Protecting your organisation against Cryptojacking

A critical look into Cryptojacking and its effect on businesses and how you can protect against it.

**Tags:** Cryptojacking, Cryptojacking for Good, Hackers, Emerging Threats in Cyber Security

# Abstract

With Cryptojacking becoming increasingly popular daily, it is crucial to deter, detect and delay such threats in all their forms. This report will include a critical analysis of the threat, a brief history, and recommendations on how a business, such as De Montfort University, can protect against these imminent threats to the company.

Andy Peterson [3] conveys a strong message; Cybercriminals are on the move. It is no longer popularised to carry out standard Ransomware hacks; we are now seeing the general hacking population move to Cryptojacking in a recent explosion in online attacks when covid hit. Recent claims suggest that Cryptojacking is more fruitful and allows hackers to increment their income in a way that most would not notice.

Contents

[Abstract 1](#_Toc121347132)

[Figures 3](#_Toc121347133)

[Introduction 4](#_Toc121347134)

[What is CryptoJacking? 4](#_Toc121347135)

[Noteworthy Cryptojacking Events 5](#_Toc121347136)

[Risk Analysis and Response 5](#_Toc121347137)

[What might be the impact of a successful attack on these assets? 6](#_Toc121347138)

[Through which routes might cryptojacking malware come into your system? 6](#_Toc121347139)

[Recommendations – Deter, Detect, Delay, and Respond 6](#_Toc121347140)

[What assets are potentially affected by cryptojacking and thus need to be protected? 6](#_Toc121347141)

[What measures could you put in place to prevent cryptojacking attacks within your organisation? 7](#_Toc121347142)

[What measures could you put in place to detect a possible cryptojacking malware infection? 7](#_Toc121347143)

[What measures could you put in place to minimise the effect of a possible cryptojacking malware infection? 7](#_Toc121347144)

[Notable Research 8](#_Toc121347145)

[Conclusion 9](#_Toc121347146)

[References 9](#_Toc121347147)

# Figures

[Contents 2](#_Toc118997855)

[Figure 1: Cryptojacking – What is it? [13] 4](#_Toc118997856)

[Figure 2: Methods of Cryptojacking [15] 5](#_Toc118997857)

[Figure 3: Cryptojacking Statistics [16] 5](#_Toc118997858)

[Figure 4: Deter, Detect, Delay, Respond 7](#_Toc118997859)

[Figure 6: Detecting Cryptojacking 8](#_Toc118997860)

# Introduction

Mostly you will not notice if you have been a victim of a cryptojacking attack; with some methods, the scripts run automatically, leaving no trace. You may see that your computing resources are running low and slow, and it will be hard to figure out why. The main goal that most hackers will have, is to remain unseen, undetected, and undeterred. As Ericka [6] mentions, “The attack methods are limited only by the cryptojackers’ creativity”. Your devices, servers, and websites could be hijacked right now, and more than likely, no one will notice. As time passes, attackers are refining their techniques and getting better at avoiding detection and evasion. This report will look at the history and ways you can deter, detect, and delay potential cryptojacking attacks.

A picture containing text, sign, outdoor

Description automatically generated

Figure 1: Cryptojacking – What is it? [13]

# What is CryptoJacking?

Cryptojacking is a form of malware that uses unsuspecting victims' computers, businesses' servers, and cloud infrastructure to mine for coins, such as Monero, without permission. There are many ways in which cryptojacking can be accomplished; more traditionally, cryptojacking was dropping malware on compute devices, delivered via phishing for unsuspecting victims to click on the shady legitimate-looking link in that email. Advanced ways of delivering illicit cryptojacking can be done through fileless malware and embedded scripts on websites and website applications. [6]

Graphical user interface, diagram

Description automatically generated

Figure 2: Methods of Cryptojacking [15]

# Noteworthy Cryptojacking Events

Here, David [4] plays devil's advocate by discussing the good ways charities are putting Cryptojacking to good use by offering the general public a way to give back by allowing said charities to mine for cryptocurrency Monero from visits to their websites. However, Coinhive is taking 30% of the profits, which brings into question whether it is ethical. Coinhive didn't think so, and in 2019, just two years after its conception decided to shut down its operations due to a large number of illicit acts hackers were using it. This initiative offered people a way to give back while also allowing donors to make an informed decision about companies and charities using cryptojacking on visiting patrons' computers, utilising their CPU or GPU to give to charity or recoup lost ad revenue.

There are business owners out there that are in a constant battle with ad blockers. Anyone with ad blockers is pre-emptively denying revenue to businesses, and with the current blow-up of cryptojacking, business owners are getting creative. Salon is just one of those businesses to take advantage of a potentially malicious piece of code and turn it into something good for their business by asking its website visitors for permission. [12]

Troy Mersch [11] has researched and discovered none less than 394 victims of the legal Javascript, Coinhive. Although Coinhive itself is not illegal, and neither is the coin that it mines, Monero, the obfuscation and using people's resources without permission make it questionable and entirely malicious. Mixed among the spreadsheet Mersch has put together of unsuspecting businesses are many education platforms, a zoo website, and governmental platforms.

[15] Discusses cryptojacking statistics and demonstrates the rise in cryptojacking style attacks over a period of time. Cook makes a note of the 19% increase in attacks year on year and notes a 30% increase at the beginning of 2022, according to a report written by Sonic Wall [8]. The information also saw a dramatic drop as the year continued, noting a pattern of increases at the start of the year and decreases towards the end of the year.

Chart, bar chart

Description automatically generated

Figure 3: Cryptojacking Statistics [16]

# Risk Analysis and Response

It is essential to consider the risks and impact that cryptojacking will have on the business and the potential costs and damage to DMU assets. As we know from this report, attackers will try to remain unseen, which may have significant consequences for the business.

Warwick Ashford [7] calls for businesses to take cryptojacking seriously, claiming that the issue is more extensive than we realise, with threat actors looking to expand and potentially setting their sights on big corporations and businesses with extensive computing infrastructure and a lot of compute, or cloud power. This way, the offenders can mine more coins, increasing their profits.

## What might be the impact of a successful attack on these assets?

If De Montfort University (DMU) is under attack or close to a breach, the most devastating impact could come from within the organisation server. It may slow down access to essential learning documents, tools and aids, and communication pathways for both staff and students. It will have availability issues should DMU experience a web hack. This could harm unsuspecting website visitors, which would impact DMU's brand and image to the outside world should it be discovered and publicised.

Firstly, the increase in power usage will hit energy consumption, increasing energy costs and decreasing performance, damaging processors, thus driving up the hardware cost to the business.

Secondly, as DMU are an educational establishment, keeping all data safe is paramount and a legal requirement, with legal ramifications if any breaches may occur. Access and availability are vital for both staff and students; with the new combined learning of online and in-person introduced since the lockdown, nothing must affect the students and staff from accessing the internal learning and communication platforms at any time. As we know that students like to study late into the night. Staff may need to prepare for the following days' activities at home.

Last but not least, threat actors are finding more creative ways to exploit vulnerabilities and may use these vulnerabilities and access them to carry out future attacks via different methods. In addition, other threat actors could use this access to carry out other cyber-attacks, making DMU exponentially more vulnerable to attack at any moment.

## Through which routes might cryptojacking malware come into your system?

As Cryptojacking is a cybercrime that will utilise individuals and business devices and resources, there are many ways to exploit this vulnerability. Below is a table detailing the attack surface of potential routes a cryptojackers may take. Note that both ways will place a script onto the victim device and some cryptojacking scripts have worming capabilities allowing infection of other linked devices. [21]

A screenshot of a computer

Description automatically generated with medium confidence

# Recommendations – Deter, Detect, Delay, and Respond

By answering the following questions, I am able to recommend the following policies and procedures to Deter, Detect, and Delay any current and future attacks from cryptojacking and to help reduce potential future vulnerabilities.

## What assets are potentially affected by cryptojacking and thus need to be protected?

The definition of an asset in Cyber Security can be many things, and in short; something is business critical, there must be a risk assessment done of all business assets and a report detailing to what degree is each asset important to the daily function of the business. In the table below I will detail a generalised overview of asset categories and potential subcategories. all Technology Components are considered an asset and should be treated as such and given the appropriate protections if possible. [20]

Graphical user interface, application

Description automatically generated

## What measures could you put in place to prevent cryptojacking attacks within your organisation?

To begin with, the DMU ITMS department needs to be fully aware of cryptojacking in all its forms. Human error and insider threats are abundantly the reason behind such attacks. Therefore learning must be a priority. Ideally, there should be a monthly program that looks at the emerging threats in Cyber Security to ensure that the team is keeping up to date with potential threats and mitigations to enable protection against cryptojacking and other cyber threats.

From a technical aspect, it is imperative that all known vulnerabilities are patched and that all software and hardware are current and up to date. The business also needs to have allotted an expert to analyse system configurations to ensure a modern and secure configuration throughout the DMU compute architecture. I highly recommend a zero trust architectural approach as laid out by the National Cyber Security Centre. [5]

## What measures could you put in place to detect a possible cryptojacking malware infection?

A task for the ITMS team would be to make available the core business network activity; this will enable ITMS to monitor network activity and highlight suspicious activity allowing ITMS to take action. To do this thoroughly and successfully, packet capturing is a top priority and will enable ITMS to monitor network activity in a detailed manner and flag any suspicious markers. Although Cryptojacking in itself is very difficult to detect due to the nature of it staying silent as possible within the system.

There are traditional methods that DMU could use, hiring a dedicated penetration tester that can test and check for vulnerabilities within the DMU system and provide a detailed report which in turn keeps on top of new and emerging threats and offers a plan to patch existing vulnerabilities.

## What measures could you put in place to minimise the effect of a possible cryptojacking malware infection?

Having a performance management system in place will benefit DMU as a whole. It will allow for precise and straightforward communication to top-level management about the future cyber risks and threats that DMU may face. DMU must be protected against any breach that may result in catastrophic losses of Data, Intellectual Property, and reputational damage. [9] According to Brian Thomas, having this kind of system in place will allow for clear communication between technical teams and management to fully understand the risks involved and the potential costs, giving a tangible security rating to DMU, which will provide a clear picture of how secure DMU are as a business and minimise any impact an attack may have on the business due the speedy response that having a performance management system in place will allow for. I recommend following the NIST Cyber Security Framework.

A picture containing diagram

Description automatically generated

Figure 4: NIST Cyber Security Framework [21]

# Notable Research

With multiple offered solutions available, it is difficult to differentiate which is the most effective, [Maurantonio](https://www.sciencedirect.com/science/article/pii/S0140366421000797?via%3Dihub" \l "!) et al. [1] provide a critical review through their research. With a proposed Crypto-Aegis framework that utilises Machine Learning (ML), this research paper offers successful results in the ordinarily evasive cryptojacking detection. By way of identifying Full Nodes through local network traffic analysis. This study's discussion of the solution to detecting cryptojacking by blacklisting is deemed ineffective, alluding to the fact that there may be several false negatives, the outside mitigating factors of URL randomisation. With introducing third-party software, it is clear to see that blacklisting will not be the most effective solution, as is the case with many other solutions.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 6: Detecting Cryptojacking [1]

In another research paper [2], Opcode Analysis seemed a viable option, claiming accuracies of up to 100%, also alluding that using this method could distinguish between varying factors, including cryptomining webpages, benign sites, and weaponised, deweaponised benign sites. Although with high success rates, the small scale of the experiment limits the information accrued through the investigation. A large-scale research project is needed to thoroughly test this method of detecting methods of cryptojacking. An exciting prospect will come by implementing Opcode analysis built-in to the browser, making this method more direct and suitable for, as a minimum, delaying potential cryptojacking attacks.

[3] Takes a fresh look at how to approach detection. Their solution offers up a cross-stack solution, taking a dynamic approach via microarchitecture and OS layers. The paper claims to have found an effective and low cost way to spot cryptojacking activities on any type of application, while most other similar research only tracks via the browser, this proposed method tracks everything, with low rates of false positives.

Hernandez-Suarez et al more recently has proposed using Machine Learning and couple it with the ‘classification power’ of deep dense neural networks, it claims to autoencoder, effectively using a ‘fingerprinting technique’. [4]

# Conclusion

Cryptojacking seemingly stormed to the stage in 2020; However, it has been around for a long time. It is only recently, in the last couple of years, become famous, for its large-scale attacks, for its millions of unsuspecting victims, but also for how some people have flipped the hack and used it for good and sometimes for profit. Some reports suggest 25% of all businesses have at some point been exploited by cryptojacking; some experts believe the number could be more significant due to the difficulty in identifying attacks. History is littered with many organisations, post-hack, wishing they had taken their own Cyber Security seriously, let’s not let that be DMU. I highly recommend keeping an eye on modern research into Cyber Threat mitigations like the ones included in this report, to allow DMU a head start in implementing any new software and technology that will secure DMU against all Cyber Threats. An up-and-coming method of detection of Cryptojacking seems to be centred around Machine Learning (ML), I recommend following this closely. While waiting for a refined and useable system to defend against cryptojacking quickly and effectively, we must be vigilant in our internal processes and procedures as recommended in this report.

# References

[1]M. Caprolu, S. Raponi, G. Oligeri, and R. Di Pietro, “Cryptomining makes noise: Detecting cryptojacking via machine learning,” *Computer Communications*, vol. 171, no. 1, Feb. 2021, doi: [10.1016/j.comcom.2021.02.016](file:///C:\Users\Student\OneDrive%20-%20De%20Montfort%20University\university\Emerging%20Topics%20in%20Security\Coursework\10.1016\j.comcom.2021.02.016).

[2]D. Carlin, P. O’Kane, S. Sezer, and J. Burgess, “Detecting Cryptomining Using Dynamic Analysis,” *IEEE Xplore*, Aug. 01, 2018. <https://ieeexplore.ieee.org/document/8514167> (accessed Nov. 07, 2022).

[3]N. Lachtar, A. Abu Elkhail, A. Bacha, and H. Malik, “Access Manager,” *idpedir.dmu.ac.uk*, Aug. 18, 2020. <https://ieeexplore-ieee-org.proxy.library.dmu.ac.uk/document/9170774> (accessed Nov. 10, 2022).

[4]A. Hernandez-Suarez *et al.*, “Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks,” *Applied Sciences*, vol. 12, no. 7, p. 3234, Mar. 2022, doi: [10.3390/app12073234](file:///C:\Users\Student\OneDrive%20-%20De%20Montfort%20University\university\Emerging%20Topics%20in%20Security\Coursework\10.3390\app12073234).

[5]A. Peterson, “Cybercriminals Are Moving from Ransomware to Cryptojacking: Kaspersky Lab,” *CCN.com*, Jun. 30, 2018. <https://www.ccn.com/cybercriminals-are-moving-from-ransomware-to-cryptojacking-kaspersky-lab/> (accessed Nov. 03, 2022).

[6]D. Balaban, “Cryptojacking for Good: Groundbreaking Examples,” *CryptoCoin.News*, Jun. 20, 2018. <https://cryptocoin.news/analysis/cryptojacking-for-good-groundbreaking-examples-15771/> (accessed Nov. 03, 2022).

[7]NCSC, “Zero trust architecture design principles,” *www.ncsc.gov.uk*. <https://www.ncsc.gov.uk/collection/zero-trust-architecture> (accessed Nov. 10, 2022).

[8]NJIT, “What is Cryptojacking? How to prevent, detect, and recover from it | Information Services and Technology,” *ist.njit.edu*, Oct. 29, 2018. <https://ist.njit.edu/what-cryptojacking-how-prevent-detect-and-recover-it> (accessed Nov. 07, 2022).

[9]E. Chickowski, “What is cryptojacking? How to prevent, detect, and recover from it,” *CSO Online*, Aug. 02, 2019. <https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html> (accessed Nov. 10, 2022).

[10]W. Ashford, “Businesses need to take cryptojacking seriously,” *ComputerWeekly.com*, 2018. <https://www.computerweekly.com/feature/Businesses-need-to-take-cryptojacking-seriously> (accessed Nov. 10, 2022).

[11]Sonicwall, “CYBER THREAT INTELLIGENCE FOR NAVIGATING THE UNKNOWNS OF TOMORROW S O N I CWAL L 2 0 2 2 C Y B E R T H RE AT R EPORT M I D -Y E A R U P D AT E,” Jun. 2022. Accessed: Nov. 10, 2022. [Online]. Available: <https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf>

[12]B. Thomas, “What is Cyber Security Performance Management?,” *www.bitsight.com*, Nov. 14, 2019. <https://www.bitsight.com/blog/what-is-cyber-security-performance-management> (accessed Nov. 10, 2022).

[13]B. Krebs, “Who and What Is Coinhive? — Krebs on Security,” *Krebsonsecurity.com*, 2017. <https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/> (accessed Nov. 07, 2022).

[14]T. Hatmaker, “Cryptojacking malware was secretly mining Monero on many government and university websites,” *TechCrunch*, May 08, 2018. <https://techcrunch.com/2018/05/08/coinhive-malware-may-troy-mursch/?guccounter=1> (accessed Nov. 07, 2022).

[15]T. Hatmaker, “Salon’s Monero mining project might be crazy like a fox,” *TechCrunch*, Feb. 13, 2018. <https://techcrunch.com/2018/02/13/salon-coinhive-cryptocurrency-mining/> (accessed Nov. 07, 2022).

[16]F. 1 Image, “CryptoJacking - A Technique Using By Hackers To Mine CryptoCurrencies,” *HackersOnlineClub*. <https://hackersonlineclub.com/cryptojacking/> (accessed Nov. 03, 2022).

[17]E. Oz, “Cryptojacking Attacks – Clever Ways to Detect and Prevent it - ox-currencies,” *ox-currencies.com*, Jun. 06, 2022. <https://ox-currencies.com/cryptojacking-attacks-clever-ways-to-detect/> (accessed Nov. 10, 2022).

[18]S. Cook, “Malware statistics & facts: Frequency, impact, cost & more [2020 edition],” *Comparitech*, May 29, 2021. <https://www.comparitech.com/antivirus/malware-statistics-facts/> (accessed Nov. 10, 2022).

[19]C. C. Editor, “asset(s) - Glossary | CSRC,” *csrc.nist.gov*. <https://csrc.nist.gov/glossary/term/asset>

[20]Kaspersky, “What is Cryptojacking? – Definition and Explanation,” *www.kaspersky.com*, Sep. 14, 2021. <https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking>

[21]NIST, “National Institute of Standards and Technology | NIST,” *NIST*, 2000. <https://www.nist.gov/>