4-бөлім Раздел 4 Section 4

Информатика Информатика Computer science

IRSTI 81.93.29

Enterprise Security Assessment Framework for Cryptocurrency Mining Based on Monero

Bissaliyev M.S.*, Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan, +77015539459
Nyussupov A.T., Institute of Information and Computational Technologies,
Almaty, Republic of Kazakhstan, +77073120047
Mussiraliyeva Sh.Zh., Al-Farabi Kazakh National University,
Almaty, Republic of Kazakhstan, +77059011283
*Email: mbissaliyev@gmail.com

Mining a cryptocurrency is profitable on someone's resources. It is becoming increasing problem in the enterprise to control the operations of its infrastructure while in idle or "off-work" time. In this paper we present enterprise security assessment framework for cryptocurrency mining based on Monero cryptocurrency. The framework consists from surveying power consumption on GPU mining farms and traditional desktop PCs, analysis of web resources for browser-based mining on both internal and external domain names, the handy network logs analysis tool based on the regular expressions. While there had been significant difference between GPU and traditional desktop PC's power consumption, computational ratio of the idle PCs after working time remains questionable. In the browser-based cryptocurrency mining, there were no data on public domains, however there had been a possibility for using the private domain names, thus further research and different tools are required. In the network analysis, there were not enough evidences on the network mining, and this leads to the different research question that attackers may use proxy techniques to bypass traffic filtering and network analysis.
Key words: cryptocurrency mining, monero, hidden mining, cloud abuse

Монеро негізінде криптовалюталық майнинг қауіпсіздік үшін кәсіпорынның қауіпсіздігін бағалау әдістері модельдері және алгоритмдері

Бисалиев М.С.*, әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы қ., Қазақстан Республикасы, +77015539459,
Нюсупов А.Т., Ақпараттық және есептеуіш технологиялар институты,
Алматы қ., Қазақстан Республикасы, +77073120047,
Мусиралиева Ш.Ж., әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы қ., Қазақстан Республикасы, +77059011283
*Email: mbissaliyev@gmail.com

Криптовалютаны өндеу басқа ресурстарда тиімді. Кәсіпорында жұмыс уақыты мен жұмыстан тыс уақыт инфраструктурасы операцияларын бақылау маңызды мәселеге айналып бара жатыр. Бұл мақалада Monero криптовалютасы негізінде криптовалюта жасайтын кәсіпорын қауіпсіздігі құрылымын бағалауды ұсынып отырмыз. Бұл құрылым GPU – да және дәстүрлі ДК жұмыс үстелінде энергияны пайдалануды қарастырудан, ішкі және сыртқы домен атауларының екеуінде де браузерге негізделген өңдеулер үшін веб-реурстарды талдаудан, регуляр өрнектерде инструмент негізінде ыңғайлы желі журналдарын талдаудан тұрады. GPU мен дәстүрлі ДК жұмыс үстелінде энергияны

пайдалану арасында айтарлықтай айырмашылық бар, ДК жұмыс істемей тұрған уақытта есептелген қатынас оның жұмысы аяқталған кезде күдікті болып қалады. Браузерге негізделген криптоволюталық қорғаныс негізінде, жалпыға қолжетімді домен атаулары жоқ, бірақ жеке домен атауларын пайдалануға болады, ол үшін қосымша зерттеулер және әр түрлі құрал-саймандар қажет. Шабуылдаушылар трафикті сүзуді және желілік талдауды айналып өту үшін прокси әдістерін пайдалана алатын желі талдауларда, желілік интеллект талдау саласында жеткілікті дәлел жоқ, және де бұл әр түрлі зерттеу сұрақтарына алып келеді.

Түйін сөздер: криптовалютаны өндеу, monero, жасырын өндеу, бұлтты теріс пайдалану

Методы, модели и алгоритмы оценки безопасности предприятия для криптовалютного майнинга на основе Monero

Бисалиев М.С.*, Казахский национальный университет им. аль-Фараби,
Алматы, Республика Казахстан, +77015539459
Нюсупов А.Т., Институт информационных и вычислительных технологий,
Алматы, Республика Казахстан, +77073120047
Мусиралиева Ш.Ж., Казахский национальный университет им. аль-Фараби,
Алматы, Республика Казахстан, +77059011283
*Email: mbissaliyev@gmail.com

Криптовалютный майнинг является выгодным, если он реализован на сторонних ресурсах. Для предприятия становится все более проблематично контролировать работу ИТ инфраструктуры внерабочее время. В этой статье мы представляем методы, модели и алгоритмы для оценки безопасности предприятия основе криптовалюты Monero. Модель состоит из исследования энергопотребления GPU и традиционных настольных ПК; анализа веб-ресурсов на наличие майнинг скриптов как во внутренних; так и во внешних доменных именах; инструмента анализа сетевых журналов на основе регулярных выражений. Несмотря на то, что разница энергопотребления между GPU и традиционным настольным ПК была значительная, соотношение бездействующих ПК после рабочего времени остается сомнительным. В основе криптовалютной защиты на основе браузера не было данных о публичных доменах, однако была возможность исследовать открытые поддомены, поэтому необходимы дальнейшие исследования и различные инструменты для исследования закрытых доменных имен. В сетевом анализе было недостаточно доказательств в скрытом майнинге, и это приводит к разным вопросам исследования, что злоумышленники могут использовать методы прокси для обхода фильтрации трафика и анализа сети.

Ключевые слова: криптовалютный майнинг, monero, скрытый майнинг, облачное злоупотребление

1 Introduction

Mining a cryptocurrency is profitable on someone else's resources. It is becoming increasing problem in enterprise to control the operations of IT infrastructure in the off-duty time. There had been reported cases, where IT personnel were involved in intentional abuse of utilizing enterprise resources for personal enrichment [1]. Also, there had been reported cases on cryptocurrency mining in public [2] and corporate sectors [3].

In this paper, we present the enterprise security assessment framework for cryptocurrency mining based on Monero cryptocurrency. The framework consists from the survey of power consumption on GPU hardware and traditional desktop PCs; analysis of web resources for browser-based mining on both internal and external domain names; handy network logs analysis tool based on the regular expressions.

In Section 2.1 we explore the miners and hidden mining; how mining software is spread in Section 2.2; mining detection methods in Section 2.3; case based framework in Section 3; the results and limitations in Section 4.

2 Literature Review

2.1 Miners and hidden mining

Miners can be compared to those who distribute files on torrent tracker: they provide work to the peer-to-peer network by making peers to download a movie or a music album, as a result, making it possible to download those files later from other peers later. In case of cryptocurrency, miners play the role of distributors, supporting the work of monetary system: they carry out transactions and keep the consensus about the unified state of cryptocurrency network. As the reward, miners receive cryptocurrency asset, which could be converted into the fiat money.

Cryptocurrency mining heavily worns out hardware, since it has to work with great intensity and computational load. In addition, the crypocurrency mining reduces the network bandwidth and causes network performance problems [4].

One of the important considerations for cryptocurrency mining is electricity: as the complexity grows, more computational capacity is required for the mining. Initially, a simple home computer was enough for mining, later on, miners switched to the top gaming graphics cards, and later, to specialized mining devices. At first, they were just reprogramming chips, and then application specific integrated circuits (ASICs), which gave them an opportunity to increase the performance of hash calculation and lower power consumption. The hash rate is the measuring unit of the processing power of cryptocurrency network. For example, the Bitcoin network must make intensive mathematical operations for securing the network. When the network reached a hash rate of 1 Th/s, it meant it could make 1 trillion calculations per second [5].

After the hardware acqusisition, the cost of the miner consists of the utility bills: electricity and the Internet. In 2011, the purchase of a top-end video game card for mining could be paid off in approximately two weeks, but with the increasing complexity, it had became increasingly expensive to get investments recovered in such short time frame.

2.2 Mining software distribution

There are many methods exists for spreading mining software from Trojans, abuse of the resources, cryptojacking and to the threat of the bring-your-own-devices.

Inserting the malicious code into the downloaded software [6]. Such programs are usually called Trojan horses, as they are masked as *genuine tools*. By misleading users, such malicious program resides in the victim's machine and activates its hidden functions.

Embedding the code in mailing lists [7]. This method is implemented on the basis of sending spam messages, which usually contain malicious code or malware. The recipients of such attachments are unaware of the danger and are often exposed to them.

Transmitting through social networks [8]. Social networks are the most favorable place for malicious activity. With the help of various methods of social engineering, on the basis of the weakness of the human factor, the active spread of malicious software is explored.

Cryptojacking web resources [9]. Cryptojacking refers to the process by which web administrators insert a piece of JavaScript code into the websites for the purpose of hidden digital currency mining. In most cases, the malicious script is the Monero miner, which is used for the hidden mining of the Monero cryptocurrency. The Monero miner is developed

on the basis of the cryptocurrency service Coinhive [10]. Especially vulnerable are the advertising modules of the most popular web resources. In reported cases, by injecting the small Javascript code, web administrator was earning $10,000 per month [11].

Bringing Your Own Device. It had been reported that attackers use enterprise technical infrastructure to bring your own device (BYOD) [12] in order to avoid paying the utility bills such as electricity and the Internet usage.

2.3 Mining detection methods

Standard antivirus tools reduce risks but do not guarantee a complete solution due to the fact that mining is a standard application process that is launched by many users [13].

Another approach is deploying the network policy at the enterprise level: there are known IP addresses, hostnames, and miner signatures. However, miners may combine their computational resources into grouped or pool mining.

While we are solving problems with the pool mining, solo or personal mining is becoming an issue, since the miners can configure network settings in their own desirable way to bypass the network filtering methods.

3 Material and Methods

Based on the literature readings, we propose the theoretical framework based on the power consumption usage, network analysis, and tool for scanning web resources (Figure 1).

The power consumption, mining software and network logs defined within the context of mining in enterprise organizations. The research method is based on the case study research methods used in software engineering [14]. The power consumption is divided into two units of analysis. First is the GPU farms power consumption. Second unit of analysis is considered that during the off-work time, the IT administrators may use the desktop PCs and make them work for their purposes. In the mining software context, we observe the Monero based web browser mining and for public and private domains based on the web resources. In the network logs analysis, we study the raw network logs generated on the firewall.

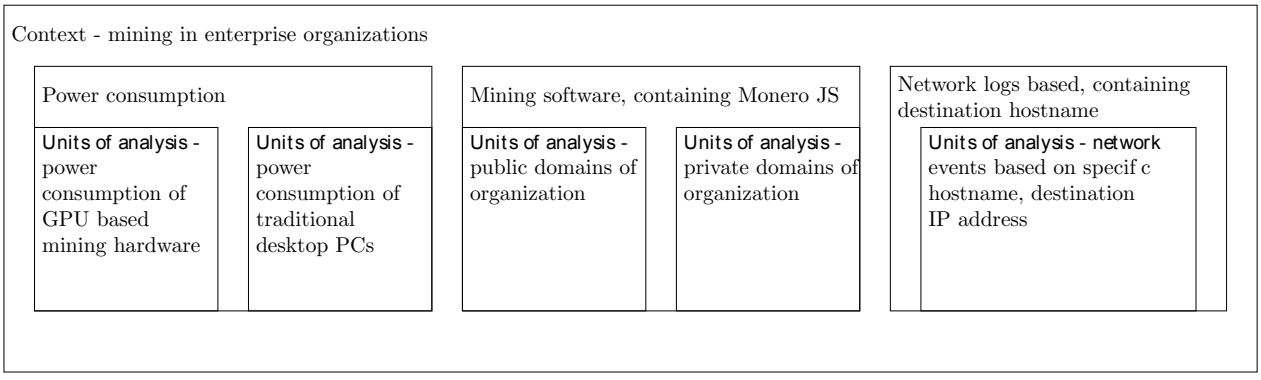

Figure 1 – The theoretical framework based on the power consumption usage, network analysis, and tool for scanning web resources.

3.1 Power consumption of mining hardware

For data collection on power consumption, *Floureon power meter Energy Monitor TS-836A* was used (Figure 2). The data had been collected during 30 days period, running 24 hours without interruptions.

The components of Setup #1 (Figure 3): 6x Nvidia GTX 1080 Ti, 1x Motherboard, 4x 2GB RAM, 1x Intel Celeron CPU, 1x 500GB HDD, 6x Power Risers Generation 4.

The components of Setup #2 (Figure 3): 2x AMD Radeon 480, 1x Nvidia GTX 1050, 1x Motherboard, 1x 500GB HDD, 4x 2GB RAM, 2x Power Risers Generation 4. The power consumption was calculated as following:

$$E_{(kWh/day)} = P_{(w)} \times t_{(h/day)} \div 1000_{(W/kW)}$$

Where:
E - electricity power consumption per day in *kilowatt-hours*
P - power in *watts*
t - time in *hours*

The data had been collected for 30 days period. The power consumption rate based in Almaty, Kazakhstan prices.

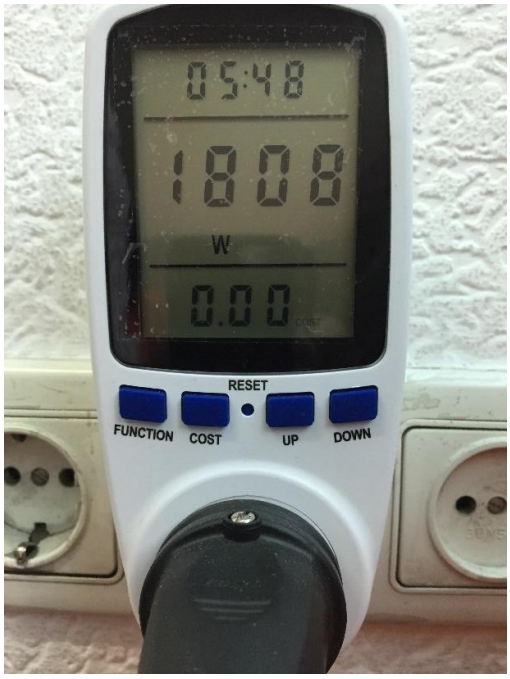

Figure 2 – Power Meter Energy Monitor TS-836A shows the power consumption of setup #1 consuming an average of 1,800 Watts per hour running on the sample rate of 5 minutes.

Figure 3 – Example of cryptocurrency miner setup: at the bottom level Setup #1 is shown; at top Setup #2 is shown. We compare data to the average power consumption of Desktop PC with LCD Display [15].

3.2 Detection framework for Monero web miner

One of the techniques is the injection of Javascript code or the Monero library into the web page. The following framework was developed.

Algorithm 1: Detect Monero Miner in Web Resources

Input : Text file with the list of websites
Output: List of websites with boolean values for Monero miner

```
Load list of websites
while The end of the file do
    Scan next website in the file
    Get the source code of the web page
    Search of malicious Javascript code, containing Monero miner
    if match = true then
        flag = true
        append website name, flag, scantime to report file
    end
end
return final report containing viruses-miners on input website
```

The method for the analysis of Monero miner is based on case study unit analysis within *Mining software, containing Monero JS* (Figure 1).

3.3 Network events log analyzer

The data was collected in the raw text containing between 7-8 million events. Due to the absence of applications for analyzing the real time traffic, the custom solutions was developed for analyzing processed traffic using regular expressions.

Algorithm 2: Universal network logs analysis based on Fortinet logs structure using regular expressions

```
Input  : Network Log Files
Output: Grouped Data From Logs
Put all files into one folder
Concatenate log files into one log file
Load list of websites
Set regex search:
(date=\d+-\d+-
\d+\s+time=\d+:\d+:\d+)(.*)(srcip=\d+\.\d+\.\d+\.\d+)(.*)(srcport=\d+)
(.*)(hostname=.+?\")
while The end of file do
    if search = true then
        Store match into the database
    end
end
```

4 Results and Discussion

4.1 Results on power consumption

The data had collected during for 30 days period, running 24 hours without interruption (Table 1). The data is limited to the traditional electricity miners, not included with the photovoltaic-based (solar miners) [16].

Table 1 – Results on of power consumption of Setup #1, Setup #2 (Figure 3) and average desktop PC with LCD display. The cost was calculated based on Almaty, Kazakhstan power grid provider rate in 2017.

Item Name	**Setup #1 (6x Nvidia GTX 1080 Ti)**	**Setup #2 (2x AMD Radeon RX480 +1 Nvidia GTX 1050 Ti)**|	**Average Desktop PC with LCD display [15]**
Average Power consumption (Watts/hour)	1.8	0.45	0.1
Hours of operation per day (hours)	24	24	24
Total kWs per day (kWs)	43.2	10.86	2.4
Price per kWh (in US Dollars)	$0.082	$0.082	$0.082
Number of operating days	30	30	30
Total cost (in US Dollars)	$106.27	$26.71	$5.90

4.2 Results on Monero miner analysis on subdomains

While we were able to make the analysis on public subdomains, however, we were unable to analyze the internal domain names. The data of the full Uniform Resource Identifier (URI) was truncated (Table 2).

Table 2 – Results on the Monero web based miner on the enterprise domain and subdomains.

URL	isExist	Scan Timestamp
kaznu.kz	FALSE	April 7, 2018 15:03:18
univer.kaznu.kz	FALSE	April 7, 2018 15:03:18
pps.kaznu.kz	FALSE	April 7, 2018 15:03:19
online-test.kaznu.kz	FALSE	April 7, 2018 15:03:20
elibrary.kaznu.kz	FALSE	April 7, 2018 15:03:21
welcome.kaznu.kz	FALSE	April 7, 2018 15:03:22
repository.kaznu.kz	FALSE	April 7, 2018 15:03:22
icd.kaznu.kz	FALSE	April 7, 2018 15:03:22
science.kaznu.kz	FALSE	April 7, 2018 15:03:23
portal.kaznu.kz	FALSE	April 7, 2018 15:03:23
journal.kaznu.kz	FALSE	April 7, 2018 15:03:24
open.kaznu.kz	FALSE	April 7, 2018 15:03:24
post.kaznu.kz	FALSE	April 7, 2018 15:03:24
student.kaznu.kz	FALSE	April 7, 2018 15:03:25
be.kaznu.kz	FALSE	April 7, 2018 15:03:25
philart.kaznu.kz	FALSE	April 7, 2018 15:03:25
cu.kaznu.kz	FALSE	April 7, 2018 15:03:26
bulletin-geography.kaznu.kz	FALSE	April 7, 2018 15:03:27
jirbis.kaznu.kz	FALSE	April 7, 2018 15:03:28
ijbch.kaznu.kz	FALSE	April 7, 2018 15:03:28
dl.kaznu.kz	FALSE	April 7, 2018 15:03:29
univer_okmpi.kaznu.kz	FALSE	April 7, 2018 15:03:30
connect.kaznu.kz	FALSE	April 7, 2018 15:03:31
bulletin-history.kaznu.kz	FALSE	April 7, 2018 15:03:32
demou.kaznu.kz	FALSE	April 7, 2018 15:03:33
atu.kaznu.kz	FALSE	April 7, 2018 15:03:34

4.3 Results on network log analysis

We analyzed between 7.5 and 8 million events with the total of 4.4 GB of logs. As the example, singular regular expression (regex) with four search groups was proposed. The groups consist of date, source IP, source port and hostname respectively. However, the regular expression may have different setup depending on the required search groups.

While the log analysis required significant amount of time to process the large datasets, on demand analysis tools are required.

In the network analysis, there were not enough evidences (Table 3) on the mining: this may lead to the different research question that attackers may use proxy techniques to bypass traffic filtering and network analysis.

Table 3 – Categorized data collected from the enterprise firewall.

Category	Number of Events	Percent
Mining	17,180	0.22605
Uncategorized	7,582,820	99.77395
Total	7,600,000	100.0

5 Conclusion

In this paper, the conceptual framework for enterprise security assessment for cryptocurrency mining detection was proposed. Within the framework, the different units of analysis in three different contexts: power consumption, application mining and network analysis were proposed. While there is significant difference in power consumption between GPU and traditional desktop PC's, the ratio of the idle PCs and GPUs after the duty time still questionable. On the browser-based cryptocurrency mining, there were no evidence that application mining exists on public domains, however, investigation on internal domain names should be considered. On the network analysis, there were little data on the network mining, and this may lead to the different research question that attackers may use proxy techniques to bypass traffic filtering and network analysis.

The results of this paper were presented in the 2nd International Summer School "Mathematical Methods in Science and Technology"held in Almaty, Kazakhstan, 28 May-08 June 2018.

References

[1] Broderick, Ryan. "How to Get Rich on Bitcoin, By a System Administrator Who's Secretly Growing Them On His School's Computers". Motherbard. 2011. Accessed May 5, 2018.
https://motherboard.vice.com/en_us/article/nzzz37/how-to-get-rich-on-bitcoin-by-a-system-administrator-who-s-secretly-growing-them-on-his-school-s-computers

[2] Getbitcoin.com.au. "Government employee caught mining using work supercomputer". Getbitcoin.com.au. 2014. Accessed May 5, 2018.
https://www.getbitcoin.com.au/bitcoin-news/government-employee-caught-mining-using-work-supercomputer

[3] Falconer, Joel. "ABC employee caught mining for Bitcoins on company servers". The Next Web. 2011. Accesssed May 5, 2018.
https://thenextweb.com/au/2011/06/23/abc-employee-caught-mining-for-bitcoins-on-company-servers/

[4] Seals, Tara. "ABC employee caught mining for Bitcoins on company servers". Infosecurity Magazine. 2018. Accessed May 5, 2018.
https://www.infosecurity-magazine.com:443/news/cryptomining-spikes-500/

[5] Bitcoin.org. "Some Bitcoin words you might hear". Vocabulary Bitcoin. 2018. Accessed May 5, 2018.
https://bitcoin.org/en/vocabulary

[6] Makandar, Aziz, and Anita Patrot. "Trojan Malware Image Pattern Classification". Paper presented at the annual International Conference on Cognition and Recognition, 253-262. Springer, Singapore, 2018.

[7] Edge, Charles, and Daniel O'Donnell. "Malware Security: Combating Viruses, Worms, and Root Kits". Paper presented at the annual conference for the Enterprise Mac Security, 221-242. Apress, Berkeley, CA, 2016.

[8] Hajli, Nick, and Xiaolin Lin. "Exploring the security of information sharing on social networking sites: The role of perceived control of information". Journal of Business Ethics, 133, no. 1 (2016): 111-123.

[9] Zalbina, M. Ridwan, Tri Wanda Septian, Deris Stiawan, Moh Yazid Idris, Ahmad Heryanto, and Rahmat Budiarto. "Payload recognition and detection of Cross Site Scripting attack". Paper present at the annual conference for Anti-Cyber Crimes (ICACC), 2017 2nd International Conference, 172-176. IEEE, Abha, 2017.

[10] Coinhive. "Coinhive – Monero JavaScript Mining". Coinhive. 2018. Accessed May 5, 2018. https://coinhive.com/

[11] Eskandari, Shayan, Andreas Leoutsarakos, Troy Mursch, and Jeremy Clark. "A first look at browser-based Cryptojacking". Accessed May 5, 2018 *a*rXiv preprint, arXiv:1803.02887, (2018).

[12] Miller, Keith W., Jeffrey Voas, and George F. Hurlburt. "BYOD: Security and privacy considerations". *I*t Professional, 14, no. 5 (2012): 53-55.

[13] Kizza, Joseph Migga. "Virus and Content Filtering". Paper presented at the annual conference for Guide to Computer Network Security, 325-343. Springer, London, 2015.

[14] Runeson, Per, Martin Host, Austen Rainer, and Bjorn Regnell. *Case study research in software engineering Guidelines and examples.* (New Jersey: John Wiley & Sons, 2012), 135-136.

[15] Pickavet, Mario, Willem Vereecken, Sofie Demeyer, Pieter Audenaert, Brecht Vermeulen, Chris Develder, Didier Colle, Bart Dhoedt, and Piet Demeester. "Worldwide energy needs for ICT: The rise of power-aware networking". Paper presented at the annual conference for Advanced Networks and Telecommunication Systems, 2008. ANTS'08. 2nd International Symposium on, 1-3. IEEE, Bombay, 2008.

[16] Torpey, Kyle. "How Bitcoin Mining Could Solve One Of The Issues With Space-Based Solar Power". Forbes. 2018. Accessed May 5, 2017. https://www.forbes.com/sites/ktorpey/2017/09/15/how-bitcoin-mining-could-solve-one-of-the-issues-with-space-based-solar-power/#1d98e4a22c8d