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 off-the-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

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.

Figure 1. Tojanized XMRIG Miner Lateral Movement.