



## TABLE OF CONTENTS

INTRODUCTION AND SUMMARY	
OBJECTIVES AND METHODOLOGY	3-5
Objectives	
Quantitative Study Methodology Overview	
Sample Design	
Control Group Design	4
Data Collection	4
Data Availability	4
Profile of a Crimeware Distribution Network	5
QUANTITATIVE FINDINGS	6-7
Sites with Malware Incidents	6
Malware Incident Rates for Users Visiting These Sites	6
How Malware is Delivered	6
Types of Malware	6
Estimated Number of Consumers Affected	7
THE INTERNET'S MOST DANGEROUS INTERSECTION: CONTENT THEFT AND MALWARE	
Malware and Its Many Types	8
Threats to Consumers	
Malware Fraud Schemes Against Consumers	
Threats to Advertisers	
How Malvertising Works	
Malware Fraud Schemes Against Advertisers	
Threats to Society	
Malware Fraud Schemes Against Society	

## TABLE OF CONTENTS

UNDERSTANDING THE "CRIMEWARE" ECONOMY	
The DarkNet	
Inside the DarkNet	
The Professional Hacker	
Crimeware Specialization	
PROFILE OF A CRIMEWARE DISTRIBUTION NETWORK	
Crimeware and Affiliate Programs	
How One Affiliate Program Works	
Payouts	22
Affiliate Earnings	23
REVENUE MODEL	
Pay-Per=Install Rates	24
Estimated Malware Exposures	24
Estimated Install Rate	24
Revenue From Malware	24
Estimating Potential Malware-Related Revenue	
CONCLUSION	
ABOUT DIGITAL CITIZENS ALLIANCE	27
ABOUT RISKIQ	
APPENDIX	
REFERENCES	

### INTRODUCTION AND SUMMARY

Content theft, or piracy as it's commonly known, poses a serious and underappreciated threat to Internet users by exposing them to harmful malware that can lead to identity theft, financial loss, and computers being taken over by hackers, according to a new report commissioned by the Digital Citizens Alliance.

Probing a sample of 800 sites dedicated to distributing stolen movies and television shows, the cyber security firm RiskIQ found that *one out of every three* content theft sites contained malware.

The study found that consumers are 28 times more likely to get malware from a content theft site than on similarly visited mainstream websites or licensed content providers.

And just as worrisome, merely visiting a content theft site can place a users' computer at risk: 45 percent of the malware was delivered through socalled "drive-by downloads" that invisibly download to the user's computer—without requiring them to click on a link.

While content theft has long been wounding creators large and small, the RiskIQ report shows that the base of victims includes the unwitting Internet users who go to content theft sites for "free" content.

By exploiting stolen content to bait mainstream consumers, bad actors have uncovered an effective means to hack into millions of computers.

Baiting Internet users, stealing their personal information, and taking control of their computers is becoming big business—an estimated \$70 million per year just from peddling malware.

Digital Citizens found a significant change in the content thieves' business model. Historically, they have profited by taking money out of the pockets of content creators. Now, content thieves have created another stream of revenue that comes from the spread of malicious materials to the computers of unsuspecting consumers. Content thieves are no longer satisfied with targeting creators, not when there is big money to be made from preying on consumers as well.

After its two <u>"Good Money Going Bad"</u> reports explored the business models behind ad-supported content theft sites, DCA commissioned RiskIQ, a leading provider of online security and ad monitoring services, to estimate the amount and type of malware that content theft sites carry and to explore the connection between content theft and malware ecosystems in the dark corners of the Internet.

What RiskIQ found should be troubling to anyone concerned about keeping Internet users safe online. The research found that once hackers get into a computer, they can use it for a wide range of criminal schemes where the user of the computer is the victim.

#### These include:

 $\rightarrow$  Stealing bank and credit card information that is then sold on underground Internet exchanges. After the hack, consumers find their bank accounts depleted or suspicious charges on their credit cards. There is an underground market for credit card information that ranges from \$2 to \$135 per credit card credential.

 $\rightarrow$  *Finding personal information* that makes it easier to sell a person's identity to the highest bidder online. In July, the FBI added five online criminals to its "Most Wanted" list for creating computer programs that stole identities and financial information.

 $\rightarrow$  *Locking a user's computer* and demanding a ransom fee before returning access to their files.

Hackers don't just steal personal information and financial records—they gain access to an Internet user's computer, enabling them to control it for nefarious purposes, including ad fraud, spamming, denial of service attacks, or extortion by threatening to cripple businesses through attacks on their computer systems.

The majority of malware installed through content theft sites was either Trojans, to spy on the consumer's computer, or adware, designed to co-opt the consumer's computer into advertising fraud schemes.

This is disturbing news for the advertising industry and consumers. The Interactive Advertising Bureau (IAB), the trade association for online advertisers and sellers, reports that revenue for online advertising totaled \$49.5 billion in 2014. This is largely due to innovations in advertising that open up the ecosystem to a mass market for any advertiser or publisher with a bank account. However, malware threatens to undermine the trust in the new market these innovations have opened.

The U.S. Department of Justice reports that 16.2 million U.S. consumers have been victimized by identity theft, with financial losses totaling over \$24.7 billion.

What is perhaps most troubling about these findings is how easy it is for hackers. Bad actors dangle free content, consumers take the bait, and the end result is millions of identities at risk and billions of dollars stolen. Then these computers are taken over to wreak more havoc, causing a nightmare for everyone from Internet users, to advertisers who get defrauded, to corporations blackmailed into paying off hackers who threaten to use those rogue computers to launch attacks.

And it can all start with a casual visit by an Internet user to a content theft site.

These revelations should be a wake-up call. *To consumers:* be wary of content theft sites that offer something valuable for "free," for there is a good chance the price you actually pay is an infected computer. *To Internet safety groups:* create awareness and education campaigns, especially aimed towards younger Internet users who often don't consider the impact of their browsing choices. *To government:* step up enforcement of laws on the books to identify and deter those who bait and defraud consumers. *And to advertisers and ad networks:* continue to build safeguards against hackers who are creating elaborate fraud schemes and ultimately undermining trust in online advertising.

If the public better understands the intersection of content theft and malware, we can reduce the number of victims. Until we do so, there will be bait... and prey.

#### **OBJECTIVES**

DCA commissioned RiskIQ to assess and analyze any links between content theft sites distributing unlicensed copies of movies and television shows and malware.

RiskIQ performed this study in two parts. The first is a quantitative study that analyzed the rate of malware exposures across a sample of content theft sites against a control group representing the general web site population. The second is a research study into the malware distribution ecosystem and the role content theft sites play. Taken together, the two pieces present a clear picture of the mechanics of what, why, and how frequently content theft site operators place malware on their sites, and the economics of the partnership between content thieves with the pushers and designers of malware.

RisklQ's focus is to detect malware incidents for web sites and advertisers trying to protect themselves from malware exploits that would affect their end consumers and partners. As such, RisklQ detects anything ranging from suspicious incidents to outright, confirmed cases of malware. RisklQ's system classifies cases as "exact" matches, which are confirmed and active cases, and "reputational" cases, which are incidents that are suspect because they use infrastructure that was previously used for a malware attack. In the interest of precision, for the purposes of this study, RisklQ used only "exact" matches. This conservative approach suggests that the actual level of malware is larger—and perhaps much larger—than the estimates found here.

#### QUANTITATIVE STUDY METHODOLOGY OVERVIEW

The quantitative study was designed to provide an objective comparison of the amount and type of malware found on content theft sites with a control group of sites, which comprise a sampling of legitimate viewing sites and random sites that are representative of the general Internet. In both groups, a broad sample of sites was analyzed, including sites that are highly popular and those less frequently visited.

RiskIQ defined malware as software designed with malicious intent to gain unauthorized access, collect private data, or inflict intentional damage.

The sites were probed for malware by simulating the behavior of users from the U.S. with a variety of browser profiles to approximate typical U.S. targets for malware distributors.

#### SAMPLE DESIGN

The sample group was comprised of *"content theft sites"* which consist of:

- $\rightarrow$  25 Sites from the March 2015 Notorious Markets Report published by the U.S. Trade Representative
- $\rightarrow\,$  The top 25 sites from the Google Transparency Report (GTR) for the month before the scan. (Note this list overlaps with the Notorious Markets Report.)
- $\rightarrow\,$  750 sites selected at random from the top (250), middle (250) and bottom third (250) of the GTR with at least 20,000 copyright infringement removal requests since the inception of the GTR

The following were excluded from the sample group of content theft sites:

 $\rightarrow$  Sites primarily dedicated to video game content theft were excluded from the study because most gaming files are executable files, which carry more apparent inherent risks of malware infection.

 $\rightarrow$  Sites with primarily adult content were also excluded. This was done by filtering out adult related domains and by running a keyword classifier for page content.

#### **CONTROL GROUP DESIGN**

*Control group sites* were intended to represent legal online media sites and the general Internet and were drawn from the following sources:

 $\rightarrow~$  100 sites were selected from the list of legal online media sites on Where to Watch, a site that promotes legal alternatives in the U.S. to content theft sites.

 $\rightarrow$  150 sites were selected, like the sample group, at random from among top third, middle third and bottom third of global Alexa-ranked sites ranging from the top ranked site to the 999.999 ranked site, and filtered so as to not overlap the sample group.

#### DATA COLLECTION

All sites in both the sample and control groups were scanned for malware for a period of four weeks from June to August 2015. RiskIQ's proprietary malware detection solution scans sites with a global proxy network of virtual users that simulate the behavior of real consumers with a variety of operating systems and browsers. For the purposes of this study, scans were limited to users across 20+ cities in the U.S. only. Malware analysis was run through a series of market standard malware detection tools, including VirusTotal and RiskIQ's own proprietary detection system.

Each simulated user was configured to navigate up to three levels deep for a maximum of 25 pages daily per site. Data collection sampled an average of just over 50 pages daily per site during the fourweek period. Scans were designed to check for the presence of malware in either "drive-by downloads" (where no user initiated action is required) or user-initiated downloads, typically delivered through pop-ups or fake software update requests. Click throughs were performed based on a link scorer that preferred links containing downloads over navigation links while clicking through 5 links per page to a depth of 3 pages within a site. Additionally, click throughs were limited to the domain of the first page in a site crawl.

The amount of malware discovered is a conservative measure because:

→ No ads were clicked on for the study. Most malicious ads deliver malware upon loading. Even though RiskIQ's system is capable of clicking through on ads, previous experience had shown that the rate of malware exposure from actually clicking on ads was extremely low, indicating that clicking on ads would not have materially changed the results of this study; and

 $\rightarrow$  No files were downloaded from the sites for the study, even though malware can be delivered through the file download, which means that the study does not include the malware risks from sites, such as torrent sites, that offer downloading of content.

These limitations of the methodology suggest that the malware uncovered by this report is a conservative measure of the total amount of malware delivered by content theft sites.

#### DATA AVAILABILITY

RiskIQ designed a study that could be easily repeated by any researcher with the capability to adequately analyze and detect malware on web sites.

The data and malware analysis from this report is available online at:

→ <u>http://www.digitalcitizensalliance.org</u>

Researchers who wish to repeat the study or have questions about the results may contact the DCA through their online contact form.

#### PROFILE OF A CRIMEWARE DISTRIBU-TION NETWORK

After calculating the amount of malware found on content theft sites, RiskIQ went on to probe the ecosystem connecting malware to content theft sites. Specifically, they looked at who deployed the malware, what kind of malware was prevalent, and how much money could be made from using content theft sites to distribute it. For the qualitative component of the study, RiskIQ sent researchers with undercover online personas into DarkNet exchanges and marketplaces to collect information about popular malware distribution programs with ties to content theft sites. Multiple programs were found. A typical program is profiled in this report with some details removed to protect the sources that provided the information. This profile provides valuable insight into the typical revenue for sites involved with malware campaigns and sheds light on how the business relationships work.

#### SITES WITH MALWARE INCIDENTS

RiskIQ found that 33 percent of sites in the Content Theft Sample group had at least one malware incident over the month in which it collected data compared with 2 percent for the Control Group.

# MALWARE INCIDENT RATES FOR USERS VISITING THESE SITES

RiskIQ found that users are 28 times more likely to be infected with malware when visiting sites in the Content Theft Sample group as compared with the Control Group. Of the Content Theft Sample group, 8 percent (1 in 12) of user visits resulted in exposure to malware, compared with 0.3 percent (1 in 333) user visits for the Control Group.

Many of the sites in the Content Theft Sample Group sustained very high exposure rates, suggesting that malware distribution was part of their ongoing modus operandi. For example, 20 of the content theft sites exposed more than three out of every four users (75 percent) that visited them to malware.

#### HOW MALWARE IS DELIVERED

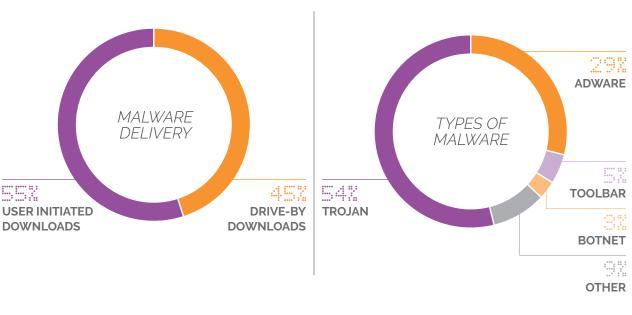
"Drive-by downloads" allows malware to be delivered without the victims even having to click on anything after arriving on the page. Drive-by downloads infect users silently and can go completely undetected. Forty-five percent of malware payloads found on the sample sites downloaded invisibly in the background and did not require the user to do anything to confirm the download. Users did not need to download media or click on any popup advertisements to be infected by these attacks.

The remaining 55 percent of the malware lured users with fake prompts for requests such as Flash downloads and anti-virus updates -- many of these prompts look virtually identical to prompts from the actual legitimate providers of such services. While some users may know enough to avoid fake prompts, attackers are often able to trick users into accepting a payload just to get rid of a pop-up. The malware payloads for these user initiated downloads are typically larger, containing more than one type of malware because they do not have to be installed surreptitiously in the background like driveby downloads.

#### **TYPES OF MALWARE**

Over half of all malware detected was classified as Trojans by RiskIQ's malware analysis tools. "Trojan" is the general term for any malware that secretly installs itself to open unauthorized access to a computer.

DIGITAL BAIT 6



🕊 #FollowTheProfit

Malicious adware and toolbar software were the next most prevalent types. The definition of Adware can range from benign to annoying to malicious. Adware detected by the anti-virus tools in this study was weighted toward the malicious end of the spectrum.

Lastly, "Other" was used to signify minor categories and instances where an exploit kit was detected but the malware type was not determined.

A subset of Trojans, Remote Access Trojans ("RATs"), were also quite prevalent. RATs can be used to steal logins and financial data, or take over a user's web cam and use it to spy on them. Below is a list of the top 10 RATs found in our scans.

#### TOP 10 REMOTE ACCESS TROJANS (RATS) IDENTIFIED IN RISKIQ SCANS

- XTREME RAT
  BIFROST
  BACK ORIFICE
  NJRAT
  ADWIND
  DARKCOMET
  BLACKSHADES
  SBU7
- 9. POISON IVY
- 10. CERBERUS

# ESTIMATED NUMBER OF CONSUMERS AFFECTED

RiskIQ estimated that each month 12 million U.S. users were being exposed to malware attacks from the specific sites they visited in the Sample Content Theft Group, based on Alexa traffic data and Risk-IQ's measure of malware incident rates.

RiskIQ applied the average malware exposure rate for each site with Alexa average monthly traffic of unique visitors. Note that Alexa data does not permit de-duplication of visitors; however, the 12 million user figure may still be a conservative estimate among the Sample Group for two reasons:

First, Alexa measures audiences by allowing Internet users to opt into a tracking panel. Many users who engage in illegal activities do not choose to opt in to the Alexa panel because they do not wish to have their online behavior tracked. For this reason, traffic to Content Theft sites, and DarkNet sites in general, is likely underreported. Second, Alexa tracks traffic data for only 21 percent of the sites in the Sample Content Theft Group. According to Alexa, the sites that were tracked average more than 88 million unique users from the U.S. each month.

Given that the remaining 79 percent of sites do not have traffic figures, and further that the non-Sample sites are not covered by this estimate; this number is a floor, not a ceiling, for the potential users affected.

## THE INTERNET'S MOST DANGEROUS INTERSECTION: CONTEFT THEFT & MALWARE

Malware inflicts significant harm on consumers, on advertisers, and on society in general. This section explains in words and in illustrations how the major types of malware work, and the serious problems they can inflict.

#### MALWARE AND ITS MANY TYPES



#### MALWARE

Software designed with malicious intent to gain unauthorized access, collect private data, or inflict intentional damage.



#### TROJANS

Software that installs itself without the user's knowledge either secretly or hidden inside a seemingly benign user action such as opening an email or web page. Most Trojans open up unauthorized access to the victim's computer.



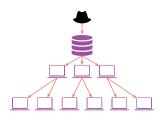
#### REMOTE ACCESS TROJANS (RATs)

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. For more information on RATs, see the DCA's report <u>Selling Slaving</u>.



#### 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. They are also frequently used for the purposes of traffic fraud. Adware can range from the benign to the annoying to the malicious. Adware detected by the anti-virus tools in this study was weighted toward the malicious end of the spectrum.



#### BOTNET

A distributed system of Internet connected computers acting as a group at the command of a Bot controller, who directs them to accomplish certain tasks. Botnets are used to fake advertising traffic, attack web sites in Distributed Denial of Service attacks (DDOS), and carry out spam and phishing campaigns.



#### EXPLOIT

Software or a script that takes advantage of a computer's security vulnerability—often with Flash or Java—to install unwanted code such as malware. Where malware is the payload, the exploit is the tool that opens the computer's back door to install the program.

#### THREATS TO CONSUMERS

Few consumers who use content theft sites, or whose family members use such sites, realize they have become targets for malware. And malware means more than just a slow computer. An infected computer exposes everyone who uses it—children, spouses, or roommates—to the risks of being victimized by any of a variety of criminal schemes.

This study found a range of malware exploits on content theft sites targeting both computers and tablets. Typically, the risks to consumers fell into three categories.

*Identity Theft* is the most prevalent problem. As noted in our findings, Trojans were by far the most prevalent type of malware RiskIQ found in its scans. Popular Trojans such as Dyre, Zeus, Shyloc, and Ramnit are designed to steal consumer credentials on a massive scale. Once a consumer has inadvertently downloaded the software, the criminal behind the exploit, known as a harvester, batches together credentials from the same financial institution, and sells them online in underground exchanges for anywhere from \$2 to more than \$135 per credential,<sup>1</sup> depending on the quality. Trojan kits were once available only to highly skilled or connected cyber criminals. Today, anyone with basic web skills can find and deploy them.

*Ransomware* is malware that installs itself on the consumer's PC, encrypts their files, and posts a message demanding they make a payment in order to regain access to their files. Typically, criminal operators demand \$100-\$500 in ransom,<sup>4</sup> the same price as a data recovery service would charge in most U.S. cities. In June 2015, the FBI reported receiving complaints amounting to \$18 million in losses due to ransomware for the past year alone.<sup>5</sup> THE DEPARTMENT OF JUSTICE REPORTS THAT U.S. CONSUMERS LOSE \$24.7 BILLION TO IDENTITY THEFT IN A SINGLE YEAR.<sup>2</sup> CONSUMER REPORTS FOUND THAT MALWARE ALONE COSTS CONSUMERS \$2.3 BILLION.<sup>3</sup>

## **UP TO \$135**

THE GOING RATE PER CONSUMER CREDIT CARD CREDENTIAL ON UNDERGROUND INTERNET EXCHANGES

## \$100-\$500

TYPICAL AMOUNT CHARGED BY RANSOMWARE OPERATORS FOR CONSUMERS TO REGAIN ACCESS TO THEIR PC

Remote Access Trojans, or RATs, are a particularly potent form of Trojans that grant the controller full access to the victim's device. Not only can they log keystrokes and collect data or files, they can also access the camera. As the DCA reported in its study, <u>Selling Slaving</u>, hackers who run networks of slaved devices sell video streams of men, women, boys, and girls as reality porn online to communities of voyeurs. Also concerning is the rise of one-to-one attacks by hackers who select a victim, "own" their computer, and proceed to blackmail and manipulate them. The most common scenario is to take compromising pictures or capture compromising secrets from the user's PC. Then, the attacker threatens to publish the pictures or information on social media if the victim does not meet their demands. As noted in the findings, RiskIQ found several popular RATs, which have large distribution and are very easy to use.

CONTENT THEFT SITES OFFER THE PERFECT VEHICLE TO DELIVER MALWARE TO MAINSTREAM CONSUMER HOUSEHOLDS. OFTEN KIDS DO THE DAMAGE BY VISITING SITE OFFERING FREE DOWNLOADS, LEAVING INFECTED THE HOUSEHOLD COMPUTER WHERE PARENTS PAY THE BILLS AND MANAGE BANK ACCOUNTS.

#### MALWARE FRAUD SCHEMES AGAINST CONSUMERS



#### "THE ID SNAG" $\rightarrow$ CREDENTIAL THEFT CYCLE

- 1. Household members visit content theft site
- 2. Site downloads Trojan or "spyware" to victim's computer

3. Spyware activates when adult members of household log in to banking site or credit card site

4. Malicious advertiser or "Harvester" grabs the consumer's logins and sells them into underground exchanges

5. "Cashiers" buy thousands of credentials and systematically exploit them

6. Victims often find later that their bank account has been drained or systematically raided with random charges that often go unnoticed for many months

#### "THE RANSOM" → RANSOMWARE SCHEME

1. Household member visits content theft site

2. Site installs malware that fully encrypts the user's files or merely posts a scare-tactic message. Some ransomware even posts fake messages about the user's "Illegal activity," demanding they pay a fine for downloading copy-righted media or illegal pornography.

3. Consumer must then negotiate with the attacker to pay a ransom fee to regain access to their computer and files



#### "THE SLAVER" → REMOTE ACCESS TROJANS

- 1. Household member visits content theft site
- 2. Site downloads Remote Access Trojan to victim's computer
- 3. Attacker then takes control of the computer in order to spy on the user's activity:
  - » Web cam can be turned on for a live web stream into the consumer's private life. Access to these web streams are commonly sold in forums to voyeurs.

» Personal data can then be used to blackmail the user with threats of posting information about their private life on their own social media accounts.

» Just as with any Trojan, identity theft is always an ultimate endgame when other options are not as fruitful for the attacker

#### THREATS TO ADVERTISERS

Malware distribution through content theft sites also defrauds advertisers. Double Verify, a leader in the ad verification business, observed in 2014 that content theft sites have unique characteristics that make them ideal for traffic laundering. They have high volume traffic from a valuable audience, but their objectionable (pirated) content drives away premium advertisers. Advertising fraud schemes offer content theft sites a way to earn money from premium advertisers without those advertisers knowing their ads appeared on such sites. For the criminals behind advertising fraud, a content theft site offers a vehicle to capture real, valuable users clicking on ads.

From the criminal's perspective, installing malware from content theft sites is an attractive line of business. Alternative money-making scams, such as phishing emails, have always been a blunt tool for targeting, and enforcement efforts have made them increasingly less effective. "Malvertising" campaigns, by contrast, are highly targeted and very efficient. The proliferation of malware via content theft sites contributes to three trends that should be of concern to anyone in advertising.

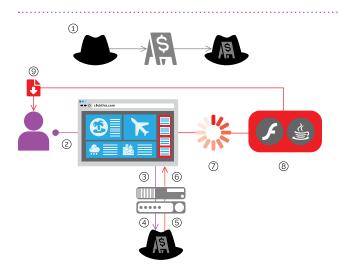
*More malware means more bots*, and more bots could mean more traffic fraud. Content theft sites use media content to draw quality audiences to their web sites. When these same consumers get **\$50-\$200** PAY RATE PER 1,000 INSTALLS FOR A TYPICAL MALVERTISING CAMPAIGN<sup>6</sup>

malware on their PC, they may become a part of the massive infrastructure that perpetrates traffic fraud on the advertising industry.

In the November 2015 report from IAB and EY, "What is an untrustworthy supply chain costing the US digital advertising industry?", researchers estimated that advertisers would lose \$4.4 billion annually to fraudulent, non-human traffic.<sup>7</sup>

*More malware means more ad blocking*. Ad blocking has been on the rise since 2012, creating more obstacles for advertisers to reach their audience, and reducing the revenue necessary to drive the creation of more sites and services. Adobe reports that over 144 million Internet users globally use Ad Blocking software.<sup>8</sup> Users who do use ad-blocking software cite privacy as their major concern. Publishers are now reporting ad-blocking rates from 10-50 percent depending on their demographic.<sup>9</sup> Continued headlines over identity theft and malware infections delivered via ads will drive this advertiser-unfriendly trend.

#### HOW MALVERTISING WORKS



1. Attacker registers as an Advertiser with Self-Service Ad Platform

- 2. User visits website
- 3. User Targeting Data sent to Ad Platform
- 4. Impression sold to Attacker
- 5. Malvertisement served to Ad Platform
- 6. Malvertisement served to Website
- 7. Exploit kit loads
- 8. Vulnerable browser plugins discovered
- 9. Malware installed on User's device

#### MALWARE FRAUD SCHEMES AGAINST ADVERTISERS



#### "THE ROBOT ARMY" $\rightarrow$ HOW BOTS GENERATE FAKE IMPRESSIONS

**1**. Content theft sites attract mainstream population from valuable households

2. Household member's device infected by malware that converts PC into

- a "bot" that browses sites in the background, loading and clicking on ads
- 3. Bot owner rents out household PC for fraud schemes

4. The family is left to wonder why their home PC is running so slow, while it surfs the web and clicks on ads to make money for the bot owner and criminal ad fraud schemes



#### "THE WASH" → MONEY LAUNDERING SCHEME

1. A criminal organization sets up web sites as a "front." Often these are sketchy sites with cheap content—even stolen content, or sites run by "mules" who are recruited by the criminals to run ads to launder money

2. The web site operators or mules register with a sketchy ad network or advertising exchange without sufficient controls to detect traffic fraud

3. The same criminal organization that set up the web sites then runs click fraud bots to view and click on the ads

4. Web sites like content theft sites attract just enough natural traffic to avoid being detected for fraud

5. Money makes full cycle from advertiser to web sites that are usually controlled by the same organization. The typical revenue share to ad network or exchange and money mules is a reasonable fee for laundering the money

#### THREATS TO SOCIETY

Malware not only affects individuals and advertisers. Infected computers can also be enlisted into criminal activities that affect society at large.

*Botnets* play an essential role in the crimeware economy. Malware can convert the consumer's PC into a "bot" or "zombie" that performs the operator's bidding. Botnets essentially act as underground distributed computing systems for criminal operators.

Distributed Denial-of-Service Attacks (DDoS) disrupt consumer services by flooding a target web site or Internet service with so many requests that it simply shuts down. With rental rates from nefarious web site operators starting as low as \$150, botnets are relatively cheap to use for DDoS attacks and can exact an expensive toll on their targets.

DDoS attacks are sometimes used by hacktivists to attack or censure governments, organizations, and publications with which they disagree. They are also used by criminals to extort money from the organizations that they target. Last but not least, DDoS attacks can be used to distract security teams and keep them busy while hackers try to penetrate their defenses. Security firm Incapsula surveyed over 270 firms in North America between 250 and 10,000 employees on the impact of DDoS attacks. The average cost of an attack across all survey respondents was estimated to be about \$500,000. For a sense of how individual firms can be affected, technology firm Neustar offers this DDoS cost calculator. DDoS attacks continue to be a tremendous cost to the private sector in terms of money, jobs, and productivity.

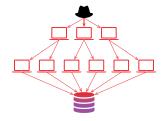
**\$1,000** THE HOURLY RATE FOR RENTING 10,000 U.S. COMPUTERS ON RECENTLY DISCOVERED BOTNET<sup>10</sup>

*Spamming and Phishing* clog the mail servers of the Internet and provide a major vector for malware distribution and credential theft. "Botted" computers acting as mail servers send out emails that would otherwise be blocked by most commercial senders. Some even host phishing sites themselves to avoid the obvious challenges of hosting them with a reputable commercial ISP. The largest documented botnets in history have been found to infect millions of computers and send out billions of emails per day.<sup>11</sup>

*Distributed Financial Fraud* is another common use for infected computers. Some bots are capable of capturing a victim's account login and then using that same computer to log in and conduct transactions on the account to avoid detection. Because the transaction comes from the victim's own computer, it is much harder for financial institutions to detect the fraud.

In summary, botnets provide criminals with the infrastructure to wreak havoc and mischief on the Internet community at large. For the consumer, the most obvious effect of botnet software is a slow computer, but participating in a botnet unwittingly assists criminals to defraud other consumers. Consumers who host bots unwittingly become a part of a global network of computers that are the underpinning of many cybercrime schemes.

#### MALWARE FRAUD SCHEMES AGAINST SOCIETY



# "THE SHAKEDOWN" $\rightarrow$ DISTRIBUTED DENIAL OF SERVICE EXTORTION AND CENSORSHIP

1. A criminal organization contacts the target organization and warns them of impending Denial of Service (DDoS) attacks if they do not cooperate. For online publishers and public-facing organizations, the demand may be political in nature. For corporations, the demand may be for money.

2. If the organization refuses to cooperate, the extortionists stage a DDoS attack by renting a botnet service to provide the computing power

3. Depending on their security posture and resources, the target will experience down time on their public site in the worst case, or a financial loss of computing and human resources At the heart of content thieves' efforts is criminal exploitation of both the creator and consumer of pirated content.

"Crimeware" refers to software written for the purpose of these criminal enterprises. To understand how it works and how such an operation can achieve scale, it is important first to understand the basic infrastructure of the economy underpinning the Internet criminal underground that has developed over the past fifteen years—which Digital Citizens calls the crimeware economy.

#### THE DARKNET

The DarkNet is the term commonly used to describe the criminal underground that operates online outside the public eye. It is made up of private forums, "friend-to-friend" private networks, and anonymous networks such as Tor that enable criminal activity without fear of being identified. In that underground, criminals buy and sell illegal wares including stolen credit cards, personal information, drugs, and human trafficking. Payments are made using anonymous payment methods such as Bitcoin, Litecoin, and Ripple<sup>12</sup> that cannot be traced by law enforcement. In this environment, criminals have operated with impunity since the early 2000s. In the DarkNet, there is a thriving market for crimeware.

#### **INSIDE THE DARKNET**

The DarkNet costs economies around the globe more than \$300 billion per year.<sup>13</sup> At the heart of the

underground economy are the online chat forums, where criminals buy and sell their wares. These forums can range from specialized "carding forums" where criminals purchase or sell stolen credit cards—to full-fledged e-commerce sites. Before it was taken down, Silk Road made millions connecting sellers of illegal drugs to interested buyers. In the post-Silk Road era, sites have emerged that sell illegal and dangerous items all on one site—including illicit drugs, personal financial information, weapons, and malware.

As of August 2015, there were about 47 such online markets.<sup>14</sup> The majority of these sites are in the English language. There are also markets in French, Finnish, Italian, Polish, and Russian.<sup>15</sup> A single carding forum can have as many as 13,000 members with 4,000 daily visits and 20 sub-forums covering a range of topics such as online security, tutorials, carding, botnets, web design, and money laundering.<sup>16</sup> It is in these underground markets that hackers peddle malware, exploits, botnets, etc.

#### THE PROFESSIONAL HACKER

Modern hackers are professional, organized, and monetarily motivated. According to Marc Goodman, author of *Future Crime*, 80 percent of hackers are affiliated with organized crime.<sup>17</sup> As Goodman points out, this radical shift has led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism, discipline, and structure of legitimate enterprises.

#### **CRIMEWARE SPECIALIZATION**

Like any market, the crimeware market has evolved to reflect a division of labor. Within the DarkNet are dozens of unique product and services categories. Anyone from professional criminals to nation states can purchase Trojan malware, Exploit kits/packs, or services such as dedicated hosting or Distributed Denial-of-Service attack services.<sup>18</sup> Many of these products and services come complete with service agreements and money-back guarantees.

The DarkNet allows individual hacking groups to specialize in specific categories and to earn money for delivery of goods and services to other criminals. For example, one organization may specialize in developing the malware that is installed on consumer devices and sell it on the web. Another organization will be responsible for distributing and installing the malware on consumer PCs or mobile devices. A third group that runs a forum might also purchase stolen consumer credentials and resell them in the DarkNet. The ultimate buyer of the credentials plays the role of *cashier* to collect cash from the credentials by actually exploiting the bank or credit card accounts. Because of the role the DarkNet plays in facilitating anonymous communication, none of these specialized groups ever has to meet one another. This enables a very efficient market for crimeware developers and distributors. To better understand the economics and working relationships behind a typical crimeware distribution network, RiskIQ sent covert agents into the DarkNet to research organized malware programs that exploited the content theft sites in the sample sites scanned in the earlier part of the study.

#### CRIMEWARE AND AFFILIATE PROGRAMS

Affiliate programs are the primary vehicle for spreading programs like malware and adware via content theft sites. These programs are a common model in the advertising world. Typically, a malware publisher or affiliate joins an ad network that rewards them on some type of "pay for performance" model. The two most common models are "Pay-Per-Click," where the advertiser pays an affiliate publisher for each user click on an ad, and "Pay-Per-Action," where the advertiser pays for a specific action such as filling out a form or making a purchase. In the world of advertising, there is a range of affiliate networks, some with high business standards, and some that operate in gray areas. It is typical for less reputable affiliate networks to offer same-daypayouts, which enable participants to join, engage in a questionable advertising campaign, and leave with their money in the same day. In the criminal underground, crimeware distribution campaigns are commonly referred to as "Pay-Per-Install" (PPI) campaigns because they pay out for every malware installation that the publisher delivers.

Affiliate programs offering a PPI model can pay as little as five cents per install to as much as \$2. For malware that involves secondary conversions, there is an additional source of revenue after the user installs the malware. These include such schemes as Fake Anti-virus or Ransomware, where the payout per user for the affiliate can be as high as \$25 for each victim that ends up paying the ransom, which (as noted above) is typically \$100-\$500.

The PPI affiliate programs work in two ways: hosting models and traffic models.

In a hosting model, the program provides the malicious download to the affiliate and relies on the affiliate to generate installs. This means the affiliate is responsible for (1) hosting the install, (2) creating a lure to trick people into downloading it (such as codecs), and (3) generating traffic to the download location.

Generally speaking, these types of programs are sophisticated and tightly guarded. For instance, a program run by one of the world's top spammers will re-package their malware every few hours in order to avoid detection by anti-virus software. The affiliate is then responsible for constantly refreshing the install if they want to avoid having it flagged by anti-virus software. In fact, this malware affiliate program is so strict that affiliates hosting old executable files that were flagged by anti-virus software are expelled from the program. This particular program is advertised only in Russian-language underground forums open only to vetted individuals; even then, the potential affiliates must also prove they have the ability to deliver traffic.

The traffic model, by contrast, relies on the affiliate to drive traffic to the page hosting the install that was created by the program. Most of the affiliate programs RiskIQ observed fell into this category. Media-related traffic is delivered via redirect links, popups and popunders. Most offer a movie download as the lure to get consumers to unwittingly install an executable malware file. Each affiliate web site is compensated for every malware install completed.

The malware RiskIQ observed from these sources tend to be adware or bloatware, which monitors traffic and slows down machines. And since many of these programs are for actual user-prompted downloads, the operators also have the ability to control what people download, which can lead to more severe infections.

#### HOW ONE AFFILIATE PROGRAM WORKS

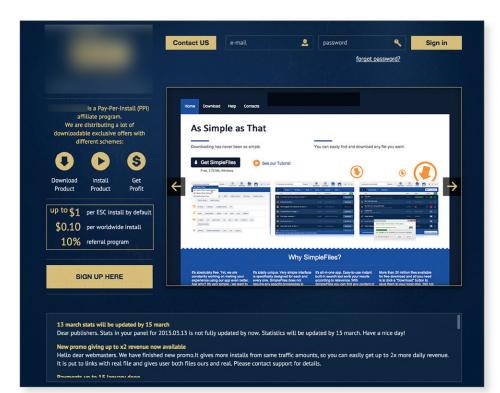
RisklQ identified one program in particular that was very popular within the content theft community. To protect sources, it is referred to it as *Advertising Underground* (not its real name).

Advertising Underground was found in RisklQ's scans of content theft sites. It has been around since 2009, a very long time for such a program, which is a testament to its durability and quality, and has been drawing a lot of attention lately in the Russian underground. As is the case with other affiliate programs, *Advertising Underground* has used different names and guises since 2009, which helps it fly under the radar of law enforcement.

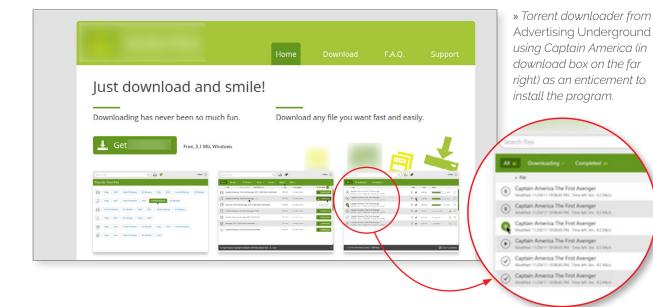
Advertising Underground, which appears to be based in Russia, has a strong reputation and is recommended in the Russian underground community, because it pays out its affiliates in a timely manner and converts traffic to installations at a high rate. Advertising Underground mainly installs toolbars, torrent download clients, and games, which are generally associated with adware, though more trusted affiliates of Advertising Underground could be given sites with more malicious and lucrative installs like ransomware.

Advertising Underground's program managers have acknowledged that it is involved in the spread of adware and other malicious programs. When asked if VirusTotal—a leading malware and anti-virus platform—will detect their malware, they respond that they frequently "clean" or repackage the installs to evade antivirus detection, just as the affiliate program discussed above did.

Advertising Underground operates both in the English and Russian languages and offers support and a personal manager. Potential affiliates are required to contact them with their web sites and eventually prove that they can deliver traffic. Following a chat over ICQ or Skype to vet potential affiliates, the affiliate must then prove their ability to deliver traffic to *Advertising Underground*.



» Advertising Underground *registration page* 

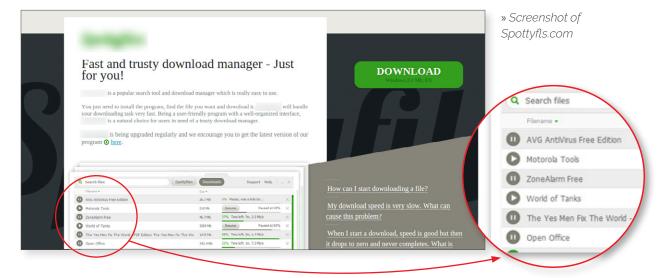


#### PAYOUTS

Advertising Underground pays for each application installed and appears to operate a traffic model. So it will provide the page with the install to which the affiliate drives traffic. They are not concerned with how the traffic is delivered to the page, except they explicitly prohibit spam traffic.

Advertising Underground claims a conversion rate of 1 download for every 7 visits, and will pay 10 cents U.S. per install in countries within the Commonwealth of Independent States and up to 20 cents U.S. for installs in Western countries. However, some installs, such as the torrent downloader client described below, will earn an affiliate up to \$2 per download. RiskIQ observed this download in the crawls as spottyfls.com, and it was tied to the general-catalog.com home page.

The spottyfls.com torrent downloader is classified as adware by VirusTotal, and, since it controls the users' results, could be used to download more malicious programs in the form of torrents.



Antivirus	Result	Update	
AVG	Generic_r.AID	20151130	
AVware	Trojan.Win32.Generic!BT	20151130	
Agnitum	PUA.Downloader!	20151130	
AhnLab-V3	PUP/Win32.YourFileDownloader	20151130	
Avast	Win32:Malware-gen	20151130	
Avira	PUA/EDownloader.Gen4	20151130	
DrWeb	Adware.Downware.13091	20151130	
ESET-NOD32	a variant of Win32/ExpressDownloader.K potentially unwanted	20151130	
K7AntiVirus	Adware ( 004b90661 )	20151130	
K7GW	Adware ( 004b90661 )	20151130	
Malwarebytes	PUP.Optional.SpottyFiles	20151130	
NANO-Antivirus	Trojan.Win32.Agent.dxesfg	20151130	
Panda	Trj/Genetic.gen	20151130	
Qihoo-360	HEUR/QVM10.1.Malware.Gen	20151130	
Rising	PE:Trojan.ExpressDownloader[1.A207 [F]	20151129	
VIPRE	Trojan.Win32.Generic!BT	20151130	
Zillya	Downloader.Agent.Win32.281189	20151130	

» VirusTotal Results for Spottyfls.com

♥#FollowTheProfit

#### **AFFILIATE EARNINGS**

According to *Advertising Underground*'s claims, one arm of *Advertising Underground* supposedly has generated more than 150 million worldwide installs since 2012 and is said to have paid out \$12 million to affiliates.

Advertising Underground has been observed reaching out to other pirated media sites that were in the list of Sample Content Theft Sites to direct traffic to the Advertising Underground's sites. In one of the underground forum threads, one of the affiliates claimed that *Advertising Underground* generated 30,000 installs a day for him. Below are statistics from several users, whose earnings are \$200-600 a day from the affiliate program.

Advertising Underground's payout vehicles are a further testament to their criminal purpose. Payments to affiliate are only available via (1) WebMoney, which is one of the *de facto* means of payment in the criminal underground, (2) Epese, a Russian anonymous payment program, or (3) Western Union/MoneyGram.

Date	Hits	Unique	Installs	Money	СРМ
• 2014-06-16	9272	6813	950	67.04	9.84
• 2014-06-15	24660	18773	2568	184.92	9.85
• 2014-06-14	22257	16897	2258	166.07	9.83
• 2014-06-13	22483	15976	2228	155.81	9.75
• 2014-06-12	21467	15834	2133	155	9.79
• 2014-06-11	22961	16352	2224	159.27	9.74
• 2014-06-10	22049	16718	2337	162.96	9.75
+ 2014-06-09	22524	16477	2228	161.48	9.8

» Sample Advertising Underground chart showing payments to affiliates

Payment list				
	Date	Amount	Status	
07.03.201	.4	\$295.49	in progress	
16.01.201	.4	\$304.71	in progress	
23.11.201	.3	\$244.00	Paid	
19.09.201	.3	\$54.35	Paid	

» Advertising Underground *statistics 2*  To better understand the incentives for distributing malware on content theft sites, RiskIQ calculated an estimate of the potential revenues these sites earn from malware.

#### **PAY-PER-INSTALL RATES**

Estimates of Pay-Per-Install rates range widely in crimeware research. Trend Micro found that the Russian Underground paid a range of 5-20 cents U.S. per install, depending on the target country.<sup>19</sup> In RiskIQ's research into Pay-Per-Install Programs, it found an active affiliate campaign with typical mid-tier content theft sites offering 10-20 cents per install. The program profiled was well reviewed by third party users, not just its own web site, and had been in existence for some years. So, for the purposes of this model, RiskIQ used 15 cents as a conservative average Pay-Per-Install rate to estimate revenue.

#### ESTIMATED MALWARE EXPOSURES

The subset of the 800 content theft sample group sites for which visitor statistics are available on Alexa (n=229) average over 88 million U.S. users per month. Taking into account the sites' average malware exposure rates indicates that an estimated 12 million U.S. users were being exposed to malware each month from these sites. There is likely some level of carryover in users across sites; however, Alexa does not measure de-duplicated visitors.

#### ESTIMATED INSTALL RATE

It is difficult to estimate the actual install rate for these malware exposures, as not every user's system is vulnerable in the same ways, and not every user clicks on the lure for user-initiated installs. In RiskIQ's underground research, it found that the program profiled claimed a 1 in 7 conversion rate for traffic (15 percent). Therefore, RiskIQ used this number for the purposes of estimating revenue.

#### **REVENUE FROM MALWARE**

Once malware is installed, there are ongoing services that add to the total lifetime value of the malware installation. Consumer credentials harvested by Trojans can be sold for \$20-45 per user (although less than \$10 if the market is flooded or the credentials are stale).<sup>20</sup> Botnets can be rented for up to \$1,000 per hour for 10,000 U.S. computers.<sup>21</sup> Lastly, as mentioned earlier, Symantec found that the typical charge for a Ransomware clean up is \$100-\$500.<sup>22</sup> For the purposes of this study, Risk-IQ focused exclusively on the money earned from malware installations through content theft sites, not on the add-ons.

#### ESTIMATING POTENTIAL MALWARE-RELATED REVENUE

Combining these estimates leads us to calculate that the operators of the sample of content theft sites studied with Alexa visitor data (n=229) are generating roughly \$3.3 million in revenue per year:

12.2 MILLION Monthly U.S. Users Exposed to Malware (for Sample Group Sites with Alexa User Data)

X 15 PERCENT Estimated Install Rate

X 15 CENTS Pay-Per-Install Rate

- = \$274,500 Monthly Revenue
- = \$3.3 MILLION Estimated Annual Revenue

This estimate has some limitations as previously described, but is within range of similar research studies on the economics of malware. For example, in 2012, Symantec found a group of sites running Pay-Per-Install malware campaigns where the top site was earning more than \$200,000 per year. This figure is in line with the data from our study, where only three exceptional sites are estimated to earn more than this figure.

Again, our estimate above is only for a small sample of sites. There are 4,865 sites in the Google Transparency Report that received 1,000 or more copyright infringing URL removal requests in the year preceding this analysis. Projecting the earnings from the 229 sites in the sample group to this broader universe suggests that these content theft sites may be generating roughly \$70 million in revenue per year:

(\$3.3 MILLION Estimated Annual Revenue for 229 Sample Group Sites

- ÷ 229 Sample Group Sites)
- X 4,865 Sites w. 1,000 or more copyright infringing URL removal requests in the past year
- = \$70 MILLION Estimated Annual Revenue

These assumptions are conservative in two respects. First, they do not take into consideration malware income from any of the many thousands of content theft sites that receive less than 1,000 notices per year. Because the malware rates across content theft sites are relatively constant regardless of size (7-9%), this may be a considerable sum. Second, they do not take into consideration the "add-ons" that content sites can earn from peddling malware.

While this is a rough estimate limited by the lack of comprehensive visitation data, it is easy to see that malware and content theft work together as a big business for the organizations behind them. Add to this estimate the obvious potential for additional revenue once the malware is installed, and it is easy to see that this is an industry that can generate hundreds of millions of dollars for the criminals behind it, at the expense of consumers, advertisers, and society.

### CONCLUSION

For the last two decades, content theft has largely been an issue for creators who were denied compensation and credit for their work. But RisklQ's research has revealed that cybercriminals have expanded the group of victims to include the hundreds of millions of Internet users who go online each day looking for high-quality content free or cheap.

By dangling such content as bait, criminals lure in unsuspecting users and infect their computers. In doing so, these criminals are exploiting a lack of understanding and awareness among users about the risks that visiting shady websites can pose.

There is an adage from the Watergate era: "Follow the money." It is clear why cybercriminals have targeted consumers. They present an enormous potential windfall to scam and cheat. And it can be done relatively inexpensively through malware and other viruses.

Over the last few years, significant breaches in the customer databases of high-profile companies have created greater awareness about the need for cyber security. The threat of content theft and malware must be part of that conversation.

For consumers, it comes down to another adage: "If it seems too good to be true, it is." The delivery of content—whether radio programs long ago or movies and TV series and sports now—has always been based on some transaction that provides a reward for the content provider—that is the creative incentive, and was most frequently funded by ad revenues or a monthly subscription payment. But the consumer who goes to a content theft site is paying someone—not the creator of the content, and not just money—they may also be giving up their user identity, access to their financial information or control of their computer. It's a great deal for the cybercriminal, and it leaves millions of Internet users victimized and wondering "what happened?"

It is not fair or reasonable to expect Internet users to understand all these risks because the Internet is an impossibly complex ecosystem. But it does underscore the importance of education campaigns to raise awareness about the threats and how to avoid them.

This report should compel law enforcement authorities to devote more attention and resources to tracking and apprehending global cybercriminals who operate in the shadows and put so many Internet users in harm's way.

And it is incumbent upon our leading digital platforms and financial facilitators to ensure that they are not aiding cybercriminals. That means choking cybercriminals at their key points: how they are found (search engines) and how they bank their ill-gotten gains.

With this report, Digital Citizens hopes to help Internet users—even those who have no care or respect for creators who are victimized by content theft—understand that there are more victims than they may think . . . and some of them are right there in the mirror.

## ABOUT DIGITAL CITIZENS ALLIANCE

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

This is the fourth report in which Digital Citizens has studied content theft sites. In 2014 and 2015, Digital Citizens released its <u>"Good Money Gone Bad"</u> reports looking at the revenues of ad-supported content theft websites. Also in 2014, Digital Citizens published <u>"Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions</u>" which broke down the profits and operating costs of the largest cyberlockers.

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

#### **OUR MISSION**

RiskIQ solves the problem of collecting and analyzing Internet-scale data. It enables security teams to expand their security program outside the firewall. Our technology addresses the growing challenge of external threats targeting the enterprise, its customers and employees.

RiskIQ is designed to detect threats that corrupt the core tenets of the Internet—the principles of open standards and information sharing—to extort, scam, invade systems and infect its users. Our mission is to provide web-scale detection to the people responsible for protecting their business against the threats that exist outside of the firewall.

#### **OUR STORY**

From the beginning, RiskIQ sought to solve the complex issues security professionals face. RiskIQ saw firsthand how the emergence of the Internet as the primary place for companies to do business also made it the ideal launching pad for malicious attacks. As security professionals build up their firewall technology in an effort to shield their companies, their greatest vulnerability continues to be outside the firewall, on the Internet, where their web sites and apps live.

At RiskIQ, we've taken a unique approach to security by creating a user-emulating security management technology that monitors the entire web and mobile attack surface from the outside in. We're the only company that sees the Internet from the perspective of the browsing public. Our intelligent software outwits the smartest adversaries by seeing what traditional malware scanners can't—even the assets our customers did not even know existed.

By empowering security teams with the ability to see what their web and mobile assets are currently serving to the public from the perspective of their users, organizations can take control of their security program outside their firewall.

At RiskIQ, we believe that knowing is the best defense.

RiskIQ was founded in 2008 and is based in San Francisco.

#### **APPENDIX ITEMS**

List of Sites in Study

#### CONTROL

Alexa Sites akita-pu.ac.jp al-7up.com altaif.org anvelope-autobon.ro artinsight.co.kr atastylovestory.com avforums.com betpasnews.com bilgievi.gen.tr bmwe34club.com bogds.in bossmp3.mywapblog.com bursarestaurant.com buygoldandsilversafely. com cesegypt.com cheki.com.ng chinacmb.com.cn comfiibags.com comtalks.com coolmath.com corlad-piura.com corobori.com cyprustimes.com dahlias.com daily-news.it digimantra.com diskonaja.com dls.ua domainsa.com ecosupp.co.il eropartner.com essence-beautyfriends.eu etradebill.co.kr extremetube.com eyecancer.com fbf.org.br febalcasa.com

Where to Watch Sites acorn.tv

adultswim.com aetv.com amazon.com animalplanet.com apple.com bet.com blockbusternow.com bravotv.com cartoonnetwork.com

У #FollowTheProfit

fin-5.ru flydata.com forever21.co.kr francecars.fr freesearch.co.uk garden-garden.biz ggsupplies.com giethoorn.com gongye360.com healingxchange.com hepsi1arada.com herbalife.com.tw homespakistan.com hotelhotel.com intermonitor.ru irananimations.ir iranmilre.com kiabi.nl kinkireins.or.jp kinoboh.ru lorraine.eu mailtester.com manastir-lepavina.org michoacaninformativo.com miragro.com moneysoldiers.com murahstore.com muskiportal.com netflixroulette.net optionpipsincome.com paavai.edu.in parkson.com.my pharmaceutical-equipment.com phpstate.com poimap.com popmech.ru portaldefacturas.com postroiv.ru

cbs.com

cc.com

cmt.com

cwtv.com

crackle.com

daystar.com

directv.com

disney.com

epixhd.com

dishanywhere.com

dramafever.com

pray-as-you-go.org premiers.ae presentation7.com pro-touring.com progressplay.net pronostici-oggi.it purewatercare.com radiusbank.com real-sex-partners.com redwoodhill.com reinsightdata.com resepmasakanpedia.com rheinbahn.de rsipa.net rv-max.com sacem.fr saji.my samotur.ru scarcitybuilder.com selcukecza.com.tr selector-wixoss.com sengokuixa.jp shairy.com shivkhera.com shopazamerica.com.br shopsomething.com shopxml.com/user/order\_stat showyu.net.cn skidkimira.ru sluhealth.org smaatware.com smartben.com sneak-a-venue.de snu kr softicons.com solar-eyes.net sosyalreklamci.com spring.me

fan.tv fandor.com filmfresh.com flixhouse.com flixster.com fox.com fxnetworks.com gowatchit.com guidebox.com hallmarkspiritclips.com hbogo.com starwoodhotels.com storefeeder.com studential.com submitrelevantsites.com surveyexpression.com syx.com tabiulala.com teamlbi.net telepacific.com thebittersideofsweet.com thecloudoffers.co.uk tintint.com torturegalaxy.com tritmonk.com tuljo.com tungstencopper.net twistyscash.com uchealth.org uninsubria.it unioneprofessionisti.com universalsewing.com urbanwearables.technology urlaubmachtspass.com urpitrek.com uzeyirdogan.com viel-unterwegs.de vlogit.fi vodovoz.ru weac.org wenxuecity.com wetshop.com.br wholesaletrade.co.in wikipower.ru worldlink.com.np wpteq.org yquem.fr zdravnsk.ru

hgtv.com history.com hitbliss.com hulu.com indieflix.com indieflix.com indiepixunlimited.com instant.warnerarchive.com jaman.com jinni.com kidoodle.tv livewellnetwork.com locatetv.com maxgo.com mediatogo.thewb.com mgo.com movies.com mvievisor.com mtv.com mubi.com mubi.com nationalgeographic.com nbc.com netflix.com nextguide.tv nick.com paramountmovies.com pbskids.org play.google.com playstation.com popcornflix.com qello.com reelhouse.org shoutfactorytv.com showtimeanytime.com smartreplay.com snagfilms.com sonyentertainmentnetwork.com spike.com syfy.com targetticket.com tbs.com televisor.com tntdrama.com toysrus.com trutv.com trutv.com tv.com tv.com tv.esquire.com tvguide.com tvland.com us.cinemanow.com usanetwork.com verizon.com vh1.com video.pbs.org videostore.bhn.rr.com viewster.com vudu.com watchi.ly watchitstream.com wolfeondemand.muvies. com yeahtv.com yidio.com youtube.com zapzit.com

#### SAMPLE CONTENT THEFT GROUP

- Notorious Markets -4shared.com baixeturbo.org bajui.com beemp3.com bitsnoop.com catshare.net chomikuj.pl cuevana.tv darkwarez.pl downloads.nl e-nuc.com elitetorrent.com
- 1) Top 3rd GTR 2download.org 2shared.com 3k0.me 4fun.cc 4shared-musica.com 4shared.net 5gg.biz 5mp3.org 88torrent.com adobetorrentz.berlin alexandrebonhomme.fr all-torrents.eu allmyvideos.net animea.net arnaudcornu.com baseofmp3.com battleit.ee baymirror.com bayproxy.com bayproxy.me bayproxy.nl
- extratorrent.cc filestube.com free-tv-video-online.me free-tv-video.me gigabytesistemas.com gosong.net hardstore.com kickass.to molten-wow.com mp3juices.com mrtzcmp3.net muzofon.com

ехца

bayproxy.org baytorrent.eu bittorrent.pm blupaw.net brmlab.cz bthunter.org cloud-vibe.com come.in condorr.at datafile.com deliciousmanga.com demonoid.ph demonoid.pw dizzcloud.com dl4all.com dotpirate.me download-music.lt downloadnow.net downloadonlinemp3.com downloadunit.com drumscum.be emp3world.so

myfreemp3.eu nakido.com novamov.com nowvideo.sx putlocker.is rapidgator.net rapidlibrary.com rutracker.org seedpeer.me thepiratebay.se torrentz.ch torrentz.eu

myfreemp3.cc

extabit.com extendify.com extratorrent.com extratorrent.ee fattylewis.com fenopy.eu file7file.com filecatch.com filehound.co.uk fileom.com filepost.com filesborn.com fileshark.pl fileshut.com filesonic.com filesonicsearch.com filesoup.com firedrive.com forumophilia.com forumwizard.net free-albums.net freemp3in.com

torrentz.in torrentz.me tucows.com uploaded.net vk.com vkontakte.com vmusice.net weblagu.com yts.re zimuzu.tv zing.vn zippyshare.com

freemp3like.com freemp3x.com fullsongs.net general-files.com genteflow.com getpirate.com gooddrama.net grooveshark.com h33tmirror.co h33tunblocked.co hdspot.net hellshare.com hotfilesearch.com houndmirror.com hugefiles.net hulkshare.com ilikerainbows.co index-of-mp3.com irfree.net itemvn.com kat.gs kat.works

kat.yt katmirror.com ketomob.com kickass.pw kickass.so kickasstornet kickasstorrent.rocks kickasstorrents.com kickasstorrents.in kickasstorrents.link kickasstorrents.rocks kickassunblock.com kickassunblock.info kickassunblock.net kset kz kuiken.co labaia.in lanunbay.org limetor.com livepirate.com lumfile.com majaa.net mangabase.co mangable.com mangabro.com mangaeden.com mangago.com mangahit.com mangajoy.com mangapark.com mangapark.me mangasee.co mangasee.com mangasky.co mangatank.com mangawindow.com mediafiredownloads.net mnova.eu monova.org movie2k.to movie4k.to

#### 2) Middle 3rd GTR

Odaydownloads.com 100500mp3.com 100torrent.com 1080p-torrents.info 4songs.pk 720p-torrents.org 720pdownloads.eu 720pdownloads.eu 7797.info a6point.net alquz.com anime-media.com animehere.com mp3facebook.com mp3forte.com mp3joy.net mp3juices.to mp3sale.ru mp3searchy.com mp3sfinder.com mp3skull.fm mp3stahuj.cz mp3truck.com mp3tx.com mp3vip.org mp3wm.com mp3ye.eu mp3yeah.com mp3ylp.com musicaddict.com musicatono.com mybay.pw myfree.cc myfreemp3.biz myfreemp3.co myfreemp3x.com myfreesongs.cc mymp3site.cf mypiratebay.cl no-ip.biz noflag.org.uk nowvideo.eu oostingwebdesign.nl org-proxy.com piratebay.me.uk piratebay1.com piratebayalternate.in piratebaybyproxy.com piratebaymirror.me piratebaysafe.me piratebayunion.com pirateflix.info aodown.com asfile.com

astroddl.com

audiocastle.net

audiovhod.net

bayproxy.net

baytorrent.nl

big.az

bestliens.com

bloglovin.com

boerse.bz

booksee.org

btstorrent.so

btbook.net

mp3-vip.org

mp3c.cc

planetsuzy.org poisk-mp3.com proxicity.info proxy-bay.com proxybay.ca proxybay.de proxybay.in proxybay.link proxytank.com guluxingba.info rapid4me.com readmanga.eu readpanda.net rnb4u.in rootmob.org sciagara.pl searchdepositfiles.com sharedir.com skit.org.ua sockshare.com songs.to su7.info sumotorrent.sx teluga.com thedutchbay.nl thegorillanetwork.com thehotfilesearch.com thepiratebay.hk thepiratebay.org.es thepiratebay.uno thepromobay.co.uk tinydl.com tnttorrent.info topboard.org torrent.pm torrentbar.com byte.to comfishfilmfest.com crazy-manga.com crocko.com daclips.in dadazee.com dailymotion.com dbpotato.net ddlstorage.com

demonoid.mk

desirulez.net

downturk.biz

downturk.net

dmart.vn

piratenpartij.nl

pirateproxy.net

pirateproxybay.org

piratepc.org

pirati.cz

torrentbit.net torrenticity.com torrentkitty.com torrentportal.com torrentproject.org torrentproject.se torrentz.ms torrentz.to tosarang.net tpb.gr tpb.lt tpb.me tpbpirate.tk tpbproxy.eu tpbunblocked.me tv-shuffle.ch uhd-downloads.eu ulub.pl unblocked-piratebay.com unblocked2.bz unlocktorrent.com uploadable.ch uploading.com uptobox.com vemium.com vibe3.com vibeclouds.net wapdam.net waptrick.io warez-bb.org warezrocker.info watch-series.ag watchtvseries.ch wbruder.eu welovetpb.com worldoffiles.net wrzuta.pl wupload.com zamob.com zwarez.net

downvv.eu easybytez.com egexa.re egotorrent.com egydown.com epubbud.com esmangaonline.com esoft.in etorrent.co.kr eval.hu exashare.com expresshare.com extratorrent.be eyeonmanga.com

fastshare.cz fc2.com filecrop.com fileprox.com filesloop.com finz.ru floads.com freedisc.pl freedl2u.me freemp3.fm freemp3go.com freemuzichka.com freshwap.net fullhd-download.net general-catalog.com general-file.com go4up.com godht.com gratismp3x.com haobt.net hipfile.com host4file.net hotnewhiphop.com hunt4tunes.com icyboy.com interflective.com isohunt.rocks isohunt.tf isohunters.net isohuntproxy.net isotorrentz.net iuvip.com jetdl.com just4freeplanet.com kat-proxy.net kat.tf katmirror.link katproxy.co katproxy.link keep2s.cc kenitra.biz kickass.casa kickass.rip kickassbittorrent.link ladytorrent.org libgen.info limetor.org limetorrenturl.com linexdown.net

3) Bottom 3rd GTR 1080p-download.eu 1080p-torrent.casa 1080p-torrent.ml 1080p-torrent.work 1080p-torrents.eu linkforums.com manga2u.co mangababy.com mangahere.com mangapill.com mangaru.me mangasee.me mangatown.com mcanime.net menthix.net mertada.com mfile.org miloman.net mixpromo.ru mixupload.org mmangareader.com mngacow.com mobiles24.com mobiletorrents.in monovaproxy.com mp3-center.org mp3ale.biz mp3bon.com mp3chunk.com mp3clan.nl mp3crop.net mp3crop.org mp3cube.net mp3dict.com mp3enter.net mp3fil.info mp3fire.me mp3ili.net mp3kiss.com mp3lemon.ws mp3limon.info mp3limone.net mp3oak.com mp3poty.com mp3ska.com mp3skull.co mp3skull.im mp3songspk.pk mp3strana.com mp3troll.com mp3tusovka.com mp3world.mobi mp3xd.com mus.ge

1080p-torrents.org 1080p.casa 1080ptorrents.casa 2drive.net 3asq.com 3tig.com music-bazaar.com musica-descargar.net musicov.net muz-muz.net muzbaron.com muzico ru muzikfiendz.net muzofun.net muzogig.net muzonka.com mypirateproxy.com myvi.ru myzlo.info nexusddl.com nhaccuatui.com nvaa.moe onlinepk.net onmanga.net ororo.tv pfv.xyz piratebaymirror.net pirateparty.be portalxd.com precyl.com primewire.ag proxypirate.eu readingmanga.com readmanga.today reptilesound.com rghost.net rockdizfile.com rus.ec rutube.ru sceper.ws scnsrc.me searchizz.com searchonzippy.com seed2peer.com sharedmusic.net sharesix.com sharingforums.net sis001.com smartorrent.com solarmovie.so solidfiles.com soudoc.com stagetorrentz.ru stop-mp3.com submanga2.com

40mp3.com 720p-download.eu 720p-torrent.info 720p-torrent.net 720p-torrents.info 720ptorrent.net subscene.com telecharger-tout.com thebay.ws thebestfiles.net thefastbay.com thefile.me thehydra.ru thepiratebay.asia thepiratebay.to theproxybay.net thevoidgroup.co.uk tinydl.eu tmanga.com tnt24.info tobrut.com torrentba.com torrentcd.org torrentdownloads.ee torrentplay.org torrentroom.net torrentsdownload.eu torrentszona.com torrenty.pl torrentz.cc torrentz.com torrentz.hk torrentz.mx torrentz.st torrindex.info tpbproxy.nl tubeplus.me tubidymp3s.com tunisia-forum.com ultimatez.net umorina.info unb7.com unblocked.bz unblocked3.co uploadc.com upstore.net uyurgezer.net vibecloud.net waptrick.mobi waptrick.us xoofoo.org xtragfx.com your360stop.com zimabdk.com

7dayz.org 7ibt.com abu.se.net adamp3.com adqtzf.org anime-sub.com anime4fun.com animecrazy.net animefactor.com animeflicks.net animeget.com animeonhand.com animesnipe.com animesstream.net animexhibit.com animez.ws ant3rame.com anysoup.ru ardent-desire.com audioz.eu bato.to bestsoftfull.com bitseek.eu bluemirrow.com bmp3z.com boardmp3.com bt-chat.com btku.org bucketgnome.com burning-seri.es byhero.biz cloudyvideos.com comeze.com cryptostorm.is cyberpirate.me czshare.com depiratenbay.be desitvforum.net devxstudis.org dilsekerodosti.com directbigboobsreloaded. net djlist.org dl4all.ws dl4hot.com dlbot.net dltobe.cc dltobe.me docin.com downdlz.biz downdlz.com downloadtorrent.me downmusicas.net downserv.com dvdrip.casa e2u me easy-share.com ebooklink.net egyptfans.net elakiri.lk elitetorrent.to epdrama.com erwap.com etproxy.com

euro-share.com extremefile.com exvagos.com fastpic.ru fileboom.me filedust.net files2share.ch filespr.net filesresidence.com filezoo.com filmovizija.com foundsuccess5.ru freetorr.com full-hd-torrent.org full-hd.link gfx4you.com gfxmore.biz golink.org goodanime.net gratispeliculas.org grifthost.com hd-torrent.link hdtorrent.info holles hotne.ws hydrabay.net iamtherealnick5.ru igla-msk.ru imagefap.com imastudios.com imgserve.net indiahdtv.com jackmp3s.com jjkko.cc jopterhorst.nl justseries.tv kat1080p.net katzzz.com kickass.pm kickasstorrents.agency kickasstorrentz.net kimsufi.com kinokopilka.tv krazymp3z.com lagukane.com lecture-en-ligne.com lekud.com leuyvo.info link2dwn.com link4file.com linkfiles.nl linkleak.se live-down.com lnkdl.com mangabull.com mangaspoon.com mangatrend.com manydl.net

melodycenta.com mixmp3.net moodyz.org moviedox.org moviestorm.eu movshare.me mp3boo.me mp3juices.is mp3mixx.com mp3s.vet mp3sk.org mp3time.com mp3title.com mp3tridi.com multifilesfind.net music22.net music88.net musicville.fm myanime.me mydnspro.net myfreesong.eu narutomanga.cz niceoppai.net nntt.org nowdownload.at nowvideo.co nulledweb.com onepieceanime.net onepieceofbleach.com oyuncehennemi.com oze.wang pantipnews.com partidopirata.com.ar pinoyanime.tv piratebaytorrents.info pirateproxy.link playgoogle.name poiskmp3.org portalnet.cl pp22pp.com purevid.com putlocker.ws rapidareena.com rapidmoviez.org rapidpich.ir rbt.xyz redbunker.net rsmoviedownloads.com scamfraudripoff.com scaminformer.com seasonwars.com seed2peer.us sfshare.se sitego.com smiling-dream.info smoz.ru softarchi.com sogou.com

solarmovie.is songily.com songsko.com sooshare.eu stagetorrents2.net studentsharez.com submanga.com super-mp3.com symbianpinoy.com syria4soft.com t411.io taobao.com the-proxy-bay.com thedarewall.com thegamepirate.com themusicbay.com thepiratebay.click thepiratebay.de.com thepiratebay.vu theresistanceseries.com theunblockedbay.info thisdown.org tohari.com tor-finder.org torcatch.net torhub.net torrentcrazyunblocked.co torrentino.ru torrentz.la torsky.org torzila.com turkoplus.biz tz.ai unbanthe.com unblocked.casa uploadboy.com uploadto.us userscloud.com videoweed.com vincent-shorette.com vitorrent.co vn-zoom.com vodly.to wallovenswarmingdrawers.com warezforest.com websitedesignecommerces.com wootmanga.com worldofscan.info wtorrent.org xvidstage.com yadisc.ru yallarab.com zapto.org zippyon.org

### REFERENCES

- 1 "Markets for Cybercrime Tools and Stolen Data", Rand National Security Research Division, 2014.
- 2 "16.6 Million People Experienced Identity Theft In 2012". Bureau of Justice. (2012).
- 3 "Online Exposure" Consumer Reports June, 2011.
- 4 "Internet Security Threat Report" Symantec April 2015.
- 5 "Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes" Federal Bureau of Investigation June 2015.
- 6 "Russian Underground Revisited" Trend Micro 2014.
- 7 "What is an untrustworthy supply chain costing the US digital advertising industry?" Interactive Advertising Bureau (IAB) and EY November 2015.
- 8 "2015 Ad Blocking Report" Adobe and PageFair August 10, 2015.
- 9 "Ad Blocking is Every Publisher's Problem Now" Digiday April 8. 2015.
- 10 "How Much Does a Botnet Cost?" ThreatPost February 28, 2013.
- 11 "Nine bad botnets and the damage they did" We Live Security February 25, 2015.
- 12 "Five Alternatives to BitCoin" We Live Security March 5, 2015.
- 13 "The Economic Impact Of Cybercrime And Cyber Espionage" McAfee July 2013.
- 14 "Updated: List of Dark Net Markets (Tor & I2P)" DeepDotWeb October 28, 2013.
- 15 "Updated: List of Dark Net Markets (Tor & I2P)" DeepDotWeb October 28, 2013.
- 16 "Internet Organised Crime Assessment Report (IOCTA)" Europol September 29, 2014.
- 17 Goodman, Marc. *Future Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It DoubleDay,* February 24, 2015.
- 18 Goodman, Marc. *Euture Crimes: Everything Is Connected, Everyone Is Vulnerable, and What We Can Do About It DoubleDay,* February 24, 2015.
- 19 "Russian Underground Revisited" Trend Micro 2014.
- 20 "Markets for Cybercrime Tools and Stolen Data", Rand National Security Research Division, 2014.
- 21 "How Much Does a Botnet Cost?" ThreatPost February 28, 2013.
- 22 "Internet Security Threat Report" Symantec April 2015.





@RisklQ

#FollowTheProfit