Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

The looming shadow of illicit trade on the internet

Peggy E. Chaudhry

Villanova School of Business, Villanova University, 800 Lancaster Avenue, Villanova, PA 19085, U.S.A.

KEYWORDS
Darknet;
Internet piracy;
Malvertising;
Crimeware;
Ransomware;
Online black market;
Cybercrime prevention

Abstract Pirates on the virtual sea are supplying their illicit digital content and goods through cyberlockers and darknet markets. The deep web hosts darknet marketplaces selling a variety of wares, such as narcotics and weapons, and is testimony to the growth of illicit trade on the internet. The challenge of web sites that host digital content piracy is exacerbated through linkages to a variety of malware schemes that have created a lucrative crimeware economy. Digital thieves target unsuspecting consumers as digital bait to derive profits from a variety of malware schemes such as ransomware and malvertising. The hijacking of access to computers and their digital content in order to ransom them back to consumers or organizations is considered to be one of the leading threats of internet crime. Malvertising schemes are plaguing the internet advertising business—criminals are reaping profits by posting legitimate advertisements at content theft sites or using an army of botnets to fake advertising traffic. A variety of stratagems are evolving to curb this illicit trade, including fostering multi-lateral enforcement tactics, updating legislation to circumvent this type of crime on the internet, training digital savvy citizens, and creating private-sector remedies.

1. The Wild West of cyberspace

Two decades ago, Barry James (1996) characterized the internet as a "Wild West frontier town without a sheriff" and warned consumers about web services that offered bogus stock, other spurious schemes involving, for example, gold mines, gemstones, and ostrich farming, and even the possible loss of identity by way of email addresses and credit card numbers. The issue of pirated digital content and counterfeit merchandise obtained via the internet has been studied for over 2 decades with key sectors examined, including music, movies, software, and pharmaceuticals (Chaudhry, 2013; Chaudhry, Cesareo, & Stumpf, 2014). But, the continued global growth of consumer access to broadband and the use of several devices to access illicit digital content is fueling the growth for this type of illicit trade (Sudler, 2013).

To illustrate the progression of internet piracy, the top pirated movie in 2011 was *Fast Five* with an

E-mail address: peggy.chaudhry@villanova.edu

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.09.002

estimated 9.26 million downloads via a torrent site, a file sharing network and system often used to distribute pirated media (Chaudhry & Zimmerman, 2013). Four years later, *Interstellar* topped the 2015 piracy list with 46.8 million downloads (BBC News, 2015). TorrentFreak.com lists the top weekly pirated movies complete with each movie's IMDb.com rating and trailer; *Warcraft* topped the chart on July 3, 2016 (Ernesto, 2016). The illicit digital content of a movie on the internet can stem from a variety of sources: images taken in the theater using a camcorder or mobile phone (i.e., a CAMrip), a copy of an uncut version of the movie from the studio (i.e., a workprint), a copy of the retail version of the DVD or Blu-Ray DVD (i.e., a DVD Full-Rip or BRRip), or a file copy from a DRM-free streaming service like Hulu (i.e., a WEBRip).

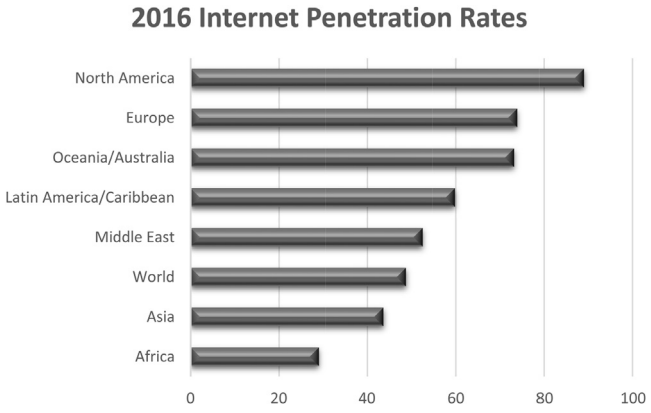
Pirates on the virtual sea continue to use different infringement ecosystems to supply illicit digital content and counterfeit goods: BitTorrents, cyberlockers, and darknet markets (NetNames, 2014). Chaudhry and Stumpf (2013) reported on the struggles of fake pharmaceuticals sold on the internet, but even more reprehensible are the Amazon-like marketplaces on the darknet selling other illicit goods such as narcotics and weapons. Consumers who visit these nefarious sites are exposed to other criminal activities like identity theft through malware and are lucrative digital bait for cybercriminals (Digital Citizens Alliance, 2015a). In July 2016, the limited geographic distribution of the new mobile game Pokémon GO created the opportunity for cybercriminals to serve unmet consumer demand by way of third-party websites. An unsuspecting Android consumer who side-loaded this game from a third-party website may have been infected with a Droidjack, a remote access control Trojan virus that gives total control over the mobile phone to the architect of the malware (Morris, 2016). The Business Software Alliance (2016) established significant linkages between installing illegitimate software and malware: the analysts discovered 430 million new pieces of malware in 2015, an increase of 36% from 2014. The internet advertising industry is struggling currently with 'malvertising' schemes that profit criminals either through the sale of advertisements that are posted on content theft sites and/or the use of an army of botnets to click repeatedly on advertising links to generate revenues.

In this article, the problem of illicit trade on the internet is addressed in the context of raising awareness about the threats and actions taken by a variety of stakeholders to mitigate this unlawful trade on the web. The main contributions advanced of this article involve: illustrating the significant growth of internet traffic for both fixed-access and mobile platforms to participate in both licit and illicit trade; describing the evolution of illicit supply chain ecosystems such as cyberlockers and darknets; recounting current malware schemes in the crimeware economy, specifically malvertising and ransomware, that ensnare unsuspecting consumers and employees of organizations as digital bait; portraying the criminal engineers involved and their ability to garner windfall profits; and discussing an array of stratagems to diffuse this trade that have been undertaken by enforcement agencies, government organizations, and companies.

2. Escalating demand for the internet

The size of the digital universe is measured in terms of the growth of internet penetration, the increased speed of bandwidth, and the number of devices used to access digital content. The Internet World Stats (2016) categorizes regions by internet penetration rates as a percent of total population. Figure 1

Figure 1. World internet penetration percentage rates by geographic region



Source: Internet World Stats (2016)

illustrates the divergent penetration rates by region, ranging from 27.5% in Africa to 86.9% in North America, with a world market internet penetration rate at 48.7%—an estimated global population of 7.34 billion for 2016.

Cisco (2016), a leading enterprise and service provider, released these projections to illustrate the exponential growth of demand on the internet:

- Global IP traffic will increase nearly threefold over the next 5 years, and will have increased nearly a hundredfold from 2005 to 2020.
- Smartphone traffic will exceed PC traffic by 2020. In 2015, PCs accounted for 53% of total IP traffic, but by 2020 PCs will account for only 29% of traffic.
- Traffic from wireless and mobile devices will account for two-thirds of total IP traffic by 2020. By 2020, wired devices will account for 34% of IP traffic, while wi-fi and mobile devices will account for 66% of IP traffic.
- Global internet traffic in 2020 will be equivalent to 95 times the volume of the entire global internet in 2005.
- The number of devices connected to IP networks will be three times as high as the global population in 2020.
- Broadband speeds will nearly double by 2020. By 2020, global fixed broadband speeds will reach 47.7 Mbps, up from 24.7 Mbps in 2015.

The data analysts at Sandvine continue to provide insight into internet trends and consumer traffic through their annual Global Internet Phenomena report. The Sandvine firm publishes internet traffic in each geographic region in various categories, including storage (e.g., Dropbox), gaming (e.g., Xbox Live), marketplaces (e.g., Apple iTunes), communications (e.g., WhatsApp), real-time entertainment (e.g., Netflix), social networking (e.g., Facebook), and web browsing (e.g., HTTP). These data analytics shed light on internet traffic patterns in upstream (data sent from a computer or network, e.g., uploading a file), downstream (data received to a computer or network, e.g., downloading a file), and aggregated total site traffic for a period of time. Table 1 illustrates the dominant internet traffic patterns in North America are real-time entertainment for downstream fixed access users. Netflix leads the aggregate category at a 32.72% share of total internet traffic. To better understand the shifts in demand due to changes in technology, in 2008, the aggregate internet traffic from fixed access using a BitTorrent was 31%; 8 years later it is 2.85%. This modification to usage patterns stems from the declining use of file sharing to employing storage applications such as iCloud, Dropbox, and Google's Cloud (Sandvine, 2016). As shown in Table 2, in the mobile access category, social networking and communications are the more prevalent options for internet consumption in this platform.

3. Creating illicit supply chain ecosystems

As illustrated in Tables 1 and 2, the licit use of cloud storages like iCloud or Google Cloud are employed in both fixed and mobile platforms. But, pirates are also using the cloud to enable others to upload illegal digital content that allows either direct download or video streaming for movies, television

Table 1. Top 10 peak period applications / North America, fixed access

Rank	Upstream	2016	Downstream	2016	Aggregate	2016
1	BitTorrent	18.37%	Netflix	35.15%	Netflix	32.72%
2	YouTube	13.13%	YouTube	17.53%	YouTube	17.31%
3	Netflix	10.33%	Amazon Video	4.26%	HTTP-Other	4.14%
4	SSL-OTHER	8.55%	HTTP-Other	4.19%	Amazon Video	3.96%
5	Google Cloud	6.98%	iTunes	2.91%	SSL-Other	3.12%
6	iCloud	5.98%	Hulu	2.68%	BitTorrent	2.85%
7	HTTP-Other	3.70%	SSL-Other	2.53%	iTunes	2.67%
8	Facebook	3.04%	Xbox One	2.18%	Hulu	2.47%
9	FaceTime	2.50%	Facebook	1.89%	Xbox One	2.15%
10	Skype	1.75%	BitTorrent	1.73%	Facebook	2.01%
	Total	74.33%	Total	75.05%	Total	73.40%

Source: Sandvine (2016)

Table 2. Top 10 peak period applications / North America, mobile access

Rank	Upstream	2016	Downstream	2016	Aggregate	2016
1	Facebook	14.85%	YouTube	20.87%	YouTube	19.16%
2	SSL-Other	14.02%	Facebook	13.97%	Facebook	14.07%
3	Google Cloud	9.28%	HTTP-Other	9.36%	HTTP-Other	9.32%
4	HTTP-Other	8.92%	SSL-Other	6.85%	SSL-Other	7.62%
5	YouTube	5.01%	Instagram	6.66%	Instagram	6.31%
6	Snapchat	4.36%	Snapchat	5.17%	Snapchat	5.09%
7	Instagram	3.35%	Netflix	3.72%	Google Cloud	3.56%
8	BitTorrent	2.16%	iTunes	3.02%	Netflix	3.41%
9	FaceTime	1.97%	Google Cloud	2.87%	iTunes	2.86%
10	iCloud	1.82%	MPEG-Other	2.37%	MPEG-Other	2.17%
	Total	65.74%	Total	74.86%	Total	73.57%

Source: Sandvine (2016)

shows, books, games, and the like. According to NetNames (2014), a leading business in online brand protection, these illicit cyberlockers monetize their operation by charging premium subscription fees to their clients, reaping advertising revenues through malvertising schemes, and selling third-party software. NetNames researched illicit activities at both direct download cyberlockers like 4Shared.com and streaming cyberlockers like YouWatch.org. The analysts at NetNames estimated total annual revenue from the 30 illegitimate sites at $96.2 million, with one illegitimate site earning $17.6 million per year.

One direct download cyberlocker, 4Shared.com, is currently offering a variety of subscription fees, including one for $9.95 per month for 100 GB of online space, ads-free sharing, and direct download links. A July 15, 2016 search for the movie *Interstellar* at 4Shared.com resulted in 853 hits in less than one second. NetNames (2014) estimated that 4Shared.com had monthly unique visitors of 55.4 million with monthly revenue at $985,024 and annual revenue at $11.82 million.

Streaming cyberlockers such as YouWatch.org give consumers the chance to earn up to $4 for 1,000 views of his or her shared video content and even offer compensation schemes for referrals via a 25% share of friends' earnings from the site. In contrast to direct download cyberlockers like 4shared.com, most streaming cyberlockers do not provide a search engine of the content of their site, so that a search engine links the viewer to its site. For example, a Google search of the phrase 'watch Interstellar' yields both licit (Google Play) and illicit (Putlocker.com) video streaming sites. A person seeking to videostream free content will navigate a learning curve of which sites to visit directly. NetNames (2014) estimated lower traffic and revenues for these types of sites since their premium subscriptions are lower than direct download sites. For YouWatch.org, the analysts estimated 13.9 million monthly unique visitors with $154,171 in monthly revenue or $1.34 million in annual revenue. The costs of doing business at these cyberlocker sites include hosting and internet infrastructure, reward schemes (e.g., payments for uploaders), financial transaction fees for processing premium accounts, employee salaries, and the like. But, profit margins for these illicit online businesses can exceed 80% (NetNames, 2014).

A team of deep web experts at BrightPlanet (2014) claims that distinctions between 'surface,' 'deep,' and 'dark' webs are necessary to better understand the internet ecosystem. The 'surface web'—sometimes referred to as the visible web, indexed web, clearnet, or lightnet—is that portion of the internet that is used to find information through standard search engines that use crawling technology to locate web links (e.g., Google, Bing). BrightPlanet coined the term 'deep web' to illustrate that other part of the internet that cannot be reached through a standard search engine—websites that hold content like electronic bank statements that cannot be crawled or indexed by search engines. The 'dark web' is simply a portion of the deep web that has been intentionally hidden and is inaccessible through common web browsers. In its study, ''Busted, but not Broken: The State of Silk Road and the Darknet Marketplace,'' the Digital Citizens Alliance (2014) reported that three basic building blocks are required to create a darknet virtual store: (1) use of the Tor Network, which enables anonymous communication through a volunteer network of servers designed to conceal a user's location and usage from network surveillance; (2) employment of a cryptocurrency payment mechanism such as Bitcoin; and (3) effective management of the online store by way of discussion forums.

Table 3. The current state of the darknet economy

Darknet Marketplaces (2014)	Drug Listings	Total Listings	Weapons
Silk Road 2.0	13,648	17,192	No
Agora	7,400	9,158	Yes
Pandora Openmarket	5,249	5,812	No
Evolution	2,623	5,523	Yes
BlueSky Marketplace	1,740	1,833	No
Dark Bay	292	329	No
The Pirate Market	247	367	Yes
Outlaw Market	230	246	No
Tor Bazaar Alpha	205	252	Yes
Black Bank Market	201	239	No
White Rabbit Anonymous MarketPlace	194	256	Yes
Total listings	32,029	41,207	

Source: Digital Citizens Alliance (2014)

The darknet provides a marketplace of disreputable illicit trade; the notorious Silk Road marketplace offered forged official documents, secret bank accounts, hacking techniques, phishing/spam services, anonymous mail drops, hard drugs, and access to other darknets. Table 3 illustrates the names of darknet marketplaces—focusing on the number of their narcotics listings and whether the organizers of these sites offer the sale of weapons (Digital Citizens Alliance, 2014).

3.1. Increasing profits through malware stratagems

A recent study, ''Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Data,'' illustrated the increasing use of software designed with a malicious intent, 'malware,' for a myriad of monetary gains on the internet (Digital Citizens Alliance, 2015a). One out of every three sites that host pirated content contains some type of malware and a person is 28 times more likely to get malware than if he or she visits a licit site with licensed content providers (Digital Citizens Alliance, 2015a). For example, current examples of malware tactics include harvesting personal data (credential theft), locking access to the computer and ransoming the rights back (ransomware), or spying on the unsuspecting person through a webcam to re-sell web streams in forums or to use as blackmail (the so-called slaver).

The Federal Bureau of Investigation (2016) reported that ransomware attacks are designed to target both individuals and organizations such as hospitals, state and local governments, and enforcement agencies. The malware is planted to entice an individual or an employee of an organization to click on a link embedded in a phishing email or at a website. But, other technology allows a cybercriminal to attach malware via drive-by download, which does not require any links to be clicked at the site (Digital Citizens Alliance, 2015a). In ransomware schemes, the goal of hijacking the computer or network is straightforward: the malware locks access to the files on the computer/network and eventually the digital thieves demand a ransom payment, typically in Bitcoin currency (FBI, 2016). In a study conducted by the Digital Citizens Alliance (2015a), analysts found that malware was almost evenly split between user initiated downloads (55%) and drive-by downloads (45%). The U.S. Department of Justice (2015) revealed through its internet crime complaint center that an estimated $57.6 million in damages have incurred since 2005 in ransomware, where consumers have paid $200—$10,000 in ransom money to regain access to their personal computers. An estimated ransom value of $24 million was paid in 2015 for this type of malware scam (Turkel, 2016).

Many managers and policymakers are focusing on this problem in the crimeware economy because the risk is great and the free movie, game, or software is literally a token enticement to reap the ultimate goal—the hijacking of the computer. In summary, Table 4 gives a succinct description of common types of malware and the estimated monetization for cybercriminals.

3.2. Growing exploitation of malvertising schemes

A PricewaterhouseCoopers (2016) study reports a 20.4% increase in online advertising revenue in

Table 4. Types of malware and monetization

Type of Malware	Monetary Value
Trojans: Software that installs itself without the user's knowledge either secretly or hidden inside seemingly benign user actions such as opening an email or web page. Most Trojans open up unauthorized access to the victims' computer.	Credit cards: Up to $135 per consumer credit card on underground internet exchanges
Remote Access Trojans: A particularly powerful form of Trojan that gives the attacker administrative access to the user's computer. Hackers use RATs to steal data and control webcams, even making videos of unsuspecting victims.	Ransomware: Between $100-$500 for consumers to regain access to their PC
Adware: Software designed to make money through ads targeted at the computer's users. Adware is often installed without the user's consent as part of another program. Adware programs can be highly invasive, running in the background and serving pop-ups to the user even when they are not browsing, and collecting their personal data in order to target them with more profitable ads.	$50-$100 pay rate per 1,000 installs
Botnet: A distributed system of internet-connected computers acting as a group at the command of a Bot controller, who directs them to perform certain tasks. Botnets are used to fake advertising traffic, attack websites in Distributed Denial of Service (DDOS) attacks, and carry out spam and phishing campaigns.	Malvertising campaigns were estimated to cost the internet ad industry $200 million in 2014

Source: Digital Citizens Alliance (2015a)

the U.S. from $49.5 billion in 2014 to $59.6 billion in 2015. Major industry sectors that are paying for online advertisements include retail (22%), financial services (13%), auto (13%), telecom (9%), leisure travel (9%), consumer packaged goods (6%), consumer electronics and computers (7%), media (5%), pharmaceuticals and healthcare (5%), and entertainment (5%). The dominant revenue categories in internet ads come from search (34%) and mobile (35%) ad formats in the U.S. (Interactive Advertising Bureau, 2016). eMarketer (2015) estimates that the global search ad spending revenue was $81.59 billion in 2015, with Google taking a dominant market share (54.5%); its closest competitor, the Baidu search engine of China, has just an 8.8% share.

The billion-dollar internet ad business with double-digit growth has attracted cybercriminals who can earn illicit ad revenue in basically two ways—either selling licit ads that appear on content theft sites and/or using malware to set up botnets that work through personal computers to generate a significant number of ad clicks (Johnson, 2015). As reported in "Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business," experts estimate that $209 million internet ad revenue was derived from the 589 illicit sites in this study. Further, these professionals claim that windfall profit margins from deploying malvertising schemes range from 86% to 93% for the architects of this type of malware (Digital Citizens Alliance, 2015b).

4. Identifying the masterminds of illicit trade on the internet

Attempting to portray the cyber desperados involved in internet crime is an elusive task; even the Federal Bureau of Investigation (FBI, n.d.) is offering large financial rewards for any information leading to the pursuit of its Cyber Most Wanted list. These architects of the dark side of the 'Wild West' internet frontier have online monikers like lucky12345, The Pro, Nitrojen26, and Dread Pirate Roberts. The Federal Bureau of Investigation (FBI) has a $4.2 million bounty on any information leading to Evgeniy Mikhailovich Bogachev—the alleged architect of the Zeus Trojan, a malware package known as GameOver Zeus that harvested bank account numbers, passwords, and personal identification numbers. If caught, Bogachev faces charges that include "computer fraud, bank fraud, wire fraud, money laundering, conspiracy to participate in racketeering activity, conspiracy to violate the computer fraud and abuse act, and aggravated identity theft" (Stevenson, 2015).

Ross Ulbricht, the alleged founder of Silk Road on the darknet under the pseudonym Dread Pirate Roberts, was described by prosecutors as "the kingpin of a world-wide digital drug-trafficking enterprise" (cited in Weiser, 2015). Silk Road was a marketplace for a plethora of illicit goods, but more well-known for its access to narcotics such as heroin and LSD. In its 3 years of existence, Silk Road

(version 1.0) was considered to be the blueprint for this type of illicit marketplace. Authorities estimated that the site facilitated 1.5 million transactions, over 100,000 buyer accounts, and $213.9 million in sales (Thielman, 2015; Weiser, 2015). In sentencing Ross Ulbricht to life imprisonment, Judge Forrest of the Federal District Court in Manhattan ruled (cited in Thielman, 2015):

> The stated purpose [of Silk Road] was to be beyond the law. In the world you created over time, democracy didn't exist. You were captain of the ship, the dread [sic] Pirate Roberts. You made your own laws.

Ross Ulbricht's case is now under appeal and a part of the defense argument ironically centers on the involvement of corrupt federal agents involved in the undercover operation to shut down Silk Road: Carl Mark Force IV of the Drug Enforcement Administration and Shaun Bridges of the Secret Service (Greenberg, 2016). Carl Mark Force IV, was sentenced to 78 months for his role in extorting Bitcoins from Ross Ulbricht and a CoinMKT customer in the undercover operation that led to the demise of Silk Road (Jeong, 2015). In 2015, the filmmakers of the documentary *Deep Web* questioned whether Ross Ulbricht could have acted alone to create Silk Road and whether it was really the first darknet marketplace for drugs in the deep web.

Seven years ago, the media reported on the founding members of The Pirate Bay—Frederik Neij, Gottfrid Svartholm Warg, Carl Lundstrom, and Peter Sunde—who were sentenced to 1 year in jail and fined $4.5 million in damages to be paid to such companies as Warner Brothers, Sony Music Entertainment, EMI, and Columbia Pictures. One must understand the bravado of the mindsets of the pirates (and their colleagues and followers) to better understand different interpretations of these criminal masterminds on the web. For example, Peter Sunde of The Pirate Bay made this media statement after the Swedish court verdict (BBC News, 2009):

> It's so bizarre that we were convicted at all and it's even more bizarre that we were [convicted] as a team. The court said we were organized. I can't get Gottfrid out of bed in the morning. If you're going to convict us, convict us of disorganized crime. We can't pay and we wouldn't pay. Even if I had the money I would rather burn everything I owned, and I wouldn't even give them the ashes.

Many pirates on the virtual sea are anonymous and adopt different codenames and/or belong to organizations that support their nefarious activities. One such organization, Darkode, was characterized as a think tank for cybercriminals that carefully vetted its membership through sponsorship. The FBI (2015a) described the induction process to Darkode reminiscent to traditional Mafia organized crime, in that:

> [A] potential candidate for forum membership had to be sponsored by an existing member and sent a formal invitation to join. In response, the candidate had to post an online introduction—basically, a resume—highlighting the individual's past criminal activity, particular cyber skills, and potential contributions to the forum. The forum's active members decided whether to approve the applications.

A key point in describing the profile of cyber criminals centers on determining whether illicit traders are involved in some type of competition to be the first to post digital content without the goal of monetary rewards. The 'warez scene' is a generic term used to describe the cybercrime community responsible for stripping software of its copyright protection and placing it on the internet for downloading without financial compensation. Members of this group can be the first-providers—the original source for the illegal trading and online distribution of pirated works. Once a release group prepares a stolen work for distribution, the material is distributed in minutes to secure, top-level servers and made available to a select clientele (Arxan, 2015).

The book *How Music Got Free: The End of an Industry, the Turn of the Century, and the Patient Zero of Piracy* (Witt, 2015) gives testimony to this type of illicit behavior with no financial motives. Dell Glover, a factory worker at a CD-burning plant in North Carolina, smuggled CDs with the primary intent to leak the digital content onto the internet to compete with other groups on the scene. This blue-collar worker is attributed to be one of the key actors leading to the demise of the music industry with no goal of financial gain—Glover simply participated in a competition to be the first to release songs onto the web. Release groups can be hierarchical, highly-structured organizations with leadership positions that control day-to-day operations, recruit new members, and manage the group's various computer archive sites (Witt, 2015). These groups exist solely to engage in content theft and compete with each other to be the first to place a newly pirated work onto the internet, often before the work is legitimately available to the public. The groups employ highly sophisticated technological measures to shield their illegal activity from victims and law enforcement.

5. Strategies to impede illegal virtual marketplaces

The problem of botnets and adware is at the very center of debate amongst the FBI, U.S. Department of Justice, Homeland Security, and industry experts in terms of how to develop tactics to defray this criminal activity. Of primary concern is consumer privacy and security issues (Slefo, 2016). Principal enforcement agencies including Europol and the FBI continue to fight the illicit businesses and each agency hosts its own centers for this type of crime: the FBI Internet Crime Complaint Center (www.ic3.gov) and Europol's European Cybercrime Centre (EC3) (www.europol.europa.eu/content/megamenu/european-cybercrime-centre-ec3-1837). The agencies continue to shut down illicit web sites, but also are focusing on malware schemes and darknet marketplaces. Both government and private-sector alliances have created online education platforms for consumers and employees to foster savvier digital users who understand the repercussions of malware for their personal computers, mobiles, and organizations. The private-sector continues to use price and licit businesses like Netflix to decrease demand for pirated digital content. The internet advertising business has created its own industry safeguards to curb the growth of malvertising schemes. A few examples of each stratagem are given to illustrate recent efforts to combat illicit trade on the internet.

5.1. Employing multi-lateral enforcement agencies

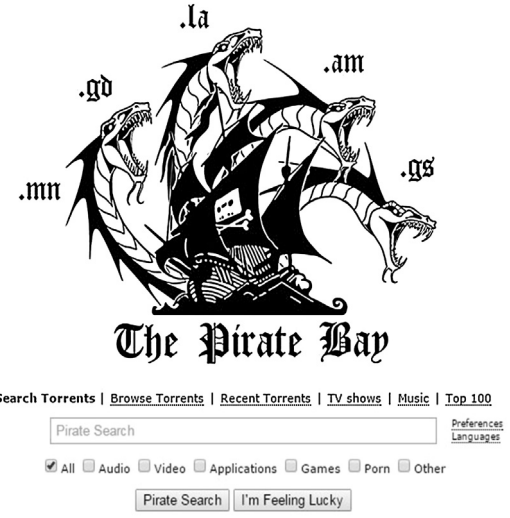
Sixteen years ago, government enforcement agencies were using undercover operations like Operation Buccaneer to target the warez scene—including groups like RiSCISO, Razor 1911, and POPZ—for their illicit distribution of content theft in the software, game, and movie sectors. Later, Operation Digital Gridlock investigated and prosecuted illicit file-sharing sites of The Underground Network, yielding felony convictions for copyright piracy that employed P2P networks. In 2005, Operation Site Down, included the assistance of the enforcement agencies of 10 countries and again targeted the warez scene for content theft in the same sectors of software, movies, music, and games. Now, over 10 years later, the undercover operations of Europol and the FBI, among others, have new targets: malware and botnet schemes and the darknet (Europol, 2015b). Multi-lateral undercover sting operations, such as Operation Shrouded Horizon in 2015, represent the joint efforts of enforcement agencies in 20 countries to pursue the cyber criminals in the Darkode forum.

The GameOver Zeus (GOZ) botnet used malware to harvest banking credentials from a global network of computers. After securing the banking credentials, the funds were redirected via wire transfer to the cybercriminal's account. The FBI (2014) estimated losses for this scheme at $100 million. The U.S. Department of Justice (2014) described GameOver Zeus as the "most sophisticated botnet the FBI and our allies have ever attempted to disrupt" and claims that 500,000 to 1 million computers are infected with the virus, an estimated 25% of which were U.S. computers. The U.S. Department of Homeland Security, through its Computer Emergency Readiness Team, provides assistance for removing the GOZ malware (https://www.us-cert.gov/ncas/alerts/TA14-150A). The darknet was targeted through Operation Onymous, resulting in the disruption of the Silk Road 2.0 and arrest of its creator. The main enforcement agencies involved in the takedown were Europol's EC3, the FBI, the U.S. Immigration & Customs Enforcement, and Homeland Security Investigations. The Head of EC3 remarked on the novelty of this taskforce by reiterating that the enforcement agencies were not just removing services from the internet, but were using the TOR network to shut down marketplaces on the darknet where criminals have considered their actions beyond the reach of the law (Europol, 2015a).

In 2015, the FBI—with the assistance of enforcement agencies in 19 countries—took down the members-only Darkode forum (estimated at 250—300 persons) that was a virtual marketplace for "buying, selling, and trading malware, botnets, stolen personally identifiable information, credit card information, hacked server credentials, and other pieces of data and software that facilitated complex cybercrimes all over the globe" (FBI, 2015a). This operation was overseen by the FBI with the assistance of Europol's EC3 and enforcement agencies in 20 countries (Europol, 2015a). Europol considered Darkode one of the top five cybercriminal forums that conducted its business in English, not a Russian platform.

Unfortunately, the analogy of the hydra is appropriate when it comes to cybercrime enforcement efforts: one illicit site is shut down and another opens. Some refer to this pattern as similar to playing the carnival game whack-a-mole with these illicit sites. For example, the demise of Silk Road 1.0 was copied into a Silk Road 2.0 marketplace by Blake Benthall (aka Defcon) and his alleged assistant, Brian Richard Farrell (aka DoctorClu) (Vinton, 2015). Today, it is claimed that a Silk Road 3.0 exists. A simple search in Google yields a "Guide on how to access the Silk Road 3.0" that is complete with an invitation to join an 'anonymity newsletter,'

Figure 2. The image of The Pirate Bay after the court decision



Key: .mn=Mongolia; .gd=Grenada; .la=Laos; .am=Armenia; .gs = South Georgia and the South Sandwich Islands. Source: www.geek.com

providing key information on how to remain anonymous online and to keep abreast of the latest news on the darknet marketplaces and deep web.[1]

After years of contention, a Swedish court seized The Pirate Bay's two main domains: thepiratebay.se and pirate.bay.se. Ironically, the pirates simply opened five additional web sites using other top-level country domains such as thepiratebay.mn (Mongolia). Figure 2 illustrates the iconic image of the hydra that circulated the web to portray the regeneration of The Pirate Bay in five other country domains immediately after the Swedish court took action (Plafke, 2015).

5.2. Updating legislation to punish digital thieves

The need for an update to copyright legislation is clear. The types of crimes are the same as those throughout the lore of the Wild West, gaining income via ransoms and theft, but technology has enabled crimes of new names and jargon such as remote access Trojan malware used for ransomware or malvertising schemes requiring armies of thousands of botnets. The U.S. Department of Justice requires new legislation to circumvent the illicit profits derived using unsuspecting consumers as digital bait. The Digital Citizens Alliance (2013) continues to be a key stakeholder in this arena and simply urges government policymakers in the U.S. Congress to contemplate a modernization of existing laws to safeguard digital platforms from becoming a safe-haven for criminal enterprises. The proposed Botnet Prevention Act of 2016 sponsored by U.S. senators Sheldon Whitehouse, Lindsey Graham, and Richard Blumenthal would establish new legislation that will close loopholes for this type of crime. The U.S. Chamber of Commerce (2016) strongly supports this act and in its letter to senators Graham and Whitehouse, both members of the Subcommittee on Crime and Terrorism state:

> [T]he Chamber urges policymakers to increase the costs on attackers. Law enforcement can point to notable successes in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity. But organizations perpetrating such acts are not fearful of attribution, extradition, and prosecution to the degree that it seriously impacts their cost/benefit calculations.

The key provisions of the Botnet Prevention Act center on (1) enhancing the Department of Justice's authority to secure injunctions and shutdown botnets that go beyond fraud or illegal wiretapping to include other criminal acts, such as destruction of data; (2) granting judges the ability to levy stiffer penalties on those who attack the computers that control infrastructure, such as power plants and hospitals; and (3) allowing penalties to include the sellers that provide access to the compromised computers on the botnet, since the seller may not be the person who initially enslaved the computers (Whitehouse, 2016).

5.3. Creating digital-savvy citizens

We have studied the variables that explain a consumer's willingness to obtain pirated digital content and/or counterfeit goods for a few decades. For example, Chaudhry and Stumpf (2011) developed a framework that included both intrinsic determinants (for example, attitudes toward the counterfeits, cultural values, and ethical perspective) versus extrinsic determinants (for example, the hedonic shopping experience of obtaining illicit goods). Anti-piracy messaging themes have employed role models to denounce piracy, educated consumers and employees to safeguard intellectual property, and created a fear of prosecution (Chaudhry & Zimmerman, 2013). Today, we see a strong focus on educating consumers and employees to understand the risks associated with internet crimes. For example, Quicke (2015) examines the

[1] See http://silkroaddrugs.org/guide-on-how-to-access-the-silk-road-3-0/

Business Software Alliance campaign "Facts Don't Lie. Using Unlicensed Software is Risky!" informing employees about the correlation between using unlicensed software and the increased risk of cyber-attacks. In its 2016 Global Software Survey, the Business Software Alliance (2016, p. 3) claims that "twenty six percent of employees admitted installing outside software on work computers, and of those 84 percent acknowledged installing two or more unauthorized programs."

In 2012, the FBI worked in conjunction with the National Center for Missing & Exploited Children, teachers, and schools to develop its Safe Online Surfing program (https://sos.fbi.gov/). Teachers can sign up to work through this website to incorporate the basic underpinnings of internet safety measures for their students. The website includes different grade levels and will administer an online quiz for each student in the class. For example, at the 7th grade module students are educated via scenarios related to copyright infringement and reputable sites. The FBI (2015b) claims that this program is a huge success and reports that 275,656 students in 5,053 schools in 49 states, D.C., Puerto Rico, and the North Mariana Islands were engaged in this programming in 2015.

The National Cyber Security Alliance (NCSA) merges both private sector and public sector stakeholders with its primary mission to train a global digital society to use the internet safely and securely. The alliance includes companies in various sectors, such as the Bank of America, Facebook, Google, Intel, and PayPal. The training modules at StaySafeOnline.org are for consumers ("I want to stay safe online"), teachers ("I want to teach online safety"), or businesses ("I want to keep my business safe online"). The NCSA site provides consumers with instruction on how to keep a clean machine with information on malware and botnets, spam and phishing, hacked accounts, and home network security. Businesses are given advice on how to assess their risks, monitor attacks, report cyber-attacks, implement a cybersecurity plan, protect customers, and train employees. The alliance hosts its own Stop.Think.Connect. campaign website in multiple languages to target a global community of internet users (https://www.stopthinkconnect.org/). Working with the Department of Homeland Security (2016), the NCSA sponsors an annual National Cyber Security Awareness Month and each week hosts a distinct topic such as recognizing and combating cybercrime.

5.4. Employing private-sector remedies

The digital content industries are at the critical juncture of making consumers believe that obtaining content through legal commerce is more convenient than stealing. Companies like Netflix, iTunes, and Hulu have proven to be valid alternatives to movie piracy, as vast libraries of motion pictures and television shows are available through either an inexpensive monthly subscription or a single rent/download. The growth of licit video streaming sites like Netflix will continue to deter piracy, but other illicit sites like Popcorn Time continue to thrive on the internet (Stone, 2015). The CFO of Netflix, David Wells, directly linked the incidence of piracy in overseas markets to the company's pricing schemes by stating (cited in Price, 2015):

> Piracy is a governor in terms of our price in high piracy markets outside the US. We wouldn't want to come out with a high price because there's a lot of piracy, so we have to compete with that.

Sony Pictures and the Industry Trust (n.d.), the film and TV industry association in the U.K., have launched the Moments Worth Paying For campaign, using role models like Spider-Man to denounce piracy. The short anti-piracy trailer developed for blockbuster movies like *Spooks: Greater Good* (released in the U.S. as *MI-5*) simply reinforces the price/value concept by showing the entertainment value of the theatrical experience.

In 2015, Microsoft boldly offered a free upgrade of Windows 10 to Chinese consumers who owned both genuine and illicit copies of its software with the goal of reengaging millions of these consumers who had been lost due to piracy. In addition, Microsoft plans to attract licit consumers in China by way of selling Office over the internet and creating a Windows 10 app for smartphones and personal computers for its QQ gaming and messaging services (Rigby & Carsten, 2015).

In 2014, the Association of National Advertisers, the American Association of Advertising Agencies, and Interactive Advertising Bureau created their own anti-piracy program, the Brand Integrity Program Against Piracy. The anti-piracy program assists advertisers and their technology partners to filter through websites using Digital Advertising Assurance Providers (DAAPs) to screen out the placement of their ads on infringing sites (Trustworthy Accountability Group, 2016). Several of the world's leading ad agencies, such as WPP's GroupM, supported this initiative (Johnson, 2015).

6. Conclusion

The goal of this article is to raise awareness about the risks and sanctions taken by several stakeholders

to mitigate the encroaching shadow of illicit trade on the internet. An overview of growing internet access and broadband speeds, evolving illicit supply chain ecosystems, flourishing malware schemes, and cunning criminal mindsets provide the main background necessary to comprehend this type of illicit trade. Technology advances on the internet provide an ironic paradox. On the one hand, internet traffic has exploded to satisfy the insatiable appetite of consumers for licit digital entertainment through Netflix, Amazon Video, Hulu, and the like. On the other hand, this has created a window for illicit supply chain ecosystems to attract unlawful consumption.

A narrative of the criminal masterminds who create darknets such as Silk Road or enslave thousands of personal computers through botnets shed an additional perspective on the architects of this nefarious trade. A key point to consider is whether these masterminds are involved for monetary gain. Some are not—for them, cybercrime is simply a competition to be the first to post illicit digital content on the web. But, by illustrating several examples of the financial gains attainable in this trade, we make it clear that criminals can reap windfall profits through content theft websites, malware schemes, and darknet marketplaces.

The growing trends of internet crime, such as ransomware that effectively ensnares unsuspecting consumers and employees of organizations as digital bait, are a major concern for both privacy and security issues. Principal enforcement agencies, such as the FBI and Europol, continue to enlist multi-country undercover operations to eradicate darknets and diffuse malware schemes. U.S. senators have taken the lead to propose new legislation to effectively penalize cyber criminals who enslave computers through botnets to commit crimes. Government agencies and the private-sector have established online training programs to foster digitally savvy citizens. Consumers and employees of organizations need to know how to safeguard their personal mobile devices, computers, and networks. The development of programs like the Safe Online Surfing program that trains youth in the U.S. to be diligent cybercitizens is testimony to the need to instill a more broad-based recognition of this challenge.

The private sector continues to assuage the illicit trade with its own remedies, ranging from price competition with high-piracy markets to creating their own brand integrity programs. Netflix is dominating licit markets in North America with its low subscription fees and quality of service and is prepared to attract consumers away from illegitimate marketplaces in other countries with lower prices. The strategy is simple: provide value and delivery to make consumers believe that legal commerce is more convenient than stealing. The Interactive Advertising Bureau has just launched its own initiative, a brand integrity program designed to screen out the placement of ads on infringing sites to diffuse the growth of malvertising schemes. The tactics discussed in this article are just a few ways designed to eradicate the crimeware economy on the web. A long-term solution requires all of us, not just cybercrime experts, to enforce lawful online behavior and protect the internet. We need to be more savvy about this dark side of the web, and to create and support more stratagems to eradicate illicit trade. If we do not, the looming shadow will persist.

References

Arxan. (2015). *A look inside the universe of pirated software and digital assets*. Available at http://landing.arxan.com/state_of_application_security/

BBC News. (2009, April 17). *Court jails Pirate Bay founders*. Retrieved July 17, 2016, from http://news.bbc.co.uk/1/hi/technology/8003799.stm

BBC News. (2015, December 30). *Interstellar is most pirated movie of 2015*. Retrieved July 1, 2016, from http://www.bbc.co.uk/news/technology-35198319

BrightPlanet. (2014, March 27). *Clearing up confusion — deep web vs. dark web*. Retrieved July 1, 2016, from https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

Business Software Alliance. (2016, May). *Seizing opportunity through license compliance: BSA global software survey*. Retrieved July 1, 2016, from http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf

Chaudhry, P. (2013). Curtailing the growth of illegal online pharmacies. *Journal of Management Systems, 23*(1), 55—68.

Chaudhry, P., Cesareo, L., & Stumpf, S. (2014). What influences rampant movie piracy? *Journal of Management Systems, 24*(4), 73—95.

Chaudhry, P., & Stumpf, S. (2011). Consumer complicity with counterfeit products. *Journal of Consumer Marketing, 28*(2), 139—151.

Chaudhry, P., & Stumpf, S. (2013). The challenge of curbing counterfeit prescription drug growth: Preventing the perfect storm. *Business Horizons, 56*(2), 189—197.

Chaudhry, P., & Zimmerman, A. (2013). *Protecting your intellectual property rights: Understanding the role of management, governments, consumers, and pirates*. Berlin: Springer-Verlag.

Cisco. (2016). *Cisco visual networking index: Forecast and methodology, 2015-2020*. Retrieved July 4, 2016, from http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

Department of Homeland Security. (2016, June 30). *National cyber security awareness month*. Retrieved July 1, 2016, from https://www.dhs.gov/national-cyber-security-awareness-month

Digital Citizens Alliance. (2013). *Digital citizens issue alert: Copyright modernization and consumer protection*. Retrieved June

30, 2016, from http://www.digitalcitizensalliance.org/cac/alliance/getobject.aspx?file=DCA_copyright

Digital Citizens Alliance. (2014, April). *Busted but not broken: The state of Silk Road and the darknet marketplaces*. Retrieved June 15, 2016, from https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/5f8d4168-c36a-4f78-b048-f5d48b18dc0a.pdf

Digital Citizens Alliance. (2015a, December). *Digital bait: How content theft sites and malware are exploited by cybercriminals to hack into internet users' computers and personal data*. Retrieved May 1, 2016, from http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=digitalbait

Digital Citizens Alliance. (2015b, May). *Good money still going bad: Digital thieves and the hijacking of the online ad business*. Retrieved February 1, 2016, from http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=GMGB2

eMarketer. (2015, March 31). *Google will take 55% of search ad dollars globally in 2015*. Retrieved July 2, 2016, from http://www.emarketer.com/Article/Google-Will-Take-55-of-Search-Ad-Dollars-Globally-2015/1012294

Ernesto. (2016, July 3). *Top 10 most pirated movies of the week*. Retrieved July 3, 2016, from https://torrentfreak.com/top-10-pirated-movies-week-062016/

Europol. (2015a, July 15). *Cybercriminal Darkode forum taken down through global action*. Retrieved July 1, 2016, from https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action

Europol. (2015b). *Exploring tomorrow's organized crime*. Retrieved January 15, 2015, from https://www.europol.europa.eu/sites/default/files/edi/EuropolReportDigitalCove.html

FBI. (n.d.). *Cyber's most wanted*. Available at https://www.fbi.gov/wanted/cyber

FBI. (2014, July 11). *GameOver Zeus botnet disrupted*. Retrieved July 1, 2016, from https://www.fbi.gov/news/stories/gameover-zeus-botnet-disrupted

FBI. (2015a, July 15). *Cyber criminal forum taken down*. Retrieved June 30, 2016, from https://www.fbi.gov/news/stories/2015/july/cyber-criminal-forum-taken-down/cyber-criminal-forum-taken-down

FBI. (2015b, June 12). *FBI safe online surfing internet challenge: Cyber safety for young Americans*. Retrieved July 1, 2016, from https://www.fbi.gov/news/stories/copy_of_fbi-safe-online-surfing-internet-challenge

FBI. (2016, April 29). *Incidents of ransomware on the rise*. Retrieved June 30, 2016, from https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

Greenberg, A. (2016, June 18). Silk Road prosecutors argue Ross Ulbricht doesn't deserve a new trial. *Wired*. Retrieved July 13, 2016, from https://www.wired.com/2016/06/silk-road-prosecutors-argue-ross-ulbricht-doesnt-deserve-new-trial/

Interactive Advertising Bureau. (2016, April 21). *U.S. internet ad revenues hit landmark $59.6 billion in 2015*. Retrieved July 9, 2016, from http://www.iab.com/news/us-internet-ad-revenues-hit-landmark-59-6-billion-in-2015/

Internet World Stats. (2016, June 30). *Internet usage statistics*. Retrieved July 1, 2016, from http://www.internetworldstats.com/stats.htm

James, B. (1996, August 5). Big brothers abound in virtual new world. *The New York Times*. Retrieved August 2, 2015, from http://www.nytimes.com/1996/08/05/business/worldbusiness/05iht-cyber.t.html

Jeong, S. (2015, March 31). Criminal charges against agents reveal staggering corruption in the Silk Road investigation. *Forbes*. Retrieved June 16, 2016, from http://www.forbes.com/sites/sarahjeong/2015/03/31/force-and-bridges/#18b6f75660cb

Johnson, L. (2015, September 23). GroupM singles out piracy websites as marketers' next ad-fraud headache costing advertisers $200 million a year. *AdWeek*. Retrieved June 30, 2016, from http://www.adweek.com/news/technology/groupm-singles-out-piracy-websites-marketers-next-ad-fraud-headache-167090

Morris, D.Z. (2016, July 10). Hackers are spreading malware through Pokémon Go. *Fortune*. Retrieved July 12, 2016, from http://fortune.com/2016/07/10/pokemon-go-malware/

NetNames. (2014). *Behind the cyberlocker door: A report on how shadowy cyberlocker businesses use credit card companies to make millions*. Retrieved July 8, 2016, from http://www2.itif.org/2014-netnames-profitability.pdf

Plafke, J. (2015, May 19). *The Pirate Bay domain seized, sets sail for new home*. Retrieved July 4, 2015, from http://www.geek.com/news/the-pirate-bay-domain-seized-sets-sail-for-new-home-1623174/

Price, R. (2015, April 17). Netflix has an ingenious, piracy-combating way to set its international pricing. *Business Insider*. Retrieved July 2, 2015, from http://uk.businessinsider.com/netflix-piracy-international-pricing-streaming-earnings-2015-4

PricewaterhouseCoopers. (2016, April 21). *IAB internet advertising revenue report*. Retrieved July 11, 2016, from http://www.iab.com/wp-content/uploads/2016/04/FY2015-PwC-IAB-Webinar-Presentation.pdf

Quicke, S. (2015, June 24). BSA targets London with software education campaign. *Computer Weekly*. Retrieved July 14, 2016, from http://www.computerweekly.com/microscope/news/4500248674/BSA-targets-London-with-software-education-campaign

Rigby, B., & Carsten, P. (2015, March 18). Microsoft tackles China piracy with free upgrade to Windows 10. *Reuters*. Retrieved August 1, 2015, from http://www.reuters.com/article/us-microsoft-china-idUSKBN0ME06A20150318

Sandvine. (2016). *2016 global internet phenomena*. Available at https://www.sandvine.com/trends/global-internet-phenomena/

Slefo, G. (2016, June 1). FBI, Justice Department, and Homeland Security set to meet industry leaders on 'malvertising': Trustworthy accountability group says law enforcement to attend meeting. *Ad Age*. Retrieved July 11, 2016, from http://adage.com/article/digital/fbi-doj-meet-tag-discuss-malvertising/304242/

Stevenson, A. (2015, July 2). The FBI is offering $4.2m for info on the creator of the world's most infamous malware. *Business Insider*. Retrieved June 30, 2016, from http://uk.businessinsider.com/fbi-zeus-cyber-crime-malware

Stone, B. (2015, February 26). This torrenting app is too good to be legal. *Bloomberg*. Retrieved June 15, 2015, from http://www.bloomberg.com/news/articles/2015-02-26/popcorn-time-torrent-app-makes-piracy-easier-than-ever

Sudler, H. (2013). Effectiveness of anti-piracy technology: Finding appropriate solutions for evolving online piracy. *Business Horizons, 56*(2), 149—157.

Trustworthy Accountability Group. (2016). *Anti-piracy program application*. Retrieved July 11, 2016, from https://tagtoday.net/anti-piracy-program-application/

The Industry Trust. (n.d.). *Promoting the value of copyright and creativity*. Retrieved July 2, 2016, from http://www.industrytrust.co.uk/what-we-do/current-campaigns/

Thielman, S. (2015, May 29). Silk Road operator Ross Ulbricht sentenced to life in prison. *The Guardian*. Retrieved June 15, 2016, from https://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced

Turkel, D. (2016, April 7). Victims paid more than $24 million to ransomware criminals in 2015—and that's just the beginning. *Business Insider*. Retrieved May 1, 2016, from http://uk.businessinsider.com/doj-and-dhs-ransomware-attacks-government-2016-4

U.S. Chamber of Commerce. (2016, May 20). *U.S. Chamber letter in support of S. 2931, the "Botnet Prevention Act of 2016."* Retrieved June 10, 2016, from https://www.uschamber.com/letter/us-chamber-letter-support-s-2931-the-botnet-prevention-act-2016

U.S. Department of Justice. (2014). *U.S. leads multi-national action against "GameOver Zeus" botnet and "Cryptolocker" ransomware, charges botnet administrator.* Retrieved July 1, 2016, from https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

U.S. Department of Justice. (2015). *2015 internet crime report*. Retrieved May 15, 2016, from https://pdf.ic3.gov/2015_IC3Report.pdf

Vinton, K. (2015, January 21). Alleged Silk Road 2.0 operator's right-hand man arrested on drug charges. *Forbes*. Retrieved July 13, 2016, from http://www.forbes.com/sites/katevinton/2015/01/21/silk-road-2-0-administrator-doctorclu-arrested-on-drug-charges/#52b575fc37a1

Weiser, B. (2015, May 29). Ross Ulbricht, creator of Silk Road website, is sentenced to life in prison. *The New York Times*. Retrieved July 1, 2016, from http://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html?_r=0

Whitehouse, S. (2016, May 19). *Whitehouse, Graham, Blumenthal announce Botnet Prevention Act*. Retrieved June 10, 2016, from http://www.whitehouse.senate.gov/news/release/whitehouse-graham-blumenthal-announce-botnet-prevention-act

Witt, S. (2015). *How music got free: The end of an industry, the turn of the century, and the patient zero of piracy.* New York: Viking Press.