Chapter 5 Crypto Mining Attacks on Cyber Security: Xmrig Is a Sophisticated Crypto Miner

Ilker Kara Çankırı Karatekin University, Turkey

> **Emre Hasgul** Hacettepe University, Turkey

ABSTRACT

The increase in popularity of blockchain and cryptocurrencies in the last decade has led cyber attackers to develop various methods. Today, countless blockchain and cryptocurrency system applications and technologies target user accounts and information systems through cryptocurrency hacking malware. Especially with offthe-shelf mining scripts readily available from untraceable cryptocurrencies (e.g., Monero and Zcash), crypto-hacking malware has become an indispensable method for attackers. This study focuses on the mechanism and detection and analysis of crypto miner malicious software attacks. In addition, precautions that can be taken to protect against crypto miner malicious software attacks are presented.

XMRİG ATTACK

Xmrig is a sophisticated and legitimate cryptominer. However, attackers use a trajonized version of it (Lebosse et al., 2017 and Mbiatem et al., 2018). In addition there is a really well thought technique that makes it dangerous (Varlioglu et al.,

DOI: 10.4018/978-1-6684-6247-8.ch005

Crypto Mining Attacks on Cyber Security

2022 and Zoghlami et al., 2016 and Taghipour et al., 2013 and Alizadeh et al., 2020 and Gao et al., 2018).

Attackers penetrate a server that has connection to both internet and intranet. However, they do not run this miner on the initially infected server. They remove their traces on it first. For example, in Linux servers, attackers changes the content of following log files with /dev/null.

- /var/log/security
- /var/log/wtmp
- /var/log/btmp
- /var/log/utx.lastlog
- /var/log/utx.log

After initial access, the attacker perform brute force attacks to SSH ports of intranet servers that are connected to initially penetrated server. After a successful brute force they have the root access to intranet server and they start to move laterally. Then they install the miner on penetrated intranet servers.





12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: <u>www.igi-</u> <u>global.com/chapter/crypto-mining-attacks-on-cyber-</u> <u>security/315968</u>

Related Content

Ranking Web Services using Web Service Popularity Score

Selwa Elfirdoussi, Zahi Jarirand Mohamed Quafafou (2014). *International Journal of Information Technology and Web Engineering (pp. 78-89).* www.irma-international.org/article/ranking-web-services-using-web-service-popularityscore/115936

Malware Threat Affecting Financial Organization Analysis Using Machine Learning Approach

Romil Rawat, Sanjaya Kumar Sarangi, Yagya Nath Rimal, P. William, Snehil Dahima, Sonali Guptaand K. Sakthidasan Sankaran (2022). *International Journal of Information Technology and Web Engineering (pp. 1-20).*

www.irma-international.org/article/malware-threat-affecting-financial-organization-analysis-usingmachine-learning-approach/304051

A Conceptual Model to Next-Generation Smart Education Ecosystem

Palanivel Kuppusamyand Suresh Joseph K. (2021). *Transforming the Internet of Things for Next-Generation Smart Systems (pp. 76-99).*

www.irma-international.org/chapter/a-conceptual-model-to-next-generation-smart-educationecosystem/278626

Navigation Path Detection for Cotton Field Operator Robot Based on Horizontal Spline Segmentation

Dongchen Li, Shengyong Xu, Yuezhi Zheng, Changgui Qiand Pengjiao Yao (2017). International Journal of Information Technology and Web Engineering (pp. 28-41). www.irma-international.org/article/navigation-path-detection-for-cotton-field-operator-robotbased-on-horizontal-spline-segmentation/182262

QoS in the Mobile Cloud Computing Environment

Zhefu Shiand Cory Beard (2016). *Web-Based Services: Concepts, Methodologies, Tools, and Applications (pp. 2221-2238).*

www.irma-international.org/chapter/qos-in-the-mobile-cloud-computing-environment/140896