Content-Agnostic Identification of Cryptojacking in Network Traffic

Yebo Feng, Devkishen Sisodia, Jun Li
University of Oregon
{yebof, dsisodia, lijun}@cs.uoregon.edu
Cryptocurrency Mining (Cryptomining)

- Validates transactions and adds valid transactions to the blockchain
- Often divides a mining task among mining devices in a mining pool
- Provides a means for a cryptocurrency to establish consensus
- Requires significant computing power
- Enables miners to make money via transaction fees and generation of new coins
Cryptojacking

- A term defined as unauthorized use of someone else’s computing resources to mine cryptocurrency

- Approaches
  - Sending a malicious email link that downloads cryptomining code when clicked
  - Creating a website with cryptomining code embedded
  - Infecting machines with cryptomining code via worms
  - etc.
Cryptocurrency mining software was installed on more than 50% of one airport’s workstations.

https://www.cyberbit.com/blog/endpoint-security/cryptocurrency-miners-exploit-airport-resources/
Researchers have uncovered the first instance of a new cryptojacking worm that propagates via malicious Docker images, according to Palo Alto Networks’ threat intelligence team Unit 42.

Solutions Against Cryptomining

- **Endpoint-based Solutions**
  - Anti-cryptojacking extension on web browsers
    - Detect cryptojacking scripts through mining code patterns
  - Antivirus software with the capability to detect cryptojacking (cryptomining)
    - Monitor abnormal use of computing resources
    - Detect the cryptojacking malware patterns (mining patterns)

- **Network-based Solutions**
  - Filtering traffic with a blacklist of mining pools
  - Deep packet inspection on packets
  - Flow-level privacy-preserving cryptojacking traffic detection
    - A missing gap!
Operational model of our approach

1. Deploy at the border router of a campus, company, or institution level network.
2. Only capture four types of information from the inbound and outbound traffic: src and dst IPs, src and dst port numbers, protocol, and packet size.
Study of mining traffic

Communication mechanism for mining:
- Login message
- Login confirmation
- Assignment allocation
- Result message
- Result confirmation
Study of mining traffic – packet intervals

Smooth the packet intervals with Gaussian filter: $G(x) = \frac{1}{\sqrt{2\pi \sigma^2}} e^{-\frac{x^2}{2\sigma^2}}$
Cryptojacking traffic pattern

An essential concept of cryptomining is the hash rate, the speed at which a device is completing an operation in the crypto-mining code. After studying the cryptojacking activities, we found that they differ from legitimate crypto-mining activities in the following aspects:

• The hash rate of legitimate crypto-mining is more stable than the hash rate of cryptojacking because cryptojacking scripts usually rely on some existing software running in the system such as the browser, terminal, or Apache server, which makes the computing resources devoted to the mining calculation erratic.

• The hash rate of cryptojacking is usually lower than the hash rate of legitimate crypto-mining, since cryptojacking scripts or malware cannot easily invoke GPU or dedicated ASIC chips to mining, further leading to a lower message rate.
Detection of cryptojacking traffic

We apply fast Fourier transform (FFT) to convert packets from the time domain to a representation in the frequency domain.

• Traffic generated from other activities, such as browsing webpage, DNS queries, and Telnet remote controlling, tends to have complicated and randomized frequency patterns. Conversely, mining traffic has clean and periodic frequency patterns.

• We define a sliding time window to monitor the ongoing traffic.
Detection of cryptojacking traffic

• For each sliding time window, we convert the packets from time domain to frequency domain. Then we use a threshold-based matching to detect cryptomining traffic.

• To identify cryptojacking traffic, we capture the hash rate difference (frequency difference, e.g., $r_n, a_n$) between different time windows.

• We input such vector into an LSTM (Long short-term memory) model to detect cryptojacking traffic.
LSTM classification

• We train the classification model with collected cryptomining traffic data (legitimate and cryptojacking).
• The LSTM model outputs two types of labels: legitimate cryptomining traffic and cryptojacking traffic.
Conclusion & Future work

• In this paper, we propose a privacy-preserving cryptojacking detection approach that only relies on content-agnostic network traffic flows to conduct detections. Our approach is efficient and easy to deploy. With the computing power of a personal computer, it is capable of providing real-time detection of cryptojacking for a company-level network.

• In the future, we will keep simulating cryptojacking activities on different platforms and collect their traffic to improve and test our approach.
Thanks!

This material is based upon work supported by Ripple Graduate Research Fellowship. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of Ripple Labs, Inc.