View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Indiana University Bloomington Maurer School of Law

Maurer School of Law: Indiana University
Digital Repository @ Maurer Law

Indiana Law Journal

Volume 93 | Issue 4 Article 2

Winter 2018

Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat

Andrew V. Moshirnia
Monash University, andrew.moshirnia@monash.edu

Follow this and additional works at: https://www.repository.law.indiana.edu/ilj


Part of the Entertainment, Arts, and Sports Law Commons, Internet Law Commons, Law and Economics Commons, Law and Society Commons, and the National Security Law Commons

Recommended Citation
Moshirnia, Andrew V. (2018) "Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat," *Indiana Law Journal*: Vol. 93 : Iss. 4 , Article 2.
Available at: https://www.repository.law.indiana.edu/ilj/vol93/iss4/2

This Article is brought to you for free and open access by the Law School Journals at Digital Repository @ Maurer Law. It has been accepted for inclusion in Indiana Law Journal by an authorized editor of Digital Repository @ Maurer Law. For more information, please contact wattn@indiana.edu.

JEROME HALL LAW LIBRARY
INDIANA UNIVERSITY
Maurer School of Law
Bloomington

Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat

ANDREW V. MOSHIRNIA*

Current academic and policy discussions regarding video game piracy focus on the economic losses inherent to copyright infringement. Unfortunately, this approach neglects the most significant implication of video game piracy: malware distribution. Copyright-motivated efforts to shut down file-sharing sites do little to reduce piracy and actually increase viral malware infection. Pirated video games are an ideal delivery device for malware, as users routinely launch unverified programs and forego virus detection. The illicit nature of the transaction forces users to rely almost entirely on the reputation of websites, uploaders, and other users to determine if a file is safe to download. In spite of this, stakeholders continue to push for ineffectual anti-infringement actions that destroy this reputational infrastructure.

Scholars and policymakers have not made a case for utility by considering only first-stage economic incentives to create content. In addition to the economic consequences, malware must be taken seriously as a threat to infrastructure and national security, especially in light of Russia's efforts to infect machines to influence and delegitimize elections. Accordingly, this Article proposes that we adopt a harm reduction philosophy that both dissuades piracy and decreases the malware risk attendant to ongoing piracy.

---

* Andrew V. Moshirnia received his J.D. from Harvard Law School, where he served as Forum Chair of the Harvard Law Review and received his PhD from the University of Kansas. He is currently a Senior Lecturer at Monash Business School, Monash University. He would like to thank Ashley Chung, Aaron Dozeman, Sonia Fleury, Hank Greenberg, Anthony Moshirnia, Brian Sheppard, and the scholars of the IPSC for their valuable assistance.

INTRODUCTION

Nearly a decade ago, Estonia[1] seriously considered invoking Article 5 of the North Atlantic Treaty when the nation's banks, parliament, ministries, and media outlets were bombarded not by gun shells, but by waves of malicious internet traffic.[2] The

1. The country has been a NATO member since 2004. *NATO Welcomes Seven New Members*, NATO (Apr. 2, 2004), http://www.nato.int/docu/update/2004/04-april/e0402a.htm [https://perma.cc/Y29K-BBFW].

2. Scheherazade Rehman, *Estonia's Lessons in Cyberwarfare*, USNEWS (Jan. 14, 2013, 3:34 PM), http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare [https://perma.cc/G4UM-Q243] ("Estonia shouted loudly from the roof tops that they were being attacked, that an act of war had being committed by the Russians, and called upon its allies to assist, but they had a hard time getting anyone to believe that this was a 'real war' and not a cybernuisance. In the end no one came to help the Estonians but what that alarm did do was to put global cyberattacks on the warfare discussion table for . . . NATO."); *see also* Michael N. Schmitt, *The Law of Cyber Warfare:*

specter of cyberwarfare has only increased since.[3] Russian cyberattacks, including pervasive election meddling, have captured the public attention.[4] In an increasingly tense political climate, cyber security is paramount. Yet, little has been done to address a significant fifth column—malware infected gaming computers.

The United States has neglected this critical threat to the integrity of our network infrastructure. Video game piracy is not only important with respect to considerations of copyright infringement, but it is also an ideal means to distribute malware to powerful computers with broadband connections. Sizeable infections have been traced to cracked copies of popular games,[5] but these incidents are rarely taken seriously in the press, treated instead as pirates' karmic desserts. Though the potential for economic and geopolitical mayhem cannot be overstated, video game piracy continues to be treated in policy and practice solely as a copyright problem.

It is hardly surprising that economic concerns dominate the discussion of video game piracy, a practice that imposes unique harms on copyright holders and complicates loss assessment. While users who download movies or music may harm ticket and unit sales, respectively, users who pirate video games may inflate service costs, consume bandwidth, and distort the community's game-playing experience.[6] Moreover, the complex relationship between piracy and video game sales[7]—where

---

Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 271, 273 (2014).

3. *See* Daniel Brecht, *Cyber Warfare and Cyber Weapons, a Real and Growing Threat*, INFOSEC INST. (Jan. 15, 2015), http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/#gref [https://perma.cc/KP7C-E3T2] (discussing possibility of crippling cyberattack); Ian Bremmer, *These 5 Facts Explain the Threat of Cyber Warfare*, TIME (June 19, 2015), http://time.com/3928086/these-5-facts-explain-the-threat-of-cyber-warfare [https://perma.cc/8225-XVXT] ("[T]he biggest threat to national security these days comes from not from aircraft carriers or infantry divisions, but a computer with a simple Internet connection."); Michael Pizzi, *Cyberwarfare Greater Threat to US Than Terrorism Say Security Experts*, AL JAZEERA (Jan. 7, 2014, 5:00 PM), http://america.aljazeera.com/articles/2014/1/7/defense-leaders-saycyberwarfaregreatestthreattous.html [https://perma.cc/E7LH-8HEP]; Schmitt, *supra* note 2, at 275 (detailing growing cyberwarfare threat).

4. NCCIC, *GRIZZLY STEPPE – Russian Malicious Cyber Activity* (Dec. 29, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [https://perma.cc/6GVY-6224] (detailing Russian interference in the 2016 presidential election); Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (Jan. 9, 2017, 7:03 AM), http://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556 [https://perma.cc/LYC7-W5H9] ("Cyberattacks in Ukraine, Bulgaria, Estonia, Germany, France and Austria that investigators attributed to suspected Russian hackers appeared aimed at influencing election results, sowing discord and undermining faith in public institutions that included government agencies.").

5. *See infra* Part II.

6. At the same time, video game developers enjoy a larger array of Digital Rights Management (DRM) opportunities than their audio-visual producing counterparts, with the ability to degrade gameplay in subtle ways. Andrew V. Moshirnia, *Giant Pink Scorpions: Fighting Piracy with Novel Digital Rights Management Technology*, 23 DEPAUL J. ART TECH. & INTELL. PROP. L. 1, 51–53 (2012) (discussing whimsical antipiracy DRM, such as "a player running a pirated version of the game finds that guns now shoot chickens instead of bullets").

7. *See* Ernesto Van der Sar, *File-Sharers More Likely To Pay for Movies, Books, Games and Concerts*, TORRENTFREAK (Oct. 18, 2012), https://torrentfreak.com/file-sharers-buy-

some evidence suggests pirates purchase more games and boost publicity, thereby driving legitimate purchases—has engendered debate as to the proper monetary valuation of each unauthorized game download.

But the dispute over the proper discount factor for pirated copies largely misses the greater evil. To be sure, economic loss due to software piracy is lamentable. But the matter of greater concern should be the delivery of malicious software to users. Software piracy, and video game piracy in particular, presents an important virus vector endangering users, networks, and cybersecurity. Pirating users download and execute unverified files, often disabling or disregarding virus detection in the process. Insufficient attention has been paid to this infection avenue, a troubling oversight in a growing climate of geopolitical cyber interference and warfare.[8]

Analysis of antipiracy efforts also has focused on the cost-benefit calculations of industries and individual actors: the developers that protect content, the hackers that remove that protection, the torrent sites that link to cracked content, and the downloading users. This balance typically considers how doggedly companies should utilize antipiracy software in the face of legitimate user complaints, how companies might entice users to purchase products, and how judicial levers (such as heightened penalties and secondary liability) might be manipulated to sap the desire to pirate or host links to pirated content. While the study of pirate motivations and corporate strategies for minimizing piracy is important,[9] to date this analysis has largely

---

more-movies-121018 [https://perma.cc/X36A-9V2D] (discussing Dutch study finding file-sharers more likely to buy games legally); Kantar Media, *OCI Tracker Benchmark Study "Deep Dive" Analysis Report* (2012), https://www.ofcom.org.uk/__data/assets/pdf_file/0021/57441/deep-dive.pdf [https://perma.cc/M7VJ-DXEL] (noting that higher infringers spent more on legal content than other users, accounting for 11% of media consumed while accounting for only 3% of the population). These findings should not be confused with a causal relationship however. It is likely that media consumers simply do not differentiate between legal and illegal methods to acquire content.

8. While the malware impact of antipiracy torrent site takedowns is not discussed at all in the literature, some attention has been paid to the potential security concerns of DRM. *See* Eric Maher, *Defenseless in the Zombie Infested Internet: Why Audio-Visual Works Demand Exemption Under the Digital Millennium Copyright Act*, B.C. INTELL. PROP. & TECH. F. 1, 8 (2013) (arguing that DRM vulnerabilities requires further exploration necessitating exemption of DRM circumvention from DMCA); Moshirnia, *supra* note 6, at 28 n.105, 34 n.126 (noting that users may consider DRM a sort of malware or rootkit). These concerns stem largely from Sony's BMG copy protection scandal, in which undisclosed DRM on music CD's installed rootkits on the user's computer that could subsequently be exploited by hackers. Eran Kahana, *Sony's Drm Experience: When Copyright Protection Attacks*, 60 CONSUMER FIN. L.Q. REP. 627 (2006); *Viruses Use Sony Anti-Piracy CDs*, BBC (Nov. 11, 2005, 11:11 AM), http://news.bbc.co.uk/2/hi/technology/4427606.stm [https://perma.cc/GQ4D-N2TG]. While not nearly as serious, Ubisoft's UPlay DRM similarly had an exploit that could have allowed hackers to gain remote access to a user's computer. Alec Meer, *Ubisoft Responds to UPlay Security Drama*, ROCKPAPERSHOTGUN (July 30, 2012, 5:30 PM), https://www.rockpapershotgun.com/2012/07/30/ubisoft-respond-to-uplay-security-drama [https://perma.cc/2UB8-Z5TN].

9. *See* Moshirnia, *supra* note 6, at 26–30 (noting "a distinct set of arguments that pirates employ to justify their conduct").

ignored external social costs imposed by the viral threats attendant to piracy and the impact of the antipiracy campaign on the spread of malware.[10] These threats to network infrastructure and security have only grown more acute as national actors have realized the crippling potential of cyberattacks.

Ignoring the link between piracy and malware has serious consequences. Failing to capture the overall impact of piracy may weaken motivations to curb it. Moreover, a refusal to contemplate the growing threat of malware is already leading to deleterious antipiracy campaigns that exacerbate viral threat by reducing malware barriers. Efforts to curb torrenting activity have centered on attempts to shutter various trackers. While campaigns to take down trackers have been successful[11] in pulling down major torrent sites, torrent traffic seems to have been unaffected.[12] Worse still, the disruption of torrent communities decreases the effectiveness of reputational barriers to viral spread. Simply put, closing torrent trackers does little to reduce piracy and actually increases malware and botnet proliferation.

This Article addresses the viral threat in video game piracy and highlights the lack of attention it receives. Such piracy presents a malware problem involving losses to consumers as well as to the security of the public at large. Part I sets out the state of the video game industry and the current legal regime addressing the rate of piracy within that industry: the various players in distributing pirated content, the struggle to measure and quantify corporate loss due to piracy, and the last decade of efforts to shutter torrent sites. Part II sets out the dangers of malware in the pirated software context by examining the avenues for malware spread, the defenses to such spread, the unique characteristics of pirated software that diminish the effectiveness of most malware defenses, case studies of widespread malware in pirated games, and the impact of shuttering torrent sites, which removes the vital reputational barrier to viral transmission. Part III proposes alternate approaches to curbing viral spread based on a harm reduction model, including a cessation of torrent site takedowns, robust Digital Rights Management (DRM) during the initial sales window, and a voluntary removal of DRM following that period. Part IV addresses likely criticisms and sets out avenues for further exploration.

I. PIRACY IN THE VIDEO GAME INDUSTRY: THE ECONOMIC DEBATE OVER PIRACY AND DRM

The video game industry is a leading revenue generator within the wider entertainment industry, with projected revenues of approximately $100 billion in 2016,[13]

---

10. To the extent these threats have been discussed, industry actors have largely focused on economic threats to the pirating user. *See infra* Part I.

11. *See infra* Part I.

12. *See infra* Part II.

13. Jeff Desjardins, *How Video Games Became a $100 Billion Industry*, BUS. INSIDER (Jan. 12, 2017, 6:02 PM), http://www.businessinsider.com/the-history-and-evolution-of-the-video-games-market-2017-1 [https://perma.cc/55HQ-K9XW] (noting size of current market and discussing large projected growth of home VR market to $162 billion within four years); Mike Minotti, *Video Games Will Become a $99.6B Industry This Year as Mobile Overtakes Consoles and PCs*, VENTUREBEAT (Apr. 21, 2016, 8:30 AM), http://venturebeat

and approximately $25 billion in the United States alone.[14] Yet video game piracy has been relatively ignored in favor of movie and music piracy, despite the smaller economic footprint of those industries.[15] For comparison, the global box office revenue in 2015 was $38 billion,[16] with approximately $11 billion in North American revenue, while global music industry revenue was flat at $15 billion in that same year.[17] By any measure, the video game industry is enormous.[18]

This wide install base, however, makes video games attractive targets for pirates and malware spreaders alike. While companies employ various technological strategies to limit piracy, these efforts have had mixed success. The cost of this piracy has always been a matter of debate, with parties differing as to the rate of the activity and the correct loss to ascribe to each download. But, unfortunately, the current focus is almost completely fixed on matters unrelated to malware protection.

This Part provides an overview of the piracy pipeline, as well as industry-wide and individual-title piracy loss estimates. Video game developers employ DRM software to protect the initial sales window for their releases; the warez scene cracks that DRM, and the public gains access to cracked games through torrents.

.com/2016/04/21/video-games-will-become-a-99-6b-industry-this-year-as-mobile-overtakes-consoles-and-pcs [https://perma.cc/TXF5-NJBU] (noting size of market and commenting on growth potential of mobile market). The wide penetration of smart phones has coincided with a large increase in game releases for mobile devices. While this Article is primarily concerned with PC video game piracy and thus PC malware, the rooting of mobile devices also presents a troubling threat to both consumer and network safety. *See, e.g.*, Matthew Reynolds, *Gooligan Malware Attack Hits One Million Google Accounts*, WIRED (Dec. 1, 2016), http://www.wired.co.uk/article/android-gooligan-ghost-push-hack [https://perma.cc/3C3B-ZAPU] (describing Gooligan, a malware attack on Android devices that has compromised approximately one million Google accounts).

14. Chris Morris, *Level up! Video Game Industry Revenues Soar in 2015*, FORTUNE (Feb. 16, 2016), http://fortune.com/2016/02/16/video-game-industry-revenues-2015 [https://perma.cc/G7QX-PQ9U].

15. This focus is especially irritating in the malware context, as movie and music piracy does not present as grave a malware threat as video game piracy. *See infra* Part II.C.

16. Pamela McClintock, *Global 2015 Box Office: Revenue Hits Record $38 Billion-Plus*, HOLLYWOOD REP. (Jan. 1, 2016, 9:18 AM), http://www.hollywoodreporter.com/news/global-2015-box-office-revenue-851749 [https://perma.cc/F5MS-US8V].

17. Jonathan Chester, *How Blockchain Startups Are Disrupting the $15 Billion Music Industry*, FORBES (Sept. 16, 2016, 11:07 AM), http://www.forbes.com/sites/jonathanchester/2016/09/16/how-blockchain-startups-are-disrupting-the-15-billion-music-industry/#1cfee8d2652c [https://perma.cc/584G-YBTS].

18. *See, e.g.*, Jeff Grubb, *October 2016 NPD: Battlefield, Mafia, and Gears Dominate the Sales Chart*, VENTUREBEAT (Nov. 17, 2016, 4:20 PM), http://venturebeat.com/2016/11/17/october-2016-npd-battlefield-mafia-and-gears-dominate-the-sales-chart [https://perma.cc/FP4V-8AX5] (noting video game industry generated $875.7 million in revenue in October 2016).

A. Piracy Pipeline: Cracking Files and Distributing Them to the Public

1. Publisher Use of DRM

The Copyright Clause, Article I, Section 8 of the United States Constitution, empowers Congress to secure exclusive rights to authors "[t]o promote the Progress of Science and useful Arts." Online piracy of video games can violate several exclusive rights granted to rights holders under the Copyright Act of 1976.[19] Video game piracy, in its most basic form, reproduces and distributes copies of a protected game.[20] Any unauthorized installation of a file may be considered piracy, but the majority of games at issue have been modified to remove copy protection software. That is, they have been "cracked." Developers have largely attempted to address the problem of software piracy, and video game piracy in particular, with DRM techniques.[21] Their effectiveness is debatable.[22] While the use of DRM may anger and inconvenience users, and various developers have lamented the use of DRM,[23]

---

19. 17 U.S.C. § 106 (2012); *see* Moshirnia, *supra* note 6, at 8 n.22 (giving overview of copyright law with regard to video games as "audiovisual works" under *Stern Electronics, Inc. v. Kaufman*, 669 F.2d 852, 857 (2d Cir. 1982)).

20. 17 U.S.C. § 106(1), (3) (right to reproduce and right to distribute).

21. *See* Moshirnia, *supra* note 6, at 33–37 (providing an overview of DRM); Greg Voakes, *Why Don't We Have a Comprehensive Solution for Video Game DRM Yet?*, FORBES (June 12, 2012, 5:28 PM), http://www.forbes.com/sites/gregvoakes/2012/06/12/why-dont-we-have-a-comprehensive-solution-for-video-game-drm-yet [https://perma.cc/X4ZN-6W3D] (listing different approaches to DRM).

22. It is of paramount importance to study the motivators for pirates: motivations of both crackers that defeat DRM and the leechers/users that consume pirated content, as this will inform the efforts to dissuade piracy. If pirates are purely rational actors, then an open pricing model should defeat piracy, provided that the lowest available price for the content is lower than the economic value of the effort needed to pirate. In such a case, DRM may still play a pivotal role in raising the cost of pirating (indeed, piracy on consoles necessitating a mod chip is far less than on PCs). *See* Moshirnia, *supra* note 6, at 26–30. Ironically, the use of DRM may make a legitimate copy of a game considerably less valuable than that pirated copy, free of constraints imposed in an effort to encourage purchase. The threat of litigation may similarly raise the cost of consumption (though this is negated somewhat by the remoteness of the threat).

23. Kara Ashbeck, *Shadow Warrior 2 Developers Take a Stand Against DRM and Anti-Piracy Software*, TOPSHELFGAMING (Oct. 24, 2016, 10:49 AM), http://topshelfgaming.net/developers-take-stand-anti-piracy [https://perma.cc/5NYZ-R2L2] (noting that developers Flying Wild Hogs and CD Projekt Red have sworn off DRM, an "[un]popular stance in the AAA industry however, with the rise of Denuvo and DRM in increasingly more high-profile games"); Michael Larabel, *LGP Introduces Linux Game Copy Protection*, PHORONIX (June 23, 2008), http://www.phoronix.com/scan.php?page=article&item=lgp_copy_protection&num=3 [https://perma.cc/3HHV-NPNX] (discussing the decision to add DRM to games, "Trust me, I don't like it, I'm not happy about it, but we HAVE to do this. I've fought for 6 years against the need for any kind of protection system and all that's happened is that for every legitimate copy of an LGP game out there, there are probably 3-4 pirated copies. . . . [W]e have to face reality in that many many people buy games and put them online for people to download. Hell, we even get people asking for tech support on games we KNOW are pirated.").

the great majority of publishers[24] use some sort of protection to prevent the unauthorized installation of video game software.[25]

Contrary to popular understanding, the purpose of DRM is not to keep the video game forever uncrackable.[26] Instead, the goal is to protect sales during the initial release window. If a protection scheme remains impervious for this period, it has succeeded. Numerous developers have commented that so long as DRM holds for only a few weeks, it has accomplished its purpose.[27] At the bare minimum, DRM exists to prevent zero-day piracy, that is, piracy on or before the release date for a title.[28]

The difficulty with DRM largely arises from consumer reaction. Purchasers may suffer under DRM that effectively breaks the game or otherwise hampers its use.[29]

---

24. *See* Ashbeck, s*upra* note 23 (noting AAA developers commonly use DRM); Mark Walton, *PSA: Get DRM-Free Versions of Steam Games You Already Own With GOG Connect*, ARS TECHNICA (June 2, 2016, 9:30 AM), https://arstechnica.com/gaming/2016/06/transfer-steam-games-to-gog-connect-drm-free [https://perma.cc/ER73-4TXH] (noting that Steam games use DRM and there are limited DRM-free versions on GOG.com); *Game Database*, DAEMON TOOLS F., https://web.archive.org/web/20160622123944/http://forum.daemon-tools.cc/gamedb.php?letter=A [https://perma.cc/X8CX-CATB] (collecting all known DRM in games).

25. Some publishers have sworn off DRM, with mixed results.

26. Moshirnia, *supra* note 6, at 18 n.69 ("The purpose of copy protection is not making the game uncrackable - it is impossible. The main purpose is to delay the release of the cracked version. Maximum sales rate usually takes place in the first month(s) after the game release. If the game is not cracked in that period of time, then the copy protection works well."); Ashbeck, *supra* note 23; Shamus Young, *DRM Is Over*, ESCAPIST MAG. (Dec. 16, 2014, 2:00 PM), http://www.escapistmagazine.com/articles/view/video-games/columns/experienced-points/12765-Denuvo-s-Success-Proves-the-Futility-of-DRM [https://perma.cc/9C7Y-J2J8] (noting "while you can't make something impossible to crack, you can make it really annoying, time-consuming, and difficult to do so").

27. One developer, Martin Slater of 2K Australia, discussed the success of the DRM used in the game *BioShock*. Moshirnia, *supra* note 6, at 34 ("We achieved our goals. We were uncracked for 13 whole days. We were happy with it. But we just got slammed. Everybody hated us for it. It was unbelievable. . . . You can't afford to be cracked. As soon as you're gone, you're gone, and your sales drop astronomically if you've got a day-one crack."); Jon Martindale, *Denuvo May Have Lost the Battle, but It Wants To Win the War*, KITGURU (Oct. 18, 2016), http://www.kitguru.net/gaming/jon-martindale/denuvo-may-have-lost-the-battle-but-it-wants-to-win-the-war [https://perma.cc/L6EQ-2JVT] (quoting a popular DRM developer, "we always tell our clients to help manage their expectations. Our scope is to prevent early cracks for every title. We want to allow an initial window when a game is released to have an uncracked version and thus guarantee sales.").

28. PC Gamer UK, *Why Steam Works: How Valve Is Revitalising PC Gaming*, GAMES RADAR (June 14, 2008), http://www.gamesradar.com/why-steam-works/#top_%20banner [https://perma.cc/5HM2-U6AQ] ("Day zero piracy is where a game is released for free by pirates before the official release. It's disastrous for the developer and publisher because whatever route gets the game out to the gamer first will be the favoured choice, so a game uploaded to the internet before the release date will have a huge impact on sales."); *see also* Moshirnia, *supra* note 6, at 34 (discussing impact of zero-day piracy).

29. This is common in "always-online" DRM, which requires a computer to access the internet to validate a game. Servicemen and women have complained that this effectively

The wider pirating community has justified its actions as a response to DRM.[30] Moreover, researchers and consumer advocates have lambasted the fact that the mere circumvention of DRM, absent an exemption from the Library of Congress, is a crime under Section 1201 of the Digital Millennium Copyright Act (DMCA).[31] The fickle, arbitrary, and broken exemption process may be most familiar to consumers who have sought to root or "jailbreak" their devices, only to discover that jailbreaking a smartphone was exempt, but jailbreaking a tablet was not exempt.[32] This obvious disparity was not rectified for three years.[33]

2. The Scene, Leakers, and Leechers

The key players in the cracking and transmission of software are the Scene, leakers, and leechers/seeders. In short, hackers in the Scene defeat DRM, leakers scrape content from the Scene and put it into public distribution channels (typically BitTorrent and netlockers), and end users (leechers/seeders) download (and further share) that content.

The first step of defeating copy protection appears to be most commonly achieved by only a few dedicated communities of like-minded pirates.[34] These communities are collectively known as "The Scene" or "The Warez Scene."[35] When a new piece

---

makes these games unplayable. Ben Kuchera, *The Victims of PC Gaming DRM: One Soldier's Story*, ARS TECHNICA (Feb. 23, 2010, 11:08 PM), https://arstechnica.com/gaming/2010/02/the-victims-of-pc-gaming-drm-one-soldiers-story [https://perma.cc/ER6Z-2Q8U] ("I'm deployed to Iraq right now, and [DRM] has ranged from annoying to unforgivable for me."). Servers may also crash, barring users from access their games. This occurred frequently in Diablo III and generated many interesting memes. IFHT Films, *If Diablo 3 Was a Girl*, YOUTUBE (May 16, 2012), http://www.youtube.com/watch?v=I43GUnZN_s4 [https://perma.cc/K42N-NAXS] (mocking the "error 37" error message displayed when a user cannot connect to the game servers); Erik Kain, *'Diablo III' Fans Should Stay Angry About Always-Online DRM*, FORBES (May 17, 2012, 1:50 PM), http://www.forbes.com/sites/erikkain/2012/05/17/diablo-iii-fans-should-stay-angry-about-always-online-drm [https://perma.cc/J4RY-664E]; Michael Lacerna, *Diablo 3 Servers Crash Within Minutes of the Game's Launch*, IGXPRO.NET (May 15, 2012), https://web.archive.org/web/20120719161354/www.igxpro.net/2012/05/15/diablo-3-servers-crash-within-minutes-of-the-games-launch/0416423 [https://perma.cc/H9TH-JYQY].

30. Moshirnia, *supra* note 6, at 26 (collecting pirate statements regarding DRM).

31. 17 U.S.C. § 1201 (2012).

32. Timothy B. Lee, *Jailbreaking Now Legal Under DMCA for Smartphones, but Not Tablets*, ARS TECHNICA (Oct. 25, 2012, 6:45 PM), https://arstechnica.com/tech-policy/2012/10/jailbreaking-now-legal-under-dmca-for-smartphones-but-not-tablets [https://perma.cc/L699-8FAS] (noting that "[a]rbitrary rulings illustrate fundamental brokenness of the DMCA").

33. Luke Villapaz, *It's Now Legal To Jailbreak Your iPhone, Android Smartphone, Tablet or Smart TV*, INT'L BUS. TIMES (Oct. 27, 2015, 12:53 PM), http://www.ibtimes.com/its-now-legal-jailbreak-your-iphone-android-smartphone-tablet-or-smart-tv-2158645 [https://perma.cc/T2YY-6R2M].

34. Enigmax, *Interview with a Warez Scene Releaser*, TORRENTFREAK (May 16, 2007), http://torrentfreak.com/interview-with-a-warez-scene-releaser [https://perma.cc/6W5V-FSFG].

35. *Id.* The Scene has a detailed hierarchy, with release groups or people who actually

of software is released, various groups race to author cracks to circumvent targeted DRM.[36] Ironically, these groups often tout the importance of recognizing creativity and the intellectual property rights of Scene members, stressing the importance of contributing to the Scene and "deploring freeriding leechers."[37] Some well-known groups that focus largely on cracking video game DRM are 3DM, ReLoaded, and Skidrow.[38]

Scene releases are initially distributed through private channels, such as File Transfer Protocol (FTP) or private torrents. These releases are typically considered malware free, as the Scene community is a dedicated social group who are ideologically driven and receives praise and support for their impressive intellectual efforts.[39] It would make little sense for the Scene to poison its internal releases, especially in light of the attendant social costs. However, "many of the motivations of hardcore pirates—pride, community loyalty, peer reinforcement—are absent from second-order pirates, who merely implement the cracks authored by first-order pirates."[40]

The introduction of malware typically occurs during the repacking and hosting of Scene releases or the creation of decoy torrents masquerading as Scene releases.[41] In the former, malware is inserted into an otherwise functioning cracked version of the game. In the latter, malware is simply renamed to mimic a game.[42] Leakers take

---

release cracked software into the Scene at the top. *The Warez Scene Hierarchy*, SCEPER, https://web.archive.org/web/20111230032021/http://sceper.eu/2006/06/the-warez-scene-hierarchy.html [https://perma.cc/KZF8-FQ8R].

36. This may include keygens or alternate install files.

37. Moshirnia, *supra* note 6, at 16.

38. *Id.*

39. *Id.* That is not to say that scene releases are always clean. The Scene group Megahertz was discovered to have included spyware in their releases. The greater torrent community was outraged, as this violated a common assumption regarding the norms governing the piracy pipeline. Andy, *Piracy Release Group Has Been Spying on Downloaders For 9 Months*, TORRENTFREAK (Nov. 11, 2013), https://torrentfreak.com/piracy-release-group-has-been-spying-on-downloaders-for-9-months-131111 [https://perma.cc/Q33U-4D2V].

40. Moshirnia, *supra* note 6, at 16–17.

41. Andy, *supra* note 39 (noting that "while viruses and malware can be added to any file online, it is rare for malicious content to be planted by those in the so-called warez scene").

42. Decoy torrents are problematic for several reasons. The most obvious is that IP creators often create decoy torrents themselves (typically with corrupted files rather than malware). This practice may lead some pirates to associate malware delivering decoys with antipiracy efforts. A common malware tactic is to release "prerelease" or "precrack" torrents. *See, e.g.*, Arshad96, Comment to *WARNING: The New Torrent Planet Coaster: Full Game Contains a Password Stealing Application and a Bitcoin Miner!*, REDDIT (Jan. 16, 2017), https://www.reddit.com/r/Piracy/comments/5o8qab/warning_the_new_torrent_planet_coaster_full_game [https://perma.cc/F6SB-VZZN] (warning of bitcoin miner and password ripper in Planet Coaster, a game not yet cracked due to Denuvo DRM); Nat Torkington, *HBO Attacking BitTorrent*, RADAR (Oct. 4, 2005), http://radar.oreilly.com/2005/10/hbo-attacking-bittorrent.html [https://perma.cc/6JWT-EC57] (documenting HBO decoy torrent and garbage packet antipiracy efforts regarding the television show *Rome*); *Madonna Swears at Music Pirates*, BBC (Apr. 22, 2003, 9:29 AM), http://news.bbc.co.uk/2/hi/2962475.stm [https://perma.cc/HR8F-W8WR] (noting Madonna's use of decoy tracks, which contain no music but instead have Madonna saying, "What the f*** do you think you are doing?"). In

Scene releases and repackage[43] them in public torrents or netlockers. This is not typically done to remove attribution of the crack and may cause scandal if the origin of the crack is obscured.[44] Digital badges and special headers often signal power users, who post many highly rated and presumptively safe software files. The new package may come nested with malware or the package itself may be virus free but hosted on a site that uses malvertising to deliver malware.

Finally, leechers (pirating users outside of the Scene) download these torrents. Users that contribute to the torrent cloud after the initial download function as seeds. Users may also comment in threads regarding torrents: offering thanks, giving troubleshooting tips, and warning of potential viral threats. Leecher motivation is typically framed as anti-DRM, anticorporate, a response to expensive or buggy games, and an opportunity to demo a game before legitimate purchase.[45]

There is considerable tension between the Scene and downstream groups,[46] in part because second-order pirates may introduce viruses in repacks, but may also be

---

contrast, game creators have seeded feature-restricted versions of their games in order to frustrate pirates and provide a demo. *See, e.g.*, Dan Crawley, *The Witness Is Getting Pirated Big Time — Creator Jonathan Blow Warns It'll Impact Future Projects*, VENTURE BEAT (Jan. 29, 2016, 5:23 AM), http://venturebeat.com/2016/01/29/the-witness-is-getting-pirated-hard-creator-jonathan-blow-warns-itll-impact-future-projects [https://perma.cc/HR8F-W8WR] (noting Jonathan Blow, creator of Braid, put out a partial version of Braid, a smash indie game, in torrents).

43. "Repack" typically designates a highly compressed release, allowing for easier download. Repack may also be used when an initial release is found to be buggy and is subsequently rereleased. Some releases may already be compressed when taken from the Scene.

44. On rare occasions, Scene groups may complain that other groups are pirating their work. Andy, *'Skidrow' Pirates Get Pirated After Removing Their Own 'DRM*,*'* TORRENTFREAK (May 4, 2014), https://torrentfreak.com/skidrow-pirates-get-pirated-after-removing-their-own-drm-140504 [https://perma.cc/VA5S-8S5B] (discussing the Skidrow Scene group's complaint that CODEX Scene group had copied Skidrow's work in release of a crack of Trials Fusion). A fascinating aspect of attribution has been the development of cracktros (animated crack intros). *See, e.g.*, CRACKTROS, http://www.cracktros.org [https://perma.cc/XFJ6-CC5Z] (featuring an archive of cracktros).

45. Moshirnia, *supra* note 6, at 26–32.

46. Reloaded, a cracking group, puts the following message in its releases:

> We, RELOADED members, would like You - Dear User, to know the following:
>
> 1. We do not want You to spread our releases outside of The Scene.
> 2. Do NOT contact technical support if You have some issues with our releases.
> 3. We hate Peer2peer networks (torrents, bearshare, …), rapidshare etc.
> 4. We do not make our releases for YOU - Mr. P2P user, we make them for The Sceners, who contribute something - unlike YOU.
> 5. To all people who repack our cracks/keygens with spyware/malware: F*** YOU
> 6. We do NOT fix game bugs, unless we can.
>
> And the most important:
>
> 7. IF YOU LIKE THIS OR ANY OTHER GAME: BUY IT!!! (Yes, we mean it)

Id. at 17.

impatient,[47] complain about glitched, buggy, or slow-running cracks,[48] and fail to contribute (in praise, bandwidth, or money) to a community.[49]

3. Transmission Method: BitTorrent

Cracked software is largely provided to the public by torrent.[50] BitTorrent is a decentralized peer-to-peer (P2P) sharing protocol, which allows for the rapid delivery of files to many users simultaneously.[51] A file distributed by torrent is segmented into small pieces, or "bits." These may be downloaded out of sequence, reducing bottlenecks if distributing users go offline.[52] The initial file is "seeded" by a user, and leeched by other users seeking to download the file in a cloud or swarm.[53] Users running a BitTorrent client may download any bit from any other user who has that bit and is currently leeching or seeding that target file.[54] Torrent trackers are servers that help coordinate the transmission of files.[55] Torrent sites index content, typically noting the title, genre, seed/leech numbers, and occasionally a user-generated rating of the torrent.

---

47. *See, e.g.*, *id.* (collecting user comments on the Skidrow webpage for Serious Sam III: "WHERE IS THE CRACK??? The game was released 1 week ago… so SKIDROW release the crack we need to play this game (:"; "where i can get the crack? it's 5 days after the game was on sale. :/"; "I couldnt w8 for the crack to release so i bought it." And site warnings: "PS: No ETA & do not ask. It will be out as soon as FIFA 13 is cracked. PLEASE BE PATIENT ! Stop with your rude & amatuer comments, we will not tolerate this kind of attitude and abusers will be permanent banned." [sic]).

48. *Id.*

49. *See id.*; *see also* Ernesto Van der Sar, *Scene Group Asks for Bitcoin Donations, Gets $0*, TORRENTFREAK (July 3, 2016), https://torrentfreak.com/scene-group-donations-160703 [https://perma.cc/6J3C-FFN6] (noting that scene group spamTV received nothing after soliciting bitcoin donations to pay for their "hobby").

50. *See* Ernesto Van der Sar, *Top 10 Most Popular Torrent Sites in 2016*, TORRENTFREAK (June 2, 2016), https://torrentfreak.com/top-10-most-popular-torrent-sites-of-2016-160102 [https://perma.cc/QZ2S-HKYZ] (collecting Alexa ranks of top torrent sites).

51. Mark F. Schultz, *Fear and Norms and Rock & Roll: What Jambands Can Teach Us About Persuading People To Obey Copyright Law*, 21 BERKELEY TECH. L.J. 651, 686–88 (2006).

52. *Id.*

53. *Id.*

54. Okechukwu Benjamin Vincents, *When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. The EC Personal Data Directive*, 16 INT'L J.L. & INFO. TECH. 270, 274 (2007).

55. Trackers are not strictly necessary due to the distributed hash table (DHT) method, which allows for "trackerless" torrents. *See* Mike Freedman, *P2P Systems and Distributed Hash Tables*, http://www.cs.princeton.edu/courses/archive/spr11/cos461/docs/lec22-dhts.pdf [https://perma.cc/6MPC-2EXX] (providing overview of P2P application history). However, trackers are still employed for user convenience. Ernesto Van der Sar, *BitTorrent's Future: DHT, PEX and Magnet Links Explained*, LIFEHACKER (Nov. 24, 2009), http://lifehacker.com/5411311/bittorrents-future-dht-pex-and-magnet-links-explained [https://perma.cc/8BAT-W57N] (providing a useful primer on systems used on trackers and torrent sites).

BitTorrent has two basic features conducive to piracy: speed and perceived safety. First, the protocol lowers bandwidth and hardware resource requirements of the original seeder.[56] As more users in a swarm gain bits, each user may begin distributing those bits, growing aggregate bandwidth and proliferating files without burdening the original provider. This lowers the cost of distribution, as the original file provider or seed is mirrored by users who have completed the download and are, in turn, providing another source for the copy as well as by users who are in the process of downloading the file and are simultaneously uploading selected pieces.

Second, pirates often use large seed clouds as a means of determining if the target file is safe.[57] This logic assumes that the target file is neither a decoy nor obviously infectious, otherwise the community would have already flagged and removed it. The safety and speed advantages of large seeding groups also provide an incentive for robust, popular pirating networks, because a greater number of users leeching a file will actually increase the speed of download and the likelihood of successful download.

B. Piracy Is Rampant but Hard Numbers Are Scarce

Piracy numbers are notoriously difficult to glean, an unsurprising fact in light of the clandestine and anonymous nature of the activity. Estimates of piracy rates range from 15% of all users to up to 90% for individual title downloads. Piracy numbers for individual PC titles may be in the millions. TorrentFreak, "a weblog dedicated to BitTorrent news, publishes an annual list of the most frequently downloaded games on BitTorrent, compiled from several sources including public torrent trackers."[58]

> In 2011, the top five most pirated PC games—*Crysis 2*, *Call of Duty: Modern Warfare 3*, *Battlefield 3*, *FIFA 12*, and *Portal 2*—each had more than three million estimated downloads; *Crysis 2* reached nearly four million. . . . These numbers were in line with estimates for 2010 (five PC games with three million downloads) and represented an increase over estimates for 2009, where only two PC games were downloaded more than three million times.[59]

---

56. *See generally* Moshirnia, *supra* note 6.

57. *How To Safely Download Torrents*, WIKIHOW, http://www.wikihow.com/Safely-Download-Torrents [https://perma.cc/Q8QA-94D3] ("Look for torrents with lots of seeders. Lots of seeders generally means that the torrent is free from viruses. . . . Check the comments before downloading. This isn't a bullet-proof solution, but the comments section of the torrent can help you determine if it contains any viruses. If there are a lot of comments but nothing about a potential virus, then chances are better that it doesn't have one. If lots of comments talk about viruses, you probably want to avoid that torrent."). Of course, this advice is most relevant when the malware target file is fairly obvious. Greater concerns develop when the malware is not readily detectible, either by covert action (as opposed to ransomware, which must make itself known) or by antivirus software.

58. Moshirnia, *supra* note 6, at 23.

59. *Id.* (citing Ernesto Van der Sar, *Call of Duty: Black Ops Most Pirated Game of 2010*, TORRENTFREAK (Dec. 28, 2010), http://torrentfreak.com/call-of-duty-black-ops-most-pirated-game-of-2010-101228 [https://perma.cc/Z9G7-GU57]; Ernesto Van der Sar, *Modern Warfare*

Industry estimates are hardly uniform, in part because some firms do not separate video game piracy from software piracy. A survey by the BSA, a global advocacy group for software developers, found that 39% of all software installed is not properly licensed.[60] Scholars have attempted to develop multivariate models to predict overall piracy rates in different countries based on total net users, overall wealth, and wealth inequality among other factors.[61] Piracy rates also differ by platform. It is well accepted that in the context of mobile apps, Android suffers a much higher piracy rate than iOS, with piracy rates ranging from 90% to 95%.[62]

There is an ongoing debate as to whether the overall piracy rate has decreased.[63] Regardless of trends at the margins, piracy remains a big business. In 2015, a security firm estimated that there were approximately 31,000 pirated game releases.[64] Industry-wide estimates frequently cite a 93% piracy rate, in part because this is the ratio of non-paying users in free-to-play games.[65] Systematic study of BitTorrent traffic casts doubts on the highest piracy estimates, but still shows significant activity, tracking 12.7 million downloads over a three-month period.[66]

---

2 Most Pirated Game of 2009, TORRENTFREAK (Dec. 27, 2009), http://torrentfreak.com/the-most-pirated-games-of-2009-091227 [https://perma.cc/MM7X-BG8X]).

60. BSA, SEIZING OPPORTUNITY THROUGH LICENSE COMPLIANCE: BSA GLOBAL SOFTWARE STUDY 2 (2016), http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf [https://perma.cc/GL9R-VVU9].

61. *See, e.g.*, Alex C. Kigerl, *Infringing Nations: Predicting Software Piracy Rates, BitTorrent Tracker Hosting, and P2P File Sharing Client Downloads Between Countries*, 7 INT'L J. CYBER CRIMINOLOGY 62, 63 (2013).

62. *See* Joel Lee, *Piracy on Android: How Bad Is It Really?*, MAKEUSEOF (Feb. 4, 2015), http://www.makeuseof.com/tag/piracy-android-how-bad-is-it-really [https://perma.cc/JX5H-SCCY] (noting range of piracy estimates); *see also* Chris Davies, *95% Andriod Game Piracy Experience Highlights App Theft Challenge*, SLASHGEAR (May 15, 2013), https://www.slashgear.com/95-android-game-piracy-experience-highlights-app-theft-challenge-15282064 [https://perma.cc/QM2N-GYRB] (noting differential between iOS and Android piracy rates).

63. *Compare* Robert Steele, *If You Think Piracy Is Decreasing, You Haven't Looked at the Data . . .* , DIGITAL MUSIC NEWS (July 16, 2015), http://www.digitalmusicnews.com/2015/07/16/if-you-think-piracy-is-decreasing-you-havent-looked-at-the-data-2 [https://perma.cc/64G4-G6XT], *with* Ernesto Van der Sar, *Pirates Switch from Torrents to Streaming and Download Sites*, TORRENTFREAK (Apr. 26, 2016), https://torrentfreak.com/pirates-switch-from-torrents-to-streaming-and-download-sites-160426 [https://perma.cc/6YBY-HLY8] (noting that torrent traffic is down but that other web based piracy sources are increasing in popularity).

64. ARXAN, 4TH ANNUAL STATE OF APPLICATION SECURITY REPORT: A LOOK INSIDE THE UNIVERSE OF PIRATED SOFTWARE AND DIGITAL ASSETS 2 (2015), https://www.arxan.com/wp-content/uploads/2015/06/State-of-Application-Security-Report-Vol-4-2015.pdf [https://perma.cc/X246-7M2Z].

65. Dan Pearson, *Guillemot: As Many PC Players Pay for F2P as Boxed Product*, GAMESINDUSTRY.BIZ (Aug. 22, 2012), http://www.gamesindustry.biz/articles/2012-08-22-guillemot-as-many-pc-players-pay-for-f2p-as-boxed-product [https://perma.cc/PY4N-BTYP] (explaining how Ubisoft CEO Yves Guillemot noted that only 5% to 7% of players pay for boxed product or for free-to-play software).

66. Anders Drachen & Robert W.D. Veitch, *Patterns in the Distribution of Digital Games via BitTorrent*, 5 INT'L. J. ADVANCED MEDIA & COMM. 80, 80 (2013); *see also* Ian Birnbaum, *The State of PC Piracy in 2016*, PC GAMER (Aug. 10, 2016), http://www.pcgamer.com/the-

While industry-wide rates may be dubious,[67] there are credible reports of 90% piracy rates for individual titles. The first title to experience a sort of BitTorrent hyper-piracy was *Spore*, though many commentators have blamed that outcome on user response to DRM. However, there are numerous hyper-pirated titles that had several characteristics that would theoretically reduce their attractiveness to pirates.

The release of *Spore*, developed by Maxis and published by Electronic Arts (EA), in 2008 was met with widespread criticism of the game's DRM.[68] The game utilized SecuROM, which required online authentication when the game was first installed and whenever online access was used. In an effort to prevent sharing of copies, the game required an install key and could only be installed on three computers, although this was later increased to five.[69] This would also naturally limit secondhand sales of the game. As a result of this, users flooded review sites with one-star reviews,[70] with Amazon recording more than 2000 one-star reviews out of 2216 reviews.[71] The game inspired a class action lawsuit on the basis that purchasers were not properly told of SecuRom.[72] At least one Maxis employee noted that EA had "screwed up" in the handling of DRM and the game's release.[73]

---

state-of-pc-piracy-in-2016 [https://perma.cc/YBQ9-XBJR] (noting that 93% piracy rate is likely an exaggeration and suggesting that "30-35% of all PC gamers pirate games, but the volume of games they pirate is astronomically higher than expected"); Matt Ployhar, *Gaming Piracy - Separating Fact from Fiction*, INTEL DEVELOPER ZONE (Sept. 22, 2012), https://software.intel.com/en-us/blogs/2012/09/22/gaming-piracy-separating-fact-from-fiction [https://perma.cc/B55F-NUXN] (arguing that piracy is exaggerated and at most would constitute 30% of steam users).

67. Ployhar, *supra* note 66 (arguing that false torrents, multiple downloads, and hacks downloaded by legitimate purchasers artificially inflate piracy numbers).

68. Erick Schonfeld, *Spore and the Great DRM Backlash*, WASH. POST (Sept. 14, 2008, 7:10 AM), http://www.washingtonpost.com/wp-dyn/content/article/2008/09/14/AR2008091400885.html [https://perma.cc/R69D-3Z7A] (concluding "that binding products with digital rights management (DRM) restrictions hurts more than it helps" in light of consumer backlash to DRM in the game).

69. Ben Kuchera, *EA Relents, Changes Spore DRM. Too Little, Too Late?*, ARS TECHNICA (Sept. 19, 2008, 10:40 AM), http://arstechnica.com/gaming/2008/09/ea-relents-changes-spore-drm-too-little-too-late [https://perma.cc/65BF-RMTR].

70. Matthew Humphries, *Amazon Customers Award Spore One Star for DRM*, GEEK.COM (Sept. 9, 2008, 4:00 AM), https://www.geek.com/games/amazon-customers-award-spore-one-star-for-drm-578338 [https://perma.cc/9Z63-24R7].

71. Frank Caron, *Amazon Temporarily Gags Spore Critics, Deletes and Restores All Customer Reviews*, ARS TECHNICA (Sept. 12, 2008, 4:21 PM), https://arstechnica.com/gaming/2008/09/amazon-gags-spore-critics-deletes-all-customer-reviews [https://perma.cc/SZY4-XQFJ].

72. Complaint at 3, Thomas v. Elec. Arts, Inc., No. 5:08-cv-04421-PVT (N.D. Cal. 2008) (alleging violations of California Consumer Legal Remedies Act, California's Unfair Competition Law, and trespass to chattel).

73. *Former Maxis Man: Spore DRM Is a Screw Up*, SPONG (Sept. 9, 2008), http://spong.com/article/16171/Former-Maxis-Man-Spore-DRM-is-a-Screw-Up [https://perma.cc/25NL-WSP6].

The game was also the highest pirated game of that year (even though it was released comparatively late in the year, September), with an estimated 1.7 million illegal downloads.[74] While piracy of an anticipated game was not unexpected, several commentators attributed the enhanced downloading of the game, "exceeding the download rate of any other pirated game in history,"[75] to the presence of onerous DRM.[76] Downloaders of the file similarly pointed to DRM: "By downloading this torrent, you are doing the right thing. You are letting [Electronic Arts] know that people won't stand for their ridiculously draconian 'DRM' viruses."[77] As the cracked version was DRM-free, it could be considered superior to a legitimate copy.[78] Some commentators suggested, however, that DRM was a red herring, because "the record number of Spore downloads is attributable to the game's unprecedented pre-release popularity, the year-over-year upturn in industry sales, the huge overall upticks in numbers of people video gaming, the increase in numbers of broadband users, the overall increase in torrent usage, and so on."[79]

The theory that piracy is driven solely by anti-DRM and anticorporate consumer response is undercut by the piracy of DRM-free independent titles.[80]

> In the case of *World Of Goo* by 2D Boy, developers initially reported a piracy rate of 90% based on the number of IPs logging high scores on the game's servers. When the accuracy of this figure was questioned, the developers conducted a thorough analysis involving numerous factors that might have served to inflate their initial conclusion, such as multiple legitimate installs. This secondary analysis still yielded a very high piracy rate of 82%.[81]

---

74. Ernesto Van der Sar, *Top 10 Most Pirated Games of 2008*, TORRENTFREAK (Dec. 4, 2008), https://torrentfreak.com/top-10-most-pirated-games-of-2008-081204 [https://perma.cc/4YBD-RXKA].

75. Ernesto Van der Sar, *Spore: Most Pirated Game Ever Thanks to DRM*, TORRENTFREAK (Sept. 13, 2008), https://torrentfreak.com/spore-most-pirated-game-ever-thanks-to-drm-080913 [https://perma.cc/5NHF-95EY].

76. *Id.*

77. Andy Greenberg & Mary Jane Irwin, *Spore's Piracy Problem*, FORBES (Sept. 12, 2008, 10:00 AM), http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html [https://perma.cc/HR5L-BVNS].

78. *See* Schonfeld, *supra* note 68.

79. Matt Peckham, *Spore Tops Piracy Charts, But Don't Blame DRM*, PCWORLD (Dec. 11, 2008, 5:08 AM), http://www.pcworld.com/article/155315/spore_piracy_drm.html [https://perma.cc/GT3T-Z6CM].

80. Moshirnia, *supra* note 6, at 42.

81. *Id.*; *90%*, 2D BOY (Nov. 13, 2008, 11:51 PM), http://2dboy.com/2008/11/13/90 [https://perma.cc/889M-YRJL].

> 1. [B]ased on the number of unique IPs and unique player IDs, we found that on average, there are 1.3 unique IP addresses per player (there is 1 player id for each profile created on any installation that submits scores to our server)[.]
> 76% of players have contacted the server from 1 IP, 13% from 2 IPs, 5% from 3 IPs, 3% from 4 IPs, 1% from 5 IPs, 1% from 6 IPs, 1% from more than 6 [IPs.]
> [T]his tells us that the dynamic IP issue is a relatively small factor in this calculation.

Similarly, the developers of *Game Dev Tycoon* reported a 93.6% piracy rate.[82] Commentators noted that these high piracy numbers were especially disheartening in light of the releases' characteristics: an independent developer, a cheap price, and a lack of DRM.[83]

C. Calculating the Cost: Lost Sales and Potential Advertising Benefits

Various industry groups have offered different damages attributable to video game piracy. CESA calculated that piracy relating to portable consoles in 2004–09 cost the industry $41.5 billion.[84] Tru Optic estimates that piracy cost the industry

---

> 2. [W]e also looked at how many players IDs were created (rather than used) from each IP address. [G]iven that the vast majority of player IDs are associated with only a single IP, this is a fairly accurate measure of how many profiles the average user created. [O]n average, a player has 1.15 profiles per installation.
>
> [W]hen we take the total number of player IDs (which is smaller than the number of unique IPs from which leaderboard entries came) and divide it by 1.15 (the average number of profiles per installation) the number of estimated unique installations drops by about 35% as compared to the estimate based on unique IPs. [L]et us further say that the average user installs the game on 1.25 computers with different IPs (i.e. not behind the same router), which i think is a high estimate [*sic*]. [T]hat lowers the estimated unique installations by another 20%. [A]fter factoring both of these in, the piracy rate would still be 82%, and we should keep in mind that this number doesn't include those who never opted to submit scores to the leaderboard (it's an option that's off by default). [S]o while it's possible that the actual piracy rate is lower than 90%, it's unlikely that it's significantly lower. 2d boy hopes this satisfies the more rigorous number crunchers out there.

Moshirnia, supra note 6, at 23 n.85.

82. Patrick Klug, *What Happens When Pirates Play a Game Development Simulator and Then Go Bankrupt Because of Piracy?*, GREENHEART GAMES (Apr. 29, 2013), http://www.greenheartgames.com/2013/04/29/what-happens-when-pirates-play-a-game-development-simulator-and-then-go-bankrupt-because-of-piracy [https://perma.cc/7ZXD-L4A4] (calculating piracy rate based on usage-data and distinct IDs).

83. Moshirnia, *supra* note 6, at 43–46 (noting that high piracy rates may conflict with stated piracy justifications centering on DRM, price, and developer need); Ian Birnbaum, *The State of PC Piracy in 2016*, PCGAMER (Aug. 10, 2016), http://www.pcgamer.com/the-state-of-pc-piracy-in-2016 [https://perma.cc/ZL2E-D9U3].

84. Eric Caoili, *CESA: Portable Piracy Cost Game Industry $41.5 Billion*, GAMASUTRA (June 7, 2010), http://www.gamasutra.com/view/news/119789/CESA_Portable_Piracy_Cost_Game_Industry_415_Billion.php [https://perma.cc/U8JJ-2FDA] (noting that the U.S. has the most servers hosting piracy sites).

approximately $74 billion in 2014.[85] At the same time, recent studies have undermined proposed losses caused by film[86] and music piracy.[87]

The true scope of economic damage caused by video game piracy is difficult to calculate. Even ignoring the proper cost to ascribe to lost sales (assume, for a moment, the veracity of "the dubious proposition that *all* pirates would not have paid *any* amount for the games they pirate"[88]) piracy still drains developer resources as pirates consume server and support provisions.[89] For example, users employing cracked versions of games routinely seek technical help from developers, either by phone or by posting their problems in developer forums.[90]

This is not to say that there are no possible advantages of piracy for the copyright holder. Studies have shown that pirating users are likely to purchase more legal

---

85. ARXAN, *supra* note 64; ZhugeEX, *Video Game Piracy on the Rise, Will Cost the Industry As Much As It Makes*, GEARNUKE (Aug. 20, 2015), http://gearnuke.com/video-game-piracy-rise-will-cost-industry-much-makes [https://perma.cc/4RWC-LCWY].

86. Christian Peukert, Jörg Claussen & Tobias Kretschmer, *Piracy and Box Office Movie Revenues: Evidence from Megaupload*, 52 INT'L J. INDUS. ORG. 188, 189–90 (2017) (noting that shutdown of Megaupload disrupted movie piracy but did not boost movie revenues).

87. BART CAMMAERTS, ROBIN MANSELL & BINCHUN MENG, COPYRIGHT & CREATION: A CASE FOR PROMOTING INCLUSIVE ONLINE SHARING 5 (London Sch. Of Econ. Media Policy Project, Media Policy Brief 9, 2013), http://www.lse.ac.uk/media@lse/documents/MPP/LSE-MPP-Policy-Brief-9-Copyright-and-Creation.pdf [https://perma.cc/GAH5-XHCP] (noting increasing digital revenues in spite of pirated-music availability and arguing against a three strikes internet ban).

88. Moshirnia, *supra* note 6, at 19.

89. Miles Jacobson, *Op-Ed: Android Piracy Is Huge Problem for Game Devs*, WIRED (May 3, 2012, 6:30 AM), http://www.wired.com/gamelife/2012/05/wired-uk-android-game-piracy [https://perma.cc/PD8U-RBJP] ("The thing is, people who make games do lose from piracy. We lose from the small percent of pirated copies that are lost sales, but we also have direct costs, both financial and opportunity costs, which can be attributed to every version, pirated or not. Whether that be server costs (for skin downloads), support costs (believe it or not, pirates still ask for customer support) and wasted time trying to deal with it all."); *see also* Comment by Nicholas, PORTAL: PRELUDE (Oct. 13, 2008), http://www.portalprelude.com/2008/10/about-pirating-and-stuff.php [https://perma.cc/39AE-Y7UN] (statement of developer denying repeated requests for technical support for pirates attempting to use the Prelude mod on a pirated copy of Portal) ("Seriously guys, stop sending us emails because you can't install the game, because you can't launch the game, or because you have weird errors everywhere. We're not going to help you make the mod work on pirated versions of Portal or without Steam. This mod needs an original and legit Portal because it also uses some of the content of Half-Life 2 that extends Portal. Of course, this content doesn't seem to be included in the pirated version of Portal." (emphasis omitted)). For more on modding, see Andrew V. Moshirnia & Anthony C. Walker, *Reciprocal Innovation in Modding Communities as a Means of Increasing Cultural Diversity and Historical Accuracy in Video Games* 362 (Situated Play, Proceedings of DiGRA 2007 Conference, 2007), http://www.digra.org/dl/db/07311.28264.pdf [https://perma.cc/V8WM-PQEG]; Note, *Spare the Mod: In Support of Total-Conversion Modified Video Games*, 125 HARV. L. REV. 789 (2012); David Kushner, *It's a Mod, Mod World*, IEEE SPECTRUM (Feb. 1, 2003, 5:00), http://spectrum.ieee.org/consumer-electronics/gaming/its-a-mod-mod-world [https://perma.cc/L67T-4XP2].

90. Moshirnia, *supra* note 6, at 20–21.

games.[91] A widespread claim in the pirating community is that users merely pirate to demo software.[92] Scene releases often include the exhortation that if users enjoy the game, they should buy it. For example, the defunct Scene group LineZer0 a/k/a Lz0 noted that,

> Our releases are made to make sure that the end-user is able to fully test a title before going into a purchase as well as give the end-user an opportunity to make backup copies of titles he or she already owns. . . . Please do respect our stance on this and make sure that you buy the required licenses upon deciding to buy the product. Respect the software authors that have put time, money and effort into creating the title you now have in your hand.[93]

Thus, a satisfied pirate may turn into a satisfied legitimate consumer.

Members of the entertainment industry have commented on the ability of piracy to raise the "buzz" for a product and signal overall market interest.[94] The overall

---

91. Andy, *'Worst' File-Sharing Pirates Spend 300% More on Content Than 'Honest' Consumers*, TORRENTFREAK (May 10, 2013), https://torrentfreak.com/0-more-on-content-than-honest-consumers-130510 [https://perma.cc/5SSN-3L7F]; Jason Mick, *Nearly Half of Americans Pirate Casually, But Pirates Purchase More Legal Content*, DAILYTECH (Jan. 21, 2013), http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm [https://perma.cc/5SSN-3L7F].

92. Moshirnia, *supra* note 6, at 28; *I Used Internet Piracy To Try Before Buying*, STUFF (Dec. 4, 2015, 5:00 AM), http://www.stuff.co.nz/stuff-nation/assignments/is-piracy-ever-justified/11521827/I-used-internet-piracy-to-try-before-buying [https://perma.cc/25WS-UPNQ].

93. Andy, *Huge Software Piracy Group Calls It Quits After 30,000 Cracked Titles*, TORRENTFREAK (Oct. 15, 2013), https://torrentfreak.com/huge-software-piracy-groups-call-it-quits-after-30000-cracked-titles-131015 [https://perma.cc/73GH-382V] (quoting release language from Lz0).

94. Caitlin Dewey, *'Game of Thrones' Exec Says Piracy Is 'Better than an Emmy.' He Has a Point*, WASH. POST (Aug. 9, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/08/09/game-of-thrones-exec-says-piracy-is-better-than-an-emmy-he-has-a-point [https://perma.cc/U27U-D3DM] ("Director David Petrarca once told a crowd in Sydney that illegal downloads help the show by generating 'buzz.' Both author George R.R. Martin and HBO programming president Michael Lombardo have called the piracy rates a compliment. And now, in perhaps the strongest endorsement of all, Jeff Bewkes -- the CEO of Time Warner, which owns HBO -- basically bragged about illegal downloads to investors during an earnings call."); Ernesto Van der Sar, *Media Companies Track Pirated Downloads for Marketing Purposes*, TORRENTFREAK (Feb. 18, 2015), https://torrentfreak.com/media-companies-track-pirated-downloads-for-marketing-purposes-150218 [https://perma.cc/LZ8N-4FY2]. *But see* LIYE MA, ALAN L. MONTGOMERY & MICHAEL D. SMITH, THE DUAL IMPACT OF MOVIE PIRACY ON BOX-OFFICE REVENUE: CANNIBALIZATION AND PROMOTION 36 (2016) (finding that "piracy lowers box-office revenue by $1.34b per year (15%)" and that "for a small number of movies (about 3% of our sample), pre-release piracy may increase sales relative to a world where piracy coincides with release . . . . all of the movies in our sample would have higher sales if there were no piracy"); Liye Ma, Alan Montgomery & Michael D. Smith, *Piracy and Buzz*, TECH. POL'Y INST. (Feb. 24, 2016), https://techpolicyinstitute.org/2016/02/24/piracy-and-buzz [https://perma.cc/442H-ZWP9] ("[A]lthough the promotional effect of piracy did increase

impact of this is disputed, however, as the cannibalization of legitimate sales may outweigh any benefit attributable to wider publicity. There also is the possibility that a satisfied pirate user may help publicize a game by praising it in forums. Thus, while a pirate may not have purchased a copy, he may motivate others to purchase legitimate copies.

D. Current Efforts To Combat Piracy: Pursuing Torrent Site Shutdowns

As detailed above, the main players in the piracy pipeline are DRM cracking groups, leakers that distribute content via torrent, and end downloaders. To date, legal focus has been trained almost exclusively against torrent sites, while DRM has been used to deter crackers and end downloaders. This Part details the various approaches adopted with respect to these actors.

The government has occasionally launched campaigns against Scene groups, with success at taking down specific groups but having little impact overall. The best-known anti-Warez operations are Operation Buccaneer, a massive operation in 2000 targeting the Drink Or Die group,[95] and Operation Fastlink, a 2004 operation targeting FairLight.[96] Commentators have noted that while these operations successfully secured felony convictions, the overall Warez Scene was largely unaffected. The entertainment industry has been disappointed by the results of other campaigns, which have resulted in only probation or fairly light charges.[97]

The video game industry has largely avoided suits against individual pirates, in contrast to the litigation approach of the film and music industries, although developers have occasionally mentioned potential lawsuits. For example, CD Projekt, the developer of *Witcher II*, released a patch removing all DRM from the game and indicated they would instead monitor torrents and sue infringing users. Widespread outcry in the gaming community eventually forced the developer to abandon legal action against pirates.[98]

---

box-office revenue by an average of 1.5 percent—the promotional impact of piracy is far outweighed by the cannibalization effect. In other words, while the pre-release piracy buzz did cause some people to pay to see the movie who wouldn't have otherwise, it caused far more people to not pay who would have otherwise.").

95. *Operation Buccaneer*, U.S. DEP'T JUST., https://web.archive.org/web/20110722172136/http://www.cybercrime.gov/ob/OBMain.htm [https://perma.cc/9KVL-LPVE].

96. Jonathan Basamanowicz & Martin Bouchard, *Overcoming the Warez Paradox: Online Piracy Groups and Situational Crime Prevention*, 3 POL'Y INTERNET 1, 7–11 (2012).

97. Andy, *Massive Piracy Case Ends in Disappointment for Hollywood*, TORRENTFREAK (July 25, 2015), https://torrentfreak.com/massive-piracy-case-ends-in-disappointment-for-hollywood-150725 [https://perma.cc/6H5V-43PH] (defendant facing copyright infringement charges relating to more than 2200 movies sentenced to probation); David Kravets, *Final Guilty Plea Wraps Up Federal "Warez" Crackdown*, WIRED (Feb. 2, 2009, 3:10 PM), https://www.wired.com/2009/02/connecticut-cou [https://perma.cc/F4BY-4RBV] (noting that eighteen defendants prosecuted by United States in two anti-Warez operations "Operation Safehaven" and "Operation Higher Education" received probation).

98. Moshirnia, *supra* note 6, at 26–32; John Walker, *The Wrong Way To Stop Video Game Piracy*, KOTAKU (Dec. 20, 2011), http://kotaku.com/5869908/the-wrong-way-to-stop-video-game-piracy [https://perma.cc/6GPW-MMCS] (originally posted on Rock, Paper Shotgun but original post is no longer available).

But there has been considerable pressure brought by the wider entertainment industry and the United States Trade Representative (USTR) to reduce piracy. The decade-old approach taken by the government and wider entertainment industry with regard to copyright infringing trackers has been to launch sudden takedowns or otherwise shutter sites through lawsuits. These have been accomplished through domain seizure, arrests of operators, and the threat of future litigation. The main takedowns involved Suprnova in 2004,[99] Lokitorrent in 2005,[100] Torrentspy in 2008,[101] Mininova in 2009,[102] BTjunkie in 2012,[103] and YIFY/YTS in 2015.[104] The most recent of these was the dual takedown of KickassTorrents and Torrentz.eu.[105]

In December 2016, the USTR released its report on so-called "Notorious Markets."[106] The report was an effort to enlist foreign governments in assisting the

---

99. Ernesto Van der Sar, *Suprnova.org: Two Years Since the Shutdown*, TORRENTFREAK (Dec. 19, 2006), https://torrentfreak.com/suprnovaorg-two-years-since-the-shutdown [https://perma.cc/5AP3-KA2S].

100. Eric Bangeman, *Judge Orders Torrent Site To Close, Release Logs*, ARS TECHNICA (Feb. 10, 2005, 11:15 PM), http://arstechnica.com/uncategorized/2005/02/4606-2 [https://perma.cc/G8UV-NXMX] (noting the move would force the "trade movies and tv shows . . . to move further underground"); Brad King, *LokiTorrent Shut Down*, MIT TECH. REV. (Feb. 10, 2005), https://www.technologyreview.com/s/403710/lokitorrent-shut-down [https://perma.cc/Y8C7-95GY].

101. Eric Bangeman, *TorrentSpy's Closure a Win for MPAA; War Far from Over*, ARS TECHNICA (Mar. 28, 2008, 2:23 PM), http://arstechnica.com/tech-policy/2008/03/torrentspys-closure-a-win-for-mpaa-war-far-from-over [https://perma.cc/TR8R-3R27]; Ernesto Van der Sar, *TorrentSpy, One Year After the Shutdown*, TORRENTFREAK (Mar. 24, 2009), https://torrentfreak.com/torrentspy-one-year-after-the-shutdown-090324 [https://perma.cc/N944-YCUW].

102. Ernesto Van der Sar, *Mininova Traffic Plummets After Going 'Legal,'* TORRENTFREAK (Dec. 5, 2009), https://torrentfreak.com/mininova-traffic-plummets-after-going-legal-091205 [https://perma.cc/PZ8W-Z6VG] (noting that ISP's felt Mininova's partial shutdown has had no noticeable effect on traffic volumes: "I didn't notice any reduction in [torrent] traffic when The Pirate Bay went down. It's hard to see how there'd be any significant change from Mininova's withdrawal.").

103. Daniel Ionescu, *Top Torrent Site BTjunkie Shuts Voluntarily*, PCWORLD (Feb. 6, 2012 6:35 AM), http://www.pcworld.com/article/249330/top_torrent_site_btjunkie_shuts_voluntarily.html [https://perma.cc/L9QM-G5JA]; Ernesto Van der Sar, *The Best BTjunkie Alternatives*, TORRENTFREAK (Feb. 6, 2012), https://torrentfreak.com/btjunkie-alternatives-120206 [https://perma.cc/3KSN-9XAA].

104. Many smaller trackers are also defunct. Ernesto Van der Sar, *Torrentz Gone, KAT Down, Are Torrent Giants Doomed To Fall?*, TORRENTFREAK (Aug. 6, 2016), https://torrentfreak.com/torrentz-gone-kat-down-are-torrent-giants-doomed-to-fall-160806 [https://perma.cc/KC6M-H3AR].

105. Ernesto Van der Sar, *Top Torrent Sites See Traffic Surge After 'Shutdowns,'* TORRENTFREAK (Sept. 3, 2016), https://torrentfreak.com/top-torrent-sites-see-traffic-surge-shutdowns-160903 [https://perma.cc/KM6U-3A29]. These shutdowns did little to stem torrent flow, however. Instead, the shutdowns caused a migration to other torrent sites, such as The Pirate Bay, which saw a 67% spike in users following the shutdowns. The concern is that displaced users will settle into sites with less robust reputational networks. Unsurprisingly, it is the most popular torrent sites that attract the greatest attention from content owners.

106. OFFICE OF THE U.S. TRADE REPRESENTATIVE, 2016 OUT-OF-CYCLE REVIEW OF

take-down of sites that facilitate copyright infringement. Unsurprisingly, the report touted the closure of KickassTorrents, following intervention of U.S. law enforcement, and the shutdown of Torrentz.eu.[107] The report went on to list numerous torrent sites, including: ExtraTorrent,[108] RARBG.to,[109] RuTracker,[110] and The Pirate Bay. For each of these sites, the USTR noted that the inclusion of the tracker was due to commenters from the book, film, and movie industries. Tellingly, neither video games nor even software generally is addressed; the sites are criticized for "illegal downloads of movies, television, music, and other copyrighted content."[111]

II. GAME VIRAL VECTORS POSE SIGNIFICANT YET NEGLECTED THREATS

As detailed in the previous Part, the discussion of video game piracy to date has centered on the prevalence and cost of the practice, and on whether the use of DRM deters or spurs the act of pirating.[112] It is unsurprising that market actors would frame the problem in economic terms. Indeed, lost profits and other economic drains due to software piracy are lamentable.

But this singular focus does not consider the public. Piracy-aided malware distribution poses a significant yet neglected threat to all users.[113] Video game piracy presents a perfect environment for malware infection: unverified executable files downloaded to powerful computers with disabled virus protection. However, to the extent that malware is discussed within the industry, it is with an eye towards persuading pirates that the act of pirating is simply not worth the risk of infection.[114] This approach is problematic, as it incorrectly cabins the harm to the bad actor (you pirate,

---

NOTORIOUS MARKETS (2016), https://ustr.gov/sites/default/files/2016-Out-of-Cycle-Review-Notorious-Markets.pdf [https://perma.cc/DHL4-BHSW].

107. *Id.* at 3.

108. *Id.* at 8 (hosted in Ukraine).

109. *Id.* at 12 (formerly a Bulgarian tracker, now located in Bosnia and Herzegovina).

110. *Id.* (currently hosted and operated from Russia).

111. *Id.* at 14.

112. Brett Makedonski, *Super Meat Boy Dev Says DRM Is More Dangerous than Piracy*, DESTRUCTOID (Mar. 19, 2013), https://www.destructoid.com/super-meat-boy-dev-says-drm-is-more-dangerous-than-piracy-249054.phtml [https://perma.cc/EEW7-B9H5].

113. *See* JOHN F. GANTZ, VICTOR LIM, STEPHEN MINTON, LARS SMITH, PAVEL SOPER & THOMAS VAVRA, INT'L DATA CORP., UNLICENSED SOFTWARE AND CYBERSECURITY THREATS 3–4 (2015), http://globalstudy.bsa.org/2013/Malware/study_malware_en.pdf [https://perma.cc/2DGV-2YZN] (noting unlicensed software use is a strong predictor (R-squared = .62) of malware encounters).

114. *See* BUS. SOFTWARE ALL., SOFTWARE PIRACY ON THE INTERNET: A THREAT TO YOUR SECURITY (2009), http://portal.bsa.org/internetreport2009/2009internetpiracyreport.pdf [https://perma.cc/9VPX-H6R2]; *The Importance of Playing It Safe*, MICROSOFT CORP. BLOG (Mar. 5, 2013), https://blogs.microsoft.com/on-the-issues/2013/03/05/the-importance-of-playing-it-safe [https://perma.cc/4XB7-DT2E] (reporting on risks of downloading software). *But see* ERNST & YOUNG LLP & FED'N OF INDIAN CHAMBER OF COMMERCE AND INDUS., COUNTERFEITING, PIRACY AND SMUGGLING: GROWING THREAT TO NATIONAL SECURITY (2013), http://www.ey.com/Publication/vwLUAssets/EY-Government-and-Public-Sector-Growing-threat-to-national-security-an-analysis/$File/EY-Counterfeiting-piracy-and-smuggling-Growing-threat-to-national-security.pdf [https://perma.cc/77R6-5RL7] (linking counterfeiting,

you pay!), thereby diminishing the credibility of the threat and distracting from the national security risks inherent to the proliferation of malware. It is foolish to believe that only pirating users will feel the consequences of rampant infection. This is especially true in light of the fact that botnets have been used repeatedly to suspend internet service.[115]

Piracy-related malware is not simply a problem for pirates. The presence of these infected, interconnected machines heightens the malware risk for all users, including users who do not engage in pirating activity. Botnets are frequently used to distribute malware-laden spam.[116] A compromised machine may generate forged emails that appear to be from trusted senders, more readily duping other users into wiring money, downloading infected attachments, or disclosing sensitive information.[117] This is typified by the "stranded traveler" hack, in which a hacker gains access to a victim's contact list and then queries those contacts for money.[118]

The public may be familiar with cataclysmic malware due to its depiction in popular culture, but the reality is less eye catching and frequently overlooked. This Part details the costs of malware generally and types of malware, the paramount danger of botnets, the exceptional vulnerabilities of video game pirates to malware, and case studies of video game malware.

A. General Harms of Malware

Malware is ubiquitous and costly, posing a significant danger. Malware contains several categories of threats, including worms, viruses, Trojans, spyware, and ransomware.[119] A worm is a replicating code with the goal of transmission to other computers. A virus is also replicating, but it additionally damages the files of the host computer. A Trojan creates a pathway into your machine. And spyware traces user movement.

---

piracy, and smuggling to funding terrorism).

115. *See infra* Part II.B.

116. Indeed, botnets are typically rented out to other hackers for this purpose. *See* Nick Clayton, *Where To Rent a Botnet for $2 an Hour or Buy One for $700*, WALL ST. J. (Nov. 5, 2012, 9:43 AM), http://blogs.wsj.com/tech-europe/2012/11/05/where-to-rent-a-botnet-for-2-an-hour-or-buy-one-for-700 [https://perma.cc/X4NC-66EG].

117. Steve Ragan, *FTC Spam Campaign Snares Thousands of Targeted Victims*, CSO (Dec. 7, 2016, 2:37 PM), http://www.csoonline.com/article/3148148/security/ftc-spam-campaign-snares-thousands-of-targeted-victims.html [https://perma.cc/FCV6-UTKM] (noting heightened danger of targeted spam that appears to be sent from a trusted sender).

118. Elisabeth Leamy & Sally Hawkins, *'Stranded Traveler' Scam Hacks Victims' Emails, Asks Their Contacts for Money*, ABC NEWS (July 13, 2012), http://abcnews.go.com/Technology/stranded-traveler-scam-hacks-victims-emails-asks-contacts/story?id=16774896 [https://perma.cc/6FFL-TRBM].

119. *What Is the Difference: Viruses, Worms, Trojans, and Bots?*, CISCO, http://www.cisco.com/c/en/us/about/security-center/virus-differences.html [https://perma.cc/WK4Q-PFFT].

There are numerous threats to consumers arising from these programs, usually with a financially motivated goal.[120] The most common is identity theft,[121] accomplished by Trojans that record user credentials. This may be done through programs such as Trojan Dridex[122] and Pony.[123] Ransomware encrypts data on a machine and ransoms the data back to the user by way of decryption. Popular ransomware includes CryptXXX,[124] CTB-Locker,[125] and Cerber.[126] Remote Access Trojans also may expose users to blackmail or invasion of privacy through access of a user's camera.[127]

The cost of malware to consumers is not limited to losses attributable to successful infection and subsequent fraud. Consumers spend time detecting malware, repairing damage, and restoring or replacing their infected systems.[128] Consumers are estimated to spend approximately 1.5 billion hours and $22 billion dealing with malware.[129] The Play It Safe campaign, an effort by Microsoft supported by joint reports

---

120. *See* Alastair Stevenson, *Tim Cook's Case Against Android Security May Have Just Gotten a Boost*, BUS. INSIDER (July 8, 2015, 8:00 AM), http://www.businessinsider.com/android-malware-hacking-smartphone-tablet [https://perma.cc/ZR6D-5S3V] ("[H]ackers are developing nearly 5,000 new Android malware variants per day, over 50% of which are designed to steal money from their victims.").

121. DIG. CITIZENS ALL. & RISKIQ, DIGITAL BAIT: HOW CONTENT THEFT SITES AND MALWARE ARE EXPLOITED BY CYBERCRIMINALS TO HACK INTO INTERNET USERS' COMPUTERS AND PERSONAL DATA 10–11 (2015), https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0f03d298-aedf-49a5-84dc-9bf6a27d91ff.pdf [https://perma.cc/54VE-2CZZ].

122. Jai Vijayan, *Dridex Malware Now Used for Stealing Payment Card Data*, DARK READING (Apr. 8, 2016, 7:00 PM), http://www.darkreading.com/vulnerabilities---threats/dridex-malware-now-used-for-stealing-payment-card-data/d/d-id/1325056 [https://perma.cc/969C-ECFD].

123. Hasherezade, *No Money, but Pony! From a Mail to a Trojan Horse*, MALWAREBYTES LABS (Nov. 19, 2015), https://blog.malwarebytes.com/threat-analysis/2015/11/no-money-but-pony-from-a-mail-to-a-trojan-horse [https://perma.cc/UV89-XMKE].

124. Caleb Fenton, *New CryptXXX Variant Discovered*, SENTINELONE (June 27, 2016), https://sentinelone.com/blogs/new-cryptxxx-variant-discovered [https://perma.cc/8W6Y-ET6Q].

125. Editor, *The Current State of Ransomware: CTB-Locker*, SOPHOS (Dec. 31, 2015), https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker [https://perma.cc/BJV5-F67S].

126. Lawrence Abrams, *The Cerber Ransomware Not Only Encrypts Your Data but also Speaks to You*, BLEEPINGCOMPUTER (Mar. 3, 2016, 6:09 PM), https://www.bleepingcomputer.com/news/security/the-cerber-ransomware-not-only-encrypts-your-data-but-also-speaks-to-you [https://perma.cc/K5LP-3JKQ].

127. Steven Nelson, *'Tape Your Webcam': Horrifying Malware Broadcasts You to the World*, US NEWS (July 29, 2015, 9:00 PM), http://www.usnews.com/news/articles/2015/07/29/tape-your-webcam-horrifying-malware-broadcasts-you-to-the-world [https://perma.cc/JD29-S344].

128. *Software Piracy Costs Billions in Time, Money for Consumers and Businesses*, MICROSOFT (Mar. 6, 2013), https://news.microsoft.com/2013/03/06/software-piracy-costs-billions-in-time-money-for-consumers-and-businesses/#sm.00003ga8tdn9yfoaqtq21eohbx2hz#WZTouELtZ7s7Y6Bl.97 [https://perma.cc/DJ6Q-7XUX].

129. *Id.*; *see also* CHRISTIAN A. CHRISTIANSEN, ALEJANDRO FLOREAN, JOHN F. GANTZ, JOE

from the International Data Corporation and the National University of Singapore, focuses on the many costs attendant to software piracy.[130] The security firm Symantec discovered approximately 430 million pieces of malware in 2015.[131] The International Data Corporation (IDC) estimates that the cost of cyberattacks in that same year totaled $400 billion.[132]

While ransoms paid to recover data represent dramatic examples of economic loss,[133] the bulk of economic harm is caused by lost productivity during downtime. Distributed denial of service (DDoS) attacks against businesses typically cost $40,000 per hour, with most attacks lasting longer than six hours.[134] The massive DDoS attack in 2016, which brought down the New York Times, Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, Electronic Arts, and the PlayStation network, occasioned further analysis of downtime costs.[135] The average cost to businesses was estimated at $22,000 *per minute*.[136]

HOWARD, CHRISTIAN LACHAWITZ, RICHARD LEE, STEPHEN MINTON, RICH RODOLFO, ATTAPHON SATIDKANITKUL, RAVIKANT SHARMA, HARISH N. TAORI, THOMAS VAVRA, RICARDO VILLATE, ALBERT WANG & MARCEL WARMERDAM, INT'L DATA CORP., THE DANGEROUS WORLD OF COUNTERFEIT AND PIRATE SOFTWARE 12 (2013), https://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf [https://perma.cc/PHK9-Z56B].

130. *The Importance of Playing It Safe*, *supra* note 114 (reporting on risks of downloading software); Singapore News Center, *Microsoft Launches Cybercrime Satellite Centre To Advance Cybersecurity in Singapore and Asia Pacific*, MICROSOFT (Feb 16, 2015), https://news.microsoft.com/en-sg/2015/02/16/microsoft-launches-cybercrime-satellite-centre-to-advance-cybersecurity-in-singapore-and-asia-pacific [https://perma.cc/3RES-8FZ6] (discussing Play It Safe campaign).

131. BSA, SEIZING OPPORTUNITY THROUGH LICENSE COMPLIANCE 1 (2016), http://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf [https://perma.cc/YSG3-4UU7].

132. *Id.*

133. A wave of ransomware attacks against hospitals generated a great deal of press coverage in 2016. *Hospitals Are Hit with 88% of All Ransomware Attacks*, BECKER'S HOSP. REV. (July 27, 2016), http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html [https://perma.cc/2CKK-QU9E]. The highest profile attack was settled for a ransom of $17,000, though cost to consumer confidence and network infrastructure was likely much higher. Keith Wagstaff, *Big Paydays Force Hospitals To Prepare for Ransomware Attacks*, NBC NEWS (Apr. 23, 2016, 6:06 AM), http://www.nbcnews.com/tech/security/big-paydays-force-hospitals-prepare-ransomware-attacks-n557176 [https://perma.cc/3VTW-YXWC]; Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 3, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets [https://perma.cc/D3S8-7339].

134. TIM MATTHEWS, INCAPSULA, INCAPSULA SURVEY: WHAT DDOS ATTACKS REALLY COST BUSINESSES 6 (2014), https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf [https://perma.cc/F38K-T7V8].

135. Adrienne LaFrance, *How Much Will Today's Internet Outage Cost?*, ATLANTIC (Oct. 21, 2016), http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025 [https://perma.cc/YP8C-6XGR].

136. DIG. CITIZENS ALL. & RISKIQ, *supra* note 121; PONEMON INST. & RADWARE, CYBER SECURITY ON THE OFFENSE: A STUDY OF IT SECURITY EXPERTS 1 (2012), https://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/CyberSecurityontheOffe

Malware also poses a threat to advertisers, costing them about $1.1 billion a year.[137] As advertisers pay for traffic, malware infected bots may fraudulently visit sites, driving up statistics.[138] Moreover, consumer reaction against malware may drive the adoption of ad and script blockers, further harming ad revenue.[139]

B. Botnets Pose Special Risk

While the aforementioned threats are troubling, botnets are especially concerning because they threaten national security and cyber infrastructure. A botnet is composed of bots. Bots or zombies are enslaved devices that act in concert to achieve a purpose.[140] Botnets may be created for a specific purpose or simply as a service to be rented to hackers and spammers.[141]

Botnets may include zombie devices from many countries.[142] However, infected machines in the United States often make up a significant part of these hordes.[143] In the Kelihos.B botnet, focused primarily on spamming and bitcoin wallet ripping, the United States was the second-largest provider of infected devices (in an unusual composition, Poland was the largest contributor).[144] In the Torpig botnet, focused on financial data stealing, the United States provided the largest number of infected devices, accounting for roughly thirty percent of the horde, with Italy as the next largest

---

nse.pdf [https://perma.cc/2PZV-Q826].

137. Allison Schiff, *The Unvirtuous Cycle: IAB Study Suggests Piracy, Malware and Bad Traffic Costs the Industry $8.2 Billion*, ADEXCHANGER (Dec. 1, 2015, 4:28 PM), https://adexchanger.com/online-advertising/the-unvirtuous-cycle-iab-study-suggests-piracy-malware-and-bad-traffic-costs-the-industry-8-2-billion [https://perma.cc/2AQV-SSPE].

138. Ben Elgin, Michael Riley, David Kocieniewski & Joshua Brustein, *How Much of Your Audience Is Fake?*, BLOOMBERG BUSINESSWEEK, https://www.bloomberg.com/features/2015-click-fraud [https://perma.cc/8TKF-XTHR].

139. Mihir Patkar, *Publishers Need To Stop Whining About Adblock*, MAKEUSEOF (Feb. 16, 2015), http://www.makeuseof.com/tag/publishers-need-stop-whining-adblock [https://perma.cc/T966-QXEC].

140. BRETT STONE-GROSS, MARCO COVA, LORENZO CAVALLARO, BOB GILBERT, MARTIN SZYDLOWSKI, RICHARD KEMMERER, CHRIS KRUEGEL & GIOVANNI VIGNA, UNIV. OF CAL. SANTA BARBARA, YOUR BOTNET IS MY BOTNET: ANALYSIS OF A BOTNET TAKEOVER 1 (2009), https://www.fbiic.gov/public/2009/may/torpig.pdf [https://perma.cc/HUP3-YB6C].

141. Clayton, *supra* note 116.

142. Joseph Cox, *Here's a Live Map of the Mirai Malware Infecting the World*, MOTHERBOARD (Oct. 3, 2016, 1:43 PM), https://motherboard.vice.com/read/heres-a-live-map-of-the-mirai-malware-infecting-the-world [https://perma.cc/7DXV-JVU7]; Tom Landesman, *Locky Volumes Plummet, One of the Worlds Largest Botnets Possibly Taken Down*, CLOUDMARK (June 9, 2016), https://blog.cloudmark.com/2016/06/09/locky-volumes-plummet-one-of-the-worlds-largest-botnets-possibly-taken-down [https://perma.cc/Q3Z9-C7H8]. International cooperation in removing botnets is necessary, as seen in the multinational takedown of the Dridex botnet.

143. Nermin Hajdarbegovic, *US Home to More Botnets than Russia and China Combined*, TECHEYE (Jan. 24, 2013), http://www.techeye.net/security/us-home-to-more-botnets-than-russia-and-china-combined [https://perma.cc/RR9Z-L437].

144. Tillmann, *P2P Botnet Kelihos.B with 100.000 Nodes Sinkholed*, CROWDSTRIKE (Mar. 28, 2012), https://www.crowdstrike.com/blog/p2p-botnet-kelihosb-100000-nodes-sinkholed [https://perma.cc/TH8E-SYPC].

provider.[145] Unsurprisingly, U.S. financial accounts made up the bulk of Torpig victims, constituting more than half of all stolen accounts.[146] An analysis of bots spread through users (bots spread through malicious drive-by downloads or infected file distribution as opposed to auto-self-propagating techniques) found that the United States was the second-largest provider of infected networks.[147] In the Mirai botnet, an especially dangerous and well-distributed botnet comprised of infected devices in 164 countries,[148] the United States provided the third-largest number of devices.[149]

To date, the reported video game piracy-related botnets have primarily been tasked with bitcoin mining, thereby creating wealth without the need for an intervening ransom or fraud. But botnets also have been employed to conduct massive DDoS attacks worldwide, leading some commentators to characterize them as "a possible new form of global warfare."[150] A DDoS attack typically entails a large volume of connection requests that overwhelm the target server.[151] The immediate aim is to disrupt service in furtherance of an ultimate goal, though the larger purpose is often difficult to discern.[152]

DDoS attacks have recently grown in size and scope. In October 2016,[153] a widespread DDoS attack[154] was launched against Dyn, a manager of the domain name server (DNS) network.[155] This brought down Twitter, the Guardian, Netflix,

---

145. STONE-GROSS ET AL., *supra* note 140, at 9.

146. *Id.*

147. SEUNGWON SHIN, RAYMOND LIN & GUOFEI GU, TEX. A&M UNIV., CROSS-ANALYSIS OF BOTNET VICTIMS: NEW INSIGHTS AND IMPLICATIONS 13 (2011), http://faculty.cse.tamu.edu/guofei/paper/Shin_RAID11_CrossAnalysis.pdf [https://perma.cc/84WC-W8S5].

148. Lorenzo Franceschi-Bicchierai, *Internet of Things Malware Has Apparently Reached Almost All Countries on Earth*, MOTHERBOARD (Oct. 11, 2016, 4:33 PM), http://motherboard.vice.com/read/internet-of-things-mirai-malware-reached-almost-all-countries-on-earth [https://perma.cc/V5VB-FHB6].

149. Ben Herzberg, Dima Bekerman & Igal Zeifman, *Breaking Down Mirai: An IoT DDoS Botnet Analysis*, INCAPSULA (Oct. 26, 2016), https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html?utm_source=twitter&utm_medium=organic_emp&utm_campaign=2016_Q4_miraiddos [https://perma.cc/R57L-5UUS].

150. Joon Ian Wong, *DDoS Attacks Have Gone from a Minor Nuisance to a Possible New Form of Global Warfare*, QUARTZ (Dec. 13, 2016), http://qz.com/860630/ddos-attacks-have-gone-from-a-minor-nuisance-to-a-possible-new-form-of-global-warfare [https://perma.cc/PW9M-R7MU].

151. *See id.*

152. *See* Lenny Zeltser, *9 Reasons for Denial-of-Service (DoS) Attacks: Why Do They Happen?*, LENNY ZELTSER (Aug. 31, 2016), https://zeltser.com/reasons-for-denial-of-service-attacks [https://perma.cc/JL7N-VLTV].

153. *Alert-TA16-288A Heightened DDoS Threat Posed by Mirai and Other Botnets*, US-CERT (Oct. 14, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A [https://perma.cc/L8TK-CXAD].

154. Michael Kan, *DDoS Attack on Dyn Came From 100,000 Infected Devices*, COMPUTERWORLD (Oct. 26, 2016, 2:21 PM), http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html [https://perma.cc/N4JS-YBBV] (noting that the attack originated from 100,000 infected devices).

155. Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, DYN (Oct. 26, 2016), http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack [https://perma.cc/JQ98-6TRM].

Reddit, and CNN, among others in Europe and the United States.[156] Commentators noted that "hundreds of thousands of websites became unreachable"[157] and that "half the internet shut down."[158] The attack was the largest of its kind, involving primarily Mirai traffic of 1.2 terabytes per second, comprising roughly twice as much data as the next largest attack.[159]

Numerous industry sectors have noted their vulnerability to DDoS attacks, characterizing the Dyn attack as a "practice run" by hackers[160] and predicting that 2017 will see even more DDoS attacks.[161] This is based in part on the new Leet Botnet, capable of delivering malicious traffic at 650 gigabytes per second.[162] December 2016 saw a spate of attacks against Ukraine, with the Ministry of Education brought down due to an attack on December 26.[163] This followed earlier attacks on the Ministry of Finance, pension fund, and Treasury.[164] 123-Reg, the largest British

156. Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [https://perma.cc/6YGC-2HAV].

157. Daniel Smith, *How Friday's Massive DDoS Attack on the U.S. Happened*, RADWARE (Oct. 23, 2016), https://blog.radware.com/security/2016/10/fridays-massive-ddos-attack-u-s-happened [https://perma.cc/2S8W-RZZ4].

158. William Turton, *This Is Why Half the Internet Shut Down Today*, GIZMODO (Oct. 21, 2016, 8:36 AM), http://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835 [https://perma.cc/W9ZE-C6KR].

159. *Heightened DDoS Threat Posed by Mirai and Other Botnets*, US-CERT (Oct. 14, 2016), https://www.us-cert.gov/ncas/alerts/TA16-288A [https://perma.cc/VNW8-MM8J]; Woolf, *supra* note 156.

160. JAMES SCOTT & DREW SPANIEL, INST. FOR CRITICAL INFRASTRUCTURE TECH., RISE OF THE MACHINES: THE DYN ATTACK WAS JUST A PRACTICE RUN (2016), http://icitech.org/wp-content/uploads/2016/12/ICIT-Brief-Rise-of-the-Machines.pdf [https://perma.cc/JA8W-BRF9].

161. Maarten van Horenbeeck, *2017 Predictions: US Isolationism, DDoS, Data Sharing*, ITPROPORTAL (Dec. 29, 2016), http://www.itproportal.com/features/2017-predictions-us-isolationism-ddos-data-sharing [https://perma.cc/PB4V-LE2B].

162. Mark Wycislik-Wilson, *Bigger Than Mirai: Leet Botnet Delivers 650 Gbps DDoS Attack with 'Pulverized System Files*,*'* BETANEWS, http://betanews.com/2016/12/28/leet-botnet-ddos [https://perma.cc/TB4J-2FPU]; *see also* Catalin Cimpanu, *New GhostAdmin Malware Used for Data Theft and Exfiltration*, BLEEPINGCOMPUTER (Jan. 17, 2017, 2:00 PM), https://www.bleepingcomputer.com/news/security/new-ghostadmin-malware-used-for-data-theft-and-exfiltration [https://perma.cc/DYC7-H5PC] (discussing GhostAdmin, a new malware botnet family).

163. *Education Ministry Website Is Under DDoS-Attack*, 112.UA (Dec. 26, 2016, 2:14 PM), http://112.international/society/education-ministry-website-is-under-ddos-attacks-12465.html [https://perma.cc/63A8-QF5P]; Vsevolod Nekrasov, *Ukraine Is Losing a Cyberwar: Hackers Attacked Public Treasury*, 112.UA (Dec. 12, 2016, 2:30 PM), https://112.international/article/ukraine-is-losing-a-cyberwar-hackers-attacked-public-treasury-11957.html [https://perma.cc/KC9W-Z4BU].

164. Nekrasov, *supra* note 163.

hosting company, was targeted in a major DDoS attack in January 2017.[165] Torrent sites also have been the victims of DDoS attacks.[166]

While the Dyn attack concerned an Internet of Things Mirai botnet (made up of "smart" devices and unprotected cameras) rather than one centered on PCs,[167] the focus on botnets comprising personal computers is well warranted. Researchers believe the newly discovered Jaku botnet, spread primarily through poisoned torrents containing counterfeit software, targets Korean and Japanese academics, engineers, and information workers.[168] Due to the botnet's behavior and strange install base, the botnet is likely the work of North Korea.[169] There are already several well-documented botnets that arose from pirated games. Moreover, gaming PCs make attractive targets due to their interconnectivity, bandwidth, and computing power.

The danger of botnets is particularly acute because the rise in DDoS power has coincided with a greater willingness of state actors to engage in cyberattacks. The recent Russian hacking of the Democratic National Committee may have heightened public awareness of cyber threats,[170] but botnets and DDoS attacks are likely to remain a powerful tool with few impediments. Botnets, simply put, are a growing risk to cyber infrastructure and national security.[171]

---

165. Kat Hall, *3... 2...1... and 123-Reg Hit by DDoSers. Again*, REGISTER (Jan. 6, 2017, 1:42 PM), https://www.theregister.co.uk/2017/01/06/123reg_hit_with_ddos_attack_again [https://perma.cc/7QDE-X2JC].

166. Ernesto Van der Sar, *ExtraTorrent Under DDoS Attacks, Pirate Bay Down*, TORRENTFREAK (Dec. 27, 2016), https://torrentfreak.com/extratorrent-under-ddos-attacks-pirate-bay-down-161227 [https://perma.cc/5CPJ-7Z6C].

167. Kan, *supra* note 154 (noting that attack originated from 100,000 infected devices).

168. ANDY SETTLE, BAPADITTYA DEY, NICHOLAS GRIFFIN & ABEL TORO, FORCEPOINT, JAKU: ANALYSIS OF A BOTNET CAMPAIGN 6 (2016), https://www.forcepoint.com/sites/default/files/resources/files/report_jaku_analysis_of_botnet_campaign_en_0.pdf [https://perma.cc/675D-QJEJ].

169. *Id.* at 29. The cyber threats attendant to North Korea were recently highlighted in the WannaCry attacks. Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, WASH. POST (June 14, 2017), https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html [https://perma.cc/5A4A-BDFG].

170. NCCIC & FBI, GRIZZLY STEPPE – RUSSIAN MALICIOUS CYBER ACTIVITY 1 (Dec. 29, 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf [https://perma.cc/H6RX-XM4N] (concluding that the Russian intelligence service conducted a campaign "to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities"); Eric Lipton, David E. Sanger & Scott Shane, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html [https://perma.cc/957C-54WU].

171. *See* Marco Deseriis, *Hacktivism: On the Use of Botnets in Cyberattacks*, 34(4) J. THEORY, CULTURE, & SOC'Y 131, 132 (2016); David Harley, *TDSS: Political Botnets*, SC MEDIA, https://www.scmagazine.com/tdss-political-botnets/article/559068 [https://perma.cc/J2V3-ZJKT].

Indeed, state-influenced DDoS attacks are not merely hypothetical.[172] There have been previous geopolitical actions related to botnets: Russian-inspired DDoS attacks on Estonia and Ukraine are well documented.[173]

1. Estonia

In 2007, a two-week long botnet DDoS attack on Estonian state websites crippled the country's cyber infrastructure.[174] Commentators likened botnets to an air force, noting, "[t]hese giant squadrons were made up of hundreds of thousands of individual computers from around the world that had been hijacked previously by hackers. The computers, known as zombies, could be made to repeatedly flood designated Internet addresses with a variety of useless network-clogging data."[175] Tracing the IP addresses revealed that the "botnet compris[ed] mostly hijacked computers in the US."[176] All told, "[t]here were nearly 130 unique DDoS attacks on Estonian websites. Two kinds occurred—from botnets and from ping flood scripts passed around on forums."[177] The attacks rendered "[a]t least six sites . . . all but inaccessible, including those of the foreign and justice ministries."[178] "[N]o country has experienced anything on this scale."[179]

Russian hackers were blamed for the coordinated cyberattack.[180] "The attacks may have been prompted by an Estonian decision to relocate a Russian World War II memorial."[181] The attack was so serious that Estonia reportedly sought to invoke Article 5 protection from its allies under the North Atlantic Treaty.[182]

---

172. Joseph Demarest, *Taking Down Botnets*, FBI (July 15, 2014), https://www.fbi.gov/news/testimony/taking-down-botnets [https://perma.cc/2MJ5-WDVT].

173. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 2, 2007, 12:00 AM), https://www.wired.com/2007/08/ff-estonia/?currentPage=all [https://perma.cc/R962-E7P6].

174. *Estonia and Russia: A Cyber-riot*, ECONOMIST (May 10, 2007), http://www.economist.com/node/9163598 [https://perma.cc/JZ5F-KGYU]; John Leyden, *Botnets Linked to Political Hacking in Russia*, REGISTER (Dec. 14, 2007, 4:00 PM), http://www.theregister.co.uk/2007/12/14/botnet_hacktivism [https://perma.cc/79FW-EBT8].

175. Davis, *supra* note 173 ("All major commercial banks, telcos, media outlets, and name servers—the phone books of the Internet—felt the impact, and this affected the majority of the Estonian population. This was the first time that a botnet threatened the national security of an entire nation.").

176. *Id.*

177. Chuck Miller, *Russia Confirms Involvement with Estonia DDoS Attacks*, SC MEDIA (Mar. 12, 2009), https://www.scmagazine.com/russia-confirms-involvement-with-estonia-ddos-attacks/article/555577 [https://perma.cc/6PNT-ZY5M].

178. *Estonia and Russia: A Cyber-riot*, *supra* note 174.

179. *Id.*

180. Davis, *supra* note 173.

181. Miller, *supra* note 177.

182. Scheherazade S. Rehman, *Estonia's Lessons in Cyberwarfare*, U.S. NEWS & WORLD REP. (Jan. 14, 2013, 3:34 PM), http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare [https://perma.cc/MD4S-DFPB].

> The Estonians were trying to evoke Article 5 when they were being attacked by the Russians in 2007, but thought better of it and did not evoke the article because of the lack of support from their NATO allies; NATO could not agree on the definition of "under attack" in this case and identifying and proving that this was a Kremlin-sponsored attack was difficult.[183]

2. Ukraine

In 2014,[184] and again in 2015, the pro-Russian hacktivist group CyberBerkut launched a series of DDoS and other cyberattacks in an attempt to disrupt and discredit Ukrainian elections.[185] "[C]omputers of Ukraine's national election commission were hit with a major attack that deleted backups, damaged hard drives, ma[d]e software unusable and changed router[] settings."[186]

> In the wee hours of the morning after polls closed, as results flowed in from Ukrainian election districts, Internet links feeding that data to the vote tally system were hit with a barrage of fake data packets—known as distributed denial of service (DDoS) attacks. So from about 1 to 3 a.m. on May 26, election results were blocked, delaying the finally [sic] tally until the early morning, a preliminary report by international election observers recounted.[187]

3. Other Politically Motivated DDoS Attacks

There are many other documented examples of DDoS based "hacktivism."[188] The year after targeting Ukraine, CyberBerkut launched similar attacks against German websites, urging "all people and government of Germany [sic] to stop financial and political support of criminal regime in Kiev, which unleashed a bloody civil war. We are CyberBerkut! We will not forget! We will not forgive!"[189] The attack brought

---

183. *Id.*

184. Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers*, CHRISTIAN SCI. MONITOR (June 17, 2014), http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video [https://perma.cc/8BNJ-C8F4].

185. Margaret Coker & Paul Sonne, *Ukraine: Cyberwar's Hottest Front*, WALL ST. J. (Nov. 9, 2015, 9:14 PM), http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671 [https://perma.cc/A8V3-DXGS].

186. Elizabeth Weise, *'Getting Twitchy': Election Threats Have Cyber Experts Worried*, USA TODAY (Nov. 4, 2016, 4:05 PM), http://www.usatoday.com/story/tech/news/2016/11/04/cyber-threats-election-2016-russia-clinton-trump-ukraine-hack-ddos-dyn-denial-of-service-attack/93249646 [https://perma.cc/NJ4S-J4SX].

187. Clayton, *supra* note 184.

188. JUAN ECHEVERRÍA & SHI ZHOU, DISCOVERY, RETRIEVAL, AND ANALYSIS OF THE 'STAR WARS' BOTNET IN TWITTER (Jun. 13, 2017), https://arxiv.org/pdf/1701.02405.pdf [https://perma.cc/C6ZS-587N] (discussing 350,000-strong twitter botnet able to sway public opinion).

189. Dennis Lynch, *Pro-Russian Hacker Group CyberBerkut Claims Attack on German Government Websites*, INT'L BUS. TIMES (Jan. 7, 2015, 9:10 AM), http://www.ibtimes.com

down "the website of Merkel's government seat and the website of Germany's legislative body, the Bundestag."[190]

Beyond the numerous accusations of Russian cyberattacks to influence the United States 2016 Presidential Election,[191] DDoS attacks have been previously linked to undermining Russian elections.[192] In 2007, DDoS attacks were launched against opposition parties led by chess grandmaster Garry Kasparov.

> The attacks shut down the opposition Web sites just as government authorities announced a change in venue for an upcoming opposition rally. With his Web site down, Kasparov had difficulty informing his followers of the change, and when they massed at the originally announced location, he was arrested for leading an illegal rally.[193]

The motives behind attacks are not always so obvious. In 2013, a Russian controlled botnet attacked Tor, an onion router used for anonymous online activity, in a move that befuddled commentators.[194]

Of course, the Russians do not have a monopoly on this practice. Thai hackers launched a DDoS attack to protest restrictive internet laws.[195] In 2015, Chinese hackers targeted Github, a website of programming code that could be helpful in circumventing state censorship.[196]

/pro-russian-hacker-group-cyberberkut-claims-attack-german-government-websites-1775874 [https://perma.cc/32CQ-MEUA].

190. *Id.*

191. Michael Riley & Jordan Robertson, *Russian CyberHacks on U.S. Electoral System Far Wider than Previously Known*, BLOOMBERG POL. (June 13, 2017, 5:00 AM), https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections [https://perma.cc/7CMR-K58S] (noting that Russian hackers hit voting systems in thirty-nine states).

192. Matt Hines, *Botnets: The New Political Activism*, INFOWORLD (Jan. 8, 2008), http://www.infoworld.com/article/2642293/security/botnets--the-new-political-activism.html [https://perma.cc/7BQN-6K4J].

193. Davis, *supra* note 173.

194. Jim Edwards, *A Russian Botnet Is Attacking the Secret Internet for Criminals—and No One Knows Why*, BUS. INSIDER (Sept. 5, 2013, 9:26 AM), http://www.businessinsider.com/a-russian-botnet-is-attacking-the-secret-internet-for-criminals-and-no-one-knows-why-2013-9 [https://perma.cc/5DRY-MEE8].

195. India Ashok, *Hackers Hit Thai Government with DDoS Attacks Protesting Against Restrictive Internet Law*, INT'L BUS. TIMES (Dec. 20, 2016, 6:57 AM), http://www.ibtimes.co.uk/hackers-hit-thai-government-ddos-attacks-protesting-against-restrictive-internet-law-1597339 [https://perma.cc/QFY9-ZPSZ].

196. Paul Mozur, *China Appears To Attack GitHub by Diverting Web Traffic*, N.Y. TIMES (Mar. 30, 2015), https://www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html [https://perma.cc/PY6Y-2DKK]; *see also* Jesse Newland (jnewland), *Large Scale DDoS Attack on github.com*, GITHUB BLOG: ENGINEERING (Mar. 27, 2015), https://github.com/blog/1981-large-scale-ddos-attack-on-github-com [https://perma.cc/M64B-VRES].

C. Avenues for Infection Associated with Piracy

Virus vectors associated with piracy include drive by downloads and downloaded executables. Drive-by downloads include inadvertent or covert downloads of malicious software when a user visits a site.[197] Downloaded executables occur when the user intends to download a target file but instead downloads malware.[198] The distinction between these two mechanisms is important, as the former is typically prevented by avoidance of known malware sites and the latter requires greater user education.

The problem of drive-by downloads is common to sites that host pirated songs, movies, and games. Users who frequent such sites are roughly "28 times more likely to [encounter] malware . . . than users of mainstream websites (such as espn.com . . .)."[199] Of course, sites related to non-infringing content may also offer a platform for the delivery of malicious code. "Malvertising" rings inject ads that redirect users or attempt to deliver malware.[200] Upon visiting a site, a user may unknowingly trigger the download of covert software.[201] Browser side intervention may help prevent this, either by presenting an initial filter of dangerous sites ("blacklisting" those sites with a security warning)[202] or by inhibiting scripts or pop-ups.[203]

The problem of downloaded executables[204] is more pernicious and is a heightened concern in the realm of pirated software rather than pirated music or movies. Music

---

197. *See* Andra Zaharia, *How Drive-By Downloads Work—From Disbelief to Protection*, HEIMDAL SECURITY, https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work [https://perma.cc/3YSD-QZGQ]; Joshua Zorabedian, *How Malware Works: Anatomy of a Drive-By Download Web Attack (Inforgraphic)*, SOPHOS NEWS (Mar. 26, 2014), https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic [https://perma.cc/PG6B-NV97].

198. *See* Jim Martin, *How To Check if Your File Contains a Virus*, TECH ADVISOR (Feb. 5, 2016), http://www.techadvisor.co.uk/how-to/security/how-check-if-file-contains-virus-3634662 [https://perma.cc/W37V-PTAK].

199. DIG. CITIZENS ALL., ENABLING MALWARE: HOW U.S.-BASED FIRMS ARE ENABLING MALWARE PEDDLERS TO BAIT CONSUMERS AND STEAL THEIR PERSONAL INFORMATION 3 (2016).

200. Liam Tung, *Pirate Bay Visitors Infected with Crypto-Ransomware via Bad Ads*, ZDNET (Apr. 27, 2016, 11:26 AM), http://www.zdnet.com/article/pirate-bay-visitors-infected-with-crypto-ransomware-via-bad-ads [https://perma.cc/9VTL-TAKP]; Rahul Kashyap, *Why Malvertising Is Cybercriminals' Latest Sweet Spot*, WIRED, https://www.wired.com/insights/2014/11/malvertising-is-cybercriminals-latest-sweet-spot [https://perma.cc/TBE7-JCN8].

201. Zorabedian, s*upra* note 197.

202. *See* STOP BADWARE, https://www.stopbadware.org [https://perma.cc/979B-6Y2S].

203. Alan Henry, *The Best Browser Extensions That Protect Your Privacy*, LIFEHACKER (Aug. 31, 2015, 1:00 PM), http://lifehacker.com/the-best-browser-extensions-that-protect-your-privacy-479408034 [https://perma.cc/MNX7-EATR] (collecting various browser extensions that block ads and scripts). This may lead to websites requiring users to disable blockers in order to access content, however. Joel Hruska, *Forbes Forces Readers To Turn Off Ad Blockers, Promptly Serves Malware*, EXTREMETECH (Jan. 8, 2016, 2:09 PM), https://www.extremetech.com/internet/220696-forbes-forces-readers-to-turn-off-ad-blockers-promptly-serves-malware [https://perma.cc/WY6F-ZHZZ].

204. If a user downloads a file using BitTorrent there is an additional avenue as the torrent

and movie files may be played in browser and typically do not require the download of files, although certain sites attempt to dupe users into downloading "players" or codecs.[205] Should music or movie files be downloaded, however, these files are unlikely to be executable files.[206] An .mp3 or .mov file, for example, does not contain a program itself, just data to be read by the appropriate software. While malicious programs can be renamed, to disguise .exe as .mp3 files, for example, users may thwart these attempts by simply turning on extensions. As a last barrier, a malicious file, even if renamed, may be detected by user-side virus protection.

D. Immunities to Infection

There are several barriers that limit the risk of infection from malware. The first is quarantine or avoidance of a site known to host malware. This may be accomplished through user knowledge or through browser intervention. Users frequently note malware-riddled sites, complaining of intrusive pop-ups and the like.[207]

---

client itself also might host malware. In the case of Transmission, a popular OSX torrent client, ransom malware was introduced twice by outside parties. Paul Szoldra, *A Popular App for Downloading Movies and Music Was Infected with Ransomware, Again*, BUS. INSIDER (Aug. 31, 2016, 2:16 PM), http://www.businessinsider.com/transmission-malware-2016-8 [https://perma.cc/E5AG-T6J5]. However, third parties need not introduce the malware. A popular BitTorrent client, uTorrent, was heavily criticized for bundling its application with Epic Scale, which is essentially a bitcoin miner. Joel Hruska, *uTorrent Accused of Bundling Cryptocurrency Malware with Popular BitTorrent Client*, EXTREMETECH (Mar. 6, 2015, 3:27 PM), https://www.extremetech.com/computing/200602-utorrent-accused-of-bundling-cryptocurrency-malware-with-popular-bittorrent-client [https://perma.cc/5FEL-JGN3]; Ernesto Van der Sar, *uTorrent Quietly Installs Cryptocurrency Miner, Users Complain*, TORRENTFREAK (Mar. 6, 2015), https://torrentfreak.com/utorrent-quietly-installs-riskware-bitcoin-miner-users-report-150306 [https://perma.cc/CZ7S-25AV]. And this was not the first time that uTorrent hosted malware—the client had previously been found to have adware "Search Protect." *Removing Advertising Offers*, UTORRENT HELP CTR. (Nov. 7, 2014, 9:33 AM), http://help.utorrent.com/customer/portal/articles/1605936 [https://perma.cc/XFW7-Q3PT] (providing uninstall options for "advertising offers" which hijack users default search engine and home page).

205. *See, e.g.*, Stelian Pilici, *Remove the VEEHD Plugin V10 Ads (Virus Removal Guide)*, MALWARETIPS (Dec. 21, 2014), https://malwaretips.com/blogs/remove-the-veehd-plugin-v10-virus [https://perma.cc/P3GH-3MN5] (providing steps to remove the VEEHD plugin that actually serves as adware delivery).

206. This is not to say that an infectious file cannot be hosted in nonthreatening file types. One method is to hide viruses in macros in document or excel files. *Macro Viruses*, NORTON, https://us.norton.com/internetsecurity-malware-macro-viruses.html [https://perma.cc/69S3-SA4S].

207. *See, e.g.*, BálintBence';DROP TABLE users#, Comment to *Top Torrent Sites See Traffic Surge After 'Shutdowns,'* TORRENTFREAK (Sept. 3, 2016), https://torrentfreak.com/top-torrent-sites-see-traffic-surge-shutdowns-160903 [https://perma.cc/6RN5-D2QT] (noting "[s]ome [torrent] sites really like to hijack your clicks for shady advertisements"); *see also* George Brand, Comment to *Top Torrent Sites See Traffic Surge After 'Shutdowns,'* TORRENTFREAK (Sept. 3, 2016), https://torrentfreak.com/top-torrent-sites-see-traffic-surge-shutdowns-160903 [https://perma.cc/U8AL-ZY4B] ("Yes, these torrent sites can act weird sometimes. Make sure you are fully armored when you visit them. Use a browser like Firefox, sandboxed if possible, with a good ad-blocker and flash blocker.").

Known risk sites may be screened out from initial visits, requiring the user to override safety warnings in order to land on the site.[208] While browser efforts to prevent infection spread are laudable, they are not without controversy.[209] Sites may be added to blacklists in error, either through a systematic filter error or through a false positive.[210] Moreover, users may perceive the blacklist as an effort to bar piracy rather than an attempt to prevent the spread of malware.[211] This view may have additional credibility in light of domain name seizures brought about by Immigrations and Customs Enforcement (ICE), in which a user's attempts to visit a page hosting pirated content are redirected to a warning page about copyright.[212] Should a user visit a page presenting a malware risk, it is possible for a file to be downloaded without user consent. These are so-called drive-by downloads.

Once on a site, users may also use sound judgment in the types of files they do download. This avoidance may rely on knowledge of file types or on the reputational, self-screening function performed on community sites. The former typically involves the avoidance of any file that is potentially an executable. The latter may take several forms, but typically involves knowledge-building through actions of other users. This may entail a message board in which users may warn of malware or a pre-screened badge affixed to files that have been found to be safe.[213] Another common approach

---

208. *See, e.g.*, *Blacklisted by Google*, STOP BADWARE, https://www.stopbadware.org/blacklisted-by-google [https://perma.cc/T4ZY-NPVH].

209. Parija Kavilanz, *Google's Dreaded 'Blacklist,'* CNN MONEY (Nov. 5, 2013, 12:11 PM), http://money.cnn.com/2013/11/04/smallbusiness/google-blacklist [https://perma.cc/UWG6-V5ZC].

210. In 2009, Google mistakenly flagged the entire internet as malware. Robin Wauters, *Google Flags Whole Internet as Malware*, TECHCRUNCH (Jan. 31, 2009), https://techcrunch.com/2009/01/31/google-flags-whole-internet-as-malware [https://perma.cc/EH7M-5FMJ].

211. Users believe this even though Google has noted it will not blacklist without specifics. Ernesto Van der Sar, *Google Refuses MPAA Request to Blacklist 'Pirate Site' Homepages*, TORRENTFREAK (Nov. 23, 2014), https://torrentfreak.com/google-refuses-mpaa-request-blacklist-pirate-site-homepages-141123 [https://perma.cc/WH8H-GJH4]. However, Google has previously taken contrary views, removing IP infringing sites from autocomplete, Kent Walker, *Making Copyright Work Better Online*, GOOGLE PUB. POL'Y BLOG (Dec. 2, 2010), https://publicpolicy.googleblog.com/2010/12/making-copyright-work-better-online.html [https://perma.cc/9M59-L9HB], and allowing the delisting of specific torrent trackers. Ernesto Van der Sar, *MPAA Kicks KickassTorrents Off Google With 'Precision' Takedown*, TORRENTFREAK (June 23, 2013), https://torrentfreak.com/mpaa-kicks-kickasstorrents-off-google-with-precision-takedown-130623 [https://perma.cc/K6W6-BFLC].

212. Andrew Moshirnia, *COICA, the Sequel: Back in Blacklist*, DIGITAL MEDIA L. PROJECT (Apr. 11, 2011, 4:18 PM), http://www.dmlp.org/blog/2011/coica-sequel-back-blacklist [https://perma.cc/MVQ9-3SDN] (noting critical response to ICE campaign); Andrew Moshirnia, *Some Say the World Will End in MAFIAAFire: Why Domain Seizures Don't Work*, DIGITAL MEDIA L. PROJECT (May 9, 2011, 1:28 PM), http://www.dmlp.org/blog/2011/some-say-world-will-end-mafiaafire-why-domain-seizures-dont-work [https://perma.cc/F5T8-QALX] (same).

213. *See supra* note 57; Doctor-Fantastic, Comment to *How to Torrent Safely (Without Getting Viruses or Malware)*, REDDIT: R/TORRENTS (Mar. 1, 2015), https://www.reddit.com/r/torrents/comments/2xlwzk/how_to_torrent_safely_without_getting_viruses_or [https://perma.cc/MC5B-LC9T] ("[M]ost anti virusses [sic] will see the crack as a virus so in that case you can never be sure. Always check the comment!").

is to look only for files with a large number of seeds.[214] Power users on a site may also be more likely to upload uninfected software.[215] This may also entail a curating process by administrators or moderators in which infected torrents or links are removed from the site.

Once a file is downloaded it typically remains to be executed. Depending on the means of delivery, operating systems issue standard warnings against files downloaded from uncertain or unverified sources.[216] To continue with the installation, the user may have to bypass this protection by turning off verification or by simply clicking an additional dialogue window.[217] This barrier is largely ineffective in the case of pirated software because the user knows that the file is unverified (were it any other way, the file would not exist).[218]

Should a file be executed, however, the last line of defense is a desktop antivirus program. Antivirus programs look for known risk files, scanning for "patterns based on the signatures or definitions of known malware."[219] Antivirus software compares downloaded software signatures to a database of known threats and blocks installation on that basis. Such programs are, of course, more effective in screening known threat categories, rather than idiosyncratic malware.[220] In an effort to catch novel or zero-day malware, antivirus software also uses heuristics to block programs exhibit-

---

214. Crashoveride420, Comment to *Looking for Good Security That Is "Pirate" Friendly*, BLEEPINGCOMPUTER (Feb. 8, 2012, 12:06 AM), https://www.bleepingcomputer.com/forums/t/441256/looking-for-good-security-that-is-pirate-friendly [https://perma.cc/VSS3-8WK7] ("[Y]ou use [The Pirate Bay] then always check the comments. I have yet to run into anything bad…just as long as your read everything carefully. The more seeders the better, no one is going to download a virus and not get pissed and report it.").

215. Christian Cawley, *10 Easy Ways To Never Get a Virus*, MAKEUSEOF (Jan. 16, 2017), https://www.makeuseof.com/tag/9-easy-ways-virus [https://perma.cc/ER7B-E8L6]; Alvas Rawuther, Comment to *Looking for Good Security That is "Pirate" Friendly*, BLEEPINGCOMPUTER (Mar. 10, 2012, 6:24 PM), https://www.bleepingcomputer.com/forums/t/441256/looking-for-good-security-that-is-pirate-friendly [https://perma.cc/JYB7-YEM3] ("The best way is to just read the comments before downloading any file. For [The Pirate Bay], have a look at seeders and see if the uploader is a trusted one.").

216. *Code-Signing, Gatekeeper, and Authenticode*, ISCREENSAVER, https://iscreensaver.com/help/notes/code_signing/code_signing.shtml [https://perma.cc/WDV9-B8AR] (including screenshots of typical warnings).

217. Daryl McCartney, *How To Disable Gatekeeper in OSX Sierra*, AMSYS (Sept. 29, 2016), http://www.amsys.co.uk/2016/09/disable-gatekeeper-in-osx-sierra [https://perma.cc/5BZQ-4TM6].

218. AnthropicMachine, *MacOS Sierra and App Privacy*, REDDIT: R/PIRACY (July 18, 2016), https://www.reddit.com/r/Piracy/comments/4tcjpl/macos_sierra_and_app_piracy [https://perma.cc/8VTM-3ENR] (discussing need to disable macOS Gatekeeper to install pirated apps).

219. *Security Tip (ST04–005): Understanding Anti-Virus Software*, US-CERT.GOV (June 5, 2015), https://www.us-cert.gov/ncas/tips/ST04-005 [https://perma.cc/YU4X-37QS].

220. Giovanni Vigna, *Antivirus Isn't Dead, It Just Can't Keep Up*, LASTLINE (May 21, 2014), http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up [https://perma.cc/ZG79-ASEC] (noting that zero-day malware is detected approximately 51% of the time, with that rate increasing over time as look-up signature tables are updated).

ing known risk behavior—such as launching a particular process or accessing a specific part of the registry. Lastly, virus protectors may only provide defense against infection if they are engaged.

E. Software Piracy Is a Special Risk

While some attention has been paid to viral vectors in music and movie piracy, software piracy presents a graver threat due to inherent need for executables and the likelihood of user-inhibition of antivirus software.

Downloading pirated software carries a much greater risk of infection than merely downloading audio-visual files due to user behaviors. First, the download of software necessitates the download of an executable file. Whereas movie and audio pirating users may be trained to avoid dangerous extensions (e.g., .exe, .bat, .cmd, .com, .lnk, .pif, .scr, .vb, .vbe, .vbs, and .wsh), the files downloaded to facilitate the pirating of software are inherently dangerous executables. Cracked games may comprise hundreds of files, and user inspection of the download package is not a reliable method to reduce infection rates. [221]

Second, pirating users often disregard automated warnings regarding the possible viral content of downloaded files. The nature of cracking software often results in false positives[222] from antivirus software employing heuristic detection. Cracked software typically alters existing executables or contains encrypted content, two behaviors common to malware. Additionally, there is a belief that virus protection software manufacturers deliberately target pirated software. Users frequently complain in forums that antivirus software prevents a successful crack install.[223] As

---

221. Hacking groups understand this limitation and thus prefer to target game torrents for infection rather than bundled music or movies. *See infra* notes 310–312 and accompanying text.

222. HeroSquared, *What Is a Good Antivirus for Pirates?*, REDDIT: R/PIRACY (Sept. 19, 2015), https://www.reddit.com/r/Piracy/comments/3lk0ls/what_is_a_good_antivirus_for_pirates [https://perma.cc/Y3Y6-XFN5] ("Every virus software I have used so far has deletes [sic] false positives . . . [s]o what virus software do you guys use?" Receiving the replies "Virtually all AV software will throw false positives about piracy cracks" and "I'm a pirate for about 8 years and antivirus just isn't for pirates use common sense. Files with a lot seeders will always be without a virus.").

223. AlexDBR, Comment to *False Positives or Paranoid Anti-Virus Cos. ??*, WILDERS SEC. F. (Feb. 21, 2010), https://www.wilderssecurity.com/threads/false-positives-or-paranoid-anti-virus-cos.265934 [https://perma.cc/SSA4-D9VZ] ("I think there is a connection between software industry and AVs. . . . You can see this when the keygens/cracks are marked as 'hack tools' or 'potentially unwanted programs'. . . . But another reason for being detected as trojans/viruses is because they sometimes use dubious exe compression/encryption (methods employed a lot by malware creators)."); ken1943, Comment to *Is ESET Detecting Cracks for Games as Viruses?*, ESET SECURITY F. (May 16, 2015), https://forum.eset.com/topic/4937-is-eset-detecting-cracks-for-games-as-viruses [https://perma.cc/EA76-ZNKL] ("Cracks are programs that modify another program. Security programs see that as a virus. The only way to use them is to shut down your security programs, but then you open yourself to getting screwed. In this day and age, cracks are a gamble."); moeburn, *How Do You Tell the Difference Between an Actual Virus and a False Positive?*, REDDIT: R/PIRACY (Sept. 6, 2015), https://www.reddit.com/r/Piracy/comments/3jvfsz/how_do_you_tell_the_difference_between_an_actual [https://perma.cc/CF2M-T8TN] ("If you go on any torrent website, chances are

such, installing a cracked game typically requires users to turn off their virus protection.[224]

For this same reason, torrent comment sections often contain claims of viruses, along with counter claims of false positives.[225] Thus, a claim that a torrent contains fake content is more likely to dissuade a downloader than a claim that the torrent contains a virus.[226] This may be an artifact of torrent poisoning, in which seeders (occasionally intellectual property rights holders) deliberately upload corrupt or mislabeled files to frustrate and detect pirates.[227] Obviously, fake content is often easier to detect than infected content, especially if the malware is designed to lay dormant or otherwise camouflage its effects on the infected system.

Video game piracy, therefore, presents a perfect environment for malware infection. The traditional barriers to malware infection are either discredited, ignored, or disabled. Users pirating video games frequent known malware sites, disregard browser side warnings, download inherently dangerous executables, and turn off desktop side antivirus programs that may otherwise limit the installation of cracked software. Worse still, users pirating video games often make attractive targets due to

---

you'll be able to find a torrent with viruses, and if you report it, they'll tell you 'Oh that's just a false positive'. Without any information, whether it really is or not, it seems the default position is for everyone to assume everything is a false positive until proven otherwise. So short of actually running the program in sandboxie to see what it tries to do, how do you tell if something is actually detected as a virus or not?"); V8VANTAGE, Comment to *Antivirus Keeps Deleting Game Crack?*, YAHOO! ANSWERS, https://answers.yahoo.com/question/index?qid=20131125233853AAu3fgM [https://perma.cc/365U-TVZH] ("A lot of antivirus programs [flag cracks as viruses], they have been designed to flag up even virus free no-cd patches as 'false positives', because these patches/cracks are almost always used illegally.").

224. Resource-intensive games necessitate powerful computers. Accordingly, video game users make attractive targets due to the potential of using computing resources for cryptocurrency mining programs.

225. *See, e.g.*, Nihilist91, *DA: I - Disable Anti Virus When Downloading the Crack*, REDDIT: R/PIRACY, (Dec. 15, 2014), https://www.reddit.com/r/Piracy/comments/2pdjvg/dai_disable_anti_virus_when_downloading_the_crack [https://perma.cc/DS98-ENCR] ("I saw a post telling me to [disable anti virus] . . . worked like a charm. Disable AV to install, false positive. Trust me it safe ;).").

226. *See* Comments in response to user HobbitH's post, REDDIT: R/PIRACY (Aug. 24, 2016), https://www.reddit.com/r/Piracy/comments/4zeo46/fake_viruswarnings_in_comments [https://perma.cc/683K-SUZ7] (noting that one cannot trust Antivirus detection and should download from reputable uploaders, preferably uploaders with a power user badge); Comment in response to user SupremeMystique's post, REDDIT: R/PIRACY (Aug. 14, 2016), https://www.reddit.com/r/Piracy/comments/4xlwba/virus_activation_during_launch [https://perma.cc/L3W7-Z4X4] (wondering if he should continue install of *Far Cry 4* repack and being told that "[i]t's safe . . . . [The uploader] was a verified uploader on [Kick Ass Torrents] and well known among the community, so yes [his repacks are] safe").

227. Pooja Balhara, *A Review on Torrent & Torrent Poisoning over the Internet*, 22 INT'L J. COMPUT. SCI. & MGMT. STUD. 7, 10 (2016), http://www.ijcsms.com/journals/Volume%2022,%20Issue%2001,%20January%202016_IJCSMSJanuary2016_7_12_Pooja.pdf [https://perma.cc/J2P3-RVYE]; Mike, *What Is Torrent Poisoning and How To Avoid It*, ARES GALAXY: FILE SHARING (Apr. 18, 2012), http://www.aresfree.net/what-is-torrent-poisoning-and-how-to-avoid-it [https://perma.cc/W8LA-2SA2].

their computers' assumed power and interconnectivity. Finally, due to a belief that antimalware efforts are simply antipiracy propaganda efforts, users will resist corporate warnings related to this situation.

F. Case Studies of Widespread Video Game Infection

Due to broad variance in claimed infection rates and widespread belief in the pirate community that all such claims are overblown, it is important to examine case studies of viral infection linked to specific games.[228] Unsurprisingly, viruses are commonly placed in the most popular titles in every genre for faster, diffused infection.

1. *Watch Dogs* Bitcoin Miner

Watch Dogs was a well-received game developed by Ubisoft that ultimately shipped nine million copies for various devices.[229] The game was announced approximately two years before release and was highly anticipated. The "[r]easonably high" system requirements for the game were announced prior to release, with commentators noting that the demands of the game were "a 64-bit system with significant oomph."[230] The game therefore presented an excellent opportunity for an enterprising hacker, as the game would be highly sought after and installed on powerful machines.

In 2014, Skidrow released a cracked version of *Watch Dogs*.[231] When the game was repackaged in a public torrent, it was bundled with malware—a bitcoin miner.[232] The game file installed "winlogin.exe," a virus named similarly to the legitimate "winlogon.exe" process, as well as a miner "itc.exe."[233] Bitcoin miners covertly enslave a device so that it dedicates resources to process bitcoins. High performance gaming rigs are especially attractive targets as they have high-end GPUs and CPUs. Users reported a diversion of approximately of computing resources.[234] The cloud

---

228. While scene releases may become infected, there is no agreement on whether specific scene groups are more prone to be attributed in infected files. *See* YtesHavNoLips, *Why Do People Say "You'll Get a Virus From Skidrow Websites,"* REDDIT (Mar. 7, 2015), https://www.reddit.com/r/Piracy/comments/2y9q69/why_do_people_say_youll_get_viruses_from_skidrow [https://perma.cc/RD3J-QHWZ].

229. Eddie Makuch, *Watch Dogs Ships 9 Million Copies, Helping Ubisoft Sale Rise Sharply*, GAMESPOT (Oct. 30, 2014, 12:42 PM), http://www.gamespot.com/articles/watch-dog-ships-9-million-copies-helping-ubisoft-s/1100-6423279 [https://perma.cc/EVG7-LMWQ].

230. Phil Savage, *Watch Dogs System Requirements Confirmed, Wants a 64-bit System with Significant Oomph*, PC GAMER (Apr. 7, 2014), http://www.pcgamer.com/watch-dogs-system-requirements-confirmed-wants-a-64-bit-system-with-significant-oomph [https://perma.cc/LRV8-S76Z].

231. Peter Downey, *Watch Dogs Torrent Secretly Installing a Bitcoin Miner on Thousands of Computers*, GAMECRASTINATE (May 24, 2014), https://gamecrastinate.com/gaming-news/watch-dogs-torrent-secretly-installing-bitcoin-miner-thousands-computers [https://perma.cc/Y8XP-VB5X].

232. *Id.*

233. *Id.*

234. Chris Burns, *Watch Dogs Torrent Installs Bitcoin Miner for Unsuspecting Thieves*,

of this torrent reached approximately 40,000 users (seeders and leechers), and it was downloaded nearly 20,000 times within a single day on a single tracker.[235] Coverage of the virus typically noted that the infection was deserved or ironic (in part because the game itself is centered on hacking).[236]

2. Repack Bitcoin Miners

A related bitcoin miner[237] utilizing Trojan:Win32/Maener.A[238] was detected in repacks of eight popular games, including:

> Tom Clancy's Ghost Recon.Future Soldier.Deluxe Edition.v 1.7 + 3 DLC.(Новый Диск).(2012).Repack
> Don't Starve.(2013) [Decepticon] RePack
> Kings Bounty Dark Side by xatab
> Sniper_Elite_III_8_DLC_RePack_MAXAGENT
> TROPICO_5
> Ghost_Recon_Future_Soldier_v1.8_Repack
> Trials.Fusion.RePack.R.G.Freedom

SLASHGEAR (May 25, 2014), https://www.slashgear.com/watch-dogs-torrent-installs-bitcoin-miner-for-unsuspecting-thieves-25330425 [https://perma.cc/JY9P-9NTB].

235. Darren Pauli, *Tens of Thousands of 'Watch Dogs' Pirates ENSLAVED by Bitcoin Botmaster: Watch Dogs Fans Targeted for Access to Their Juicy GPUs*, REGISTER (May 28, 2014, 5:02 PM), http://www.theregister.co.uk/2014/05/28/watch_dogs_pirate_gamers_botnet [https://perma.cc/6BQH-4QMG] (noting "[g]amers were choice targets for Bitcoin mining malefactors because they often ran high-end graphical processing units (GPUs) and shunned resource-draining anti-virus platforms").

236. Leo Sun, *Pirating 'Watch Dogs' Could Turn Your PC Into a Bitcoin Mining Slave*, MOTLEY FOOL (May 27, 2014, 11:19 AM), http://www.fool.com/investing/general/2014/05/27/pirating-watch-dogs-could-turn-your-pc-into-a-bitc.aspx [https://perma.cc/K2RR-RSWW] (noting that justice was served to *Watch Dogs* pirates and analogizing bitcoin miners to whimsical DRM); Rob Waugh, *Watch Dogs Pirates Hit by Scurvy Bitcoin-Mining Malware*, WELIVESECURITY (May 27, 2014, 4:37 PM), http://www.welivesecurity.com/2014/05/27/watch-dogs-malware [https://perma.cc/XTZ2-W2PN] (noting "irony comes from that fact that the game itself is themed around hacking"); *Pirated 'Watch Dogs' Made a Bitcoin Mining Botnet*, DARKNET (Sept. 9, 2015), http://www.darknet.org.uk/2014/05/pirated-watch-dogs-game-made-bitcoin-mining-botnet [https://perma.cc/5VQN-KP9W] (explaining "another reason gamers make a good target as they often don't even use AV software or disable it for maximum performance").

237. *Trojan:Win32/Maener.A*, MICROSOFT (Aug. 20, 2014), https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Maener.A [https://|perma.cc/J3B8-C8ZZ].

238. Darren Pauli, *Game Pirates 'Donate' Compute Power to Bitcoin Miners*, REGISTER (Sept. 23, 2014, 5:27 PM), http://www.theregister.co.uk/2014/09/23/game_pirates_donate_compute_power_to_bitcoin_miners [https://perma.cc/8NKM-S8AQ]; Donna Sibangan, *Download at Your Own Risk: Bitcoin Miners Bundled with Game Repacks*, MICROSOFT (Sept. 9, 2014), https://cloudblogs.microsoft.com/microsoftsecure/2014/09/09/download-at-your-own-risk-bitcoin-miners-bundled-with-game-repacks [https://perma.cc/S3LH-ZJKP].

King's Bounty Dark Side.(2014) [Decepticon] RePack [239]

The total number of downloads for these files is unknown. Reports of bitcoin miners in repacks of other popular games are common, with miners detected in repacks of games in the *Attack on Titan*, *Doom*, *Fallout*, *Far Cry*, *Grand Theft Auto*, *Just Cause*, and *Tomb Raider* series.[240]

3. Multiple *Pokémon Go* Infections

The infection record of *Pokémon Go* is especially interesting, as it shows the malware risk of an unauthorized download of an otherwise free game. *Pokémon Go* was released in July 2016 and broke the App Store's one-week download record.[241] However, the app was not released in all regions simultaneously. Users who downloaded the Android Application Package (APK) directly for their Android devices were saddened to learn that the app contained Droidjack Malware.[242]

---

239. Sibangan, *supra* note 238.

240. Users have reported infections on Reddit, in the subreddit CrackStatus. *See, e.g.*, B-Knight, *[Update] The Doom Preload Files on Kat Contain Malware. Avoid for the Time Being!*, REDDIT: R/CRACKSTATUS (May 15, 2016), https://www.reddit.com/r/CrackStatus/comments/4jh7u6/update_the_doom_preload_files_on_kat_contain [https://perma.cc/ZH2H-PFGY] (noting malware in *Doom*); Kristopher Benz, *Do a Virus Scan if You've Downloaded Seyter's Repack: It Contains Bitcoin Miner*, PANJURY (Aug. 11, 2016), https://gaming|.panjury.com/verdict/post84861207535347 [https://perma.cc/8A5U-C5YV] (reporting bitcoin miner in *Rise of the Tomb Raider* repack); Cattahand, *I Found a Bitcoin Miner in My Game. You Could Have It Too*, REDDIT: R/PIRATEDGTA (Apr. 25, 2015), https://www.reddit.com/r/PiratedGTA/comments/33p7o7/i_found_a_bitcoin_miner_in_my_game_you_could_have [https://perma.cc/4LV8-RG2G] (noting Bitcoin miner in *Grand Theft Auto 5* repack and being told that user should not have downloaded no name repacks); FromThatOtherPlace, *How To Check for and Disinfect Bitcoin Miner*, REDDIT: R/CRACKSTATUS (Aug. 11, 2016), https://www.reddit.com/r/CrackStatus/comments/4x71iv/how_to_check_for_and_disinfect_bitcoin_miner [https://perma.cc/CV7J-TZ8W] (noting bitcoin miner in *Far Cry 3* and *Just Cause* repack); iPolar, *Bitcoin Miner on Attack on Titan : Wings of Freedom ^^noSTEAM^^*, REDDIT: R/CRACKSTATUS (Aug. 27, 2016), https://www.reddit.com/r/CrackStatus/comments/4zvvbb/bitcoin_miner_on_attack_on_titan_wings_of_freedom [https://perma.cc/2ACP-DKDG] (reporting bitcoin miner in *Attack on Titan: Wings of Freedom*).

241. *Should You Believe Those Pokemon Go Download Numbers?*, BBC NEWS (July 25, 2016), http://www.bbc.com/news/magazine-36868076 [https://perma.cc/6DB2-TMQP].

242. Killian Bell, *Infected Pokémon Go APKs Spread 'Droidjack' Malware on Android*, TECHNOBUFFALO (July 11, 2016), http://www.technobuffalo.com/2016/07/11/infected-pokemon-go-apks-spread-droidjack-malware-on-android [https://perma.cc/WV39-W79V]. The relative ease of installing APKs contributes to a well-known problem of malware in downloads outside of Google Play. *See Q3 Mobile Threats in Play*, F-SECURE (Nov. 13, 2012, 1:29 PM), https://www.f-secure.com/weblog/archives/00002454.html [https://perma.cc/EH6B-YP9M] (noting that from 28,398 malicious samples, 146 came from Google Play). For example, a malware riddled APK purporting to be Super Mario Run was widely available. Aaron Brown, *Super Mario Run Android Release Date - Game APK Is 'Available NOW' but Do NOT Download It*, DAILY EXPRESS (Dec. 22, 2016, 8:50 AM), http://www.express.co.uk/life-style/science-technology/745100/Super-Mario-Run-APK-Download-Release-Date [https://

Several other attempts were made by hackers to leverage the popularity of *Pokémon Go*. In August 2016, a piece of ransomware mispackaged as *Pokémon Go* targeted Arabic-speaking users.[243] In September 2016, a companion app, *Guide For Pokémon Go*, was confirmed to contain a Trojan (HEUR:Trojan.AndroidOS .Ztorg.ad) that could potentially root the device.[244] Troublingly, this app was hosted on Google Play and was downloaded approximately 500,000 times before the malware discovery.[245] Similarly, a piece of ransomware (nullbyte, a variant of DetoxCrypto) pretended to be a rebuild of the *NecroBot Pokémon Go* bot, a cheating hack that allowed users to catch *Pokémon* while not playing the game.[246]

The malware dissemination approach used for *Pokémon Go* has since spread to other highly anticipated mobile games. The vice president of research for app security company Axran noted that *Super Mario Run*:

> [a]s Nintendo's second foray into mobile gaming with one of their lead franchises, . . . is immediately going to be a prime target for attackers trying to exploit its code – especially with the number of users which will be downloading this game. Just as with the previous smash hit *Pokémon Go*, we anticipate the appearance of corrupted fake apps used to spread malware.[247]

---

perma.cc/XAH7-D3WL].

243. *PokemonGo Ransomware Comes with Some Clever Tricks*, MALWAREBYTES LABS (Aug. 22, 2016), https://blog.malwarebytes.com/threat-analysis/2016/08/pokemongo-ransomware-comes-with-some-clever-tricks [https://perma.cc/DH2T-JLGP].

244. Roman Unuchek, *Rooting Pokémons in Google Play Store*, SECURELIST (Sept. 14, 2016, 11:50 AM), https://securelist.com/blog/mobile/76081/rooting-pokemons-in-google-play-store [https://perma.cc/9FK3-3MR9]. The infection of companion apps to popular games has been widely observed. In 2014, a companion hack app for the popular game *Hearthstone* was infected with a Trojan. Luke Parker, *Bitcoin Stealing Malware Evolves Again*, BRAVE NEW COIN (Feb. 11, 2016), http://bravenewcoin.com/news/bitcoin-stealing-malware-evolves-again [https://perma.cc/23E9-FXKS].

245. *Guide for Pokémon Go Trojan Catches Pokémon Trainers*, KASPERSKY LAB (Sept. 14, 2016), https://blog.kaspersky.com/pokemon-go-malware/12953 [https://perma.cc/KHD5-FXPB].

246. Lawrence Abrams, *The Nullbyte Ransomware Pretends To Be the NecroBot Pokemon Go Application*, BLEEPING COMPUTER (Sept. 1, 2016, 12:02 PM), https://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application [https://perma.cc/5HPZ-6GHE]; Steven Asarch, *'Pokémon Go' Necrobot Shuts Down, Cheating Software Removed by Developers*, PLAYER.ONE (Aug. 12, 2016), http://www.player.one/pokemon-go-necrobot-shuts-down-cheating-software-removed-developers-550219 [https://perma.cc/2493-3WRV] (describing Necrobot as a cheating device). Security firms report that hacks are frequently infected, though the wider gamer community largely mocks this belief. Pierluigi Paganini, *Almost All Game Hacks Are Infected with Malware*, SECURITY AFF. (Apr. 17, 2013), http://securityaffairs.co/wordpress/13640/malware/almost-all-game-hacks-are-infected-with-malware.html [https://perma.cc/9BU3-HRV7] (noting that "90% of hacked or cracked games downloaded via file-sharing sites are infected with malicious code").

247. Brown, *supra* note 242.

4. Coverage of Video Game Malware

Stories of pirate losses due to malware are widely reported as deserved punishments, even in the face of disproportionate damage. A report of a potential bitcoin raider linked to a pirated copy of *Fallout 4* occasioned a great deal of media coverage framing the loss as karmic justice.[248] The treatment of these stories, involving the theft of thousands of dollars of a pirating user's property, is problematic because they fail to address the wider social cost of malware.

So-called piracy-punishing malware is not new. In 2010, malware in the erotic game *Cross Days* sought to humiliate pirates:

> the installer pretends to be the game but using personal information gathered from the victim's computer (including IP address), it presents a survey which asks for more personal information – including their email address and password. Once completed, the information is uploaded to a website for all the Internet to see – accompanied by a screenshot of the victim's desktop.[249]

G. Torrent Takedowns Exacerbate Viral Threat

Efforts to stop piracy by targeting torrent sites have been ineffective and deleterious in light of the viral threat. Repeated tracker takedowns have shown that they have a negligible impact on overall torrenting traffic. Moreover, the pulling down of tracker infrastructure removes reputational barriers that prevent viral spread.

---

248. *See* Bohs Hansen, *Fallout 4 Pirate Learns Expensive Lesson as Bitcoins Go Missing*, ETEKNIX, http://www.eteknix.com/fallout-4-pirate-learns-expensive-lesson-as-bitcoins-go-missing [https://perma.cc/LMQ7-9BJ7] (describing loss as "expensive lesson"); Duncan Riley, *Bitcoin Stolen via Malware-Infect Pirated Copy of Fallout 4*, SILICONANGLE (Dec. 2015, 11:12 PM), http://siliconangle.com/blog/2015/12/06/bitcoin-stolen-via-malware-infected-pirated-copy-of-fallout-4 [https://perma.cc/LD67-SHYJ] ("[T]he irony of the situation here is that [the poster], in this case, could have purchased Fallout 4 for far, far less than the amount he had stolen."); Geoffrey Tim, *Pirated Copy of Fallout 4 Ends Up Being Really, Really Expensive*, CRITICAL HIT GAMING (Dec. 7, 2015), https://www.criticalhit.net/gaming/pirated-copy-fallout-4-ends-really-really-expensive [https://perma.cc/6R8M-TXL5] ("It's the most beautiful sort of instant karma."); Ryan Whitwam, *Fallout 4 Pirate Gets Instant Karma When His Bitcoins Are Stolen*, GEEK.COM (Dec. 6, 2015, 11:31 AM), http://www.geek.com/games/fallout-4-pirate-gets-instant-karma-when-his-bitcoins-are-stolen-1641350 [https://perma.cc/8F3V-J66Q] (describing loss of approximately $2000 worth of bitcoin as karmic justice). *But see Bitcoin Stealing Malware Attacks Gamers*, ALTCOIN TODAY (Dec. 15, 2015), http://www.altcointoday.com/bitcoin-stealing-malware-attacks-gamers [https://perma.cc/NX6V-JHBV] (treating matter seriously).

249. Enigmax, *Fake Game Installer Punishes Pirates via Epic Privacy Breach*, TORRENTFREAK (Mar. 23, 2010), https://torrentfreak.com/fake-game-installer-punishes-pirates-via-epic-privacy-breach-100323 [https://perma.cc/2TBR-4BFJ]. Another interesting example involved an infected screensaver containing a virus threatening P2P users with death. Enigmax, *Bizarre Virus Threatens To Kill File-Sharers*, TORRENTFREAK (Mar. 1, 2007), https://torrentfreak.com/bizarre-virus-threatens-to-kill-file-sharers [https://perma.cc/2TUC-83L4].

1. Takedowns Do Not Decrease Torrent Traffic

While governments have succeeded in shutting down particular trackers, including Suprnova,[250] EliteTorrents,[251] BtJunkie[252] and Demonoid,[253] the effects of these shutdowns have been negligible.[254] When a torrent tracker is taken down, traffic to other torrent trackers spikes. The futility of this exercise is frequently noted, with commentators likening it to whack-a-mole.

An analysis of the KickassTorrents shutdown helps demonstrate this trend. KickassTorrents was shut down on July 20, 2016. The next day saw a sustained spike in Google searches of the term "torrent sites."[255] Unsurprisingly, other trackers saw large boosts in visits in the immediate aftermath. The Pirate Bay saw an increase of

---

250. *See, e.g.*, Van der Sar, *supra* note 99 (noting that the sites servers were seized by Slovenian police in cooperation with a French antipiracy group); *File-Swap Site Folds for Good*, WIRED (Dec. 20, 2004, 1:53 PM), http://www.wired.com/entertainment/music/news/2004/12/66099 [https://perma.cc/F2QP-QVGM].

251. Enigmax, *Dramatic BitTorrent Site Shutdowns of the Decade*, TORRENTFREAK (Dec. 31, 2009), http://torrentfreak.com/dramatic-bittorrent-site-shutdowns-of-the-decade-091231 [https://perma.cc/RE3A-BW5U]; Jon Healey, *U.S. Shuts Website in Piracy Crackdown*, L.A. TIMES (May 26, 2005), http://articles.latimes.com/2005/may/26/business/fi-torrent26 [https://perma.cc/S2GJ-GWJD].

252. *BTJunkie Shuts Down over Fears of Legal Action*, WEBPRONEWS (Feb. 6, 2012), http://www.webpronews.com/btjunkie-shut-down-2012-02 [https://perma.cc/Q6V5-H7PH] (voluntarily shut down after megaupload's take down, leaving with the note: "This is the end of the line my friends. The decision does not come easy, but we've decided to voluntarily shut down. We've been fighting for years for your right to communicate, but it's time to move on. It's been an experience of a lifetime, we wish you all the best!"); Ernesto Van der Sar, *BitTorrent Giant BTjunkie Shuts Down for Good*, TORRENTFREAK (Feb. 6, 2012), http://torrentfreak.com/btjunkie-shuts-down-for-good-120206 [https://perma.cc/9SAZ-2PBH].

253. Adrian Covert, *Ukraine Officials Shut Down Demonoid To Impress US Government*, GIZMODO (Aug. 6, 2012, 11:36 AM), http://gizmodo.com/5932143/ukraine-officials-shut-down-demonoid-to-impress-the-us-government [https://perma.cc/YYL2-48FD] (noting that the site's servers were seized by the Ukrainian government as a good will gesture to the United States); Enigmax, *Demonoid Busted as a Gift to the United States Government*, TORRENTFREAK (Aug. 6, 2012), http://torrentfreak.com/demonoid-busted-as-a-gift-to-the-united-states-government-120806 [https://perma.cc/EN2G-4UGQ].

254. Sebastian Anthony, *BitTorrent Usage Increases in Europe, Following the Blockade of The Pirate Bay*, EXTREMETECH (July 5, 2012), http://www.extremetech.com/extreme/132328-bittorrent-usage-increases-in-europe-following-the-blockade-of-the-pirate-bay [https://perma.cc/MFC5-3AG9] (noting that European bittorent use actually increased after the blocking of the most popular bittorrent tracker, The Pirate Bay); Paul Resnikoff, *The MegaUpload Shutdown Hasn't Reduced File-Trading at All . . .*, DIGITAL MUSIC NEWS (Feb. 10, 2012), https://web.archive.org/web/20120502055118/http://www.digitalmusicnews.com/permalink/2012/021012postmegaupload [https://perma.cc/HZL6-B5YW] (noting that though global internet traffic decreased by 2% after the closure of megaupload, full traffic resumed shortly thereafter).

255. *Number of Searches for "Torrent Sites" After Shutdown of KickassTorrents*, GOOGLE TRENDS, https://trends.google.com/trends/explore?date=2016-06-01%202016-08-25&q=Torrent%20Sites [https://perma.cc/9V5P-FHGK].

67%, ExtraTorrent saw an increase of 101%, while "RARBG, 1337x.to and YTS.ag, saw their visitor numbers go up by 45%, 53%, and 44% respectively."[256] "With millions of people moving to new sites, it's safe to say that the torrent 'community' is in turmoil, trying to find a new status quo."[257] The takedown of KAT was fairly short lived, as numerous site members migrated to KATcr.co, a successor site, just a few months after KAT's demise.[258]

In 2014 and 2015, a similar pattern attended the takedown of the Swedish domains for The Pirate Bay.[259] Immediately before the takedown of the popular tracking site, 101.5 million unique IP addresses were reportedly engaged in torrenting content.[260] Immediately after the seizure, that number dropped to 95 million, but rebounded to 99 million in two days. Temporary disruption and displacement traffic also happened upon the shutdown of MegaUpload[261] and the Italian domain of The Pirate Bay.[262]

When authorities lack the means to pulldown entire tracking sites, they may instead block these sites at the domain level. In response, users will often rely on proxies and seek out mirrors. But these proxies are rife with malware.[263] The continued survival of The Pirate Bay, perhaps the most well-known torrent site, demonstrates the difficulty of terminating the reach of a global site. The Pirate Bay is currently operating from the Swedish domain, thepiratebay.se, and has previously been registered in the following sixteen top-level domains: .GL, .IS, .SX, .AC, .PE, .GY, .AM, .LA, .GD, .MN, .VG, .FM, .SH, .MU, .TW, and .MS. Indeed, the USTR unlawful market report notes "[d]espite enforcement actions around the world and drawn-out legal battles against its operators, The Pirate Bay is of symbolic importance as one of the longest-running and most vocal torrent sites for admittedly illegal downloads."[264]

---

256. Van der Sar, *supra* note 105.

257. *Id.*

258. Ernesto Van der Sar, *KickassTorrents Brought Back to Life by Original Staffers (Updated)*, TORRENTFREAK (Dec. 16, 2016), https://torrentfreak.com/kickasstorrents-brought-back-to-life-by-original-staffers-161216 [https://perma.cc/UW5S-6VCQ].

259. *See* James Geddes, *Kickass Torrents, Torrentz Take Over as Court Orders the Pirate Bay Shutdown*, TECH TIMES (May 19, 2015, 8:35 PM), http://www.techtimes.com/articles/54033/20150519/kickass-torrents-torrentz-take-over-as-court-orders-pirate-bay-shutdown.htm [https://perma.cc/S7ZL-7VV4].

260. Todd Spangler, *Pirate Bay Shutdown Has Had Virtually No Effect on Digital Piracy Levels*, VARIETY (Dec. 13, 2014, 11:11 AM), https://variety.com/2014/digital/news/pirate-bay-shutdown-has-had-virtually-no-effect-on-digital-piracy-levels-1201378756 [https://perma.cc/5WBX-JRCW].

261. *See* Kevin Fogarty, *MegaUpload Takedown Didn't Slow Pirate Downloads, Just Moved Them Offshore*, ITWORLD (Feb. 7, 2012), http://www.itworld.com/article/2732230/security/megaupload-takedown-didn-t-slow-pirate-downloads--just-moved-them-offshore.html [https://perma.cc/6XYU-5X4V].

262. *See* Ernesto Van der Sar, *Blocked Pirate Bay Users Flock to Other Torrent Sites*, TORRENTFREAK (Feb. 16, 2010), https://torrentfreak.com/blocked-pirate-bay-users-flock-to-other-torrent-sites-100216 [https://perma.cc/53DN-9LTA].

263. Ernesto Van der Sar, *Torrent Site Proxies Rife with Malware Injecting Scripts*, TORRENTFREAK (Aug. 6, 2015), https://torrentfreak.com/torrent-site-proxies-rife-with-malware-injecting-scripts-150806 [https://perma.cc/A7R9-USAD].

264. OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 106, at 14.

The total amount of data shared by users also indicates that the torrent pulldown campaign has done little to push down overall torrent traffic. File-sharing increased in North America by 44%, from 555 petabytes to 797 petabytes during the five-year period of frequent torrent takedowns (2008 to 2013).[265] Even the most optimistic forecasters attribute a slight decrease in torrent traffic to Netflix rollout and bandwidth management.[266]

2. Takedowns Strip Antiviral Reputation Barriers

While it seems clear that the takedown of any one torrent site has a minor impact (if any) on overall torrent traffic, the removal of a site is not without consequence. When major torrent sites go down, reputational infrastructure and capital is pulled down with them.[267] This should be of special concern in light of pirates' reliance on that infrastructure to prevent malware infection.

When a torrent site goes dark, users no longer have access to several reputational tools that aid in preventing the spread of malware. As an initial matter, users lose access to message board or comment sections for individual torrents. These message boards host information relating to the release, including aspects related to viral spread (the type of virus detectors used on the product, a history of clean releases from the scene group or from the uploader, and likely false positives). Of course, the most obvious aspect is a warning that malware has been detected in the subject torrent. Another important function, though, is warning users of other malware-infected releases for the same title. It is common to see, by way of thanks, comments noting that a torrent is not infected while similar torrents are.

Torrent trackers also have individual administrators, moderators, and forum members policing content. Specific forum members are referred to as power users, who have earned special privileges through seeding, longevity in the community, and by invitation from tracker moderators.[268] Depending on the hierarchy of the tracker, power users may accrue privileges to view torrents early and the ability to delete torrents. In effect, power users may function as moderators. These users frequently

---

265. Steele, *supra* note 63.

266. Matt Hickey, *Netflix: "We Kill Piracy!"; BitTorrent: "Yeah, so, About That Piracy Thing?,"* FORBES (May 7, 2013, 11:40 PM), http://www.forbes.com/sites/matthickey/2013/05/07/netflix-we-kill-piracy-bittorrent-yeah-so-about-that-piracy-thing/#3df41184294c [https://perma.cc/7YBY-UHMN] (noting that "the Micro Transport Protocol, which works to reduce BitTorrent traffic during times of peak Internet usage to give priority to other types of Internet activity – such as that utilized by Netflix. When people use apps like Netflix, then, yes, the BitTorrent traffic is reduced, but not because Netflix is replacing piracy, but because the protocol is designed to work that way."); Glenn Peoples, *Business Matters: How Netflix Reduces Piracy*, BILLBOARD (May 6, 2013, 5:15 PM), http://www.billboard.com/biz/articles/news/digital-and-mobile/1560720/business-matters-how-netflix-reduces-piracy [https://perma.cc/3MVH-M89H].

267. Van der Sar, *supra* note 263.

268. rackzone, *How To Become a Power User on Specific Trackers*, TORRENT-INVITES (Jan. 25, 2013), http://www.torrent-invites.com/bittorrent/232092-power-user-specific-trackers.html [https://perma.cc/38QA-CB39] (collecting comprehensive information on trackers' classes of members, privileges, and requirements).

are the first "tasters" of content; their delivery priority serving as an important first indicator of safety and quality.

Just as individual actors on a torrent site have reputations to protect and uphold within that community, so too do the torrent sites themselves. While it is by no means clear that an established site is immune to hosting malware, for example several torrent sites were black listed by browsers,[269] it is widely believed that novel torrent sites are infectious. Indeed, commentators assume that a number of "scam" torrent sites will appear in the immediate aftermath of a site shutdown, as displaced pirates visit several new torrent sites.[270] A common complaint of leechers is that the search for a new torrent site exposes them to malware. For example, in the comment thread announcing the pulldown of KickassTorrents, numerous users complained: "So I checked out 'Torlock' in the link above. Practically every place I clicked on their site took me to ransomware or some other browser-hijacking malware operation."[271] Indeed, it is for this reason that torrent sites may warn users of using malicious copycat sites.[272]

3. Takedowns Weaken Trust in Other Diversion Efforts

The entertainment industry is already attempting to use the viral threat as a means to reduce piracy.[273] However, these efforts are unlikely to be successful and may in fact undermine attempts to curb viral spread. It is already clear that pirates regard antiviral efforts as disingenuous antipiracy efforts, considering the spread of false positives as directed and deliberate.[274] Indeed, mainstream commentators have made

---

269. Liam Tung, *Pirate Bay Visitors Infected with Crypto-Ransomware via Bad Ads*, ZDNET (Apr. 27, 2016, 11:26 AM), http://www.zdnet.com/article/pirate-bay-visitors-infected-with-crypto-ransomware-via-bad-ads [https://perma.cc/5JQ9-W55L].

270. *See* Ernesto Van der Sar, *Scammers Take Over Popular KickassTorrents 'Mirror*,*'* TORRENTFREAK (Aug. 10, 2016), https://torrentfreak.com/scammers-take-kickasstorrents-mirror-160810 [https://perma.cc/X6PN-TX7N].

271. Papoukla, Comment to *Top Torrent Sites See Traffic Surge After 'Shutdowns*,*'* TORRENTFREAK (Sept. 3, 2016), https://torrentfreak.com/top-torrent-sites-see-traffic-surge-shutdowns-160903 [https://perma.cc/KHR9-VXWT]; *see also* George Brand, *supra* note 207 ("Yes, these torrent sites can act weird sometimes. Make sure you are fully armored when you visit them. Use a browser like Firefox, sandboxed if possible, with a good ad-blocker and flash blocker.").

272. Ernesto Van der Sar, *KickassTorrents Warns Users of "Malicious" Copycats*, TORRENTFREAK (Oct. 9, 2015), https://torrentfreak.com/kickasstorrents-warns-users-of-malicious-copycats-151009 [https://perma.cc/K8JR-6RJ8].

273. Leigh Alexander, *Spore & Piracy: EA, ESA, Analysts Weigh in*, GAMASUTRA (Sept. 29, 2008), http://www.gamasutra.com/php-bin/news_index.php?story=20424 [https://perma.cc/PGL2-MBVF] (noting pirated version of Spore contained a virus); Ryan Faughnder, *Piracy Sites Tempt Users with Free Movies as Malware Lies in Wait, Report Says*, L.A. TIMES (July 27, 2016), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-piracy-malware-20160718-snap-story.html [https://perma.cc/9K7J-HSPX].

274. *See, e.g.*, Ben Jeremy, Comment to *Antivirus Software Starts Blocking Pirate Websites*, TORRENTFREAK (Feb. 4, 2014), https://torrentfreak.com/anti-virus-pirate-block-140204 [https://perma.cc/7PRA-KBUP] ("How about a switch to disable those false positives on keygens or patchers? One thing that is my biggest pet peeve about AV software is when it

identical arguments, comparing warnings of malware to prohibition-motivated, exaggerated side effect warnings employed by the government in the War on Drugs.[275] The pulldown of torrent sites gives lie to industry efforts to frame their actions as designed to prevent viruses rather than infringement.

III. PROPOSED SOLUTIONS—COMPREHENSIVE HARM REDUCTION

Attempts to stymie piracy by eliminating pirate platforms have been ineffective at best and deleterious to antimalware operations at worst. Concerned actors should instead launch harm-reduction campaigns. These of course could include warnings and requests to forgo piracy. But if pirating sites will be used, a series of best practices to minimize user and social harm should be developed. This viral targeting would consist of two main avenues: (1) restoring user confidence in the veracity of viral warnings, and (2) reducing the supply of cracks through the use of time-limited, robust DRM.

A. Underlying Principles of a Harm Reduction Approach

In the case of video game piracy, efforts to stop piracy have largely failed while simultaneously exacerbating viral threat. Instead of repeated application of deleterious policies, the problem of video game piracy should be examined through harm-reduction principles. While first coined in relation to drug addiction[276] and later applied to sexual behaviors, harm reduction is any program or policy designed to reduce

---

triggers false positives on keygen programs . . . to me, this is akin to sending a man to the electric chair for a murder he didn't commit, that you know he didn't commit. These false positives make me question the validity of the AV software in general. Note to AV software developers: Stop obfuscating your attempts to thwart piracy! Make it clear that you are merely warning because it is potentially infringing, and give me the option of ignoring the warning or turning it off entirely for that class of software!!"); Ben Kuchera, *EA DRM Can't Accomplish Job One: 500K Spore Torrents So Far*, ARS TECHNICA (Oct. 2, 2008), http://arstechnica.com/gaming/2008/10/ea-drm-cant-accomplish-job-one-500k-spore-torrents-so-far [https://perma.cc/HR98-BBDC] ("The 'pirated copies are riddled with viruses' argument is the same scare tactic police used to tell schoolchildren during D.A.R.E. class: you shouldn't buy drugs because you never know what's in it. The truth is that people who create the pirated versions of these games and the groups that spread them live and die by their reputations, and are sophisticated enough to make sure nearly every file is clean."); MrTom4, Comment to *Malicious Torrent Network Tool Revealed by Security Company*, TORRENTFREAK (Sept. 21, 2016), https://torrentfreak.com/malicioubs-torrent-network-tool-revealed-by-security-company-160921 [https://perma.cc/4EB6-6WAE] ("Now that's one way to virtually stop software piracy. Pollute the whole ecosystem and get the word out to everyone. Make sure everyone knows you'll most likely get infected downloading software. Good job."); Ernesto Van der Sar, *Warning: Don't Visit Torrent Sites, You May Catch a Virus*, TORRENTFREAK (Jan. 21, 2011), https://torrentfreak.com/warning-dont-visit-torrent-sites-you-may-catch-a-virus [https://perma.cc/F4Q5-S2XW] (mocking virus warnings throughout article and concluding "[o]h yeah, and you shouldn't play any games either").

275. *See, e.g.*, Kuchera, *supra* note 274.

276. Gordon Roe, *Harm Reduction as Paradigm: Is Better than Bad Good Enough? The Origins of Harm Reduction*, 15 CRITICAL PUB. HEALTH 243, 243 (2005).

behavior-related harm that does not require immediate cessation of that behavior.[277] The main principles of harm reduction are pragmatism,[278] focus on harm, prioritization of goals, flexibility, autonomy, and evaluation.

Pragmatism. It is apparent that video game piracy is widespread and that some users will choose to pirate content, should that content be available.[279] Methods such as three-strikes internet cessation,[280] individual lawsuits, and torrent site takedowns have done little to ameliorate piracy rates. Rather than focusing on a zero-piracy society, we should acknowledge that some piracy is likely to continue and reduce the harms attendant to that activity.

Focus on Harm. The harmful consequences of video game piracy have not been fully appreciated, with a focus on lost sales by the IP rights holder. While piracy may negatively impact the market for a good, it also threatens the pirating user, as well as cyber security and network infrastructure.

Prioritization of Goals. While the wider goal of lessening piracy remains important, the intermediate goal of society at large and the pirate community should be in protecting network infrastructure and users from malware. The ultimate goals of the two communities diverge, but the priority should be on the immediate, shared, and realizable goal of lowering the malware threat.

Flexibility. The suggested approach encourages pirating communities to aid in malware policing and may potentially allow in-roads with pirating users. The dynamic response of users to torrent site shutdowns has demonstrated that a singular approach is unlikely to succeed.

Autonomy. Pirate users have circumvented antiviral measures that they perceive to be antipiracy attempts. A decoupling of antipiracy and antimalware campaigns will engage users and present them with greater agency for risk avoidance. A better informed and more trusting user may elect not to engage in high-risk torrenting behavior.

Evaluating. The goal of the campaign, the reduction of malware spread, may be evaluated by measuring reported infection rates and monitoring piracy forums.

---

277. *CAMH and Harm Reduction: A Background Paper on Its Meaning and Application for Substance Use Issues*, CTR. FOR ADDICTION & MENTAL HEALTH (May 2002), http://www.camh.ca/en/hospital/about_camh/influencing_public_policy/public_policy_submissions/harm_reduction/Pages/harmreductionbackground.aspx [https://perma.cc/U8DQ-EJF6].

278. In the context of addiction, this is typically termed compassionate pragmatism as contrasted with moralistic paternalism. *Id.*

279. *See* Moshirnia, *supra* note 6, at 41–44 (providing examples of users pirating content that would cost one penny, less than the labor cost of piracy).

280. *See* Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW 185 (John A. Rothchild ed., 2016); Andrew Moshirnia, *UN Disapproves of Three Strikes Digital Executions*, DIGITAL MEDIA L. PROJECT (June 22, 2011), http://www.dmlp.org/blog/2011/un-disapproves-three-strikes-digital-executions [https://perma.cc/P2JJ-6WYH] (noting that the UN "Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights").

B. Proposal Plank 1: Minimizing Malware Spread by Increasing User Confidence in Viral Warnings

Users currently have three separate levels of viral warnings, which are actively disregarded or undermined in current antipiracy practice. Users receive warnings at the browser level when a site is blacklisted, at the forum level when other users warn of viral content in torrent message boards, and at the machine level in the form of desktop antivirus programs or virus detectors. This proposal suggests intervention on all three levels.

1. Forbearance in Tracker Takedowns and Redirects

As should be fairly evident, the takedown of various torrent sites has done little to stem piracy. Moreover, these attempts increase viral threat by stimulating the demand for malware-riddled proxies[281] or less-well-known torrent trackers,[282] while decreasing the reputational barriers to viral infection. The removal of any one "notorious market" does little in the overall scheme of things.[283] Moreover, the game of whack-a-mole is doubly costly—the efforts are largely wasted while increasing the social cost of piracy and weakening the credibility of malware warnings.

In light of these problems, there should be forbearance in seeking torrent tracker shutdowns. The record of server relocation indicates that this problem requires widespread international cooperation.[284] While the ultimate goal of removing trackers need not be abandoned and a more comprehensive solution should be explored in international agreements,[285] the current piecemeal approach to torrent tracker shuttering or redirecting must stop.

2. Increasing Transparency in the Blacklist Process

When users are faced with a blacklist or redirect when entering a site, they frequently react by bypassing the warning or by using proxies to reach the desired content. When Google Chrome and Firefox repeatedly flagged KickassTorrents in 2015, the community reacted with confusion and distrust.[286] In April 2015,

---

281. *See* Van der Sar, *supra* note 263.

282. Van der Sar, *supra* note 262.

283. Steele, *supra* note 63.

284. *See supra* note 142 and accompanying text (discussing Dridex); *see supra* note 260 and accompanying text (discussing The Pirate Bay).

285. While commentators have noted that a multilateral treaty on secondary liability may address the torrent issue, *see, e.g.*, Scott Burger, *Eradication of a Secondary Infringer's Safe Havens: The Need for a Multilateral Treaty Addressing Secondary Liability in Copyright Law*, 18 MICH. ST. J. INT'L L. 143 (2009), an analysis of the feasibility of this ultimate step is beyond the scope this Article. It is worth noting that torrent trackers are not strictly necessary due to trackerless torrents. *See supra* note 55. Arguments could be made that a global pulldown of tracker sites would inconvenience pirating users but at the cost of removing other safeguards provided by torrent communities.

286. Ernesto Van der Sar, *Chrome and Firefox Block KickassTorrents Over "Harmful Programs,"* TORRENTFREAK (Oct. 9, 2015), https://torrentfreak.com/chrome-and-firefox-

KickassTorrents was flagged as a "phishing" site.[287] The site was also removed from Google search results that July for similar reasons.[288] Both of these were due to the presence of malicious advertisers. The rapid removal of the blacklist further advanced the notion that the takedown was motivated by antipiracy, rather than antiviral concerns.[289] In light of the wave of blacklisting of The Pirate Bay and KickassTorrents, commentators noted that "Chrome and Firefox users should be familiar with these intermittent warning notices as well, and can take steps to bypass the blocks if they are in a gutsy mood."[290]

The process could be improved by providing users with more specifics as to the types of threats encountered on the site and the reason for the listing. Specifics would allow users to better assess the risk of using the site and also allow them to conduct antiviral countermeasures, such as using an ad-block, script-block, or flash-block. This reasoning would also reinforce the message that the site is being blocked for reasons unrelated to pirated content.

3. Refining Virus Detectors

While the use of virus detectors is never perfect, pirating users frequently disable their antivirus software in order to install cracked software. Existing virus detectors could be improved to better categorize the likely threats in cracked software, identifying known cracking methods and incorporating those into the analysis presented to the user. This may have fairly weak impact due to the difficulty in detecting novel malware, but it may do more to convince pirates that antiviral efforts are not always motivated by antipiracy concerns.

C. Proposal Plank 2: Use of Robust, Temporary DRM To Limit Malware-Delivering Cracks

Recognizing the importance of reputational barriers and stopping futile tracker pulldowns should not be confused with simply waving the white flag to piracy in the

---

block-kickasstorrents-over-harmful-programs-151009 [https://perma.cc/7G6Z-AR35]; Ernesto Van der Sar, *Chrome, Firefox and Safari Block KickassTorrents as "Phishing" Site*, TORRENTFREAK (Apr. 12, 2016), https://torrentfreak.com/chrome-and-firefox-block-kickasstorrents-as-phishing-site-160412 [https://perma.cc/QUA8-CPNT] (noting "[i]mpatient or adventurous users who want to bypass the warning can do so by disabling their browser's security warnings altogether in the settings, at their own risk of course" with a comment section debating whether blacklists were due to piracy, overzealous google blocking, or legitimate antiviral concerns).

287. Van der Sar, *Chrome, Firefox and Safari Block KickassTorrents as "Phishing" Site*, *supra* note 286.

288. Vijay, *Google Removes Kickass Torrents From Its Search Results*, TECHWORM (July 18, 2015), http://www.techworm.net/2015/07/google-removes-kickass-torrents-from-its-search-results.html [https://perma.cc/QM6Z-SDZ7].

289. *Id.*

290. Van der Sar, *Chrome and Firefox Block Pirate Bay Over "Harmful Programs*," *supra* note 286.

short term. Instead, a main focus of antipiracy efforts (aside from fairly costless appeals to users to not pirate)[291] should be in reducing the amount of cracked software available. This may be accomplished by encouraging the use of robust, time-limited DRM, as this will (1) reduce the flow of cracks for newly released games and (2) remove the necessity (and thus the market) for cracks of games outside of the initial purchase window.

Government assistance in the development of robust DRM will be crucial, either through direct deployment of cyber security resources, subsidy, or simply greater information sharing. To date, the government's role in supporting DRM has been to criminalize circumvention under the Digital Millennium Copyright Act, § 1201.[292] This section was heavily lobbied by the entertainment industry.[293] However, there are strong arguments that this measure is an unconstitutional restriction on speech and actually restricts DRM improvement by limiting civil research.[294] In effect, the section provides additional legal tools in an attempt to dissuade piracy, but does so at the expense of iterative DRM development.[295]

---

291. It is worth noting that the industry has been making these sorts of appeals for decades. The most famous of these being the "Piracy. It's a Crime" series, which likened movie downloading to stealing movies and cars. *See* Jeff, *Piracy, It's a Crime*, STRATEGIC RETREAT (Nov. 14, 2007), http://thestrategicretreat.com/piracy-its-a-crime [https://perma.cc/MMK2-X9DC]. This campaign was widely mocked in the internet meme "You wouldn't download a car." Ernesto Van der Sar, *Porsche Proves MPAA Wrong, Wants You To Download a Car*, TORRENTFREAK (Dec. 17, 2013), https://torrentfreak.com/porsche-proves-mpaa-wrong-wants-you-to-download-a-car-131217 [https://perma.cc/UN5L-TN9X]; *Piracy, It's A Crime*, KNOW YOUR MEME, http://knowyourmeme.com/memes/piracy-it-s-a-crime [https://perma.cc/V5E4-DGDT].

292. 17 U.S.C. § 1201(a)(1) (2012) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title.").

293. Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121, 135–38 (2006).

294. For an excellent analysis of this issue, see Rebecca Tushnet, *I Put You There: User-Generated Content and Anticircumvention*, 12 VAND. J. ENT. & TECH. L. 889 (2010); *see also* Complaint for Declaratory and Injunctive Relief, Green v. Dep't of Justice, Case No. 1:16-cv-01492 (D.D.C. 2016), https://www.eff.org/files/2016/07/21/1201_complaint.pdf [https://perma.cc/SK4U-XXGR]; Jerome H. Reichman, Graeme B. Dinwoodie & Pamela Samuelson, *A Reverse Notice and Takedown Regime To Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 1013 (2007) (noting the provision "shamelessly sacrificed the public interest provisions of copyright law"); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L.J. 519, 538 (1999); Joe Mullin, *EFF Sues US Government, Saying Copyright Rules on DRM Are Unconstitutional*, ARSTECHNICA (July 22, 2016), https://arstechnica.com/tech-policy/2016/07/eff-sues-us-government-saying-copyright-rules-on-drm-are-unconstitutional [https://perma.cc/FQ22-G9NQ].

295. For a greater exploration of § 1201's chilling effect on scientific research, see ELEC. FRONTIER FOUND., UNINTENDED CONSEQUENCES: TWELVE YEARS UNDER THE DMCA (2010), https://www.eff.org/wp/unintended-consequences-under-dmca [https://perma.cc/2DWS-JA4S].

In light of the security threat attendant to video game piracy, the government must rethink its DRM stance. The government must rescind or clarify the anticircumvention provision, or at the very least grant permanent, blanket exemptions to researchers with respect to the provision in the interest of national security.[296] Additionally, the government should increase information sharing so that developers and the public may benefit from the government's expertise in encryption and foreign malware, respectively. Lastly, the government may directly subsidize DRM research.

While a technologically impervious DRM is unlikely to arise,[297] the recent cases involving Denuvo DRM show promise in reducing piracy of sought-after games. The DRM of *Doom*, one of the most highly anticipated games of the year, held up for approximately four months.[298] After the scheme had been broken, the DRM was removed from this version of the game.[299] The new generation of Denuvo DRM has

---

296. The current exemption for good faith security researchers may represent a small step in the right direction, though it has several troubling limitations, not least of which is that it must be renewed every three years. *See* Aaron Alva, *DMCA Security Research Exemption for Consumer Devices*, FTC (Oct. 28, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices [https://perma.cc/A3NC-BNBG]; Tom Spring, *EEF Files Lawsuit Challenging DMCA's Restrictions on Security Researchers,* THREATPOST (July 21, 2016), https://threatpost.com/eff-files-lawsuit-challenging-dmcas-restrictions-on-security-researchers/119410 [https://perma.cc/Q28H-NEE2].

> (i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986, as amended and codified in title 18, United States Code; and provided, however, that, except as to voting machines, such circumvention is initiated no earlier than 12 months after the effective date of this regulation, and the device or machine is one of the following: (A) A device or machine primarily designed for use by individual consumers (including voting machines); (B) A motorized land vehicle; or (C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care. (ii) For purposes of this exemption, "good-faith security research" means accessing a computer program solely for purposes of good-faith testing, investigation and/or correction of a security flaw or vulnerability, where such activity is carried out in a controlled environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.

37 C.F.R. § 201.40 (2018).

297. *See* Moshirnia, *supra* note 6, at 7; Peter K. Yu, *Anticircumvention and Anti-Anticircumvention*, 84 DENV. U. L. REV. 13 (2006).

298. Andy, *Denuvo: We Don't Give Refunds When Games Get Cracked*, TORRENTFREAK (Dec. 19, 2016), https://torrentfreak.com/denuvo-we-dont-give-refunds-when-games-get-cracked-161219 [https://perma.cc/7K4Y-X57J].

299. Kyle Orland, *After Cracks, Developers Remove Denuvo DRM from Their Games*, ARSTECHNICA (Dec. 9, 2016), http://arstechnica.com/gaming/2016/12/after-cracks-

produced several notable successes, including *Rise of the Tomb Raider*, which remained uncracked for 193 days. However, the rapid cracking (within six weeks) of *Inside*, another game with Denuvo DRM, may mean that Denuvo's streak of successful DRM may be broken.[300] While short-lived, the period of Denuvo DRM imperviousness motivated scene closures.[301]

At the same time, it is clear that any DRM will eventually be cracked. By removing DRM after a set amount of time (the month-long initial sale's window),[302] companies may dramatically shorten the cracking opportunity for scene members and garner goodwill with anti-DRM consumers. A voluntary removal of DRM would also lessen speech concerns attendant to DRM's perception as a barrier to user-created, fair-use products, such as modifications within games.[303] This would further undermine pro-piracy claims that piracy is necessary to protect consumers from DRM. At a minimum, a decision to drop DRM would remove the necessity for cracks to install an unlicensed copy of the game. While users may still elect to pirate the game, they would do so with diminished viral threat.

Though there may be concern that purchasers would be put off by the knowledge that their early purchase would be saddled with DRM, this would not likely result in widespread decisions not to buy products during the initial DRM-window. Consumers are already aware that first purchasers typically pay more for a less valuable product, as initial releases come with higher prices and will have bugs that will be patched only later.

D. Reasons To Adopt Harms Reduction Proposal

The approach suggested above eliminates a wasteful torrent takedown and redirect strategy that has yielded little in the way of actual piracy reduction. Moreover, the approach addresses a neglected concern that will only gain in importance as national cyber security is threatened at home and abroad. Finally, the approach may offer an important inroad to the wider pirating community, allowing for more effective antipiracy countermeasures.

---

developers-remove-denuvo-drm-from-their-games [https://perma.cc/MBL7-U5MD].

300. Andy, *Denuvo Weakens After 'Inside' Gets Cracked in Record Time*, TORRENTFREAK (Aug. 24, 2016), https://torrentfreak.com/denuvo-weakens-after-inside-cracked-in-record-time-160824 [https://perma.cc/4LFN-HD48].

301. Fahad Arif, *Pirate Group 3DM Immediately Stops Cracking PC Games To Measure Impact on Genuine Game Sales*, WCCFTECH (Feb. 16, 2016), http://wccftech.com/3dm-biggest-piracy-groups-world-quitting-piracy-singleplayer-pc-games [https://perma.cc/697C-J24D]; Luke Plunkett, *Pirates Worried that PC Games Are Becoming Too Hard To Crack*, KOTAKU (Jan. 6, 2016), http://kotaku.com/pirates-worried-that-pc-games-are-becoming-too-hard-to-1751434049 [https://perma.cc/6P7C-JY9L].

302. *See* Jon Martindale, *Denuvo May Have Lost the Battle, but It Wants To Win the War*, KITGURU (Oct. 18, 2016), http://www.kitguru.net/gaming/jon-martindale/denuvo-may-have-lost-the-battle-but-it-wants-to-win-the-war [https://perma.cc/9ZJR-82A3] (a popular DRM developer noted "we always tell our clients to help manage their expectations. Our scope is to prevent early cracks for every title. We want to allow an initial window when a game is released to have an uncracked version and thus guarantee sales.").

303. *See, e.g.*, Note, *supra* note 89 (noting concerns of DRM interference with user-created modifications).

The futility of torrent site pulldowns is apparent to nearly all actors. Torrenting traffic is largely unaffected and user behavior (as evinced by Google queries for alternate sites) is unchanged.[304] The result of this campaign has been the consumption of state resources and the diversion of pirates to riskier avenues in the form of mirrors or simply less-established torrent sites. While the take down of specific sites may, as addressed by the USTR, provide important optics, the entire endeavor appears to yield nothing but pyrrhic victories.[305]

The malware threat must be addressed now, before network exposure becomes critical. It is hardly premature to anticipate a likely threat. Piracy-related botnets are already appearing.[306] The current restriction of most of these botnets to financially motivated schemes is little comfort in an increasingly dangerous global cyber climate.

The widespread belief that the corporate entities within the wider entertainment and software industries are merely crying wolf with regard to malware hampers antimalware efforts while strengthening anticorporate arguments within pirating communities.[307] Clarifying the message, identifying specific malware threats, and assisting all users in avoiding those threats may assist in outreach efforts. Moreover, a commitment to limited-time DRM will remove an important pro-piracy argument without compromising the economic viability of releases.[308]

IV. CRITICISMS AND NEED FOR GREATER STUDY

A. Other Means of Spreading Malware

Of course, torrents are not the only means of distributing malware. As discussed above, malware may be hosted in legitimate channels, such as in Google Play. Android applications have been repeatedly flagged as containing malware. In a recent study of 283 VPN applications offered for Android on Google Play, researchers found that 38% percent contained malware or malvertising.[309]

However, the incident rate of such avenues pales in comparison to the amount of infected games hosted illegitimately.[310] While it is possible that malware networks

304. *Torrent Sites*, GOOGLE TRENDS, https://www.google.com/trends/explore?date=today%2012-m&q=torrent%20sites [https://perma.cc/2LEU-FLKA] (moving from a popularity score of 32 to 90 at time of shutdown).

305. *See supra* Part II.

306. SETTLE ET AL., *supra* note 168.

307. *See* MrTom4, *supra* note 274 (comparing virus warnings to drug overdose D.A.R.E. warnings and imploring antivirus developers to stop obfuscating their attempts to thwart piracy).

308. Moshirnia, *supra* note 6, at 51–53 (arguing a similar effect can be achieved through whimsical DRM).

309. MUHAMMAD IKRAM, NARSEO VALLINA-RODRIGUEZ, SURANGA SENEVIRATNE, MOHAMED ALI KAAFAR & VERN PAXSON, ACM, AN ANALYSIS OF THE PRIVACY AND SECURITY RISKS OF ANDROID VPN PERMISSION-ENABLED APPS (2016), https://research.csiro.au/ng/wp-content/uploads/sites/106/2016/08/paper-1.pdf [https://perma.cc/25BX-TR4D].

310. *See Q3 Mobile Threats in Play*, F-SECURE LABS (Nov. 13, 2012), https://www.f-secure.com/weblog/archives/00002454.html [https://perma.cc/4KEL-6F7D] (noting that of 28,398 malicious APK samples, only 146 came from Google Play).

would adjust their spreading strategies to include online marketplaces and netlockers, the current exposure of torrenting communities counsels immediate intervention.

B. Malware Networks Are Already Adapting to Reputational Barriers

A well-trafficked idea within the pirating community is that viruses may be quickly discovered before torrents spread very far and thus, torrents with many seeds are safe.[311] If torrents are dropped from trackers before a large seed cloud forms, the number of transmissions of the infected file will be limited. While this Article proposes a means of strengthening reputational infrastructure, this barrier is not always effective. Leecher claims of a virus in the file are often dismissed as false positives, and covert malware may evade detection long enough for a large seed group to form.

More critically, criminal elements are aware of this "only leech from large seeds" advice and are developing countermeasures. These groups understand the need for widespread seeding of a file and will enlist bots and enslaved computers to maintain the number of seeds for a sustained period.[312] This is best seen in RAUM, a malware distribution tool used to seed malware in torrents.[313] Using a pay-per-install model, malware spreaders essentially monitor the most popular torrents, spoof and then join those torrents with malware, then rent their services to criminal elements looking to ensure the weaponized torrent is widely disseminated.[314] Malicious torrents using this method have remained live for more than forty-five days and been downloaded thousands of times.[315] Unsurprisingly, "[o]ne of the most attractive categories for the monitoring and repackaging of torrents with malware is through various PC-based online-games along with the activation files for current operating systems including Microsoft Windows and Mac OS." [316]

While RAUM presents a challenge to reputational barriers, it also highlights the importance of outside intervention to reduce the viral threat. Wider awareness of the credible malware threat (in contrast to industry warnings that are seen as hyperbolic

---

311. *See, e.g.*, Crashoverride420, *supra* note 214 ("[Y]ou use [the pirate bay] then always check the comments. I have yet to run into anything bad . . . just as long as you read everything carefully. The more seeders the better, no one is going to download a virus and not get pissed and report it.").

312. *See InfoArmor Uncovers Malicious Torrent Distribution Network*, INFOARMOR (Sept. 20, 2016), https://www.infoarmor.com/infoarmor-uncovers-malicious-torrent-distribution-network [https://perma.cc/7V9V-8J4H].

313. *See id.*

314. *Id.*; Doug Olenick, *RAUM Weaponizes Torrents To Deliver Malware*, SCMAGAZINE (Sept. 21, 2016) https://www.scmagazine.com/home/security-news/raum-weaponizes-torrents-to-deliver-malware [https://perma.cc/X6HA-9JYA?type=image].

315. CISCO, ANNUAL SECURITY REPORT (2015), https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf [https://perma.cc/P85U-DYJ2]; *InfoArmor Uncovers Malicious Torrent Distribution Network*, *supra* note 312 (noting that "[i]n some cases, the lifespan of these seeded malicious files exceeded 1.5 months and resulted in thousands of successful downloads").

316. *InfoArmor Uncovers Malicious Torrent Distribution Network*, *supra* note 312; Michael Kan, *Hackers Sell Tool To Spread Malware Through Torrent Files*, PCWORLD (Sept. 21, 2016), http://www.pcworld.com/article/3122600/hackers-sell-tool-to-spread-malware-through-torrent-files.html [https://perma.cc/JMT2-DSE7].

and self-serving) may help communities deal with concerted infection networking. In any event, so long as torrenting activity will continue, a partial reputational barrier is preferable to none.

C. Piracy Encouragement and the Need for Further Study of User Behaviors and Infection Rates

A common criticism of any harm-reduction approach is that by reducing the risk attendant to the target behavior, the intervention will actually encourage that behavior.[317] Critics may argue that by attempting to make the act of piracy less likely to result in malware infection, the approach advanced by this Article will increase pirating activity. As in other contexts, this argument turns on the notion that the target behavior is informed by static concerns; that users considering piracy engage in cost-benefit analysis before engaging in the activity.

The difficulty with this argument is that pirating users appear to continue to pirate even when it makes little economic sense to do so. For example, open pricing products are still pirated, regardless of the fact that the consumer may set an artificially low price—including a price presumably cheaper than the cost of labor attendant to piracy.[318] Additionally, this argument presupposes that pirates are currently cognizant of the viral risk inherent in installing cracked software such that a lessening of

---

317. For example, a common specious argument against the HPV vaccine is that its application will increase promiscuity by lowering the threat of infection and subsequent cervical cancer. Trevor Stammers, *HPV Vaccine - Providing Protection or Promoting Promiscuity?*, CHRISTIAN MED. FELLOWSHIP (2006), http://www.cmf.org.uk/resources/publications/content/?context=article&id=1748 [https://perma.cc/ZJN7-SK24]. Though this theory has been debunked by longitudinal studies, it resists eradication at the highest levels of government. *See* Anupam B. Jena, Dana P. Goldman & Seth A. Seabury, *Incidence of Sexually Transmitted Infections After Human Papillomavirus Vaccination Among Adolescent Females*, 175 JAMA INTERNAL MED. 617 (2015), http://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2109856 [https://perma.cc/K8RG-WZ62]; Rebecca Perkins, Natalie Pierre-Joseph, Cecilia Marquez, Sandra Iloka & Jack A. Clark, *Parents' Opinions of Mandatory Human Papillomavirus (HPV) Vaccination: Does Ethnicity Matter*?, 20(6) WOMEN'S HEALTH ISSUES 420, 423 (2010), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3032271 [https://perma.cc/3KTN-92TC] (noting that parents continued to express worry that vaccine would increase promiscuity); Leah M. Smith, Jay S. Kaufman, Erin C. Strumpf & Linda E. Lévesque, *Effect of Human Papillomavirus (HPV) Vaccination on Clinical Indicators of Sexual Behaviour Among Adolescent Girls: The Ontario Grade 8 HPV Vaccine Cohort Study*, 187(2) CMAJ E74 (2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4312170 [https://perma.cc/RP8L-2PZP]; CBC News, *HPV Vaccination Concerns About Promiscuity Deemed 'Unwarranted,'* CBCNEWS (Dec. 8, 2014), http://www.cbc.ca/news/health/hpv-vaccination-concerns-about-promiscuity-deemed-unwarranted-1.2864264 [https://perma.cc/8J4D-26QF]. Similar arguments exist in the drug context and have been the subject of repeated study. NEIL HUNT, A REVIEW OF THE EVIDENCE-BASE FOR HARM REDUCTION APPROACHES TO DRUG USE, https://www.hri.global/files/2010/05/31/HIVTop50Documents11.pdf [https://perma.cc/GR4M-LSNF] (noting that needle replacement programs are criticized as increasing drug use and that this hypothesis is unsupported by evidence).

318. See, for example, the pirating of the humble bundle, which at the time allowed users to set a price of a download to one penny, inspired disgust in some pirates and amusement in others. Ben Kuchera, *Humble Bundle Gives Pirates What They Want, Gets Ripped Off*,

that risk will have an impact on pirating behavior. Finally, the forbearance on torrent site shutdowns is unlikely to increase overall torrenting activity for the simple fact that current torrent site shutdowns seem to have no impact on download frequency.

Though case studies suggest that users will respond to viral warnings provided these are substantiated and provided by non-corporate actors, it is unclear how receptive pirating users will be to warnings from corporate or governmental actors. While malware may be quantified, user perception of malware risk may vary by technical expertise, torrenting frequency, and prior malware exposure. Pirating users must be surveyed to tailor interventions in light of best practices. Lastly, the frequency and type of malware in video games must be empirically studied to determine if targeting specific genres or pirating communities is warranted.

CONCLUSION

Video game piracy presents a copyright problem and a malware problem. We are currently ineffectively addressing the former and exacerbating the latter. Concerned actors must abandon this fixated approach. Instead, a harm-reduction policy, including refraining from shuttering trackers along with their reputational antiviral infrastructure, while encouraging the use of robust time-limited DRM by developers to reduce the market for cracks, will lessen a critical malware threat and undermine pro-piracy justifications. The paramount danger to our cyber and national security warrants thoughtful action in an increasingly volatile geopolitical environment.

ARSTECHNICA (May 10, 2010, 1:27 PM), http://arstechnica.com/gaming/2010/05/humble-bundle-gives-pirates-what-they-want-gets-ripped-off [https://perma.cc/XFE2-977D] ("A lot of these people don't just pirate the game, they take pleasure in spreading the pirated links to their friends or anonymous buddies for fun . . . . They just don't care, and if you can't get someone to pay a penny in this case—will they really pay full price for a game?"); *see also* Moshirnia, *supra* note 6, at 49 (quoting a comment from torrent discussion board regarding same ("Oh for christ's sake.. you can buy this for A PENNY! Anyone who downloads this should be fucking ashamed of themselves. Why do you think it was ANONYMOUS that uploaded it? Didn't want a target painted on his thick fucking skull. I hope the mods have the good taste to remove this, if only for the fact that anyone who downloads this should be going straight to hell anyway.") and the mocking response ("It's funny how these Indie Bundles suddenly give some of the thieves here a moral backbone. Who the hell are you to dictate to others what's right or wrong? I can afford to pay for this, and I don't really want the games, but just to give you the shits, I'm downloading it. Then I'll be uploading it to all the private sites I'm a member of.")).