INFOSEC 2018 SURVEY REPORT

# Threats, Politics, and Cryptocurrency Mining

## Table of Contents

AlienVault® has simplified the way organizations detect and respond to today's ever-evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management®, with the power of AlienVault's Open Threat Exchange®, the world's largest crowd-sourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital, and Correlation Ventures.

# 1. Executive Summary

## 1.1 Introduction

With Infosecurity 2018 happening shortly after GDPR came into force, and thus ended months of preparation, we were interested as to whether security professionals have found GDPR to be a friend or foe over the last couple of years.

While GDPR may have had a go-live date, cyber security is a never-ending cycle, and the job of securing technology is very rarely "done". So we were curious as to what threats on the horizon concern CISO's from both within and external to their organizations.

In terms of ongoing trends, mining of cryptocurrencies has made headlines throughout the year, both from a legitimate, and illegal perspective. We wanted to hear from security professionals on what they thought of cryptocurrency mining, and what level of acceptance there is.

## 1.2 Key Findings

- Looking forward, cloud security threats are the most concerning external threat
- Internally, phishing (55%) and ransomware (45%) lead the pack of worries for security departments
- 92 percent would rather pay a subscription fee, allow ads, or leave a website altogether rather than allow a website to mine cryptocurrency
- 56 percent believe cybersecurity has become a political pawn

## 1.3 Methodology

This report is based on experience of the author and a survey of 928 participants at Infosecurity Europe 2018.

Demographic data of survey respondents was not collected and respondents were not prompted for their answers, nor was any clarification provided about the terms or definitions.

This report was written by Javvad Malik, Security Advocate, AlienVault. Any questions about the methodology should be addressed to him at jmalik@alienvault.com.

# 2. Threats

Threats are what keep many security executives awake at night. But, what types of threats are the most worrying?

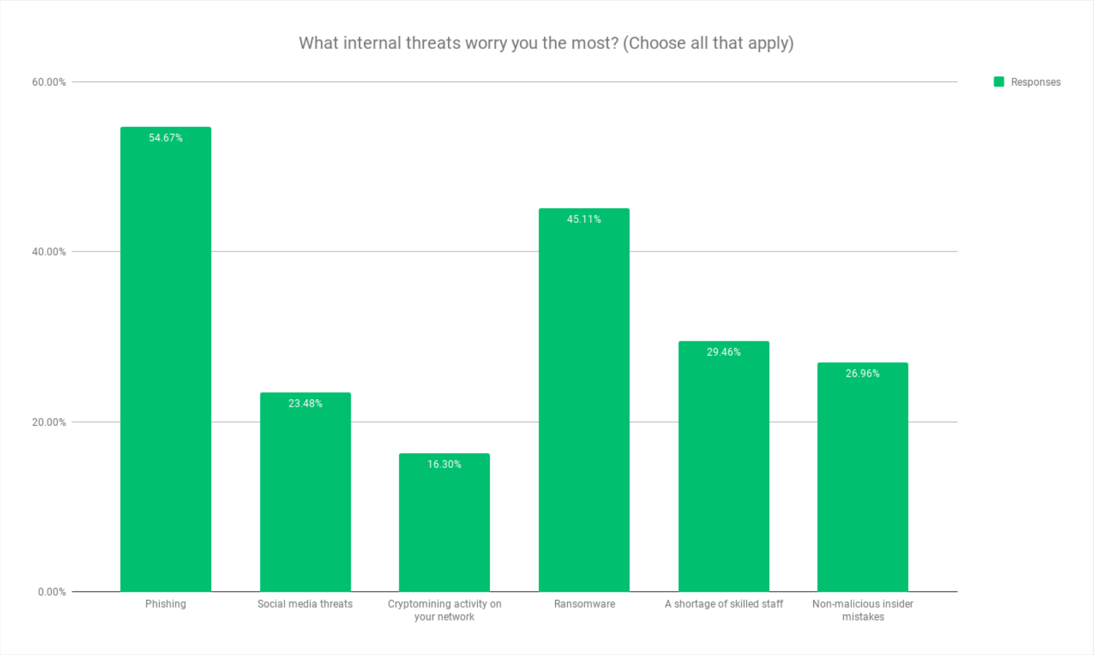
Phishing tops the list of internal threats with the most impact that are triggered internally — nearly 55 percent of participants agreed it was the biggest worry.

The human element of phishing is what makes it attractive to attackers, and concern for security departments. No single control can defend against a phishing attack, and ultimately, humans make mistakes. In fact, human error can be traced back to the root cause of many breaches.

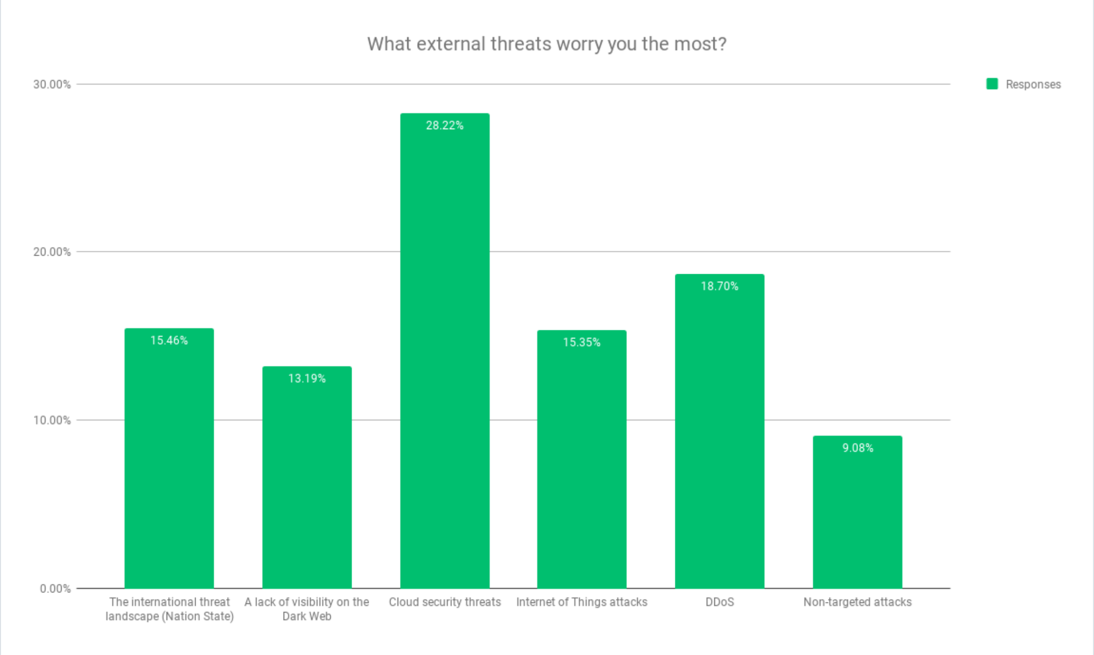
User awareness and education are definitely important, but that alone isn't enough — and companies should create a layered defense comprising of people, technology and processes.

This can include having email filtering in place, alerting users to emails that have originated outside of the organization, as well as having an established process for users to report suspicious emails.

Finally, it's vitally important to have capabilities to detect and respond to incidents where a user may have fallen victim to a phishing email. This would involve deploying a combination of network and endpoint threat detection capabilities, having security teams monitor alerts, and having a documented and tested response plan.



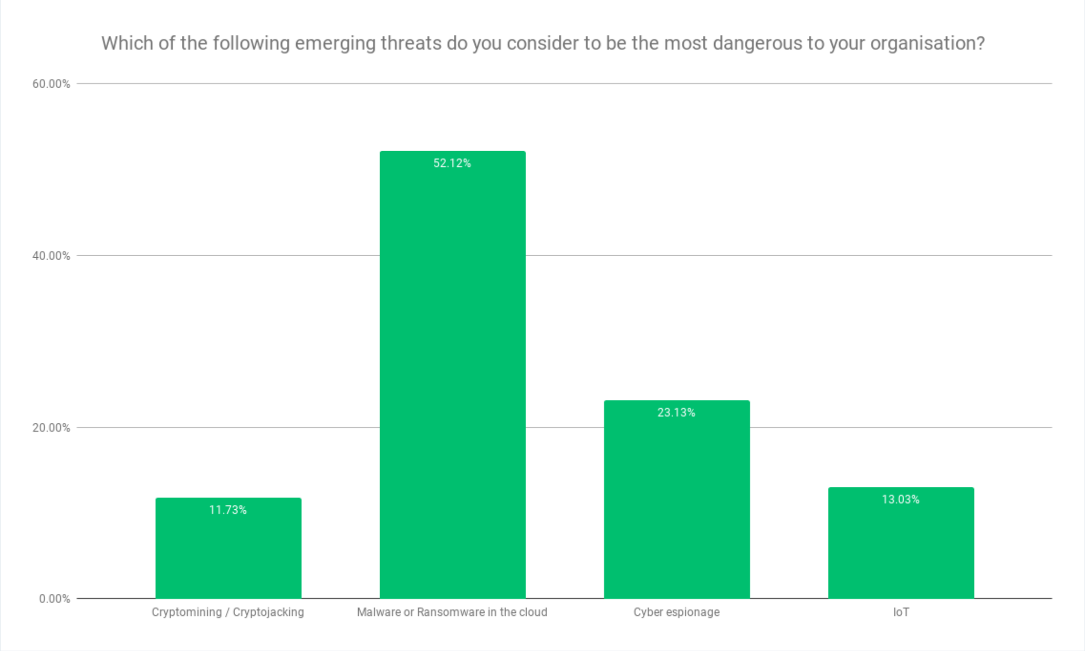
At 45 percent, ransomware was second on the list of internal worries. While malware can go undetected and is designed to be stealthy when infecting systems, ransomware is a very public threat; designed to be loud and visible, and perhaps the only thing worse than a security incident is a very public security incident inciting pressure and stress on the business to resolve the issue in the public eye and under a spotlight.



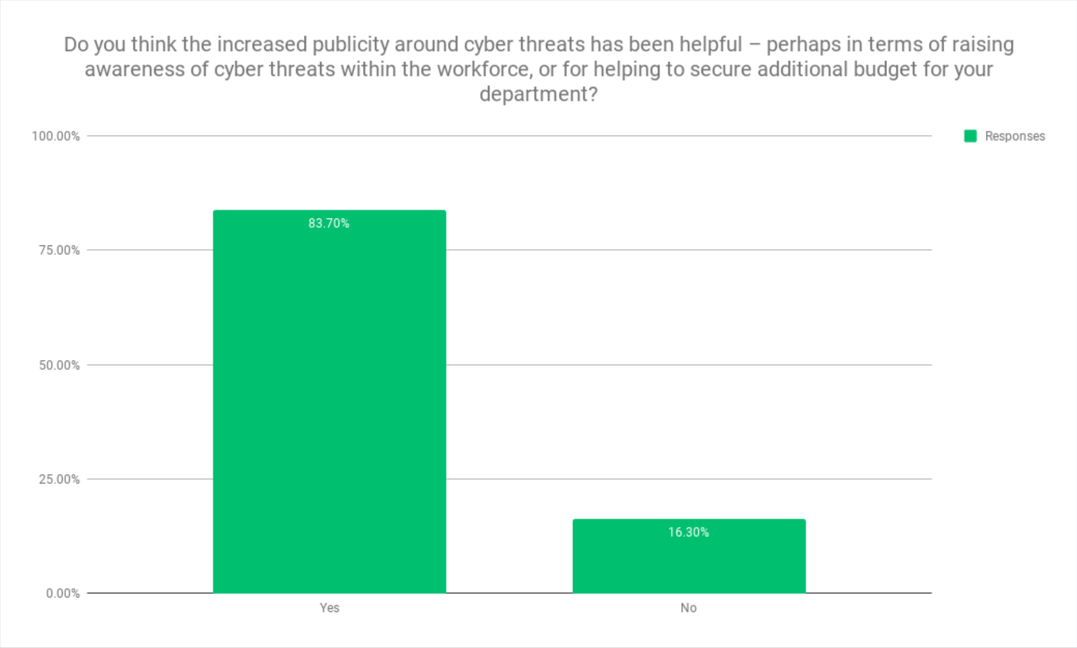
Looking to the future, most participants are fearful of the attacks that could materialise in the cloud. While the cloud offers many benefits to enterprises, there are risks - many of which haven't been fully understood.

The cloud shared responsibility model is well publicised, yet still not fully understood or appreciated by many companies, which has led to many breaches as a result of poorly secured cloud instances.

It's an unfortunate, but defensible observation with 52 percent of survey respondents citing concern that cloud-based threats will likely increase in the future.



But not all security publicity is bad publicity. The vast majority, at 84 percent, believe that the increased publicity around cyber threats has been very useful. While, the survey didn't go into the specifics of why it has been useful, it is likely that large public breaches raise awareness for the need of cyber security.



## 3. Security and Politics

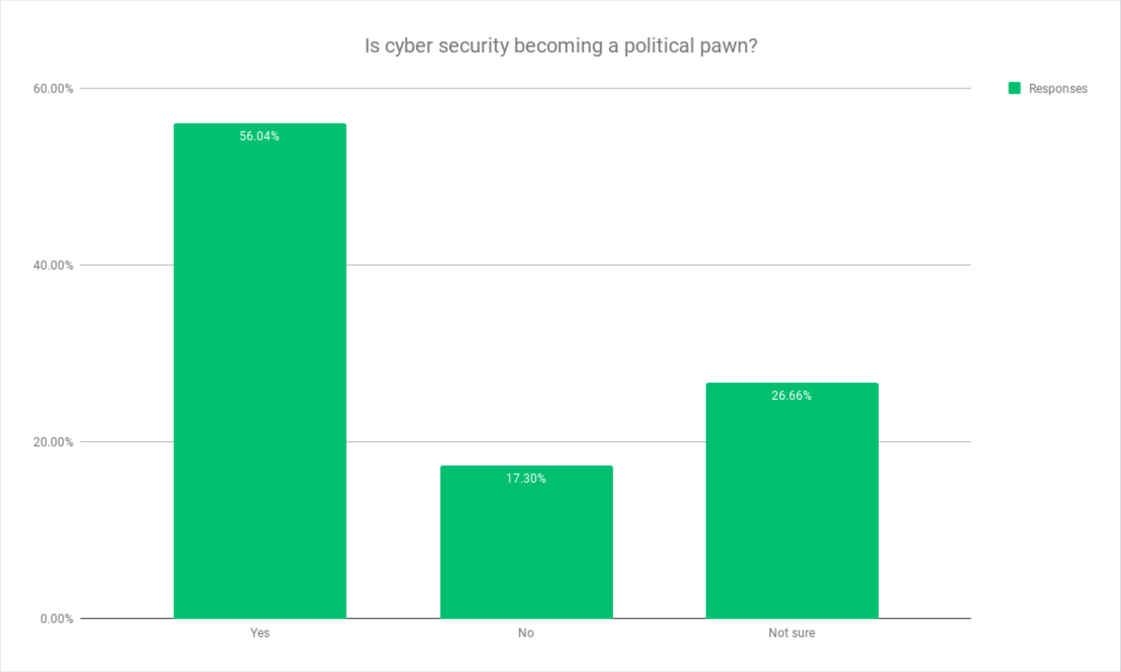
2018 marked the 20-year anniversary since L0pht Heavy Industries testified before a United States Senate Committee.

Much has changed in the last 20 years with regards to the state of the industry and how it is perceived. Security researchers used to be poorly understood, thought of as criminals and illegal hackers. But, over time the industry legitimised, offering critical capabilities required by nearly every company today.

However, in the past decade, the world has become more reliant on connected technology. Storing and processing all manner of information, ranging from corporate intellectual property, to the number of steps an individual takes in a day. As a result, the impact of a security attack or breach can be felt wide and far.

This is not something that has gone unnoticed, not only by criminals, but by governments, legislators, and industry bodies. The downside being that it can become tempting to leverage cyber security - something that 56 percent of participants believe is the case, stating that cyber security is becoming more of a political pawn.

It’s easy to see why many professionals feel this way. Encryption, in particular, finds itself at the forefront of many discussions, polarizing opinion as to whether or not law enforcement should have ‘back doors’ or other means of accessing communication to crack down on crime.

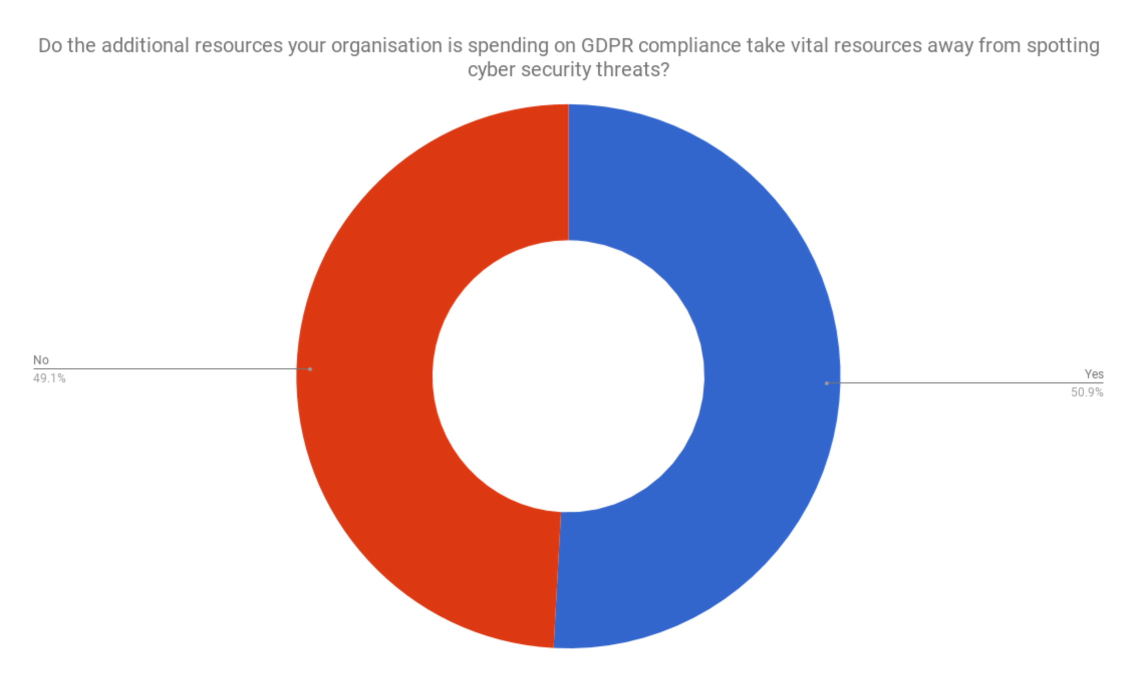


## 4. GDPR, Friend or Foe?

The General Data Protection Regulation (GDPR) has come into play, but is far from over - many industry observers are keenly waiting for the first big breach to see if the GDPR bite is as bad as its bark.

While GDPR has brought some benefits in terms of individual privacy, it has forced companies to consider its assets, and how it manages customer records.

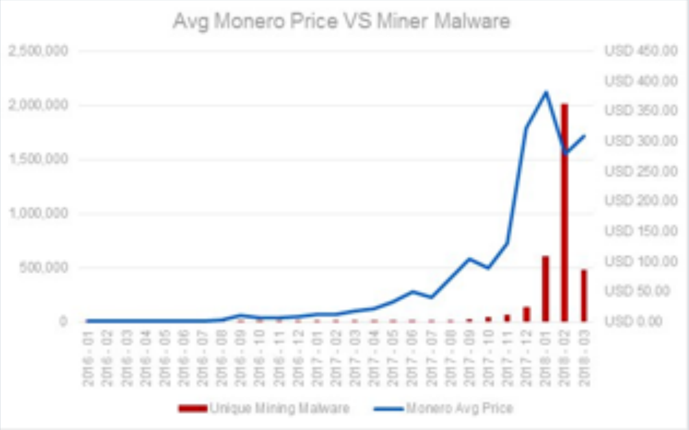
However, opinion is split almost down the middle on whether the focus on GDPR has been beneficial with half the respondents believing that GDPR has taken away vital resources needed to detect cyber security threats.



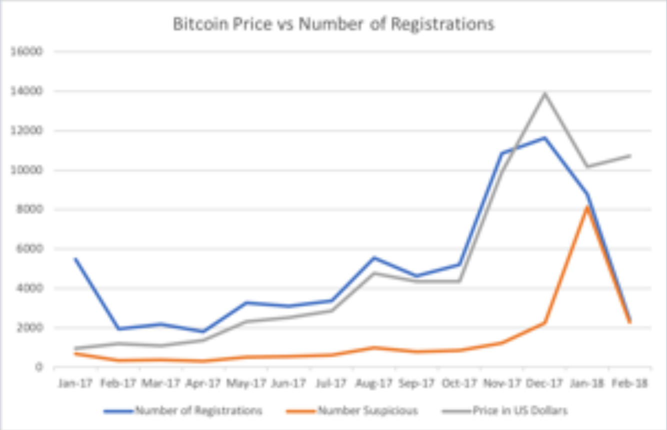
## 5. Cryptocurrency Mining

Cryptocurrency mining has received much interest. In fact, mining for cryptocurrencies on compromised machines has been on the upward trend over the last year while ransomware has been declining.

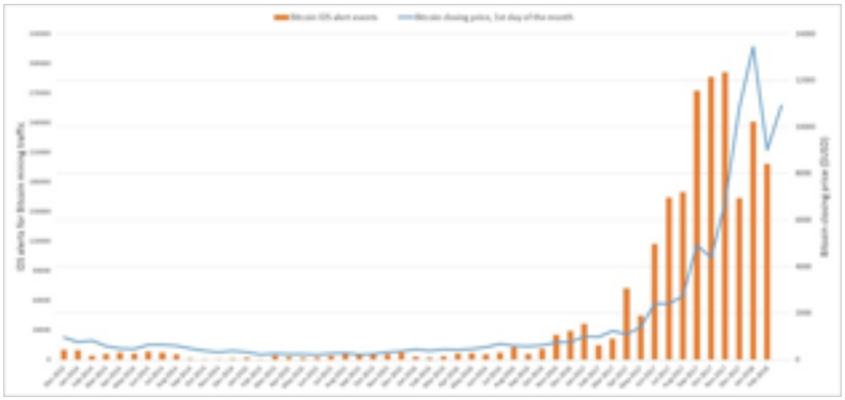
And while correlation is not causation, multiple vendors have reported seeing the same trends, that the more valuable a currency becomes, the greater the number of miners.



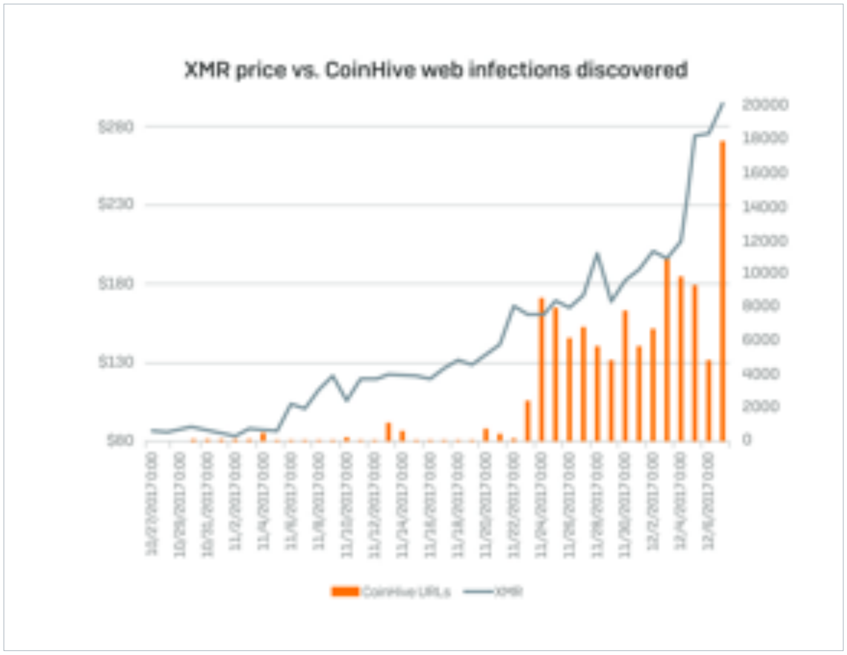
Monero Price vs Mining Malware (McAfee)



Bitcoin Price vs Bitcoin Phishing Pages



Bitcoin Price vs Mining IDS Alerts (SecureWorks)



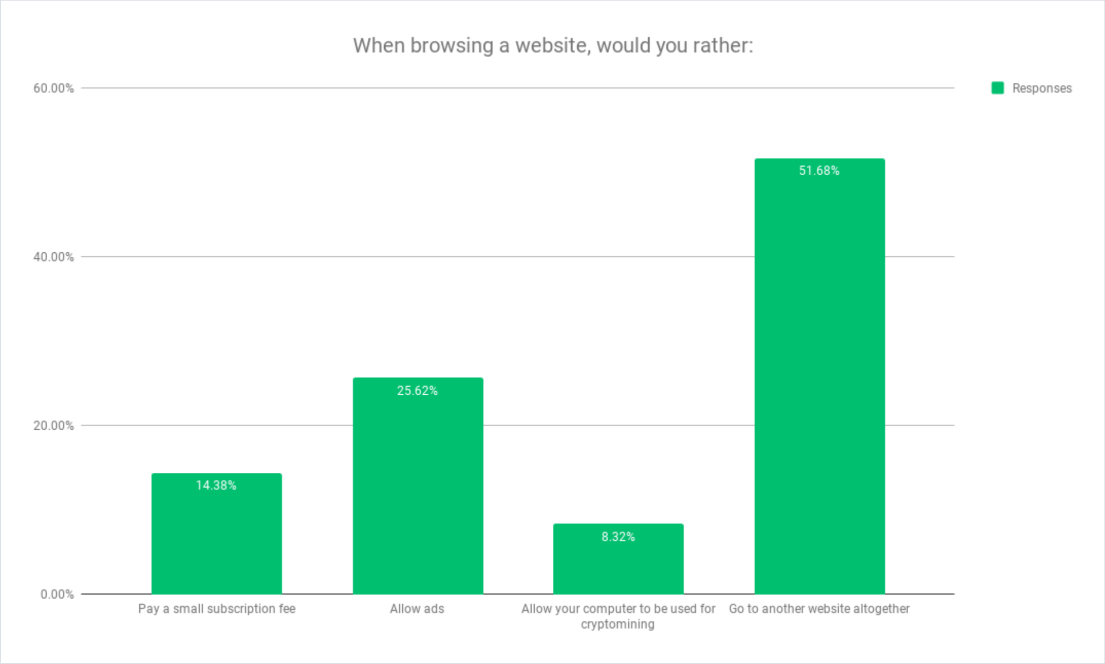
Coinhive infections vs Monero Price (Sophos)

But it's not just criminals looking to maliciously infect machines to mine bitcoin. The growing popularity of ad-blockers has left many online publishers looking for alternative ways to generate revenue. Some have resorted to either putting some of the content behind a subscription wall, or asking to use the visitors computer to mine cryptocurrency.

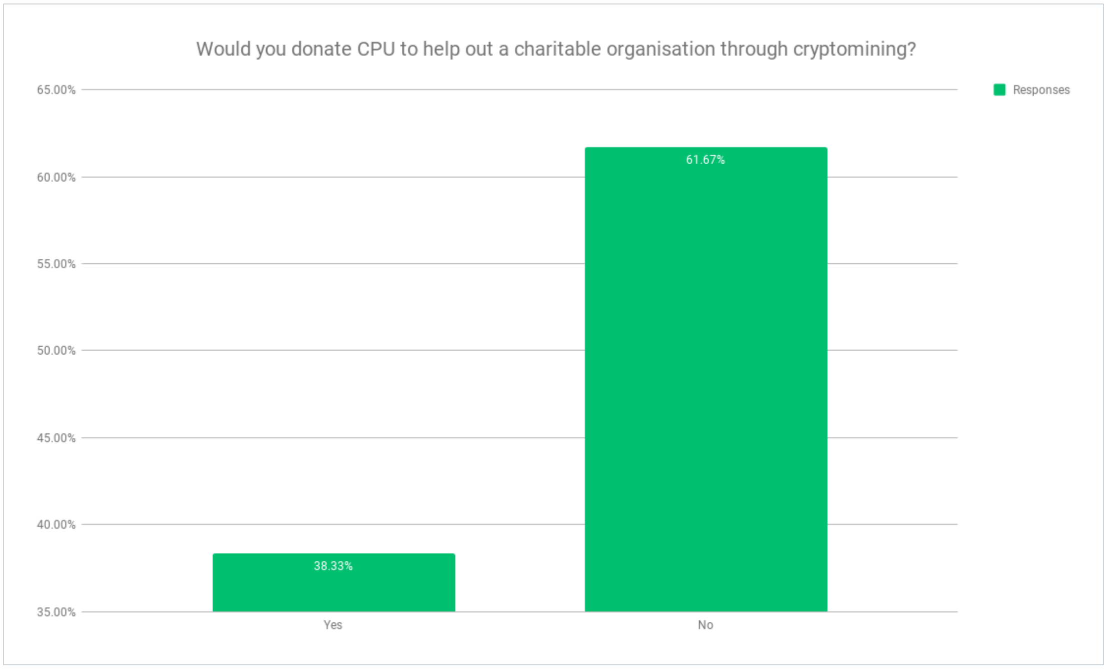
Unsurprisingly, the majority of respondents, at 52 percent, would rather not visit or support such a website at all.

26 percent would allow ads, while 14 percent would be happy to pay a small subscription fee to access the content.

Only 8 percent stated they would willingly allow their computer to be used for cryptomining in exchange for accessing content on the website.

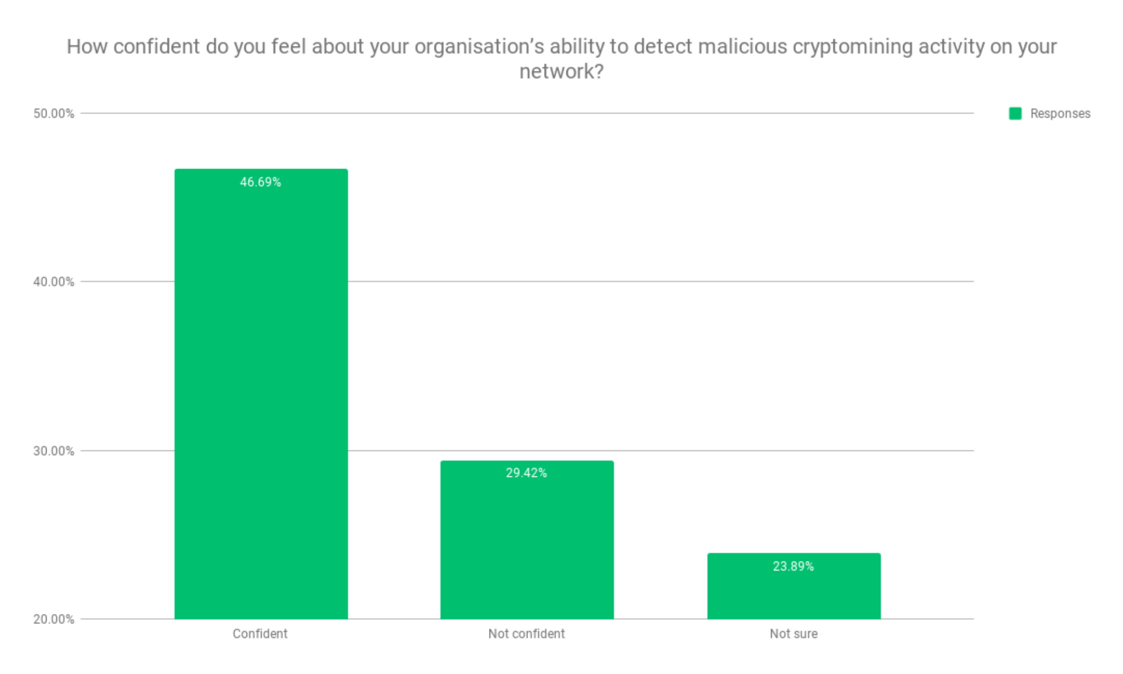


While charitable causes move the needle slightly, 62 percent of respondents would still refuse to allow their computers to be used for cryptomining, even if the proceeds were going to a charitable organization.



With cryptomining on the increase, both from a malicious, and not-so-malicious perspective, it is important for companies to have the capabilities in place to detect if any of their resources are being used for mining.

47 percent of respondents were confident that they had the right tools and resources in place to detect malicious cryptomining activity on the network. 29 percent were not confident, and 24 percent were not sure if they would be able to detect mining activity or not.


How confident do you feel about your organisation's ability to detect malicious cryptomining activity on your network?
50.00%
40.00%
30.00%
20.00%
🟩 Responses
46.69%
29.42%
23.89%
Confident
Not confident
Not sure

## Conclusions

The cloud has been at the forefront of adoption in recent years. Cal Corcoran, CIO of Gatwick Airport has gone as far as to suggest that too many companies are “Cloud Junkies”, rapidly adopting cloud for services that may be best-suited to remain on-premises.

With rapid adoption of any new technology there are new risks - some of which aren’t always fully apparent. The cloud offers companies a flexible way to store and process data, and in the process makes it almost too easy for companies to use it as a digital dumping ground without thinking through the security required.

Publicly-accessible AWS S3 buckets that have exposed millions of records have made it into the headlines many times over the last year. And, while this is a trend that may be stemmed in time, there are other potentially unknown attack vectors that will be used against the cloud once there is sufficient adoption. This makes it very important for companies to not ignore the need for security controls in the cloud, regardless of which flavor (public, private, hybrid).

User awareness will remain an ongoing task. It’s naive to believe that 100 percent success will ever be achieved - but a suitably informed workforce combined with appropriate security controls, and incident response processes can reduce the overall risk.

Cryptocurrency mining is perhaps the anomaly. Alongside criminals, there are some websites trying to utilise it for legitimate purposes. However, it will likely remain an uphill battle to get the masses to willingly allow untrusted code to run on a machine to mine cryptocurrencies.

As cyber security becomes mainstream, it impacts nearly every aspect of people’s lives. Therefore, it is not surprising to see the political discussions which surround it. Every time there is criminal gang activity, the question is asked whether weaker encryption could have helped law enforcement, whether manufacturers should cooperate more with police to unlock the phones belonging to deceased suspects.

The reality is that the influence cyber security has in everyday life will continue to expand, and with it, the challenges will broaden from technical, to societal and political.

# Appendix

## The Questions

1. What internal threats worry you the most (Choose all that apply)

    a. Phishing
    b. Social media threats
    c. Cryptomining activity on your network
    d. Ransomware
    e. A shortage of skilled security staff
    f. Malicious insiders
    g. Non-malicious
    h. Insider mistakes

2. What external threats worry you the most (Choose all that apply)

    a. A lack of visibility on the Dark Web
    b. Cloud security threats
    c. Internet of Things attacks
    d. DDoS
    e. Non-targeted attacks

3. Do you think the increased publicity around cyber threats has been helpful – perhaps in terms of raising awareness of cyber threats within the workforce, or for helping to secure additional budget for your department?

    a. Yes
    b. No

4. Is cyber security becoming a political pawn?

    a. Yes
    b. No
    c. Not Sure

5. Which of the following emerging threats do you consider to be the most dangerous to your organization? (Choose all that apply)

    a. Cryptomining / Cryptojacking
    b. Malware or Ransomware in the cloud
    c. Cyber espionage
    d. IoT

6. Do the additional resources your organization is spending on GDPR compliance take vital resources away from spotting cyber security threats?

    a. Yes
    b. No

7. How confident do you feel about your organization's ability to detect malicious cryptomining activity on your network?

    a. Confident
    b. Not confident
    c. Not sure

8. When browsing a website, would you rather: (Choose all that apply)

   a. Pay a small subscription fee
   b. Allow ads
   c. Allow your computer to be used for cryptomining
   d. Go to another website altogether
   e. None of the above

9. Would you donate CPU to help out a charitable organization through cryptomining?

   a. Yes
   b. No