Detecting cryptocurrency miners with NetFlow/IPFIX network measurements

<table>
<thead>
<tr>
<th>Title</th>
<th>Detecting cryptocurrency miners with NetFlow/IPFIX network measurements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publication Type</td>
<td>Conference Paper</td>
</tr>
<tr>
<td>Year of Publication</td>
<td>2019</td>
</tr>
<tr>
<td>Authors</td>
<td>Muñoz, Jordi Zayuelas i, Suárez-Varela, José, Barlet-Ros, Pere</td>
</tr>
<tr>
<td>Conference Name</td>
<td>2019 IEEE International Symposium on Measurements Networking (M N)</td>
</tr>
<tr>
<td>Date Published</td>
<td>July 2019</td>
</tr>
<tr>
<td>Publisher</td>
<td>IEEE</td>
</tr>
<tr>
<td>ISBN Number</td>
<td>978-1-7281-1273-2</td>
</tr>
</tbody>
</table>

**Keywords**
- computer network security
- cost-efficiency miner detection
- cryptocurrencies
- cryptocurrency miner detection
- cryptocurrency mining
- cryptojacking
- Cryptojacking detection
- data mining
- deep packet inspection
- Distributed databases
- DNS traffic
- Human Behavior
- human factors
- Internet
- Internet activity
- IP networks
- IPFIX network measurements
- learning (artificial intelligence)
- machine learning
- Metrics
- mine cryptocurrencies
- NetFlow measurements
- NetFlow network measurements
- pubcrawl
- resilience
- Resiliency
- telecommunication computing
- telecommunication traffic
- unknown mining servers
In the last few years, cryptocurrency mining has become more and more important on the Internet activity and nowadays is even having a noticeable impact on the global economy. This has motivated the emergence of a new malicious activity called cryptojacking, which consists of compromising other machines connected to the Internet and leverage their resources to mine cryptocurrencies. In this context, it is of particular interest for network administrators to detect possible cryptocurrency miners using network resources without permission. Currently, it is possible to detect them using IP address lists from known mining pools, processing information from DNS traffic, or directly performing Deep Packet Inspection (DPI) over all the traffic. However, all these methods are still ineffective to detect miners using unknown mining servers or result too expensive to be deployed in real-world networks with large traffic volume. In this paper, we present a machine learning-based method able to detect cryptocurrency miners using NetFlow/IPFIX network measurements. Our method does not require to inspect the packets' payload; as a result, it achieves cost-efficient miner detection with similar accuracy than DPI-based techniques.

DOI 10.1109/IWMN.2019.8804995
Citation Key munoz_detecting_2019