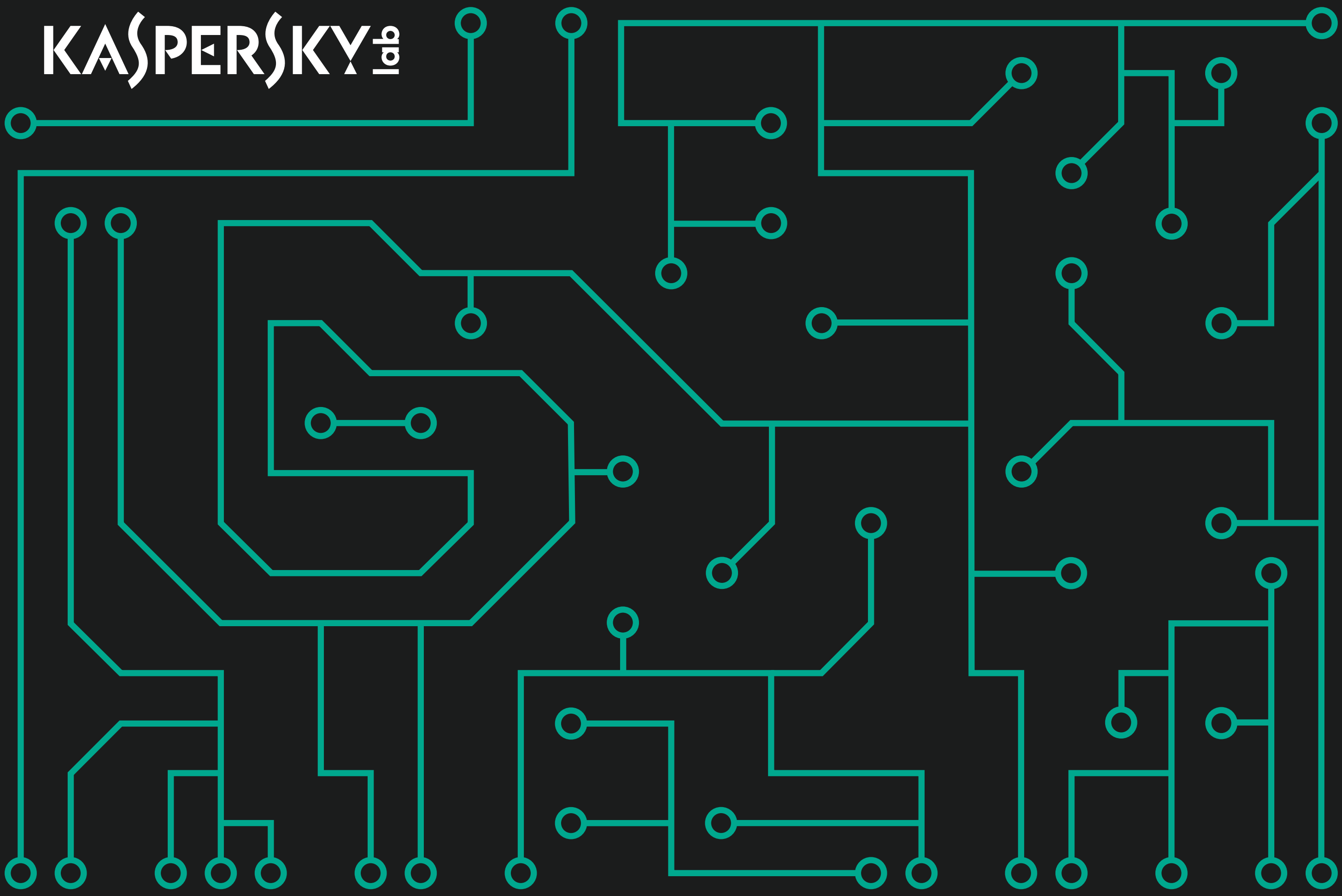
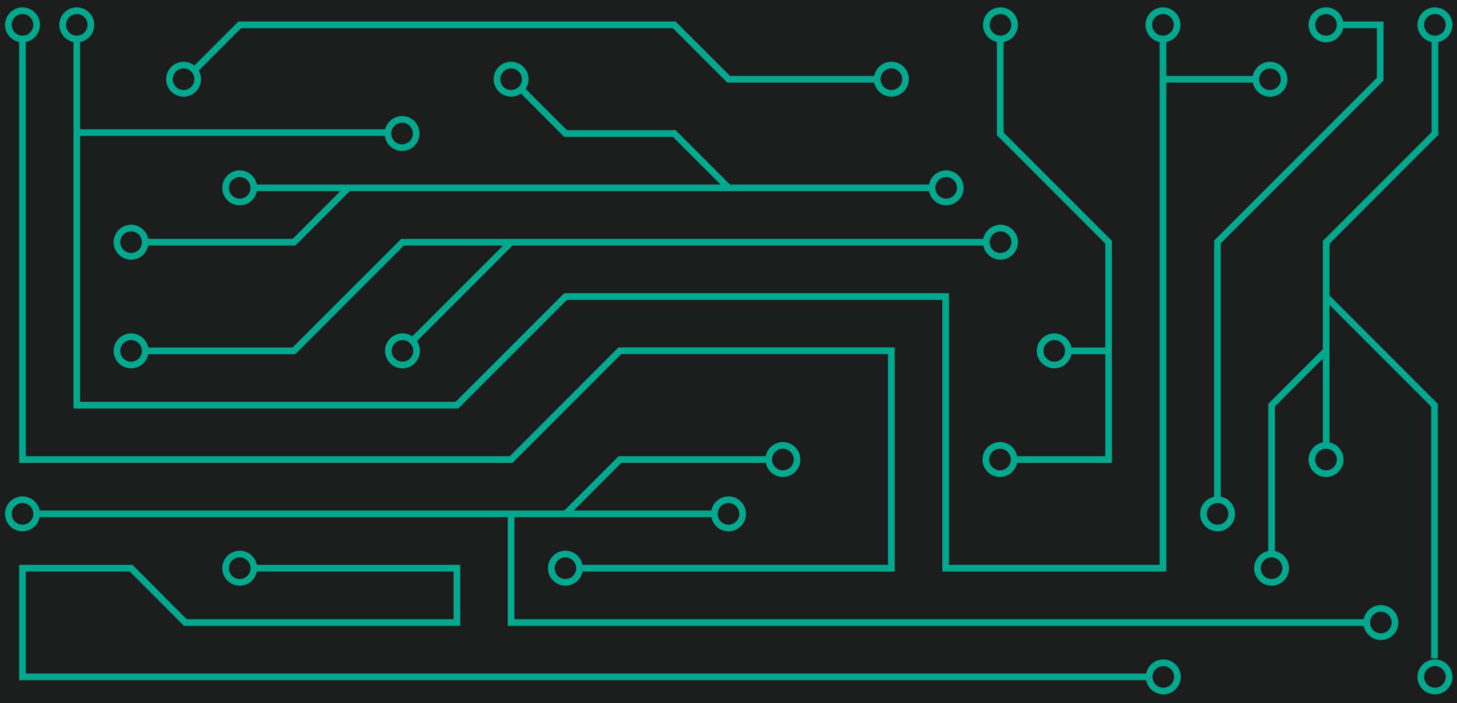


Kaspersky Security Bulletin 2018

STORY OF THE YEAR: MINERS



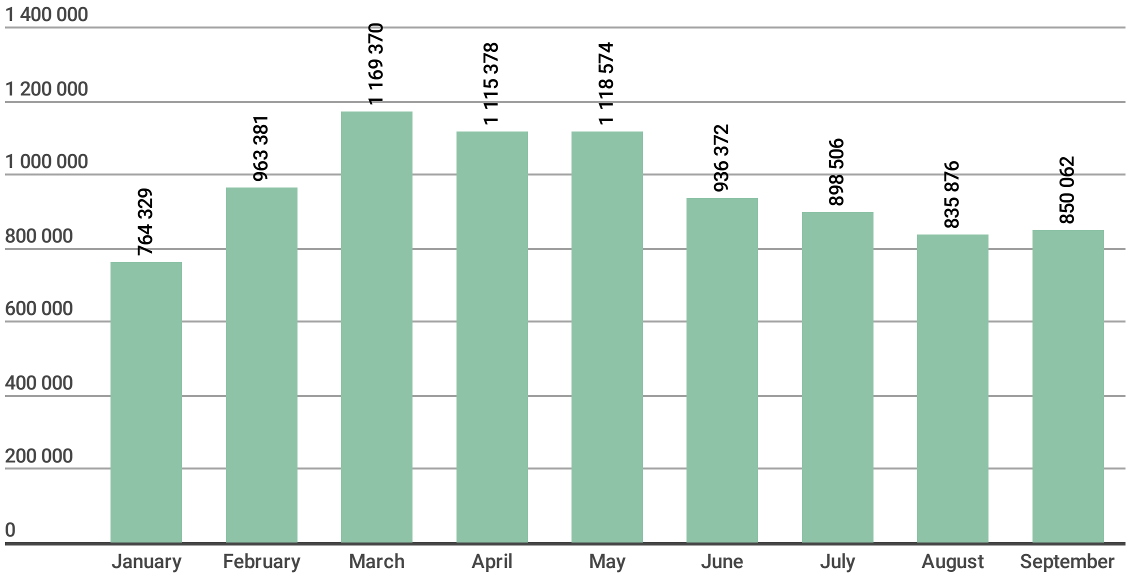
CONTENTS

Cryptocurrency miners that infect the computers of unsuspecting users essentially operate according to the same business model as ransomware programs: the victim's computing power is harnessed to enrich the cybercriminals. Only in the case of miners, it might be quite a while before the user notices that 70–80% of their CPU or graphics card power is being used to generate virtual coins. Encrypted documents and ransomware messages are far harder to miss.

Cryptominers usually find their way onto user computers and corporate machines along with adware, hacked games, and other pirated content. What's more, the present "entry threshold" — that is, the actual process of creating a miner — is rather low: cybercriminals are assisted by ready-to-use affiliate programs, open mining pools, and miner builders. If that weren't enough, there is another way to steal computing resources through a webpage-embedded mining script that starts when the user opens the site in a browser. A separate category of cybercriminals are those who target not private computers, but the servers of large companies, for which the infection process is considerably more resource-intense.

TRENDS

2018 began with a rise in the number of miner-related attacks. However, after a drop in the value of the main cryptocurrencies, which lasted from January to February, infection activity noticeably declined. General interest in cryptocurrencies also waned. Yet the graph clearly shows that while the number of cryptominer attacks decreased, the threat is still current. As for how the November collapse in the Bitcoin exchange rate will affect the number of infections, time will tell.



Number of unique users attacked by miners in Q1–Q3 2018

Hidden mining software was very popular among botnet owners, as confirmed by our statistics on files downloaded by zombie networks: Q1 2018 saw a boom in cryptominers, and the share of this malware in the first half of the year was 4.6% of the total number of files downloaded by botnets. For comparison, in Q2 2017 this figure was 2.9%. It follows from the data that cybercriminals have come to view botnets as a means of spreading software for mining cryptocurrencies.

	H2 2017		H1 2018	
1	Lethic	17.0%	njRAT	5.2%
2	Neutrino.POS	4.6%	Lethic	5.0%
3	njRAT	3.7%	Khalesi	4.9%

4	Emotet	3.5%	Miners	4.6%
5	Miners	2.9%	Neutrino.POS	2.2%
6	Smoke	1.8%	Edur	1.3%
7	Cutwail	0.7%	PassView	1.3%
8	Ransomware	0.7%	Jimmy	1.1%
9	SpyEye	0.5%	Gandcrab	1.1%
10	Snojan	0.3%	Cutwail	1.1%

Most downloaded threats, H2 2017–H1 2018

Still on the topic of botnets, it is impossible not to mention that in Q3 2018 we registered a decline in the number of DDoS attacks, the most likely reason being, according to our experts, the "reprofiling" of botnets from DDoS attacks to cryptocurrency mining. This was induced not only by the high popularity of cryptocurrencies, but also the high competition in the "DDoS market", which made the attacks less expensive for clients, but not for the botnetters themselves, who still have to cope with more than a few less-than-legal "organizational issues."

Mining differs favorably for cybercriminals in that, if executed properly, it can be impossible for the owner of an infected machine to detect, and thus the chances of encountering the cyberpolice are far lower. And the reprofiling of existing server capacity completely hides its owner from the eyes of the law. Evidence suggests that the owners of many well-known botnets have switched their attack vector toward mining. For example, the DDoS activity of the Yoyo botnet dropped dramatically, although there is no data about it being dismantled.

Moreover, mining has started to command as much (or more) attention as ransomware: this year we encountered several examples of reprofiled malware with added functionality for cryptocurrency mining. And the techniques used by the creators of miners have become more sophisticated.

For instance, an interesting miner implementation, which we dubbed PowerGhost, caught our eye in July this year. The malware can stealthily establish itself in the system and spread inside large corporate networks, infecting workstations and servers alike. To go unnoticed by users and security solutions for as long as possible, the miner employs various fileless techniques. Infection occurs remotely using exploits or remote management tools (Windows Management Instrumentation), and involves running a single-line powershell script that downloads the main body of the malware and immediately starts it without writing to the hard drive.

Another example of reprofiling is the ransomware Trojan Trojan-Ransom.Win32.Rakhni, the first samples of which were detected by Kaspersky Lab back in 2013. Its mining functions are a 2018 innovation. At the same time, their activation depends on whether the folder %AppData%\Bitcoin is present on the infected machine. If it exists, the loader downloads the ransomware. If there is no such folder and, in addition, the computer has more than two logical processors, a miner is downloaded. To keep the malware hidden in the system, the developers made it look like an Adobe product. This can be seen by the icon and the name of the executable file, as well as the fake digital signature, which uses Adobe Systems Incorporated as the company name.

Another piece of malware that has learned how to seed computers with mining utilities is the previously adware-only PBot. The malware spreads through affiliate sites that inject scripts into their pages for redirecting users to sponsored links. The standard distribution scheme looks as follows:

1. The user visits one of the sites in the affiliate network.
2. Clicking anywhere on the page causes a new browser window to appear, where an intermediate link opens.
3. The link directs the user to the PBot download page, which is tasked with downloading and running the malware by deceptive means.

The most common coin among all illegally mined cryptocurrencies is Monero (xmr). This is due to its anonymous algorithm, relatively high market value, and ease of sale, since it is accepted by most major cryptocurrency exchanges. For botnets mining this coin illegally, it is important that CPU resources can be utilized. By some accounts, a total of $175 million has been mined illegally, representing around 5% of all Monero currently in circulation.

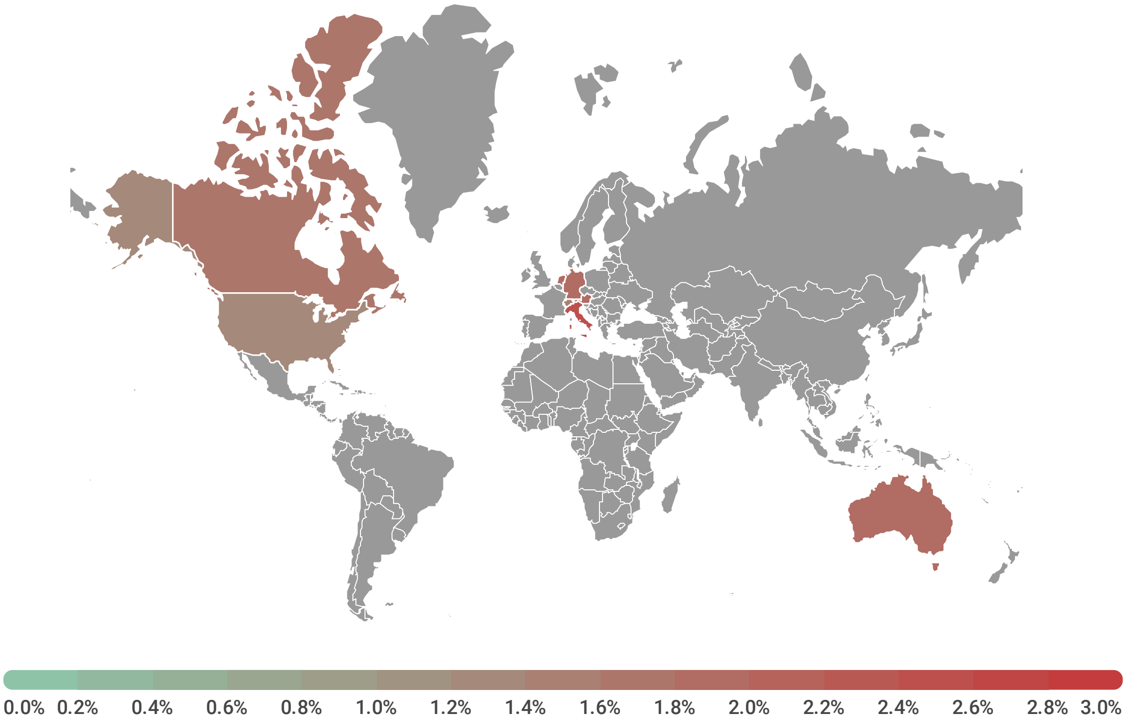
FACTORS AFFECTING THE DISTRIBUTION OF MINERS

The conclusion based on data we obtained from various sources is that legislative control over cryptocurrencies has little impact on the spread of hidden mining. For example, in Algeria and Vietnam cryptocurrencies are either prohibited or severely restricted under domestic law. Yet Vietnam is third in the ranking of leading countries by number of miner attacks, and Algeria is sixth. Meanwhile, Iran, which is presently drafting legislation to govern cryptocurrency and developing plans to issue its own "coins," is in seventh place.

Country	Cryptocurrency status	% of attacks
Kazakhstan	Not prohibited, Not legalized	16.75%
Vietnam	Issuance (mining) prohibited	13.00%
Indonesia	Recognized as an exchange commodity	12.87%
Ukraine	Circulation governed by law	11.19%
Russia	Legislation under consideration	10.71%
Algeria	Prohibited	9.03%
Iran	Legislation in preparation, creation of own cryptocurrency planned	7.21%
India	Ban under consideration, hearings in progress	7.20%
Thailand	Circulation governed by law	6.76%
Taiwan	Not prohibited	5.81%

Top 10 countries by share of miner attacks, January–October 2018 (includes only countries with more than 500,000 Kaspersky Lab clients)

At the other end of the scale, US users were the least affected by cryptominters (1.33% of the total number of attacks), followed by users in Switzerland (1.56%) and Britain (1.66%).



Map representing countries with the lowest share of miner attacks, January–October 2018 (includes only countries with more than 500,000 Kaspersky Lab clients)

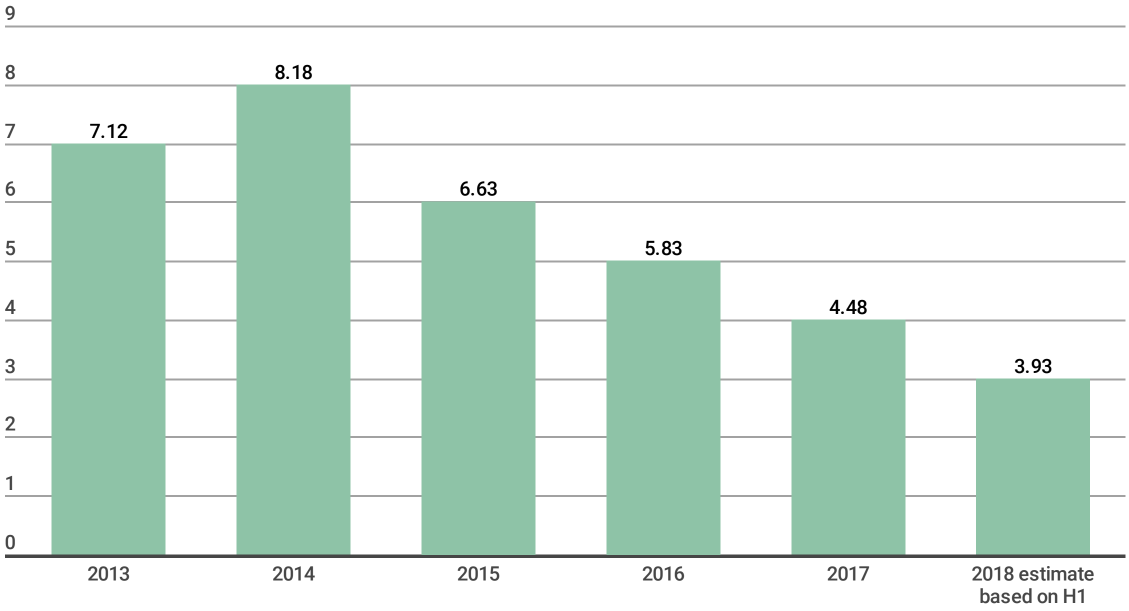
The prevalence of miners is not impacted by the cost of electricity, which varies greatly from country to country. Again, this factor is not a consideration for cybercriminals as they exploit third-party resources.

DISTRIBUTION METHODS

Looking at the distribution of pirated software in countries with the highest number of miner attacks, one sees a clear correlation: the more freely unlicensed software is distributed, the more miners there are. This is confirmed by our statistics, which indicates that miners most often land on victim computers together with pirated software.

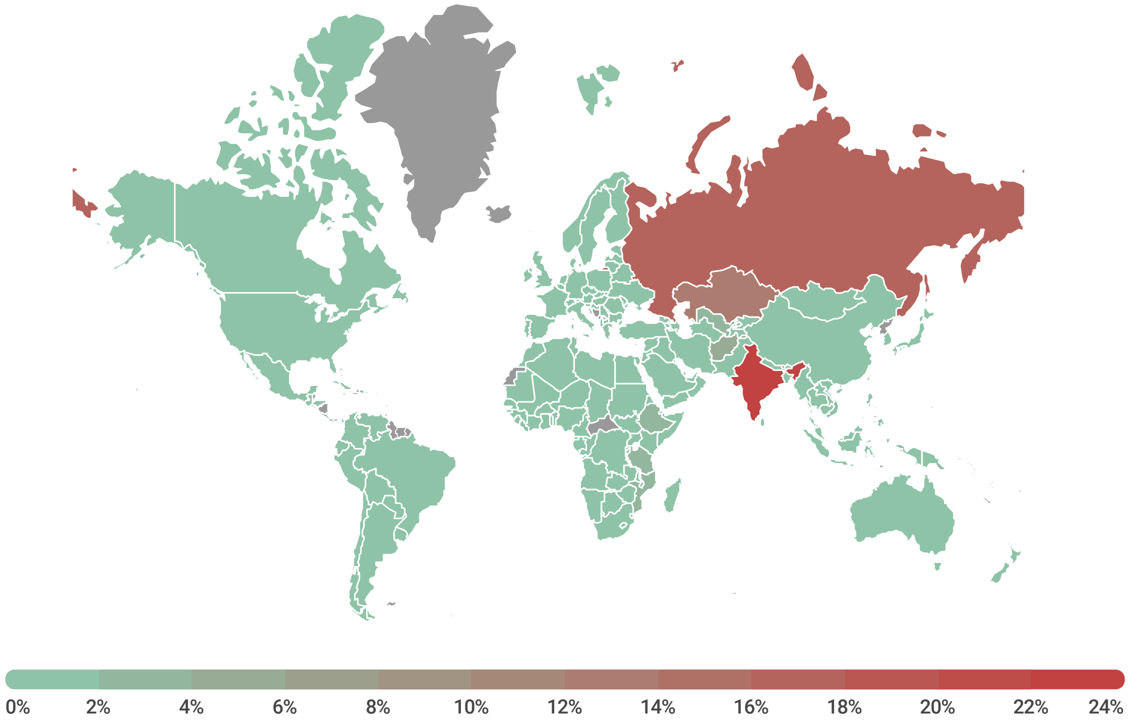
Another penetration vector for miners is adware installers distributed using social engineering. More sophisticated options (for example, propagation through vulnerabilities such as EternalBlue) are aimed at server capacities and are less frequently encountered.

And it should not be forgotten that USB drives have been used to distribute cryptocurrency mining software since at least 2015. The percentage of detections of the popular Bitcoin miner Trojan.Win64.Miner.all on removable devices is growing annually by about one-sixth. In 2018, one in ten users affected by malware transmitted through flash drives was the victim of this particular miner (roughly 9.22%; for comparison, in 2017 it was 6.7%, and in 2016 4.2%).



Millions of unique users found to have malware in the root directory, which is the main sign of infection via removable drives, 2013–2018. Source: KSN.

Trojan.Win32.Miner.ays/Trojan.Win.64.Miner.all was detected in India (23.7%), Russia (18.45%), and Kazakhstan (14.38%), but some cases were also logged in Asia, Africa, and Europe (Britain, Germany, the Netherlands, Switzerland, Spain, Belgium, Austria, Italy, Denmark, Sweden), as well as the US, Canada, and Japan.



Share of users impacted by Bitcoin miners on removable drives, 2018. Source: KSN (includes only countries with more than 10,000 Kaspersky Lab clients)

CONCLUSION

Summing up the past year, we can highlight the following bullet points:

1. Given the growing value and popularity of cryptocurrencies, cybercriminals are investing resources in the development of new mining technologies, which, according to our data, are gradually replacing ransomware Trojans.
2. Hidden mining activity declines when cryptocurrency prices fall.
3. The spread of hidden mining is not impacted by factors such as domestic legislative control or cost of electricity.
4. Miners often get on victims' computers during the download of unlicensed content or installation of pirated software. As a consequence, this type of threat is most prevalent in countries with poor regulation of the unlicensed software market, as well a low level of overall digital literacy among users.