack other computers), or how to access information that may be stored on the device itself (including photographs, passwords, and credit cards). The investigators discovered that threat actors see an opportunity to modify piracy apps to reveal the user names and passwords that users chose to access their devices and the content on those devices.

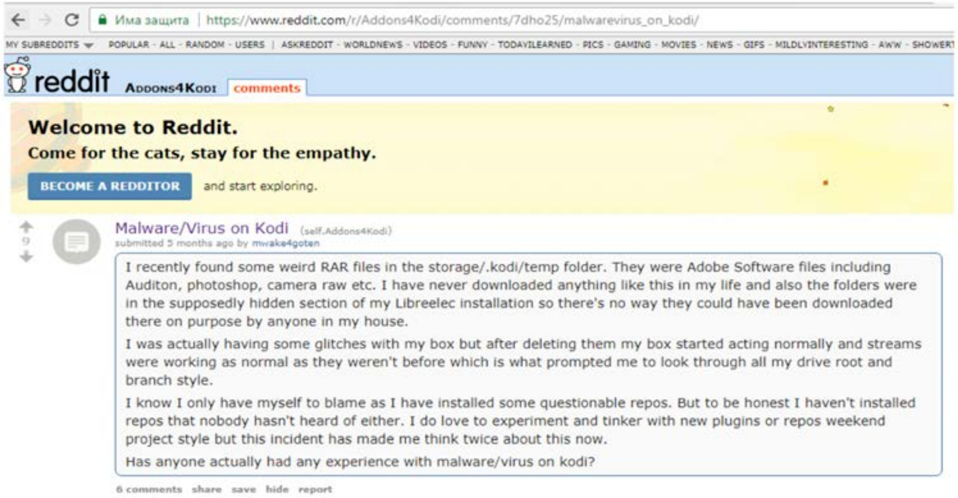
This is disturbing because many Internet users rely on a single user name and password across multiple devices, platforms and websites. Assume that “sallyjennings” uses the same “ilovedogs123!” password for her piracy device as well as her computer and home Wi-Fi network.

On the Dark Web, GroupSense found specific examples of would-be threat actors searching for malware tools targeting Kodi. These exploits included:

- An exploit tool named “17.0 Local File Inclusion” that enables threat actors to access a user’s content on a Kodi box, which can also include personal photographs and videos and other media files.
- An exploit tool named “Kodi 15 Arbitrary File Access” that allows threat actors to exploit a security vulnerability to access sensitive information on a user’s device.
- A distributed denial of service (DDoS) virus named “Kodi Web Server 16.1” that enables a threat actor to launch an attack on Kodi boxes using a user’s network and bandwidth.

In looking at the risks of the malware associated with these devices, GroupSense found the following threats to consumers associated with threat actors targeting piracy apps:

- Attacks that enable a threat actor to intercept and monitor traffic. Called a “man-in-the-middle attack,” a user thinks he or she is connecting, for example, to a legitimate service to pay by credit card, but in fact a malicious person is watching the connection. This allows for passwords, credit cards, and other information to be stolen.
- Kodi add-ons also expose users to malware that gives threat actors access to all forms of content either on or accessed through Kodi. Because Kodi is used by many consumers as a “media organizer,” they may often access personal pictures and videos through their Kodi-powered devices. And as these devices become more sophisticated, they are likely to be used as a portal to access other personal content.


Има защита | https://www.reddit.com/r/Addons4Kodi/comments/7dho25/malwarevirus_on_kodi/
MY SUBREDDITS
POPULAR - ALL - RANDOM - USERS | ASKREDDIT - WORLDNEWS - VIDEOS - FUNNY - TODAYILEARNED - PICS - GAMING - MOVIES - NEWS - GIFS - MILDLYINTERESTING - AWW - SHOWER
reddit
Addons4Kodi
comments
BECOME A REDDITOR
9
6 comments share save hide report

Welcome to Reddit.

Come for the cats, stay for the empathy.

and start exploring.

Malware/Virus on Kodi (self.Addons4Kodi)

submitted 5 months ago by mwake4goten

I recently found some weird RAR files in the storage/.kodi/temp folder. They were Adobe Software files including Auditon, photoshop, camera raw etc. I have never downloaded anything like this in my life and also the folders were in the supposedly hidden section of my Libreelec installation so there's no way they could have been downloaded there on purpose by anyone in my house.

I was actually having some glitches with my box but after deleting them my box started acting normally and streams were working as normal as they weren't before which is what prompted me to look through all my drive root and branch style.

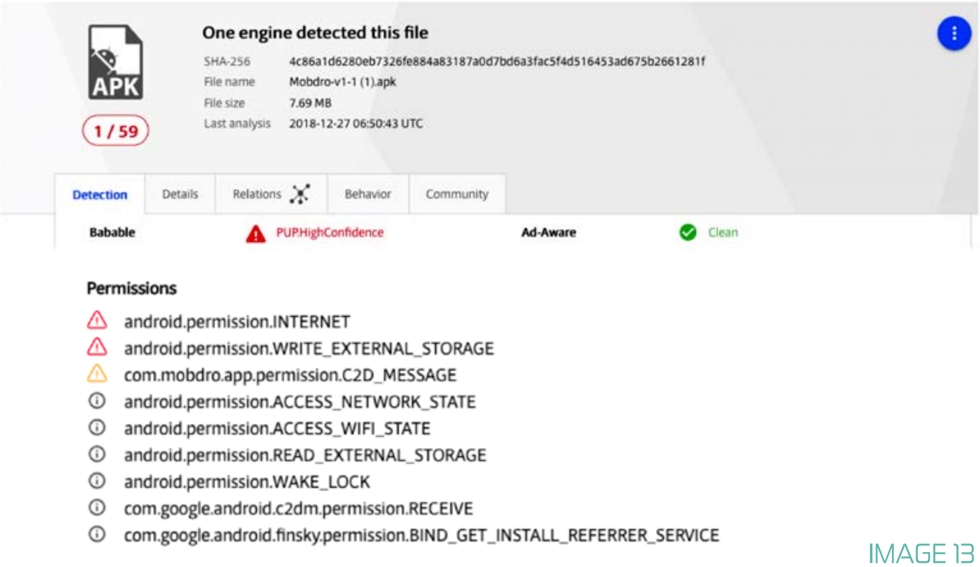
I know I only have myself to blame as I have installed some questionable repos. But to be honest I haven't installed repos that nobody hasn't heard of either. I do love to experiment and tinker with new plugins or repos weekend project style but this incident has made me think twice about this now.

Has anyone actually had any experience with malware/virus on kodi?

IMAGE 12

In the case above, a Kodi user, under the title "Malware/Virus on Kodi", reports suspicious files added to his device after downloading add-ons. Backdoor viruses can be difficult to fully remove from a device.

The malware Dark Wolfe discovered in the rogue apps sought permission to grant access to other Android apps, which the researcher – who creates and teaches reverse engineering for Android apps - had never before seen. Researchers also found rogue apps, coming from videos downloaded from either torrents or websites operated outside of the United States, delivered highly invasive malware that "port knocked," looking for other malware.



One engine detected this file

SHA-256 4c86a1d6280eb7326fe884a83187a0d7bd6a3fac5f4d516453ad675b2661281f

File name Mobdro-v1-1 (1).apk

File size 7.69 MB

Last analysis 2018-12-27 06:50:43 UTC

Babable	⚠ PUP.HighConfidence	Ad-Aware	✓ Clean

Permissions

⚠ android.permission.INTERNET
⚠ android.permission.WRITE_EXTERNAL_STORAGE
⚠ com.mobdro.app.permission.C2D_MESSAGE
ⓘ android.permission.ACCESS_NETWORK_STATE
ⓘ android.permission.ACCESS_WIFI_STATE
ⓘ android.permission.READ_EXTERNAL_STORAGE
ⓘ android.permission.WAKE_LOCK
ⓘ com.google.android.c2dm.permission.RECEIVE
ⓘ com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

IMAGE 13

That means they searched for other movie sources and files on the researchers' network and "talked" with the TVs on the network. Dark Wolfe researchers noted that "legitimate software doesn't do things like that. This is also indicative of a piece of a very complex malware ecosystem."

In the future, DCA researchers hope to do research similar to our earlier Digital Bait report that showed how content thieves work with malware makers to make millions of dollars. Our future research would pick up from our findings here, examining how pirate app developers also make money spreading malware.

Americans and Piracy Devices and Apps

Over the last five years, piracy devices and apps have moved from the fringe towards the mainstream. According to the Digital Citizens research survey, 13 percent of Americans report having a piracy device in the home. That number would be generally consistent with what the research firm Sandvine reported for device usage in North America.

But even though a majority of Americans are somewhat familiar with these devices, they aren't familiar with how they work or the risks they could pose. According to the survey, 59 percent said, "most consumers are probably unaware of the security risks that can occur when plugging one of these devices into a home network, and if they did know, they would be much less likely to allow them in their home."

Given that, the finding that those who have a device that accesses piracy apps in their homes are six times more likely to have dealt with a malware issue in the last 18 months is not surprising. While we stress that the data cannot prove that the malware came from using a device with piracy apps, it underscores the challenges of risky behavior online. The fact that 44 percent of those with a piracy device experienced a problem with malware should not be overlooked.

The research survey data also offers hope for consumer protection arms of government, such as the Federal Trade Commission and state attorneys general, that awareness campaigns can be an effective tool.

The survey found that Americans respond to information that lays out the risks of these devices:

- 81 percent said Americans should be concerned about an unverified box that by being plugged into a home network bypasses a good portion of home security, such as a firewall.
- 75 percent said that if having a device that offered illegal apps to access pirated content could leave them more vulnerable to malware that could compromise their network, they wouldn't allow one of them in their home because of the risks.
- 70 percent said they are concerned that a so-called Kodi box or jailbroken Fire TV Stick do not prioritize security or police what apps can go on the devices in the same way that established companies such as Apple or Roku do.

Given that the growth of streaming is likely to spur a larger market for piracy devices and apps – and attract the attention of criminals and hackers who flow to where the action and money is – it's imperative that we both learn more about Americans' attitudes about their entertainment choices and raise awareness about the risks of unverified devices.

Conclusion

The streaming piracy ecosystem is built on making money from stealing, selling, and weaponizing pirated movies, TV shows, sporting events, games, and music. Often uninformed of the risks, users of this software are baited into trying something they think is free or cheap but comes with a hidden cost: malware.

In addition, the multiple online conversations about how to infect Kodi add-ons and business model discussions about how to profit are red flags that signal that the problem will grow if left unaddressed.

For that reason, Digital Citizens calls for the following actions:

- Enhanced law enforcement attention to the distributors of piracy devices and apps.
- Action from mainstream resellers including Amazon, eBay, Facebook Marketplace, and Craigslist cracking down on ads promoting jailbroken and/or fully loaded streaming devices.

- Ad agencies stepping up to make sure their client's ads don't show up on ad-supported app shadow sites.
- Support from regulators and lawmakers to crack down on black hat threat actors profiting from developing malware and exotic delivery systems designed specifically to deceive consumers.
- Support for the cybersecurity researchers shedding light on this criminal activity and protection for those doing work to educate consumers and support law enforcement.
- Pressure on free and/or cheap storage sites that enable the malware business to be so profitable.

But first and foremost, it starts with consumers. People using piracy apps and jailbroken and/or fully loaded devices need to know that security and privacy are not a concern of those who sell piracy devices. Even worse, the business model for many is banking on offering add-ons primed for malware and invading networks. Until other remedies are taken, consumers must be careful about what devices they invite into their homes.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer- oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders— individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org

About Dark Wolfe Consulting

Dark Wolfe Consulting is a cybersecurity firm that provides specialized and commercialized network security assessments, vulnerability assessments, network penetrating testing, application assessments and application penetration testing.

digitalcitizens
alliance