Assessing the Actual Impact of a Cryptojacking Attack on Individual IT Systems and Measuring Legal Responses

Mikołaj BOROWSKI[1], Jakub DYSARZ[2], Maciej REICHWALD[3]
[1] Attorney at law, Poland
[2] DG CONNECT, European Commission, Belgium
dysarz.jakub@gmail.com
[3] Sunhill Technologies GmbH, Germany

Abstract

Mining cryptocurrencies is much more profitable if one is not paying for equipment or the electricity used for the mining. This is the main reason why cryptojacking has become so prevalent as one of the predominant cybersecurity threats facing Europe today. While the robustness of an organisation is important, one should also know what to do following a security incident or breach. Whilst post-incident analyses are important, an organization should also ascertain their legal standing as well as any possible ways forward after the damage has been done. In order to have a better idea of such a situation, we conducted an in-depth analysis of what a cryptojacking attack would do to our computer network. We did not do that to better protect ourselves, but rather to assess what management can do after an attack happens. Furthermore, we present areas that should be taken into account when assessing damage and propose legal measures effective at the European Union level, relying on criminal, civil and data protection provisions.

Index terms: cryptojacking, malicious cryptomining, web-based attacks, cybercrime, malicious software

References

[1]. H. L. J. Bijmans, T. M. Booij, and C. Doerr, "Inadvertently making cyber criminals rich: A comprehensive study of cryptojacking campaigns at internet scale," Proc. 28th USENIX Secur. Symp., pp. 1627–1644, 2019.
[2]. ENISA, "List of top 15 threats - ENISA Threat Lanscape," 2020.
[3]. H. Lau, "Browser-Based Cryptocurrency Mining Makes Unexpected Return from the Dead," Symantec Enterprise Blogs/Threat Intelligence, 2017.
[4]. BitCoinTalk, "Hash Rate / CPU Comparison Table," 2021. [Online]. Available: https://bitcointalk.org/?topic=1628.0;wap2.
[5]. BitcoinPlus, "Bitcoin Miner for Websites," 2011.

[6]. Coinhive.com, "A Crypto Miner for your Website," 2019. [Online]. Available: https://web.archive.org/web/20190429040938/https://coinhive.com/. [Accessed: 31-Jan-2021].
[7]. "Bail Bloc," 2021. [Online]. Available: https://bailbloc.thenewinquiry.com/. [Accessed: 31-Jan-2020].
[8]. C. Haan, "Bail Bloc Charity Project Mines Monero for Bail," Crowdfund Insider, 2018.
[9]. M. Salat, "The End of Coinhive; The end of cryptojacking?," Avast Blog, 2019. [Online]. Available: https://blog.avast.com/coinhive-shuts-down. [Accessed: 28-Feb-2021].
[10]. J. Cox, "Creators of In-Browser Cryptocurrency Miner 'Coinhive' Say Their Reputation Couldn't Be Much Worse," 2018. [Online]. Available: https://www.vice.com/en/article/vbpbz4/creators-of-in-browser-cryptocurrency-miner-coinhive-say-their-reputation-couldnt-be-much-worse. [Accessed: 28-Feb-2021].
[11]. Krebs on Security, "Who and What Is Coinhive?," 2018. [Online]. Available: https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/. [Accessed: 28-Feb-2021].
[12]. Europol, "Internet Organised Crime Threat Assessment (IOCTA)," 2019.
[13]. S. Eskandari, A. Leoutsarakos, T. Mursch, and J. Clark, "A First Look at Browser-Based Cryptojacking," Proc. - 3rd IEEE Eur. Symp. Secur. Priv. Work. EURO S PW 2018, no. March, pp. 58–66, 2018.
[14]. S. Pastrana and G. Suarez-Tangil, "A first look at the crypto-mining malware ecosystem: A decade of unrestricted wealth," Proc. ACM SIGCOMM Internet Meas. Conf. IMC, no. ii, pp. 73–86, 2019.
[15]. M. Saad, A. Khormali, and A. Mohaisen, "End-to-end analysis of in-browser cryptojacking," arXiv, 2018.
[16]. United States Department of Justice, "Report of the Attorney General's Cyber Digital Task Force," 2020.
[17]. Forcepoint, "What is Cryptojacking?" [Online]. Available: https://www.forcepoint.com/cyber-edu/cryptojacking. [Accessed: 28-Feb-2021].
[18]. Malwarebytes, "Cryptojacking – What is it?" [Online]. Available: https://www.malwarebytes.com/cryptojacking/. [Accessed: 28-Feb-2021].
[19]. Fortinet, "What is Cryptojacking?" [Online]. Available: https://www.fortinet.com/resources/cyberglossary/cryptojacking. [Accessed: 28-Feb-2021].
[20]. Encyclopedia by Kaspersky, "Cryptojacking." [Online]. Available: https://encyclopedia.kaspersky.com/glossary/cryptojacking/. [Accessed: 28-Feb-2021].
[21]. M. Pizzol, "Life Cycle Assessment of Bitcoin Mining," Environ. Sci. Technol., 2019.
[22]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," bitcoin.org, 2008.
[23]. A. Back, "Hashcash - A Denial of Service Counter-Measure," hashcash.org, 2002.
[24]. P. Papadopoulos, P. Ilia, and E. P. Markatos, "Truth in web mining: Measuring the profitability and cost of cryptominers as a web monetization model," arXiv, 2018.
[25]. Eurostat, "Electricity price statistics," 2020.
[26]. M. Platini, T. Ropars, B. Pelletier, and N. De Palma, "CPU overheating characterization in HPC systems: A case study," Proc. FTXS 2018 8th Work. Fault

Toler. HPC Extrem. Scale, Held conjunction with SC18 Int. Conf. High Perform. Comput. Networking, Storage Anal., pp. 69–78, 2018.

[27]. Court of Justice of the European Union, Åklagaren v Hans Åkerberg Fransson, vol. Case C-617. 2013.

[28]. Court of Justice of the European Union, "Press release No 34/18 - The ne bis in idem principle may be limited for the purpose of protecting the financial interests of the EU and the financial markets thereof," 2018.

[29]. Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[30]. D. Y. Huang et al., "Botcoin: Monetizing Stolen Cycles," in NDSS 2014, 2014, pp. 1–16.

[31]. National Police of Ukraine, "Кіберполіція встановила молодика, який майнив криптовалюту за рахунок більш як мільйона українців," 2019. [Online]. Available: https://cyberpolice.gov.ua/news/kiberpolicziya-vstanovyla-molodyka-yakyj-majnyv-kryptovalyutu-za-raxunok-bilsh-yak-miljona-ukrayinczіv-2658/. [Accessed: 14-Feb-2021].

[32]. The Next Web, "Japan court lets Monero cryptojacker walk away free," 2019. [Online]. Available: https://thenextweb.com/hardfork/2019/03/27/coinhive-cryptojacking-criminal-japan/. [Accessed: 14-Feb-2021].

[33]. The Japan Times, "Tokyo court convicts man of using website to install cryptomining programs on computers," 2020. [Online]. Available: https://www.japantimes.co.jp/news/2020/02/07/national/crime-legal/tokyo-court-cryptojacking/. [Accessed: 14-Feb-2021].

[34]. Finance Magnates, "Japanese Man Sentenced to a Year in Prison for Using Cryptojacking Malware," 2018. [Online]. Available: https://www.financemagnates.com/cryptocurrency/news/japanese-man-sentenced-year-prison-using-cryptojacking-malware/. [Accessed: 14-Feb-2021].

[35]. ZDNet.com, "Japan issues first-ever prison sentence in cryptojacking case," 2018. [Online]. Available: https://www.zdnet.com/article/for-the-first-time-remote-cryptojacker-sentenced-for-exploiting-coinhive. [Accessed: 14-Feb-2021].

[36]. U.S. District Court for Western District of Washington at Seattle, Indictment United States v. Ho. 2019.

[37]. S. Jamieson, "The Ethics and Legality of Port Scanning," 2021.

[38]. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

[39]. Council of Europe, "Convention on Cybercrime." ETS No. 185, 2001.

[40]. Council of Europe, "Explanatory Report to the Convention on Cybercrime," Nov. 2001.