The summer heat of cryptojacking season : Detecting cryptojacking using heatmap and fuzzy

Firdaus, Ahmad[a]*; Aldharhani, Ghassan Saleh*[b]*; Ismail, Zahian*[a]*; Ab Razak, Mohd Faizal*[a]

[a] College of Computing and Applied Sciences, Universiti Malaysia Pahang, Faculty of Computing, Pahang, Pekan, Malaysia

[b] Digital Innovation Institute of Computer Science and Digital Innovation (ICSDI), UCSI University, Kuala Lumpur, Malaysia

ABSTRACT

Cryptojacking is a subset of cybercrime in which hackers use unauthorised devices (computers, smartphones, tablets, and even servers) to mine cryptocurrencies. Similar to many other forms of cybercrime, the objective of cryptojacking is achieve profit illegally. It is also designed to remain entirely concealed from the victim's view. However, its attacks continue to evolve and spread, and their number continues to rise. Therefore, it is essential to detect cryptojacking malware, as it poses a significant risk to users. However, in machine learning intelligence detection, an excessive number of insignificant features will diminish the detection's accuracy. For machine learning-based detection, it's important to find important features in a minimal amount of data. This study therefore proposes the Pearson correlation coefficient (PMCC), a measure of the linear relationship between all features. After that, this study employs the heatmap method to visualise the PMCC value as a colour version of heat. We utilised The Fuzzy Lattice Reasoning (FLR) classifier for classification algorithms in machine learning. This experiment utilised actual cryptojacking samples and achieved a 100 percent detection accuracy rate in simulation.

KEYWORDS

Cryptojacking; Cyber security; Cybercrime; Fuzzy lattice reasoning (FLR); Fuzzy logic

REFERENCES

[1] Vala Khushali, “A Review on Fileless Malware Analysis Techniques,” *International Journal of Engineering Research & Technology (IJERT)*, vol. V9, no. 05, May 2020, doi: 10.17577/IJERTV9IS050068.
[2] D. Tanana, “Behavior-Based Detection of Cryptojacking Malware,” *Proceedings - 2020 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology, USBEREIT 2020*, pp. 543–545, 2020, doi : 10.1109/USBEREIT48449.2020.9117732.
[3] European Union Agency for Cybersecurity, “Cryptojacking - Cryptomining in the browser,” 2017. https://www.enisa.europa.eu/publications/info- notes/cryptojacking-cryptomining-in-the-browser (accessed Apr. 22, 2021).
[4] L. Caviglione *et al.*, “Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection,” *IEEE Access*, vol. 9, pp. 5371–5396, 2021, doi: 10.1109/ACCESS.2020.3048319.
[5] F. Naseem, A. Aris, L. Babun, E. Tekiner, and A. S. Uluagac, “MINOS: A Lightweight Real-Time Cryptojacking Detection System,” in *Proceedings 2021 Network and Distributed System Security Symposium (NDSS)*, 2021, pp. 1–15. doi: 10.14722/ndss.2021.24444.