Effective Mitigation for XMRig-based Cryptojacking on Web Servers

Shuhei Enomoto
Kobe University
Japan
215t801t@gsuite.kobe-u.ac.jp

Hiroki Kuzuno
Kobe University
Japan

Yoshiaki Shiraishi
Kobe University
Japan

Masakatu Morii
Kobe University
Japan

Cryptojacking, a form of malicious software (malware), mines cryptocurrency without user consent. Traditionally, cryptojacking was executed inside the web browsers on victims' PCs. However, the termination of Coinhive has led to a decrease in cryptojacking. Currently, vulnerable web servers [1–3], are the primary targets of cryptojacking with XMRig implementation. Cryptojacking requires increased CPU resources for execution, leading to the performance overhead of web servers.

To detect cryptojacking, rule-based detections, such as scanning files and networks using predefined patterns, are effective. However, executing these methods on web servers is challenging because they incur high overhead. Furthermore, behavior-based cryptojacking detections [4, 5] are not compatible with web servers. First, identifying user processes with high CPU usage as cryptojacking [4] can result in false positives because web servers also induce high usage. Second, identifying virtual machines (VMs) running cryptojacking from the host OS [5] requires modification outside of VMs, the cloud users of Infrastructure as a Service (IaaS) cannot install this mechanism. Third, these mechanisms inhibit live forensics that require maintaining the malware execution because they terminate cryptojacking after the detection.

This study addresses the following question: *Is it possible to implement mitigation against cryptojacking on web servers running on real-world cloud IaaS?* This paper presents an effective mitigation against XMRig-based cryptojacking on web servers. Our system detects XMRig-based cryptojacking by monitoring user processes based on the primitive behaviors of XMRig, which include mining using huge pages to improve performance and communicating with mining pool servers as a network client to submit results.

Our system is driven by the following design goals; first, monitoring and detecting must incur low overhead; second, the detection mechanism must produce few false positives; third, introducing the mechanism should require no additional components outside the OS for easy deployment; and finally, the motivations for maintaining XMRig-based cryptojacking for live forensics and minimizing performance impact must be balanced.

To satisfy these goals, our system monitors accessing to huge pages and writing content to network client sockets. Our system hooks only certain kernel functions to maintain low overhead. In general, web servers contain no implementation for huge pages and network client sockets, our system does not detect web servers as malware, unlike previous studies. Furthermore, our system is implemented as a kernel module and is deployable across real-world cloud IaaS. Subsequently, our system provides two operational responses for detected user processes: *suspension*, to eliminate performance impact, and *suppression*, to maintain XMRig-based cryptojacking execution while reducing its impact.

We conducted preliminary experiments about security and performance. We confirmed our system can run on Linux 5.4.0-153 executed on Amazon Elastic Compute Cloud, and successfully detects variants of XMRig. Moreover, the performance experiments using real-world web servers and XMRig show that our system prevents 15.2 to 56.4% throughput reduction on Nginx, Apache HTTP Server, Lighttpd, and h2o.

This study remains to be further evaluated. First, we are now evaluating the detection of benign applications to analyze false positives in our system. Furthermore, we plan to conduct a security capability experiment to evaluate the detection of wild cryptojacking, and a performance experiment to compare existing detection solutions and our system.

References

[1] NATIONAL VULNERABILITY DATABASE. Cve-2021-40438. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-40438, 2021.

[2] NATIONAL VULNERABILITY DATABASE. Cve-2021-41773. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-41773, 2021.

[3] NATIONAL VULNERABILITY DATABASE. Cve-2021-42013. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-42013, 2021.

[4] Tanana Dmitry. Behavior-based detection of cryptojacking malware. In *Proceedings of the 3rd Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT '20)*, pages 543–545. IEEE, 2020.

[5] Anupam Das Mohammad Ahmad Carl A. Gunter Fareed Zaffar Matthew Caesar Rashid Tahir, Muhammad Huzaifa and Nikita Borisov. Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. In *Proceedings of the 20th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID '17)*, pages 287–310. Springer, 2017.