

ABSTRACT

Cryptocurrencies such as Monero are becoming increasingly popular due to their high privacy and anonymity features. However, these features also attract cybercriminals who use cryptojacking techniques to mine cryptocurrency without the user's knowledge. Cryptojacking can cause significant damage to IT infrastructure, including system performance degradation, high power consumption, and potential hardware damage. This report aims to identify and analyze network traffic patterns related to Monero activity using the MITRE ATT&CK framework. Additionally, this report formulates effective mitigation strategies to reduce the risks of Monero cryptojacking. The study results show that by understanding network traffic patterns and utilizing the MITRE ATT&CK Framework, organizations can enhance their network security and protect computing resources from cryptojacking threats.

Keywords: MITRE ATT&CK, Cryptocurrency, cryptojacking