Iniquitous Cord-Cutting: An Analysis of Infringing IPTV Services

***Abstract*— Large scale, subscription based, Internet Protocol Television (IPTV) media piracy is occurring despite current of copyright enforcement. Cybercriminals are abusing legitimate services to setup and maintain illegitimate business operations offering pirated media content on a subscription basis. Due to the underground aspect of these pirated IPTV operations, these services are not well understood and so current enforcement action against them appear is not be effective. In this paper, we empirically measure the network infrastructure, payment, and order intermediary services that are used by a subset of the infringing IPTV ecosystem. We demonstrate how the measurements we make in this paper give insight into the business behind subscription based pirated media. Lastly, we show how these measurements can lead to potentially more informed policy decisions and intervention measures against subscription based IPTV piracy.**

***Index Terms*—IPTV, Kodi, cybercrime, media piracy**

I. Introduction

Illegally streaming or downloading online content has become a thriving industry that makes up a large part of the cybercrime economy [4], [11], [23], [28], causing financial losses in the hundreds of billions [32]. Some of the services providing free live streaming attract millions of viewers every month [29]. Despite copyright enforcement efforts [19] and better methods of detecting this piracy [24], the crimincal ecosystem still exists continues to grow.

Although there are efforts to thwart free media piracy activity, little is known about the subscription-based infringing content distribution business models. In Thomas et al. [40] researchers argue that security practitioners need a clear framework for investigating the cost and infrastructure behind internet crime and without one, there is no basis to evaluate intervention strategies. In this regard, we researched the distribution hardware and software architectures, and the economic value chains of these pay-to-pirate illicit media distribution services.

Our main motivation in studying subscription based illegal content distribution is three fold. First, we want to bring awareness to the complex inner workings of these services. This includes all the third-party services that they depend on to continue their illicit media distribution operations, such as middleware hardware and software, major CDNs, and online payment processors. This understanding allows us to shine a light on the challenges that these bad actors have to overcome to deploy these systems, and the gaps in security practices that allow them to exist. Second, we want to estimate the economic activity around subscription based illegal content distribution, which until now has been a gap in this literature. Lastly, we discuss the current ongoing legal based intervention efforts undertaken largely by the companies who's content is being infringed upon by these illicit services. The goal of our study being to provide a lens into how these illicit providers are able to exist and operate under the shadow of copyright law.

In summary, the main contributions of this work can be described as the following:

- We provide an analysis of the ecosystem architecture of subscription-based illegal content distribution.
- We provide an economic analysis of the revenue streams accumulated by bad actors providing pirated content.
- We highlight the third-party software, hardware, and other services like CDNs and payment processors, that subscription-based illegal content distribution relies on.
- We evaluate the efficacy of ongoing efforts to disrupt these infringing media distribution services and suggest a streamlined intervention process.

The remainder of this paper is structured is as follows. Section II discusses related work in this area, its shortcomings, and touches on how this research fits into the larger picture. Section III presents the structure of the infringing ecosystem and touches on the ethical and legal aspects of these services. Then section IV presents an economic and technical analysis of the illicit subscription based ecosystem. Section V describes some in depth case studies of several pieces of the infringing architecture. Finally section VI provides some insight into the limitations of our study, the inefficacy of existing methods to disrupt these practices and suggests a streamlined intervention process. We conclude in section VII.

II. Related Work

Related work on illegal media streaming focuses specifically on how different IPTV frameworks are implemented, their attack surfaces, and how they track and abuse users with advertisements and malicious software. A key limitation of previous studies is their focus on "free" ad-based services instead the pay-to-play subscription based ones.

To our knowledge, our work is also the first to present an economic estimation and technical infrastructure analysis of subscription based illegal streaming ecosystems. We are motivated by related work like Ganan et al. [25] on how to thoroughly research the economic impact of cybercrime. We are focused only on understanding major stakeholders and the infrastructures these pay-to-play services rely on.

Ibosiola et al. [31] focused on online video piracy (OVP) and its relationship to streaming cyberlockers, or illegal streaming sites. What they found is that the OVP ecosystem

is very centralized, with just a handful of dominant players, and that copyright enforcement only targets a small set of the ecosystem. Although this work focuses on measuring the scale of the illegal streaming ecosystem, it doesn't provide any insight into the economic value and incentives the actors supporting this ecosystem are reacting to. We cover this the economic analysis in section IV.

In Hsiao et al. [29], the focus is on the behavior of illegal sports streaming websites. They compared the behavior of illegal and legitimate streaming services to analyze user tracking similarities and differences. Turns out, illegal activity implements more technology to track users than legitimate services and over all go to greater lengths to avoid detection, monetize traffic and exploiter users. This fact is only true though of free illegal streaming services where as subscription based services often times don't have any advertisements at all.

In the Rafique et al. [39] study, the focus is on free broadcasts of live streams on the web, and refers to them as free live streaming services (FLIS). This study is similar to those previously mentioned in that they investigate the infrastructure used by FLIS, perform an analysis based on the user activity of FLIS, and perform a security review of FLIS websites. In a similar way to other studies, they found that users of FLIS are exposed to highly deceptive ads, malware, malicious browser extensions and other scams. Lastly, they build a classifier to characterise FLIS webpages to enable less false-positives when performing take copyright take downs.

Nikas et al. [38] focuses on the different attacks performed in peer-to-peer illegal streaming services and how joining and participating in one of these networks not only endangers your security as a user but the security of other peers as well. This work also demonstrates how the Kodi free media player app is abused for illegal streaming and used to conduct malicious attacks targeting users. Lastly, they present methods of collecting data from the Kodi platform to enable investigators to take down illegal services. This work is similar to ours in that Kodi is a piece of the piracy ecosystem explored however different in that our paper focuses on ecosystems that are not peer-to-peer.

Our work is similar to previous work in that it provides an economic lens into a cybercriminal activity [37]. The methodologies described throughout this paper are reflective of several studies focused on understanding the economics and technical aspects of cybercrime [17]. As we will discuss, some responses to IPTV piracy are very ineffective due to enforcer's inability to collect fines. The methodologies described throughout this paper are reflective of several studies focused on understanding the economics and technical aspects of cybercrime and is is similar to that in prior studies where systems were subscription based [34]. For example, similar to our work, in Kanick et al. [33] they measure order volume and purchasing behavior of modern spam and show how these types of inference techniques allow them to peer inside the spam-advertised businesses and make informed policy making and interventions. Similarly to McCoy et al. [36], following the money in subscription based pirated IPTV services leads us to a more fine grained understanding of the way this cybercrime operates.

III. Background and Ecosystem

A. Ethics and Legal

In order to abide by an ethical framework throughout this study, when purchasing pirated copyright materials, we always consulted with the intellectual property holder. We performed this consultation first to ensure that they were aware when we were required to purchase and or use illegal IPTV subscription services to perform some of the methodologies described in section IV.

We justify the purchases by showing this methodology was the only available way to derive the types of analysis we performed. For example, in order to estimate economic revenue, we needed to make purchases to measure order volume. When making these purchases, we always chose the cheapest option to minimize the amount of money given to these services. In total we spent no more than $500. Most payments were made through PayPal and assumed proper controls were in place at PayPal to mitigate the risk of money flowing to criminals. For example, we made a purchase of a "fully-loaded" Kodi firestick on eBay and observed these listings were consistently removed from the eBay platform. We also went to lengths to make return purchases after buying subscriptions in order to avoid providing any revenue to bad actors pirating copy-right media.

The data we collected and present in this work does not contain any PII and therefore abides by our institution's IRB. Lastly, it is important to note that although this work may present information that could point to specific kinds of legal conduct, it should not be used as proof in any sort of trial or conviction. Establishing any legal proof of criminal activity was not the goal of this work.

B. Stakeholders

Creating an illegal subscription based content delivery services involves a number of different stakeholders. The relationship between these parties is illustrated in Figure 1 and described below. This diagram is not meant to depict the only set-up available to illegally stream content with IPTV but it is a method we have observed in the wild.

Media Providers These stakeholders take legitimate content from cable/satellite/terrestrial TV and make it deliverable through IP Protocol so an end-user's set-top-box or PC can play it. They utilize a wide range of dedicated hardware and software to deliver this service.

Broadcasting Servers The broadcasting server delivers unscrambled TV channel streams with desired properties to middleware after decryption and transcoding. The desired properties can be audio-video format or bitrate. The IPTV infrastructure can be made from installing various software (free or paid) on general purpose computers or used with IPTV dedicated hardware available in market.

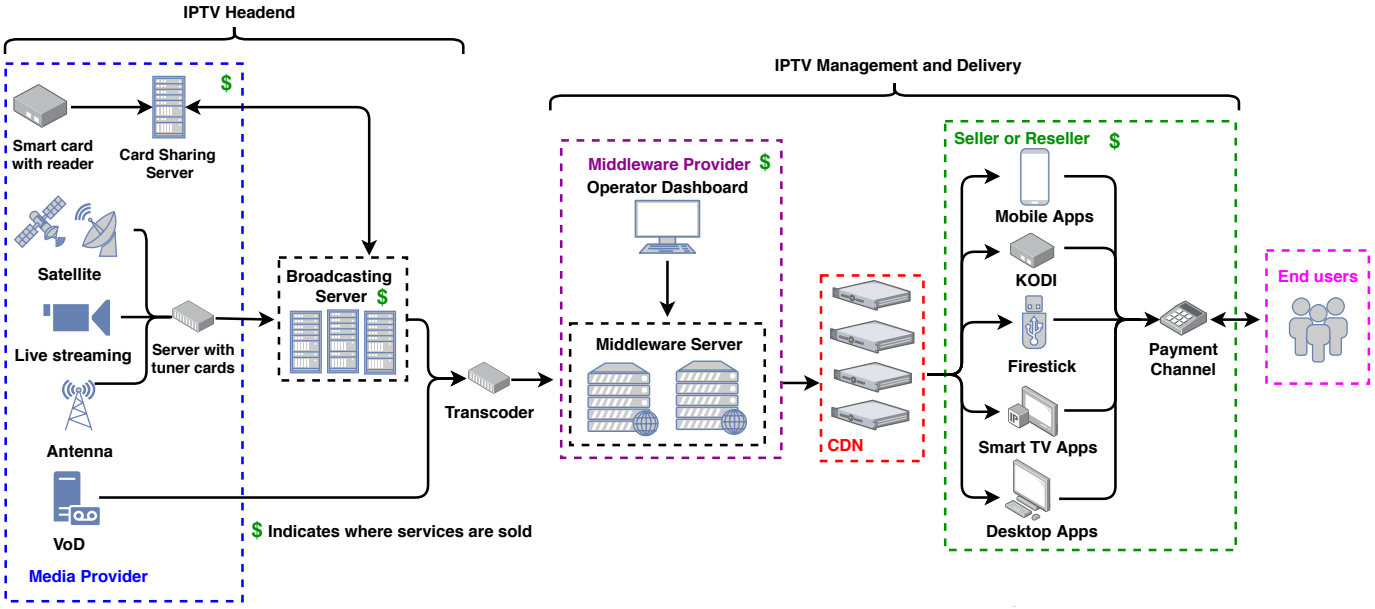

Figure 1: IPTV Architecture. The "$" indicates where in this ecosystem services are bought and sold.

Middleware Provider A middleware provider creates dedicated software and hardware to handle functionality like subscriber management, billing or reporting. Middleware software also provides IPTV output streams. These services can come as suites of any combination of content acquisition, management and delivery services.

Seller Sellers are websites which sell IPTV connections to end-users and resellers. They provide the connection in the form of m3u playlist files, custom desktop applications, mobile applications, Kodi boxes, Amazon Firesticks, or smart TVs.

Reseller Resellers typically purchase credits from sellers and then sell the IPTV connections to end-users. Resellers don't purchase or create the infrastructure themselves to pirate the media but instead just purchase subscriptions and resell them to end-users.

End-Users These are the customers purchasing IPTV subscriptions from sellers or resellers and then viewing them in any of the following formats:

- In VLC player by running a m3u file.
- Through a custom application desktop or mobile application.
- Kodi installed on a TV stick device or box.
- Kodi installed on a desktop machine.

C. Customer Acquisition

To maximize their profits, these infringing IPTV services need to market their services in order to grow their numbers of active paying subscribers. Based on our informal investigation, customers are acquired through a number of advertising and sales channels including IPTV forums, eBay, through YouTube videos providing setups instructions, and also through targeted online advertisements such as the ones shown in Figure 2. We suggest the demand and appeal for these services comes from

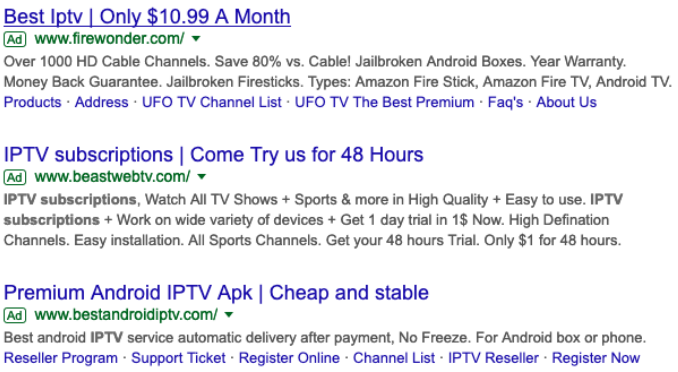

Figure 2: A screenshot of payed Google adwords advertisements for subscription based IPTV services providing pirated content.

the array of media content services all available in a single location for a small cost. There is no need for multiple streaming accounts, multiple subscriptions and different applications when all the content is in one location.

IV. Analysis

We selected four services for the order volume analysis and we identified twelve services for the network and payment processor based analyses. We chose these services by acting in the same way customers would and simply searching for IPTV subscription services i.e. Top results of Google search by keyword "IPTV subscription". Although there is overlap between the two sub-sets of services identified, we were constrained when selecting services for the economic analysis. We did not want to include IPTV services that offered free content because this in turn would prevent a lower-bound economic estimation.

We acknowledge both lists are not a complete set but just a small part of the potential services available. Furthermore, each of the twelve total IPTV providers are illegitimate and fail the following litmus test.

Several of the services in this pirated IPTV ecosystem either directly infringe on copyright, or turn a blind eye to the infringement practices of others. We selected HBO content to serve as a litmus test for whether a service infringes directly or indirectly by allowing distributors to use their services. This is because a HBO subscription is only available through one of the following methods:

- HBO NOW subscription.
- Adding HBO to your TV Package and getting access to HBO On Demand and HBO GO.
- Digital subscription through Amazon, Hulu, DIRECTV NOW or Playstation Vue.

Therefore, if a seller or reseller is marketing or providing HBO content, we can be sure that it is obtaining the content via methods which infringe copyright.

A. Economic Analysis

The importance of understanding the economic incentives of cybercrime when discussing a potential kill chain is highlighted in several previous works [27], [37]. We follow a similar framework and present analyses of the payment processors that are accepted in the pirated IPTV ecosystem and an estimate of the amount of money pirated IPTV providers are making.

Payment processors Our list of possible payment options for pirated IPTV content is fairly distributed although several payment methods, like credit card, are more popular than others. Table I depicts the main payment providers accepted by the twelve IPTV providers we investigated. The reason the number of providers does not total 12 is because some services accepted multiple payment methods. Of the IPTV providiers investigated, all 12 accepted credit card payments directly through a third-party, such as PayPal. We note that we were only able to study a limited number of infringing IPTV providers and that our result is potentially not representative of other services which we did not study. Furthermore, some payment processors, like Paymentwall, accept various payment types like WeChat payments [1] or Subway gift cards.

Only 3 of the investigated infringing IPTV providers accepted forms of cryptocurrency but none of them solely accepted cryptocurrency payments. This high usage of regulated payment methods such as Visa and Mastercard indicates that there is likely not much intervention pressure being placed on payment processing. Prior studies have shown that disrupting an illicit service's ability to accept payments through regulated payment channels causes them to primarily accept cryptocurrencies. However, the same study saw this switch to cryptocurrencies followed by a 50% decline in revenue likely due to the usability [21].

[1]WeChat is a Chinese multi-purpose messaging, social media and mobile payment app developed by Tencent. It is one of the world's largest standalone mobile apps in terms of monthly user.

Payment Method	No. of providers
Credit card	12
PayPal	3
VoguePay	2
coinpayments.net	2
Debit card	1
OKPAY	1
Authorize.net	1
Money transfer	1
Payoneer	1
Bitcoin	1
Paymentwall	1
SOFORT Banking by Payssion	1
Paysera (bank transfer)	1

Table I: This table depicts which payment processors are accepted by a total of 12 different IPTV services. They sum to more than 12 because some of the payment processors accept multiple payment methods.

Revenue Estimation We use a technique called "purchase pair" in order to estimate revenue by measuring how many subscriptions were sold during a certain time period [33]. The high level idea of this method is that if order numbers are sequentially incremented then we can derive the order volume during a period of time. If the order numbers are not assigned sequentially then this method is not effective for estimating the order volume and revenue of that service. This method works in the following way: First we perform consecutive purchasing of the service to determine if the service is assigning order numbers sequentially. If the order numbers for our consecutive purchases are consecutive and increment by one we assume they are assigned sequentially and our method can estimate order volume. For those services that do assign order number sequentially we waiting some time, and then making a another purchase. We can measure the order volume by subtracting the two order number and dividing by the elapsed time period. An example of our method is depicted in Figure 3.

The final step is to estimate the average order cost which can be multiplied with the order volume estimate to extrapolate a revenue estimation [33]. Since we do not have a good estimate of average order cost for infringing IPTV services. Therefore, we use the minimum subscription cost of a service to produce what we believe is a conservative lower bound estimate of revenue. However, there are many other factors such as refunds that we cannot measure.

Table II shows our estimated revenue for four providers that we subscribed to repeatedly. We received explicit permission from a content distributor to purchase these providers to avoid copy-right issue. We estimate that some of these IPTV providers likely make upwards of $12,400 per month. However, these are smaller players compared to one of the largest illegitimate IPTV provider Set TV, that has faced legal action and is reported to have had upwards of 180,000 sub-

scribers [14]. The amount of subscribers and income directly indicates the demand for pirated services.

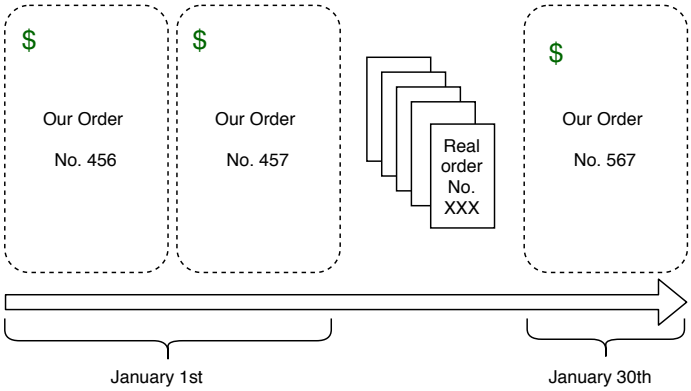

Figure 3: This figure depicts our methodology for estimating order volume. By consecutively purchasing the service to verify that order numbers are assigned sequentially, and then waiting some time to make a final purchase, we can deduce the order number incrementation and estimate the total number of orders in the elapsed time frame. For example consider a first purchase resulted in order 456 and 30 days later, a third purchase resulted in order 567. The calculation to measure the number of orders per day is $(567 - 456)/30 = 3.7$

B. Network Analysis

In this sub-section we describe the observed network movements when using these services providing Live TV and Video on Demand content. In each instance, an end-user application loads an m3u or m3u8 file containing a URL and makes a GET request to receive the pirated content stream or file. From the response, we are able to infer metadata about the hosted or streaming content such as the CDN and hosting provider. Table III displays the different network infrastructure utilized by the illegitimate IPTV providers. Although there is a range of providers, we do see some main overlap between IPTV services, implying that they may be abusing the same infrastructure.

C. Technical Analysis

IPTV providers serve two main types of media content: LIVE TV Channels and Video on demand (VoD). Here, we will analyze and discuss technical operations of these IPTV providers. This information was gathered by monitoring IPTV related forums and contacting consultants on these forums. For the most part, this information is not readily available because these consultants sell their skills of developing illegitimate IPTV business set-ups and thus are reluctant to share this information.

IPTV Headend IPTV headend is a term we are using to describe an infrastructure setup which takes input media input and always outputs unscrambled channel streams that are ready for delivery through the IP protocol. An IPTV headend can be described as an combination of following sub-parts:

a) TV Input: The TV stream input to an ITPV headend can be scrambled or unscrambled live TV Channels from either satellite TV, cable TV or terrestrial TV. These inputs generally rely on communication based on international open standards for digital television called the Digital Video Broadcasting (DVB) standards.

b) TV Tuner Cards: TV tuner cards are used to receive TV streams on a computer from a TV input. These tuner cards can be used in a general purpose computers or there are dedicated IPTV streaming servers which have slots for these cards. For example, a TBS2951 MOI PRO AMD card, which is an IPTV Streaming Server, has 4 PCIe slots and can take up to 32 TV inputs. This streaming server, has a user friendly web interface and is manufactured by a Chinese company called TBS Technologies International Ltd. They make TV tuner cards, IPTV streaming servers with pre-loaded software, transcoders and all the other requirements for an IPTV infrastructure. Their software and hardware is popular on IPTV forums where bad actors discuss setups for pirated content.

c) Broadcasting Server: A broadcasting server is loaded with software capable of taking DVB satellite input from TV tuner cards and publishing streams to later be transmitted on IP based data networks using protocols like real-time transport protocol (RTP) or HTTP live streaming (HLS). The software installed on a broadcasting server has a web-based user interface which can be used to configure different DVB sources and encode the input into desirable output stream while assigning a multicast IP Address to each stream.

d) Card Sharing Server: The two types of TV channels distributed by providers are free to air (FTA) channels and encrypted or scrambled channels. The FTA channels are ready to be transmitted without any intervention unlike scrambled channels which need to be decrypted via a smart card used with a set-top-box or STB. The decryption happens using a cryptographic key called a Control Word (CW) [35]. IPTV pirates intercept CW so that they can use it to unscramble channels for their business and then monetize it further by redistributing it to other illegitimate IPTV businesses. In this way, a paid subscription from a legal TV provider meant for one user is used to unscramble channels for multiple users. Hence, the name Card Sharing. To intercept the CW, IPTV pirates set-up a server with a software known as softcam. This server is connected to a smart card reader using a valid TV smart card. Softcam emulates the decryption process of channels and intercept the CW while doing that.

IPTV Management and Delivery. The IPTV headend described in the last section provides unscrambled TV channels in some of the following formats; HLS (HTTP live streaming) streams [3], MPEG transport streams (transport stream, MPEG-TS, MTS or TS), or RTP streams. In this section, we will discuss management, delivery and monetization of these streams.

e) Transcoder: Transcoding the HLS streams is not required but is done in some cases to improve user experience.

IPTV providers	D	S	$\frac{S}{D}$	$M(\$)$		Total $ per day	Total $ per month
www.iptv-subscription.net	43	474	∼11	7.38	3,498.12	81.18	2,535.8
www.iptvsubscription.us	43	9	∼0.2	5	45	1	31
www.iptvlocal.com	20	847	∼42.4	5	4,235	212	6,572
www.iptvsubscription.net	31	1,252	∼40	10	12,520	400	12,400

Table II: Sample order volume analyses, based on the cheapest plan and a 31 day month. D corresponds to the number of days, S corresponds to the number of subscribers, M corresponds to the cost for the least expensive plan. This analysis began January 26th 2018 and continued until n days after where n corresponds to the "Days" column.

Network Provider	IPTV		VoD
	CDN	Hosting	Hosting
AKAMAI	**4**	-	-
BAREFRUIT	-	1	-
CONTABO	-	-	1
DATACAMP LIMITED	-	**4**	**4**
DIGITAL OCEAN	-	2	-
LEVEL 3 COMMUNICATIONS	-	2	-
NETERRA	-	1	-
ONLINE SAS	-	2	1
OVH	-	-	1
UK SERVERS	-	1	1
WORLDSTREAM	-	2	**4**

Table III: This table depicts which CDN and hosting providers are used for IPTV or VoD services across 12 different IPTV services.

Transcoding in general means altering the video/audio to accommodate:

- End-users with different levels of bandwidth - Bit rate of video is altered so that users with different bandwidth can be served streams accordingly. HLS streaming is an adaptive bit rate technology which can handle transcoding.
- End-Users having different devices - Re-sizing the video frame to adjust resolution suited best for the device the end-user is using like computer, phone, or tablet.

Transcoding is a resource intensive operation and requires dedicated hardware with enough resources. The transcoding job is sometimes handled by middleware software which is discussed in next sub-section.

f) Video on demand: A video on demand (VoD) server holds MP4 files of pre-recorded content like movies and TV series. These MP4s are fed into middlware software for further distribution. Depending on the desired content quality, there are many services like opendrive and cloud storage, for VoD distribution. The VoD content is distributed from providers outlined in Table III. Some of the investigated IPTV providers use multiple hosting providers and so there are more than 12.

g) IPTV Middleware: Middleware is a crucial part of the IPTV ecosystem because it acts as the glue between the headend and delivery. IPTV middleware is software capable of various tasks, including but not limited to, subscriber management, reseller management, stream management, load-balancing, transcoding and generating TV output channel playlists. It works by taking the input streams from broadcasting server in and generating output streams. These streams of different channels can be combined to form a "bouquet" which is a package of selected TV channels offered to an end-user. As mentioned before, pirated pre-prepared streams are sold on forums and plugged into middleware. This means that for some, middleware providers are the first step in their infrastructure.

h) Content Delivery Network (CDN): Content Delivery Network (CDN) is used to ensure that the user get the content with high availability and performance. CDN services are used to reduce overall bandwidth cost and ensure that streams are delivered with high availability around the globe. Not all the IPTV providers investigated used CDN for streaming as seen in Table III. However those that do, all use Akamai.

i) Content Delivery Methods: End-user use various applications to play the content. For communicating the source of media streams to the applications there are broadly three different mechanisms we have observed to be used:

```
#EXTM3U
#EXTINF:-1 tvg-id="" tvg-name="US:HBO" tvg-logo="" group-title="USA",US:HBO
http://tv.onsecc.com:6227/live/3Ta826Hqz/vhJ531emS5/16944.ts

#EXTINF:-1 tvg-id="" tvg-name="US:HBO Comedy HD" tvg-logo="" group-
title="USA",US:HBO Comedy HD
http://tv.onsecc.com:6227/live/3Ta826Hqz/vhJ531emS5/16949.ts

#EXTINF:-1 tvg-id="" tvg-name="Marvel's Luke Cage S02 E13" tvg-
logo="http://tv.onsecc.com:6227/images/dWqB2rTdqzoHT7OhZljBfMd0n2Y_small.jpg"
group-title="Series",Marvel's Luke Cage S02 E13
http://tv.onsecc.com:6227/series/3Ta826Hqz/vhJ531emS5/19691.mp4
```

Figure 4: m3u file containing URL of MPEG-TS files for LIVE TV and MP4 files for Video On Demand

m3u File When the output stream format is chosen to be MPEG-TS then m3u files have been observed to be used for delivery. m3u (MP3 URL or Moving Picture Experts Group Audio Layer 3 Uniform Resource Locator) files are multimedia playlists containing all the TV Channel information and links to the streams in a format which many multimedia players like VLC media player can understand and play. User download the file and open with a media player like VLC which shows all the TV Channels and Video On Demand in a playlist. The following Figure 4 is an example of the content of an m3u file.

m3u8 File In this case, a service provider asks user to download and install a custom application as per the operating

system or device of the user. Instead of providing the playlist file to be be directly downloaded, these files are used in network interaction between the custom applications used and a middleware server.

Stalker Add-on In case the end-user is using specific hardware like Kodi software on an Amazon Firestick, there is a custom add-on software used called as Stalker client. This add-on acts as an interface between hardware and the middleware server to exchange media. The service provider asks for the hardware's MAC address which is configured in middleware software. In exchange, service provider gives an stalker URL (`http://<host>:<port>/c`) to be configured in hardware after installing the Stalker client add-on. This establishes an authenticated communication channel between the hardware running Kodi and a middleware server.

V. Case Studies

We will discuss in this section three case studies which represent the behaviour of economic operations and the scale of the technology abused used to infringe on digital content copyrights. In some cases we applied the HBO litmus test, whereas if a service offered HBO content we assumed that they were pirating. In other cases, we did not apply the litmus test because the IPTV provider was already accused of violating copy-rights by the content owners. We also contacted some third party end-to-end IPTV solution providers where we were not clear about the specifics of their offerings.

A. Kodi Ecosystem

Kodi [2] is a free and open-source media player developed by the XBMC Foundation that does not include any infringing media content. However, there is a large ecosystem of free and paid third-party add-ons (i.e., IPTV subscription service add-ons) which provide access to infringing media [5]. Initially, technically savvy users started installing free infringing Kodi add-ons to access a wide range of pirated media. Merchants noticed this trend and started selling what are termed "fully loaded Kodi boxes" which are normally jailbroken Amazon Firesticks and other Android devices with infringing Kodi add-ons pre-installed.

In summary, revenue in the infringing Kodi ecosystem is primarily derived from two sources: (1) One-time payment for buying marked up jailbroken TV sticks loaded with infringing Kodi add-ons, or (2) Paying for IPTV subscriptions that are connected to infringing Kodi add-ons.

Authorities have started cracking down on copyright infringing Kodi devices. In November 2017, some developers of popular Kodi add-ons received a 'Notice of Copyright Infringement' by the Motion Picture Association (MPA) and Alliance for Creativity and Entertainment (ACE) [3] after which they ceased to manage the add-on software. In 2018, the Federal Communications Commissions (FCC) wrote a letter to the CEO of Amazon and eBay, requesting a crackdown on the sale of these infringing Kodi devices [1].

[2]https://kodi.tv/

[3]MPA and ACE represent a coalition of media, film and entertainment companies

B. SET TV

SET TV was an IPTV business which provided premium IPTV subscriptions for $20 monthly and $200 annually. SET TV quickly appeared to become a popular infringing IPTV service that delivered premium channels such as HBO through a standalone computer application. The application was strikingly similar in appearance to Nora Go, an app developed by end-to-end IPTV solution provider SetPlex. We estimate that SetPlex sold about 5,810 subscriptions per day on average. We calculated this figure by the Order Volume Analysis described in 3. In 2018, Dish Network and NagraStar filed a joint federal court lawsuit against SET TV for copyright infringement. SET TV was found in violation of the Federal Communications Act (FCA) and Dish was awarded statutory damages of $90,199,000 [7].

After SET TV closed, we found several other IPTV providers that we suspect to be connected. Our suspicion is based the similarity of their network footprint and app they use to distribute content.

IPTV Provider	CDN	Hosting
setvnow.com	Akamai	Datacamp (185.59.223.14)
tvstreamsnow.com	Akamai	Datacamp (185.59.223.14)
vustreamtv.com	Akamai	Datacamp (185.59.223.14)
bimotv.com	Akamai	Datacamp (185.59.223.14)

Table IV: This table depicts the similarity between SET TV and other three IPTV services which came after it. All three are still operational.

We found these services have a similar network footprints to SET TV which is shown in Table IV and was generating by using the same network analysis method described in Section IV. Just like SET TV, the other three copyright infringing services are connecting to the same IP Address 185.59.223.14 (Datacamp) for steaming VoD content. They all use the same CDN, Akamai Technologies. Also, all three services use the Nora Go application by SetPlex to deliver content.

In the case of IPTV, all three services request infringing media streams from the same host tk3.fastbroad.com. The Registrant contact information derived from whois.icann.org for domains fastbroad.com and setplex.com are the same. In the case of VoD, all three services fetch media files from the host cdnvod.setv.ca.

This case study shows that it is likely difficult to ensure that after successful legal action, the infringing service actually has ceased operations. This, combined with the low barrier of entry for new actors, causes an inevitable game of whack-a-mole. In each case, products/services originally used by SetPlex were likely still utilized by these new infringing IPTV services. This reflects the agileness of abuse of end-to-end IPTV solution providers.

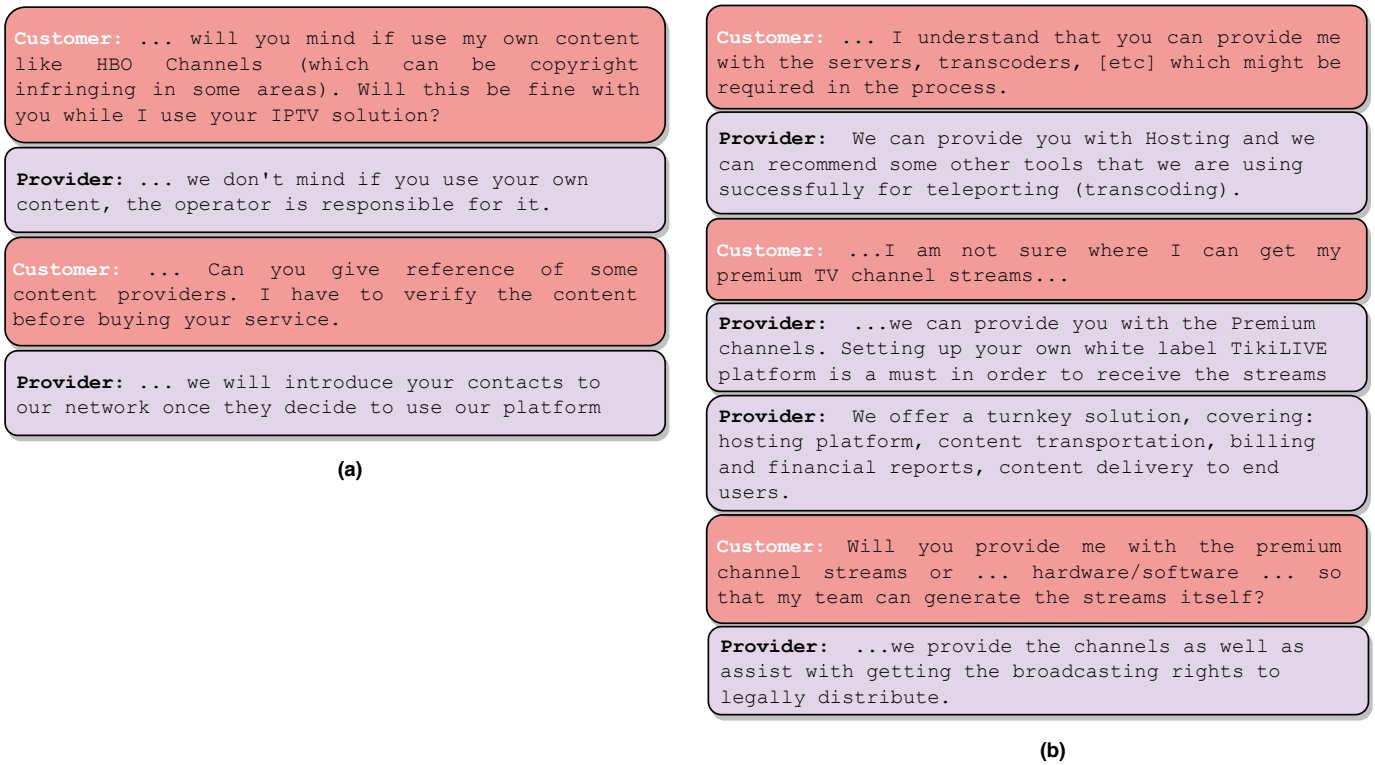

Figure 5: (a) Transcript from Mware Solutions, an end-to-end IPTV provider. (b) Transcript from contacting representatives from TikiLIVE, an Omniverse distributor.

C. Omniverse

One World Television (Omniverse) is an illegitimate stream provider who provides premium streams to distributors who deliver content to end-users. These distributors profit in two main ways: (1) Selling subscriptions to end-user, (2) Providing end-to-end IPTV Solutions to enable starting a new IPTV business. Distributors then mention on their websites "In Cooperation with Omniverse One World Television Inc." or "Powered by Omniverse". The Omniverse distributors that fail our litmus test of providing HBO content are SkyStreamTV, Flixon TV, and TikiLIVE. They all provide subscription based IPTV and VoD content to end-users.

We contacted TikiLIVE who offer premium channels such as HBO and lists itself as an authorized distributor of Omniverse. We asked them for details about their end-to-end IPTV solution, depicted in Figure 5 (a). In summary, they claim that they can obtain the broadcasting rights to legally distribute content, such as HBO. In February 2019, members of the Alliance for Creativity and Entertainment (ACE) filed a lawsuit against Omniverse. Although the lawsuit does not name Tikilive, we assume that they cannot arrange the legal rights for all the premium channels, such as HBO, listed in their subscription based service [15].

This case study describes a middle-man third-party service, Omniverse, which offers most of the infrastructure and content required to operate a streaming media service. Omniverse is accused of provided unlicensed infringing content to IPTV services [2]. These IPTV services redistributing content provided by Omniverse marketed themselves as legitimate [4]. Apart from this, we found that two Omniverse distributors, Tikilive and NKT TV, are listed as official providers on Sony Movie Channel website [9]. As stated in lawsuit, these conditions create confusion when distinguishing between legitimate and illegitimate content providers [2].

D. Mware Solutions

Mware Solutions is a third party end-to-end IPTV solution provider. As part of our methodology, we contacted them to get information regarding their offerings and Figure 5 (a) illustrates the conversation with them. As observed through this conversation, they turned a blind eye towards HBO copyright infringement. This case study is an example of intermediaries not taking liability for their customers actions. It appears that Mware Solutions is not proactively preventing their customers from streaming infringing content. Although legally speaking, Section 230 of the Communications Decency Act (CDA) largely insulates intermediaries from the illegal actions of their customers.

[4]It is unclear if these IPTV services did not know that the content they were provided from Omniverse was not legally licensed.

VI. Discussion

A. Limitations

We encountered several challenges while researching infringing subscription based IPTV services. The first, is that we had to purchase a subscription to each service that we analyzed in order to identify which networking providers they were using for content delivery and to confirm that each service was providing access to infringing media. This purchasing requirement constrained the number of infringing services that we could analyze. Another challenge we faced when performing our economic analysis was that many of these infringing content sellers do not operate for long thus it is difficult to measure properties of them such as their revenue since our purchase pair technique requires periodic purchases. Therefore, the measurements of the limited and potentially biased sample of infringing services we analyzed in this paper are a lower bound of the number of services that are operating. While our study is not comprehensive, it does provide an initial understanding of the potential scale and how subscription-based infringing media services are structured.

An avenue for future work could be an automated method to collect metadata about and analyze potentially infringing services. Doing this study at a larger scale would be helpful in order to capture a wider net of potentially illicit content distributors.

Lastly, some sellers are moving toward accepting cryptocurrency as payment which adds a new layer of payment blockchain tracking in order to measure payment activity. Although we don't expect to see a situation where IPTV pirates only accept cryptocurrency because revenue has been show to taper for criminals in those situations [21]. That being said, following cryptocurrency payments can lead to insight on who is purchasing the products and where the cryptocurrency is being exchanged to fiat. [30]

B. Legal interventions

Previous work has highlighted the economic and ethical importance of copy-right, and how for-profit infringing content distribution adversely affects content creators [12]. However, enforcement of existing laws against infringing content distribution is largely left to the rights holders. What we have observed in our analysis, is the likely ineffectiveness and limitations of the current legal strategy.

While observing the current landscape of legal interventions, we saw that Digital Millennium Copyright Act (DMCA) take-down notices and legal complaints asserting claims under Copyright Act and Federal Communications Act are typically sent out by content-owners. Recently, members of the Alliance for Creativity and Entertainment (ACE) filed legal complaints against copyright infringing media services like SET TV, Omniverse, Tickbox, Dragonbox [2], [6], [8], [10].

That being said, DMCA notices are found to be ineffective according to studies by Boyden [20] and Goldman [26]. According to the Boyen study, in spite of DMCA notices, the infringing content mostly reappears. The legal complaints imposed by ACE members against SET TV resulted in a permanent injunction where they were required to cease all operations and handover infrastructure. That being said, we showed that three other pirated IPTV services with the same network fingerprint spawned up after SET TV ceased operations. In summary, we can say that aforementioned legal interventions will sometimes win a battle but are losing the war.

Our measurements of the subscription based IPTV ecosystem are likely not complete enough to propose potential choke points [22] for disrupting the services and thus we leave this to a further study. However, we can provide a discussion of prior studies and their efficacy in public and private interventions methods against other similar online infringing and illicit merchants.

As any other business, illegitimate IPTV providers depend on third-party intermediaries for monetization and efficient service delivery. We have shown some important intermediaries like hosting providers and payment processors. According to study done by by Aniket Kesari et al. [18], utilizing intermediaries to interrupt these operations provides a streamlined approach. We propose a two step streamlined intervention inspired by this.

Identifying Intermediaries Content-owners can use a user complaint system to collect intelligence from investigations to identify the intermediaries used in IPTV providers operation. We have described methods to identify intermediaries, like payment processors, CDN providers, or hosting service providers. These intermediaries may or may not be aware of their participation and role in these illegitimate operations [16]. Intermediaries may be willing to denying services to such illegitimate operations reported by content-owners [33]. This would result in interruption of services for IPTV providers and economic loss.

Legal Intervention If the identified intermediaries are not voluntarily willing to deny services to IPTV providers, content-owners can use Rule 65 of the Federal Rules of Civil Procedure (FRCP) to obtain a Temporary Restraining Order (TRO). TRO can legally force intermediaries to deny services to illegitimate IPTV providers. Rule 65 is recommended instead of CDA 230 or DMCA because it is swift (TRO observed to be received within 9 days [13] after filing of Motion for a TRO) and *ex parte* (TRO recieved without notice to defendant). TRO then is used to force intermediary intervention before court issue a preliminary injunction and finally a Judgment Order.

Working with payment processors to stop services to IPTV operations would demotivate IPTV operations financially [27] and has been effective in the past at limiting the ability of illicit services to accept regulated payment methods such as credit cards and PayPal [34]. Overall, a form of content watermarking combined with a streamlined approach would lead to more successful IPTV piracy counter measures. That being said, there needs to be a balance between manual effort and automation in the streamlined approach so that they aren't abused.

VII. Conclusion

In this paper we described and measured the current state of the subscription based pirated IPTV ecosystem. Our work presents a lower bound on the scale to which these business operate globally. We demonstrated that current efforts to thwart these business are ineffective at preventing for-profit media piracy. We offered a subset of measurements to demonstrate the third-party services that these cybercriminals rely on to conduct their day-to-day business. Our hope is that an increased understanding as a result of these empirical measurements of network and payment methods can lead to a more effective streamlined process when implementing restricts on these pirated services.

References

[1] FCC asks Amazon and eBay to stop selling fake pay TV boxes. https://techcrunch.com/2018/05/29/fcc-asks-amazon-and-ebay-to-stop-selling-fake-pay-tv-boxes/.

[2] Hollywood tries to cripple several alleged pirate TV services in one lawsuit. https://arstechnica.com/tech-policy/2019/02/pirate-tv-provider-lied-about-paying-for-licensing-hollywood-lawsuit-says/.

[3] HTTP Live Streaming. https://goo.gl/crRhm9.

[4] Illegal streaming is dominating online piracy. https://www.businessinsider.com/illegal-streaming-is-dominating-online-piracy-2016-8.

[5] Kodi users face crackdown over illegal add-ons. https://www.independent.co.uk/life-style/gadgets-and-tech/news/kodi-boxes-addons-downloads-legal-crackdown-copyright-films-fact-a7809306.html.

[6] Netflix, Amazon and studios sue Dragon Box streaming device seller, alleging copyright theft. https://www.latimes.com/business/hollywood/la-fi-ct-netflix-dragon-box-piracy-20180111-story.html.

[7] SET TV is Ordered To Pay Dish $90 Million in Piracy Damages. https://www.cordcuttersnews.com/set-tv-is-ordered-to-pay-dish-90-million-in-piracy-damages/.

[8] Set TV, the streaming service sued by Netflix, Amazon, is 'unavailable'. https://www.cnet.com/news/set-tv-streaming-service-sued-by-netflix-amazon-is-unavailable/.

[9] Sony Movie Channel Affiliates. https://www.sonymoviechannel.com/affiliate.

[10] TickBox Agrees to $25 Million Judgment in Copyright Infringement Case. https://variety.com/2018/digital/news/tickbox-copyright-suit-25-million-1202936712/.

[11] Traffic Report: Online Piracy and Counterfeiting. https://www.markmonitor.com/download/report/MarkMonitor_-_Traffic_Report_110111.pdf.

[12] Illegal streaming and cyber security risks: A dangerous status quo? https://cryptome.org/2014/09/illegal-streaming-malware-epoch-times-full-14-0923.pdf, 2014.

[13] *Luxottica Grp. S.p.A. v. The Partnerships and Unincorporated Associations*. Sept 2016.

[14] *Dish Network L.L.C. and Nagrastar LLC. v. Nelson Johnson, Jason Labossiere, Set Broadcast LLC, Streaming Entertainment Technology LLC*. Nov 2018.

[15] *Paramount Pictures Corp. v. Omniverse One World Television, inc.* Feb 2019.

[16] Alrwais, S., Liao, X., Mi, X., Wang, P., Wang, X., Qian, F., Beyah, R., and McCoy, D. Under the shadow of sunshine: Understanding and detecting bulletproof hosting on legitimate service provider networks. In *2017 IEEE Symposium on Security and Privacy (SP)* (May 2017), pp. 805–823.

[17] Anderson, R. J., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., and Savage, S. Measuring the cost of cybercrime. In *WEIS* (2012).

[18] Aniket Kesari, C. H., and McCoy, D. Deterring cybercrime: Focus on intermediaries. In *32 BerkeleyTech. L.J. 1093 (2018)* (2018).

[19] Ballard, B. Premier League knocks out Wiziwig in illegal streaming crackdown. http://goo.gl/ETCjH2.

[20] Boyden, B. How the dmca's online copyright safe harbor failed. In *George Mason University, School of Law* (2014).

[21] Brunt, R., Pandey, P., and McCoy, D. Booted: An Analysis of a Payment Intervention on a DDoS-for-Hire Service . In *Workshop on the Economics of Information Security (WEIS)* (2017).

[22] Clayton, R., Moore, T., and Christin, N. Concentrating correctly on cybercrime concentration. In *WEIS* (2015).

[23] Elstein, A. Web pirates are stealing from sports broadcasters. http://goo.gl/TVOxRi.

[24] Englehardt, S. *Automated discovery of privacy violations on the web*. PhD thesis, Princeton University, 2018.

[25] Gañán, C. H., Ciere, M., and van Eeten, M. Beyond the pretty penny: The economic impact of cybercrime. In *Proceedings of the 2017 New Security Paradigms Workshop* (New York, NY, USA, 2017), NSPW 2017, ACM, pp. 35–45.

[26] Goldman, E. The failure of the dmca notice and takedown system: A twentieth century solution to a twenty-first century problem. In *3 NTUT J. of Intell. Prop. L. and Mgmt. 195* (2014).

[27] Goldman, Z. K., and McCoy, D. Deterring financially motivated cybercrime. In *Journal of National Security Law and Policy* (2016).

[28] Herley, C., and Florencio, D. Economics and the underground economy, July 2009. Black Hat.

[29] Hsiao, L., and Ayers, H. The price of free illegal live streaming services, 2019.

[30] Huang, D. Y., Aliapoulios, M. M., Li, V. G., Invernizzi, L., Bursztein, E., McRoberts, K., Levin, J., Levchenko, K., Snoeren, A. C., and McCoy, D. Tracking ransomware end-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)* (May 2018), pp. 618–631.

[31] Ibosiola, D., Steer, B., García-Recuero, Á., Stringhini, G., Uhlig, S., and Tyson, G. Movie pirates of the caribbean: Exploring illegal streaming cyberlockers. *CoRR abs/1804.02679* (2018).

[32] Kal Raustiala, C. S. How much do music and movie piracy really hurt the u.s. economy? http://freakonomics.com/2012/01/12/how-much-do-music-and-movie-piracy-really-hurt-the-u-s-economy/.

[33] Kanich, C., Weaver, N., McCoy, D., Halvorson, T., Kreibich, C., Levchenko, K., Paxson, V., Voelker, G. M., and Savage, S. Show me the money: Characterizing spam-advertised revenue. In *USENIX Security Symposium* (2011).

[34] Karami, M., Park, Y., and McCoy, D. Stress testing the booters: Understanding and undermining the business of ddos services. In *WWW* (2016).

[35] Koemmerling. Card sharing countermeasures, Jun 2011.

[36] Mccoy, D., Dharmdasani, H., Kreibich, C., Voelker, G. M., and Savage, S. Priceless: The role of payments in abuse-advertised goods. In *In Proceedings of the 19th ACM conference on Computer and communications security* (2012).

[37] Moore, T., Clayton, R., and Anderson, R. The economics of online crime. *Journal of Economic Perspectives 23*, 3 (September 2009), 3–20.

[38] Nikas, A., Alepis, E., and Patsakis, C. I know what you streamed last night: On the security and privacy of streaming. *Digital Investigation* (03 2018).

[39] Rafique, M. Z., Goethem, T. v., Joosen, W., Huygens, C., and Nikiforakis, N. It's free for a reason: Exploring the ecosystem of free live streaming services. *NDSS* (2016), 1–15.

[40] Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S., and Vigna, G. Framing dependencies introduced by underground commoditization. In *Workshop on the Economics of Information Security* (2015).