# ACJS: "Anti-Crypto Jacking System" Security Development.

Ahmed Mabrook Rafeequ[1], Intan Farahama Binti Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]

[1'2]Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia.

[1]ahmedrafeequ@gmail.com, [2]intan.farahana@staffemail.apu.edu.my, [3]zety@staffmail.apu.edu.my, [4]hemalata@staffmail.apu.edu.my

***Abstract* – Computer users globally are common targets for attackers, including for the rising threat of crypto jacking. The threat on illegal crypto mining, has been ongoing since 2017, and it has done devastating levels of damage to users and organization's devices all around the world. Few solutions had been developed by various communities to mitigate the threat. However, there has not been a solution brought whereby a single software is able to automate the steps and processes to remove crypto jacking threat from user devices, till date. The aim of this research is to propose a single software based automated solution to eliminate the threat of crypto jacking from its users, through means of system analysis and threat removal approach by automation. At the initial stage of research, numerous surveys, analysis, and literature review will be carried out. From here, a prototype of the proposed systematic solution will be developed with the results harvest in the former stage. Finally, the proposed application will be promoted to computer users, as a step to ensure secure computer usage, and to eliminate crypto jacking.**

***Index Terms***

Blockchain Technology, Cryptocurrency, Crypto Jacking, Crypto Mining, Cyber Threat, Ransomware, Malware, Security Development.

## 1. Introduction

The world is advancing in fields of technology and science in a daily basis. It plays an essential role in making lives convenient and successful. Most businesses, societies and families are adapting to such changes, and is embracing technology as the new way of making progress in life. While this is an achievement for community, with such great advancements, certain obstacles must be confronted.

People are exposed to socializing, communication, exploration and learning regularly, through means of online resources and applications. Apart from such, the world is embracing the new technology of Blockchain, and online currency, better known as crypto currency. Huge investments are made to these blockchains annually. People utilize these forms of currency to perform transections and use it as a form of payment for most available services in society.

Crypto mining is the process of validating a cryptocurrency transaction. Since Crypto mining can be accomplished by any organization and household (being said that it is legal to conduct in place of residence, and user has the appropriate hardware and environment for the process), users thrive to come up with new ways to raise their rewarded income through this process. While tools, applications came to proper developments, many users have utilized them to connect their hardware to the dedicated mining pools, and to join part with the mining community. However, there are cyber criminals, who makes use of such software to follow a practice called Crypto jacking, which is the unauthorized use of another user's computer/hardware to mine cryptocurrency.

There are various ways in which an attacker conducts Crypto jacking, with the utilization of malicious mining scripts. These mining scripts works in background, while unsuspecting victims use their computers normally. The only sign they would notice, would be the slower performance/lags during its execution. Such scripts can cause devastating harm to victims' device over short period of time.

To ensure proper level of protection of user devices, a software can be used to utilize multiple set of tools, which aims to detect and eliminate such threats from executing user devices at the soonest. The tools would mainly focus on Pre-detection, Isolation of the crypto jacking scripts, and elimination of the threat from the device before the device falls to being victim of crypto jacking.

This research concept paper would highlight an approach to counter the threat of crypto jacking, while emphasizing on the methods used by the application to mitigate such threats, how data is collected and circulated for the application to function and provide a better understanding on why this application would play a vital role on providing protection service to its consumer, to ensure that their online experience is safer and convenient.

## 2. Literature Review

## 2.1 Research Domain

### 2.1.1 Blockchain, Crypto Mining and Crypto Jacking.

Blockchain is a chain of information that timestamps digital transactions, so that they cannot be duplicated or backdated from record. It is an open platform for anyone to access. The technology was first outlined by Stuart Haber and W.Scott Stornetta, two mathematicians who desired to implement a system where document stamps could not be tempered with [1]. Blockchain consist of crypto currencies, which are digital currencies used for transections, and is earnable through means of mining (reward for breaking block algorithm) and investment. To the current year, there are more than 10,000 active cryptocurrencies based on blockchain, in addition to several hundred more non cryptocurrency blockchains [2].

Crypto Mining refers to the competitive process of verifying and adding new transections to the blockchain for a cryptocurrency that utilizes the proof-of-work (PoW) method [3].

According to [4], Crypto jacking is defined to be the illegal act of crypto mining, that happens when cybercriminals hijack user devices to install mining scripts/software. Such scripts utilize the computer's power and resources to mine cryptocurrencies, or steal crypto wallets owned by its victims.

Crypto jacking was first noticed in September 2017, when Bitcoin (A cryptocurrency) prices were at its peak. Coinhive had a script released in its website during that period, which was intended to be a mining tool for website developers to passively earn income, through means of ad display on their websites. However, it was soon noticed by cybercriminals as a potential to earn cryptocurrency at large scale, and from that time, crypto jacking evolved [4].

A midyear threat report from Webroot in 2018, showed that crypto jacking had a 35 percent share of all web threat [5]. Since the evolution of Blockchain technology, many criminals try to come up with ways to gain lot of income by exploiting vulnerable devices. There are three methods on which crypto jacking is executed by cyber criminals.

- File-based Crypto Jacking:

  Malware is downloaded and runs an executable file which infects a crypto mining script throughout the victim's device. The method has been a more efficient way of crypto mining than web-based mining, being 25 times more profitable [6].

- Browser-based Crypto Jacking:

  Hackers use crypto mining scripts which are embedded into web browser, through means of website plugins, text, or ads. The Threat Landscape Trends Report for Q2, 2020 showed that crypto jacking saw a 163% rise in detections, in comparison to the past quarters [6].

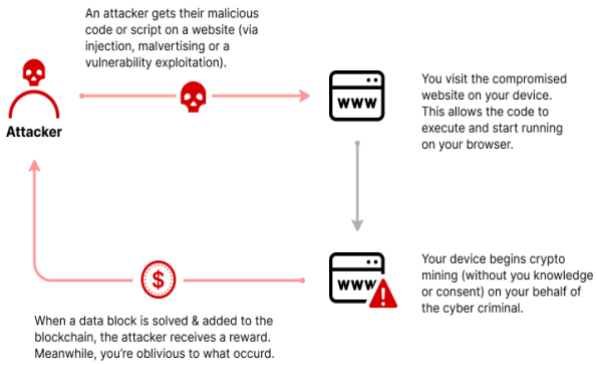


**Figure 1: Browser-based crypto jacking illustration.**

- Cloud-based Crypto Jacking:

  Cloud crypto jacking involves hacker attempting to gain access through the organization's cloud services (with access to API key). If access is gained, attackers would be able to siphon unlimited CPU resources for crypto mining. The attacker scans the network for vulnerable systems in any environment, often which are cloud providers, as they are opportunistic to such attacks [7].

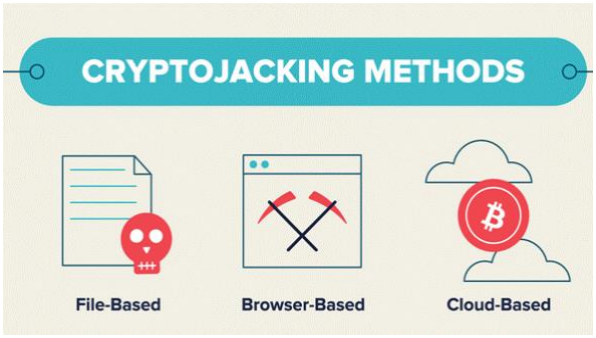


**Figure 2: The three main methods of Crypto Jacking.**

In the year 2019, 39.3% of the crypto mining infections targeted Japan, 20.8% targeted India, 14.2% targeted Taiwan [8]. Crypto jacking has its victims targeted worldwide, and this is due to lack of awareness amongst many daily computer users, and enterprises. Victims of crypto jacking mostly notice a slower performance on their computers, yet they may be unaware that their machines are held as a source for crypto mining to attain cryptocurrency [9].

Based on [10], there are various ways on detecting and eliminating the threats of crypto jacking from one's device, but there isn't a single-step solution to mitigate the overall approach of crypto jacking. Likewise, many studies that backup on ways to mitigate crypto jacked devices, usually show manual steps on multiple approaches, to ensure the proper removal of the mining

script from user device, hence indicating the need of a system will all-in-one solution against crypto jacking. Therefore, in this research, all 3 methods of crypto jacking would be taken to consideration to be mitigated through the development of a single, automated systematic solution against crypto jacking.

### 2.1.2 Cyber threats and Security Development

According to [11], a cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. These types of threats indicate the possibility of a successful cyber-attack, which may have the aim to gain unauthorized access into an information technology asset, network, or property.

Security development is the process which involves people and practices to ensure that a certain threat is eliminated through means of confidentiality, integrity, and availability. Under security development, consist of software security development. According to [12], Secure software development is a methodology that incorporates into every step of software developing life cycle, when creating a software.

For over two decades, the internet has played an essential role in global communication and has become increasingly integrated into the lives of people around the globe. Innovations and low cost in the subsequent area have exorbitantly raised the availability, use and performance of the internet, and has resulted with almost 3 billion internet users worldwide [13]. As such, the internet became a platform for attackers to prey on users, for various causes, and purposes. According to the Crypto Crime report [14], 2020 was the "year of Ransomware" due to the vast growth in crypto currency extorted in ransomware attacks. By January 2022, it was identified that there were ransomware payments worth over $692 million in 2020 [14]. Attackers based most of their attacks with the growth of blockchain industry, and most these attacks were targeted to users due to the number of vulnerabilities present in user devices.

Therefore, in this research, the threat of ransomware in association to crypto jacking would be taken to consideration to be mitigated through the implementation of secure software development for the proposed software.

### 2.2 Similar System

To current date, there have been numerous usage and upgrades brought to antivirus software's, to address crypto jacking. Antivirus tools help reduce the threat of crypto jacking, by reducing the entry and spreading of mining malware and scripts in system.

A good example, Kaspersky, provide web security service against web mining. The antivirus brand also provides on-system protection to prevent malware and other harmful viruses from settling in the device.

Anti-Crypto mining browser extension had also been developed, that works on protection user from web-based exploitation (mining) when enabled by the respective browser in-use (Example, NoCoin web-extension).

| Features | Antivirus | Web extension | Proposed ACJS Application |
|---|---|---|---|
| **Protection against web-mining** | Some, mostly through premium subscription. | Available | Available |
| **File/script-based mining** | Available | Unavailable (Only web) | Available |
| **Automation (Automatic threat detection)** | Some, requires manual scanning | Available (Only Web) | Available Fully automated, runs in background |
| **Basic safety against virus** | Available | Unavailable Specific protection against web-based threats | Unavailable, only specialized to protect against crypto jacking |

**Table 1: Difference between proposed application, antivirus, and anti-mining web extension regarding anti-crypto jacking.**

As per the Table 1, the proposed ACJS application provide complete automated solution to all crypto jacking-based threats (Both web-based and filed-based) in a single software. However, the proposed solution does not provide any assistance when dealing with other forms of threats, as it is dedicated to mitigating threats specified for crypto jacking only. Hence, the development of ACJS would prove to be a great step to fight against crypto jacking, as a single automated security application.

## 3. Problem Statement

Most of our daily activities are associated within the internet. Users interact with online resources very frequently, whether it be an image, video, application or even a message. As such, users often must confront the potential threat of having their devices harmed by the execution of harmful files, like crypto jacking scripts. Users face a lot of problems regarding the stated threat. Firstly, insecure internet browsing experience as crypto jacking codes can be embedded in major file formats. The execution of malicious mining script results in significant loss of performance in devices. In addition to that, crypto mining triggered by

the tool harms user's hardware, making a huge loss financially.

The problem of crypto jacking came to notice from September of 2017, when attackers first got their attacks on users through the accidental release of a remote mining script from the organization, Coinhive, which was intended to provide a source of income for web developers [15]. Since then, attackers have continued to utilize various methods to gain control over user devices, to establish a connection and hence, misuse the connection to gain income.

One concerning approach by crypto jackers, to hijack a user's computer, is direct web connection to the user's device. Many attackers have utilized the infamous Coinhive service, which allows websites to use their victim's device to mine Monero cyptocurrency [16]. As such, several websites that we visit daily gets affected with plugins getting hijacked, due to servers getting hacked from mining codes.

A surge in such attacks were seen from the start of 2018, whereby several high profit companies, became victims of the crypto jacking trend. Starbucks in Buenos Aires and media giant YouTube were two companies that were majorly targeted for the attacks, as they had tremendous number of visitors, making them easy targets for attackers back in time. Four online video sites, providing close to one billion users monthly, were potentially appealing their users in crypto mining unknowingly [17]. Another example on how Crypto jacking became a major issue, was when the LA times website was compromised, which became a drive-by mining site for many attackers due to the poorly established configuration of Amazon Web Service (AWS), along with Tesla's public cloud service.

To the current date, there had been few potential countermeasures taken against mining from web exploitation, which is blacklisting domains based on their resource consumption. As for user storage protection from such mining scripts, antivirus software's often provide a layer of protection to save known script injections and connections from taking place. The flaw on such countermeasure, is that these approaches are easily mitigated by attackers, as they can develop new approach to establishing a connection to user's device and continue mining remotely.

## 4. Research Aims and Objectives

### 4.1 Research Aims

The aim for this project is to solve the problem faced by computer users, regarding potential exposure to crypto mining scripts, through means of digital automation (to ease user interactivity with the application) with the implementation single-software approach to overcome all crypto jacking-based threats.

### 4.2 Research Objectives

The objectives of this project, are as follows:

- To integrate automation and system program activity analysis to detect crypto jacking scripts from any file format.
- To evaluate user device safety and security through the usage of the proposed all-in-one anti-crypto jacking application against illegal crypto mining.
- To broaden the database based on the various approaches made by attackers to infiltrate user devices and promote alternative approach to mitigate such threats from similar attacks in future.
- To collect data based on infective scripts that enter the user's device, and store profiles in database.

## 5. Research Significance

The outcomes from this research would provide support to the user device safety, regardless the platform and type of device in use. Users can establish an understanding on the threat of crypto jacking, and how it affects their devices when infested. Centered on this, users can continue to investigate whether their device is a victim of such threat, by conducting an analysis on the changes in system performance.

For the researchers, this proposal would provide some insight into the potential of using a single-application solution to address the problem of web-based and file-based crypto jacking. As such, a better application that can address and alleviate crypto jacking threats in addition to other forms of cyber hazards might be invented in the future.

## 6. Methodology

To conduct the research paper effectively, quantitative research has been carried out to develop an understanding on why crypto jacking is posing threat to user devices, and how hard it is to counter the mining infestation from the devices. The research will involve a short survey, which consist of questions regarding the user experience with dealing crypto jacking threats.

For the purpose of research, the questionnaire had been conducted through mean of survey as most users can be approachable online. Due to the pandemic, physical interactions have been restricted, and the only proper mean to interact with people, is through online socialism. Hence, it is best to conduct quantitative research through survey-based questionnaire as it is easier to reach to such users online, and the survey takes less time to complete.

The survey consists of 7 multiple choice questions, and 3 questions with Likert scale ranging from 1 to 7. For the aim of achieving efficiency in research, Google forms would be used to deliver the questions to the users. Google forms is a good choice to conduct the survey with, as it helps collect data from respondents, and provide visual and graphical representation of the results obtained, based on its respective options. In addition to that, the responses can be viewed privately.

To classify the respondents that would be selected for the research analysis, a sampling method known as Systematic sampling will be utilized. For every 1 person selected, the following 5 subsequent users will be skipped. As such, the process is intended to be repeated until the sample has a total of 150 people, and the followed questionnaire will be sent to them accordingly. Respondents would be provided with 2 days' time from the date they receive the questionnaire. After the duration of 2 days, the results obtained would be analyzed, and would be cleared of any repetition to ensure accuracy of results obtained. The resulting 70 respondent's results are marked qualified for the research.

To ensure that the results received meets the criteria mentioned, a comparison would be made, between the literature review and the results from the questionnaire. A general conclusion can be made on how the users are affected with crypto jacking, and on how they are targeted. Based on research data gathered from the previous research, a prototype will be developed to address the ways they get targeted for crypto jacking, and how quickly (through their everyday browsing activities made online.). The developed prototype would be sent to few participants of the survey, whereby each candidate would be given a set of 3 months to explore, test and report any form of difficulties or bugs they face when using the prototype. Feedbacks and suggestions for the prototype are also openly accepted.

After the testing phase for 3 months, the respondents who engaged with the prototype will do the same questionnaire again, this time based on their current experience. This will be used to make a comparison on the results obtained before. This is to establish a good understanding on whether the proposed system would help users mitigate the threat of crypto jacking. Based on the results obtained, new improvements would be brought to the application to ensure better performance and rection time.

## 7. Overview of the Proposed System

The proposed system has a simple yet efficient approach to resolve the problem of crypto jacking.

The following shows how the attack usually takes place, followed by how the proposed system would function to mitigate the threat from the device.

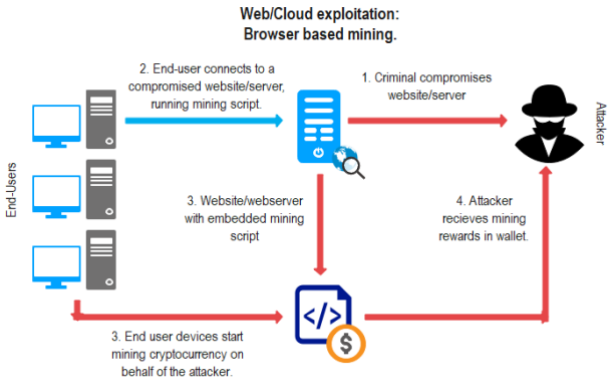


**Figure 3: Web/Cloud based Crypto jacking.**

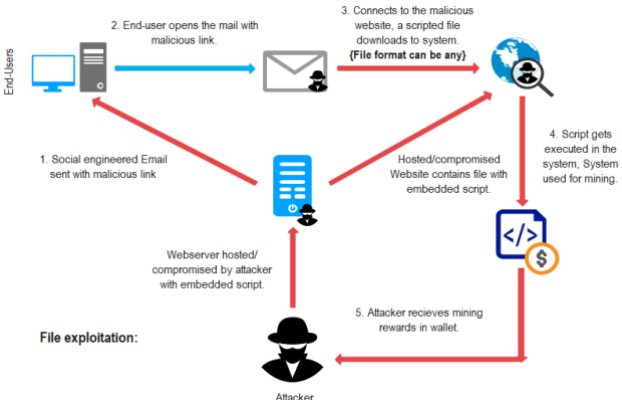


**Figure 4: File based Crypto jacking.**

The two illustrations show above are the base approach made by attackers to infiltrate to user device and utilize the system for crypto mining.

To counter these two issues combined, the proposed application would follow the following methods.

- Web based protection: The proposed application monitors incoming and outgoing network traffic and determines if the website was flagged for mining/incoming and outgoing communication is used for mining (also monitors system performance based on browser activity, individually).

  If it is flagged, the inbound and outbound connection is blocked, and a report would be generated and would be sent to universal database.

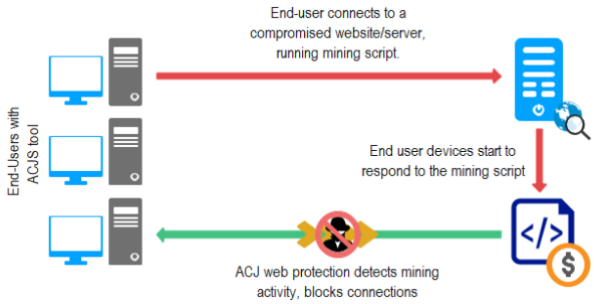


**Figure 5: Web-based protection against crypto jacking.**

- File based protection: The proposed system carries out two major functions to protect user device from crypto mining.

  Firstly, device performance is kept in check, and storage is often scanned (Light-scan to avoid performance disruption) to ensure that there is no script present in the device.

  Secondly, a detailed scan is made from all files that are being downloaded to system (file of any format) to check for any hidden text/embedded script, based on the crypto-mining connection pool and any identification of a wallet (such records can be accessed online as they are free source, e.g., Mining pool hostnames).

  If, in either case, a script was flagged by the application, it will remove and lock the inbound connection to severe the connection between the mining pool and device.

  Here, a detailed report is generated, and the threat is safely disposed from the system.

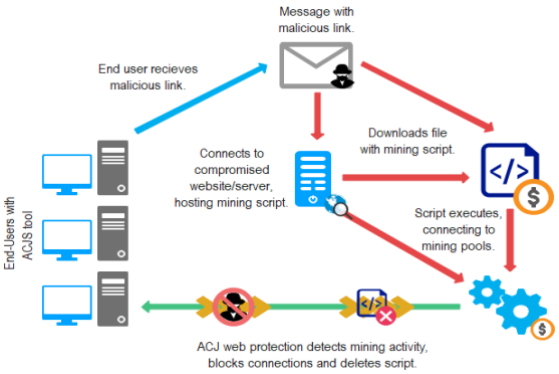


**Figure 6: File-based protection against crypto jacking.**

## 8. Conclusion

With the development of the ACJS application and implementation, the system can monitor the device's performance level, connections and the activities hosted by the device. These analysis steps would allow the application to determine any sense of crypto jacking activity that might be associated with the device in use. When a threat gets flagged, the user will be pinged with the notification, and regardless, the application would take the necessary steps to mitigate the threat from the device. With this, user's online usage would be made more secure, and device health can be maintained efficiently.

## Acknowledgments

The highest gratitude to Ms Intan Farahana who offers guidelines and advice in a module called Research Methodology in Computing and Technology (RMCT). Through this, an opportunity is provided for creating the research paper. Thanks to Asia Pacific University of Technology and Innovation (APU) for the international conference opportunity and for the journal publication.

## References

- **[1]** Coinbase. (n.a.). *What is a Blockchain*. Coinbase. https://www.coinbase.com/learn/crypto-basics/what-is-a-blockchain
- **[2]** CoinGecko (2022). *Cryptocurrency Prices by Market Cap.* CoinGecko. https://www.coingecko.com/
- **[3]** PCmag (n.a.). *Crypto mining*. The PCmag. https://www.pcmag.com/encyclopedia/term/crypto-mining#:~:text=(CRYPTOcurrency%20mining)%20The%20competitive%20process,the%20ways%20mining%20is%20performed.
- **[4]** Rob, S. (2021, January 29). *What is Cryptojacking? Prevention and Detection Tips.* Varonis. https://www.varonis.com/blog/cryptojacking
- **[5]** Newman, L.H. (2018, December 24). *The year Crypto jacking ate the Web.* Wired. https://www.wired.com/story/cryptojacking-took-over-internet/
- **[6]** Threat Hunter Team (2019, April 24). Beapy: *Crypto jacking worm hits Enterprises in China.* Symantec. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/beapy-cryptojacking-worm-china
- **[7]** Gohil, S. (2018, May 18). *Cloud Crypto jacking Affecting 25% of Organisations.* Tech Monitor. https://techmonitor.ai/technology/cybersecurity/cloud-cryptojacking-organisations

- **[8]** Micro (2019, October 28). *Defending systems against cryptocurrency miner malware.* Trend Micro. https://www.trendmicro.com/vinfo/be/security/news/cybercrime-and-digital-threats/defending-systems-against-cryptocurrency-miner-malware

- **[9]** Holt, M. (2018, April 03). *Security Think Tank: Use awareness, education, and controls to halt crypto jacking.* Computer Weekly. https://www.computerweekly.com/opinion/Security-Think-Tank-Use-awareness-education-and-controls-to-halt-cryptojacking

- **[10]** Uba, J. (2021, August 26). *A Guide to Crypto jacking: Detection, Prevention and Protection Against Crypto Jacking Attacks.* Mondaq. https://www.mondaq.com/nigeria/fin-tech/1105584/a-guide-to-cryptojacking-detection-prevention-and-protection-against-cryptojacking-attacks

- **[11]** Tunggal, A.T. (2022, February 24). *What is a Cyber Threat?* UpGuard. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

- **[12]** Hyperproof Team (2022, January 27). *Secure Software Development: Best Practices, Framework and Resources.* HyperProof. https://hyperproof.io/resource/secure-software-development-best-practices/

- **[13]** Tan, S., et al. (2021, January 24). *Attack detection design for dc microgrid using eigenvalue assignment approach*. Energy Reports 7. Pp 469 – 476. https://reader.elsevier.com/reader/sd/pii/S2352484721000469?token=0302B5E5282C8A4632893402DD8FE787022948452CF2E27D67F767B4846FEA3AAEF72A5BD9EF90DA54C4F06AD8AB5F08&originRegion=eu-west-1&originCreation=20220428135724

- **[14]** ChainAlysis Team (2022, February 10). *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict.* Chainalysis. https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/

- **[15]** Allot. (2018, May). *Threat Bulletin: Crypto Jacking.* Allot. https://www.allot.com/resources/TB_Cryptojacking.pdf

- **[16]** Segura, J. (2017, November 29). *Persistent drive-by crypto mining coming to a browser near you.* Malwarebytes. https://blog.malwarebytes.com/cybercrime/2017/11/persistent-drive-by-cryptomining-coming-to-a-browser-near-you/

- **[17]** Meshkov, A. (2017, December 13). *Crypto-streaming Strikes Back.* AdGuuard Research. https://adguard.com/en/blog/crypto-streaming-strikes-back.html