The 15th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2020)

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.

CYBERBIT
PROTECTING A NEW DIMENSION

SOLUTIONS PLATFORM PARTNERS MSSP COMPANY RESOURCES SCHEDULE A DEMO

Cryptocurrency Miners Now Using Evasive Tactics to Exploit Airport Resources

Meir Brown | Oct 16, 2019

While rolling out Cyberbit's Endpoint Detection and Response (EDR) in an international airport in Europe, our researchers identified an interesting crypto mining infection, where cryptocurrency mining software was installed on more than 50% of the airport's workstations. The findings raise concerns regarding the ease of installing malicious software within corporate networks despite being protected by antivirus systems.

How we have detected the crypto-mining software

The malware was discovered while rolling out Cyberbit EDR, an advanced behavioral detection and threat hunting platform, in an international airport in Europe. Based on further analysis we can associate this malware with the anti-coinminer campaign reported by Zscaler in August 2018.

During a standard rollout process, we install our kernel-level EDR Agents on the customer's workstations. The Agent collects endpoint activity and the data is centralized in a big-data repository where it is analyzed using a set of behavioral algorithms. The behavioral engine then generates alerts for endpoint behaviors that are potentially malicious. Cyberbit's team of analysts examines these alerts and whitelists legitimate processes. This enables our customers to achieve accurate detection of evasive activity, which often bypasses antivirus systems, while minimizing false positives during ongoing operation after rollout.

During this process, our behavioral engine alerted on suspicious use of the PAExec tool. The tool was used multiple times over a short period to launch an application named player.exe. PAExec is a redistributable version of Microsoft's PSExec, used for running Windows programs on remote systems without having to physically install software on these systems. The use of PAExec is often an indication of malicious activity, moreover the

Cyberbit
@CYBERBITHQ
#cyberattacks are hitting the financial sector hard. Leading banks seek military-grade EDR to prevent costly breaches buff.ly/31VEGQT

the Banking & Finance Post

10h

Cyberbit
@CYBERBITHQ
Cyberbit discovers international #airport riddled with #bitcoinmining #malware. Known exploits are tweaked to evade #NGAV but can't hide from behavior analysis. buff.ly/2BkbKqk

Oct 18, 2019

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.

Cryptojacking worm uses Docker to infect over 2,000 systems to secretly mine Monero

by RAVIE LAKSHMANAN — 5 days ago in SECURITY

54 SHARES

https://tnw.to/FxulM

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.

Dubbed "Graboid," the worm infects compromised hosts with malware that covertly abuses the systems to mine privacy-focused cryptocurrency Monero before randomly spreading to the next target.

Docker is a popular platform-as-a-service (PaaS) solution for Linux and Windows that

Most popular

1. RIP: How to stop Google from stealing all your data after you die — Cara Curtis · 1 day ago
2. Why Elon Musk is wrong about LiDAR technology — Sam Kamel · 1 day ago
3. Facebook begins testing dark mode and a Twitter-like interface for desktop — Ivan Mehta · 12 hours ago
4. Microsoft's open-source election software now has a bug bounty program — Ravie Lakshmanan · 11 hours ago
5. Instagram is testing a feature to clean up your pity follows — Ivan Mehta · 10 hours ago

Never miss out

Stay tuned with our weekly recap of what's hot & cool by our CEO Boris.

Email DO IT

Join over 260,000 subscribers!

Who's Hiring Add your company

Philips

Don't just make a living, make a difference. Hiring for 150+ jobs in The

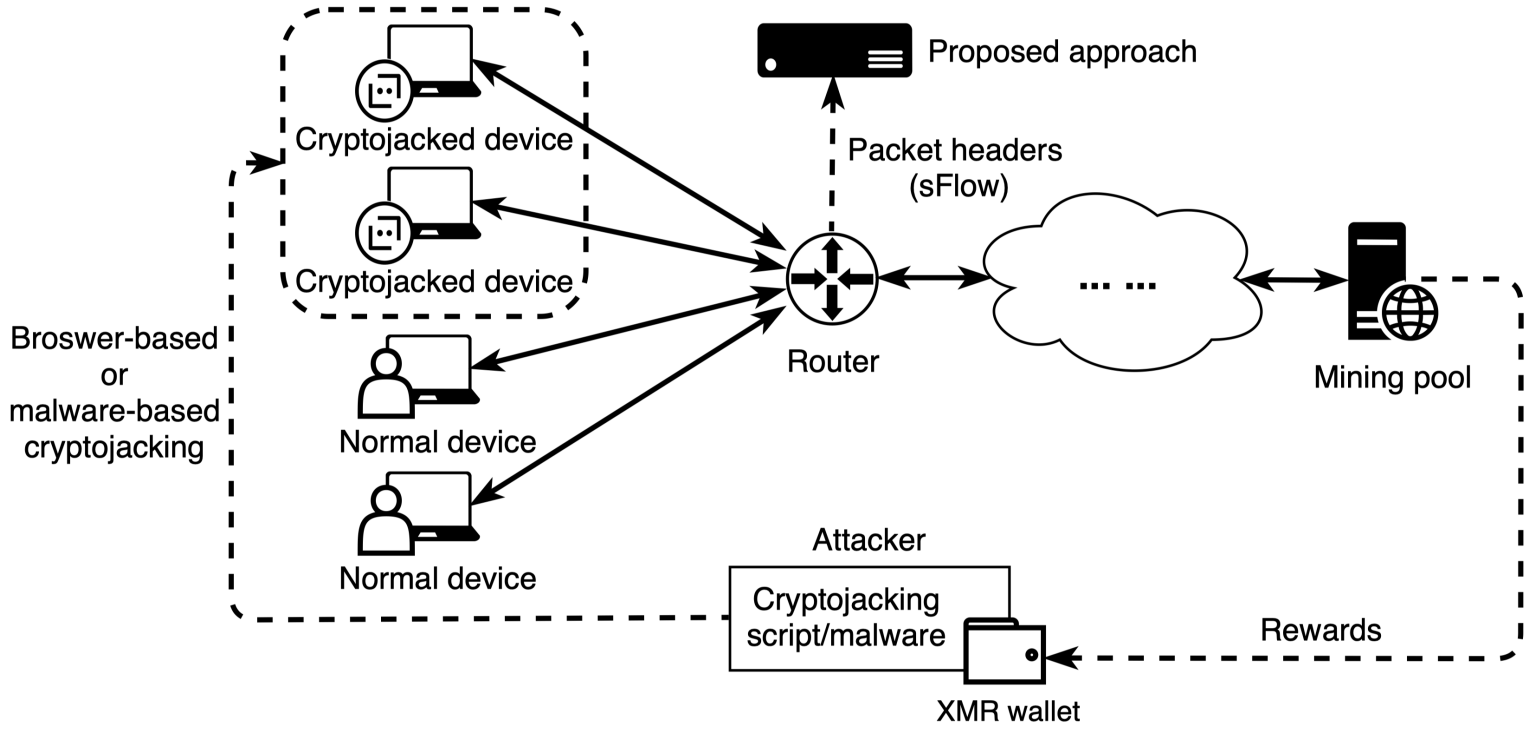
https://thenextweb.com/security/2019/10/16/cryptojacking-worm-uses-docker-to-infect-over-2000-systems-to-secretly-mine-monero/

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

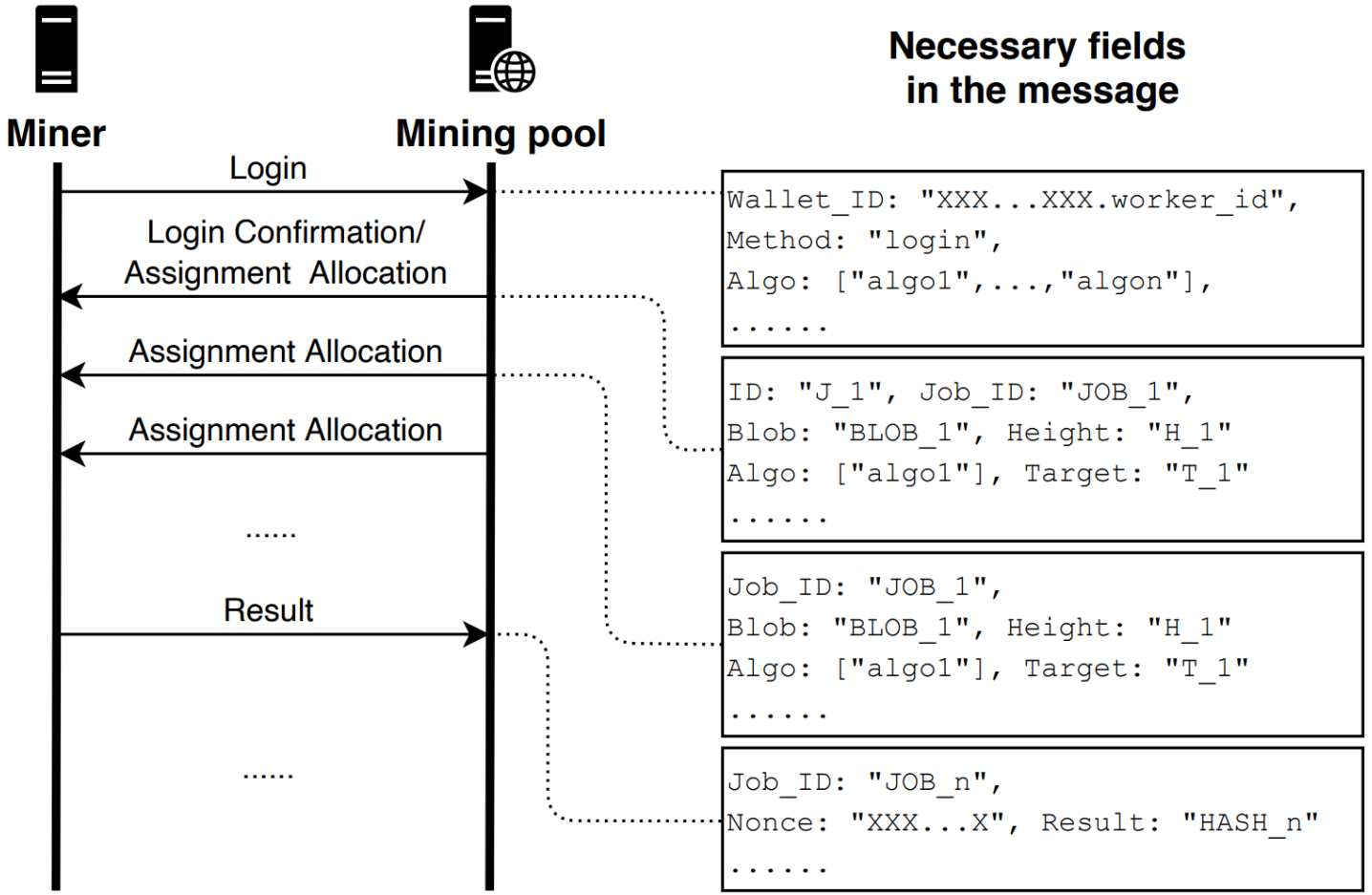
1. Deploy at the border router of a campus, company, or institution level network.
2. Only capture four types of information from the inbound and outbound traffic: src and dst IPs, src and dst port numbers, protocol, and packet size.



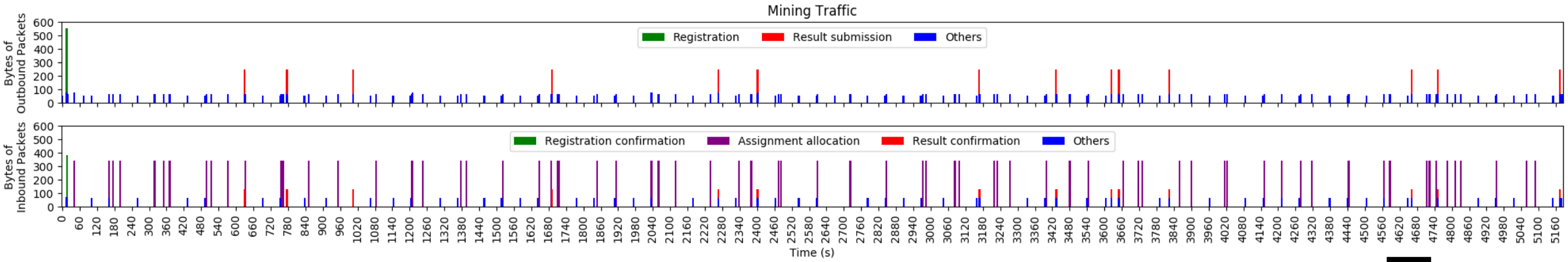
Study of mining traffic

Communication mechanism for mining:

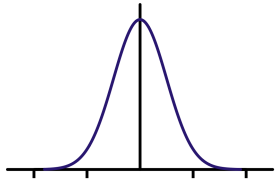
- Login message
- Login confirmation
- Assignment allocation
- Result message
- Result confirmation

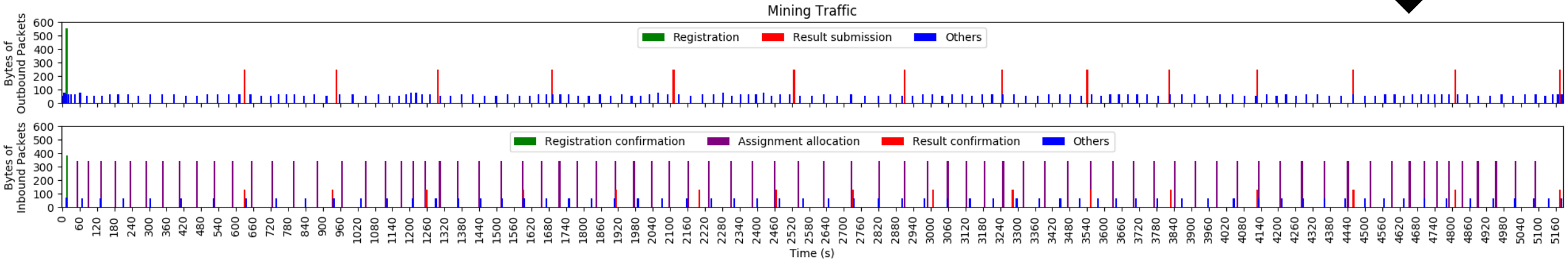


Study of mining traffic – packet intervals



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

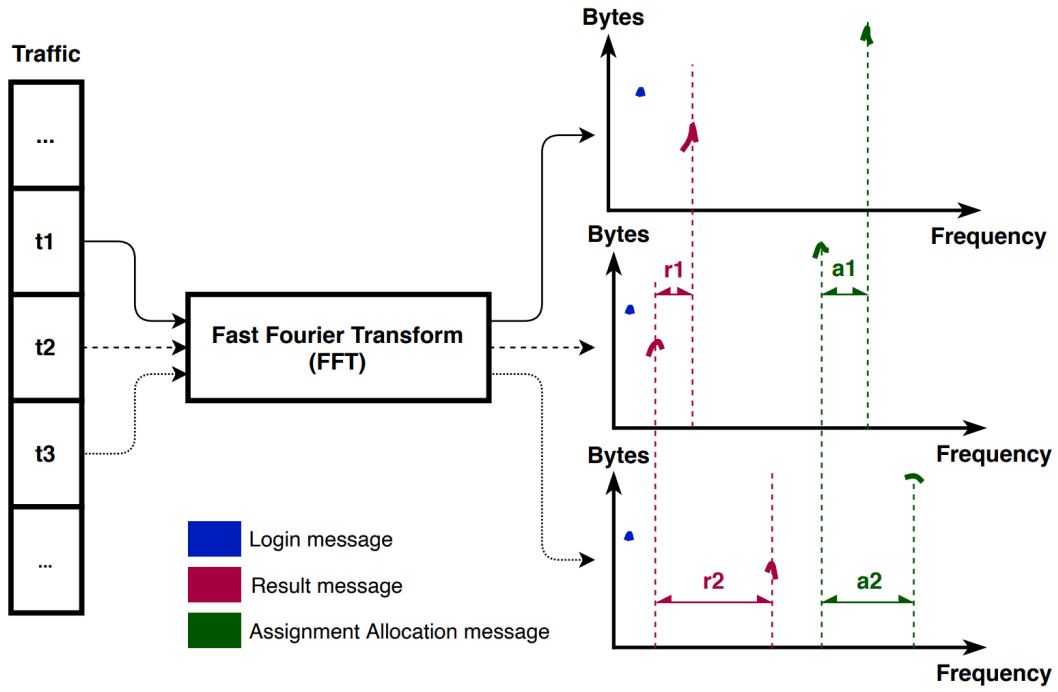
An essential concept of cryptomining is the hash rate, the speed at which a device is completing an operation in the crypto-mining code. After studying the cryptojacking activities, we found that they differ from legitimate crypto-mining activities in the following aspects:

- 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

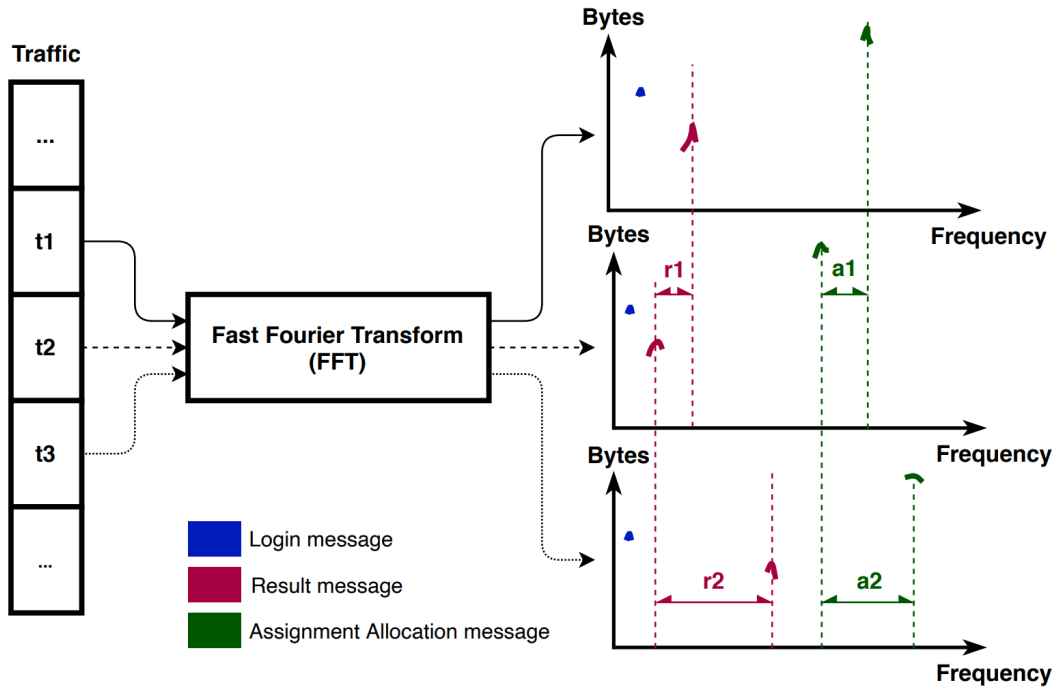
We apply fast Fourier transform (FFT) to convert packets from the time domain to a representation in the frequency domain.

- 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.

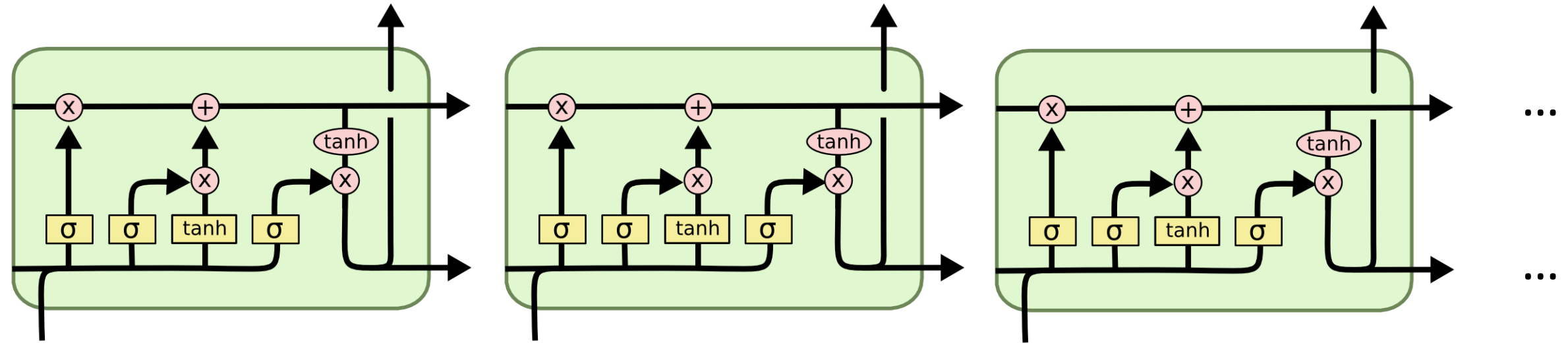


Detection of cryptojacking traffic

- 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.