Panda Adaptive Defense 360

Limitless Visibility, Absolute Control

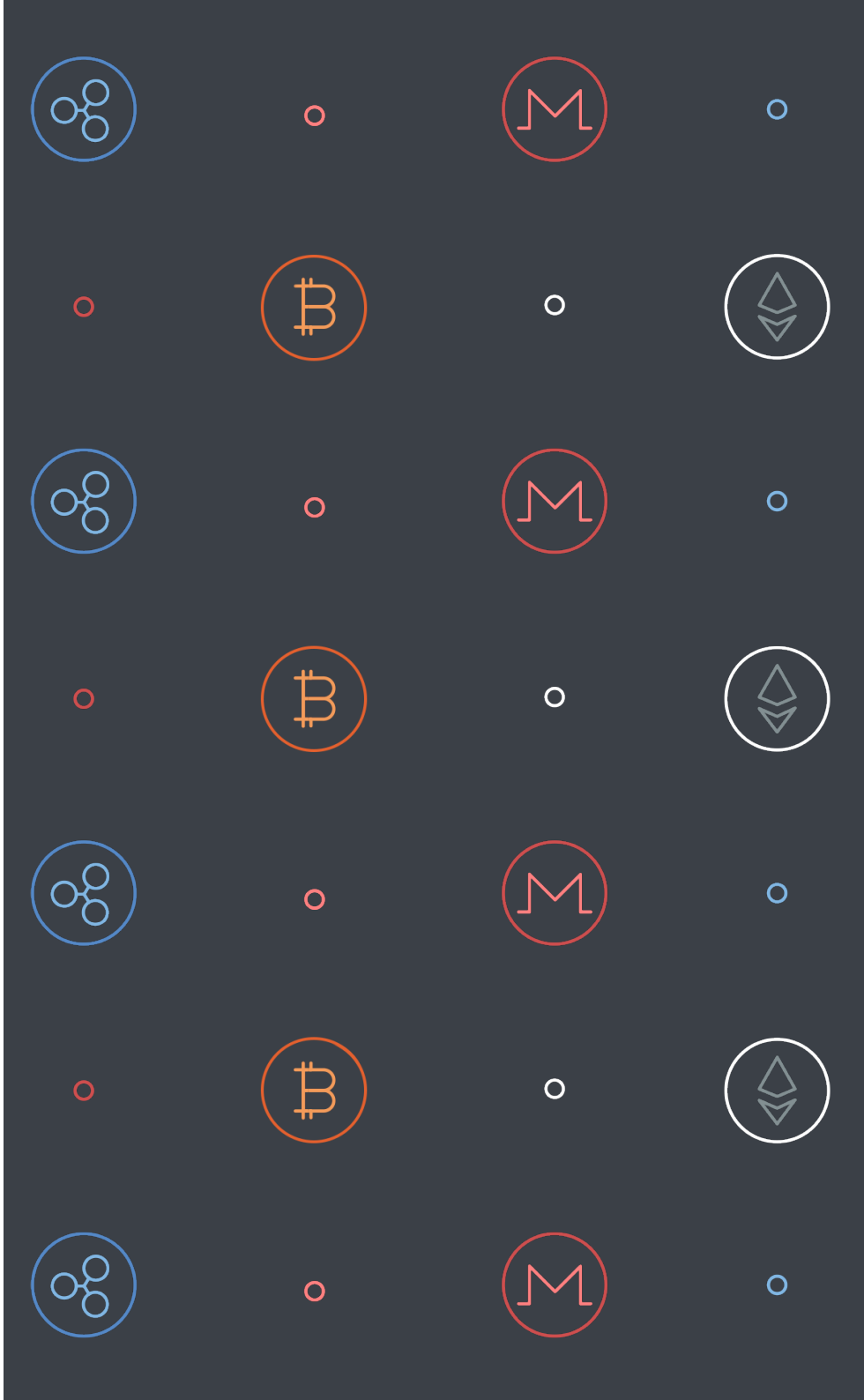
CRYPTOJACKING

A HIDDEN COST

panda

pandasecurity.com/business/adaptive-defense/

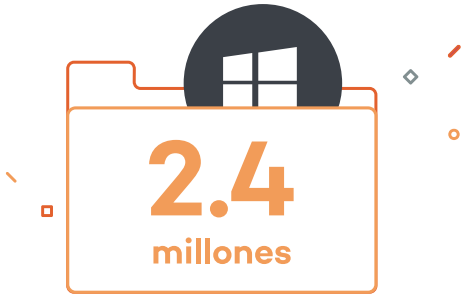
Table of Contents.



panda

1. A hidden cost

Cryptojacking is the concept that is defining 2018 in terms of cybersecurity. It has become the main threat to the security and performance of electronic devices throughout the first half of the year. So far this year, we have seen [2.4 million instances of this attack], which is booming among black hat hackers.

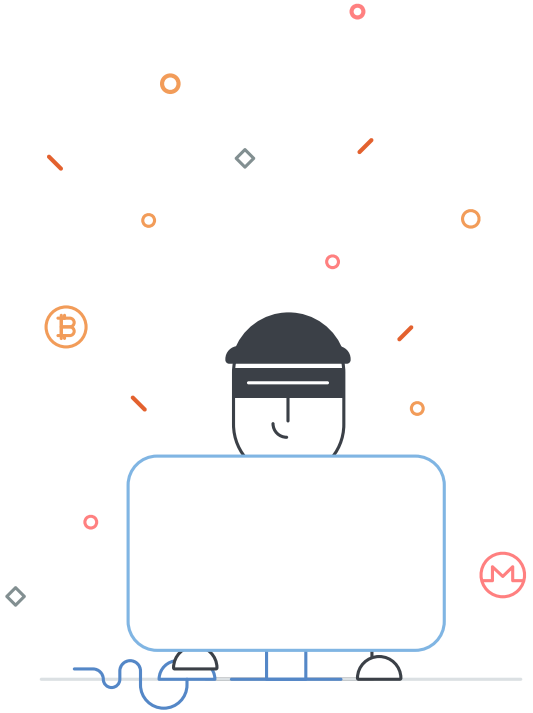


This is the picture that **PandaLabs**, Panda Security's antimalware laboratory, paints: although "traditional" types of malware like Trojans or worms are still heavily used by attackers, new trends – like fileless or malwareless attacks and cryptominers – show the fastest growth rates.

This trend is such that **bitcoin**, the most widely used digital currency, was included on Fundéu BBVA's shortlist for word of the year in 2017, highlighting the impact that virtual currencies are currently having.

Cybercriminals are [constantly developing their techniques], coming up with new ways to line their pockets. And it's this continual evolution that has helped them to hit upon a new motherlode: **cryptomining.**

But to understand how and why "the bad guys" want to mine cryptocurrencies at our expense, we're going to take a look at the whole process...



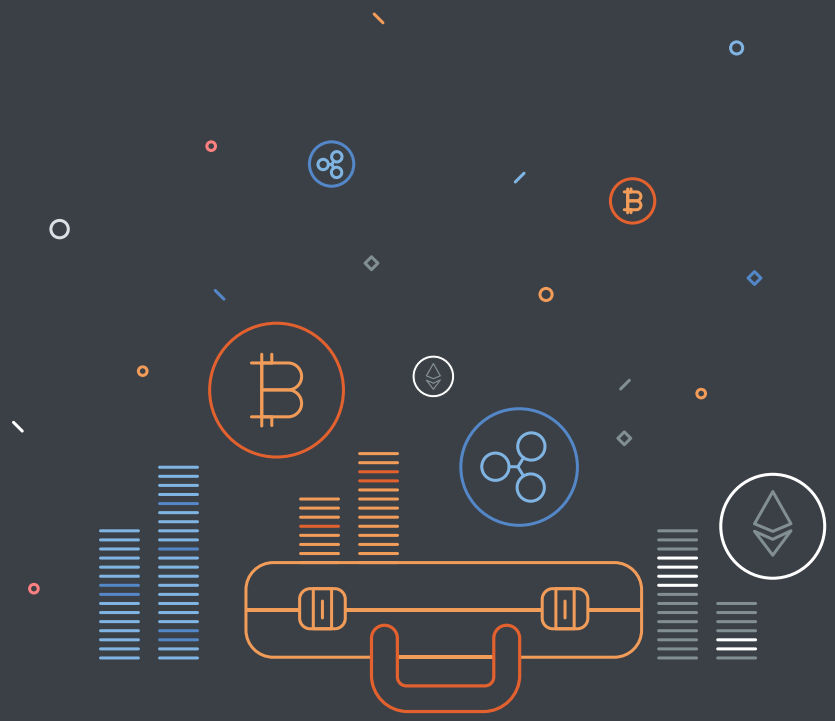
2. What are cryptocurrencies?

The appearance of the first cryptocurrencies is associated with the need to carry out anonymous transactions. In 2009 the first one was created: bitcoin. **Currently there exist more than 1,300 different cryptocurrencies**, with varying origins and characteristics, but which all share their digital nature and their **intention to assure the anonymity of their transactions.**

The legality of using cryptocurrencies is currently something of a hot topic: some countries are discussing banning them, while in others, the value of these currencies is in something of a legal limbo.

Ultimately, it is a double edged sword: a digital currency that ensures transparency and simplicity in transactions could seem to be the ideal tool to pay for the illegal services of a hacker. It's also ideal for cybercriminals: currently pretty much every ransomware attack requests payment of the ransom in bitcoins or some other cryptocurrency, due to their untraceable nature.

The rise in the value of cryptocurrencies such as **Bitcoin**, **Ethereum** or **Ripple** has meant that these currencies have become one of the main sources of income for cybercriminal organizations.



3. Blockchain, cryptocurrencies' raison d'être

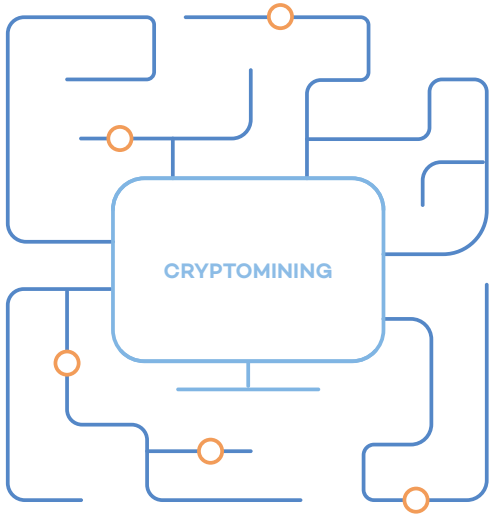
One of the issues that gives rise to a lot of doubts about cryptocurrencies is the possibility of "mining" them, something that is known as cryptomining. **Many of these digital currencies can be obtained by resolving mathematical operations**, almost as if it were just any old calculation.

However, mining for cryptocurrencies is an ever more complex task that consumes more and more energy resources and computing power. This is in part due to blockchain technology.

Blockchain technology is the cornerstone of cryptocurrencies' impenetrable defense, as well as of their anonymity. Blockchain was created to underpin bitcoin. Cryptomining is vital in order for the system to work: it is the computing activity that is needed in order to process the transactions that are carried out on the already existing blockchains. It serves to produce new cryptocurrency and to confirm the transactions on the blockchain network. I.e., to create more cryptocurrency, it's necessary to mine it. **Without mining, the system would collapse.**

A blockchain consists of a distributed database, and by design, **blockchains are completely tamper-proof.** To that effect, cryptocurrencies use trusted timestamping, which proves the exact time that data existed along the chain.

It's therefore no surprise that, in order to work, this process needs an amount of computing power that is prohibitive even for the largest tech companies. This is exactly why hackers have found a way to make it easier: they get onto other people's computers and put them to work trawling the web, consuming their resources to mine cryptocurrencies.



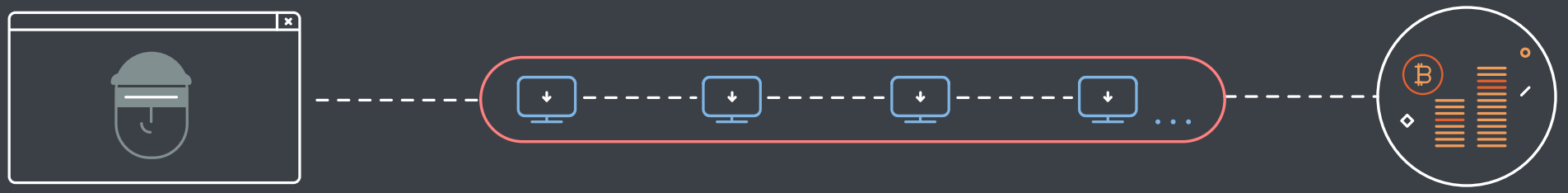
4. Working for the enemy

Cryptojacking is the unauthorized use of a user's device to mine cryptocurrencies. Put simply, attackers use malware to take over these computers, tablets, or smartphones, and exploit part of their processing power to covertly mine cryptocurrencies. **This is how you could end up being put to work for the bad guys, using your energy resources without even realizing.**

How... The user will probably notice their devices slowing down, but may not be aware of the fact that this is due to an attack whose goal is to mine cryptocurrencies. One of the most common techniques involves **appropriating the victim's CPU or GPU when they visit a website infected with cryptomining malware**, as happened recently on YouTube.

Another attack technique consists of **using the online video function in Microsoft Word**, which allows videos to be inserted into documents without having to embed or link them. In this case, the attackers make use of this feature of Word to insert malicious scripts and secretly use the victim's CPU.

Why... Cryptocurrencies have become the gold of the 21st Century. For this reason, this year we're seeing an increase in the number of attacks that mine cryptocurrencies. Now that IT teams and state security forces are keeping a keen eye on ransomware attacks, cybercriminals are opting for more secure ways to make a buck, and they seem to have hit a promising new vein with the illicit use of IT resources for this kind of mining. **The more computing power they can steal, the faster the mining is.** This is giving rise to fights between different attackers trying to gain control of as much of a user's CPU as possible.



Josu Franco, Technology and Strategy Consultant at Panda Security states that the boom in mining lies in the fact that "it is an easy way to make money, and doing it is really cheap. Cryptojacking kits can be bought on the dark web for around $30. The attacker can install it on 100 machines, for example, and all of them will constantly contribute money by generating cryptocurrency with little risk. What's more, we're seeing a significant increase in legitimate websites infected with CoinHive, a JavaScript that means that it isn't even necessary to install mining software; it simply runs as long as the user is active on that page. However, with ransomware, the attacker will maybe get a few victims to pay out just once."

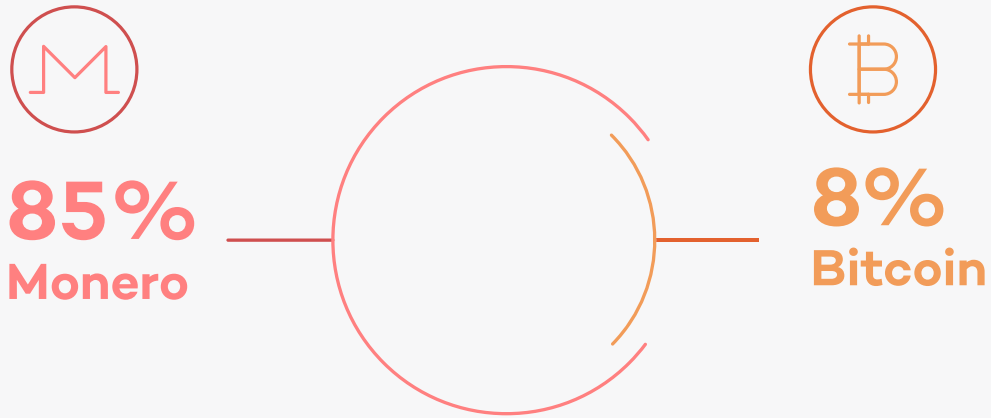
As is the case with ransomware, **companies are the principal target for attackers in 2018,** since, if they manage to get onto a corporate network, they will have a tremendous amount of resources at their fingertips.

Cybersecurity experts affirm that **criminals are shifting from ransomware to cryptoming because it is much less intrusive, and requires fewer resources to avoid detection.** With ransomware there is no guarantee that the victim will pay the ransom, as they may well have a backup of all their files. By contrast, with cryptomining, it is far more likely that the money invested will be recovered, and it is much less invasive. Mining can be carried out on any kind of device, not being restricted to Windows, Mac or Linux as is the case with ransomware, and the victim's system will keep working in spite of the attack.

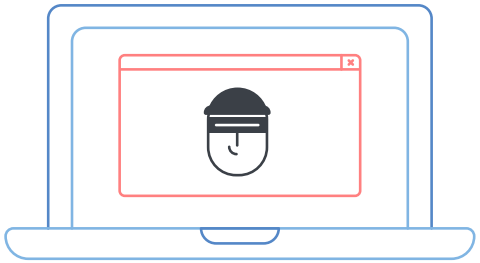
5. Which cryptocurrencies are cybercriminals after?

The most well-known – and "oldest" – cryptocurrency is bitcoin. However, these days mining this cryptocurrency is nigh on impossible for amateurs, since it requires so much energy, along with specialized processors, that it is only feasible for companies dedicated to this activity. So much so that in the last few years, Iceland has seen a rush of bitcoin mining companies, attracted by the country's cheap energy, as well as its cold climate, which eliminates the need to spend more money on cooling systems for the processors. In fact, according to Johann Snorri Sigurbergsson who works in the country's energy sector, bitcoin's energy consumption could soon overtake domestic energy consumption.

If cybercriminals can't easily generate bitcoins with cryptojacking, what exactly are they after? The answer is Monero, a cryptocurrency created in 2014. This currency is ideal for illicit mining operations, as it doesn't require special equipment, it doesn't use so much computing power, and it also has increased privacy compared with other cryptocurrencies. In fact, **85% of cryptojacking attacks seek to generate Monero, while only 8% are trying to generate bitcoin.**



6. The way in to your computer



As is the case with many of the cyberthreats that we see these days, cryptojacking has **multiple attack vectors** that it uses to get onto computers and IT systems and start to harness the computing power of the affected devices.

Infected websites

One of the most common methods for harnessing CPU is the use of websites that secretly take advantage of users' Internet connections to mine, thus **tricking visitors to these sites into providing resources for a third party.**

The origin of this technique lies with **CoinHive**, a company launched in September 2017 as a legitimate alternative to ads on websites. However, it wasn't long before cybercriminals took advantage of this service's code for their own malicious ends. The technique involves gaining access to websites, injecting the CoinHive code, and extracting the cryptocurrency generated with the **CPU** of visitors to these websites.

Indeed, CoinHive is the most commonly used script for this kind of attack. A study by the security researcher Troy Mursch has detected **50,000 websites infected with cryptojacking script,** with 80% of these using CoinHive. Codes like CoinHive generate an estimated $250,000 every month..

Something that greatly facilitated hackers was the fact that, to begin with, CoinHive didn't require user permission on the websites where it was run. This meant that it was possible to carry out the attack without the visitor realizing. Although the company now asks users for permissions, cybercriminals were able to copy and edit the code to suit their own needs.

This isn't something marginal: among the affected websites are such well-known organizations as *The LA Times*, and public institutions like the Government of Australia. In fact, for the attackers, **the more popular the website the better**, since more visitors mean more CPU, and therefore, more cryptocurrency.

This was exactly what happened with YouTube, the second most visited website in the world. In this case, the advertising platform **DoubleClick** was the victim of an attack that hid the CoinHive cryptojacking code in YouTube adverts.

How does this kind of code get onto websites? A lot of the time, criminals get in using vulnerabilities in the content management systems used to make these websites. One of the most popular vulnerabilities for this kind of attack is in Drupal, which has been exploited hundreds of times

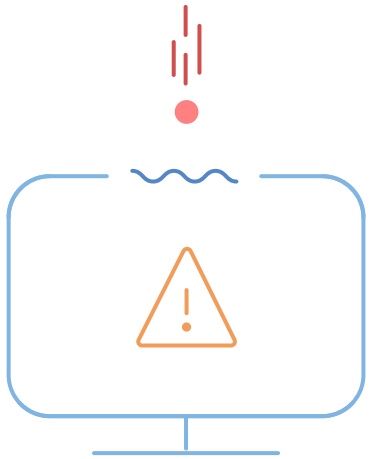
A particularly interesting case is use of a vulnerability in **Apache Struts** – a web application that has already caused rather a lot of problems. In this case, it is used by a piece of malware that, once on the website, looks for other cryptomining malware and, if it finds any on the system, deactivates it to be able to use as much of the user's CPU as possible, all for itself.

Vulnerabilities

One of the most popular points of entry for cryptojacking are vulnerabilities. We have already seen several cases of vulnerable websites, but attackers also take advantage of **vulnerabilities in operating systems to get malware onto the endpoint.**

One of the most problematic vulnerabilities of the last year is one that affects Microsoft Server Message Block (SMB), and is called **EternalBlue.** The most infamous use of EternalBlue was the global ransomware attack, WannaCry. However, a few months after this attack, **PandaLabs discovered another exploitation of this vulnerability:** the fileless malware, WannaMine, that was being used to mine Monero.

This vulnerability was also how Adylkuzz got onto systems. This malware, like WannaMine, was used to generate Monero, and infected thousands of computers all around the world. In fact, it is believed to have affected even more people than WannaCry.



Phising

Over 90% of the malware in the world arrives via email. It is therefore perhaps not surprising that cryptojacking malware is no exception.

One popular technique is to use seemingly legitimate documents. One example is the use of **Word documents.** Here, the attacker places the cryptojacking code in a video within a Word document, which is then attached to an email. Once the document is opened, the cryptojacking script is starts to run.

Another particularly dangerous piece of malware is **WinstarNssmMiner**. This malware also gets in using phishing, as well as infected websites. Once on a system, it uses all of the computer's power to mine cryptocurrency. If it is discovered, or if someone tries to remove it from the system, it crashes the infected computer.

Internet of Things (IoT)

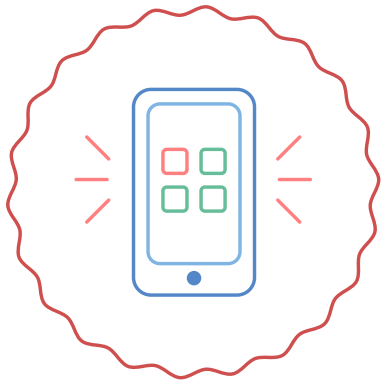
The diffusion of Internet connected mobile devices is widespread, and their use has become the norm. It's therefore only to be expected that black hat hackers have started to **exploit the applications found on these devices to extend their criminal activity.**

One of the first cases that was seen in the field of IoT was HiddenMiner, a piece of malware that got onto mobile devices via applications downloaded from third party app stores – i.e., unofficial stores. One of the features that makes it so dangerous is that, in older versions of Android, it is almost impossible to get rid of. What's more, once on a device, it uses all the device's resources, **making it overheat or even crash.**

In fact, there have been cases in which **so much energy was used by the malware that it almost caused the infected device – in this case a smartphone – to explode.**

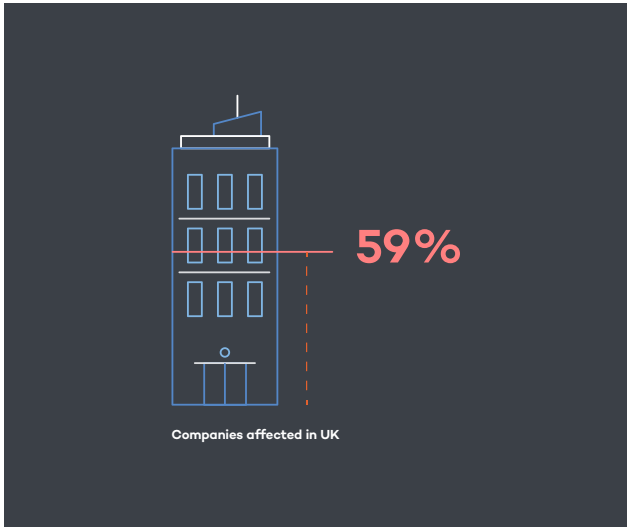
But it's not just apps downloaded from untrusted sources that can cause problems. At the start of the year, **several applications available on the Google Play Store were found to contain cryptojacking malware.** Among the applications were a VPN, games, and even an app that claimed to donate the cryptocurrency it mined to a charity.

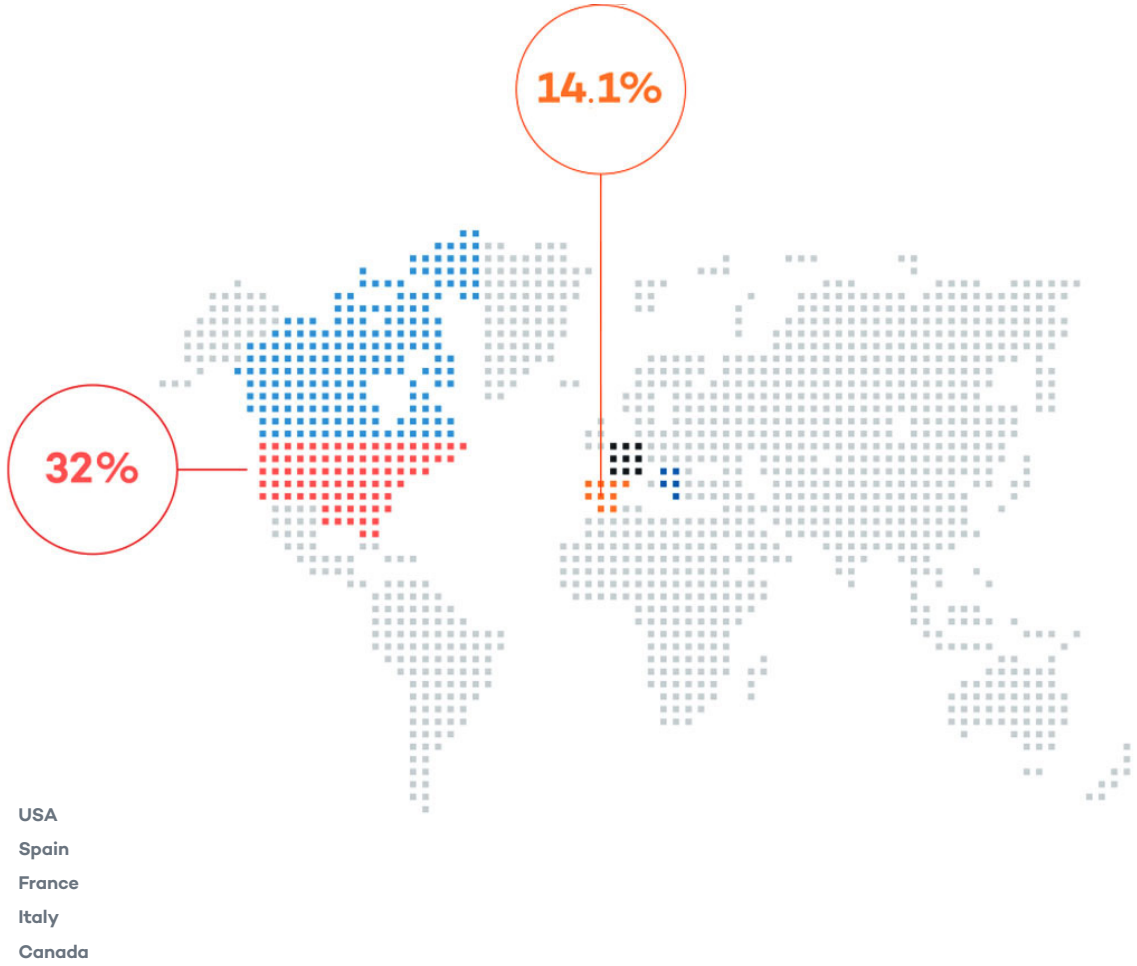
Other IoT devices – such as security cameras **– haven't escaped from these cryptojacking attacks either.** These devices are especially susceptible to being attacked due to the fact that, generally speaking, the security measures protecting them are less rigorous.



The geography of Cryptojacking

Cryptojacking is a global phenomenon, which affects nearly every country in the world. Up to 59% of companies in the UK have been affected by this kind of attack at some point. But the countries that are most affected are the United States (32% of cases) and Spain (14.1% of cases), followed by France, Italy, and Canada.



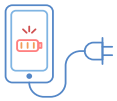


Mediacenter Panda Security: "From the year of ransomware to the year of cryptojacking"

Malwarebytes report "A look into the global 'drive-by cryptocurrency mining' phenomenon" - October 2017.

7. What effects can it have?

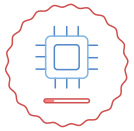
While it may seem as though this type of malware is relatively innocuous – especially if we consider that certain strains are specifically designed to avoid detection and to limit the amount of CPU used – it is in fact, like all malware, **a serious threat to IT security.**



High energy demand. One of the first indications of a cryptojacking malware infection is a significant increase in power consumption. According to some sources, mining the cryptocurrency Monero uses around **332 million kWh a year**, a consumption comparable to that of a small country. This is one of the reasons cybercriminals seek third party computers to mine it: to avoid its costs.

The professionalization of this attack is such that certain types of cryptojacking malware contain code that deactivates hibernation modes in order to keep mining, increasing the power consumption even more, since **the affected computers are constantly mining cryptocurrencies 24/7.**

If cryptojacking malware makes its way into your company, sooner rather than later, you will notice the incredible increase in your energy bill, since cryptojacking will tap into every last computer, and use them as often it can.



CPU use. The aim of cryptojacking is to use the CPU of the affected computers to mine cryptocurrencies, so an increase in consumption of computing power is to be expected. If multiple employees report that their computers are slowing down or overheating, it could be that there is a case of cryptojacking in the company.

Physical damage Excessive CPU use doesn't just cause your company's computers to slow down; excessive use can cause the **destruction of corporate devices.** If mining is carried out for an extended period of time, the temperature of the devices and their batteries can reach such extreme levels that they stop working.

Dangers for corporate cybersecurity. If cryptojacking malware has made its way onto your company's IT network, that means that **there is an open door somewhere.** And this open door means that there is a way in for all kinds of threats – threats that can endanger your company.

Change of strategy. We have seen cases of cryptojacking malware that had previously been used as **ransomware**. It could be the case that, seeing that cryptojacking isn't as profitable as they would like, the cybercriminal falls back on a more direct attack to make some money. There is even a piece of malware that **includes both attacks**, and decides whether to deploy ransomware or cryptojacking, depending on the characteristics of the computer.

A ransomware attack isn't the only secondary consequence that an intruder can trigger if they've managed to make their way onto the network with cryptojacking malware. Once inside the system, **the attacker can gain access to the entire contents of the computer**, including the company's data. A very popular method for cybercriminals to make money is the theft and sale of data – whether it's clients' personal data, credit card numbers, or industrial secrets.

It may even be the case that, once the cybercriminal has access to the IT system for the cryptojacking attack, **they earn more money by "renting out" this access to other cybercriminals**, so that they can exploit the system in their own way.

8. How can I protect my company from cryptojacking?

The cybersecurity experts at PandaLabs affirm that the way to protect against this menace is the same as for any other kind of malware, since cryptomining is carried out using malicious code that is run on your computer. As such, the basic advice is: be sure to have an advanced cybersecurity solution such as Panda Adaptive Defense 360, and don't click on or download unknown files.

Furthermore, to efficiently protect against a cryptomining attack, it's important to follow these security measures:

Carry out periodical risk evaluations to identify vulnerabilities. Panda Patch Management automatically searches for necessary patches to keep the devices on your system safe, prioritizing the most urgent updates. According to data from the analysts at Gartner, establishing appropriate patching policies allows you to reduce the attack surface due to vulnerabilities by up to 80%.

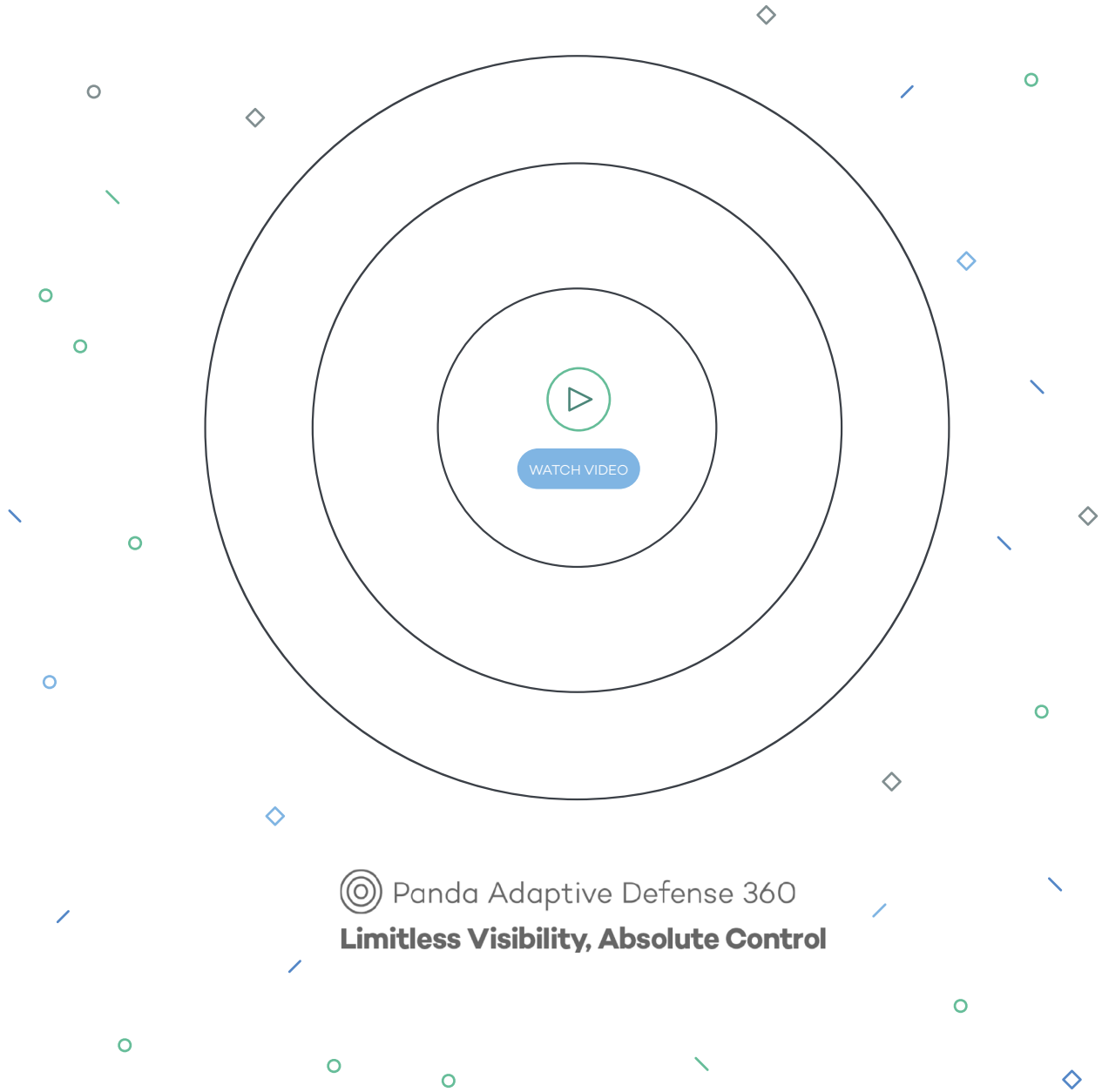
Analyze your resources. All operating systems have some kind of tool similar to System Monitor that analyzes the resources that are being consumed by your company's computers at all times. Keep track of this to make sure there is no unusual activity.

Careful with your browser. If you suspect that cryptojacking is getting in via websites, install plugins to block these sites on your browser.

Thoroughly investigating any spikes in IT problems related to unusual CPU performance. If multiple employees report that their computers are slowing down or overheating, it could be a case of cryptojacking.

Regularly update all of the company's systems and devices, and consider uninstalling software that isn't being used.

Create a safe browsing environment at the company: activating the website access control that is available on advanced cybersecurity solutions, and blocking cryptomining URLs is the best way to protect your endpoint and your company's resources.



These actions need to be accompanied with the implementation of an advanced cybersecurity solution that provides key features such as detailed visibility of the activity on every endpoint, and that provides control of all running processes. All of this is provided by **Panda Adaptive Defense 360**, Panda Security's cybersecurity suite, which is primed to protect all your company's computers against any kind of cyberthreat, be it the classics, or the latest trends.

Follow these tips to keep cryptojacking from undermining your company's reputation and putting the continuity of your company at risk.

Panda Adaptive Defense 360

Limitless Visibility, Absolute Control

More info at:

pandasecurity.com/business/adaptive-defense/

Let´s talk:

900 90 70 80

panda