KSN REPORT: RANSOMWARE IN 2014-2016

June 2016

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. This report covers the evolution of the threat over the last two years.

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. 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. Nowadays, encryption ransomware is widely regarded as synonymous with ransomware, although, according to Kaspersky Lab statistics the number of users that regularly encounters blockers remains high.

Main findings:

- The total number of users who encountered ransomware between April 2015 and March 2016 rose by **17.7%** compared to the previous 12 months (April 2014 to March 2015) – from **1,967,784 to 2,315,931** users around the world;
- The proportion of users who encountered ransomware at least once out of the total number of users who encountered malware rose 0.7 percentage points, from **3.63%** in 2014-2015 to **4.34%** in 2015-2016;
- Among those who encountered ransomware, the proportion who encountered cryptors rose dramatically – **up 25** percentage points, **from 6.6%** in 2014-2015 **to 31.6%** in 2015-2016;
- The number of users attacked with cryptors rose 5.5 times, **from 131,111** in 2014-2015 to **718,536** in 2015-2016;
- The number of users attacked with Win-lockers decreased **13.03%,** from **1,836,673** in 2014-2015 to **1,597,395** in 2015-2016;
- The number of users attacked with mobile ransomware **grew almost 4 times**: from **35,413 users** in 2014-2015 to **136,532 users** in 2015-2016.

Introduction: A brief history of ransomware

Although it has only now started to attract the widespread attention of the media and the security community, ransomware (including crypto-ransomware) as a type of malware has been known about for years: at least since 1989 when the first-known malware capable of encrypting file names (the AIDS Trojan) was discovered.

Another example of extortion malware was discovered by security researchers as long ago as the middle 2000s. This was the Gpcode malware, capable of encrypting files on infected machines with its own encryption algorithm. Gpcode was followed by several other families, like Krotten, Cryzip etc. From time to time another copycat or slightly different version of Gpcode emerged. The appearance of such programs would provoke relatively small incidents, but never resulted in something that looked anything like an epidemic.

This situation remained unchanged for years.

The Blockers epidemic

The first real ransomware epidemic started in 2010 with thousands of home users in Russia and some neighboring countries encountering cryptic windows that covered all other windows on their desktop. These windows usually contained a message from criminals asking the victim to send money to a given Premium-SMS number in order to unlock the screen or browser of their infected PC.

The scale of the problem turned out to be so great and the number of victims so significant that it prompted law enforcement agencies to become involved and gained extensive media coverage in Russia, from television to the blogosphere. Mobile phone operators did what they could to combat the threat, introducing new rules for registering and operating premium-rate (short) numbers, blocking accounts that had been used to perpetrate fraud and informing their customers about this type of fraud.

In late August 2010, several people were arrested in Moscow and accused of creating blockers. According to the Russian Ministry of the Interior, the illegal income generated by the criminal group was estimated at 500 million rubles (about 12.5 million euros).

The rise of so-called blockers was powered mainly by the fact that the creation of malware capable of blocking an OS browser or desktop did not require significant programming skills and generated a relatively reliable income for the criminal. Comparatively easy DIY sets for creating blockers were available on underground forums and this attracted a lot of low-level cybercriminals.

The security industry and law enforcement agencies reacted quickly: the arrest of the group, combined with the release of a number of services offering the free unlocking of locked systems made criminal efforts to extort money in this way both more risky and less profitable.

Nevertheless, blockers remain on the threat landscape to this day – as illustrated in this report.

At the end of 2010, Kaspersky Lab researchers predicted that despite the arrests, the problem was unlikely to go away. Cybercriminals, the experts predicted, would simply use other methods to receive payment for 'unblocking' their victims' computers, such as electronic money systems.

That is exactly what happened several years later when ransomware's big comeback began.

Ransomware returns with encryption

The biggest difference between the two types of ransomware: blockers and encryption ransomware is that blocker damage is fully reversible. Even in the worst case scenario, the owner of an infected PC could simply reinstall the OS to get all their files back. In addition, the way in which blockers work allowed security researchers to develop automated technologies that help to fight against blockers even after infection. One such patented technology is implemented in Kaspersky Lab products and it basically puts a stop to the blocker threat for Kaspersky Lab clients.

However, when it comes to encryption ransomware things are much more complicated because the encrypted files are impossible to decrypt without a special key, which is usually stored on the cybercriminals' servers. This makes it more important than ever to take a proactive approach to protection.

The severity of the consequences of successful infection is one of the reasons why encryption ransomware is enjoying a resurgence in popularity among cybercriminals. However, it is not the only one. The analysis in this report attempts to assess the scale of the problem, and to highlight possible reasons for its re-emergence almost ten years after the first encryption ransomware appeared on the threat landscape.

Part 1. PC ransomware: From blockers to crypto-ransomware

One doesn't need to look at the statistics to see that ransomware is once again a major problem for Internet users. You only need to read or watch the news. Nevertheless, the statistics help to show how big the problem is and whether there are aspects to the problem that you won't learn from yet another news story about yet another ransomware infection.

The total number of users who encountered ransomware over the12 month period from April 2015 to March 2016 grew by **17.7%** in comparison to the previous year: April 2014 to March 2015 – from **1,967,784 to 2,315,931** users around the world

The proportion of users who encountered ransomware at least once out of the total number of users who encountered malware rose 0.7 percentage points, from **3.63%** in 2014-2015 to **4.34%** in 2015-2016.

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 prevalence of ransomware has been sporadic, rising and falling every few months. The rise in the use of crypto-malware has been more consistent: showing a steady increase in the number of attacked users, particularly from March 2015, before peaking in December 2015. Interestingly enough, from October 2015, all other types of ransomware were declining dramatically in number and by the turn of the year just a very small number of users encountered old school blockers and other non-encrypting ransomware.

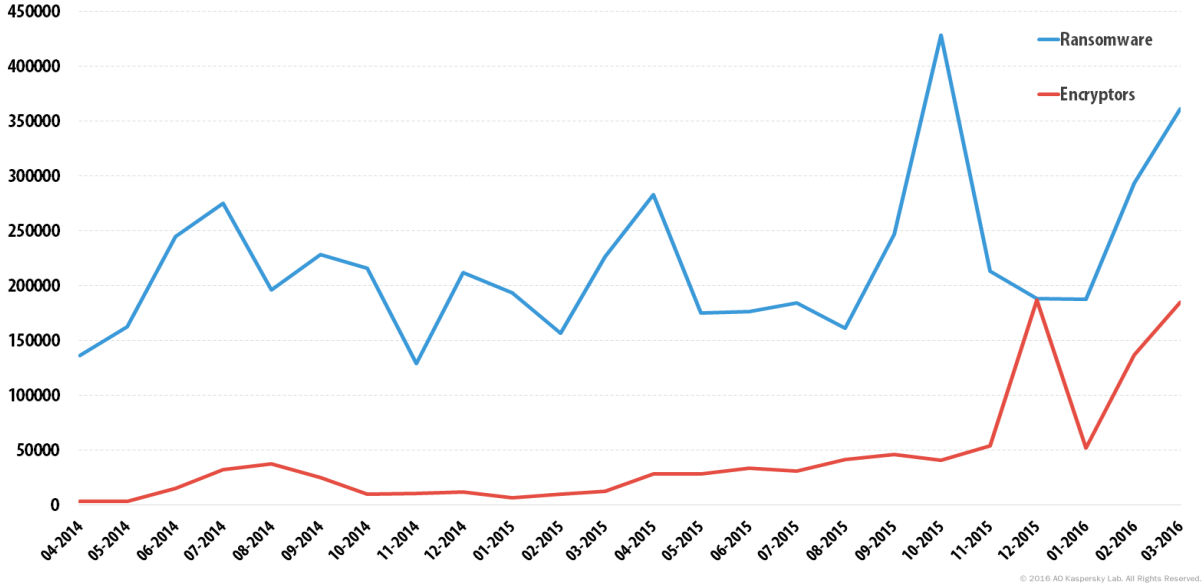

Fig. 1: The number of users encountering ransomware (including Encryptors and Downloaders that load encryptors) at least once in the period from April 2014 to March 2016

The decline did not last long. In February 2016, both categories started to recover from the dramatic fall in January, and numbers continue to rise.

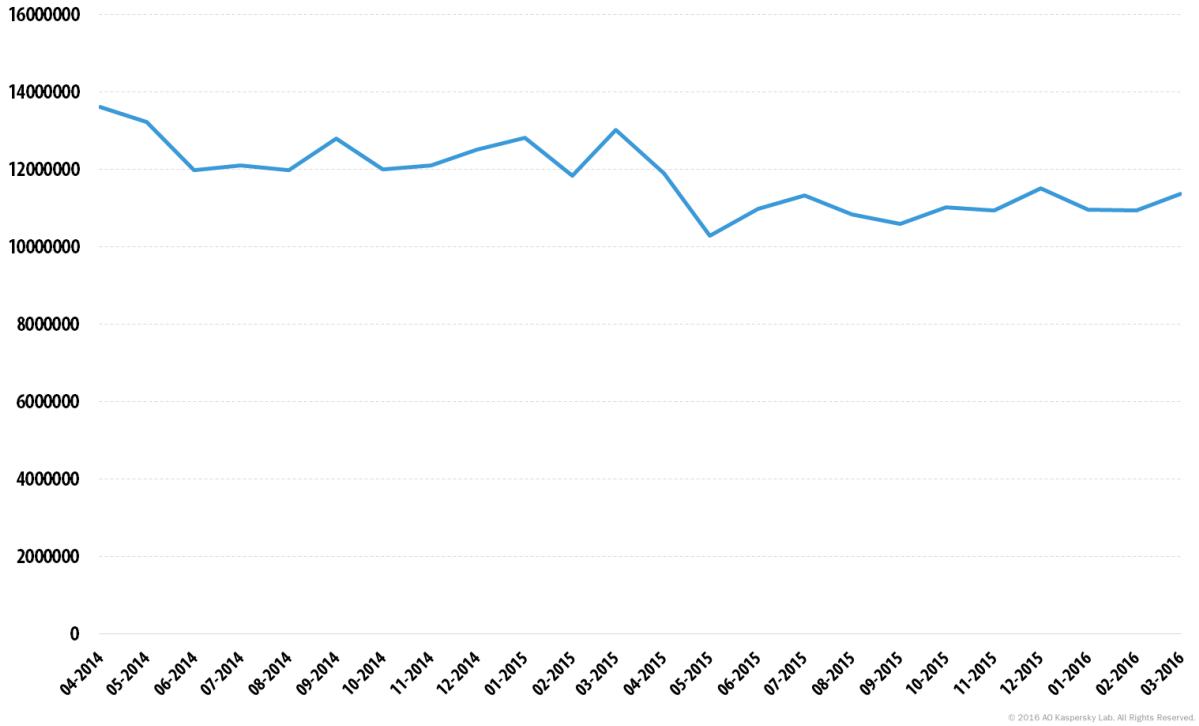

Fig. 2: Number of users attacked with any malware 2014-2016

As seen in Fig. 2, the behavior of ransomware does not reflect overall attack trends. To discover the possible reasons behind the peaks and troughs we need to look deeper into the ransomware attack statistics.

The first main spike in the period under investigation was registered in July 2014 with more than 274 thousand users encountering some form of ransomware. The main reason for this surge was the Trojan-Ransom.JS.SMSer.pn, a browser-locker that attacked more than one-in-three (31%) those affected by ransomware that month. Encryptors were encountered by one-in-ten (11.63%) of all those who faced malware from the Trojan-Ransom category.

The next peak was registered in April 2015, when 282.5 thousand users were attacked with ransomware. This was provoked by several groups of malware, and about 10% of those affected encountered encryption ransomware.

October 2015 saw ransomware achieve an all-time-high with more than 428.4 thousand users attacked. Of those affected, 9.38% were hit with encryption ransomware. In March 2016, when another surge of ransomware attacks took place, the situation was very different: over half (51.9%) of those who encountered Trojan-Ransom malware were dealing with encryptors. This was mostly due to the activity of a small number of ransomware groups led, among others, by the infamous TeslaCrypt encryption ransomware.

The results for April and May 2016 – although beyond the scope of this report – confirm this trend: encryption ransomware affected 54% of attacked users in April 2016 and 35.7% in May, still well above the average for the previous 12 months.

Main actors of encryption ransomware

Looking at the malware groups that were active in the period covered by this report, it appears that a rather short list of suspects is responsible for most of the trouble caused by crypto-ransomware. In the first period, from April 2014 to March 2015, the most actively propagated encryptors were the following groups of malware: CryptoWall, Cryakl, Scatter, Mor, CTB-Locker, TorrentLocker, Fury, Lortok, Aura, and Shade. Between them they were able to attack 101,568 users around the world, accounting for 77.48% of all users attacked with crypto-ransomware during the period.

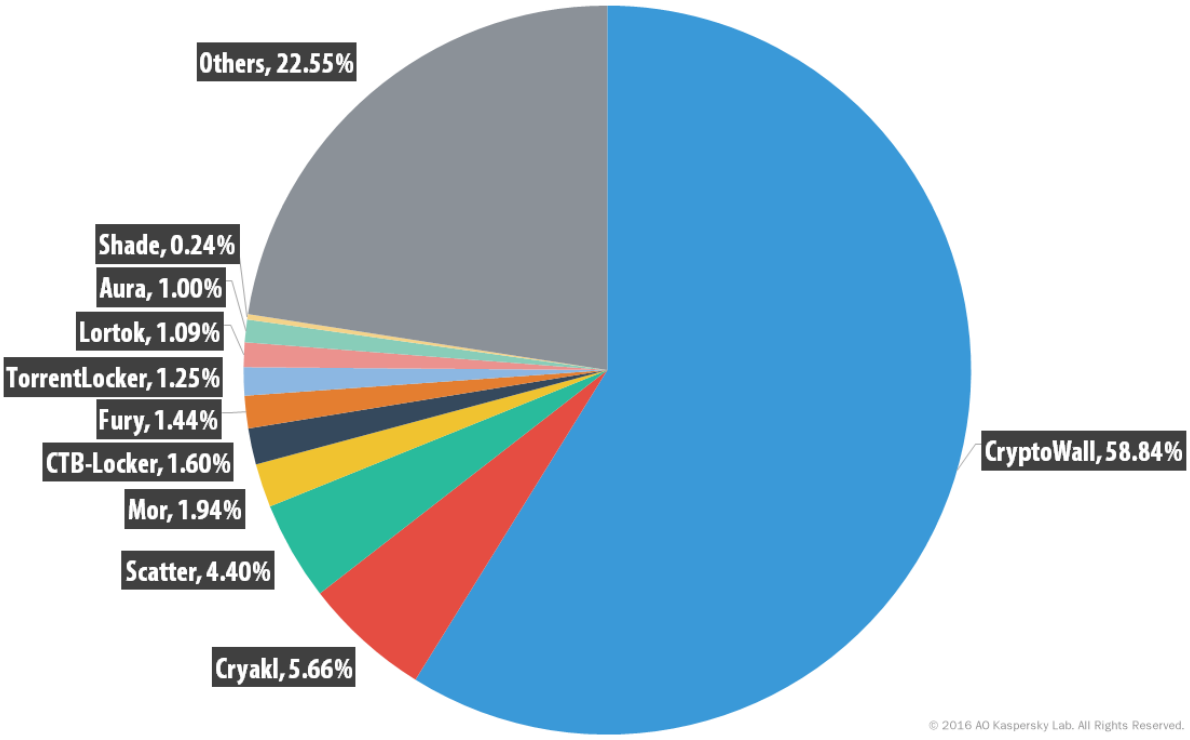

Fig. 3: Distribution of users attacked with different groups of encryption ransomware in 2014-2015

A year later the situation had changed considerably. TeslaCrypt, together with CTB-Locker, Scatter and Cryakl were responsible for attacks against 79.21% of those who encountered any crypto-ransomware.

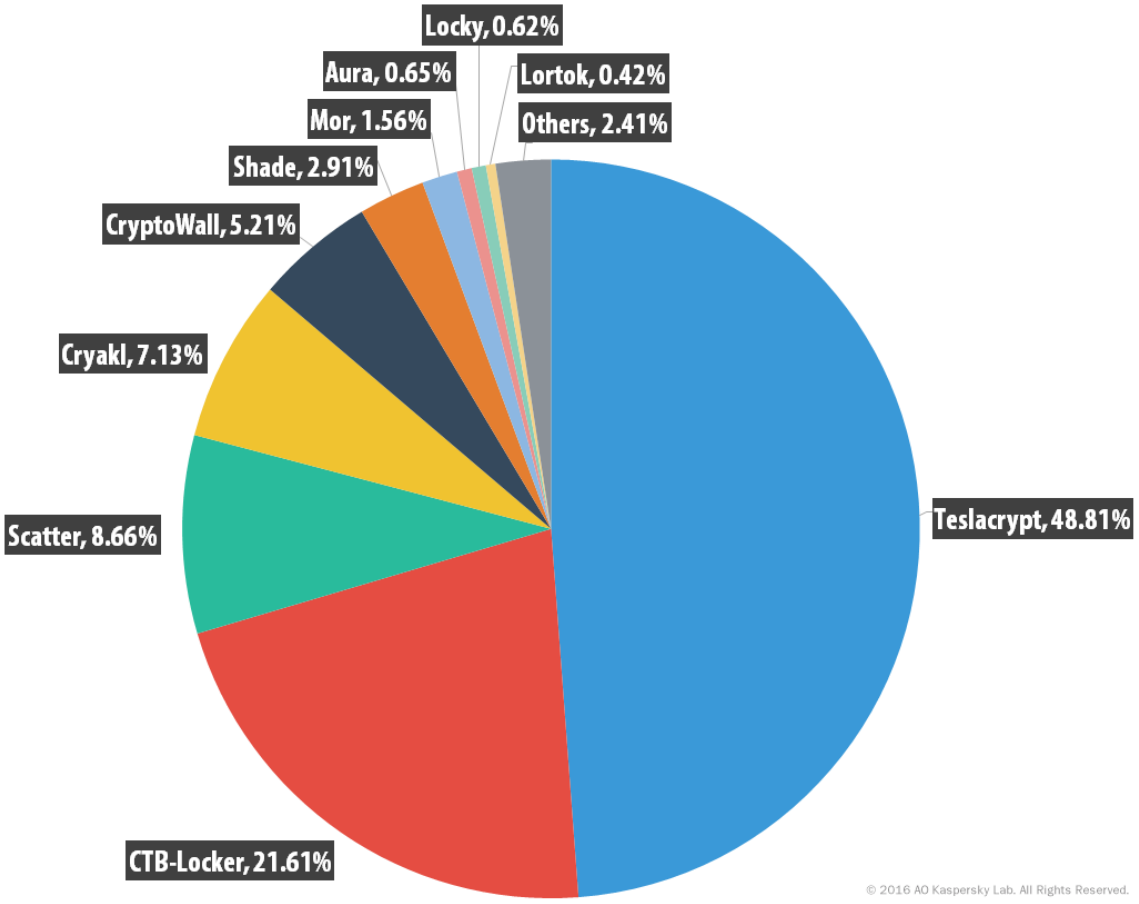

Fig. 4: Distribution of users attacked with different groups of encryption ransomware in 2015-2016

Interestingly, in 2015-2016 the “Others” category decreased to 2.41% of attacked users while a year earlier it had accounted for 22.55%. This drop could be a sign of the development of criminal-to-criminal infrastructure. Instead of developing their own, unique crypto-ransomware, criminals started to purchase off-the-shelf, ready-to-use malware. You can read more about this process in the “How it is done” section of this report. But before that, let’s see what kind of users the malicious actors behind ransomware were after.

Type of users attacked with ransomware

Most ransomware attacks are directed at home users. That was the case with the 2010-blockers epidemic in post-soviet territories, and also for the first period covered by this report. 93.2% of the users who encountered ransomware were users of home products, while the remaining 6.8% were corporate users. In the second period, however, the share of corporate users attacked with ransomware more than doubled to 13.13%, a rise of over 6 percentage points. All “thanks to” encryption ransomware.

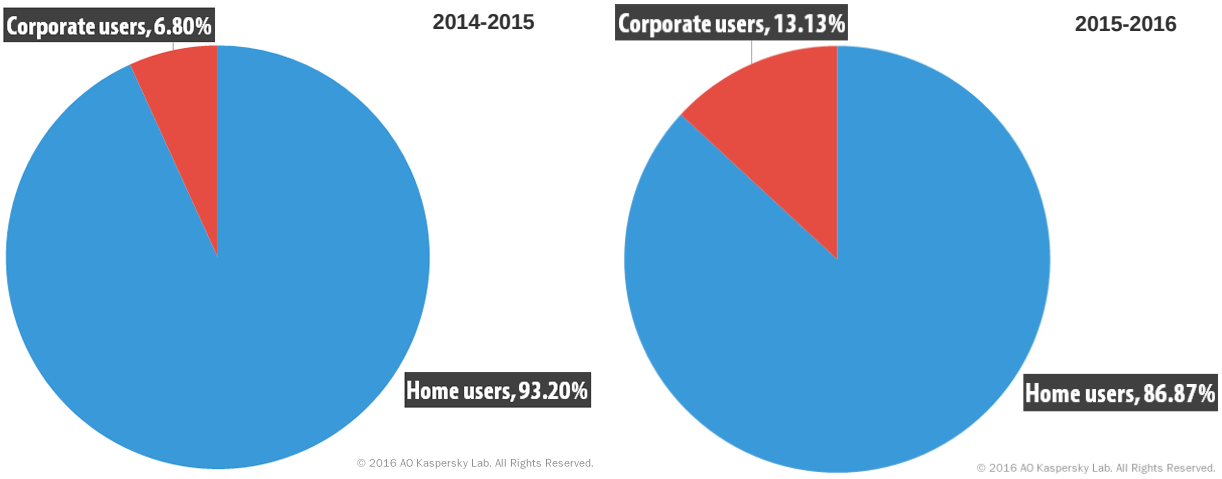

Fig. 5: Type of users encountering ransomware in 2014-2016

When looking at crypto-ransomware, the situation is different: throughout the 24 months covered by the report the share of corporate users attacked with encryptors remained steady at about 20% (rising only slightly to 22.07% in 2015-2016). But this apparent stability is not reflected in the actual numbers.

The number of corporate users attacked with crypto-ransomware increased nearly six-fold (5.86 times): from 27 thousand in 2014-2015 to 158.6 thousand in 2015-2016, with home users hit nearly as hard: up 5.37 times.

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.

As a result, in order to understand accurately 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 2014-2015, 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
Kazakhstan	6.99%
Algeria	6.23%
Ukraine	5.87%
Italy	4.69%
Russian Federation	4.63%
Vietnam	3.86%

India	3.77%
Germany	3.00%
Brazil	2.60%
United States	2.07%

Fig. 6: The list of countries with the biggest share of users attacked with ransomware as a proportion of all users attacked with any kind of malware in 2014-2015

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

One year later, the situation had changed significantly: India moved from 7th to 1st place, with 9.6% of users. The share of Russian users also rose to 6.41%, followed by Kazakhstan, Italy, Germany, Vietnam and Algeria. In the previous year these countries were all in the second half of the Top 10.

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. 7 the list of countries with the biggest share of users attacked with ransomware as a proportion of all users attacked with any kind of malware in 2015-2016

Of these, India, Brazil, Russia and Germany lead the list of countries with the biggest growth in the number of attacked users, while the number in the US, Vietnam, Algeria, Ukraine and Kazakhstan has notably decreased.

Country	2014-2015	2015-2016	Y-to-Y change
Russian Federation	562190	867651	up 54.33%
India	143973	325638	up 126.18%
United States	107755	55679	down 48.33%
Germany	102289	138750	up 35.65%
Vietnam	96092	89247	down 7.12%
Ukraine	69220	39246	down 43.3%
Kazakhstan	62719	39179	down 37.53%
Algeria	61623	38530	down 37.43%

Italy	49400	59130	up 19.7%
Brazil	43674	70078	up 60.46%

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

The above numbers are evidence of the change in the whole Trojan-Ransom category. If we look deeper into the share of users attacked with Trojan-Ransom who experienced an attack by encryption ransomware, the picture becomes significantly different.

Country	% of users attacked with encryption ransomware in 2014-2015	% of users attacked with encryption ransomware in 2015-2016
Russian Federation	6.09%	20.43%
India	3.34%	6.93%
United States	14.27%	39.79 %
Germany	4.64%	94.41%
Vietnam	2.32%	22.87 %
Ukraine	1.34%	28.86%
Kazakhstan	1.14%	25.59%
Algeria	1.18%	13.48 %
Italy	8.93%	89.7%
Brazil	2.56%	31.83%
Other	41.16%	46.3%

Fig. 10: 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.

The ten countries above accounted for 64.14% of all users who encountered any kind of ransomware, and 52.83% of those who encountered cryptors. In 2015-2016 these figures rose to 64.57% and 61.32% respectively.

It is clear from Fig. 10 that during 2014-2015 encryption ransomware was, in most countries (except the US) yet another type of ransomware, with a relatively small percentage of attacked users. A year later, encryption ransomware became much more visible on the threat landscape, increasing its share of attacks by well over 20% in some countries (the US, Brazil, Kazakhstan, Ukraine, Vietnam and Russia). And for some countries, like Germany and Italy, encryption ransomware became almost synonymous with the Trojan-Ransom category.

To conclude the issue of geography, we can say that while, overall, the share of users attacked with malware from Trojan-Ransom barely changed, the actual number of attacked users increased by double digits. Although in some countries the exact number of users attacked with any type of ransomware decreased, there is no country in the list that showed a decrease in the share of users attacked with encryption ransomware. This of course doesn't give a clear answer to the question: Did the actual number of users attacked with encryption ransomware actually increase in these countries or is the increase in the share of users attacked with encryption simply the result of a declining number of users being

attacked with blockers? As can be seen in Fig. 11, the answer is yes, and in some countries, like Germany, Brazil, Ukraine, Kazakhstan and Italy, the growth rate was extremely high, which obviously means that users, especially in these countries should be extremely cautious when surfing the web.

Country	2014-2015	2015-2016	Year-to-Year Change (times)
Russian Federation	34226	177249	+5,18
India	4803	22572	+4,70
United States	15380	22155	+1,44
Germany	4744	96566	+20,36
Vietnam	2230	20409	+9,15
Ukraine	925	11257	+12,17
Kazakhstan	716	10025	+14,00
Algeria	728	5195	+7,14
Italy	4412	53039	+12,02
Brazil	1116	22307	+19,99
Others	61853	277962	+4,49

Fig. 11: the year-on-year growth rate of users attacked with encryption ransomware in the top 10 countries with a higher proportion of such users.

Part 2: Mobile ransomware

Statistics

The activity of mobile ransomware, although not as widely covered in the media as PC ransomware, also skyrocketed over the period covered by this report. Especially in the second half.

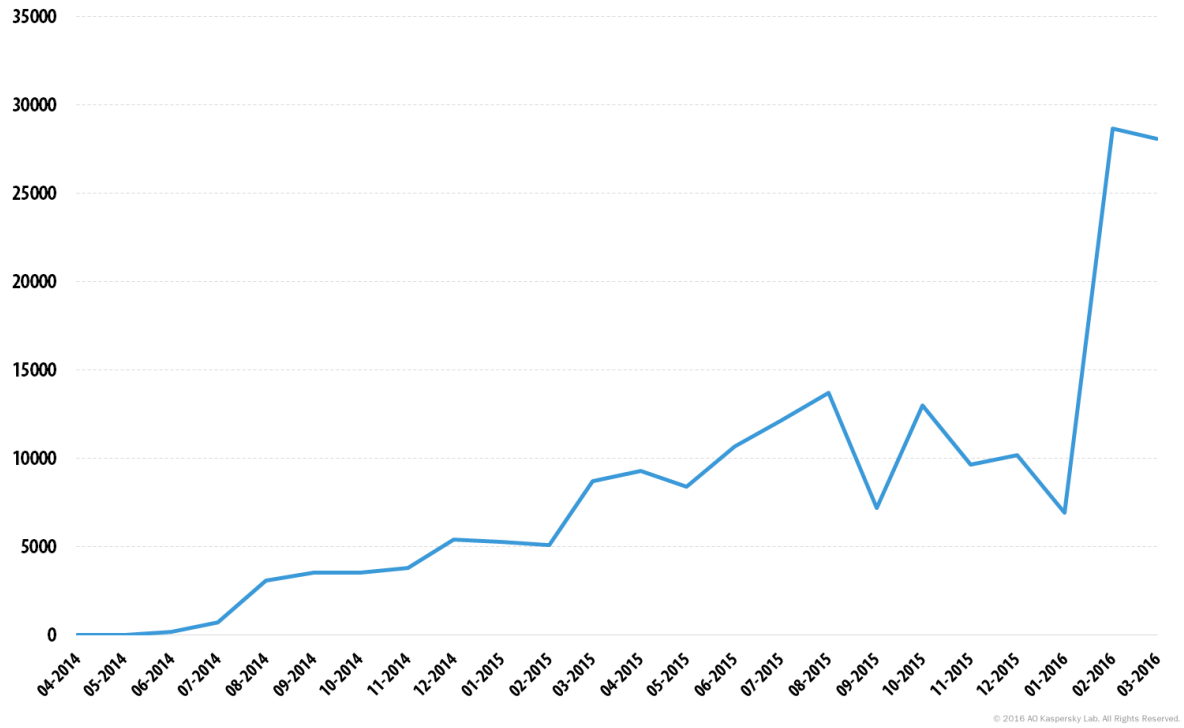

Fig. 12: The number of users encountering mobile ransomware at least once in the period April 2014 to March 2016

From April 2014 to March 2015, Kaspersky Lab security solutions for Android protected 35,413 users from mobile ransomware. A year later the number had increased almost four-fold to136,532 users. The share of users attacked with ransomware as a proportion of users attacked with any kind of malware also increased: from 2.04% in 2014-2015 to 4.63% in 2015-2016. The growth curve may be less that that seen for PC ransomware, but it is still significant enough to confirm a worrying trend.

The geography of mobile ransomware is quite similar to the one for PC ransomware, with a few notable differences. In 2014-2015 the percentage of mobile users attacked with ransomware was fairly low, much lower than that seen for PCs.

Country	% of users attacked with ransomware out of all users encountering malware
United States	10.4%
Kazakhstan	7.8%
Ukraine	6.7%
Germany	4.5%
United Kingdom	2.6%
Russian Federation	2.5%
Belarus	1.7%
S. Arabia	1.6%
Switzerland	1.5%
Brazil	0.16%

Fig. 13: 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 5,000 unique users of Kaspersky Lab products for Android devices). Period: April 2014 – March 2015.

As can be seen in Fig. 13, in 2014-2015 the list of countries where users were most likely to encounter mobile ransomware looked very different to the one based on data for PC users. The United States led the chart with 10.4% of users attacked with ransomware, followed by Kazakhstan (7.8%) Ukraine (6.7%) and Germany (4.5%). Russia was lower down the top ten list, mostly because the local threat landscape at the time was highly affected by Trojan-SMS malware.

In 2015-2016, the list changed significantly, both in terms of the order of countries and in the proportion of users encountering ransomware.

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. 14: 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%).

Clearly the target profile of mobile ransomware is dramatically different to the one for PC ransomware. It is hard to say precisely why this is the case, but we can assume that in countries that feature at the top of the mobile ransomware list, mobile and e-payment infrastructure is much more developed and has deeper penetration than in countries that are at the bottom of the list or not on it at all. Criminals like to get as close to their victim's money as possible and attacking a user who can transfer the ransom in couple of taps or clicks is likely to have the most appeal.

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, Svpeng significantly reduced its activity hitting just a small share of the attacked users.

At some point during 2014-2015, Svpeng - originally known as a banking malware - was modified by its creators to be able to lock an infected device. Since then we have tracked both versions of Svpeng: the banking one and the ransomware. The ransomware branch gained visibly in popularity during 2014-2015, accounting for 5.64% of users attacked with any malware.

This changed during the second period, with the ransomware dropping to the lower end of the Top 30 threats. However, the banking branch of Svpeng resumed activity, which probably means that the malware creators simply lost interest in developing the ransomware and decided to concentrate on the banking one.

Roughly the same thing happened to Pletor – the malware considered to be the first example of ransomware and allegedly created by the authors of the infamous Acecard banking Trojan. In 2014-2015 it secured a fairly visible share of the pie of mobile users attacked with ransomware, but by 2015-2016 it had disappeared from the top, leaving only three big ransomware families on the "market".

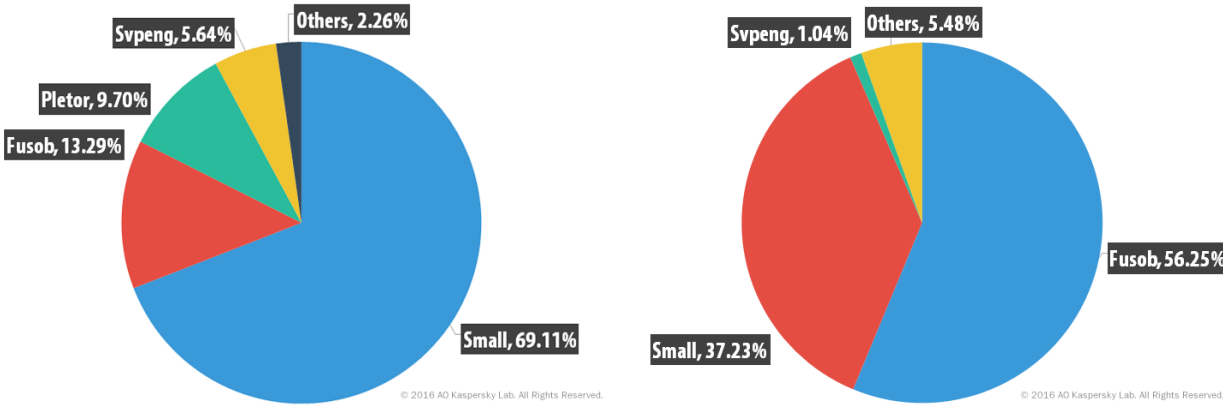

Fig. 15: The distribution of the share of attacked users between the most active mobile ransomware families in 2014-2015 (left) in comparison to the one in 2015-2016 (right).

Another significant thing seen during the 24 months covered by the report was the competition between two big ransomware families: Small and Fusob. In 2014-2015, the Small family was the leader, at least in terms of the share of attacked users. It accounted for 69.11% of all users encountering mobile ransomware at least once. But a year later, the Fusob family had taken over the lead hitting 56.25% of users. The Small family, however, remained number two with 37.23% of attacked users. The Svpeng, Pletor, Small and Fusob malware are likely to be sold by their authors to other cybercriminals or propagated through affiliate networks – all four families have undergone a lot of modifications. However, Small and Fusob appear to have been modified the most and this is clearly visible in the statistics.

Unlike PC ransomware, which is already relatively widely covered by researchers from different companies, including Kaspersky Lab, mobile ransomware has so far not been researched in depth. In order to address this, we provide a brief description of the most widespread and dangerous mobile ransomware examples as of April 2016.

Fusob ransomware

In April 2016, Trojan-Ransom.AndroidOS.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.

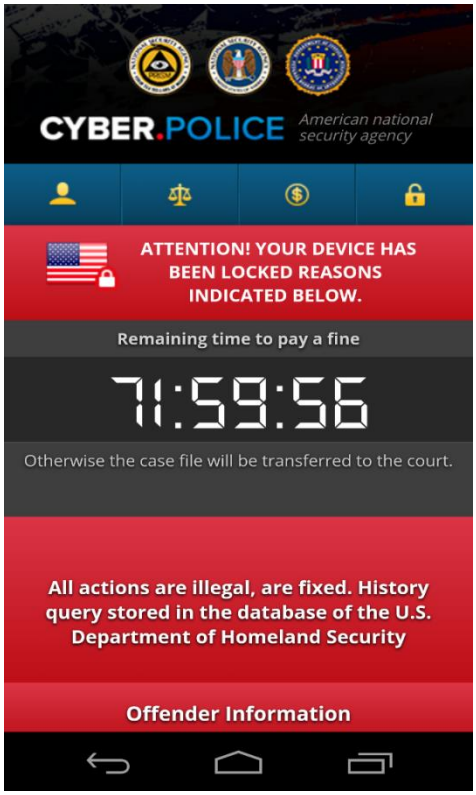

Fig. 16: Message displayed by Fusob ransomware

Trojan-Ransom.AndroidOS.Fusob was most actively distributed in the following countries:

Country	% of users attacked by Fusob
Germany	41.5
United States	14.5
United Kingdom	11.4
Italy	8.8
Mexico	4.4
Canada	3.6
Switzerland	1.9
Netherlands	1.6
Spain	1.4
Japan	1.2

Fig.16: The percentage of users attacked with Fusob ransomware as a proportion of all users attacked with any kind of mobile ransomware

Once the Trojan is executed [?], it runs a check of the device language (Locale.getDefault().getCountry()), and for the following countries it will not perform any malicious actions:

- KZ Kazakhstan
- AZ Azerbaijan

- BG Bulgaria
- GE Georgia
- HU Hungary
- UA Ukraine
- RU Russian Federation
- AM Armenia
- BY Belarus

If the country is not included in the list, the Trojan asks for device administrator rights and displays a message notifying the user that the device is being updated. The device can be still used, but the Trojan blocks access to the device settings by overlaying them with its own window. This is how it protects itself from being removed.

Meanwhile, the Trojan collects information about the device and sends it to the attackers. In doing so, it uploads two different sets of data to the Command and Control (C&C) server. The first set of data contains information about the device, such as device model, the version of the operating system, etc. This data is encoded with the Base64 algorithm and uploaded to the criminals' server. The second data set, among other things, contains the user location and the call log with names from the contact list. This set is encrypted by the AES algorithm and loaded to a malicious C&C server.

The Trojan then waits for the attackers' command with the necessary data to block the device.

For this purpose, the Trojan uses an HTML file received from the C&C. The Trojan itself includes functionality that can be activated from this file.

```
public String getImage()
{
    return fl.poof.comparator.a.c(getContext());
}

public void inst()
{
    fl.poof.comparator.c.q(getContext());
}
```

Fig. 17: A fragment of Fusob ransomware's code

Among several functions integrated into the Trojan, two functions cause particular concern. They are: getImage(), which takes a photo with the help of the device's front camera, and inst() used to install a previously downloaded APK file.

The criminals usually demand between $100 and $200 to unblock the device. The ransom has to be paid in the form of codes from pre-paid iTunes cards.

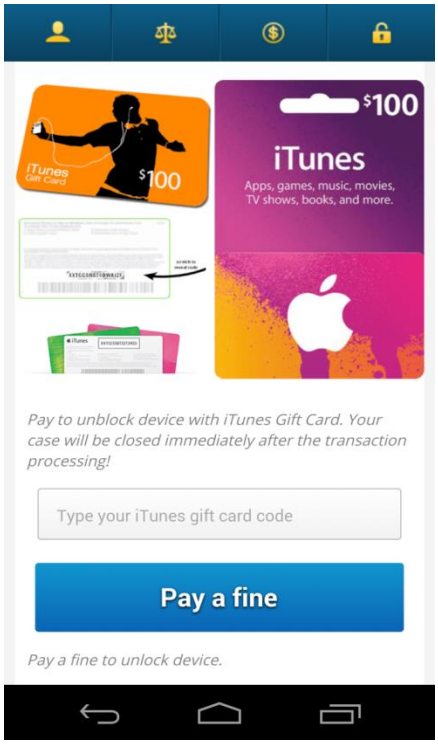

Fig. 18. The dialog window to enter the code of the gift card in exchange for unlocking the device

This family is mainly spread via porn sites; its representatives usually appearing under the name xxxPlayer and mimicking a multimedia player application used for watching porn videos.

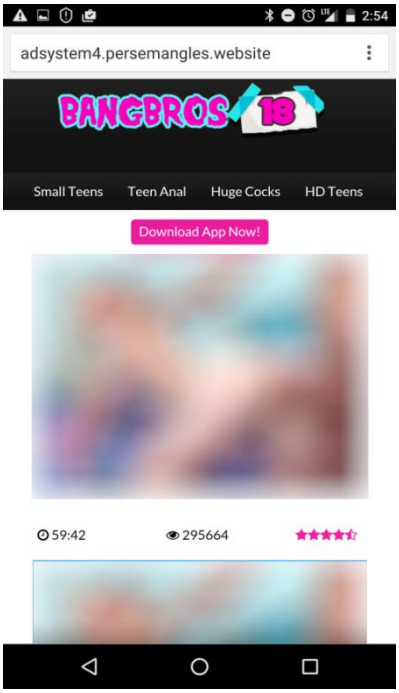

Fig. 19: An example of the kind of webpage through which the Fusob malware is distributed

On clicking the "Download App Now!" button, the Fusob ransom Trojan is downloaded onto the user's device. Interestingly, after a while this site redirected us to another site, which began to extort $100 in a similar way to Fusob.

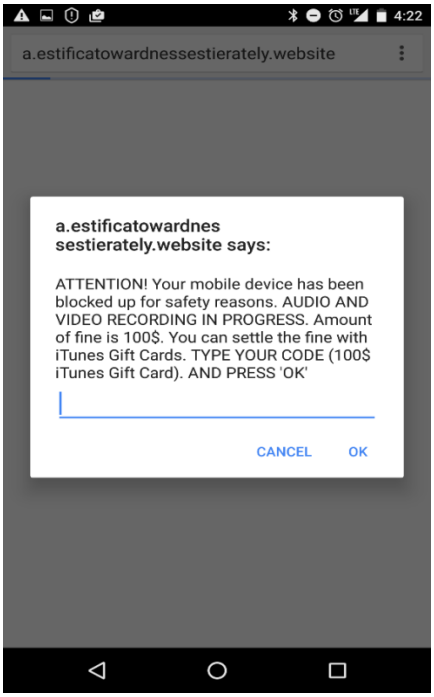

Fig. 20: A web page that appears after the Fusob malware is downloaded.

In addition, a number of cases have been registered recently where an exploit kit was used to deliver this Trojan to Android devices silently in the background.

We have analyzed those sources of infection that were most active at the time of writing this report. Most of them are registered to email addresses in the yandex.ru domain. In addition, the majority of this Trojan's C&C servers are hosted in Russia, or carry registration data that suggests the person who registered them speaks Russian. However, analysis of the large number of modifications of this Trojan, starting from the earliest incarnations, did not provide any evidence that could confirm the authors' language. The only clue we could find in the code of the HTML file used to block the device is some commentary in Russian. All this, along with the fact that the Trojan doesn't attack Russian users, suggests that either the authors of the Trojan or the criminals distributing it are Russian-speaking attackers.

```
// Диалоги тут!
jQuery.fn.select2Buttons = function(options) {
  return this.each(function(){
    var $ = jQuery;
    var select = $(this);
    var multiselect = select.attr('multiple');
    select.hide();
```

Fig. 21: A fragment of Fusob's code pointing at the possible origin of its authors

The Small ransomware

In April 2016, over 12% of attacked users were hit by representatives of the Trojan-Ransom.AndroidOS.Small family, which made it the second most popular ransomware Trojan family. It has been on our radar since mid-June 2014.

Almost 99% of users attacked by this Trojan are located in just three countries:

Country	% of attacked users
Russian Federation	54.6
Kazakhstan	26.9
Ukraine	17.2

Fig. 22: Distribution of infection attempts by the Small ransomware in April 2016

This family can be divided into three main groups:

The first group of the Trojan-Ransom.AndroidOS.Small family includes small and very basic ransom Trojans. Once run, they ask for device administrator rights to prevent the Trojan from being removed. Immediately after that they display a message demanding a ransom which appears on the screen overlaying all other windows. This makes it impossible to use the device.

Fig. 23: Message displayed by the Small ransomware (group 1)

They mainly target Russian-speaking users and demand about 700 to 3,500 rubles to unblock the device. There are also samples targeting English-speaking users. Their functionality is similar, but they demand $300 to unblock the device.

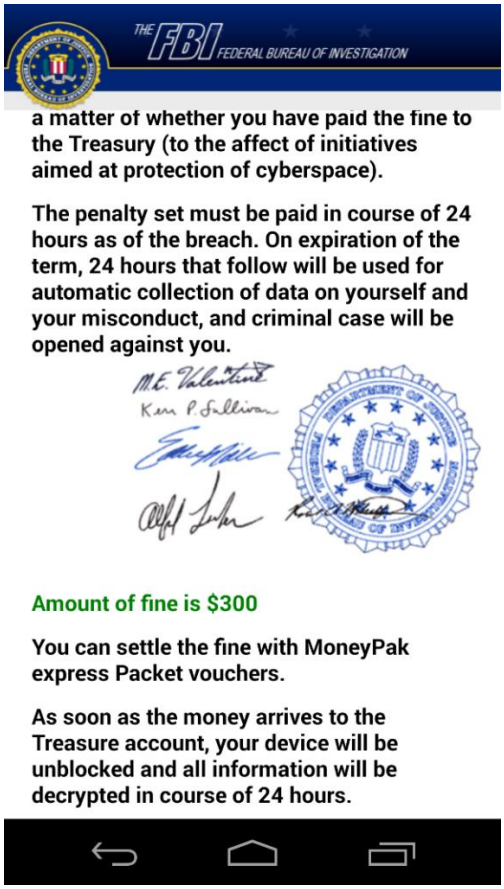

Fig. 24: Message displayed to English-speaking users by the Small ransomware (group 1)

The second group from the Trojan-Ransom.AndroidOS.Small family are encryptors. Their functionality is almost identical to that described above – the only difference is the fact that after blocking the device, they start encrypting files on the memory card.

```
if ((!localFile.getName().endsWith(".enc")) && (!localFile.getName().endsWith(".apk")))
{
  encryptFile(localFile);
  localFile.renameTo(new File(localFile.getAbsolutePath() + ".enc"));
  continue;
  if ((localFile.isDirectory()) && (!localFile.getName().equals("Android"))) {
    collectFiles(localFile.getAbsoluteFile(), paramString);
  }
```

Fig. 25: A fragment of code of the Small ransomware

The third group of the Trojan-Ransom.AndroidOS.Small family is a multifunctional ransomware Trojan. Its behavior depends on the commands it receives from the C&C. Once run, the Trojan asks for the device administrator rights and loads information about the device to a malicious server. This information includes the phone number, the device model, the IMEI, and the version of the operating system. In addition, the Trojan is registered in the

GCM system. The Trojan can receive commands from both the C&C and via GCM. It can perform the following commands:

- START – start the main service of the Trojan
- STOP - stop the main service of the Trojan
- RESTART – restart the main service of the Trojan
- URL – change the C&C address
- MESSAGE – send an SMS to a specified number with a specified text
- UPDATE_PATTERNS – update the rules for processing incoming SMSs
- UNBLOCK – disable the device administrator rights
- UPDATE – download a file form the specified URL and install it
- CONTACTS – send out a specified SMS to all contacts from the list of contacts
- PAGE – address a specified C&C for a command
- ALLMSG – upload all SMSs from the device to the criminals' server
- ALLCONTACTS - upload all contacts from the device to the criminals' server
- ONLINE – address the C&C
- NEWMSG – save a specified SMS on the device
- LOCKER – display text with the ransom demand
- LOCKER_UPDATE – update the text with the ransom demand
- LOCKER_BLOCK – block the device
- LOCKER_UNBLOCK – unblock the device
- CHANGE_GCM_ID – change GCM ID

Once launched, the Trojan also intercepts incoming SMSs. It processes them in accordance with the rules received from the C&C. In addition, it can receive the following commands via SMS:

- 3458 – disable the device administrator rights
- Deblock – unblock the device
- hi - enable mobile data transfer
- ask - disable mobile data transfer
- privet – enable WiFi

- ru – disable WiFi
- 393838 – in addition to the command the message should contain a new encrypted C&C address

In most cases we received similar commands to block the device with a ransom demand to the tune of 1900 rubles.

"command": "job", "data": {"command": "LOCKER", "data":{"payMsg": "To pay the fine, transfer no less than 1,900 rubles to the phone number: +79688343708 from any terminal to top up mobile accounts in Russia! "}}}"

We also received several commands to send SMSs to the number of a major Russian bank. This trick can be used to steal money from a bank account if it is associated with the victim's phone number.

The ransomware Trojans of this family are mainly distributed via porn sites; however, we also registered them in SMS spam.

The C&C registration data, the area where the Trojan is distributed, and the lines of Russian in its code suggest that the Trojan-Ransom.AndroidOS.Small family was developed by Russian-speaking writers.

Svpeng ransomware

Over 97% of users attacked by this family of ransomware Trojans were located in the US. In April 2016, we detected this family in a total of 9 countries. We first discovered this ransomware Trojan family in June 2014 and believe it was created by the same attackers as the banking Trojan Svpeng.

Once run, the Trojan requests device administrator rights. It then collects the information that it requires: the list of calls and the history of visited sites; it also takes a picture with the device camera. Then the Trojan blocks the device by overlaying all windows with an HTML file. With the help of this file it can get access to previously prepared information.

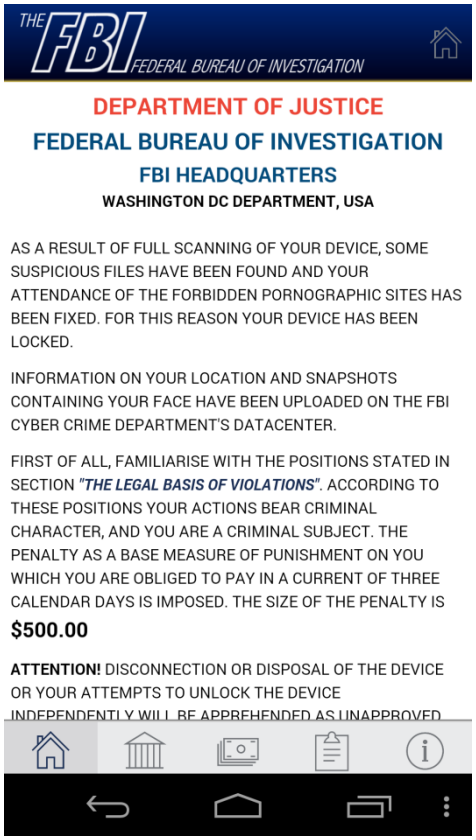

Fig. 26: The message displayed by Svpeng ransomware

In most cases the Trojan demands $500 to unblock the device. Like other groups of mobile ransomware, it is distributed via porn sites.

Differences between PC and mobile ransomware

Unlike PC ransomware, most of the mobile examples are rather simple blockers that use some of the technical features of the Android OS in order to show the window with the ransom message on top of other windows. From time to time Kaspersky Lab researchers discover examples of Android-ransomware capable of encrypting files on the infected device. However, Kaspersky Lab experts don't believe that encryption ransomware for mobile will undergo any noticeable development in the future. This is because of the security features implemented recently into the Android OS, which limits the ability of third-party apps to get unlimited access to users' files. Also, encryption is not as effective on mobile as it is on a PC, because the Android OS and popular Android apps often come with features that enable data to be backed-up automatically to the cloud, which is obviously not the case for PCs.

In short, criminals targeting mobile devices don't need to invest resources in the development of encryption malware, since the damage it can do is limited. The same cannot be said for classic blockers; these are much more efficient on a mobile device than on a PC. The difference is simple: if a PC user encounters blocker ransomware – even a sophisticated one – then in the worst case scenario they will be able to remove the hard drive from the infected PC, attach it to another PC and manually remove all malicious files. It is almost

impossible to do the same with a mobile device as its hardware is impossible to remove easily and analyze with the help of an extraneous device.

Perhaps this is the main reason why the mobile ransomware landscape is mostly a landscape of blockers.

Part 3. How it is done

As mentioned before, crypto-ransomware has existed for years. Sporadic attempts to turn crypto-ransomware into a profitable business-model were spotted by Kaspersky Lab researchers as early as 2006 with the Gpcode ransomware family and the copycats that followed. The approach was standard: after a successful infection, the malicious program would show a ransom message and would demand money, usually a hundred dollars or so, sent through a bank transfer.

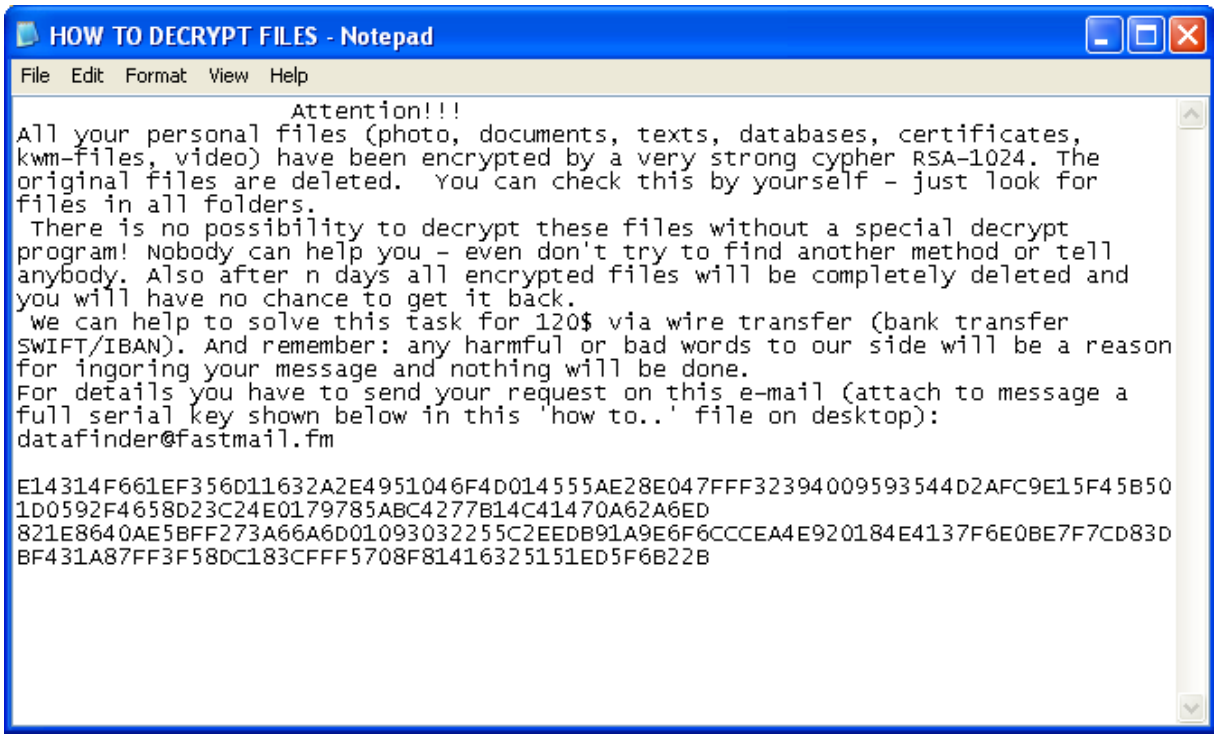

Fig. 27: An example of a message left by criminals on a PC infected with Gpcode-like ransomware, from 2008

But there was no big criminal-to-criminal industry behind those initial attempts to spread crypto-ransomware. Usually it was the work of a single criminal or a small group of criminals, and although in the period from 2006 to 2011, Gpcode or similar samples of crypto-ransomware appeared regularly on our radar, the intensity of attacks at that time cannot be compared with what we see today.

Several years after the last waves of attacks with Gpcode and its followers, crypto-ransomware was chosen by big financial malware actors as a way of earning illegal income. Perhaps the brightest example of this trend was the infamous Gameover Zeus botnet. Originally created for stealing credentials in order to access online banking services, at some point the botnet creators started to use it to infect victims with Cryptolocker ransomware and demand a ransom. The damage done by this botnet was extensive, but luckily, in 2014, following an international effort led by Europol and the FBI, the botnet was shut down.

Allegedly, the ransomware scheme was a sort of side business for the creators of the botnet – a way of monetizing those PCs in the botnet that had no access to online banking systems. A few other groups of criminals known for spreading financial malware have also been spotted undertaking crypto-ransomware activities. But at the end of the day, this model hasn't become widespread and it is not what brought crypto-ransomware to the level of attacks that we see today.

How it works: the business of affiliate networks

It is no secret that most of today's crypto-ransomware has Russian roots, both in terms of the authors of the malicious code and of the actors who spread the malware and demand the ransom. The groups behind ransomware attacks are mainly small or medium-sized and they cooperate by means of a business scheme: affiliate networks.

Small groups often consist of non-professional but very motivated members willing to invest money and time into any cybercriminal activity promising money. Middle-sized groups usually contain some professional programmers and web technology specialists. They are able to produce malware and to build and support the IT infrastructure that forms the technological backbone for the malware.

Over the last few years, middle-sized groups have been able to create several "products" that, in the case of ransomware comprise a kind of DIY set that less-skilled criminals can buy, modify into their own unique version of the malware, and then use to make money. For this they would tune the set in order to make it work with certain C&C servers, encrypt files with certain keys etc. After that they would either try to spread the newly-created malware themselves (investing additional money into buying traffic, spam mailings or renting exploit-kits), or would urge other criminals – entry-level ones – to do this through affiliate programs.

Through this business scheme, multiple affiliates receive a unique version of the malware from the owner of the affiliate network, and take charge of its distribution: spreading it through websites, spam and other ways of propagation. Every time a victim infected with such malware pays the ransom, the affiliate receives some cash from the owner of the network, who gets the lion's share of the ransom.

There is nothing new in the affiliate network business model being used by cybercriminals in order to ease the propagation of malware. In the past, this model has been used to propagate Blockers, SMS-Trojans and of course banking Trojans, along with thousands of different adware and pornware strings.

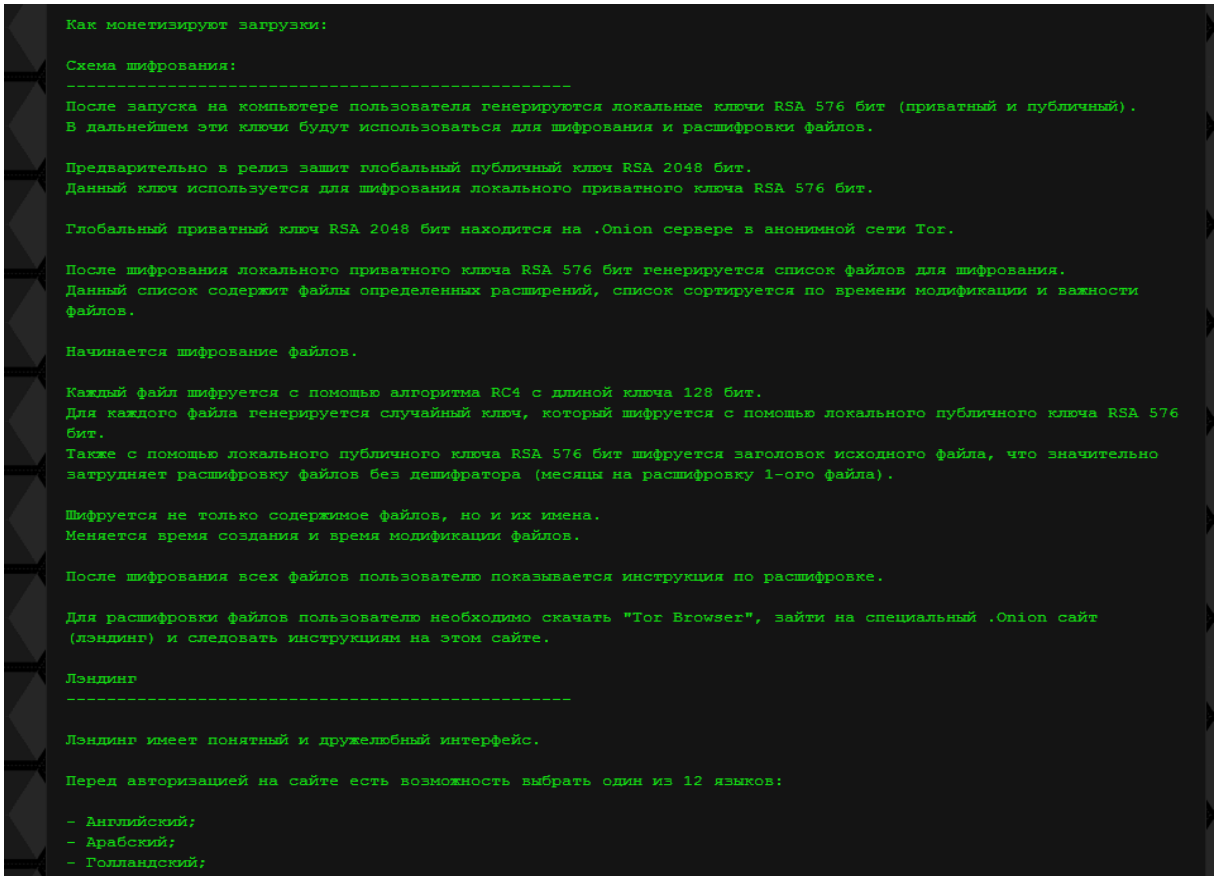

Fig. 28: A description of the capabilities that the affiliate program would give a participant. Along with s strong encryption algorithm, this affiliate program offers its partners a user-friendly interface for a landing page in a Tor-network which would serve as a web-proxy for ransom transactions

This business model appears to be more viable for ransomware than for any other type of malware. The main reason for this is the fact that victims of ransomware tend to pay for releasing their files and thereby pour money into the underground economy of cybercrime.

Why is ransomware skyrocketing?

First and foremost, because users pay.

It seems that in recent years regular users and companies have reached the point where the information stored on their PC is valuable enough to consider paying a ransom on demand. The massive transition in organizations towards the use of digital documents and automated business processes for accounting and other day-to-day activities is helping to accelerate this. A company whose tax documentation, for example is encrypted with ransomware just before the deadline for submitting returns to the tax regulator, has no choice but to pay the ransom – and this is what criminals exploit. As a result, crypto-ransomware has become, almost uniquely, a type of malware that can cause tangible business damage by making critical operational files unreadable. This damage cannot not always be rolled back, so sometimes paying the ransom is the only way to retrieve the data.

Another important factor which has positively affected the rise of ransomware is the appearance of new payment tools. New crypto-currencies, for example are now often

accompanied by how-to-use guides “for dummies” that teach mainstream users how to use such currencies.

In the past, cybercriminals tended to use either legitimate payment systems or semi-legitimate services in order to transfer money to each other and from their victims. The problem for criminals is that legitimate payment systems, reacting to the rise in fraudulent payments, have started to track and block suspicious transactions, making money transfer a far more risky business for cyber-crooks.

With underground and semi-legal payment systems the problem is that no guarantees are given to the users of such systems (no refunds, no protection from other criminals) and the privacy of these transactions is also always questionable. At the end of the day the fate of each known underground payment system (from E-gold to Liberty Reserve) is always the same: sooner or later it goes down, due to a law enforcement investigation or some other reason.

That is why money transaction for cybercriminals has always been an area of risk. But things changed significantly when the price of crypto-currencies – bitcoin in particular – rose and stabilized enough to allow a lot of users to convert real money. Criminals have started to exploit the advantages crypto-currencies over other type of e-currency: anonymity and a distributed nature, which both allow them to hide fraudulent transactions and make it impossible for a law enforcement agency to do anything, as the system has no center and no owner. These features help to support individual privacy rights but, unfortunately also give cybercriminals a very reliable and secret payment tool. The main outcome of this is that ransomware has become the new black in the underground.

It has acquired a fairly viable criminal ecosystem where, powered by money from attacked users, specific niches for different types of criminals have emerged. Affiliate networks have become the main way for all of them to generate profit. And – what is more dangerous – they have opened doors to the criminal world for those who doesn’t have enough knowledge and expertise to develop their own ransomware. With multiple affiliate networks on the market, they need only basic skills in programming and web design.

Another important reason for the rise in crypto-ransomware is the fact that law enforcement can find it difficult to respond. Most victims of cryptors are ordinary people who do not always report the attack to the police. This leaves law enforcement agencies and forensic experts with a very limited amount of evidence to work with: law enforcement representatives generally have too few reported cases to justify an investigation, and forensic specialists lack enough actual evidence to use against the actors behind crypto-ransomware. At Kaspersky Lab we are eager to change this situation and we are ready to help law enforcement agencies and other interested organizations with technical analyses of malware. The pressure of the law is a valuable tool in the fight against ransomware. This was proven by the case against the criminals who spread screen blocker malware in 2010. The arrests that took place in August 2010 in Russia showed other cyber-criminals that the consequences of their actions could be severe. The wave of screen blockers started to fade after those arrests and we believe that the same approach would work with crypto-ransomware criminals.

Conclusions and Predictions

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

- On PCs, encryption ransomware has removed blockers from the threat landscape making the Trojan-Ransom category almost synonymous with encryption ransomware.

- In contrast, mobile ransomware is all about malware with the ability to lock the screen of the device, and it is unlikely that crypto-ransomware for mobile devices will gain in popularity among cybercriminals anytime soon.

- Although the statistics show that attacks with crypto-ransomware operate on a massive scale, responsibility for most of the attacks rests with just a few groups of malware, most of them spread via affiliate programs.

- One of the main reasons for the current skyrocketing of encryption ransomware is the availability of off-the-shelf sets for the creation of new versions of ransomware. As was the case with blockers and banking Trojans, encryptors are the new black of the cybercriminal underground.

- Payment and infrastructure anonymity tools help criminals to leverage ransomware schemes with a relatively low of risk of being compromised. That, combined with the availability of plug-and-play malicious tools has brought a lot of low-skilled cybercriminals into the market.

Alongside 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. Mobile ransomware emerged as a follow-up to PC ransomware and it is likely that it will be followed-up with malware targeting devices that are very different to a PC or a smartphone. These could be connected devices: like smart watches, smart TVs, and other smart products including home and in-car entertainment systems. There are a few proof-of-concepts for some of these devices, and the appearance of actual malware targeting smart devices is only a question of time.

- As legal action is one of the few way to actually disrupt the activity of groups behind crypto-ransomware, more arrests of ransomware dealers will take place. In 2015, Kaspersky Lab assisted the Dutch police in the investigation of the CoinVault

ransomware attacks. The result of this investigation was the arrest of two suspects and the publication of decryption keys online.

    - New arrests are a must for an effective fight against crypto-ransomware as they significantly increase the risks for criminals embarking on such malicious activity.

- Technologies to protect users from encryption ransomware will be created. Kaspersky Lab products are equipped with special technology that can detect an attempt by an unknown application to encrypt files, and create back-up copies of these files, thus saving users' data. We expect similar technologies to be created by other security vendors.

What to do in order to protect yourself from crypto-ransomware attacks

While crypto-ransomware is one of the most dangerous types of malware ever created, and the consequences of it could be really severe, we at Kaspersky Lab believe that there are ways to protect yourself or your organization against this threat.

Tips to consumers:

- Back-up is a must. If you ever thought that one day you would finally download and install that strange boring back-up software, today is the day. The sooner back-up becomes yet another rule in your day-to-day PC activity, the sooner you will become invulnerable to any kind of ransomware

- Use a reliable security solution. And when using it do not turn off the advanced security features which it most certainly has. Usually these are features that enable the detection of new ransomware based on its behavior.

- Keep the software on your PC up-to-date. Most widely-used programs (Flash, Java, Chrome, Firefox, Internet Explorer, Microsoft Windows and Office) have an automatic updates feature. Keep it turned on, and don't ignore requests from these applications for the installation of updates.

- Keep an eye on files you download from the Internet. Especially from untrusted sources. In other words, if what is supposed to be an mp3 file has an .exe extension, it is definitely not a musical track but malware. The best way to be sure that everything is fine with the downloaded content is to make sure it has the right extension and has successfully passed the checks run by the protection solution on your PC.

- Keep yourself informed of the new approaches cyber-crooks use to lure their victims into installing malware. For this, read the news and specialized information resources like Kaspersky Lab's Securelist.com and Kaspersky Daily.

- If for some reason your files are encrypted with ransomware and you are asked to a pay ransom, don't pay. Every bitcoin transferred to the hands of criminals builds their confidence in the profitability of this kind of cybercrime, which in its turn leads to the creation of new ransomware. At the same time, a lot of security companies, including Kaspersky Lab fight ransomware on daily basis. Sometimes it is possible to create a decryption tool for certain kinds of ransomware, and sometimes as a result of cooperation with law enforcement agencies, it becomes possible to get the encryption keys for certain families of ransomware, which could eventually lead to decryption of your files. Last but not least: the creation, spreading and demanding of a ransom for decryption are all actions that are defined as criminal in most countries around the globe. Report an attack to the police in order to start an investigation.

Tips to businesses

- Back-up is a must. Upon the infection of your corporate PCs, the ransomware is likely to start encrypting files that are required for the daily work of your company. If it is technically impossible to back-up all the files you have in the corporate network, choose the most critical (accounting documents, clients' data, legal documents etc.), isolate them and back-up regularly.

- Use a reliable, corporate-grade security solution and don't switch off its advanced features, as these enable it to catch unknown threats.

- Educate your personnel: very often the ransomware infection happens due to a lack of knowledge about common cyberthreats and the methods criminals use to infect their victims.

- Undertake regular patch management.

- Avoid paying a ransom and report the attack to police.

Kaspersky Lab offers multi-layered protection against this widespread increasing threat. Kaspersky Lab's solutions combat all known types of ransomware to secure user's data. When these solutions are in place, most ransomware is "caught" when it is attempting to penetrate a device. Nonetheless, even if malware does manage to sneak through, there is another layer of protection – System Watcher technology – that is able to block and roll back malicious changes made on a device, such as the encryption of files or blocked access to the monitor.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy