



KSN Report: Ransomware and malicious cryptominers 2016-2018

Contents

KSN Report:	1
Ransomware and malicious cryptominers 2016-2018	1
Executive summary and main findings.....	3
Introduction: A disappearing species - a brief look at ransomware decline over a year	5
Game changer – how cryptocurrency miners beat them all	18
Part 1. PC miners	18
Part 2. Mobile miners	24
Part 3. Between black and white: are risk tools replacing malware?	29
Conclusions and predictions	33
Fighting back	34

Executive summary and main findings

Ransomware is not an unfamiliar threat. For the last few years it has been affecting the world of cybersecurity, infecting and blocking access to various devices or files and requiring users to pay a ransom (usually in Bitcoins or another widely used e-currency), if they want to regain access to their files and devices.

The term ransomware covers two main types of malware: so-called window blockers (which block the OS or browser with a pop-up window) and cryptors (which encrypt the user's data). The term also encompasses select groups of Trojan-downloaders, namely those that tend to download encryption ransomware once a PC is infected.

Kaspersky Lab has a tradition of reporting on the evolution of ransomware – and you can find previous reports on the threat [here](#) and [here](#).

This year, however, we came across a huge obstacle in continuing this tradition. We have found that ransomware is rapidly vanishing, and that cryptocurrency mining is starting to take its place.

The architecture of cryptocurrencies assumes that, in addition to purchasing cryptocurrency, a user can create a new currency unit (or coin) by harnessing the computational power of machines that have specialized 'mining' software installed on them.

Cryptocurrency mining is the process of creating these coins – it happens when various cryptocurrency transactions are verified and added to the digital blockchain ledger. The blockchain, in its turn, is a chain of successive blocks holding recorded transactions such as who has transferred bitcoins, how many, and to whom. All participants in the cryptocurrency network store the entire chain of blocks with details of all of the transactions that have ever been made, and participants continuously add new blocks to the end of the chain.

Those who add new blocks are called miners, and in the Bitcoin world, as a reward for each new block, its creator currently receives 12.5 Bitcoins. That's approximately \$30,000 according to the exchange rate on July 1, 2017. You can find out more about the mining process [here](#).

Given the above, this report will examine what is hopefully ransomware's last breath, in detail, along with the rise of mining. The report covers the period April 2017 to March 2018, and compares it with April 2016 – March 2017.

Methodology:

This report has been prepared using depersonalized data processed by Kaspersky Security Network (KSN). The metrics are based on the number of distinct users of Kaspersky Lab products with the KSN feature enabled, who encountered ransomware and cryptominers at least once in a given period, as well as research into the threat landscape by Kaspersky Lab experts.

Main findings:

- The total number of users who encountered ransomware fell by almost **30%**, from **2,581,026** in 2016-2017 to **1,811,937** in 2017-2018;
- The proportion of users who encountered ransomware at least once out of the total number of users who encountered malware fell by around **1 percentage point**, from **3.88%** in 2016-2017 to **2.80%** in 2017-2018;
- Among those who encountered ransomware, the proportion who encountered cryptors fell by around **3 percentage points**, from **44.6%** in 2016-2017 to **41.5%** in 2017-2018;
- The number of users attacked with cryptors almost **halved**, from **1,152,299** in 2016-2017 to **751,606** in 2017-2018;
- The number of users attacked with mobile ransomware fell by **22.5%** from **130,232** in 2016-2017 to **100,868** in 2017-2018;
- The total number of users who encountered miners rose by almost **44.5%** from **1,899,236** in 2016-2017 to **2,735,611** in 2017-2018;
- The share of miners detected, from the overall number of threats detected, also grew from almost **3%** in 2016-2017 to over **4%** in 2017-2018;
- The share of miners detected, from overall risk tool detections, is also on the rise – from over **5%** in 2016-2017 to almost **8%** in 2017-2018;
- The total number of users who encountered mobile miners also increased – but at a steadier pace, growing by **9.5%** from **4,505** in 2016-2017 to **4,931** in 2017-2018.

Introduction: A disappearing species - a brief look at ransomware decline over a year

Early 2017 witnessed a dangerous trend: cybercriminals started to turn their attention away from attacks against private users, to targeted ransomware attacks against businesses. Focusing mainly on financial organizations worldwide, ransomware actors were hunting new and more profitable victims. On the one hand, this change led to ransomware being the '[story of the year](#)'. On the other hand, this change turned out to be more of an isolated surge than a trend.

The past year's most remarkable ransomware trend was the rapid spread of threats such as [Wannacry](#) and [Badrabbit](#). These were global epidemics that triggered a huge peak in the number of ransomware victims in a very short space of time. Taking a closer look, we found that ransomware was also used by advanced threat actors to mount attacks for data destruction, rather than for pure financial gain.

However, our quarterly analysis also showed us that ransomware was leaving the scene: see [here](#) for more information.

This discovery led us to speculate whether the ransomware business model was starting to crack. Was there a more lucrative alternative for cybercriminals looking to make money? What could it be? Our guess was that criminals were starting to turn their backs on ransomware, to focus on cryptocurrency mining instead.

Kaspersky Lab's [threat predictions for cryptocurrencies](#) in 2018, suggested a rise in targeted attacks for the purpose of installing miners. While ransomware can provide cybercriminals with potentially large but one-off rewards in a turbulent landscape, miners might make less money out of their victims, but through a more sustainable/ longer-term model.

PC ransomware

The numbers for the observed period prove the above theory.

The total number of users who encountered ransomware over the 12 month period from April 2017 to March 2018 fell by almost **30%** in comparison to the previous year: April 2016 to March 2017 – from **2,581,026 to 1,811,937** users around the world. This change is even more dramatic if you consider that ransomware had risen by **17.7%** from April 2015 to March 2016, and **11.4%** from April 2016 to March 2017 (see previous reports for more details).

The proportion of users that encountered ransomware at least once, out of the total number of users who encountered malware, is also falling steadily: **4.34%** in 2015-2016, **3.88%** in 2016-2017, and **2.80%** in 2017-2018.

The following graphs illustrate the change in the number of users encountering ransomware at least once in the 24-months covered by this report. As can be seen in Fig. 1, the volume of

ransomware attacks has been steadily decreasing, barely exceeding 350,000 per month. The two peaks, in May and in July, can be simply explained by the [Locky ransomware](#), which was active at these times.

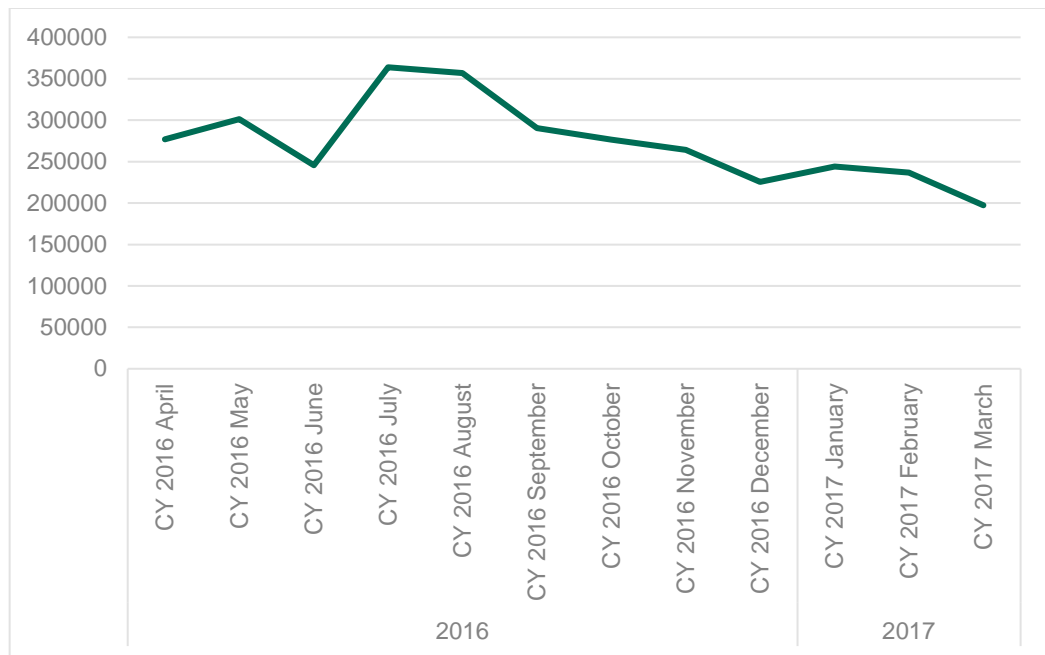


Fig. 1: The number of users encountering ransomware at least once in the period from April 2016 to March 2017

The drop in June can be explained by a slowdown in the activities of several ransomware families. The following year the pattern looks similar, but shows even lower volumes at between 200,000 and 250,000 detections per month.

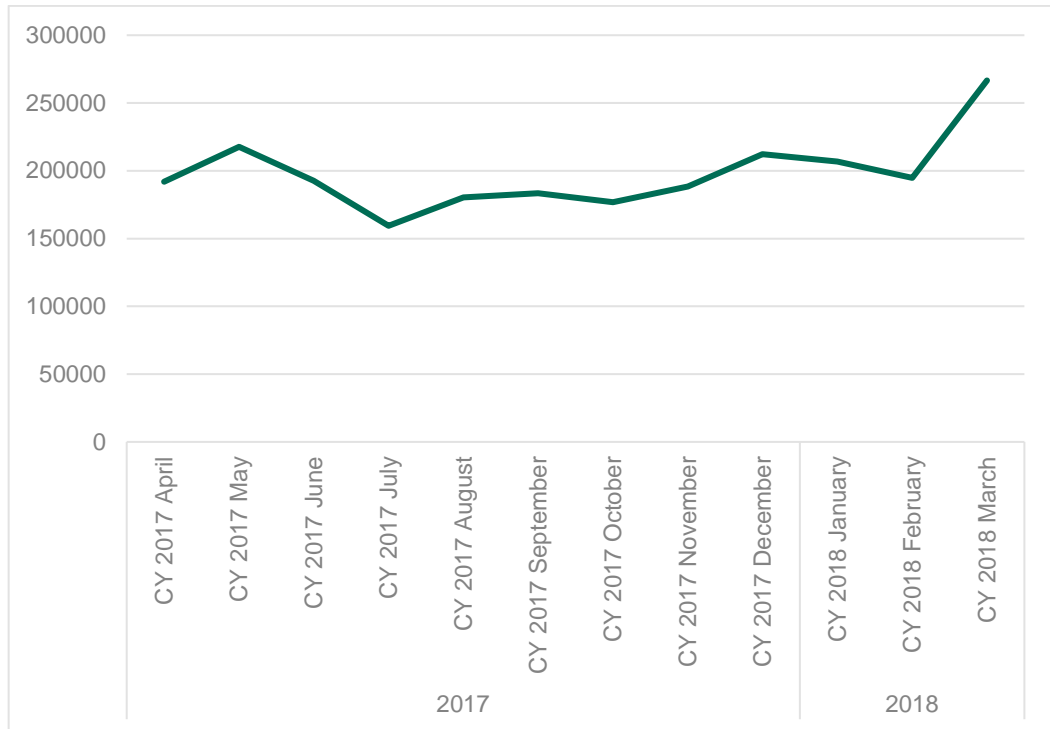


Fig. 2: The number of users encountering ransomware at least once in the period from April 2017 to March 2018

The slight peak in May 2017 was fueled by the WannaCry pandemic, and the [SynAck](#) targeted ransomware, which used the Doppelgänger technique and was also prevalent in the spring. The drop in ransomware in July was caused by a brief slowdown in the activities of Locky, Jaff and ExPetr.

Both of the above graphs show that ransomware is decreasing in volume. However, it is still a dangerous threat.

Main actors of crypto-ransomware

Looking at the malware groups active in the period covered by this report, it appears that a rather diverse list of suspects is responsible for most of the trouble caused by crypto-ransomware. In the first period, 2016-2017, most of the attacks were from [Locky](#), [CryptXXX](#), Zerber, Shade, Crusis, Cryrar, Snocry, Cryakl, Cryptodef, Onion and [Spora](#) – with these threats attacking about a third of all crypto-ransomware victims during the period.

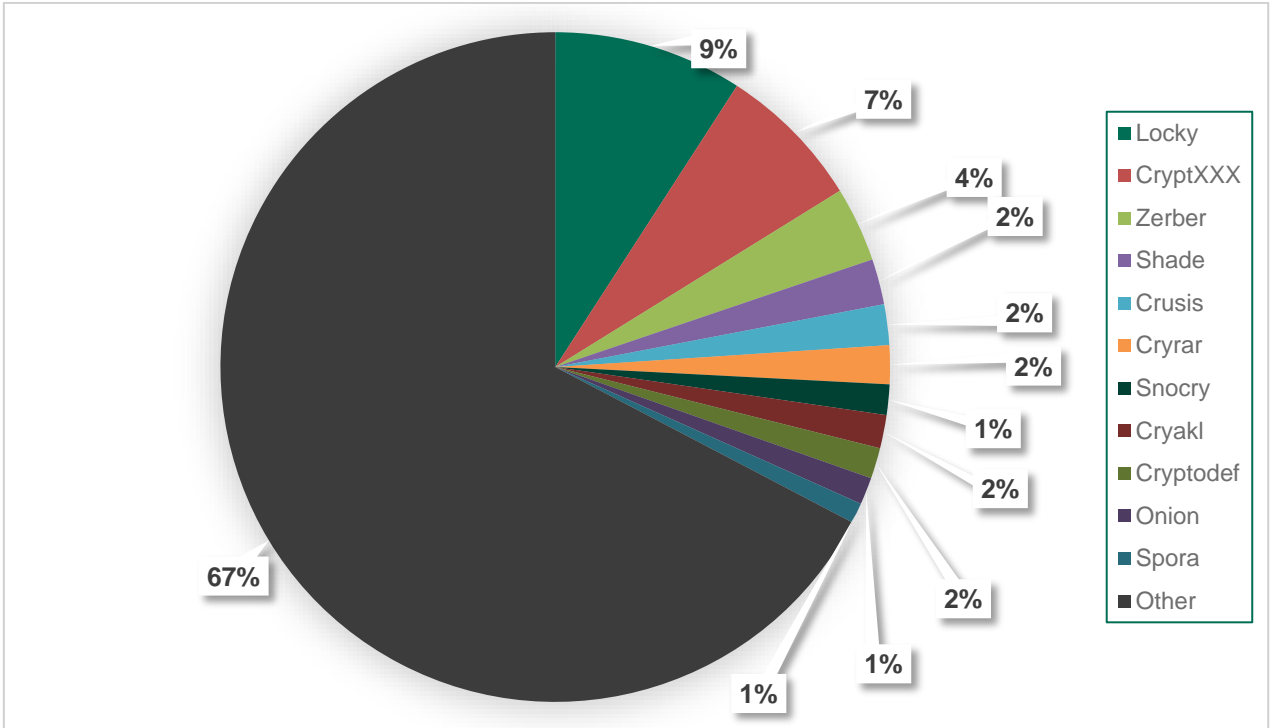


Fig. 3: Distribution of users attacked with different groups of encryption ransomware in 2016-2017

A year later, the landscape looked different. The main change was the domination of WannaCry, with other ransomware leaders such as Locky, Zerber, and Shade retaining about the same share of victims.

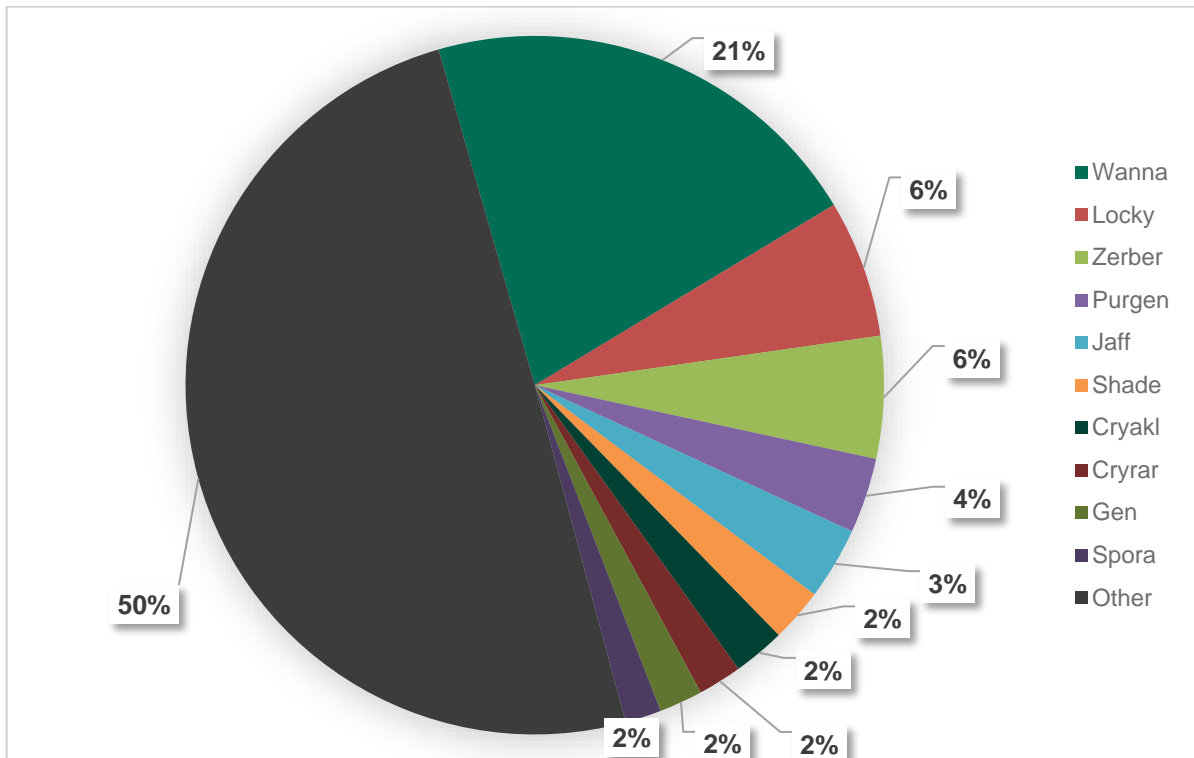


Fig. 4: Distribution of users attacked with different groups of encryption ransomware in 2017-2018

So what else changed? Well, the share of victims affected by the top ransomware actors grew from 33% to 50% (even through the number of attacks in this period was significantly lower than before). Thus, we can say that while the share grew, the numbers fell – making the landscape more centralized and less competitive.

Interestingly, the drop in the number of victims was not experienced by every ransomware family – for instance, the number of internet users affected by Zerber and Shade remained the same (40,000 and 20,000 respectively).

Geography

When analyzing the geography of attacked users, we always consider the fact that the numbers are influenced by the distribution of Kaspersky Lab's customers around the world.

That is why we use special metrics: the percentage of users attacked with ransomware as a proportion of users attacked with any kind of malware. In order to keep statistics representative, the list of countries includes regions with over 30,000 unique users of Kaspersky Lab products.

In 2016-2017, the list of countries with the highest share of users attacked with ransomware was as follows:

Country	% of users attacked with ransomware out of all users encountering malware
Turkey	7.93%
Vietnam	7.52%
India	7.06%
Italy	6.62%
Bangladesh	6.25%
Japan	5.98%
Iran	5.86%
Spain	5.81%
Algeria	3.84%
China	3.78%

Fig.5: The list of countries with the biggest share of users (each country has more than 30,000 unique users of Kaspersky Lab products) attacked with ransomware as a proportion of all users attacked with any kind of malware in 2016-2017

During this period, new countries, including Turkey, Bangladesh, Japan, Iran, and Spain, entered the list. These changes could mean that attackers had switched to targeting previously unaffected territories, where users are not as well-prepared for fighting ransomware, and where competition among criminals is not so high.

One year later the landscape had changed again.

Country	% of users attacked with ransomware out of all users encountering malware
Thailand	9.57%
United Arab Emirates	8.67%
Iran	8.47%
Bangladesh	7.62%
Vietnam	6.17%
Saudi Arabia	5.45%
China	5.36%
India	4.28%
Algeria	3.59%
Turkey	3.22%

Fig.6 The list of countries with the biggest share of users (each country has more than 30,000 unique users of Kaspersky Lab products) attacked with ransomware as a proportion of all users attacked with any kind of malware in 2017-2018

As we can see, the list looks very similar, including more or less the same regions. However, it is worth noting that Turkey fell from first to tenth place, while Japan left the list entirely. This was due to the decrease in Crusis and Locky activities. The UAE joined the ranking, taking second place, while Iran hit the top three. Let's take a closer look at how these states have evolved in this time.

Country	2016-2017	2017-2018	Y-to-Y change (%)
Thailand	445,458	494,972	Up 11.1%
United Arab Emirates	423,627	401,580	Down 5.2%

Iran	701,540	757,491	Up 8%
Bangladesh	562,798	528,840	Down 6%
Vietnam	2,412,909	2,172,184	Down 10%
Saudi Arabia	671,923	650,465	Down 3.2%
China	974,045	992,610	Up 1.9%
India	4,147,085	3,880,599	Down 6.4%
Algeria	1,012,279	918,836	Down 9.2%
Turkey	982,417	954,711	Down 2.8%

Fig. 7: The year-on-year change in the number of users attacked with any type of ransomware

Interestingly, while these countries top the rankings in terms of the share of users attacked with ransomware, out of all users encountering malware, if we look at absolute figures the ranking would be different – states like Vietnam, India or Algeria have higher numbers of attacks than others. Their percentages are more moderate due to the overall number of malware detections.

According to our statistics, increases in China, Iran and Thailand were also fueled by the activities of several families – in the case of China for example, WannaCry was a game changer.

The numbers above highlight horizontal changes in the global ransomware landscape. But if we look deeper into the share of users attacked with a Trojan-ransom actors, and who experienced an attack by encryption ransomware, the picture becomes slightly different.

Country	% of users attacked with encryption ransomware in 2016-2017	% of users attacked with encryption ransomware in 2017-2018
Thailand	3.43%	9.57%
United Arab	6.08%	8.67%
Iran	5.86%	8.47%
Bangladesh	6.25%	7.62%
Vietnam	7.52%	6.17%
Saudi Arabia	3.48%	5.45%
China	3.78%	5.36%
India	7.06%	4.28%
Algeria	3.84%	3.59%
Turkey	7.93%	3.22%
Other	44.77%	37.60%

Fig. 8: The year-on-year change in the share of users attacked with encryption ransomware as a proportion of users attacked with any kind of ransomware.

As we can see, the share in 2017-2018 is higher in most cases and explains why, for example, Thailand, UAE, and Iran hit the top three countries in this period. At the same time, the overall share of the top 10 countries did not change significantly – it grew slightly, by around seven percentage points, amid an overall decrease in ransomware activities.

The above section clearly demonstrates that, while ransomware is slowing down across the world, we can still see changes in its global geographic distribution. This obviously means that users, especially in these affected countries, should be particularly cautious when surfing the web.

Mobile ransomware

By 2017-2018 the number of users attacked with mobile ransomware had fallen by **22.5%**, from **130,232** in 2016-2017 to **100,868** in 2017-2018, accelerating the previous year's trend, when the pace decreased by **4.62%** y-o-y.

However, despite this decline in the total number of users impacted, mobile ransomware Trojans remain a serious threat, because they have become much more technically advanced and more dangerous than before.

For instance, Trojan-Ransom.AndroidOS.Svpeng obtains administrator rights to the device, and whenever the user tries to reclaim these, it blocks the screen of the smartphone, requiring the user to enter their PIN code. If the latter has not been installed, the device becomes inaccessible to the victim. In this case, the only way they can restore the device is by going back to its factory settings.

The broader timeline of mobile ransomware activities is interesting. Across the years, mobile ransomware has grown, leaving a lot of users defenseless. From April 2014 to March 2015, Kaspersky Lab security solutions for Android protected 35,413 users from mobile ransomware. The following year, the number had increased almost four-fold to 136,532 users. The first months of 2017 gave us a sign of possible further growth: mobile ransomware activity skyrocketed in early 2017 with 218,625 mobile Trojan-Ransomware installation packages – that is 3.5 times more than in the previous quarter.



Fig. 9: The number of users encountering mobile ransomware at least once in the period April 2015 to March 2017

But then – well, you might be able to guess what happened next.

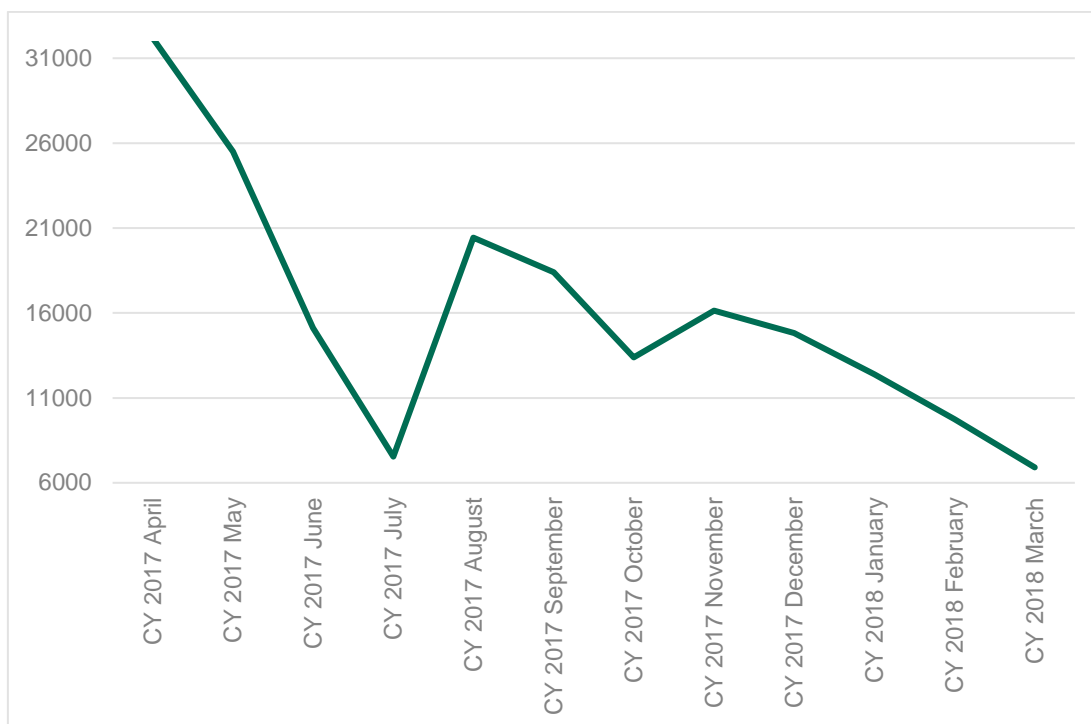


Fig. 10: The number of users encountering mobile ransomware at least once in the period April 2017 to March 2018

That is what happened. The number decreased; reaching its minimum in the summer, following the same pattern as PC ransomware. Indeed, July 2017 became the worst month for ransomware success across the observed periods. This was mainly due to a decrease in the activity of all ransomware families we were monitoring within this period. Despite a slight relief in August, the trend remained the same – mobile ransomware activity is falling, reaching another low point in March 2017.

It is worth noting that the share of mobile users attacked with ransomware, as a proportion of users attacked with any kind of malware, experienced some relief in the earlier period: it was 2.04% in 2014-2015, but grew to 4.63% in 2015-2016 and then dropped again to 2.78% in 2016-2017. The same trend was witnessed with PC ransomware, which means that the overall volume of malware is growing faster than the ransomware attacks. The situation changed in 2017-2018 with the share dropping to 0.65%. Clearly therefore, we are witnessing an overall downturn in this cybercriminal landscape.

The geography of mobile ransomware differs significantly from that of PC ransomware. With mobile ransomware in the 2016-2017 period, the list of countries includes regions with over 2,500 unique users of Kaspersky Lab products.

Country	% of users attacked with ransomware out of all users encountering malware
United States	18.65%

Canada	17.97%
Germany	15.46%
United Kingdom	13.37%
Italy	11.87%
Kazakhstan	6.78%
Spain	6.35%
Mexico	5.85%
Ukraine	1.96%
Russian Federation	0.88%

Fig. 11: Top 10 countries with the highest percentage of mobile users attacked with Trojan-Ransom malware, as a proportion of users attacked with any kind of mobile malware (each country has more than 2,500 unique users of Kaspersky Lab products for Android devices). Period: April 2016 – March 2017.

The United States took first place, followed by Canada and Germany. At the same time, Russia took the lowest position in the ranking, something which could be explained by the simultaneous growth of overall malware attacks, combined with a decline in ransomware attacks in the region.

The next period looked different – due to the downturn, we even had to increase the minimum number of unique users of Kaspersky Lab products to 10,000. Moreover, the highest share fell from 18.65% to 1.64%.

Country	% of users attacked with mobile ransomware out of all users encountering
United States	1.64%
Kazakhstan	1.60%
Belgium	1.16%
Italy	1.10%
Poland	1.03%
Romania	0.78%
Mexico	0.70%
Ireland	0.68%
Germany	0.66%
China	0.66%

Fig. 12: Top 10 countries with the highest percentage of mobile users attacked with Trojan-Ransom malware, as a proportion of users attacked with any kind of mobile malware (each country has more than 10,000 unique users of Kaspersky Lab products for Android devices). Period: April 2017 – March 2018.

While the United States retained its leading position, Kazakhstan and Germany shifted up the ranks, hitting the top three. Russia left the ranking, being replaced by China on almost the same terms – with a share at the level of 0.66%.

The main issue, however, remained the same – despite the overall slowdown and downturn in mobile malware, this threat continues to target developed or large developing markets. The reasons for this are simple: they not only have a higher level of income, but also a more advanced and more widely used mobile and e-payment infrastructure. You can find more [details](#) about this trend in a previous report.

The main mobile ransomware actors

In 2016-2017, users of our products encountered the following mobile ransomware families the most:

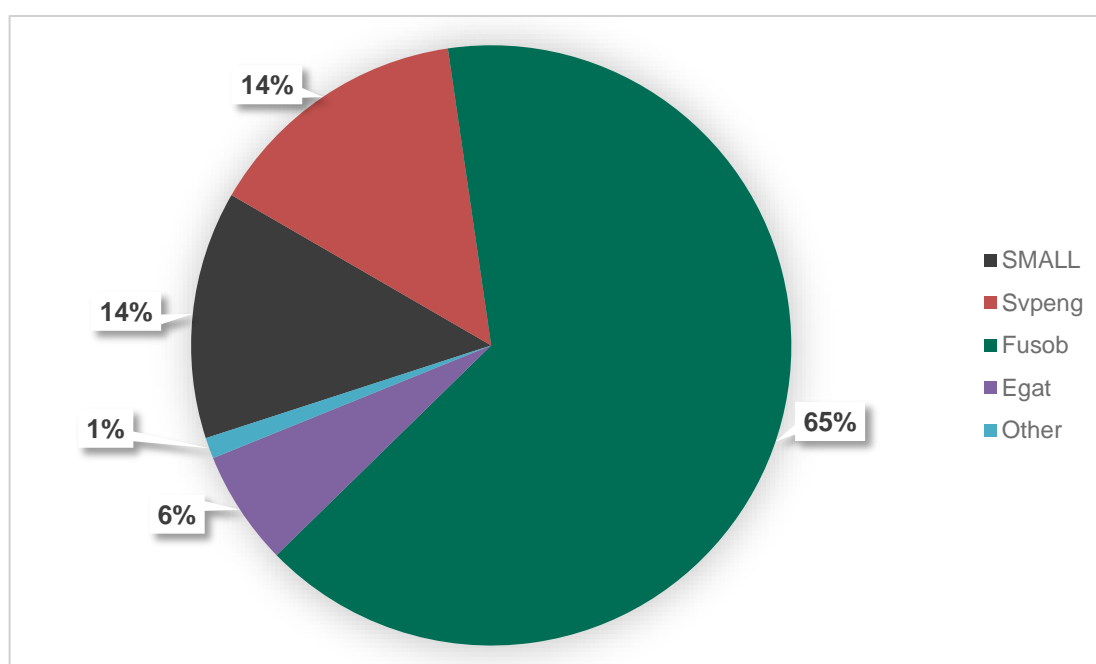


Fig. 13: The distribution of the share of attacked users between the most active mobile ransomware families in 2016-2017.

The 'other' section dropped significantly, from 22% in 2015-2016 to just 1%, mainly due to the expansion of the Fusob family (from 47% to 65%) and the return of Svpeng activity (from 1% to 14%). Together with SMALL, these were the most active families in the previous period.

One year on, the distribution looked like this:

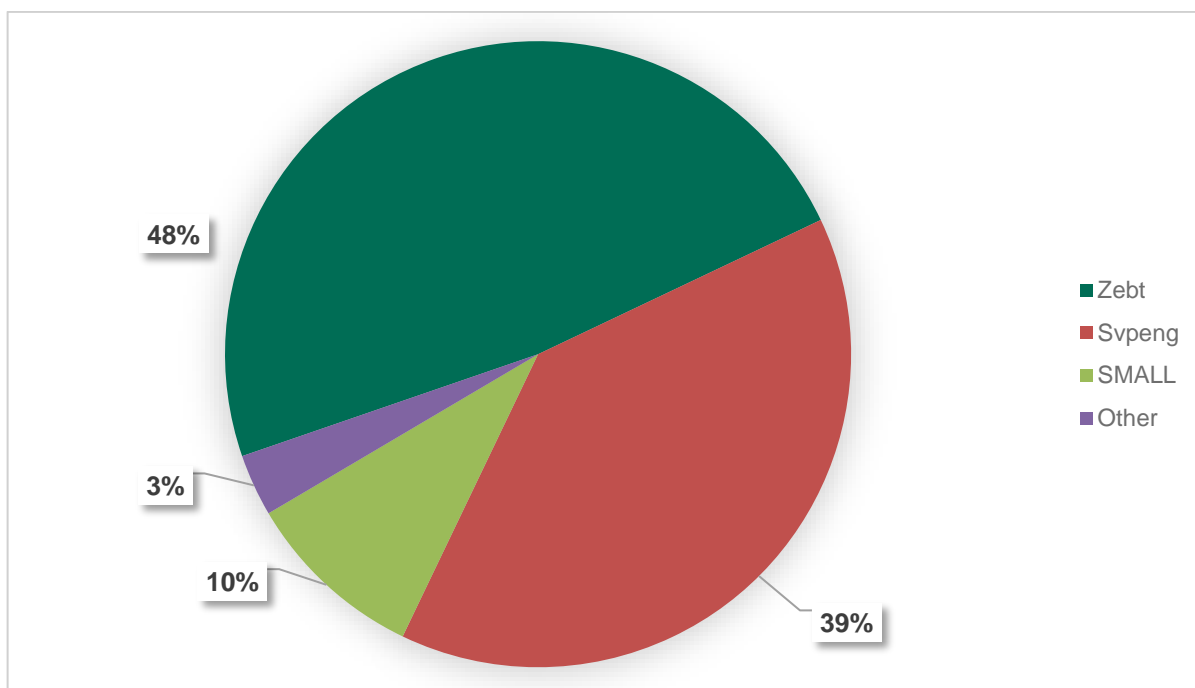


Fig. 14: The distribution of the share of attacked users between the most active mobile ransomware families in 2017-2018.

As you can see, SMALL and Svpeng continue to consolidate their dominance across the mobile ransomware landscape – the number of most active actors has decreased from four to three, while the ‘other’ section has stayed at the minimum level. The new entry is Zebt, a fairly simple Trojan whose main goal is to block a device with its window and demand a ransom. Zebt tends to attack users in Europe and Mexico and we have covered its activities [here](#) and [here](#). Zebt became the most widespread mobile ransomware in Q1 — when it was encountered by more than half of all users.

In summary, while mobile ransomware has decreased, it has also demonstrated the same trends as the year before – it has focused on wealthy countries and a few families have monopolized the market. This means that the actors behind them are disciplined, focused, and take a targeted approach to making their money.

Game changer – how cryptocurrency miners beat them all

We have discussed the status quo of ransomware in the past 12 months and found that this type of malware, and the authors behind it, are either losing interest (and are looking for new ways to make money), or they are using ransomware for other purposes (such as data destruction at important companies in a range of sectors). But if ransomware no longer wears the threat crown, what is the new king?

Cryptocurrency has become a hot topic in recent years, becoming more lucrative, and attracting more and more admirers around the world. With these credentials, cybercriminals couldn't ignore cryptocurrency – and even in the age of ransomware, most ransoms were demanded in cryptocurrency (such as anonymous and unregulated Bitcoins). It was just a matter of time before miners came on the threat scene.

Miners are a discreet and modest way to make money by exploiting users, and are a far cry from the noisy and very noticeable encryption of victim devices. Instead of the large one-off payout achieved with ransomware, cybercriminals employing mining as a tactic can benefit from an inconspicuous, stable and continuous flow of funds.

Moreover, although there are groups of people who hoodwink unwitting users into installing mining software on their computers, or who exploit software vulnerabilities to do so, mining is legal. It simply results in threat actors receiving cryptocurrency, while their victims' computer systems experience a dramatic slowdown.

In 2017 we started seeing botnets designed to profit from concealed cryptomining, and attempts to install miners on servers owned by organizations. When these attempts are successful, business processes suffer at victim companies, because data processing speeds fall substantially.

Part 1. PC miners

The number of victims is key here – the more victims you have, the more money you are able to mine at their expense. The growth in this number is something we have already seen and reported [on](#).

It is clear that the number of users that have encountered cryptocurrency miners has increased dramatically in recent years – from around 205,000 in 2013 to over 700,000 in 2014. The years that followed were marked with spikes in cryptocurrency, and the price of Bitcoin and Altcoins, for example, continuously beat records throughout 2017.

As a result, by the end of 2017, 2.7 million users had been attacked by malicious miners – this is almost 1.5 times more than in 2016 (when the figure was 1.87 million). Let's have a closer look:

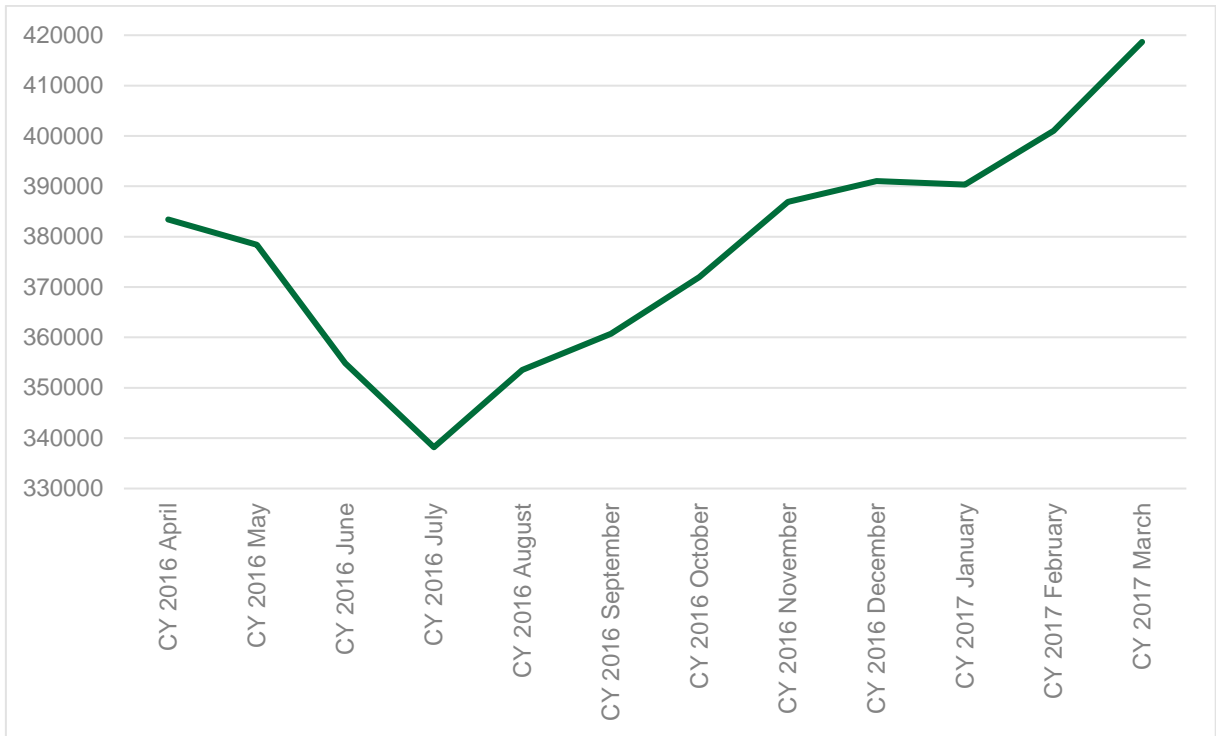


Fig. 15: The number of users encountering miners at least once in the period from April 2016 to March 2017.

The true spike in mining started in summer 2016, and the increase became more and more steady, resulting in over 400,000 hits a month, while fluctuating with cryptocurrency prices. Monero for instance, increased its price several times in approximately the same period of time.

A year later, the situation remained the same, but on steroids, with the number of hits exceeding not 400,000 but 600,000 per month.

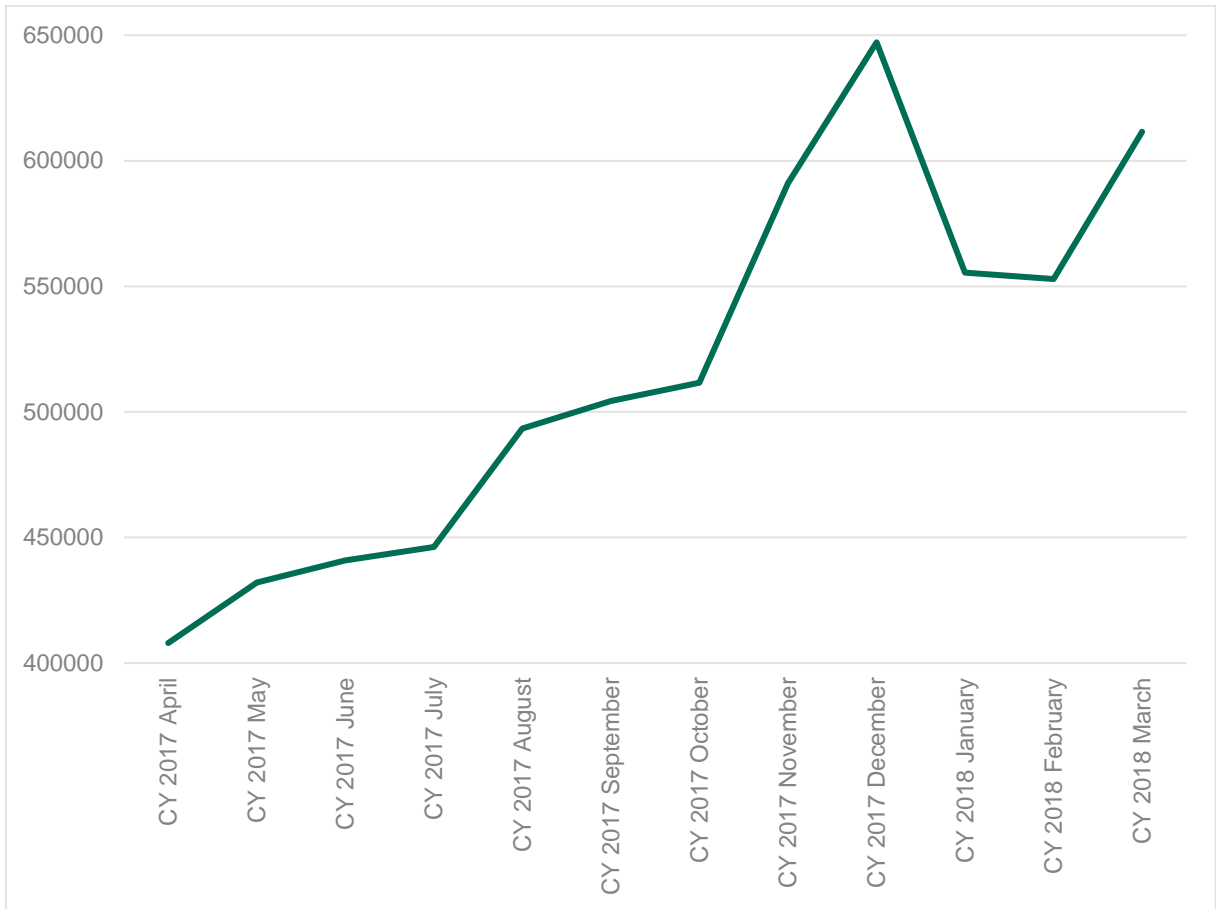


Fig. 16: The number of users encountering miners at least once in the period from April 2017 to March 2018.

The above pattern also heavily matches cryptocurrency prices – Bitcoin and Monero peaked in December, then fell, leading to a reduction in mining activities.

Let's now have a look at the other side of the battle – where users suffer from unclear data processing speeds. Let's first evaluate the 2016-2017 timeline:

Country	% of users attacked with miners out of all users encountering malware
Afghanistan	27.28%
Ethiopia	25.29%
Uzbekistan	24.57%
Tajikistan	22.34%
Zambia	20.79%
Turkmenistan	19.71%

Kazakhstan	16.36%
Mozambique	15.05%
Tanzania	12.21%
Kyrgyzstan	9.77%

Fig. 17 the list of countries with the biggest share of users (each country has more than 30,000 unique users of Kaspersky Lab products) attacked with miners as a proportion of all users attacked with any kind of malware in 2016-2017.

This list differs from the one about PC ransomware in the same period – it does not feature any developed markets. The authors behind miners tend to focus on developing markets instead, as proven by the fact that Afghanistan, Ethiopia, and Uzbekistan are in the top three.

A year later, the landscape had changed:

Country	% of users attacked with miners out of all users encountering malware
Ethiopia	31%
Afghanistan	29%
Turkmenistan	24%
Tajikistan	21%
Mozambique	19%
Uzbekistan	18%
Zambia	18%
Kazakhstan	17%
Tanzania	15%
Kyrgyzstan	12%

Fig. 18: The list of countries with the biggest share of users (each country has more than 30,000 unique users of Kaspersky Lab products) attacked with miners as a proportion of all users attacked with any kind of malware in 2017-2018.

As we can see, the changes are not significant, yet they strongly differ from the PC ransomware trends in the same period. This could be due to the fact that people from developing markets are not so eager to pay a ransom.

Comparing the evolution of the threat across these countries, in the 24-month period, can provide us with a better understanding of global mining trends.

Country	2016-2017	2017-2018	Y-to-Y change (%)
Ethiopia	14,184	18,646	Up 31.46%
Afghanistan	24,214	24,744	Up 2.19%
Turkmenistan	6,614	8,600	Up 30.03%
Tajikistan	8,345	8,335	Down 0.12%
Mozambique	13,154	15,380	Up 16.92%
Uzbekistan	23,950	21,301	Down 11.06%
Zambia	10,897	9,254	Down 15.08%
Kazakhstan	109,524	125,001	Up 14.13%
Tanzania	22,236	26,648	Up 19.84%
Kyrgyzstan	4,037	5,233	Up 29.63%

Fig. 19: The year-on-year change in the number of users attacked with miners.

We have compared the percentage of miners detected in these countries, against the number of risk tool detections (including other risks such as adware). This enables us to understand how and where cybercriminals are making their money nowadays. As we can see, the list is more or less the same:

Country	% of users attacked with riskware out of all users encountering malware
Ethiopia	57%
Afghanistan	44%
Turkmenistan	42%
Tajikistan	42%
Mozambique	35%
Uzbekistan	31%
Zambia	30%
Kazakhstan	26%
Tanzania	25%
Kyrgyzstan	21%

Fig.20: The list of countries with the biggest share of users (each country has more than 30,000 unique users of Kaspersky Lab products) attacked with risk tools as a proportion of all users attacked with any kind of malware in 2017-2018.

A comparison with riskware instead of malware shows us the same ranking, but with higher rates. While it is clear that miners belong in the riskware category; this is an interesting subject for speculation. We will return to it later in the mobile section of this report.

Part 2. Mobile miners

The number of users attacked with mobile miners has also experienced growth – but at a steadier pace, growing by **9.5%**, from **4,505** in 2016-2017 to **4,931** in 2017-2018.

Overall, the timeline for the two-year period looks like this:

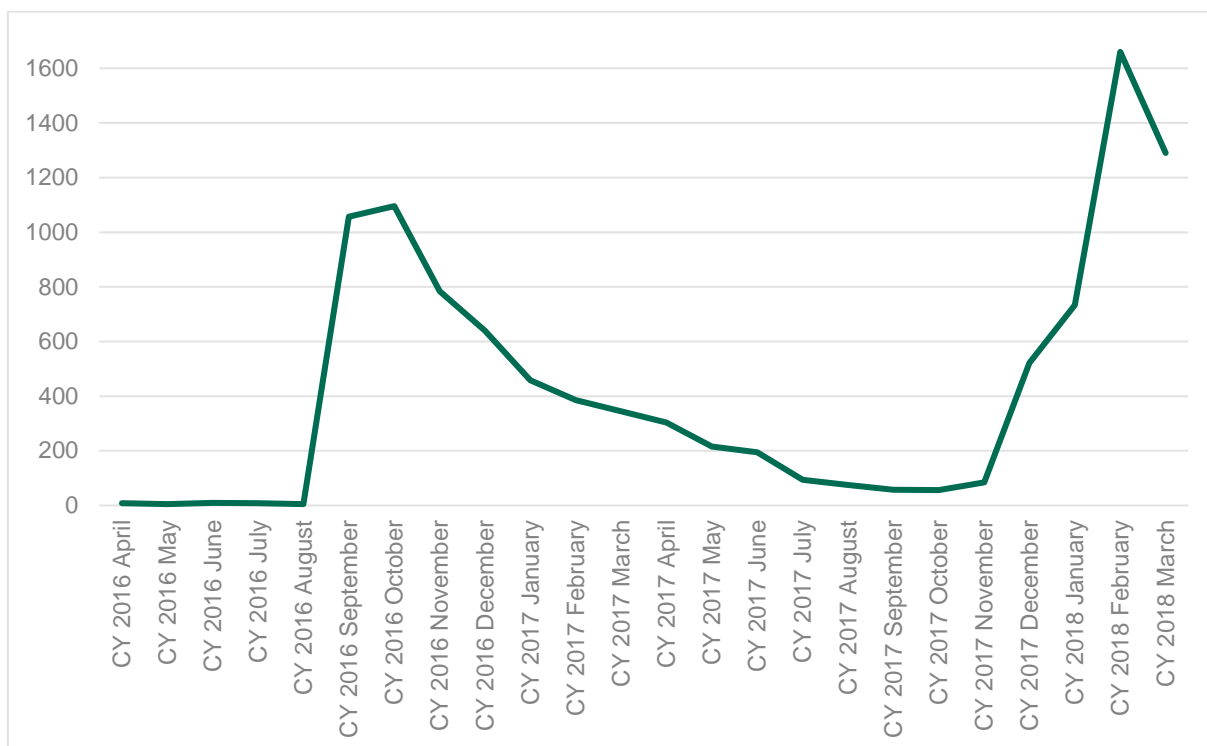


Fig. 21: The number of users encountering mobile miners at least once in the period from April 2016 to March 2018.

Like PC miners, mobile miners increased in the summer of 2016 – yet, their growth was not that steady and at a lower rate.

It is also interesting to look at the same timeline with malware and riskware.

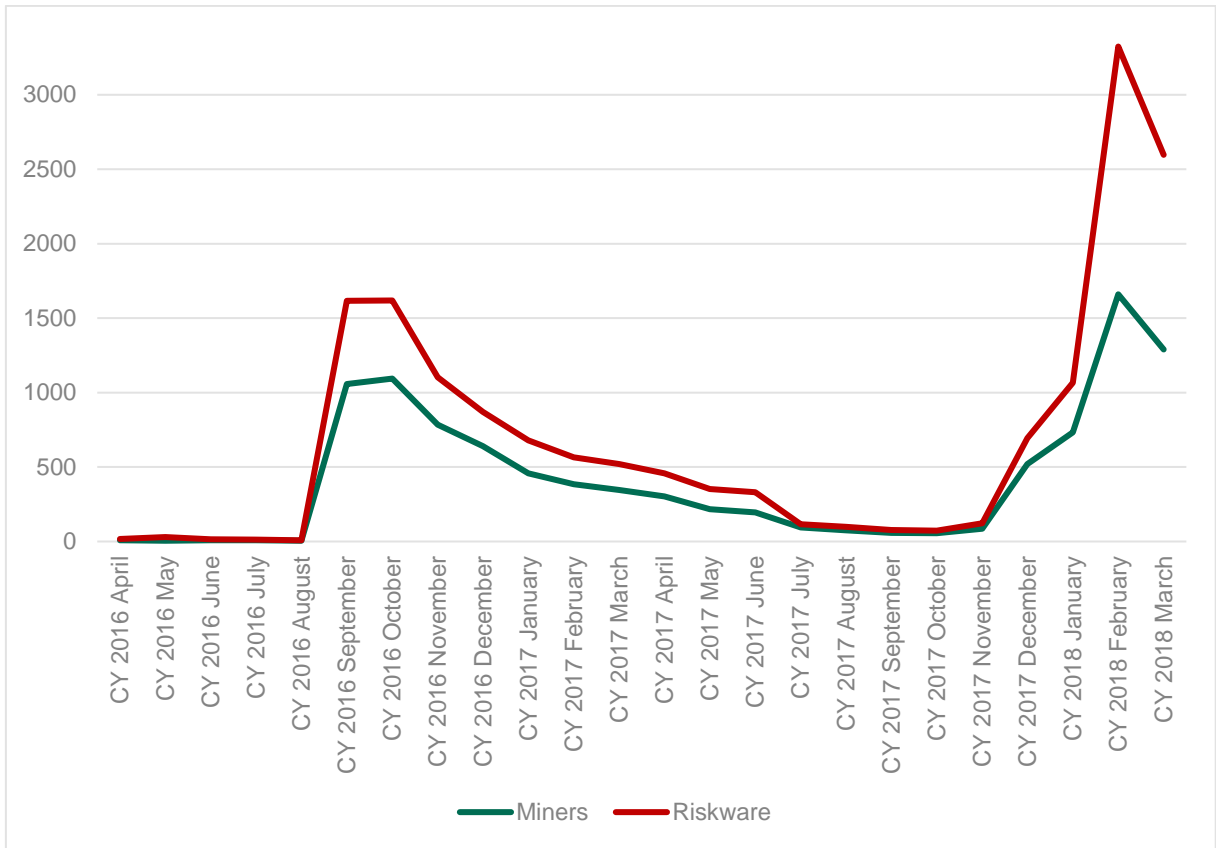


Fig. 22: The number of users encountering miners and riskware at least once in the period from April 2016 to March 2018.

As we can see, the riskware and miner patterns are almost identical. However, let's have a look at how this corresponds with malware trends – at least during the second period.

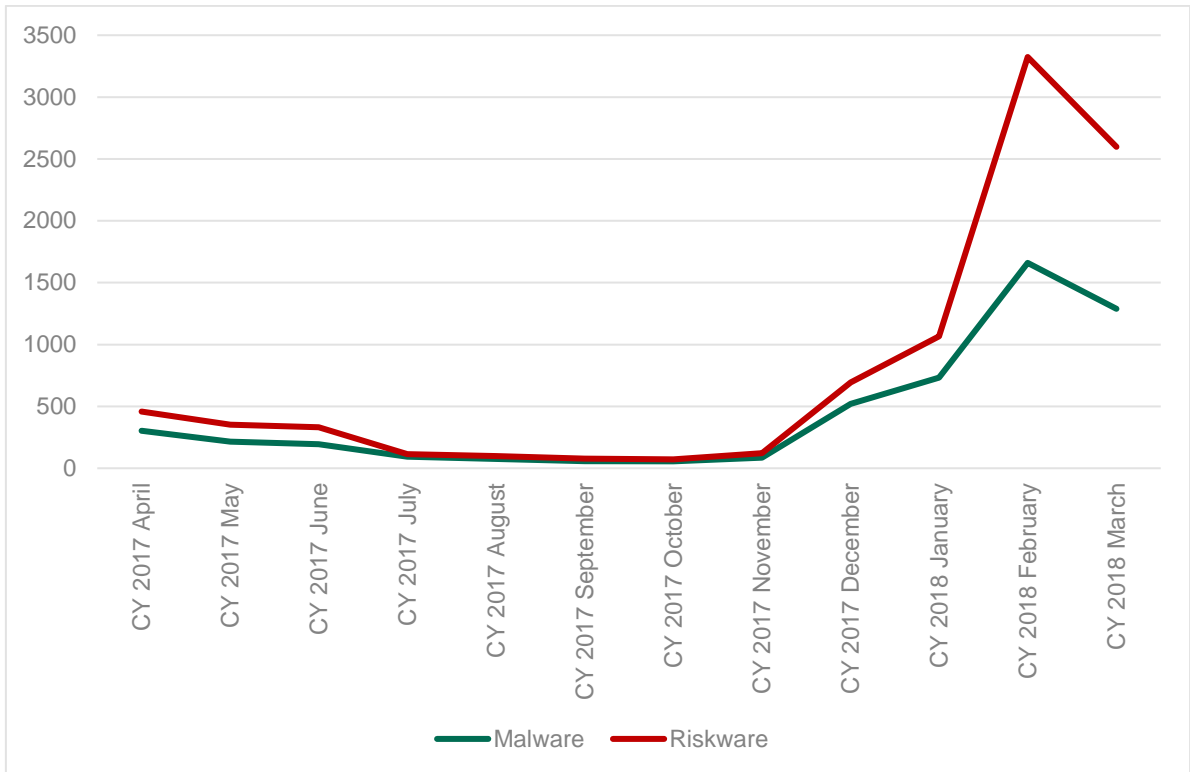


Fig. 23: The number of users encountering malware and riskware at least once in the period from April 2017 to March 2018.

They also follow the same trend. Apparently, amid the decrease in ransomware and the increase in mining, riskware is dominating malware and is now setting the rules of the game, affecting the presented timeline.

Just as with PC miners, let's have a deeper look at the geographic distribution to find out where cybercriminals are focusing their mining efforts. In 2016-2017 the list looked like this:

Country	% of users attacked with mobile miners out of all users encountering malware
Venezuela	0.14%
Myanmar	0.1%
Nepal	0.1%
Indonesia	0.09%
Philippines	0.09%
Cambodia	0.08%

Nigeria	0.08%
Kyrgyzstan	0.07%
Macedonia	0.07%
Yemen	0.07%

Fig. 24: Top 10 countries with the highest percentage of mobile users attacked with mobile miners, as a proportion of users attacked with any kind of mobile malware (each country has more than 10,000 unique users of Kaspersky Lab products for Android devices). Period: April 2016 – March 2017.

Unlike ransomware, mobile miners tend to target developing markets like Venezuela, Myanmar and Nepal, which made up the top three in 2016-2017. A year later, the pattern had not changed but the list had:

Country	% of users attacked with mobile miners out of all users encountering malware
Venezuela	0.45%
Nepal	0.31%
Turkmenistan	0.24%
China	0.16%
Bolivia	0.15%
Philippines	0.15%
Malaysia	0.09%
Pakistan	0.08%
Vietnam	0.08%
Bangladesh	0.08%
Indonesia	0.08%
Moldova	0.08%

Fig. 25: Top 10 countries with the highest percentage of mobile users attacked with mobile miners as a proportion of users attacked with any kind of mobile malware (each country has more than 10,000 unique users of Kaspersky Lab products for Android devices). Period: April 2017 – March 2018.

Venezuela again topped the ranking, followed by Nepal and Turkmenistan. While all the countries presented can be considered as developing, the size of the Chinese market, ranked fourth, is worrisome here – mainly due to the number of potential victims.

Country	2016-2017	2017-2018	Y-to-Y change %
Venezuela	44	118	Up 168.18%
Nepal	34	90	Up 164.71%
Turkmenistan	13	41	Up 215.38%
China	8	111	Up 1287.5%
Bolivia	10	33	Up 230%
Philippines	135	196	Up 45.19%
Malaysia	79	167	Up 111.39%
Pakistan	16	29	Up 81.25%
Vietnam	58	73	Up 25.86%
Bangladesh	51	79	Up 54.90%
Indonesia	303	217	Down 28.38%
Moldova	14	28	Up 100%

Fig. 26: The year-on-year change in the number of users attacked with mobile miners.

The figures above suggest that the mining threat may come from China – as this region demonstrates an increase of over 1287.5%.

Both percentages and absolute figures show us that mobile mining is an emerging threat, targeting developing countries. The reason is that cybercriminals tend to choose PCs as a target, because PCs provide much more power than a mobile device. At first glance, it may seem that mobile miners are not worth considering.

However, overall growth rates indicate that we should still monitor mobile mining carefully. Moreover, our studies show that mining capabilities are often included in the list of features of many popular malware families – as an added value, and as one more way for criminals to make money at the user’s expense. This was certainly the case with the infamous [Loapi](#) – an intriguing malware with multiple modules, which allowed for an almost endless number of malicious features - from cryptocurrency mining to DDoS attacks.

There has also been an interesting twist: tests on one randomly selected mobile phone demonstrated that Loapi malware creates such a heavy workload on an infected device that it even heats it up, and can deform its battery. Apparently, the malware’s authors didn’t really want this to happen, as they are hungry for as much money as they can get by keeping the malware running! But their lack of attention to the malware’s optimization has led to this unexpected physical ‘attack vector’ and possibly serious damage to user devices.

Part 3. Between black and white: are risk tools replacing malware?

Well, mining is now beginning to eclipse ransomware as a way for cybercriminals to make money illegally. Just like in other industries, the numbers tell the stories best. Falling off the radar, ransomware has become a rather typical infection vector once again. It has now been abandoned by commercial cybercriminals but embraced by sophisticated actors instead. It is a noisy way to make money out of victims - it attracts a lot of media and state attention. It looks like criminals increasingly think ransomware is not worth the trouble.

So how can cybercriminals make illegal money, in a discreet and stable way, and with lower risks? Apart from malware, there are a lot of ways to make money – through various risk tools, adware, and cryptocurrency mining. The numbers have proven this; let's now try to understand the particular reasons behind mining's popularity.

1) There is a simple monetization model

While victims have no obligation to actually pay a ransomware ransom, and can wait until a successful decryption tool is available, the mining model is easier and more stable – you attack your victims, build cryptocurrency using CPU or GPU power, and then earn real money through legal exchanges and transactions.

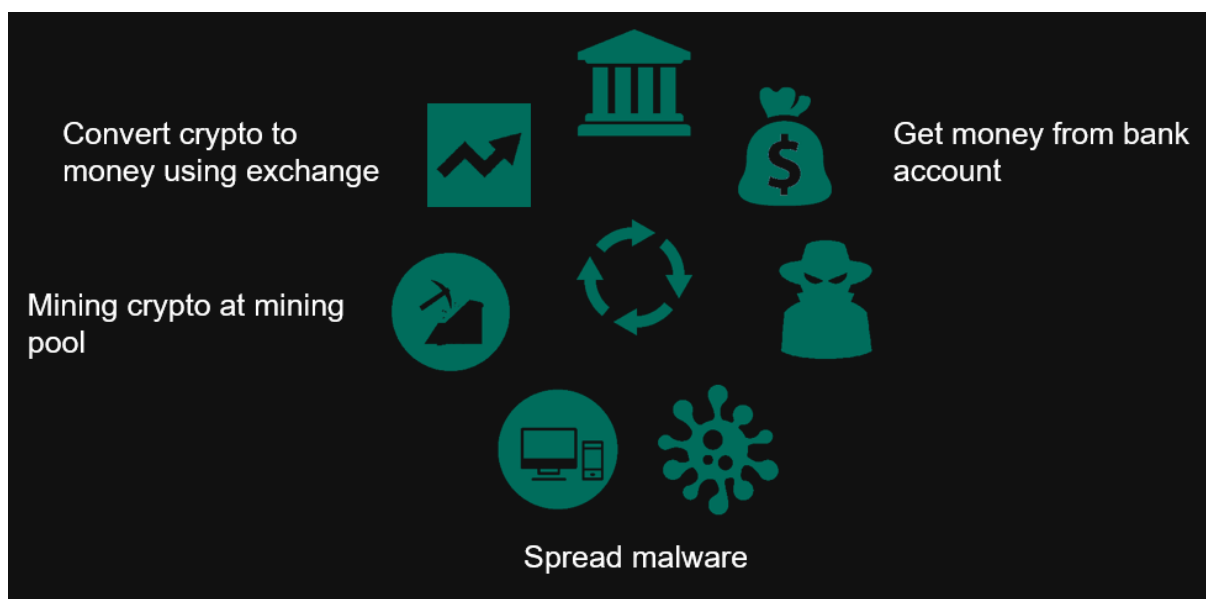
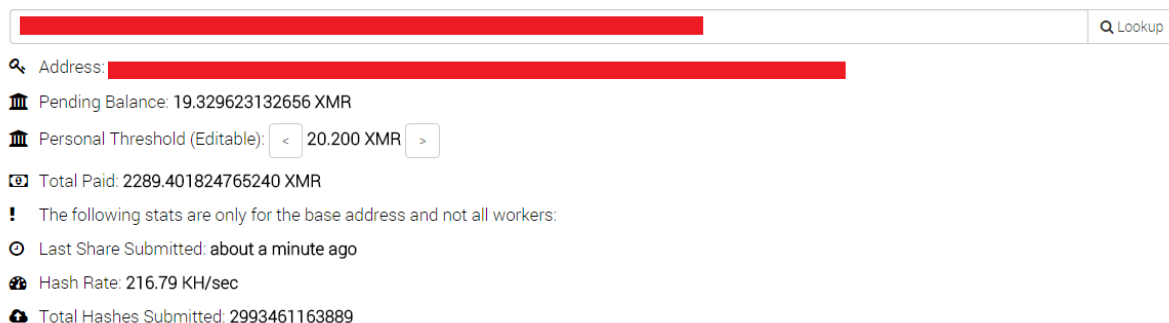


Fig. 27: The mining monetization process.

The two currencies most often used in concealed mining are monero (XMR) and zcash. These two ensure the anonymity of transactions, which is very handy for threat actors. According to the most conservative [estimates](#), the mining network can generate anything up to \$30,000 a month for its owners.

Your Stats & Payment History

Look at [worker stats](#) for hash rates and worker stats



The screenshot shows a mining wallet interface with the following details:

- Address: [Redacted]
- Pending Balance: 19.329623132656 XMR
- Personal Threshold (Editable): < 20.200 XMR >
- Total Paid: 2289.401824765240 XMR
- ! The following stats are only for the base address and not all workers:
- Last Share Submitted: about a minute ago
- Hash Rate: 216.79 KH/sec
- Total Hashes Submitted: 2993461163889

Fig. 28: The wallet of a mining botnet.

2) Its discreet nature

Again, unlike with ransomware, it is very hard for anybody to understand if they have been infected by miners or not, due to their specific nature and operating principles. Most people seldom use most of their computer's processing power; and miners harness the 70 to 80 percent that is not being used for anything else. Moreover, some miners have special functions to reduce mining capacities or to cancel the process if another resource-demanding program (for example, a videogame) is launched.

Often, a crypto-miner comes with extra services to maintain its presence within the system, such as automatically launching every time the computer is switched on, and operating without the user's knowledge.

These services can, for example:

- Try to turn off security software;
- Track all application launches, and suspend their own activities if a program is started that monitors system activities or running processes;
- Ensure a copy of the mining software is always present on the hard drive, and restore it if it is deleted.

3) It is now very easy to make your own miner

Those interested can get everything that they need:

- Ready to use partner programs
- Open mining pools
- Multiple miner-builders

As a result, crypto-miners are installed – on the computers of consumers and businesses alike – alongside adware, cracked games, and pirated content. It's becoming easy for cybercriminals to create miners, because of ready to use partner programs, open mining pools and miner-builders. Another method is web mining, where cybercriminals insert a

script into a compromised website that mines cryptocurrencies while the victim browses the site. Some other criminal groups are more selective, using exploits to install miners on the servers of large companies, rather than trying to infect lots of individuals. Some of the ways cybercriminals install malicious miners in the networks of their corporate victims are very sophisticated, resembling the methods of APT attackers.

Like ransomware did [some time ago](#), miner authors could also shift to targeted attacks to make more money. It will be interesting to see if this happens.

PS. Stay alert to miners' propagation methods

Last but not least, it is worth discussing the propagation methods of miners. The main way miners spread is via social engineering.

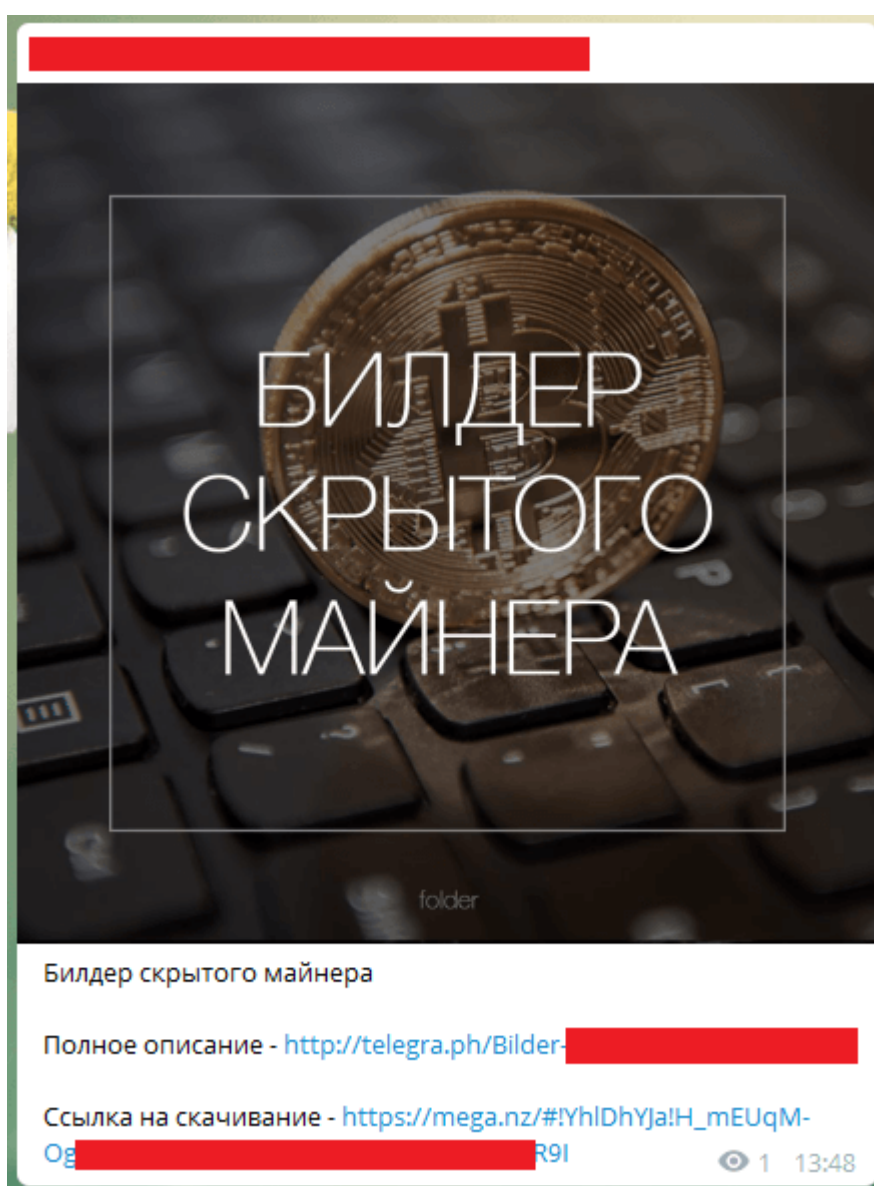


Fig. 29: Advert for a mining builder in a telegram channel advertising opportunities to earn money online.

Usually, threat actors collaborate with potentially unwanted application partner programs (PUA) to spread miners. However, some small criminal groups try to spread malware by using different social engineering tricks, such as fake lotteries, etc. In these cases, potential victims need to download a random number generator from a file-sharing service, and run this on their PC to participate. It is a simple trick, but a very productive one.

Another popular method is web-mining through a special script executed in the victim's browser. For example, in 2017 our security solutions [stopped](#) the launch of web miners on more than 70 million occasions. The most popular script used by cybercriminals is Coinhive, and most cases of its use in the wild are websites with a lot of traffic. The longer the user session on those sites, the more money the site's owner earned from mining. Major incidents involving Coinhive include hacked web pages, such as the Pirate Bay case, [YouTube ads](#) or the [UFC fight pass](#) mining incident. However, other examples of its legal use are also known.

There are other groups, which do not need to spread miners to many people. Instead, their targets are powerful servers in big companies. For instance, [Wannamine](#) spread in internal networks using an EternalBlue exploit, and earned nine thousand Monero this way (approx. two million dollars). However, the first miner that used the EternalBlue exploit was [Adylkuzz](#). In previous [research](#) we have also described another miner family – Winder – that has used an extra service to restore a miner when it was being deleted by an AV product. This botnet earned half a million dollars.

Conclusions and predictions

This report confirms what we [predicted](#) earlier:

Ransomware

While ransomware activities are falling across the globe, they still pose a threat, and should be treated as such. PC ransomware is used in powerful, sophisticated, and destructive attacks. 2017 was, after all, a tough year in terms of destructive attacks. The ExPetr/NotPetya attack, which was initially considered to be ransomware, turned out to be a cleverly camouflaged wiper as well. ExPetr was followed by other waves of 'ransomware' attacks, in which there was little chance for the victims to recover their data; as the threats were all cleverly masked 'wipers as ransomware'. We don't think this trend will change anytime soon.

Actors behind mobile ransomware are, at the same time, still targeting wealthy nations and are capitalizing on the markets of their choice. In parallel, they have increased consolidation – with a few actors now dominating the market. This trend has been witnessed for two years in a row, and we expect it will continue.

Miners

As discussed, while ransomware has provided a potentially large but one-off income for its cybercriminals, miners will provide a lower, but longer lasting one. Last year we asked what tips the scales for cybercriminals? Today, this is no longer a question. Miners will keep spreading across the globe, attracting more people.

It is highly likely that the additional growth of mining will come at the expense of mobile miners. For now, they are growing, but at a very steady pace. However, once criminals find a technological solution that makes the profits from mining on mobile devices equivalent to those from mining on PCs, mobile mining will quickly become equal. Particularly worrying here is that some of the criminals' key target geographies – China and India – [account](#) for around a third of all smartphones in the world. The population of these countries will therefore be particularly vulnerable if smartphone mining really takes off.

The number of targeted attacks on businesses, for the purpose of installing miners, raises questions about whether mining might eventually follow in the footsteps of ransomware actors. Big money loves silence, and if miner actors attract as much attention to themselves as ransomware did, life will get complicated for them.

Fighting back

Standing up to ransomware and miners – how to stay safe

1. Treat email attachments, or messages from people you don't know, with caution. If in doubt, don't open it.
2. Back up data regularly.
3. Always keep software updated on all the devices you use. To prevent miners and ransomware from exploiting vulnerabilities, use tools that can automatically detect vulnerabilities and download and install patches.
4. For personal devices, use a reliable consumer security solution and remember to keep key features – such as System Watcher – switched on.
5. If you're a business, enhance your preferred third party security solution with Kaspersky Lab's **free anti-ransomware tool** (see below for more information).
6. For superior protection use an endpoint security solution that is powered by behavior detection and able to roll back malicious actions.
7. Carry out regular [security audits of your corporate network](#) for anomalies.
8. Don't overlook less obvious targets, such as queue management systems, POS terminals, and even vending machines. As the miner that relied on the EternalBlue exploit shows, such equipment can also be hijacked to mine cryptocurrency.
9. Use application control to track malicious activity in legitimate applications. Specialized devices should be in Default Deny mode. Use dedicated security solution, such as [Kaspersky Endpoint Security for Business](#) that includes these functions.
10. To protect the corporate environment, educate your employees and IT teams, keep sensitive data separate, restrict access, and always back up everything.
11. Last, but not least, remember that ransomware is a criminal offence. You shouldn't pay. If you become a victim, report it to your local law enforcement agency.

Improve your protection level for free

Kaspersky Lab has recently launched a new version of its free [Kaspersky Anti-Ransomware Tool](#). The solution is designed to protect your business data from ransomware encryption and cryptominers that may be unknowingly downloaded and run on PCs in real-time. It works alongside your current vendor's security applications, to detect and block existing, new and unknown malware. By using the latest behavioral detection technologies, the tool can significantly boost your overall protection levels, keeping you safe from all ransomware threats. To see how it can strengthen your defenses, [install](#) it now.