CJ-Sniffer: Measurement and Content-Agnostic Detection of Cryptojacking Traffic

Authors and Publication

This research paper, *CJ-Sniffer: Measurement and Content-Agnostic Detection of Cryptojacking Traffic*, is written by **Yebo Feng, Jun Li, and Devkishen Sisodia** from the **University of Oregon, USA**. It was published in the **25th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID 2022)**, held in **Limassol, Cyprus**. The paper is available in the ACM Digital Library.

Introduction

What is Cryptojacking?

Imagine you are using your computer for everyday tasks like watching videos, browsing websites, or working on documents. Suddenly, your computer becomes very slow, your fan is running loudly, and your battery drains faster than usual. You might think it's just an old computer, but in reality, someone might be using your device without your permission to mine cryptocurrency. This is called Cryptojacking.

What is Cryptocurrency Mining?

Cryptocurrency mining is a process where powerful computers solve complex mathematical problems to generate digital coins like Bitcoin or Monero. This process requires a lot of processing power, electricity, and specialized hardware. Hackers have found a way to steal computing power from unsuspecting users by running mining scripts in the background of their devices—this is cryptojacking.

Why is Cryptojacking a Problem?

Slows Down Your Computer – Mining takes up a lot of CPU power, making normal tasks sluggish.

Increases Electricity Bills – Since mining is power-intensive, it causes increased electricity consumption.

Reduces Device Lifespan – Excessive workload can lead to overheating and hardware damage.

Happens Without Your Knowledge – You won't see any notifications; it runs silently in the background.

What is CJ-Sniffer?

CJ-Sniffer is a smart detection system designed to identify cryptojacking activities on a network without inspecting personal user data. Traditional methods like antivirus software or browser extensions are not very effective because:

> Hackers constantly change their tactics to avoid detection. Organizations have large networks with thousands of devices, making individual monitoring difficult.

> Some cryptojacking attacks use encrypted connections that antivirus programs cannot analyze.

> CJ-Sniffer works at the network level, meaning it observes how data moves through an internet connection rather than scanning individual devices

Methodology and Results

CJ-Sniffer works in **three phases**:

1. **Traffic Filtration** – Removes irrelevant network traffic (e.g., general browsing, emails, media streaming) to focus on suspicious activity.
2. **Cryptomining Detection** – Uses **packet interval analysis** and a **Kolmogorov-Smirnov (KS) test** to detect mining activities.
3. **Cryptojacking Detection** – Uses a **Long Short-Term Memory (LSTM) machine learning model** to differentiate between **user-initiated mining** and **unauthorized cryptojacking**.

Key Findings

- **CJ-Sniffer achieves 99% accuracy** in detecting cryptojacking.
- **Fast real-time detection** makes it ideal for large networks.
- **Privacy-focused** – Does not inspect packet content, ensuring user privacy.

Challenges

CJ-Sniffer faces the following challenges:

- **Cryptojacking traffic is small** – Hard to detect compared to general internet traffic.
- **Hackers use evasion techniques** – Attackers use encryption, VPNs, and proxies to hide mining activity.
- **Balancing speed and accuracy** – Needs to operate in real-time while keeping false positives low.

Results

- **CJ-Sniffer successfully detects cryptojacking with 99% accuracy**.
- **Real-time processing ensures quick detection in enterprise networks**.
- **Unlike traditional methods, CJ-Sniffer differentiates between legal and unauthorized mining**.

Conclusion

CJ-Sniffer is an effective tool for detecting cryptojacking in **large-scale networks**. Unlike traditional methods, it does not block all cryptocurrency mining but specifically targets **unauthorized mining**.

Future Improvements

- Expanding detection to **more cryptocurrencies**.
- Enhancing resistance to **advanced evasion techniques**.

CJ-Sniffer provides a **robust, privacy-preserving, and efficient** solution to protect networks from cryptojacking attacks.

Reference

Yebo Feng, Jun Li, Devkishen Sisodia. *CJ-Sniffer: Measurement and Content-Agnostic Detection of Cryptojacking Traffic*. 25th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID 2022), October 26–28, 2022, Limassol, Cyprus. DOI: https://doi.org/10.1145/3545948.3545973