Cryptojacking

Nir Kshetri, University of North Carolina at Greensboro
Jeffrey Voas, IEEE Fellow

The cybersecurity community never ceases to amaze or disappoint; it continually adds words to the English dictionary. Here's another: "cryptojacking." It's not carjacking or hijacking, but similar. It is a word that you might wish to know more about.

Cryptojacking attacks involve hijacking computers and then mining cryptocurrencies covertly. According to a report of the threat intelligence and cybersecurity consulting organization Unit 42, 17% of organizations worldwide with cloud-based infrastructures had cryptojacking activity during December 2020–February 2021.[1] In February 2019, Check Point named cryptojacking malware Coinhive, designed to mine Monero cryptocurrency, as the "most wanted malware" for the 15th successive month.[2]

AN ATTRACTIVE VENTURE

Cryptojacking may be more economically attractive when compared to other cyberattacks. Cryptojacking as a service involves cryptojacking kits that can be purchased on the dark web for about US$30.[3] Whereas cyberattacks such as ransomware have been on the radar of law enforcement agencies, cryptojacking attacks are characterized by a high degree of stealth. Ransomware suspects employ coercion, blackmail, and intimidation, and they face imprisonment. Cryptojacking, on the other hand, is seen as a "legally gray area." It doesn't involve information stealing or coercing.

ARE CRYPTOJACKING ACTIVITIES TIED TO CRYPTOCURRENCIES' VALUES?

Cryptojacking perpetrators use victims' computers to mine cryptocurrencies. For these perpetrators, higher cryptocurrency values yield higher profits. For instance, the value of Bitcoin increased by more than 400% in the last three quarters of 2020. NTT DATA Corporation reported that cryptojacking malware

Digital Object Identifier 10.1109/MC.2021.3122474
Date of current version: 12 January 2022

0018-9162/22©2022IEEE

accounted for 41% of all detected malware in 2020.[4]

However, some "high-profile" cryptojacking perpetrators were forced to shut down when cryptocurrency values fell. In August 2018, Coinhive controlled about 62% of the cryptojacking market.[5] Coinhive closed down in March 2019. In a blog post, Coinhive gave two reasons: 1) Monero's value declined significantly, which reduced the attractiveness of Monero mining activities with cryptojacking (Monero's value fell by 85% in 2019); 2) the currency became harder to mine.[6]

VICTIMS

Companies that are affected by cryptojacking malware can face adverse outcomes. Data processing overloading can cause wear-out and overheating to the hardware involved. Reduced CPU performance can also have an adverse effect on service delivery. Other effects can include higher energy costs and bandwidth latency. Companies may also suffer reputation damages if it is publicly known that they were victimized by cryptojacking.[7]

> Whereas cyberattacks such as ransomware have been on the radar of law enforcement agencies, cryptojacking attacks are characterized by a high degree of stealth.

DISCLAIMER

The authors are completely responsible for the content in this article. The opinions expressed are their own.

REFERENCES

1. F. Erazo, "Cryptojacking activity decreased for the first time since 2018, says intelligence report," Bitcoin, Apr. 8, 2021. [Online]. Available: https://news.bitcoin.com/cryptojacking-activity-decreased-for-the-first-time-since-2018-says-intelligence-report/
2. "February 2019's most wanted malware: Coinhive quits while still at the top," Checkpoint, Mar. 11, 2019. [Online]. Available: https://blog.checkpoint.com/2019/03/11/february-2019s-most-wanted-malware-coinhive-quits-gandcrab-cryptomining-ransomware/
3. M. Nadeau, "Cryptojacking explained: How to prevent, detect, and recover from it," CSO Online, May 6, 2021. [Online]. Available: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html
4. "Cryptojacking scams are on the rise once again, after declining for two years," *Business Insider*, Jun. 8, 2021. [Online]. Available: https://www.businessinsider.in/cryptocurrency/news/cryptojacking-scams-are-on-the-rise-once-again-after-declining-for-two-years/articleshow/83335965.cms
5. J. Porter, "Popular 'cryptojacking' service Coinhive will shut down next week," *The Verge*, Feb. 28, 2019. [Online]. Available: https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date
6. "Discontinuation of Coinhive," Coinhive, 2019. [Online]. Available: https://coinhive.com/blog/en/discontinuation-of-coinhive
7. S. Gush, "Why cryptojacking is better than ransomware for cybercriminals," makeuseof.com, Jun. 24, 2021. [Online]. Available: https://www.makeuseof.com/why-cryptojacking-is-better-than-ransomware-for-cybercriminals/s

NIR KSHETRI is a professor of management in the Bryan School of Business and Economics, University of North Carolina at Greensboro, Greensboro, North Carolina, 27412, USA, and the "Computing's Economics" column editor for *Computer*. Contact him at nbkshetr@uncg.edu.

JEFFREY VOAS, Gaithersburg, Maryland, USA, is the editor in chief of *Computer*. He is a Fellow of IEEE. Contact him at j.voas@ieee.org.