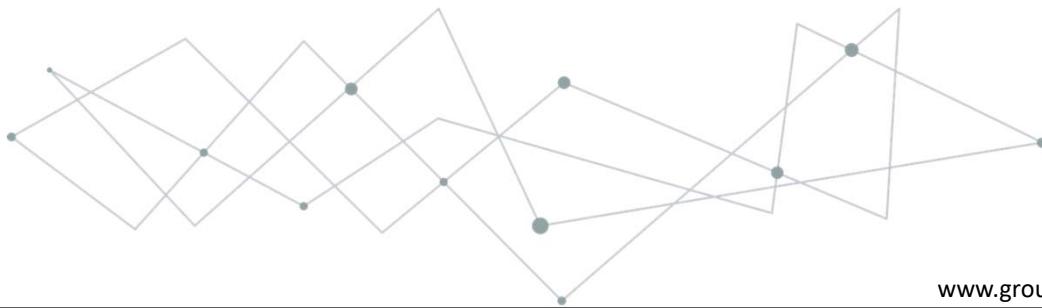




Roberto Sanchez, MBA, CISSP  
Vice President of Intelligence

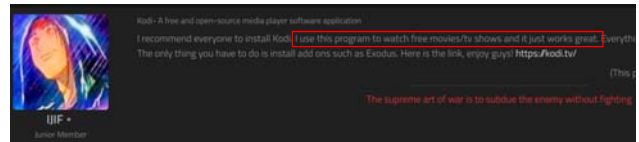
CWAG Presidential Initiative  
May 2018



[www.groupsense.io](http://www.groupsense.io)

# Why is Kodi So Popular?

- Open source, large community
- Single interface, collaborative, ease-of-use
- Illegal free content viewing (videos, music, podcasts, movies, tv shows, photos)
  - Netflix
  - Amazon Prime Video
  - Hulu
  - Sling TV
  - HBO Now
  - iTunes
  - Spotify Premium



Source: Twitter, Sinister.ly Forum

### Third-Party Add-ons

PPV	Movies	TV Shows	Music
  	  	  	  

# Which Is The Legitimate Application?



Source: Closed Sources

# Third-Party Add-ons (Tor-enabled Marketplace)

**Dream Market**  
kchudlyqmq-8dij.onion  
Established 2013

Shop Messages: 0

Bitcoin (BTC) 80 Logout

17 search results (0.004 seconds)

Filter

Ships to:  Ships from:  Escrow:  Category:  Cryptocurrency:

Price:  Searchtext:  Sort by:  Vendor:

Exchange

BTC	1.0
mBTC	1000.0
BCH	6.3
XMR	31.8
USD	6393.3
EUR	7676.9
GBP	6717.2
CAD	12236.9
AUD	12275.3

Installing Kodi 17 Krypton on Raspberry Pi 3 2017

ORBITIPTV.NET - ★PREMIUM ACCOUNT★ [LIF]

colombiaconnection (1750) (4.89★) (€ 300, 4.71/5)

Price: €0.002768 (\$26)

Ships to: Worldwide

Escrow: Yes


ORBITIPTV.NET - ★PREMIUM ACCOUNT★ [LIF]

Vendor: colombiaconnection (1750) (4.89★) (€ 300, 4.71/5)

Price: €0.002768 (\$26)

Ships to: Worldwide

Escrow: Yes



**Product description**

Enjoy the best IPTV service in the world! 1550+ ipn Channels FULL Europe + Greek + Italia + Germany + UK + Spain + Turk + Norway + Sweden + Netherlands + Portugal + Scandinavian + Arabic + Africa + Tunisia + Morocco + Algeria + India + USA + International channels.

Europe Channels: Full Italia, UK, Germany, Turkish, France, Greece, Netherlands, Portugal, Spanish, Scandinavian, Albania, India, Arabic, USA, Africa, etc.

USA & Canada: Sign up and get access to all your USA and Canada favorite ipn server channels: news, sports, comedy, cartoons, etc.

Asia Channels: Whenever you live in India, Pakistan, etc. we are sure you will be entire satisfied. Sign up to our ipn server now.

CHANNELS LIST | 1550+ CHANNELS -> <http://www.orbitiptv.net/www/orbitiptv.net/channels-list.html>

**Links**

- Forum
- Help
- Conferences
- Vendor application
- Earn money

**Exchange**

BTC	1.0
mBTC	1000.0
BCH	6.3
XMR	31.8
USD	6393.3
EUR	7676.9
GBP	6717.2
CAD	12236.9
AUD	12275.3

**News**

- New Forum
- Downtime & Recovery
- Deposit delays
- Forum under maintenance
- Earn money by finding bugs

Source: Dream Market Forum

# Exposed Kodi Devices in the U.S.

(Current as of April 25, 2018)

- 6% of North American households have devices with add-ons giving access to unlicensed content
- Default username: "Kodi" and default password: "blank"
- Security Risks
  - Malicious add-ons
  - Man-in-the-Middle (MiTM) attacks
    - Lack of encryption
    - Lack of strong authentication methods
  - Exposure of IP address and habits to ISP/authorities
  - Unauthorized content viewing

The screenshot shows the Shodan search engine interface. At the top, there is a search bar with the text "SHODAN" and a search icon. Below the search bar, there are navigation tabs: "Exploits", "Maps", "Share Search", "Download Results", and "Create Report". The main content area displays search results for "Kodi".

**TOTAL RESULTS: 908**

**TOP COUNTRIES:** A world map highlights the United States.

**United States: 908**

**TOP CITIES:**

Los Angeles	16
Chicago	12
Miami	7
Seattle	6
Las Vegas	5

**TOP SERVICES:**

HTTP (8080)	780
HTTP	60
HTTPS	31
Kerberos	8
Android/Java	7

**TOP ORGANIZATIONS:**

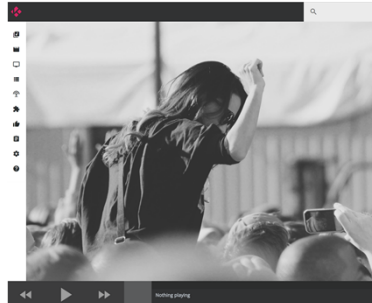
Time Warner Cable	143
Comcast Cable	131
Spectrum	50
Verizon Fios	20
AT&T U-verse	20

**Search Results:**

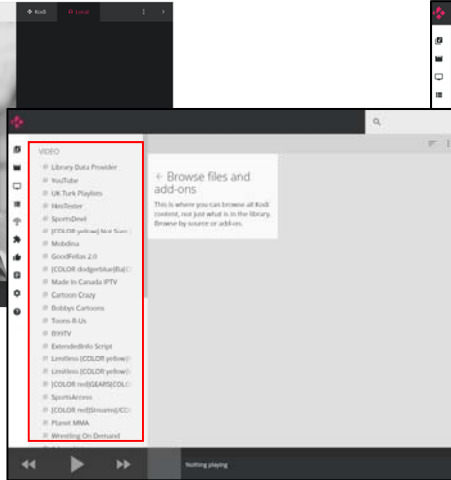
- Kodi**
  - HTTP/1.1 200 OK
  - Connection: Keep-Alive
  - Content-Length: 2019
  - Last-Modified: Sat, 22 Apr 2018 03:37:13 GMT
  - Content-Type: text/html
  - Cache-Control: private, max-age=0, no-cache
  - Accept-Ranges: bytes
  - Date: Wed, 25 Apr 2018 18:04:20 GMT
- Chorus 2 - Kodi web interface**
  - HTTP/1.1 200 OK
  - Connection: Keep-Alive
  - Content-Length: 1190
  - Last-Modified: Wed, 03 Jan 2018 03:12:33 GMT
  - Content-Type: text/html
  - Cache-Control: private, max-age=0, no-cache
  - Accept-Ranges: bytes
  - Date: Wed, 25 Apr 2018 09:44:02 GMT
- Chorus 2 - Kodi web interface**
  - HTTP/1.1 200 OK
  - Connection: Keep-Alive
  - Content-Length: 1190
  - Last-Modified: Thu, 25 May 2017 04:44:13 GMT
  - Content-Type: text/html
  - Cache-Control: private, max-age=0, no-cache
  - Accept-Ranges: bytes
  - Date: Wed, 25 Apr 2018 09:34:13 GMT

Source: Shodan

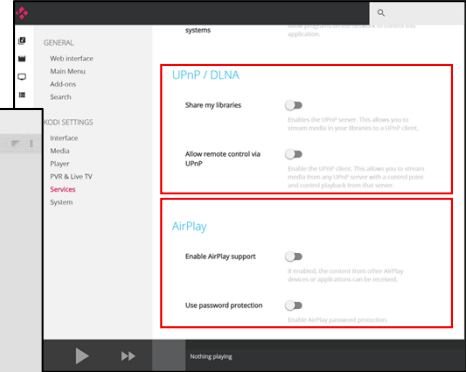
# Example of Publicly Exposed Kodi



Kodi Chorus 2 Web Interface



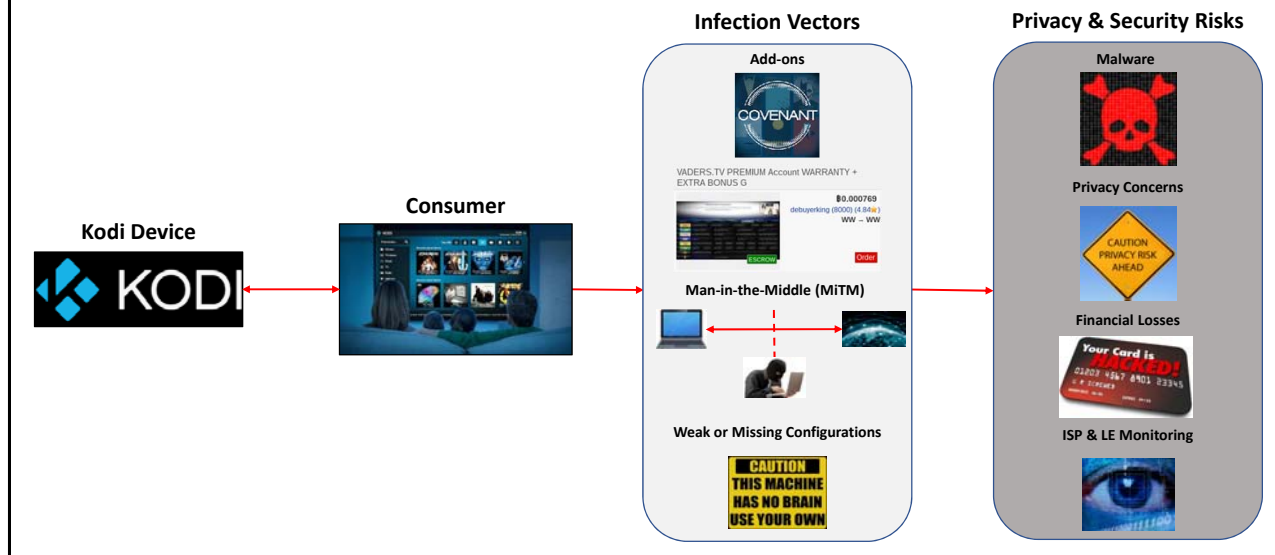
Kodi Library



Kodi Services Settings

Source: Closed Sources

# Infection Chain



This graphic depicts a typical chain of infection when individual consumers install the Kodi application onto their devices from smart tvs to laptops to smartphones. During the installation process, there are a number of default settings unless explicitly changed by the consumer, which most often does not happen, that exposes their systems to a multitude of privacy and security risks such as unauthorized content viewing and unencrypted communications. The primary reason for using Kodi is to view, free-of-charge streaming services such as video, tv shows, music, movies, and photos. To access the illegal copyrighted content, consumers download and install third-party add-ons from the Internet and Tor-enabled (Dark Web) marketplaces. Unbeknownst to the consumer these third-party add-ons further introduces them to risks such as copyright violations, malware infection, disclosure of IP address and Internet behavior, and the loss of the confidentiality of their communications. Additionally, the communication between their Kodi application and the third-party add-ons are unencrypted and unauthenticated meaning that an attacker can introduce malicious code into the communication stream or compromise the third-party add-on before the recipient (consumer) receives the data; thereby, infecting their device to incorporate into a botnet or steal privileged information such as user credentials.



# Thank you

