OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

EXECUTIVE OFFICE OF THE PRESIDENT

2019 Review of Notorious Markets for Counterfeiting and Piracy

Issue Focus: Malware and Online Piracy

The "issue focus" section of the NML highlights an issue related to the facilitation of substantial counterfeiting or piracy. Past issue focuses highlighted free trade zones (2018), illicit streaming devices (2017), stream ripping (2016), emerging marketing and distribution tactics in Internet-facilitated counterfeiting (2015), and domain name registrars (2014).

This year's issue focus explores the nexus between online piracy and malware, which has been discussed in past publications of the NML in the context of specific online markets such as 1Fichier, MPGH, and ThePirateBay. Malware, a combination of the words malicious and software,[8] is unwanted software that is installed on computers or mobile devices without consent and is often used to take advantage of computers or personal information in unwanted ways.[9] The most insidious form of malware is perhaps backdoor Trojans, which secretly grant remote access privileges of an infected device to attackers, who may proceed to steal any personal information or financial records stored on the device, provide unauthorized access to a device, monitor device activities, and install additional malware.[10] Cryptominers, run as a program or on a malicious website, take control of the computing power of an infected device and turn it toward mining cryptocurrency, which greatly slows down the performance of the device and increases electricity consumption.[11] Ransomware denies access to a device by encrypting all stored data and demanding payment in return for keys to unlock the encryption.[12]

---

[8] Some definitions of malware also include "adware," which is often undesirable software used to deliver ads to users but may not be malicious.

[9] Federal Trade Commission, Malware (Nov. 2015), https://www.consumer.ftc.gov/articles/0011-malware.

[10] *See* Malwarebytes Labs, 2019 State of Malware, https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf.

[11] *See* Malwarebytes Labs, 2019 State of Malware, https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf; O. Harpaz & D. Goldberg, The Nansh0u Campaign – Hackers Arsenal Grows Stronger (May 29, 2019), https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger; D. Fuscaldo, Crypto Mining Malware Grew 4,000% This Year (Dec. 28, 2018), https://www.forbes.com/sites/donnafuscaldo/2018/12/28/crypto-mining-malware-grew-4000-this-year.

[12] *See* C. Stupp, Hackers Get More Sophisticated With Ransomware Attacks (Dec. 18, 2019), https://www.wsj.com/articles/hackers-get-more-sophisticated-with-ransomware-attacks-11576665001; P. Muncaster, Over 1000 US Schools Hit by Ransomware in 2019 (Dec. 18, 2019), https://www.infosecurity-magazine.com/news/over-1000-us-schools-hit-by; D. Winder, Infection Hits French Hospital Like It's 2017 as Ransomware Cripples 6,000 Computers

Botnets turn infected devices into "robots" that, in coordination with other infected devices, conduct mass cyberattacks, such as distributed denial-of-service (DDOS) attacks.[13]

The nexus between online piracy and malware is tied to financial incentives. Cybercriminals who create and operate malware benefit in correlation with the spread of the malware among infected devices: they sell stolen personal and financial information, mine for cryptocurrency, collect ransoms, rent botnets, and sell cyberattack capabilities. These bad actors pay piracy websites and apps to deliver malware to those who visit the websites or use the apps—between $50–$200 per 1,000 malware installations, according to a 2015 study.[14] This study estimated that 229 piracy websites, including notorious online markets identified by USTR in its 2015 NML, generated roughly $3.3 million that year by delivering malware to their visitors. Cybercriminals also pay for advertisements on pirate websites, and some of these advertisements will install malware when displayed or clicked.[15] According to a 2016 study, 51% of ads on 260 suspected piracy websites contained malware.[16] The money collected by the

---

(Nov. 20, 2019), https://www.forbes.com/sites/daveywinder/2019/11/20/infection-hits-french-hospital-like-its-2017-as-ransomware-cripples-6000-computers.

[13] *See* C. Cimpanu, A Decade of Malware: Top Botnets of the 2010s (Dec. 3, 2019), https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s; Council to Secure the Digital Economy, International Botnet and IOT Security Guide 2020 (Nov. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf; A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[14] Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015).

[15] A 2015 study found that 55% of malware was downloaded when a user clicked on a link, often a prompt that resembled a legitimate action, and 45% of malware was downloaded invisibly in the background upon visiting a webpage. Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015). A malicious advertisement can automatically install malware without user interaction by can exploiting out-of-date software or browsers with incorrectly configured security options. *See* D. Bradbury, Chrome Will Soon Block Drive-by-Download Malvertising (Mar. 13, 2019), https://nakedsecurity.sophos.com/2019/03/13/chrome-will-soon-block-drive-by-download-malvertising. Malicious advertisements can also hijack traffic from the sites that host the ads and redirect the traffic to malicious domains that host malware. *See* R. Wright, Inside 'Master 134': Propeller Ads connected to malvertising campaign (Apr. 30, 2019), https://searchsecurity.techtarget.com/feature/Inside-Master134-Propeller-Ads-connected-to-malvertising-campaign (describing the "Master 134" malvertising campaign, tied to the AdsTerra and Propeller Ads network).

[16] European Observatory on Infringements of Intellectual Property Rights, Digital Advertising on Suspected Infringing Websites (Jan. 2016), https://euipo.europa.eu/ohimportal/documents/%2011370/80606/Digital+Advertising+on+Suspected+Infringing+Websites.

cybercriminals from the pirate websites and apps, as well as revenue generated through other advertising, donations, and subscriptions, significantly enables and incentivizes the facilitation of online piracy.

The nexus between online piracy and malware is also tied to the pirated content itself. Websites that require users to download rather than stream the infringing content, such as cyberlockers or bittorrent sites, may contain malware-infected content, including software, games, movies, music, and books. Pirated games are a particularly popular vector of this type of malware infection, since many pirated games require the user to download additional programs, known as "cracks," to circumvent the game's built-in technological protection measures, and cracks are common places to hide malware.[17] Pirated games are also a popular target for cryptominer malware as computers used for gaming tend to have high-end hardware that makes mining more efficient.[18] Cybercriminals also disguise malware as TV shows or movies—malware masquerading as Game of Thrones episodes reportedly accounted for 17% of all infected pirated content in 2018.[19] In addition, malware is commonly disguised as pirated essays or textbooks, targeting students who search for this free content.[20]

Illicit IPTV apps that run on set-top boxes can stream unlicensed sports, movies, and TV shows to a user's television, but these apps may themselves be malware.[21] According to a 2019 report on these apps, researchers found that some apps attempted to access every smart device

---

[17] *See* A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[18] *See* A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[19] M. Kan, Pirating 'Game of Thrones'? That File Is Probably Malware (Apr. 1, 2019), https://www.pcmag.com/news/367529/pirating-game-of-thrones-that-file-is-probably-malware; *see generally* Ernesto, Game of Thrones is the Most Torrented TV-Show of 2019 (Dec. 28. 2019), https://torrentfreak.com/game-of-thrones-is-the-most-torrented-tv-show-of-2019-191228.

[20] R. Hodge, Back-to-School Malware Is Hiding in Those Digital Textbooks (Sept. 3, 2019), https://www.cnet.com/news/back-to-school-malware-is-hiding-in-those-digital-textbooks; W. Maxson, Free Movies, Costly Malware (Apr. 12, 2017), https://www.consumer.ftc.gov/blog/2017/04/free-movies-costly-malware.

[21] Research into the availability and popularity of these malicious IPTV apps is still needed. *See* Andy, Rampant Kodi Malware? It's Time to Either Put Up or Shut Up (Jun. 10, 2018), https://torrentfreak.com/rampant-kodi-malware-its-time-to-either-put-up-or-shut-up-190610 ("[T]here are at least some [apps] that are clearly malicious but [do not] seem to serve other real purpose for the [] users.").

connected to the same network as the malware, install additional malware on those devices, collect information stored on those devices, and send the information to a remote location.[22] The apps also allowed remote access to and control of the device.

To avoid malware infections from piracy sites, consumers should rely on legitimate sources of copyright-protected content, such as licensed video streaming providers, and should purchase software and games from licensed vendors.[23] Purchasing legitimate content reduces exposure to malware; unsurprisingly, users who access pirated content have more malware infections.[24] Consumers should also proactively protect their devices from malware infection by installing antivirus software from legitimate providers.

[22] Digital Citizens Alliance, Fishing in the Piracy Stream: How the Dark Web of Entertainment Is Exposing Consumers to Harm (Apr. 2019), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf; *see also* A. Puig, Malware from Illegal Video Streaming Apps: What to Know (May 2, 2019), https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know.

[23] A. Puig, Malware from Illegal Video Streaming Apps: What to Know (May 2, 2019), https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know.

[24] R. Telang, Does Online Piracy make Computers Insecure? Evidence from Panel Data (Mar. 2018), https://ssrn.com/abstract=3139240 (estimating that doubling the visits to a pirated sites adds an extra 0.05 of a piece of malware per month); Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015) (finding that 1 out of every 3 piracy websites contains malware and that visitors were 28 times more likely to get malware from an infringing site than on a similarly situated non-infringing site).