Detection of illicit cryptomining using network metadata

Michele Russo (✉ michele.russo1@huawei.com)

Huawei Technologies Duesseldorf GmbH <https://orcid.org/0000-0001-6876-2798>

Nedim Šmđić

Huawei Technologies Duesseldorf GmbH

Pavel Laskov

University of Liechtenstein: Universitat Liechtenstein

Research

Keywords: detection, malware, cryptomining, Monero, NetFlow, machine learning, one-class classification

Posted Date: July 1st, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-607598/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Version of Record: A version of this preprint was published at EURASIP Journal on Information Security on December 1st, 2021. See the published version at <https://doi.org/10.1186/s13635-021-00126-1>.

Abstract

Illicit cryptocurrency mining has become one of the prevalent methods for monetization of computer security incidents. In this attack, victims' computing resources are abused to mine cryptocurrency for the benefit of attackers. The most popular illicitly mined digital coin is Monero as it provides strong anonymity and is efficiently mined on CPUs.

Illicit mining crucially relies on communication between compromised systems and remote mining pools using the de facto standard protocol Stratum. While prior research primarily focused on endpoint-based detection of in-browser mining, in this paper we address network-based detection of cryptomining malware in general. We propose XMR-Ray, a machine learning detector using novel features based on reconstructing the Stratum protocol from raw NetFlow records. Our detector is trained offline using only mining traffic and does not require privacy-sensitive normal network traffic, which facilitates its adoption and integration.

In our experiments, XMR-Ray attained 98.94% detection rate at 0.05% false alarm rate, outperforming the closest competitor. Our evaluation furthermore demonstrates that it reliably detects previously unseen mining pools, is robust against common obfuscation techniques such as encryption and proxies, and is applicable to mining in the browser or by compiled binaries. Finally, by deploying our detector in a large university network, we show its effectiveness in protecting real-world systems.

Full Text

This preprint is available for [download as a PDF](#).

Figures

Figure 1

Typical stratum mining workflow

Figure 2

Example of stratum communication between a mining pool and client

Figure 3

Typical deployment scenario for XMR-Ray

Figure 4

System architecture

Figure 5

Detection performance as a function of window size l_W

Figure 6

Detection performance on novel mining pools

Figure 7

Comparison on detecting novel mining pools