KASPERSKY lab THE POWER OF PROTECTION

KSN Report: Ransomware in 2016-2017

www.kaspersky.com

Contents

Executive summary and main findings

Ransomware is a type of malware that, upon infecting a device, blocks access to it or to some or all of the information stored on it. In order to unlock either the device or the data, the user is required to pay a ransom, usually in bitcoins or another widely used e-currency.

The term ransomware covers mainly two types of malware: so-called Windows blockers (they block the OS or browser with a pop-up window) and encryption ransomware. The term also includes select groups of Trojan-Downloaders, namely those that tend to download encryption ransomware upon infection of a PC.

This report covers the evolution of the threat from April 2016 to March 2017 and compares it with the period of April 2015 to March 2016.

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 at least once in a given period, as well as research into the ransomware threat landscape by Kaspersky Lab experts.

Main findings:

- The total number of users who encountered ransomware between April 2016 and March 2017 rose by **11.4%** compared to the previous 12 months (April 2015 to March 2016) – from **2,315,931** to **2,581,026** users around the world;
- The proportion of users who encountered ransomware at least once out of the total number of users who encountered malware fell by almost **0.8 percentage points**, from **4.34%** in 2015-2016 to **3.88%** in 2016-2017;
- Among those who encountered ransomware, the proportion who encountered cryptors rose by **13.6 percentage points**, from **31%** in 2015-2016 to **44.6%** in 2016-2017;
- The number of users attacked with cryptors rose almost **twice**, from **718,536** in 2015-2016 to **1,152,299** in 2016-2017;
- The number of users attacked with mobile ransomware fell by **4.62%** from **136,532** users in 2015-2016 to **130,232**.

Introduction: A brief look at ransomware evolution over a year

The rise of Ransomware-as-a-Service

In May 2016 Kaspersky Lab discovered Petya ransomware that not only encrypts data stored on a computer, but also overwrites the hard disk drive's master boot record (MBR), leaving infected computers unable to boot into the operating system.

The malware is a notable example of the Ransomware-as-a-Service model, when ransomware creators offer their malicious product ‘on demand’, spreading it by multiple distributors and getting a cut of the profits. In order to get their part of the profit, the Petya authors inserted certain “protection mechanisms” into their malware that do not allow the unauthorized use of Petya samples.

While Ransomware-as-a-Service is not a new trend, this propagation model continues to develop, with more and more ransomware creators offering their malicious product. This approach has proved immensely appealing to criminals who lack the skills, resources or inclination to develop their own malware.

Notable examples of ransomware that appeared in 2016 and used this model were Petya/Mischa and Shark ransomware, which was later rebranded under the name Atom.

The growth of targeted attacks

In early 2017, Kaspersky Lab’s researchers have discovered an emerging and dangerous trend: more and more cybercriminals are turning their attention from attacks against private users to targeted ransomware attacks against businesses.

The attacks are primarily focused on financial organizations worldwide. Kaspersky Lab’s experts have encountered cases where payment demands amounted to over half a million dollars.

The trend is alarming as ransomware actors start their crusade for new and more profitable victims. There are many more potential ransomware targets in the wild, with attacks resulting in even more disastrous consequences.

The analysis in this report attempts to assess the scale of the problem, and to highlight possible reasons for the new angles of ransomware developments globally.

Part 1. PC ransomware: ransomware – conveyor of targets

The numbers for the observed period show that ransomware is still on the rise – albeit at a slower growth rate. The total number of users who encountered ransomware over the12 month period from April 2016 to March 2017 grew by **11.4%** in comparison to the previous year: April 2015 to March 2016 – from **2,315,931** to **2,581,026** users around the world. This is a weaker pace compared with **17.7%** increase in the previous period.

The proportion of users who encountered ransomware at least once out of the total number of users who encountered malware fell by almost 0.5 percentage points, from **4.34%** in 2015-2016 to **3.88%** in 2016-2017.

The following graphs illustrate the change in the number of users encountering ransomware at least once in the 24-month period covered by the report. As can be seen in Fig. 1, the volume of ransomware attacks has been rather sporadic, rising and falling with two peaks in October 2015 and March 2016. These periods were marked with Locky ransomware activities.

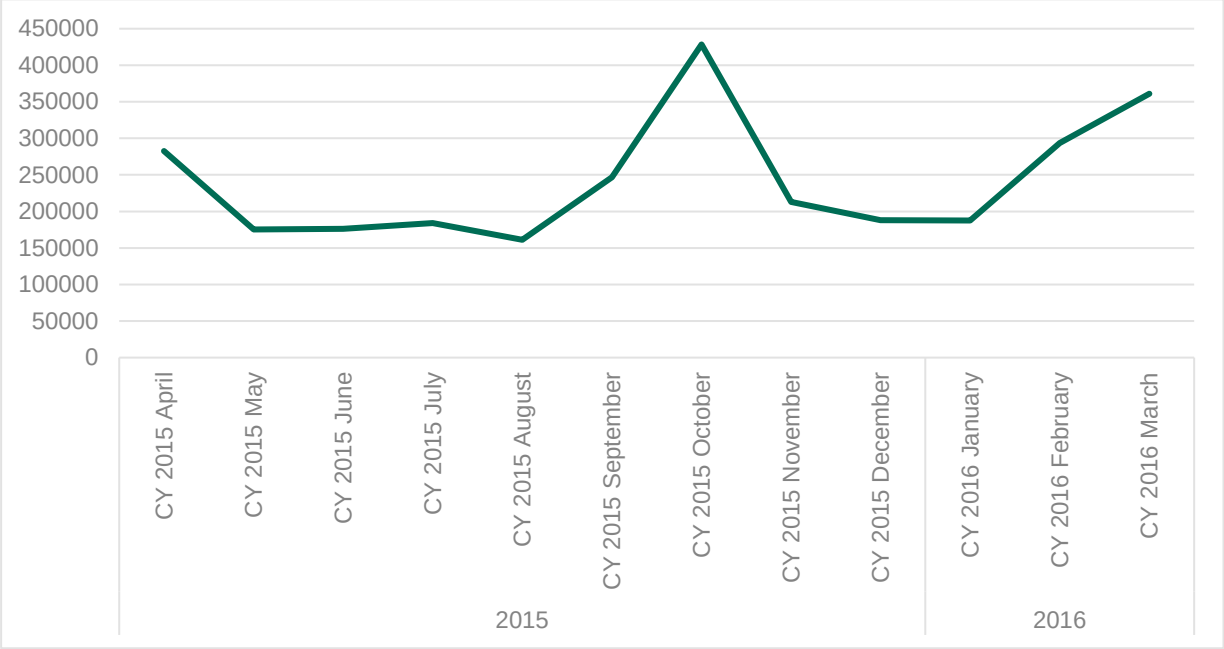


Fig. 1: The number of users encountering ransomware at least once in the period from April 2015 to March 2016

The following year, the situation looks slightly different – yet still filled with anxiety. Between April 2016-March 2017 the volume of ransomware attacks remained stable, at 20,000-25,000 hits per month on average. This is higher than in the previous period and could indicate an alarming trend – a shift from chaotic and sporadic actors' attempts to gain a foothold in the threat landscape to steadier and higher volumes. Also of interest was the peak between June and July. During these months there were many detections of the Onion ransomware family.

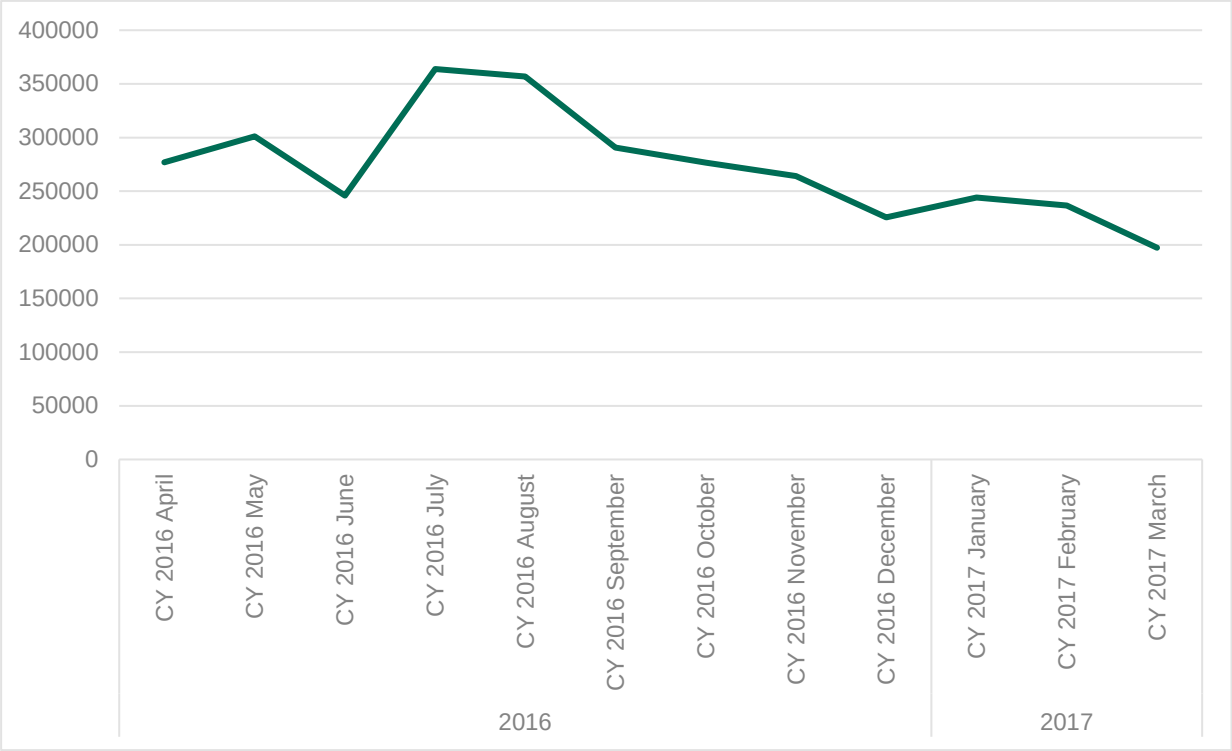


Fig. 2: The number of users encountering ransomware at least once in the period from April 2016 to March 2017

However, two things may be considered positive. Firstly, the modest growth rate could be a sign of success for the collaborative retaliation from vendors of security solutions, various law enforcement agencies, and other actors. It could also be due to increasing threat awareness, fueled by global media coverage on the most prominent fraudulent campaigns. Secondly, the end-of-the-year status also changed, from a rise in March 2016 to a fall of March 2017.

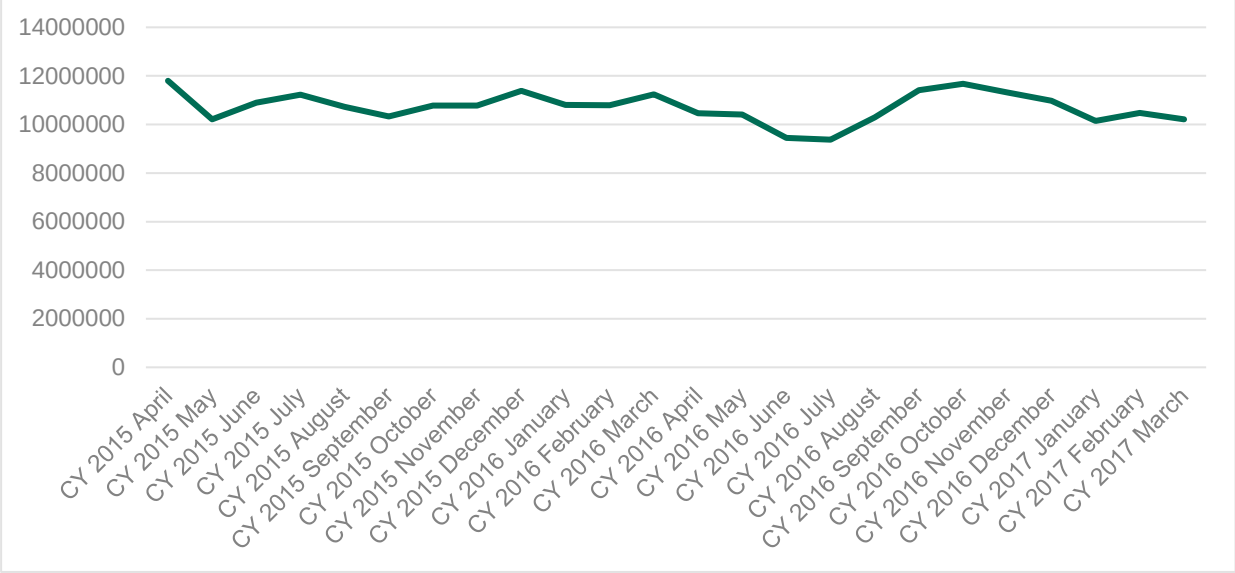


Fig. 3: Number of users attacked with any malware 2015-2017

As seen in Fig. 3, the behavior of ransomware does not reflect overall attack trends. While we witnessed peak of ransomware in autumn 2015 and a fall in autumn-winter 2016, malware statistics show the opposite fluctuations. To discover the possible reasons behind the peaks and troughs, we need to look deeper into the ransomware attack statistics.

Main actors of crypto-ransomware

Looking at the malware groups that were active in the period covered by this report, it appears that a rather diversified list of suspects is responsible for most of the trouble caused by crypto-ransomware. In the first period, from April 2015 to March 2016, the most actively propagated families were the following: Bitman, Cryakl, Cryptodef, Onion, Shade, and Mor. They were able to attack 223,782 users around the world, yet accounted for less than 31% of all users attacked with crypto-ransomware during the period.

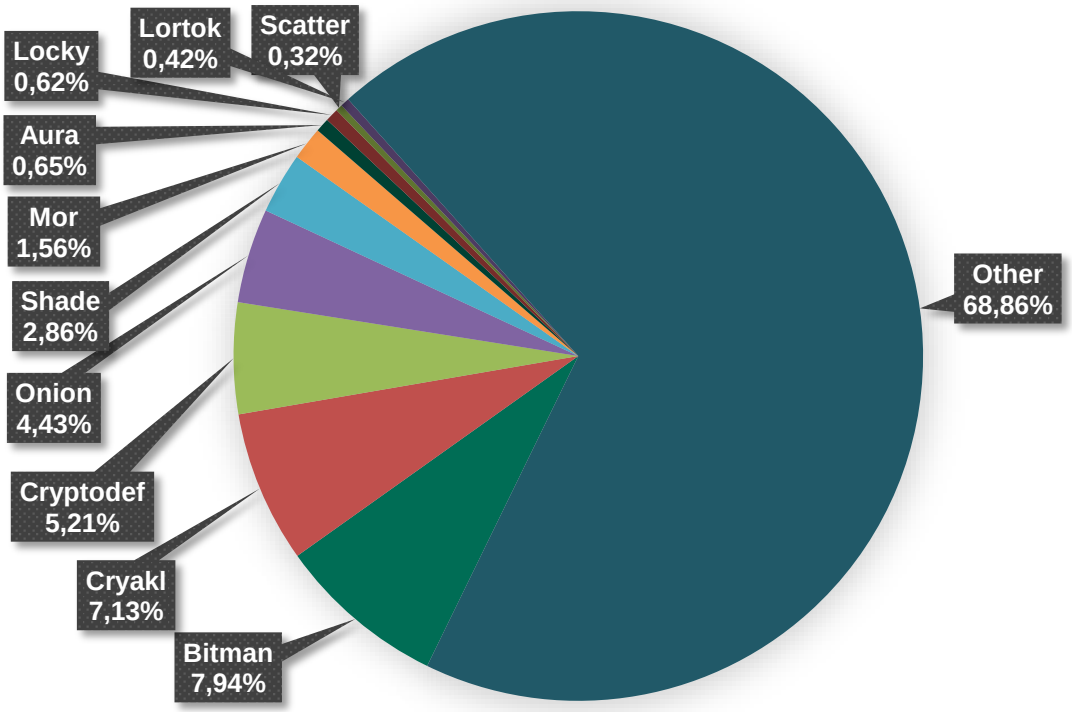


Fig. 4: Distribution of users attacked with different groups of encryption ransomware in 2015-2016

A year later the situation had not changed considerably. Most widespread families, including Locky, CryptXXX, Zerber, Shade, Crusis, Cryrar, Snocry, Cryakl, Cryptodef, Onion and Spora, together hit about 33% of all users attacked with crypto-ransomware during the period.

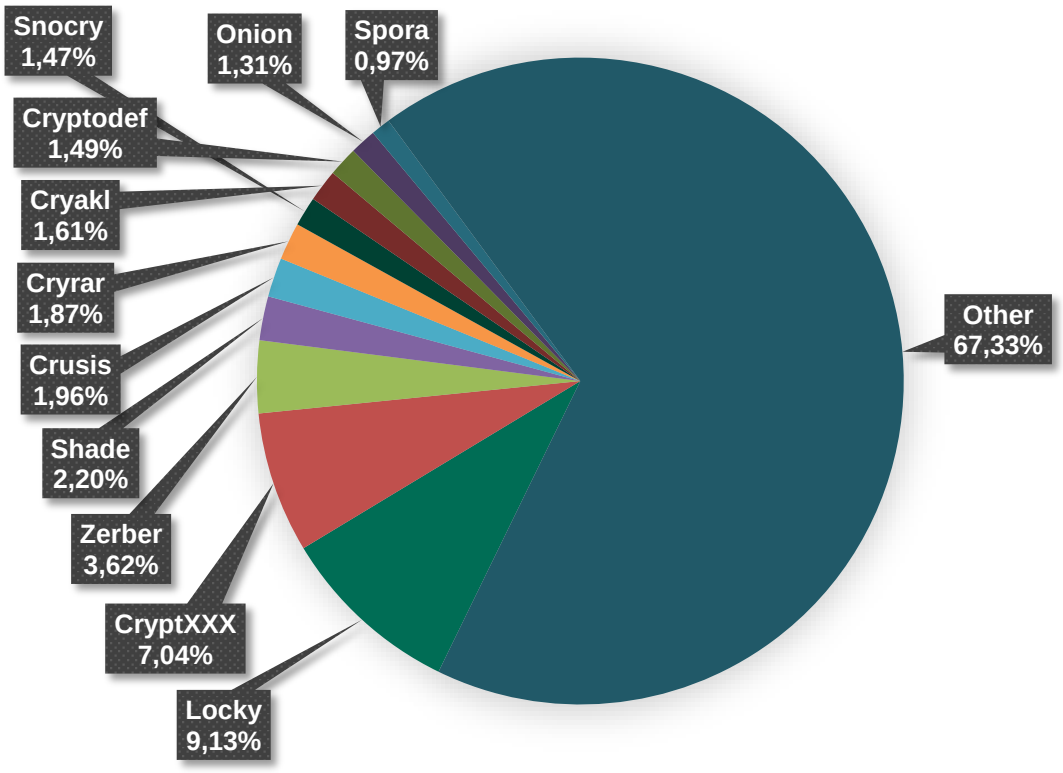


Fig. 5: Distribution of users attacked with different groups of encryption ransomware in 2016-2017

Interestingly, the high share of “others” indicates that the list of crypto-ransomware actors becomes more and more diversified. This is due to crypto-ransomware downloaders that are not linked to specific families. This could be a sign of the development of criminal-to-criminal infrastructure that is fueling the emergence of easy-to-go, ad hoc tools to attack users and extort money. You can read more about this process in “Part 3. How it is all orchestrated” section of this report. But before that, let’s have a closer look at the geographic statistics.

Geography

When analyzing the geography of attacked users, it is important to bear in mind that the numbers are influenced by the distribution of Kaspersky Lab’s customers around the world.

In order to accurately understand where most of the users attacked with ransomware lived, we use special metrics: the percentage of users attacked with ransomware as a proportion of the users attacked with any kind of malware. We believe this gives a much more precise picture of the threat landscape than direct comparison between users hit by ransomware in each territory. In order to keep statistics representative, the list of countries include the regions with over 30,000 unique users of Kaspersky Lab products.

In 2015-2016, the list of countries with the highest share of users attacked with ransomware looked as follows:

Country	% of users attacked with ransomware out of all users encountering malware
India	9.60%
Russian Federation	6.41%
Kazakhstan	5.75%
Italy	5.25%
Germany	4.26%
Vietnam	3.96%
Algeria	3.90%
Brazil	3.72%
Ukraine	3.72%
United States	1.41%

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 2015-2016

India, Russia, Kazakhstan, Italy, and Germany led the list with the percentage of attacked users exceeding 4%.

One year later, the situation had changed significantly: Turkey, Bangladesh, Japan, Iran, and Spain entered the list, all exceeding 5%. At the same time, India moved from first to third place, with 7.06% of users. The share of Vietnam users rose to 7.52%, while Italy kept fourth position. These changes could mean that attackers switch to previously unreached countries, where users are not so well prepared for fighting ransomware, and where competition among criminals is not so high.

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.7 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

Of these five, Japan, Turkey, and Vietnam experienced the most severe growth. According to statistics, these experienced growing activities of the Crysis and Locky families in 2016-2017. At the same time, India became the only country that faced a slight relief in the number of attacks.

Country	2015-2016	2016-2017	Y-to-Y change
Turkey	25,259	77,894	up 208.38%
Vietnam	89,247	181,469	up 103.33%
India	325,638	292,846	down 10.07%
Italy	59,130	101,558	up 71.75%
Bangladesh	22,005	35,160	up 59.78%
Japan	12,822	63,472	up 395.02%
Iran	31,131	41,145	up 32.17%
Spain	29,182	67,314	up 130.67%
Algeria	38,530	38,914	up 1%
China	12,247	36,815	up 200.6%

Fig. 8 The year-on-year change in the number of users attacked with any type of ransomware

The numbers above indicate a change in the ransomware global landscape. If we look deeper into the share of users attacked with Trojan-Ransom who experienced an attack by encryption ransomware, the picture becomes slightly different.

Country	% of users attacked with encryption ransomware in 2015-2016	% of users attacked with encryption ransomware in 2016-2017
Turkey	1.19%	2.15%
Vietnam	0.91%	2.17%
India	0.67%	0.98%
Italy	4.72%	4.36%
Bangladesh	1.02%	2.1%
Japan	4.7%	10.38%
Iran	0.76%	1.43%
Spain	1.2%	1.93%
Algeria	0.53%	0.85%
China	0.45%	1.34%
Other	76.54%	69.01%

Fig. 9: 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, in terms of share of users attacked with encryption ransomware as a proportion of users attacked with any kind of ransomware, the changes are not as significant.

The ten countries above accounted for 26.36% of all users who encountered any kind of ransomware in 2015-2016, rising to 40.44% in 2016-2017 respectively. A similar increase can be witnessed with crypto-ransomware numbers – from over 20% to more than 40%.

Country	2015-2016	2016-2017	Year-on-Year change (times)
Turkey	10,302	21,097	+2,05
Vietnam	20,409	52,339	+2,56
India	22,572	40,562	+1,78
Italy	53,039	66,983	+1,26
Bangladesh	5,380	11,816	+2,19
Japan	32,470	110,168	+3,39
Iran	4,144	10,013	+2,42
Spain	10,516	22,329	+2,12
Algeria	5,195	8,635	+1,66
China	4,537	13,018	+2,87
Other	549,972	795,339	+4,7

Fig. 10: the year-on-year growth rate of users attacked with encryption ransomware.

When it comes to the issue of geography, we can conclude that while, overall, the share of users attacked with malware from Trojan-Ransom changed significantly in some countries, the global number of attacked users barely increased. This could be a sign of, once again, the trend to diversify and spread attacks to yet unreached regions. This obviously means that users, especially in these countries should be extremely cautious when surfing the web.

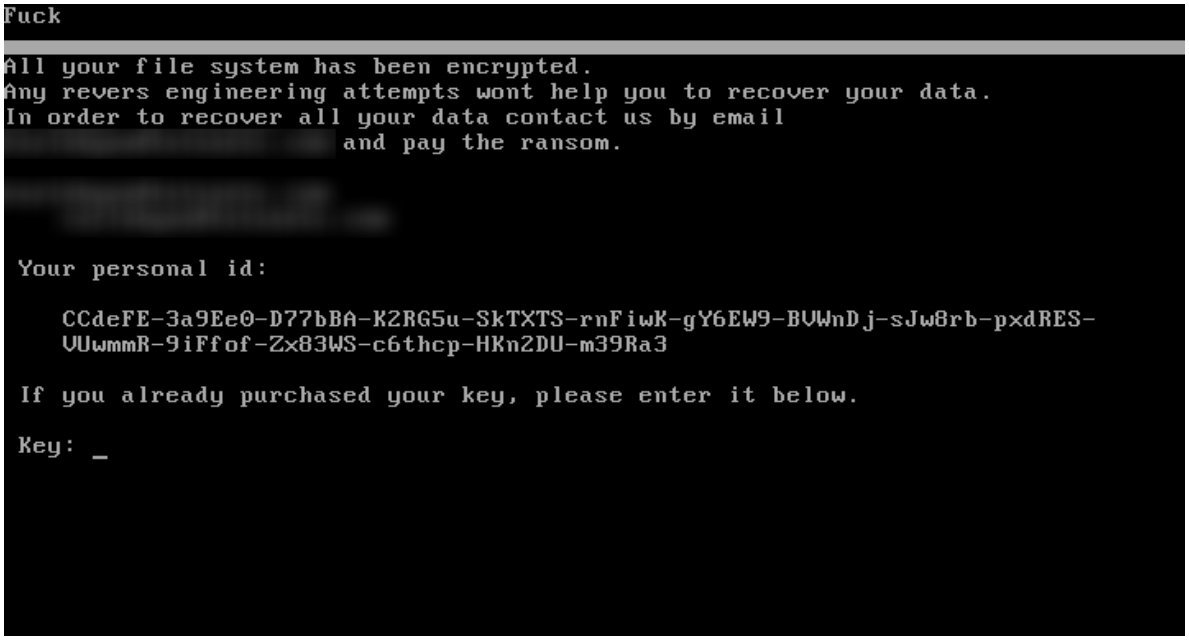
Ransomware intra-species massacre

As mentioned earlier, infamous Petya authors inserted certain “protection mechanisms” in their malware that do not allow the unauthorized use of Petya samples. In March, 2017, Kaspersky Lab researchers discovered PetrWrap, a new malware family that exploits the original Petya ransomware module distributed through a Ransomware-as-a-Service platform, to perform targeted attacks against organizations. PetrWrap is also an example of a ransomware tool ‘stolen’ by one cyber-attacker from another – its authors managed to overcome the mechanisms and have found a way to use Petya without paying its authors a penny.

It is unclear yet how PetrWrap is being distributed. After infection, PetrWrap launches Petya to encrypt its victim’s data and then demands a ransom. PetrWrap authors use their own private and public encryption keys instead of those that come with “stock” versions of Petya. This means they can operate without needing a private key from the Petya operators for decryption of the victim’s machine, should the ransom be paid.

Apparently, it is no coincidence that the developers of PetrWrap have chosen Petya for their malicious activities: this ransomware family now has a rather flawless cryptographic algorithm that is hard to break – the most important component of any encryption ransomware. In several cases in the past, mistakes in cryptography have allowed security researchers to find a way to decrypt files and ruin all of the efforts that criminals have put into their malicious campaigns. This has happened with previous versions of Petya and since then its authors have fixed almost all of their mistakes.

Because of this, a victim’s machine is reliably encrypted when it is attacked with the latest versions of Petya – so it is clear why the criminals behind PetrWrap decided to use it in their activities. Moreover, the lock screen shown to PetrWrap victims does not reflect any mentions of Petya, making it harder for security experts to assess the situation and quickly identify what family of ransomware has been used.



The screen of the infected machine

As a result of all the manipulations, PetrWrap achieves the following goals:

1. The victim's machine is locked and the MFT of NTFS partitions is encrypted securely (because Petya v3 used in this attack doesn't have the flaws of earlier versions and implements Salsa20 correctly);
2. The lock screen doesn't contain any mentions of Petya which makes it harder to assess the situation and determine the extent of the damage caused;
3. The developers of PetrWrap didn't have to write low-level bootloader code and risk making mistakes, similar to those observed in earlier versions of Petya.

Given all that, it could be stated that threat actors are starting to devour each other. This is a sign of growing competition between ransomware gangs. Theoretically, this is good, because the more time criminal actors spend on fighting and fooling each other, the less organized and effective their malicious campaigns will be. The worrying thing here is the fact that PetrWrap is used in targeted attacks. This is not the first case of targeted ransomware attacks and unfortunately is unlikely to be the last.

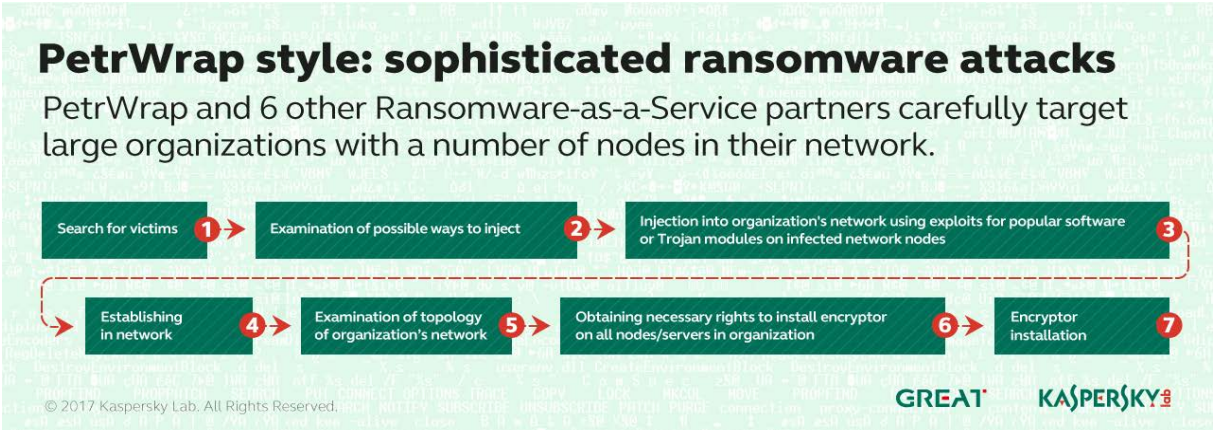
Targeted attacks

Targeted ransomware attacks are becoming more and more popular. The reason for the trend is clear – criminals consider targeted ransomware attacks against businesses potentially more profitable than mass attacks against private users. A successful ransomware attack against a company can easily stop its business processes for hours or even days, making owners of affected companies more likely to pay the ransom.

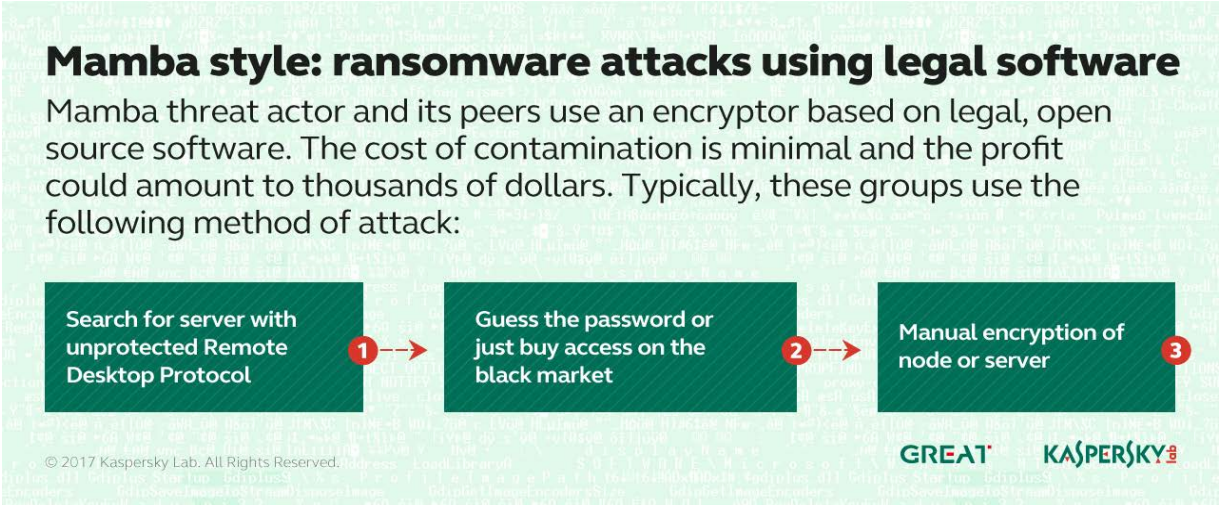
In 2017 Kaspersky Lab identified eight groups, who have attacked financial organizations worldwide, including the PetrWrap authors, the infamous Mamba group, and six unnamed groups also targeting corporate users.

In general, the tactics, techniques and procedures used by these groups are very similar. They infect the targeted organization with malware through vulnerable servers or spear phishing emails. Then they establish persistence in the victim's network and identify the valuable corporate resources to encrypt, subsequently demanding a ransom in exchange for decryption. In addition to their similarities, some groups have their own unique features.

An example of unique tools used in targeted ransomware attacks comes from PetrWrap. This group mainly targets major companies that have a large number of network nodes. The criminals carefully select targets for each attack, that can last for some time: PetrWrap has been persistent in a network for up to 6 months.



Another example is the Mamba group that uses its own encryptor malware, based on the open source software DiskCryptor. Once the attackers gain a foothold in the network, they install the encryptor across it, using a legal utility for Windows remote control. This approach makes the actions less suspicious for security officers of the targeted organization. Kaspersky Lab's researchers have encountered cases where the ransom amounted up to one bitcoin (around $1,000 to the end of March 2017) per one endpoint decryption.



WannaCry pandemic

Early May 2017 saw the beginning of the Trojan encryptor WannaCry outbreak – the fact we could not miss in the report even considering its timeline.

The outbreak appeared to be a global epidemic. More than 45,000 cases of the attack were counted in just one day, but the true number is much higher.

The timeline for attacks in the first week shows intelligibly the impact of cybersecurity efforts in fighting a threat.

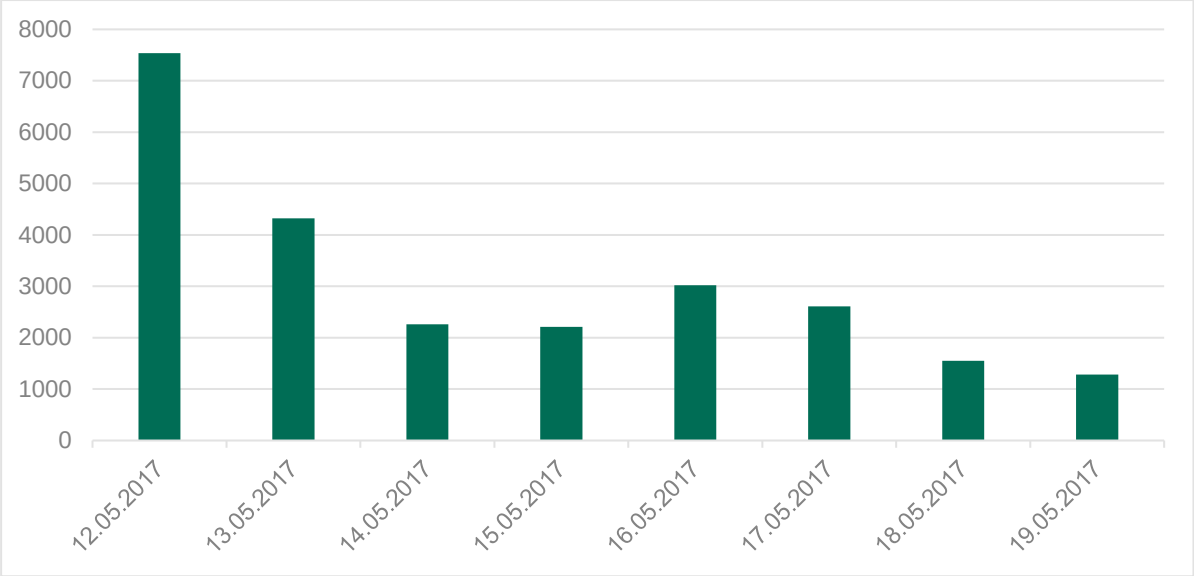
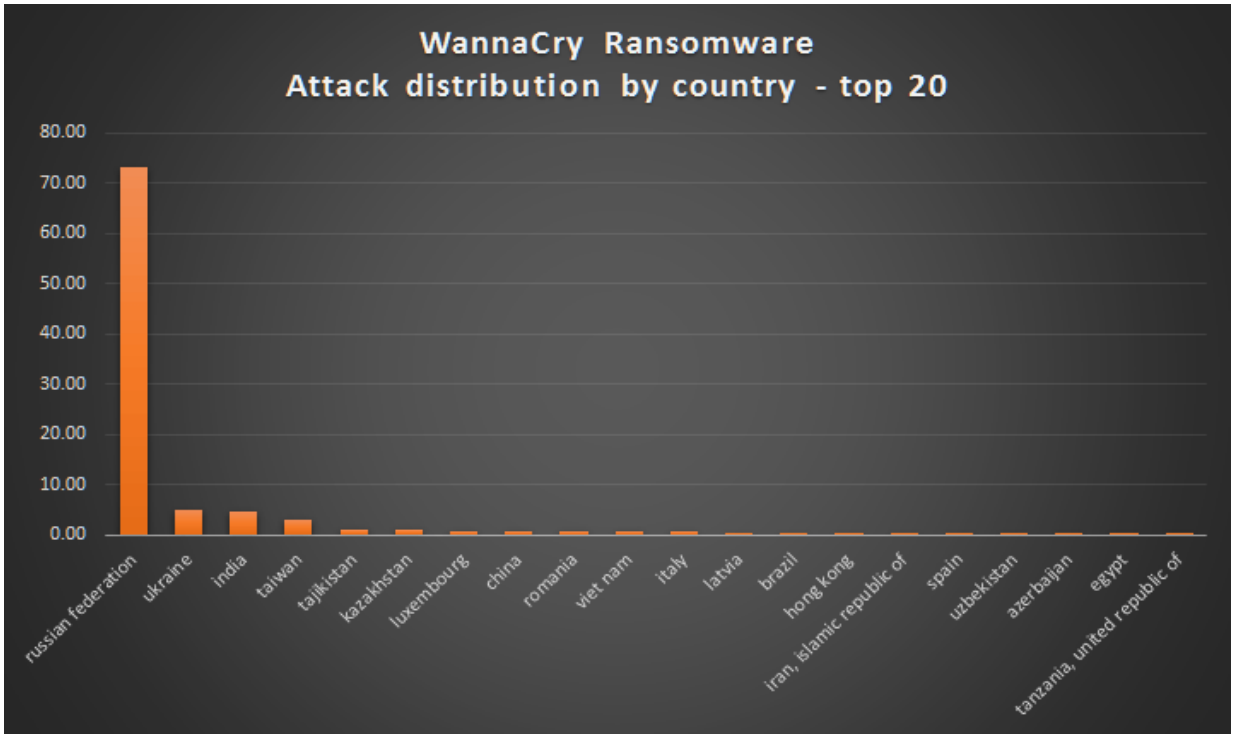


Fig. 11: The number of users encountering WannaCry attacks in the period of May 12-May 19

The largest number of attacks occurred in Russia, but Ukraine, India, and Taiwan have also suffered much damage from WannaCry. In just the first day of the attack, we found WannaCry in 74 countries.



Generally, WannaCry comes in two parts. First, it's an exploit whose purposes are infection and propagation. The second part is an encryptor that is downloaded to a computer after it has been infected.

The first part is the main difference between WannaCry and the majority of encryptors. To infect a computer with a common encryptor, a user has to make a mistake, for example by clicking a suspicious link, allowing Word to run a malicious macro, or downloading a suspicious attachment from an e-mail message. A system can be infected with WannaCry without the user doing anything.

The creators of WannaCry have taken advantage of the Windows exploit known as EternalBlue, which relies on a vulnerability that Microsoft patched in security update MS17-010, dated March 14 of this year. By using the exploit, the malefactors could gain remote access to computers and install the encryptor.

Given the importance of the Microsoft vulnerability, it is interesting to analyze how the share of users with Windows XP, 7 and Windows 10 changed throughout the first week.

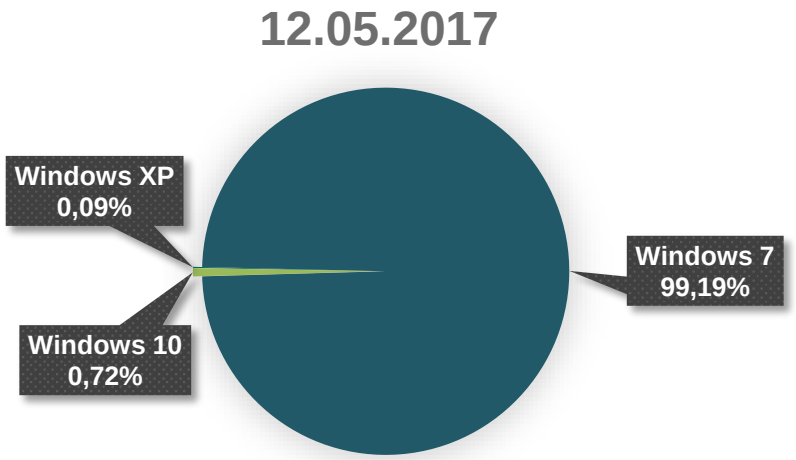


Fig. 12: The share of users with Windows XP, 7 and Windows 10 in May 12

As statistics shows, Windows 7 was the absolute leader among the platforms to the first day of attack.

Next week, the situation slightly changed – while Windows 7 kept it first ranking, the share of Windows 10 users grew almost nine times, rising from 0,69%% to more than 6%.

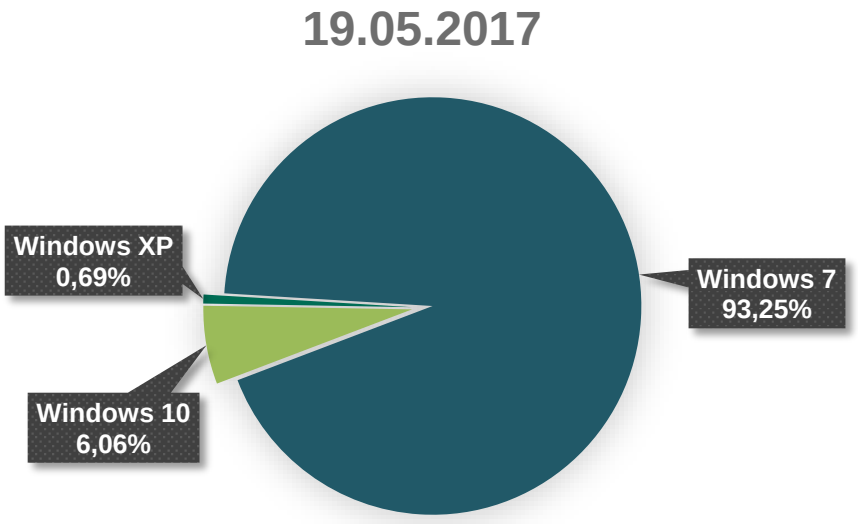


Fig. 13: The share of users with Windows XP, 7 and Windows 10 in May 19

After hacking a computer successfully, WannaCry attempts to spread itself over the local network onto other computers, in the manner of a computer worm. The encryptor scans other computers for the same vulnerability that can be exploited with the help of EternalBlue, and when WannaCry finds a vulnerable machine, it attacks the machine and encrypts files on it.

Therefore, by infecting one computer, WannaCry can infect an entire local area network and encrypt all of the computers on the network. That's why large companies suffered the most from the WannaCry attack — the more computers on the network, the greater the damage.

As an encryptor, WannaCry (sometimes called WCrypt or, for no discernable reason, WannaCry Decryptor) behaves like any other encryptor; it encrypts files on a computer and demands ransom to decrypt them. It most closely resembles a variation of the infamous CryptXXX Trojan.

WannaCry encrypts files of various types (the full list is here) including office documents, pictures, videos, archives, and other file formats that potentially contain critical user data. The extensions of the encrypted files are renamed .WCRY, and the files become completely inaccessible.

After this, the Trojan shows a window that contains information about the infection and actions that the user supposedly has to perform to recover the files. WannaCry spreads notifications as text files with the same information across folders on the computer to ensure that the user receives the message.

As usual, the actions entail transferring a certain amount of money, in bitcoins, to the wallet of the perpetrators. After that, they say, they will decrypt all of the files.

Initially, cybercriminals demanded $300 but after a period of time this demand is automatically raised to $600.

Kaspersky Lab researchers conducted in depth research into this ransomware. It became clear that the ransomware developers had made many mistakes and the code quality is very low. For those infected by the WannaCry ransomware, there is a high probability that they can restore a lot of the files on the affected computer by using free utilities available for file recovery. We advise organizations share this article with their system administrators – as they can use the file recovery utilities on affected machines in their network

Part 2: Mobile ransomware Statistics

The number of users attacked with mobile ransomware in the observed period fell by 4.62% from 136,532 users in 2015-2016 to 130,232.

The activity of mobile ransomware skyrocketed in early 2017 with 218, 625 mobile Trojan-Ransomware installation packages – 3.5 times more than in the previous quarter. The activity then fell to the average level of the observed 2-year period.

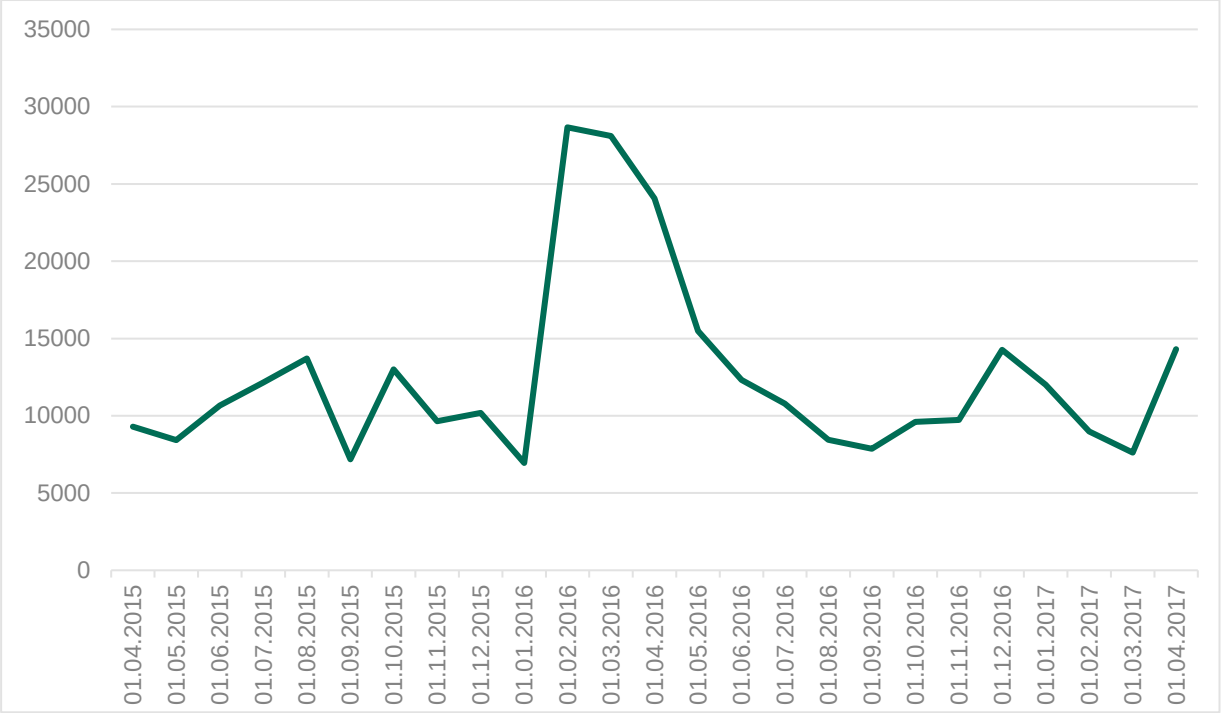


Fig. 14: The number of users encountering mobile ransomware at least once in the period April 2015 to March 2017

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 to136,532 users. This was mainly due to Fusob ransomware activities, with its increased number of attacks in Germany. However, the activity then demonstrated a sharp decline from 24,061 in April 2016 to 7,855 in September 2016. The trend continued across the rest of the period with only one exception – a peak in December 2016 at the level of 14,274. This was caused by Svpeng family intensification, whose attacks grew more than 3 times.

The share of users attacked with ransomware as a proportion of users attacked with any kind of malware also experienced some relief: from 2.04% in 2014-2015 to 4.63% in 2015-2016 and 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 geography of mobile ransomware differs significantly from that of PC ransomware. This is due to the fact that major ransomware family Fusob is focused in Europe, Canada and United States, while another big player, Small, mainly targets CIS.

Country	% of users attacked with ransomware out of all users encountering malware
Germany	22.90%
Canada	19.61%
United Kingdom	16.13%
United States	15.64%
Kazakhstan	14.42%
Italy	12.54%
Netherlands	12.30%
Spain	5.27%
Russian Federation	4.91%
Ukraine	4.63%

Fig. 15 Top 10 countries with the highest percentage of mobile users attacked with malware in the Trojan-Ransom category as a proportion of users attacked with any kind of mobile malware. (Each country has more than 5,000 unique users of Kaspersky Lab products for Android devices.)
Period: April 2015 – March 2016.

Germany became the leader with 22.9% of attacked users, followed by Canada (19.61%), the UK (16.13%) and the US (15.64%).

One of the explanations for the different list of regions could be the fact that developed and rich countries not only have a higher level of income, but also more advanced and deeper penetrated mobile and e-payment infrastructure. This is appealing to the criminals as they can obtain access to the opportunity to transfer the ransom in a couple of taps or clicks.

In 2016-2017 the list changed significantly, both in terms of the order of countries and in the proportion of users encountering ransomware. However, these changes impact mostly the bottom of the ranking, while top-3 leaders are more or less on the same page.

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. 16: Top 10 countries with the highest percentage of mobile users attacked with malware Trojan-Ransom category 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 period showed significantly fewer numbers of Trojan-Ransom detections across the countries. To keep the statistics representative, we broadened the list of countries, including the regions with over 2,500 unique users of Kaspersky Lab products for Android devices.

The United Stated shifted from 4th to 1st position, while Canada and Germany retained their top-3 ranking. A rise in the United States occurred largely due to attacks by Svpeng and Fusob – with the first of these mainly targeting America, with only 3% of its attacks occurring in other regions. As for Fusob, it was initially focused in Germany, but since Q1 2017 America topped its list of targets with 28% of attacks while Germany accounted for 24%. Increased attention in the United Stated could be attributed to the availability of anonymous means of payment, such as iTunes cards and MoneyPak.

The sharp fall in Russia could be explained by simultaneous growth of overall malware attacks, combined with a decline in ransomware attacks on the region. The volume of Small attacks also experienced a significant decline.

Main actors of mobile ransomware

Across the whole period covered by the report, Kaspersky Lab researchers were able to identify a few families of mobile ransomware that users of our products encountered most often. In 2014-2015 these were: Pletor, Fusob, Svpeng and Small. In 2015-2016, Fusob became the most popular mobile Trojan: users in more than 100 countries worldwide were attacked by this Trojan-Ransom program.
The first samples of Trojan-Ransom.AndroidOS.Fusob were discovered by Kaspersky Lab experts in early January 2015.

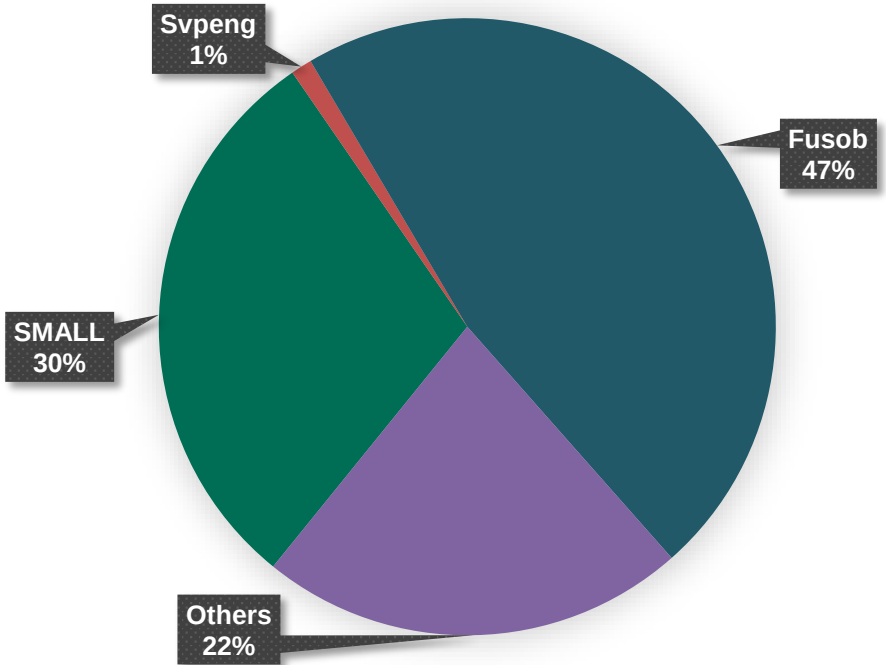


Fig. 17: The distribution of the share of attacked users between the most active mobile ransomware families in 2015-2016.

Unlike PC ransomware, the mobile threat landscape is dominated by just a few actors responsible for almost 80% of attacks. The situation in 2016-2017 is slightly different.

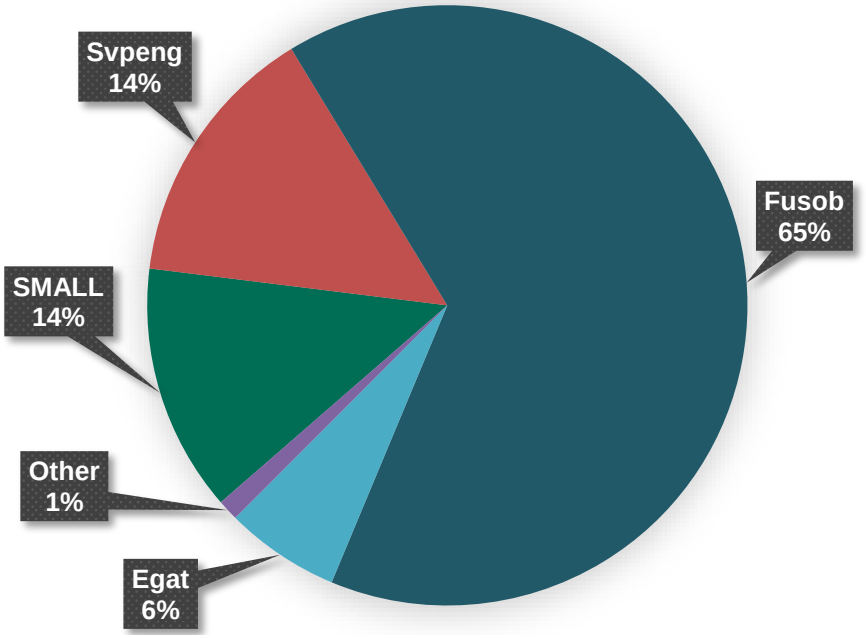


Fig. 18: The distribution of the share of attacked users between the most active mobile ransomware families in 2016-2017.

The “other” section dropped significantly from 22% 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%). Given the dominant position of the Fusob family, let’s delve a little deeper into its evolution during the period.

Fusob ransomware

The increase in the number of mobile ransomware installation packages in the first half of 2016 is mainly due to the active spread of the Trojan-Ransom.AndroidOS.Fusob family. In the second half of the same year, the activity of this family fell, which affected the number of detected installation packages. The growth resumed in the fourth quarter of 2016 and sharply accelerated in Q1 2017.

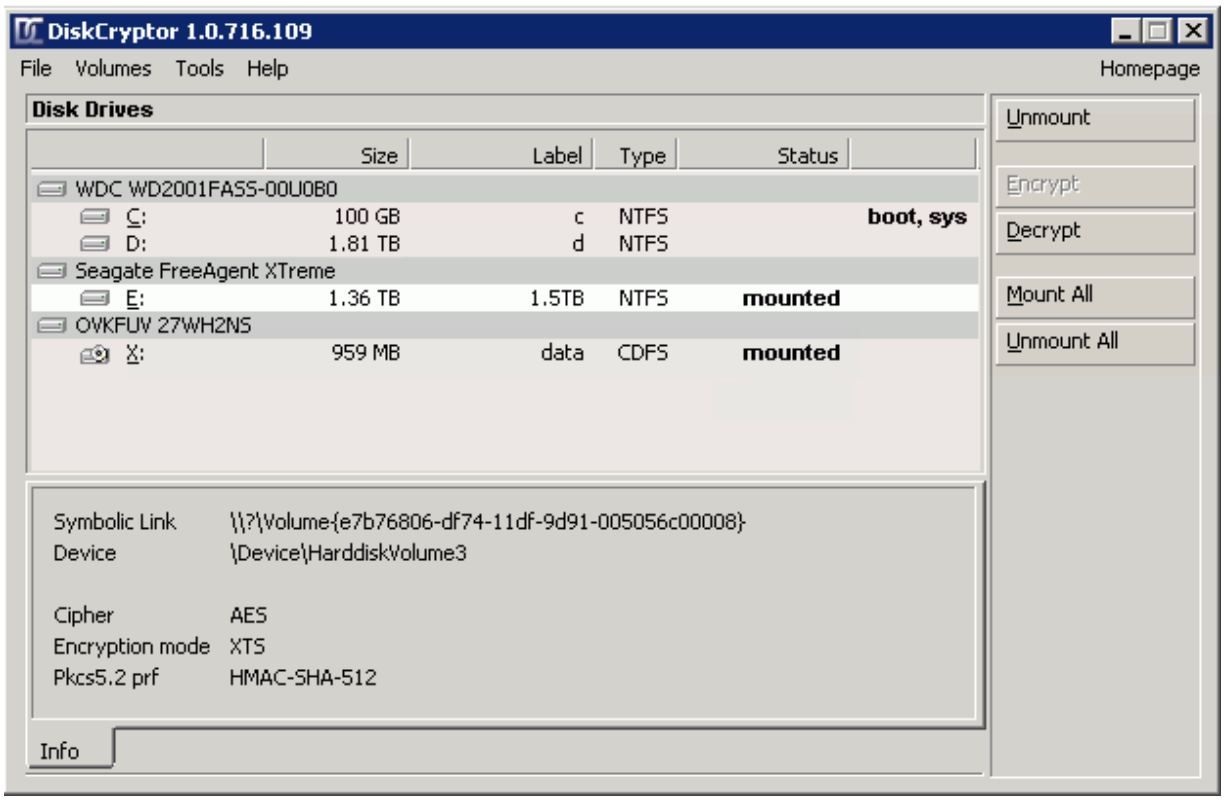
Trojan-Ransom.AndroidOS.Fusob.h remained the most popular mobile Trojan-Ransomware in the first quarter, accounting for nearly 45% of users attacked by mobile ransomware. Once run, the Trojan requests administrator privileges, collects information about the device, including GPS coordinates and call history, and downloads the data to a malicious server. After that, it may receive a command to block the device.

Part 3. How it is all orchestrated

Given the signs of growing competition in the ransomware market, Ransomware-as-a-Service is also becoming more and more popular, attracting new actors. However, this is not the only channel that makes the market very easy to join.

Over the last 12 months, ransomware has grown in sophistication and diversity, offering a lot of ready-to-go solutions to those with fewer skills, resources or time – through a growing and increasingly efficient underground ecosystem.

Today, an attacker (or group) can easily create their own encryptor without making any special effort. A vivid example is the Mamba encryptor based on DiskCryptor open source software. Some cybercriminal groups do not even go to the trouble of involving programmers; instead, they use this legal utility “out of the box.”



DiskCryptor utility

There are three main reasons for this:

- It’s easy to buy a ransomware build or builder on the underground market
- It’s easy to buy a distribution service
- Crypto ransomware, as a business, has a very clear monetization model through cryptocurrencies

In other words, this is a fine tuned, user friendly and constantly developing ecosystem. In the last few years we, at Kaspersky Lab, have been monitoring the development of this ecosystem.

There are three types of involvement in the ransomware "business". The underground crypto ransomware market offers criminals three different ways of entering the illegal business:

- Create new ransomware for sale
- Become a partner in a ransomware affiliate program
- Become the owner of an affiliate program

The first type of involvement requires advanced code writing skills, including a deep knowledge of cryptography. The actors which we have observed in this category are like gun traders: they usually don't participate in actual attacks, but only sell code. Sometimes, authors of the malware sell their "products" with all the source code for a fixed price (usually several thousand dollars) and sometimes they sell their builder – the tool which allows criminals with no programming background to build the crypto ransomware with a specific list of functions.

Builders are usually much cheaper than the full source code of unique ransomware – hundreds of dollars. However, authors (and owners) of software like this often charge customers for each new build of malware created with the help of their software.

Pay-per-build is another type of monetization used by the authors of the original ransomware. In this case the price drops even lower, to tens of dollars, but the client would receive the malware with a fixed list of functions.

Affiliate programs, the third type of involvement in the ransomware criminal business, are a rather standard form of cybercrime: owners of the program provide partners with all the necessary infection tools, and then the partners work on distributing the malware. The more successful their efforts, the more money they receive. Participation in such programs requires nothing, but the will to conduct certain illegal activities and a couple of bitcoins as a partnership fee.

In contrast, "elite" programs will not accept just any kind of partner. In order to join, a candidate has to provide a personal recommendation from one of the acting partners in the program. In addition, the candidate must prove that they have certain malware distribution capabilities. In one case we observed in the last year, the candidate had to demonstrate their ability to complete at least 4,000 successful downloads and installations of the malware on victims' PCs. In exchange, the partner gets some free tools for the obfuscation of ransomware builds (in order to make them less visible to security solutions) and a good conversion rate – up to 3%, which is a very good deal, at least compared to rates that legal affiliate programs offer.

To summarize: flexibility is the key feature of the current underground ransomware ecosystem. It offers lots of opportunities to people with a propensity towards criminal behavior, and it almost doesn't matter what level of IT experience they have.

Conclusions and predictions

Based on the statistics and trends described in this report, we have come to the following conclusions:

- Ransomware actors are starting to devour each other. This is a sign of growing competition between ransomware gangs.
- The geography statistics show that attackers switch to previously unreached countries, where users are not as well prepared for fighting ransomware, and where competition among criminals is not so high.
- The worrying thing here is the fact that ransomware attacks are becoming increasingly targeted, hitting financial infrastructure across the globe. The reason for the trend is clear – criminals consider targeted ransomware attacks against businesses potentially more profitable than mass attacks against private users.
- The numbers show that ransomware on PCs are still on the rise – albeit at a slower growth rate.
- Moreover, the number of users attacked with mobile ransomware in the observed period fell. This could be a sign of successful collaboration between vendors of security solutions, various law enforcement agencies, and other actors. Increased threat awareness, fueled by global media coverage on the most prominent fraudulent campaigns can also have a part to play.
- Another reason is the development of joint industry efforts to protect users from encryption ransomware.
- Although the statistics show that attacks with ransomware operate on a massive scale, responsibility for most of the mobile attacks rests with just a few groups of malware, most of them spread via affiliate programs. At the same time, PC ransomware shows quite the opposite status, with a lot of malicious actors in the wild conducting ad hoc attacks.

Along with these conclusions we believe that the current ransomware threat landscape provides a good basis for several predictions on how this threat will evolve in the future.

Predictions:

- The extortion model is here to stay. More stable growth, which is at a higher level on average, could indicate an alarming trend: a shift from chaotic and sporadic actors' attempts to gain foothold in threat landscape, to steadier and higher volumes.
- Given the signs of growing competition on the ransomware market, Ransomware-as-a-Service is also becoming more and more popular, attracting new actors.
- Ransomware is growing in sophistication and diversity, offering a lot of ready-to-go solutions to those with fewer skills, resources or time – through a growing and increasingly efficient underground ecosystem.
- Development of criminal-to-criminal infrastructure is fueling the emergence of easy-to-go, ad hoc tools to perform targeted attacks and extort money, making attacks more dispersed. This trend has already taken place and will likely continue in the future.
- Global initiatives which protect users from encryption ransomware will keep gaining momentum.

Fighting back

- **Through technology**

Kaspersky Lab provides a free anti-ransomware tool which is available for all businesses to download and use, regardless of the security solution they have installed.

- **Through collaboration: The No More Ransom Initiative**
- **On 25 July 2016**, the Dutch National Police, Europol, Intel Security and Kaspersky Lab announced the launch of the No More Ransom project - a non-commercial initiative that unites public and private organizations and aims to inform people of the dangers of ransomware and help them to recover their data.
- The online portal currently carries 50 decryption tools, seven of which were made by Kaspersky Lab.
- Since the NMR launch, more than 29.000 victims from all over the world have been able to unlock their files for free thanks to Kaspersky Lab tools.
- The NMR portal is currently available in 14 languages: English, Dutch, French, Italian and Portuguese, German, Spanish, Slovenian, Finnish, Hebrew, Ukrainian, Korean, and Japanese.

Standing up to ransomware – how to stay safe

1. Back up data regularly.
2. Use a reliable security solution, and remember to keep key features – such as System Watcher – switched on.
3. Always keep software updated on all the devices you use.
4. Treat email attachments, or messages from people you don't know, with caution. If in doubt, don't open it.
5. If you're a business, you should also educate your employees and IT teams; keep sensitive data separate; restrict access; and back up everything, always.
4. If you are unlucky enough to fall victim to an encryptor, don't panic. Use a clean system to check our No More Ransom site; you may well find a decryption tool that can help you get your files back.
5. The latest versions of Kaspersky Lab products for smaller companies have been enhanced with anti-cryptomalware functionality. In addition, a free anti-ransomware tool has been made available for all businesses to download and use, regardless of the security solution they have installed.
6. Last, but not least, remember that ransomware is a criminal offence. Report it to your local law enforcement agency.

Why you shouldn’t pay

- You become a bigger target.
- You can't trust criminals – you may never get your data back, even if you pay.
- Your next ransom will be higher.
- You encourage the criminals.

Can we ever win the fight against ransomware?

Yes – but only by working together. Ransomware is a lucrative criminal business. To make it stop the world needs to unite to disrupt the criminals’ operations and make it increasingly difficult for them to profit from attacks.