Cryptocurrency Mining Craze Going for Data Centers

Paying the Bill for Mining Cryptocurrency

Bitdefender®

Abstract

Cryptocurrency is a virtual currency that uses cryptography to guarantee anonymity and provide anti-counterfeit features, enabling anyone to make transactions without being regulated by government or banking institutions. Anonymous and decentralized, virtual currency became synonymous with money laundering, tax evasion, and cybercrime.

This new attack wave started making media headlines in 2017, but gained momentum in the past few months by employing advanced tools to penetrate large enterprises and SCADA systems.

While the process of generating cryptocurrency is usually referred to as "mining," the increased complexity of constantly generating new currency units requires more and more processing power. This means not just scaling up hardware resources, but also picking up the power bill. It's not very profitable to host your own mining rig, because hardware and power consumption costs don't cover the virtual currency's value. And cybercriminals are known to focus on ROI.

This obstacle was overcome by compromising large pools of physical computers, cloud infrastructures and even compromised legitimate websites to collectively mine on cybercriminals' behalf.

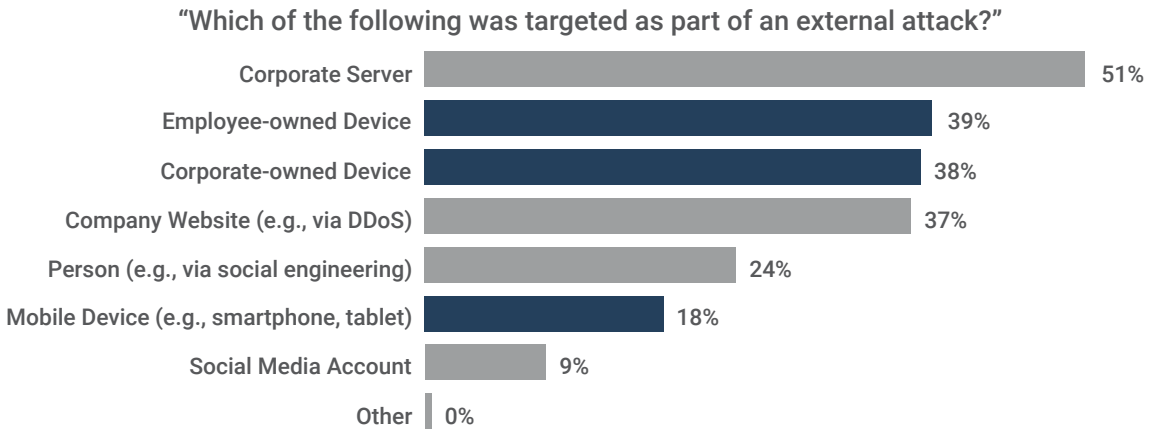
Between September 2017 and January 2018, we witnessed an impressive **increase in global crypto miner reports (130.10 percent)**, showing that cybercriminals are intensely interested in this new money-making scheme.

Cybercriminals sometimes leverage remote code execution (RCE) vulnerabilities to deliver crypto-mining malware to targeted machines. Even the leaked EternalBlue NSA exploit used in 2017 to spread the WannaCry[1] ransomware to more than 150 countries was recently used to target servers to mine cryptocurrency. Worm-like behavior was also embedded into the attack – dubbed WannaMine - automatically spreading through targeted infrastructures and spreading the mining software to other vulnerable servers.

The rising number of attacks and newly employed advanced attack techniques can penetrate data centers, private and public cloud, which rely on massive hardware infrastructures that crypto miners yearn for.

Even recent web-based software – or web scripts - injected into web pages can turn a visitor into a cryptocurrency miner directly from the browser. More than 50,000 legitimate websites were recently[2] found harboring various cryptojacking mining scripts – with or without their owners' knowledge – effectively hijacking visitor's CPU (Central Processing Unit) resources. Cryptojacking web browsers is a business with very high potential, with experts estimating financial gains from Monero campaigns alone can generate more than $100 million per year[3]. The browser-based Monero JavaScript miner is becoming increasingly popular amongst cybercriminals, having increased more than 3,000 percent in the past 12 months.Amid the cryptocurrency frenzy that propelled Bitcoin – one of the most popular virtual currencies – to a whopping $19,000 per unit, raising its market value to $250 billion, threat actors developed new methods for disseminating cryptocurrency-mining malware. Computing power is obviously a key factor in mining, and organizations, data centers, and employee endpoints have naturally become a gold mine for cryptojacking.

Corporate servers, followed by employee-owned devices and corporate-owned devices, are the top three most-targeted devices for cryptocurrency mining, according to analyst company Forester.



Base: 245 global network security decision makers whose firms have had an external security breach in the past 12 months (1,000+ employees)
Source: Forrester Data Global Business Technographics® Security Survey, 2017

Fig. 1 - Forester

Since the preferred method for compromising corporate servers remains leveraging unpatched systems or exploiting unknown vulnerabilities, this trend is expected to last for a long time, as the need for increased computing resources remains.

1. Bitdefender, Protect the Enterprise with Next Generation Machine Learning
The WannaCry ransomware mega-attack and EternalBlue zero-day exploit didn't stand a chance against Bitdefender's advanced machine learning and memory introspection technologies, 2017
2. TheNextWeb, Researcher finds 50,000 sites infected with cryptocurrency mining malware, March, 2018
3. Talos, Ransom Where? Malicious Cryptocurrency Miners Takeover, Generating Millions, January, 2018

Executive Summary

Cybercriminals have always been financially motivated, and cryptocurrency mining is the latest trend in generating revenue by abusing the same age-old malware attack vectors previously associated with ransomware dissemination. The recent Bitcoin craze, with the currency peaking at $19,000 per unit, has focused cybercriminals on crypto mining, instead of traditional ransomware.

Bitdefender telemetry has shown that crypto currency-enabled malware is increasingly outdoing ransomware in popularity, with the rise in adoption picking up in the past six months. In October 2017, the number of coin miner reports **increased from 9.47 percent in September to 17.54 percent in October, from the total amount of coin miner reports during the six-month timeframe**. Around the same time, the Bitcoin frenzy was at its peak. Another surge occurred in January 2018, after coin miner reports **increased from 18.06 percent in December to 21.79 percent in January**.

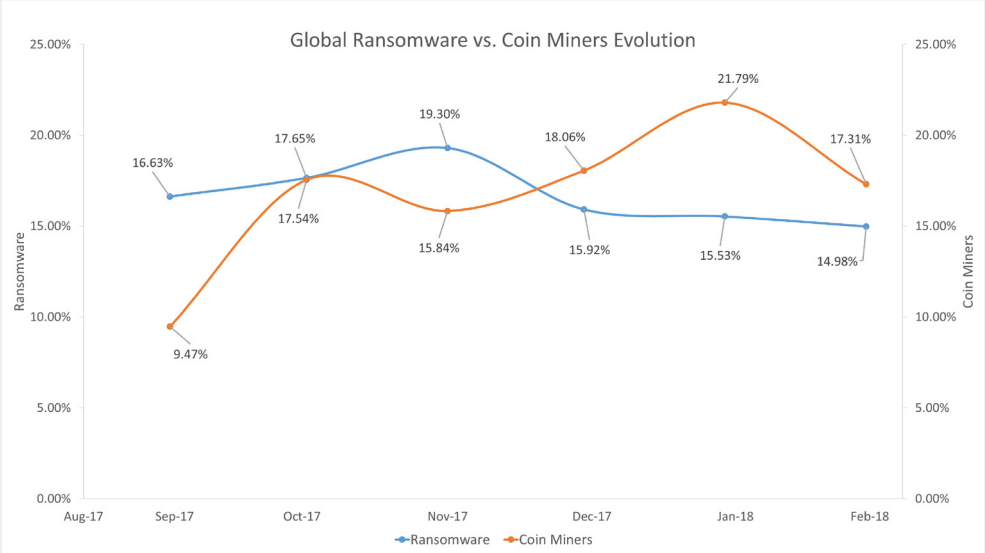


Fig. 2 – Global ransomware vs. virtual currency miner evolution

Our own telemetry also shows that the number of **ransomware reports** has also begun to decrease, **dropping** 3.38 percentage points, which represents **17.52 percent** from November 2017 to December 2017 and continuing on a descending path. The drop in ransomware incidents coincides with a 2.22 percentage point increase **(or 14.03 percent)** in coin miner detection that occurred during the same timeframe. However, the emergence of browser-based web scripts, such as Coinhive, make it extremely easy for cybercriminals to compromise high-traffic websites and plant the cryptocurrency mining script, rather than deploying spear phishing campaigns to infect a large number of victims, as ransomware does.

Reports[4] estimate that the number of websites and domains hosting this specific CPU-consuming cryptocurrency miner advanced 725% percent, possibly meaning that hundreds of thousands of websites have been compromised and rigged to mine virtual currency using visiting users' CPU resources.

The True Magnitude of the Problem

Cybercriminals are nothing if not resourceful. Consequently, the emergence of Coinhive – a web-based miner – has led to a wave of attacks on websites that leverage outdated plugins, services and software, for the sole purpose of using their user base to mine for Monero.

Although Coinhive is a legitimate service, as anyone can embed it in their website and warn users about its deployment, it has been abused by cybercriminals in recent campaigns.

For example, a vulnerability in a popular accessibility plugin, named Browsealoud, present in more than 4,000 UK-based websites[5] – including the UK's Information Commissioner's Office – was exploited to deliver Coinhive to visiting users. Although active for about four hours, it was not an isolated incident.

The L.A. Times's website was also injected with the CoinHive Monero-mining script. By leveraging an improperly secured Amazon Web Services (AWS) S3 bucket, and configuring the miner not to max out CPU consumption, hackers remained undetected. This technique would have enabled the attack to remain stealthy for a considerable time, if not found in time.

Even popular desktop messaging applications, such as Telegram, have been recently[6] abused to deliver crypto currency miners to victims. Although the attack was mostly aimed at mining Zcash (ZEC) and Monero (XMR), some attacks that abused[7] YouTube advertisements delivered only the Monero-mining Coinhive. While malvertising is not a new technique for disseminating malware through legitimate websites and services, the incident did represent a first in terms of distributing cryptocurrency mining software.

4. Cyren, 725% increase in cryptocurrency mining threatens more than just your CPU, March, 2018
5. TechCrunch, Cryptojacking attack hits ~4,000 websites, including UK's data watchdog, February, 2018
6. Blockexplorer, Telegram Desktop App Latest Victim of Cryptocurrency Mining Malware, February, 2018
7. Arstechnica, Now even YouTube serves ads with CPU-draining cryptocurrency miners, January, 2018

One of the most interesting attacks involved the use of industrial control systems that were used for the first time to mine for cryptocurrency. The industrial control systems (ICS) and SCADA (supervisory control and data acquisition) servers of a water utility in Europe[8] were used for the first time to mine Monero.

Because some industrial systems still rely on outdate operating systems and software, it's relatively easy for threat actors to leverage known but unpatched vulnerabilities, and plant malware or mining software that remains undetected for a long time. In this example, the mining process went on for three weeks before it was picked up by security teams.

Reaching the data center

The more cryptocurrency has been mined, the more resource-intensive the process becomes. This makes it unfeasible for cybercriminals to target and control pools of individual users. It is expected that large data centers and cloud infrastructures are next in line, as their elastic computing power enables cybercriminals to virtually spawn and control large mining farms without paying any bills.

Data centers usually allow organizations to scale their business by letting them optimize costs and computing resources based on their immediate requirements. However, if virtual infrastructures become compromised and cloud admins lose authentication credentials via searching attacks, social engineering, or unpatched security vulnerabilities, cybercriminals seize control. From there, it's just a matter of spinning up powerful and resource-intensive rogue virtual instances that come pre-installed with cryptocurrency mining malware.

Since it may take several weeks – or until the bill comes in – to spot rogue virtual hosts, hackers would have already mined tens or hundreds of thousands worth of cryptocurrency while the affected organization is left holding the power/services bill.

As recent events have proven, exploiting the EternalBlue vulnerability to infect Windows servers is just one way for cybercriminals to access fast amounts of computing resources. Even the known Apache Struts (CVE-2017-9805[9]) vulnerability impacting the Struts REST plugin with XStream handler and used during the Equifax data breach[10], was allegedly used by cybercriminals to compromise and gain persistency on Linux-powered machine.

Daisy-chaining exploits and persistency tools together to compromise servers and automatically propagate across networks enables threat actors to successfully plant mining software and leverage the cloud's computing power.

New cryptojacking attacks can hide their tracks better by limiting the strain put on the CPU. By leveraging Powershell, scripts or advance exploits to avoid endpoint detection, attackers can effectively run mining software directly within the memory of the targeted server. Because a server update is always a key business factor and because the attack does not fully throttle the CPU, it can remain undetected for a considerable time.

Attackers have proven creative and can use any client or server-side attack techniques to deliver their payload and start mining away, consuming a company's hardware resources.

A Compromised Data Center is a Damaged Data Center

A confirmed and successful cryptojacking attack involving the business can indicate the presence of a security gap that can also be leveraged by other attacks. This could be disastrous to a business's continuity and reputation.

For example, the WannaCry ransomware attack that used the EternalBlue exploit – also used by WannaMine - is estimated to have caused $53 billion in damage worldwide. Coupling the EternalBlue component with the MimiKatz post-exploitation tool for extracting authentication credentials from memory, have made WannaCry and WannaMine two attacks to be taken seriously by data centers.

Mining for cryptocurrencies is not just about having the hardware resources to solve math algorithms. It's also about sustained stress on the hardware components being used – specifically, CPU and GPU (Graphics Processing Unit) – which may degrade their capabilities a lot faster than estimated.

Speeding up CPU cycles heavily impacts consolidation ratios and virtualization density in your data center. Which is why when workloads are infected by cryptojacking, most infrastructure admins or dev-ops quickly solve the situation by increasing resources on the workloads to bring services on-line. At this point, some don't investigate further, content that the problems are solved.

Constant throttling of CPUs and GPU at 100 percent ultimately burns them out, rendering them useless. This directly translates into operational costs for the data center as they need to be quickly replaced so as not to affect performance.

However, power consumption is equally affected, as CPUs under constant load drain more power than "optimum" usage, meaning racked up IaaS bills without any apparent cause, forcing you to purchase more resources to reestablish critical services. For example, some organizations use a level of automation for implicit scalability purposes, relying on resource monitoring. Whenever a threshold is reached, new resources are automatically provisioned. This can rack up bills if successfully exploited by an attacker seeking to mine virtual currencies.

There's also the risk of having mining software spread to your critical infrastructure. The advanced techniques uncovered in recent cryptojacking attacks lead to more critical security concerns, such as the ability to penetrate internal perimeters and move laterally to critical infrastructures. From industrial control systems to POS devices, internal units are known for running dated, unpatched software, often because new operating systems and updates can inadvertently destabilize the systems.

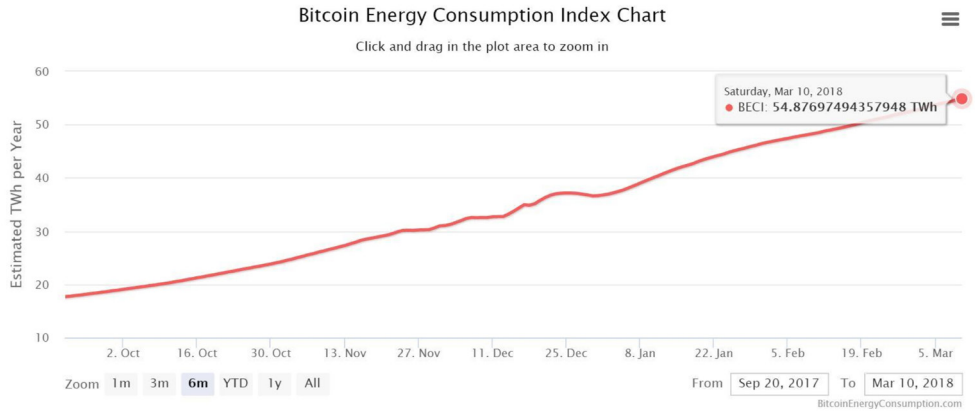
8. eWeek, Water Utility in Europe Hit by Cryptocurrency Malware Mining Attack, February, 2018
9. NIST, CVE-2017-9805 Detail, September, 2017
10. Apache Software Foundation, Apache Struts Statement on Equifax Security Breach, September, 2017

Mining software will also reduce the lifespan of your CPUs and even cause physical destruction by overstraining them, potentially leading to repairs or even the need to replace damaged hardware.

Of course, all this increased throttling also means a bigger impact on the environment. The amount of energy consumed is turning into a real economic problem as powerlines are becoming overburdened and hardware prices, especially graphics cards, are going up.

For instance, prices for some graphics cards has increased by 200 percent[11], while some countries fear[12] that power consumption may outpace production, and some countries even experience blackouts.

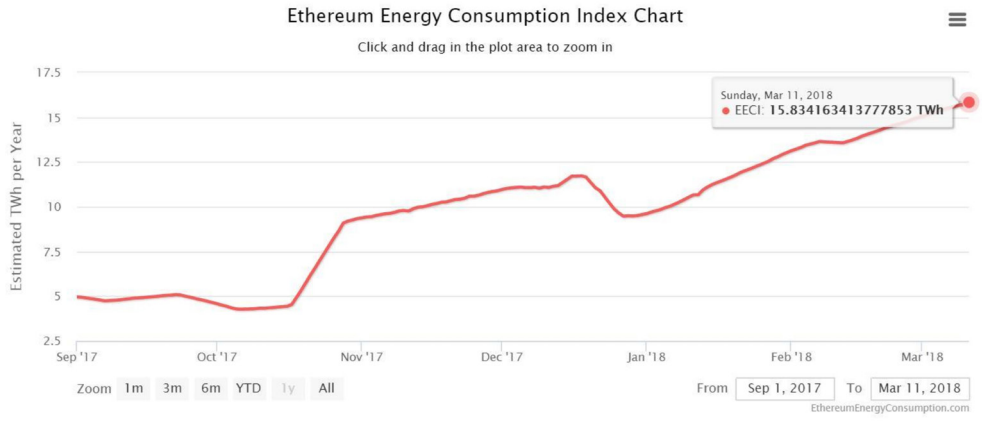
Because miners are also responsible for validating transactions not just mining for new units, the larger the block, the more time and computing power is usually necessary for validation. Experts believe global Bitcoin mining efforts alone consumes more power than used by 159 countries[13], the hardware alone consuming around 31 terawatt hours of energy per year.



Source: DigiConomist

For popular cryptocurrencies, such as Bitcoin and Etherium, the energy consumption index that describes the total amount of energy consumption pins Bitcoin at 55.06 terawatt[14] hours of energy per year, as of March 11th, 2018. Etherium, the second-most-popular cryptocurrency, tops out at 11.83 terawatt[15] hours of energy per year.

On an interesting note, Bitcoin mining[16] is estimated to be more energy-intensive and generate a larger carbon footprint than gold mining.



Source: DigiConomist

11. LI Blog, 2018 Graphics Cards Pricing Update: Current Prices vs. Original Retail Price, January, 2018
12. Washington Post, Cryptocurrency mining in Iceland is using so much energy, the electricity may run out, February, 2018
13. DailiMail, Bitcoin mining 'is using so much energy that it is causing electricity blackouts' amid fears it will consume more power than the world by 2020, December 2017
14. DigiConomist, Bitcoin Energy Consumption Index, March, 2018
15. DigiConomist, Ethereum Energy Consumption Index (beta), March, 2018
16. DigiConomis, Bitcoin Mining is more Polluting than Gold Mining, February, 2018

Both cryptocurrencies have shown a steady increase in energy consumption over the past six months. In 2020, experts predict cybercriminals will use the same amount of power in a year for mining as the rest of the world uses annually.

Securing Data Centers and Endpoints from Cryptojacking

Leveraging most of the advanced techniques used by threat actors to deploy cyberespionage or file-encrypting malware, cryptojacking seems to successfully dodge traditional security solutions. Securing data centers and virtual infrastructures against this new type of threat requires a multi-layered approach to security, comprised of multiple defense technologies that provide the same consistent security levels across the entire infrastructure - physical, virtual, hybrid, on-premise or Cloud – without impacting consolidation ratios or deterring workload performance.

Bitdefender GravityZone Elite provides layered next-generation security that helps prevent and detect cryptojacking file-based and fileless attacks during various stages of the attack lifecycle, both inside the data center and on endpoints. Memory protection technology can detect any exploit-enabled delivery mechanisms looking to distribute cryptomining software onto endpoints.

Fileless and script-based attacks - such as Powershell, cmd and wscript - are detected during pre-execution by our HyperDetect technology, while Bitdefender's proprietary Process Inspector technology augments these capabilities by jumping in during execution.

Since hijacking webpages to deliver Coinhive or other cryptominers to visiting users is also becoming a trend, Bitdefender's Cloud Malware technology will detect not just C&C (command and control) servers that deliver malware, but also websites that contain the mining client.

If, by any chance, attackers deliver payloads such as coin miners or scripts, they will be detected by Bitdefender's core antimalware technologies. Any previously unseen payloads associated to new attacks will be intercepted by Process Inspector technology.

A powerful prevention technology that can help keep data centers from falling victim to highly advanced cryptojacking threats, such as WannaMine that leverages the EternalBlue vulnerability[17], Hypervisor Introspection, can prevent this type of attack from reaching networks by detecting zero day or advanced kernel-level exploits used to penetrate the infrastructure. Since this is a complementary security layer that works with any existing in-guest security solutions, Bitdefender HVI is uniquely capable of defending against zero day vulnerabilities and advanced threats, whether their purpose is to plant cyberespionage malware or deliver cryptocurrency mining software.

Since cryptocurrency mining isn't going anywhere any time soon and computing power necessary for mining operations will constantly increase, data centers and organizations need to deploy the same advanced layered security technologies as they would to defend against advanced and sophisticated threats. Leveraging government-leaked or unpatched vulnerabilities, cryptojacking is becoming a serious business and security concern. While such an attack can remain stealthy for a long time, detecting it is not just a matter of optimizing resource consumption, but also a security matter as it indicates the presence of threat actors within your infrastructure.

Ransomware and Coin Miners Distribution by Region

In terms of the region-specific evolution of both ransomware and coin miners, coin miner reports in the United States seem to have climbed steeply. During September 2017 we detected **9.17 percent** of the total coin miner reports in the United States for the previous six months, but January was by far the most prolific, with **21.24 percent** of all coin miner reports during the same timeframe.

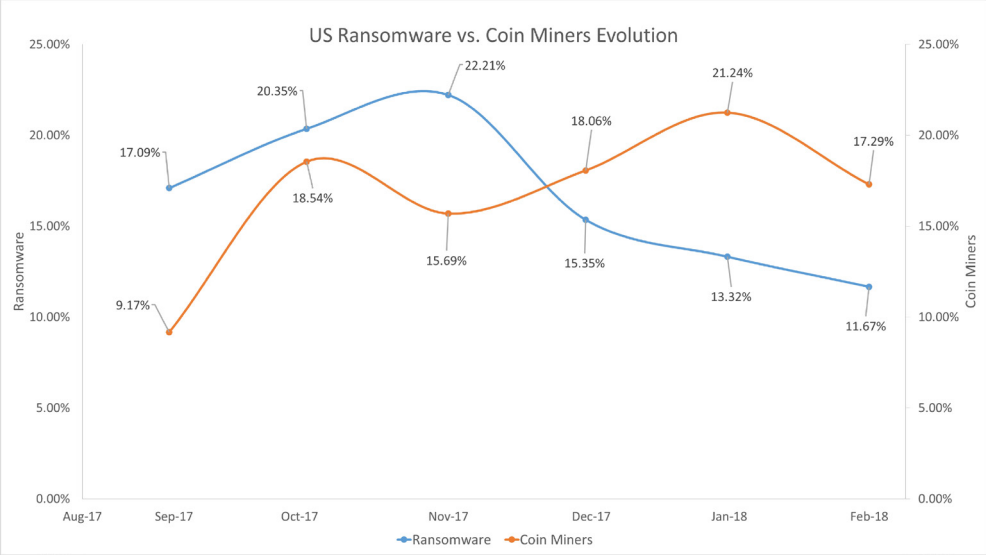


Fig. 3 - US ransomware vs. virtual currency miner evolution

Ransomware reports, on the other hand, have been steadily decreasing in the **United States**. If during September 2017 we saw **17.09**

17. Bitdefender, Hypervisor Introspection defeated Eternalblue a priori, April, 2017

percent of the total number of ransomware reports in the US, by February that dropped to **11.67 percent**. Side-by-side comparison of the evolution of both ransomware and coin miners within the United States clearly indicates that cybercriminals have been focusing more on the latter.

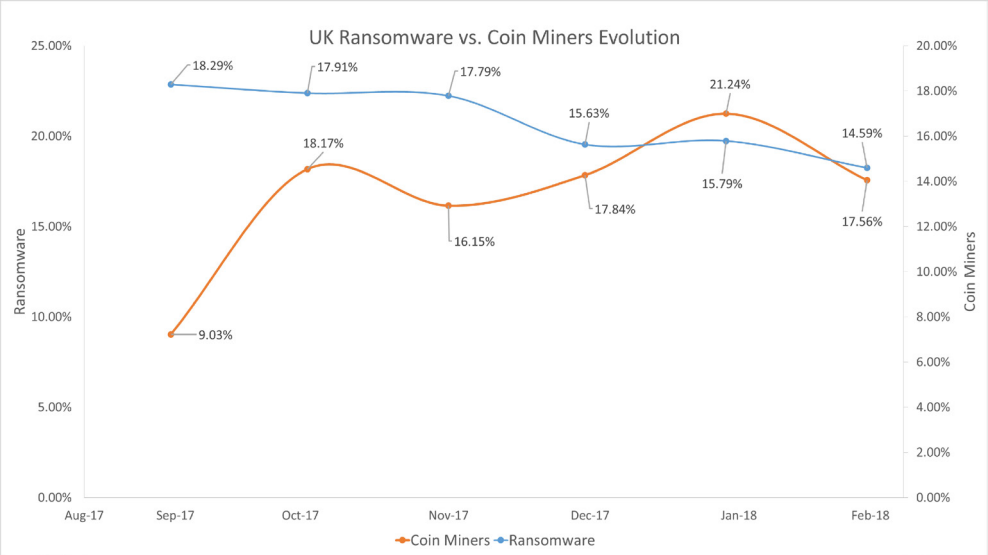


Fig. 4 - UK ransomware vs. virtual currency miner evolution

The descending ransomware evolution can also be observed in the **UK**, where from **18.29 percent** of the total number of ransomware reports in the UK during the six-month timespan, the percentage dropped to **14.59 percent** in February. This drop has been consistent throughout the analyzed six months and seems to be directly related to the evolution of coin miners.

For example, from September's **9.03 percent** of the total number of coin miner reports in the UK, to **21.24 percent** in January 2018, coin miner evolution in the UK has increased by **12.21 percentage points**. This is actually a **135.17 percent increase** in reported coin miners in less than six months.

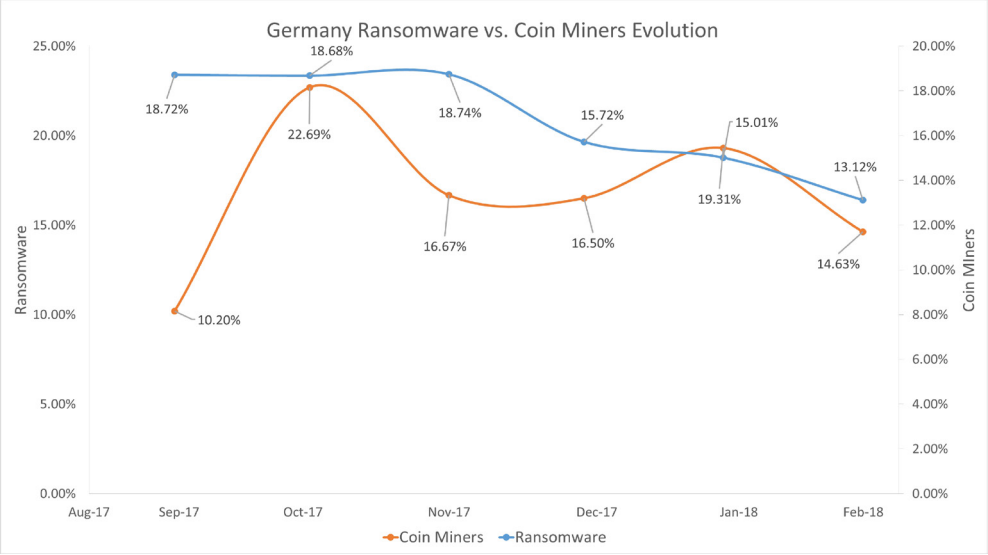


Fig. 5 - Germany ransomware vs. virtual currency miner evolution

While ransomware reports slightly decreased during the past six months, from 18.72 percent of the total number of ransomware reports in **Germany** during September to 13.12 percent in February, coin miners have had ups and downs. From **10.20 percent** of the total number of coin miner reports in **September** to a whopping **22.69 percent in October**, coin miner reports have fluctuated, ending at **14.63 percent in February**. Unlike ransomware, which has only been on a descending curve, coin miner reports in Germany seem to have had their ups and downs.

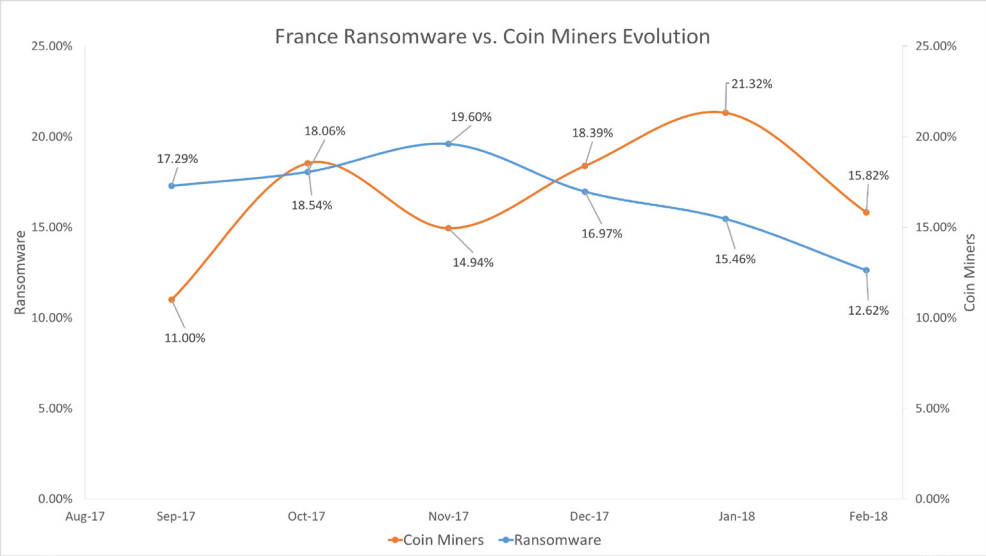


Fig. 6 - France ransomware vs. virtual currency miner evolution

The ransomware-versus-coin-miner trend seems to be present in **France** as well, as ransomware reports seem to have taken a nose dive while coin miners have significantly increased compared to September 2017. From **17.29 percent** of the total number of ransomware reports in France for the previous six months, to **12.62 percent in February 2018**.

The only noteworthy spike in ransomware reports seems to have occurred in **November, increasing by 2.31 percentage points**, while at the same time coin miner reports dropped by **3.6 percentage point**s compared to **October**, reaching **14.94 percent** of the total number of coin miner reports in France, during the analyzed six months. Overall, coin miner reports steadily increased from **11 percent in September**, to **15.82 percent in February**, peaking at **21.32 percent in January 2018**.

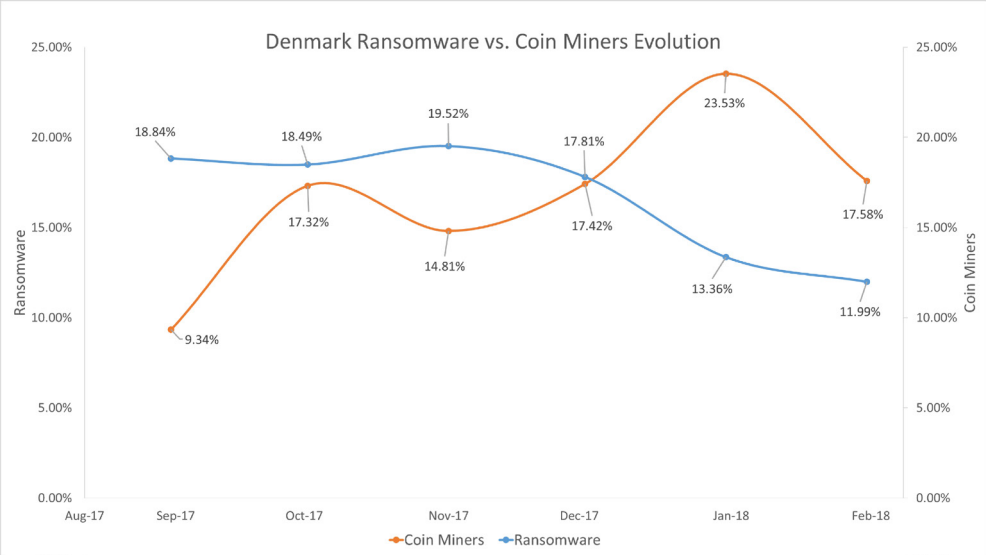


Fig. 7 - Denmark ransomware vs. virtual currency miner evolution

The evolution of coin miners in **Denmark** is probably the steepest observed during the past six months, peaking in **January at 23.53 percent** of the total number of coin miner reports in Denmark for the previous six months, from **9.34 percent** in September 2017. The **14.19 percentage-point** increase translates into a **151.88 percent increase** in coin miner reports **between September 2017 and January 2018**. Ransomware evolved in line with the global trend, dropping in February to 11.99 percent of the total number of ransomware reports during the analyzed six months, after **peaking at 19.52 percent in November 2017**.

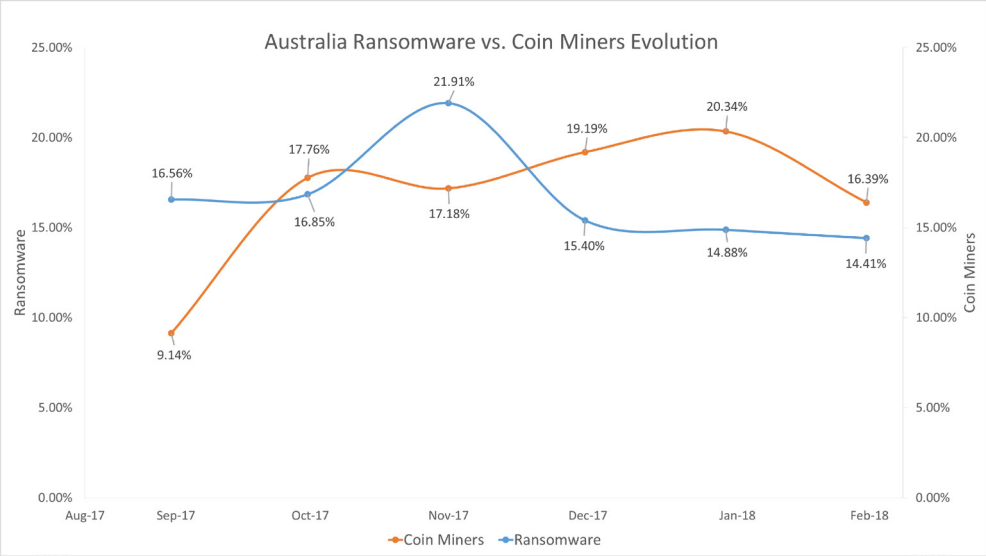


Fig. 8 - Australia ransomware vs. virtual currency miner evolution

The most notable ransomware report spike in Australia occurred in **November 2017**, reaching **21.91 percent** of the total number of ransomware reports within six months in Australia. By **February**, the number of ransomware reports plummeted by 7.5 percentage points, reaching the lowest value, of **14.41 percent**, within the analyzed timeframe.

As expected, coin miners also grew in popularity, peaking in January 2018 at 20.34 percent of the total number of coin miner reports in Australia during the past six months. Increasing by **11.2 percentage points compared to September 2017**, this points to an increase of **122.50 percent** in coin miner reports in five months alone.

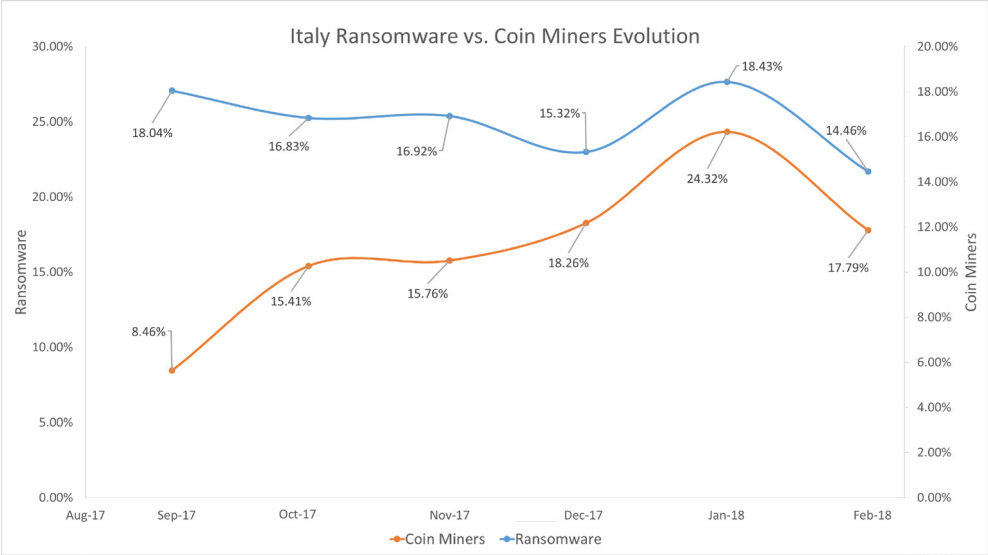


Fig. 9 - Italy ransomware vs. virtual currency miner evolution

Both ransomware and coin miner evolution in **Italy** follows the footprints of the global trends. Although ransomware has remained somewhat constant, it did **drop in February to 14.46 percent** of the total number of ransomware reports in Italy between September 2017 and February 2018. The most ransomware reports occurred in **January (18.43 percent)**, rising slowly from **18.04 percent in September 2017**.

Coin miner reports significantly increased from **September's 8.46 percent** of the total number of reports in Italy during the past six months. Peaking in **January at 24.32 percent**, coin miner reports have increased by **110.40 percent compared to September 2017**.

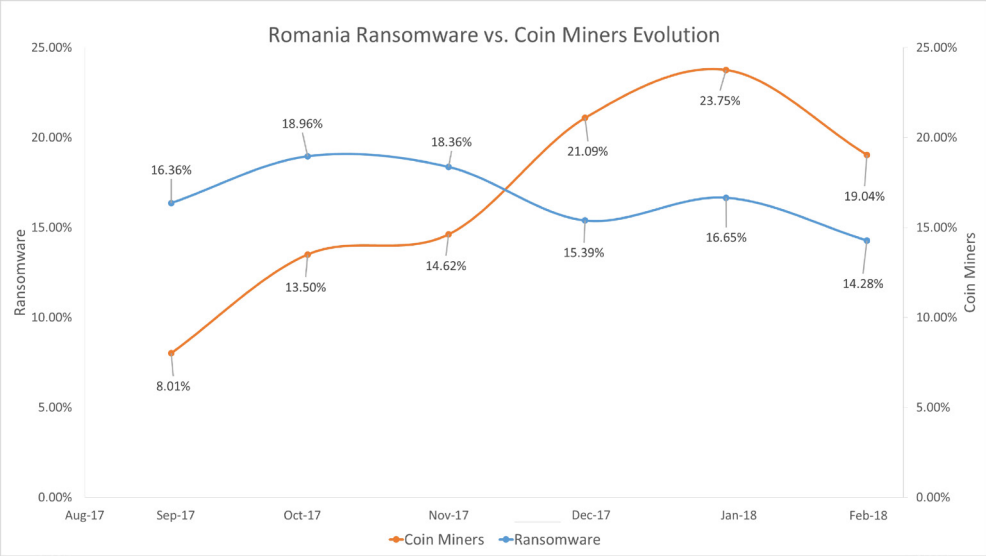


Fig. 10 - Romania ransomware vs. virtual currency miner evolution

The evolution of ransomware and coin miners in **Romania** is highly representative, as reports also indicate that coin miners have increased in popularity while ransomware reports have plateaued and even declined.

Starting **in September with 16.36 percent** of the total number of ransomware reports in Romania during the analyzed six months, ransomware reports quickly declined to **14.28 percent in February 2018**.

Coin miners, on the other hand, steadily increased from **September's 8.01 percent** of the total number of coin miner reports in Romania in the previous six months, reaching **23.75 percent in January 2018**. Both ransomware's descending curve and the coin miner's ascending trend can be clearly observed in Fig. 10 above.

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.

© 2018 Bitdefender. All rights reserved. All trademarks, trade names, and products referenced herein are property of their respective owners. FOR MORE INFORMATION VISIT: bitdefender.com/business