KASPERSKY lab

IT THREAT EVOLUTION IN Q2 2016

David Emm, Roman Unuchek, Maria Garnaeva, Anton Ivanov, Denis Makrushin, Fedor Sinitsyn

Contents

Overview

Targeted attacks and malware campaigns

Cha-ching! Skimming off the cream

Earlier in the year, as part of an incident response investigation, we uncovered a new version of the Skimer ATM malware. The malware, which first surfaced in 2009, has been re-designed. So too have the tactics of the cybercriminals using it. The new ATM infector has been targeting ATMs around the world, including the UAE, France, the United States, Russia, Macau, China, the Philippines, Spain, Germany, Georgia, Poland, Brazil and the Czech Republic.

Rather than the well-established method of fitting a fake card-reader to the ATM, the attackers take control over the whole ATM. They start by installing the Skimer malware on the ATM – either through physical access or by compromising the bank's internal network. The malware infects the ATM's core – the part of the device responsible for interaction with the wider bank infrastructure, card processing and dispensing of cash. In contrast to a traditional card skimmer, there are no physical signs that the ATM is infected, leaving the attackers free to capture data from cards used at the ATM (including a customer's bank account number and PIN) or steal cash directly.

The cybercriminal 'wakes up' the infected ATM by inserting a card that contains specific records on the magnetic stripe. After reading the card, Skimer is able execute a hard-coded command, or receive commands through a special menu activated by the card. The Skimer user interface appears on the display only after the card is ejected and only if the cybercriminal enters the correct session key within 60 seconds. The menu offers 21 different options, including dispensing money, collecting details of cards that have been inserted in the ATM, self-deletion and performing updates. The cybercriminal can save card details on the chip of their card, or print the details it has collected.

The attackers are careful to avoid attracting attention. Rather than take money directly from the ATM – which would be noticed immediately – they wait (sometimes for several months) before taking action. In most cases, they collect data from skimmed cards in order to create cloned cards later. They use the cloned cards in other, non-infected ATMs, casually withdrawing money from the accounts of the victims in a way that can't be linked back to the compromised ATM.

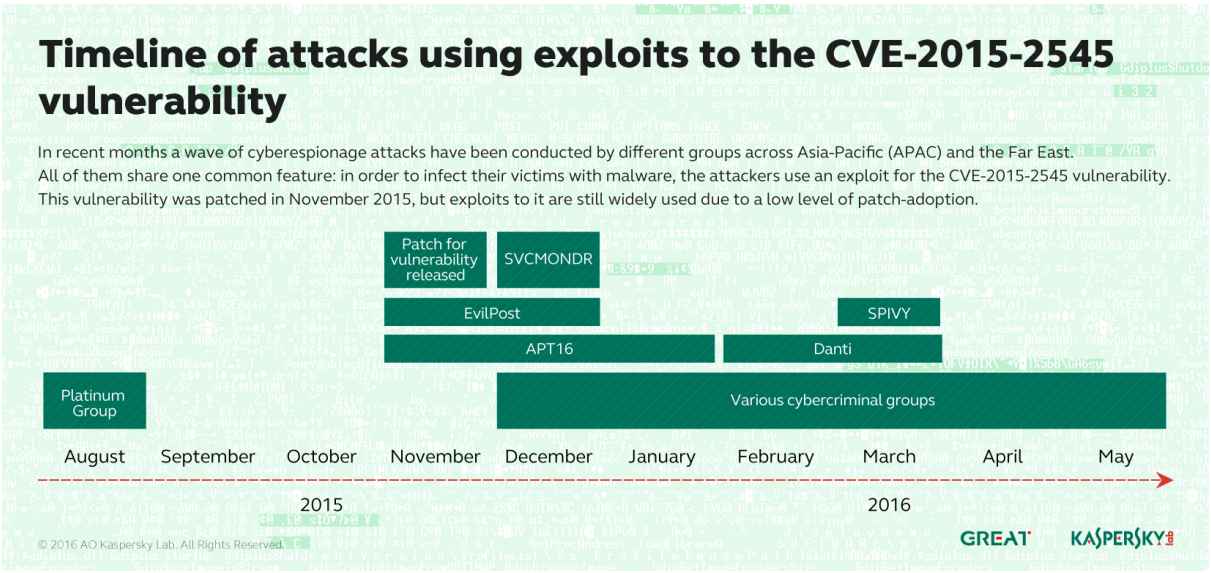
Kaspersky Lab has several recommendations to help banks protect themselves. They should carry out regular anti-virus scans; employ whitelisting technologies; apply a good device management policy; make use of full disk encryption; password protect the BIOS of ATMs; enforce hard disk booting and isolate the ATM network from the rest of the bank infrastructure. The magnetic strip of the card used by the cybercriminals to activate the malware contains nine hard-coded numbers. Banks may be able

to proactively look for these numbers within their processing systems: so we have shared this information, along with other Indicators of Compromise (IoCs).

In April, one of our experts provided an in-depth examination of ATM jackpotting and offered some insights into what should be done to secure these devices.

New attacks, *old* exploit

In recent months we have been tracking a wave of cyber-espionage attacks conducted by different APT groups across the Asia-Pacific and Far East regions. They all share one common feature: they exploit the CVE-2015-2545 vulnerability. This flaw enables an attacker to execute arbitrary code using a specially crafted EPS image file. It uses PostScript and can evade the Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP) protection methods built into Windows. The Platinum, APT16, EvilPost and SPIVY groups were already known to use this exploit. More recently, it has also been used by the Danti group.



Danti, first identified in February 2016 and still active, is highly focused on diplomatic bodies. The group predominantly targets Indian government organizations, but data from the Kaspersky Security Network (KSN) indicates that it has also infected targets in Kazakhstan, Kyrgyzstan, Uzbekistan, Myanmar, Nepal and the Philippines.

The exploit is delivered using spear-phishing e-mails spoofed to look as though they have been sent by high-ranking Indian government officials. When the victim clicks on the attached DOCX file, the Danti backdoor is installed, allowing the attackers to capture sensitive data.

The origin of the Danti group is unclear, but we suspect that it might be connected to the NetTraveler and DragonOK groups: it's thought that Chinese-speaking hackers are behind these attacks.

Kaspersky Las has also seen another campaign that makes use of the CVE-2015-2545 vulnerability: we've called this SVCMONDR after the Trojan that is downloaded once the attackers get a foothold in the victim's computer. This Trojan is different to the one used by the Danti group, but it shares some common features with Danti and with APT16 – the latter is a cyber-espionage group believed to be of Chinese origin.

One of the most striking aspects of these attacks is that they are successfully making use of a vulnerability that was patched by Microsoft in September 2015. In November, we predicted that APT campaigns would invest less effort in developing sophisticated tools and make greater use of off-the-shelf malware to achieve their goals. This is a case in point: using a known vulnerability, rather than developing a zero-day exploit. This underlines the need for companies to pay more attention to patch management to secure their IT infrastructure.

New attack, *new* exploit

Of course, there will always be APT groups that seek to take advantage of zero-day exploits. In June, we reported on a cyber-espionage campaign – code-named 'Operation Daybreak' and launched by a group named ScarCruft – that uses a previously unknown Adobe Flash Player exploit (CVE-2016-1010). This group is relatively new and has so far managed to stay under the radar. We think the group might have previously deployed another zero-day exploit (CVE-2016-0147) that was patched in April.

The group have targeted a range of organizations in Russia, Nepal, South Korea, China, India, Kuwait and Romania. These include an Asian law enforcement agency, one of the world's largest trading companies, a mobile advertising and app monetization company in the United States, individuals linked to the International Association of Athletics Federations and a restaurant located in one of Dubai's top shopping centres. The attacks started in March 2016: since some of them are very recent, we believe that the group is still active.

The exact method used to infect victims is unclear, but we think that the attackers use spear-phishing e-mails that point to a hacked website hosting the exploit. The site performs a couple of browser checks before redirecting victims to a server controlled by the hackers in Poland. The exploitation process consists of three Flash objects. The one that triggers the vulnerability in Adobe Flash Player is located in the second SWF file delivered to the victim. At the end of the exploitation chain, the server sends a legitimate PDF file, called 'china.pdf', to the victim: this seems to be written in Korean.

The attackers use a number of interesting methods to evade detection, including exploiting a bug in the Windows Dynamic Data Exchange (DDE) component in order to bypass security solutions – a method not seen before. This flaw has been reported to Microsoft.

Flash Player exploits are becoming rare, because in most cases they need to be coupled with a sandbox bypass exploit – this makes them tricky to do. Moreover, although Adobe is planning to drop Flash support soon, it continues to implement new mitigations to make exploitation of Flash Player

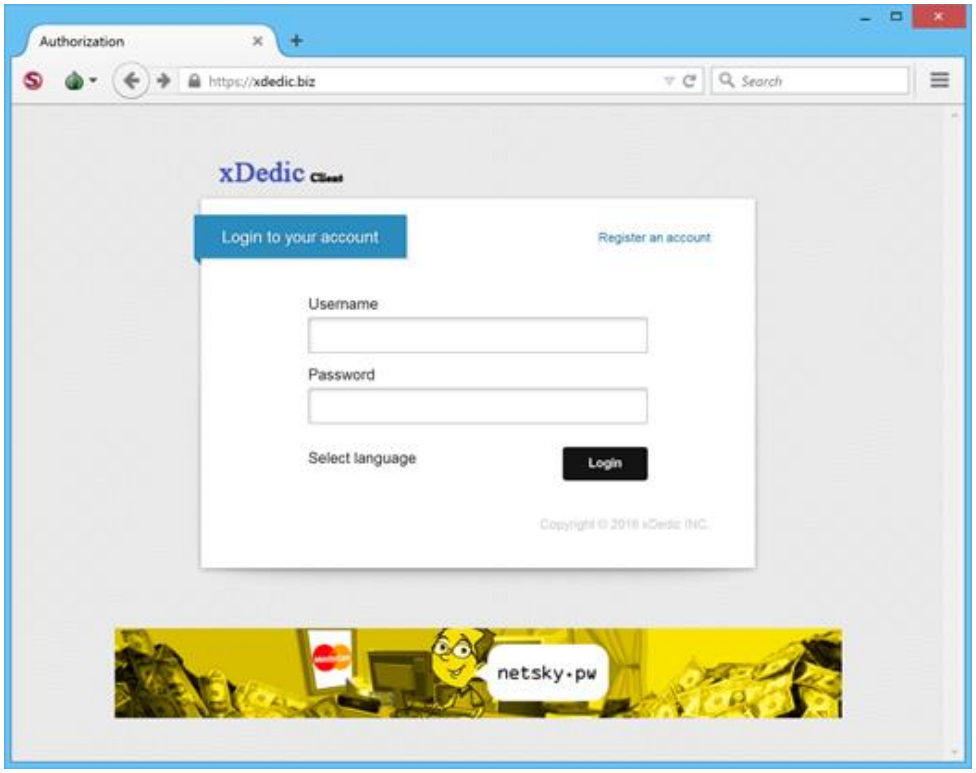
increasingly difficult. Nevertheless, resourceful groups such as ScarCruft will continue to try and find zero-day exploits to target high-profile victims.

While there's no such thing as 100 per cent security, the key is to increase security defences to the point that it becomes so expensive for an attacker to breach them that they give up or choose an alternative target. The best defence against targeted attacks is a multi-layered approach that combines traditional anti-virus technologies with patch management, host-based intrusion prevention and a default-deny whitelisting strategy. According to a study by the Australian Signals Directorate, 85 per cent of targeted attacks analysed could have been stopped by employing four simple mitigation strategies: application whitelisting, updating applications, updating operating systems and restricting administrative privileges.

Kaspersky Lab products detect the Flash exploit as 'HEUR:Exploit.SWF.Agent.gen'. The attack is also blocked proactively by our Automatic Exploit Prevention (AEP) component. The payloads are detected as 'HEUR:Trojan.Win32.ScarCruft.gen'.

XDedic: APT-as-a-Service

Kaspersky Lab recently investigated an active cybercriminal trading platform called xDedic, an online black market for hacked server credentials around the world – all available through the Remote Desktop Protocol (RDP). We initially thought that this market extended to 70,000 servers, but new data suggests that the XDedic market is much wider – including credentials for 176,000 servers. XDedic includes a search engine, enabling potential buyers to find almost anything – from government and corporate networks – for as little as $8 per server. This low price provides 'customers' with access to data on such servers and their use as a bridgehead for further targeted attacks.



The owners of the 'xdedic[.]biz' domain claim that they have no relation to those selling access to hacked servers – they are simply selling a secure trading platform for others. The XDedic forum has a separate sub-domain, 'partner[.]xdedic[.]biz', for the site's 'partners' – that is, those selling hacked servers. The Xdedic owners have developed a tool that automatically collects information about the system, including websites available, software installed and more. They also provide others tools to its partners, including a patch for RDP servers to support multiple logins for the same user and proxy installers.

The existence of underground markets is not new. But we are seeing a greater level of specialisation. And while the model adopted by the XDedic owners isn't something that can be replicated easily, we think it's likely that other specialized markets are likely to appear in the future.

Data from KSN helped us identify several files that were downloaded from the XDedic partner portal: Kaspersky Lab products detect these files as malicious. We have also blacklisted the URLs of control servers used for gathering information about the infected systems. Our detailed report on XDedic contains more information on hosts and network-based IoCs.

Lurking around the Russian Internet

Sometimes our researchers find malware that is particular about where it infects. On the closed message boards used by Russian cybercriminals, for example, you sometimes see the advice 'Don't work with RU' – offered by experienced criminals to the younger generation: i.e. don't infect Russian computers, don't steal money from Russians and don't use them to launder money. There are two

good reasons for this. First, online banking is not as common as it is in the west. Second, victims outside Russia are unlikely to lodge a complaint with the Russian police – assuming, of course, that they even know that Russian cybercriminals are behind the malware that has infected them.

But there are exceptions to every rule. One of these is the Lurk banking Trojan that has been used to steal money from victims in Russia for several years. The cybercriminals behind Lurk are interested in telecommunications companies, mass media and news aggregators and financial institutions. The first provide them with the means to transfer traffic to the attackers' servers. The news sites provide them with a way to infect a large number of victims in their 'target audience' – i.e. the financial sector. The Trojan's targets appear to include Russia's four largest banks.

The primary method used to spread the Lurk Trojan is drive-by download, using the Angler exploit pack: the attackers place a link on compromised websites that leads to a landing page containing the exploit. Exploits (including zero-days) are typically implemented in Angler before being used in other exploit packs, making it particularly dangerous. The attackers also distribute code through legitimate websites, where infected files are served to visitors from the .RU zone, but others receive clean files. The attackers use one infected computer in a corporate network as a bridgehead to spread across the organization. They use the legitimate PsExec utility to distribute the malware to other computers; and then use a mini-dropper to execute the Trojan's main module on the additional computers.

There are a number of interesting features of the Lurk Trojan. One distinct feature, that we discussed soon after it first appeared, is that it is 'file-less' malware, i.e. it exists only in RAM and doesn't write its code to the hard drive.

The Trojan is also set apart because it is highly targeted. The authors do their best to ensure that they infect victims that are of interest to them without catching the attention of analysts or researchers. The incidents known to us suggest Lurk is successful at what it was designed for: we regularly receive reports of thefts from online banking systems; and forensic investigations after the incidents reveal traces of Lurk on the affected computers.

Malware stories

Cybercriminals get ready for Rio

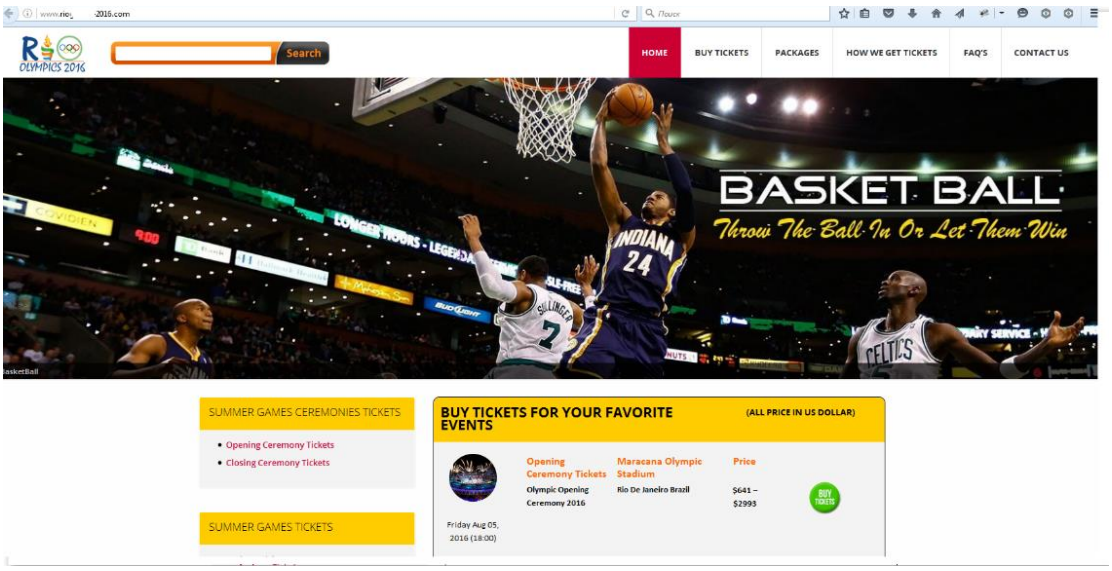
Fraudsters are always on the lookout for opportunities to make money off the back of major sporting events, so it's no surprise that we've seen an increase in cybercriminal activity related to the forthcoming Olympic Games in Brazil.

We've seen an increase in spam e-mails. The spammers try to cash in on people's desire to watch the games live, sending out messages informing the recipient that they have won a (fake) lottery

(supposedly organized by the International Olympic Committee and the Brazilian government): all they need to do to claim their tickets is to reply to the e-mail and provide some personal details.

View the attached file

Some messages point to fake websites, like this one offering direct sale of tickets without the need to make an application to the official lottery:



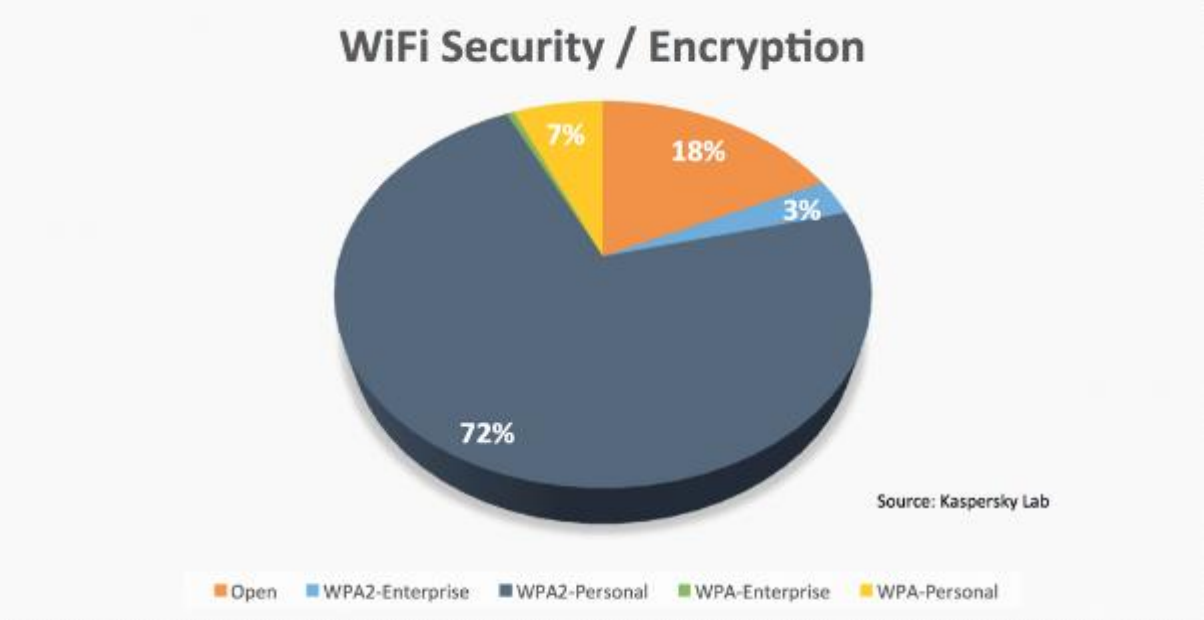
These fake ticketing sites are very convincing. Some fraudsters go the extra mile by obtaining legitimate SSL certificates to provide a secure connection between the victim's browser and the site – displaying 'https' in the browser address bar to lure victims into a false sense of security. The scammers inform their victims that they will receive their tickets two or three weeks before the event, so the victim doesn't become suspicious until it's too late and their card details have been used by the

cybercriminals. Kaspersky Lab is constantly detecting and blocking new malicious domains, many of which include 'rio' or 'rio2016' in the title.

It's too late to buy tickets through official channels, so the best way to see the games is to watch on TV or online. We advise everyone to beware of malicious streaming websites – probably the last-ditch attempt by cybercriminals to scam people out of their money.

Cybercriminals also take advantage of our desire to stay connected wherever we go – to share our pictures, to update our social network accounts, to find out the latest news or to locate the best places to eat, shop or stay. Unfortunately, mobile roaming charges can be very high, so often people look for the nearest Wi-Fi access point. This is dangerous, because data sent and received over an open Wi-Fi network can be intercepted. So passwords, PINs and other sensitive data can be stolen easily. On top of this, cybercriminals also install fake access points, configured to direct all traffic through a host that can be used to control it – even functioning as a 'man-in-the-middle' device that is able to intercept and read encrypted traffic.

To gauge the extent of the problem, we drove by three major Rio 2016 locations and passively monitored the available Wi-Fi networks that visitors are most likely to try and use during their stay – the Brazilian Olympic Committee building, the Olympic Park and the Maracana, Maracanazinho and Engenhao stadiums. We were able to find around 4,500 unique access points. Most are suitable for multimedia streaming. But around a quarter of them are configured with weak encryption protocols: this means that attackers can use them to sniff the data of unsuspecting visitors that connect to them.



To reduce your exposure, we would recommend any traveller (not just those who plan to visit Rio!) to use a VPN connection, so that data from your device travels to the Internet through an encrypted data channel. Be careful though. Some VPNs are vulnerable to DNS leak attacks – meaning that, although your immediate sensitive data is sent via the VPN, your DNS requests are sent in plain text to the DNS

servers set by the access point hardware. This would allow an attacker to see what you're browsing and, if they have access to the compromised Wi-Fi network, define malicious DNS servers – i.e. letting them redirect you from a legitimate site (your bank, for example) to a malicious site. If your VPN provider doesn't support its own DNS servers, consider an alternative provider or a DNSCrypt service.

There's one other thing that we need if we want to stay connected – electricity: we need to keep our mobile devices charged. Today you can find charging-points in shopping centres, airports and even taxis. Typically they provide connectors for leading phone models, as well as a USB connector that a visitor can use with their own cable. Some also provide a traditional power supply that can be used with a phone charger.

But remember that you don't know what's connected to the other end of the USB connector. If an attacker compromises the charging-point, they can execute commands that allow them to obtain information about your device, including the model, IMEI number, phone number and more: information they can use to run a device-specific attack that would then enable them to infect the device. You can find more information about the data that's transmitted when you connect a device using USB and how an attacker could use it to compromise a mobile device.

This doesn't mean that you shouldn't charge your device when you're away from home. But you should take steps to protect yourself. It's always best to use your own charger, rather than using charging cables at a public charging-point or buying one from an unknown source. You should also use a power outlet, instead of a USB socket.

Cybercriminals also continue to exploit established ways to make money. This includes using ATM skimmers to steal credit card data. The most basic skimmers install a card reader and a camera to record the victim's PIN. The best way to protect yourself from this is to cover the keypad as you enter your PIN. However, sometimes cybercriminals replace the whole ATM, including the keypad and screen, in which case the typed password is stored on the fake ATM system. So it's also important to check the ATM before you insert your card. Check to see if the green light on the card reader is on: typically, they replace the card reader with a version where there is no light, or it's switched off. Also check the machine to see if there is anything suspicious, such as missing or broken parts.

Card cloning is another problem facing visitors to Rio 2016. While chip-and-PIN makes life harder for cybercriminals, it's possible for them to exploit flaws in the EMV transaction implementation. It's difficult to protect yourself against this type of attack, because usually the point-of-sale is modified in order to save the data – to be collected later by the cybercriminals. Sometimes they don't need physical access to extract the stolen data, as they collect it via Bluetooth. However, there are some steps you can take to reduce your exposure to this type of attack. Sign up for SMS notifications of card transactions from your bank, if they provide this service. Never give your card to the retailer: if they can't bring the machine to you, go to the machine. If the device looks suspicious, use a different payment method. Before typing your PIN, make sure you're on the card payment screen and ensure that your PIN isn't going to be displayed on the screen.

Ransomware: backup or pay up?

Towards the end of last year, we predicted that ransomware would gain ground on banking Trojans – for the attackers, ransomware is easily monetized and involves a low cost per victim. So it's no surprise that ransomware attacks are increasing. Kaspersky Lab products blocked 2,315,931 ransomware attacks between April 2015 and April 2016 – that's an increase of 17.7 per cent on the previous year. The number of cryptors (as distinct from blockers) increased from 131,111 in 2014-15 to 718,536 in 2015-16. Last year, 31.6 per cent of all ransomware attacks were cryptors. You can find further

information, including an overview of the development of ransomware, in our KSN Report: PC ransomware in 2014-16.

Most ransomware attacks are directed at consumers – 6.8 per cent of attacks in 2014-15 and 13.13 percent in 2015-16 targeted the corporate sector.

However, the figures are different for cryptors: throughout the 24 months covered by the report, around 20 per cent of cryptor attacks targeted the corporate sector.

Hardly a month goes by without reports of ransomware attacks in the media – including recent reports of a hospital and online casino falling victim to ransomware attacks. Yet while public awareness of the problem is growing, it's clear that consumers and organizations alike are not doing enough to combat the threat; and cybercriminals are capitalizing on this – this is clearly reflected in the number of attacks we're seeing.

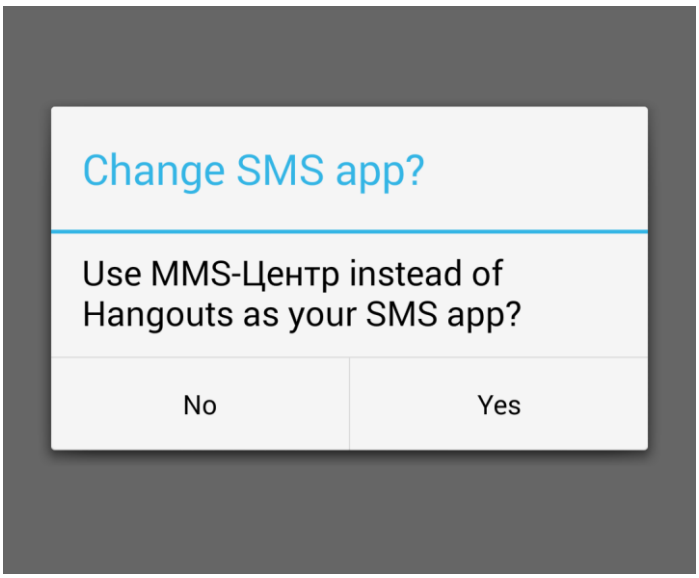
It's important to reduce your exposure to ransomware (and we've outlined important steps you can take here and here). However, there's no such thing as 100 per cent security, so it's also important to mitigate the risk. In particular, it's vital to ensure that you have a backup, to avoid facing a situation where the only choices are to pay the cybercriminals or lose your data. It's never advisable to pay the ransom. Not only does this validate the cybercriminals' business model, but there's no guarantee that they will decrypt your data once you've paid them – as one organization discovered recently to its cost. If you do find yourself in a situation where your files are encrypted and you don't have a backup, ask if your anti-malware vendor is able to help. Kaspersky Lab, for example, is able to help recover data encrypted by some ransomware.

Mobile malware

Displaying adverts remains one of the main methods of monetization for detected mobile objects. Trojan.AndroidOS.Iop.c became the most popular mobile Trojan in Q2 2016, accounting for more than 10% of all detected mobile malware encountered by our users during the reporting period. It displays adverts and installs, usually secretly, various programs using superuser privileges. Such activity quickly renders the infected device virtually unusable due to the amount of adverts and new applications on it. Because this Trojan can gain superuser privileges, it is very difficult to delete the programs that it installs.

In our report IT threat evolution in Q1 2016 we wrote about the Trojan-Banker.AndroidOS.Asacub family of banking malware. Representatives of this family have an unusual technique for bypassing the security mechanisms used by operating systems – they overlay the regular system window requesting device administrator privileges with their own window containing buttons. The Trojan thereby conceals the fact that it is gaining elevated privileges in the system, and tricks the user into approving these privileges. In Q2 2016, Asacub introduced yet another method for deceiving users:

the Trojan acquired SMS messenger functionality and started offering its services in place of the device's standard SMS app.



Dialog window of Trojan-Banker.AndroidOS.Asacub.i asking for the rights to be the main SMS application

This allows the Trojan to bypass system constraints first introduced in Android 4.4 as well as delete or hide incoming SMSs from the user.

Back in October 2015, we wrote about representatives of the Trojan-PSW.AndroidOS.MyVk family that steal passwords from user accounts on the VK.com social network. This quarter, those responsible for distributing Trojans from this family introduced a new approach for bypassing Google Play security mechanisms that involved first publishing an app containing useful functionality with no malicious code. Then, at least once, they updated it with a new version of the application – still without any malicious code. It was more than a month after the initial publication that the attackers eventually added malicious code to an update. As a result, thousands of users downloaded Trojan-PSW.AndroidOS.MyVk.i.

Data breaches

Personal information is a valuable commodity, so it's no surprise that cybercriminals target online providers, looking for ways to bulk-steal data in a single attack. We've become accustomed to the steady stream of security breaches reported in the media. This quarter has been no exception, with reported attacks on beautifulpeople.com, the nulled.io hacker forum (underlining the fact that it's not just legitimate systems that are targeted), kiddicare, Tumblr and others.

Some of these attacks resulted in the theft of huge amounts of data, highlighting the fact that many companies are failing to take adequate steps to defend themselves. It's not simply a matter of defending the corporate perimeter. There's no such thing as 100 per cent security, so it's not possible to guarantee that systems can't be breached. But any organization that holds personal data has a duty of care to secure it effectively. This includes hashing and salting customer passwords and encrypting other sensitive data.

Consumers can limit the damage of a security breach at an online provider by ensuring that they choose passwords that are unique and complex: an ideal password is at least 15 characters long and consists of a mixture of letters, numbers and symbols from the entire keyboard. As an alternative, people can use a password manager application to handle all this for them automatically. Unfortunately, all too often people use easy-to-guess passwords and re-use the same password for multiple online accounts – so that if the password for one is compromised, all the victim's online IDs are vulnerable. This issue was highlighted publicly in May 2016 when a hacker known as 'Peace' attempted to sell 117 million LinkedIn e-mails and passwords that had been stolen some years earlier. More than one million of the stolen passwords were '123456'!

Many online providers offer two-factor authentication – i.e. requiring customers to enter a code generated by a hardware token, or one sent to a mobile device, in order to access a site, or at least in order to make changes to account settings. Two-factor authentication certainly enhances security – if people choose to take advantage of it.

Several companies are hoping to replace passwords altogether. Apple allows fingerprint authorization for iTunes purchases and payments using Apple Pay. Samsung has said it will introduce fingerprint, voice and iris recognition for Samsung Pay. Amazon has announced 'selfie-pay'. MasterCard and HSBC have announced the introduction of facial and voice recognition to authorize transactions. The chief benefit, of course, is that it replaces something that customers *have to remember* (a password) with something they *have* – with no opportunity to short-circuit the process (as they do when they choose a weak password).

Biometrics are seen by many as the way forward. However, they are not a security panacea. Biometrics can be spoofed, as we've discussed before (here, here and here); and biometric data can be stolen. In the end, multi-factor authentication is essential – combining something you *know*, something you *have* and something you *are*.

Statistics

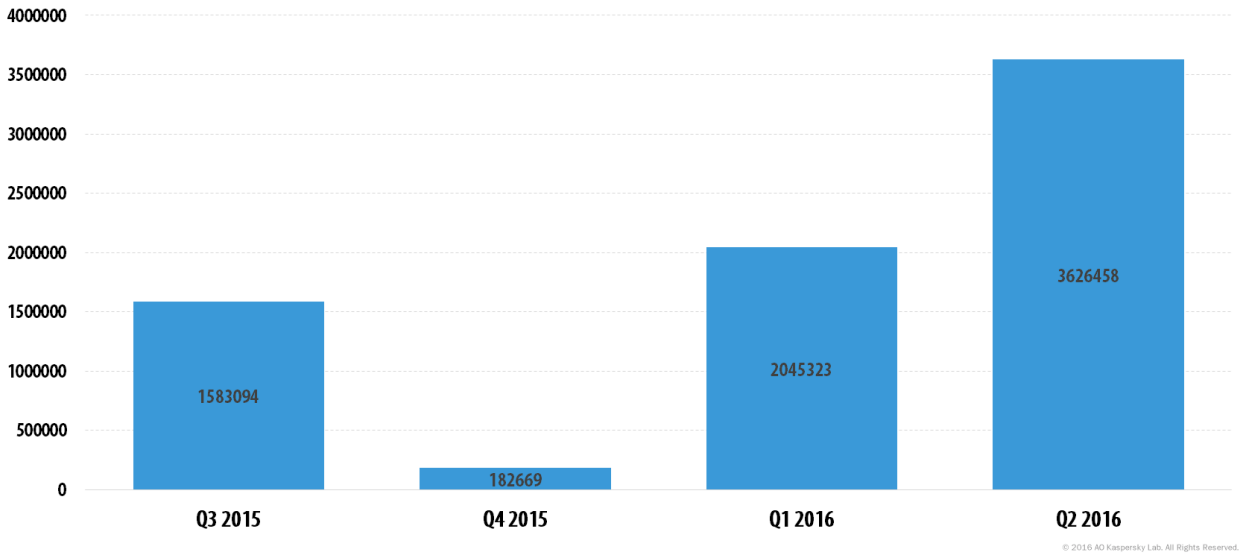
All the statistics used in this report were obtained using Kaspersky Security Network (KSN), a distributed antivirus network that works with various anti-malware protection components. The data was collected from KSN users who agreed to provide it. Millions of Kaspersky Lab product users from 213 countries and territories worldwide participate in this global exchange of information about malicious activity.

Q2 figures

- According to KSN data, Kaspersky Lab solutions detected and repelled **171,895,830** malicious attacks from online resources located in 191 countries all over the world.
- **54,539,948** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **16,119,489** unique malicious objects: scripts, exploits, executable files, etc.
- Attempted infections by malware that aims to steal money via online access to bank accounts were registered on **1,132,031** user computers.
- Crypto ransomware attacks were blocked on **311,590** computers of unique users.
- Kaspersky Lab's file antivirus detected a total of **249,619,379** unique malicious and potentially unwanted objects.
- Kaspersky Lab mobile security products detected:
- **3,626,458** malicious installation packages;
- **27,403** mobile banker Trojans (installation packages);
- **83,048** mobile ransomware Trojans (installation packages).

Mobile threats

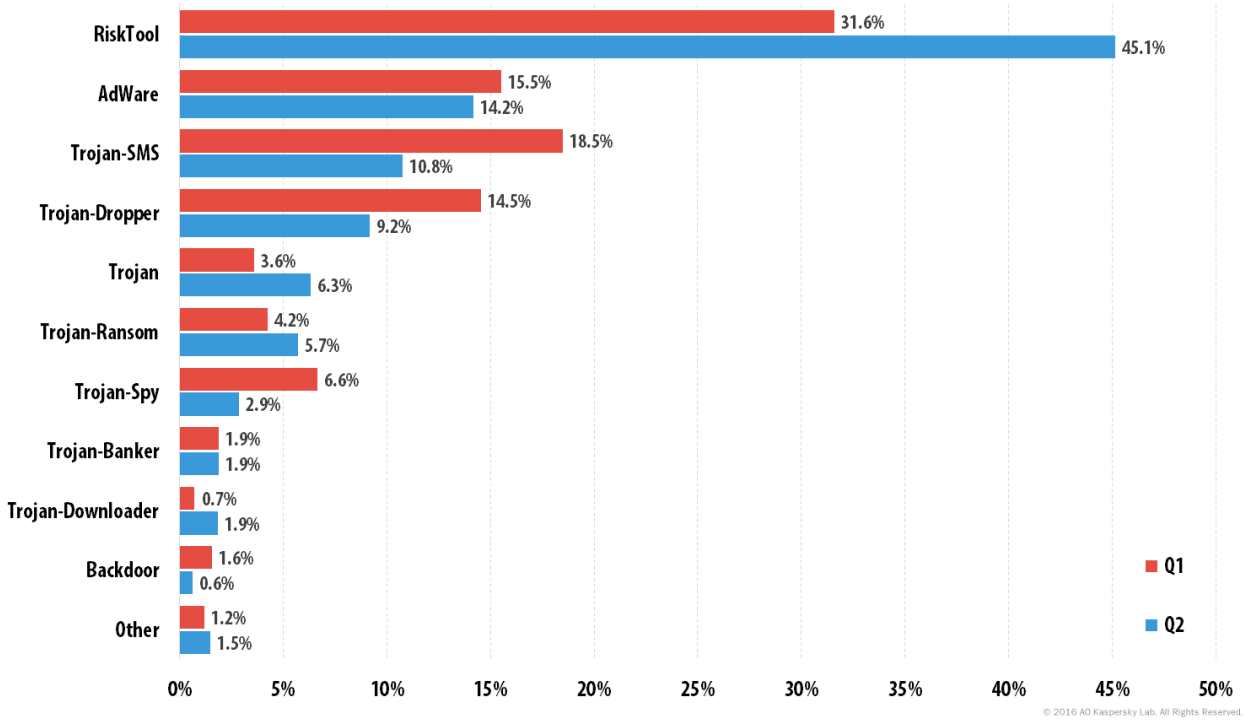
In Q2 2016, Kaspersky Lab detected **3,626,458** malicious installation packages – 1.7 times more than in the previous quarter.



Number of detected malicious installation packages (Q3 2015 – Q2 2016)

Distribution of mobile malware by type

As of this quarter, we will calculate the distribution of mobile malware by type based on ***the number of detected malicious installation packages rather than modifications***, as was the case in earlier reports.



Distribution of new mobile malware by type (Q1 2016 and Q2 2016)

In Q2 2016, RiskTool software, or legal applications that are potentially dangerous to users, topped the ranking of detected malicious objects for mobile devices. Their share increased from 31.6% in Q1 to 45.1% this quarter.

Adware occupies second place. The share of these programs fell 1.4 p.p. compared to the previous quarter, and accounted for 14.2%.

The share of SMS Trojans fell from 18.5% to 10.8%, pushing this category of malicious programs down from second to third place in the ranking. Trojan-SMS.AndroidOS.Agent.qu and Trojan-SMS.AndroidOS.Agent.f accounted for most of the detected SMS Trojans, with both accounting for approximately 30% of all malicious files in this category.

The Trojan-Dropper share also fell – from 14.5% in Q1 to 9.2%. Trojan-Dropper.AndroidOS.Agent.v led the way: we detected more than 50,000 installation packages related to this Trojan.

TOP 20 mobile malware programs

Please note that this ranking of malicious programs does not include potentially dangerous or unwanted programs such as RiskTool or adware.

	Name	% of attacked users*
1	DangerousObject.Multi.Generic	80.87
2	Trojan.AndroidOS.Iop.c	11.38
3	Trojan.AndroidOS.Agent.gm	7.71
4	Trojan-Ransom.AndroidOS.Fusob.h	6.59
5	Backdoor.AndroidOS.Ztorg.a	5.79
6	Backdoor.AndroidOS.Ztorg.c	4.84
7	Trojan-Ransom.AndroidOS.Fusob.pac	4.41
8	Trojan.AndroidOS.Iop.t	4.37
9	Trojan-Dropper.AndroidOS.Gorpo.b	4.3
10	Trojan.AndroidOS.Ztorg.a	4.30
11	Trojan.AndroidOS.Ztorg.i	4.25
12	Trojan.AndroidOS.Iop.ag	4.00
13	Trojan-Dropper.AndroidOS.Triada.d	3.10
14	Trojan-Dropper.AndroidOS.Rootnik.f	3.07
15	Trojan.AndroidOS.Hiddad.v	3.03
16	Trojan-Dropper.AndroidOS.Rootnik.h	2.94
17	Trojan.AndroidOS.Iop.o	2.91
18	Trojan.AndroidOS.Rootnik.ab	2.91
19	Trojan.AndroidOS.Triada.e	2.85
20	Trojan-SMS.AndroidOS.Podec.a	2.83

* *Percentage of unique users attacked by the malware in question, relative to all users of Kaspersky Lab's mobile security product that were attacked.*

First place is occupied by DangerousObject.Multi.Generic (80.87%), the classification used for malicious programs detected by cloud technologies. Cloud technologies work when the antivirus database contains neither the signatures nor heuristics to detect a malicious program, but the cloud

of the antivirus company already contains information about the object. This is basically how the very latest malware is detected.

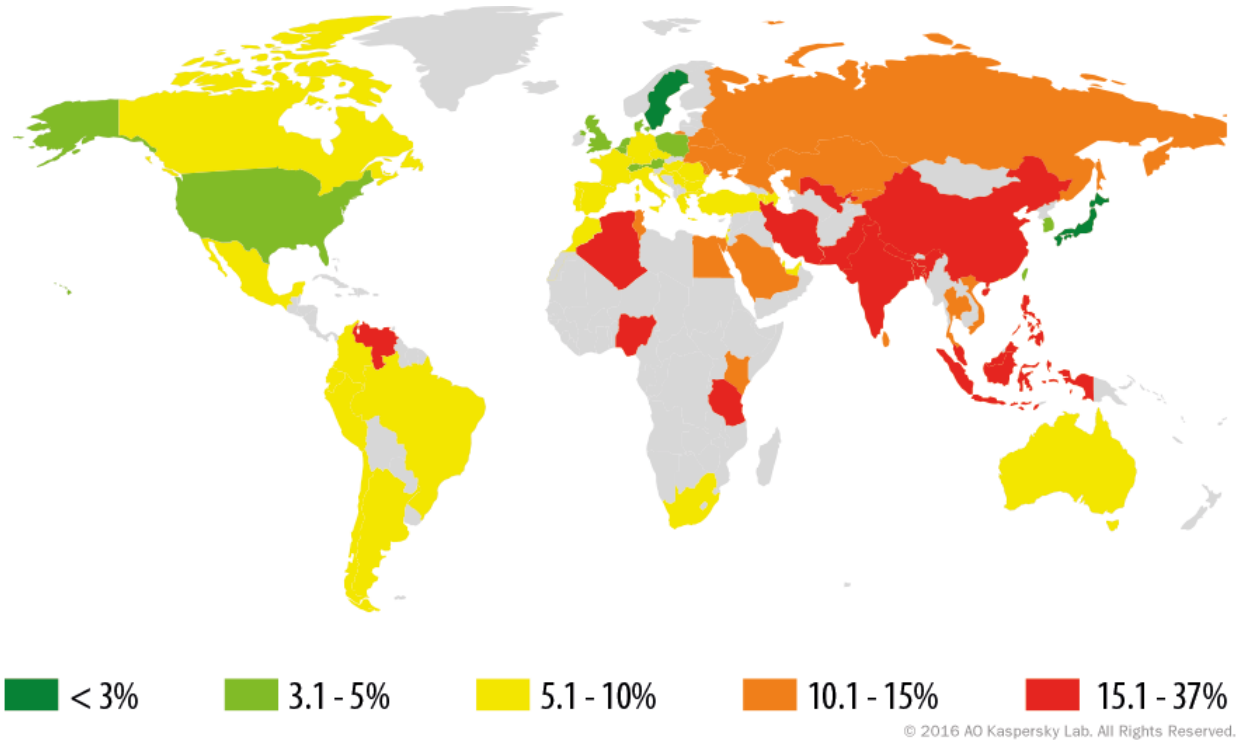
As in the previous quarter, 16 Trojans that use advertising as their main means of monetization (highlighted in blue in the table) made it into the TOP 20. Their goal is to deliver as many adverts as possible to the user, employing various methods, including the installation of new adware. These Trojans may use superuser privileges to conceal themselves in the system application folder, from which it will be very difficult to delete them.

Trojan.AndroidOS.Iop.c (11.38%) moved from third to second in the TOP 20 and became the single most popular malicious program of the quarter. Over the reporting period we detected this Trojan in 180 countries, but the majority of attacked users were in Russia, India and Algeria. Iop.c can exploit a variety of vulnerabilities in the system to gain superuser privileges. The main method of monetization is displaying advertising and installing (usually secretly) various programs on the user's device, including other malicious programs.

Representatives of the Trojan-Ransom.AndroidOS.Fusob ransomware family claimed fourth and seventh places. These Trojans demand a ransom of $100-200 from victims to unblock their devices. Attacks using this Trojan were registered in over 120 countries worldwide in Q2, with a substantial number of victims located in Germany and the US.

Trojan-SMS.AndroidOS.Podec.a (2.83%) has now spent over a year in the mobile malware TOP 20, although it is starting to lose ground. It used to be an ever-present in the TOP 5 mobile threats, but for the second quarter in a row it has only made it into the bottom half of the ranking. Its functionality has remained practically unchanged; its main means of monetization is to subscribe users to paid services.

The geography of mobile threats



The geography of attempted mobile malware infections in Q2 2016 (percentage of all users attacked)

TOP 10 counties attacked by mobile malware (ranked by percentage of users attacked)

	Country*	% of users attacked **
1	China	36.31
2	Bangladesh	32.66
3	Nepal	30.61
4	Uzbekistan	22.43
5	Algeria	22.16
6	Nigeria	21.84
7	India	21.64
8	Indonesia	21.35
9	Pakistan	19.49
10	Iran	19.19

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*

*** Percentage of unique users attacked in each country relative to all users of Kaspersky Lab's mobile security product in the country.*

China topped the ranking, with more than 36% of users there encountering a mobile threat at least once during the quarter. China also came first in this ranking in Q1 2016.

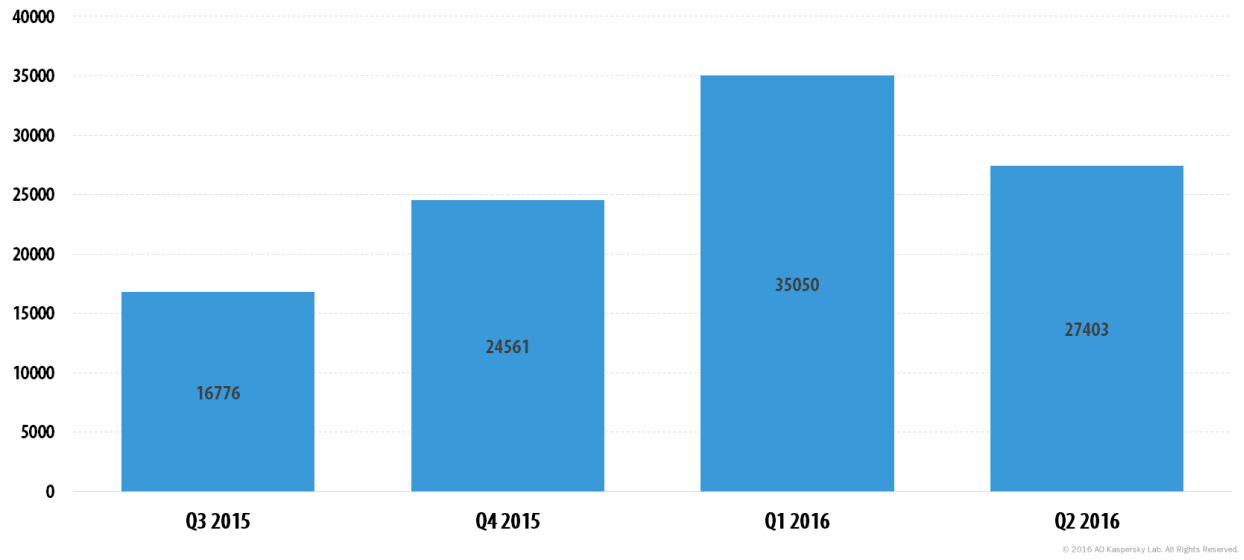
In all the countries of this ranking, except China, the most popular mobile malware was the same – advertising Trojans that appeared in the TOP 20 mobile malware, and AdWare. The most popular malicious program was Trojan.AndroidOS.Iop.c. In China, a significant proportion of attacks also involved advertising Trojans, but the majority of users there encountered the Backdoor.AndroidOS.GinMaster and Backdoor.AndroidOS.Fakengry families, while Trojan.AndroidOS.Iop.c only occupied sixteenth place.

Russia (10.4%) was 26th in this ranking, Germany (8.5%) 38th, Italy (6.2%) 49th, and France (5.9%) 52th. The US (5.0%) came 59th and the UK (4.6%) 64th.

The safest countries were Austria (3.6%), Sweden (2.9%) and Japan (1.7%).

Mobile banking Trojans

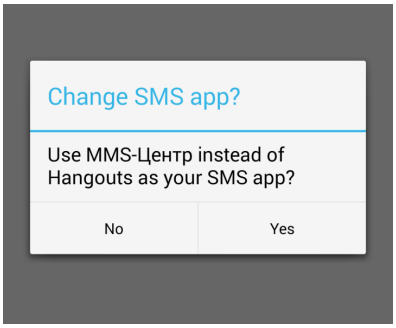
As of this quarter, we will calculate the distribution of mobile malware by type based on ***the number of detected malicious installation packages rather than modifications***, as was the case in earlier reports. Over the reporting period, we detected 27,403 mobile Trojans, which is 1.2 times less than in Q1.



Number of mobile banking Trojans detected by Kaspersky Lab solutions (Q3 2015 – Q2 2016)

The TOP 5 most popular mobile banking Trojans in Q2 consisted of representatives from just two families – Trojan-Banker.AndroidOS.Asacub and Trojan-Banker.AndroidOS.Svpeng.

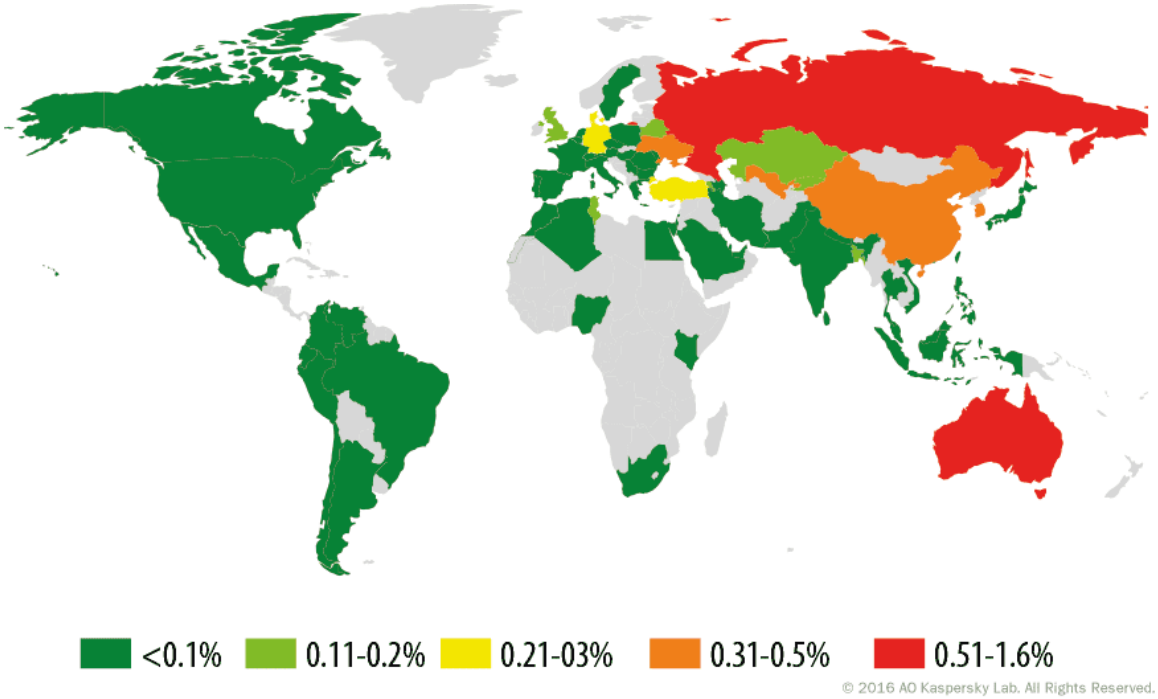
Trojan-Banker.AndroidOS.Asacub.i was the most popular mobile banking Trojan of the quarter. It uses different methods to trick users and bypass system constraints. In Q1 we identified a modification of this mobile Trojan that overlaid the regular system window requesting device administrator privileges with its own window containing buttons. The Trojan thereby conceals the fact that it is gaining elevated privileges in the system from the user, and tricks the user into approving these privileges. In Q2, we detected a modification that requested the user's permission to become the main SMS application.



Dialog window of Trojan-Banker.AndroidOS.Asacub.i asking for the user's approval to become the main SMS application

This allows the Trojan to bypass the system constraints introduced in Android 4.4, and to hide incoming SMSs from the user (as a rule, it hides messages from banks and payment systems). In order to make users save this malicious program in the settings as the main SMS application, the Trojan authors had to, among other things, implement a messenger interface. Asacub is actively distributed via SMS spam.

Russia and Germany lead in terms of the number of users attacked by mobile banking Trojans:



Geography of mobile banking threats in Q2 2016 (percentage of all users attacked)

The number of attacked users depends on the overall number of users within each individual country. To assess the risk of a mobile banker Trojan infection in each country, and to compare it across countries, we created a country ranking according to the percentage of users attacked by mobile banker Trojans.

TOP 10 counties attacked by mobile banker Trojans (ranked by percentage of users attacked)

	Country*	% of users attacked **
1	Russia	1.51
2	Australia	0.73
3	Uzbekistan	0.45
4	Korea	0.35
5	China	0.34
6	Ukraine	0.33
7	Denmark	0.28
8	Germany	0.24

9	Turkey	0.23
10	Kyrgyzstan	0.17

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*

*** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all users of Kaspersky Lab's mobile security product in the country.*

In Q2 2016, first place was occupied by Russia (1.51%) where the majority of affected users encountered the Trojan-Banker.AndroidOS.Asacub, Trojan-Banker.AndroidOS.Svpeng and Trojan-Banker.AndroidOS.Faketoken families of mobile banker Trojans.

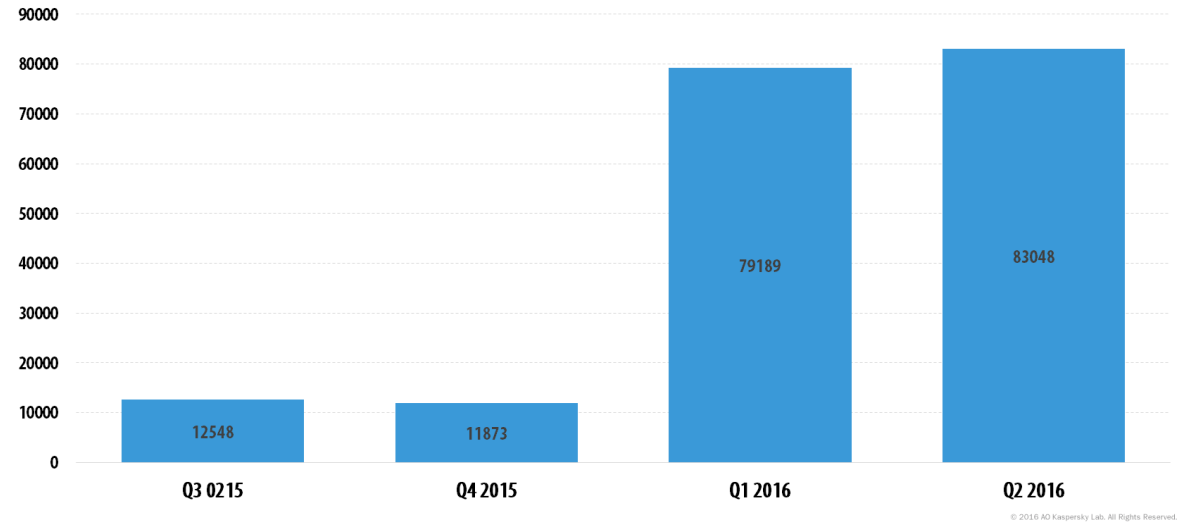
China, last quarter's leader, fell to fifth place this quarter. In second place again was Australia where the Trojan-Banker.AndroidOS.Acecard family was replaced by the Trojan-Banker.AndroidOS.Marcher family as the most popular threat.

Banking Trojans were especially popular with attackers in Russia and Australia. The percentage of users attacked by this malware in the two countries relative to all attacked users accounted for 14%.

Mobile Trojan-Ransom

As of this quarter, we will calculate the distribution of mobile malware by type based on ***the number of detected malicious installation packages rather than modifications***, as was the case in earlier reports.

In Q2 2016, we detected 83,048 mobile Trojan-Ransomware installation packages, which is about the same number as the previous quarter and seven times more than in Q4 2015.

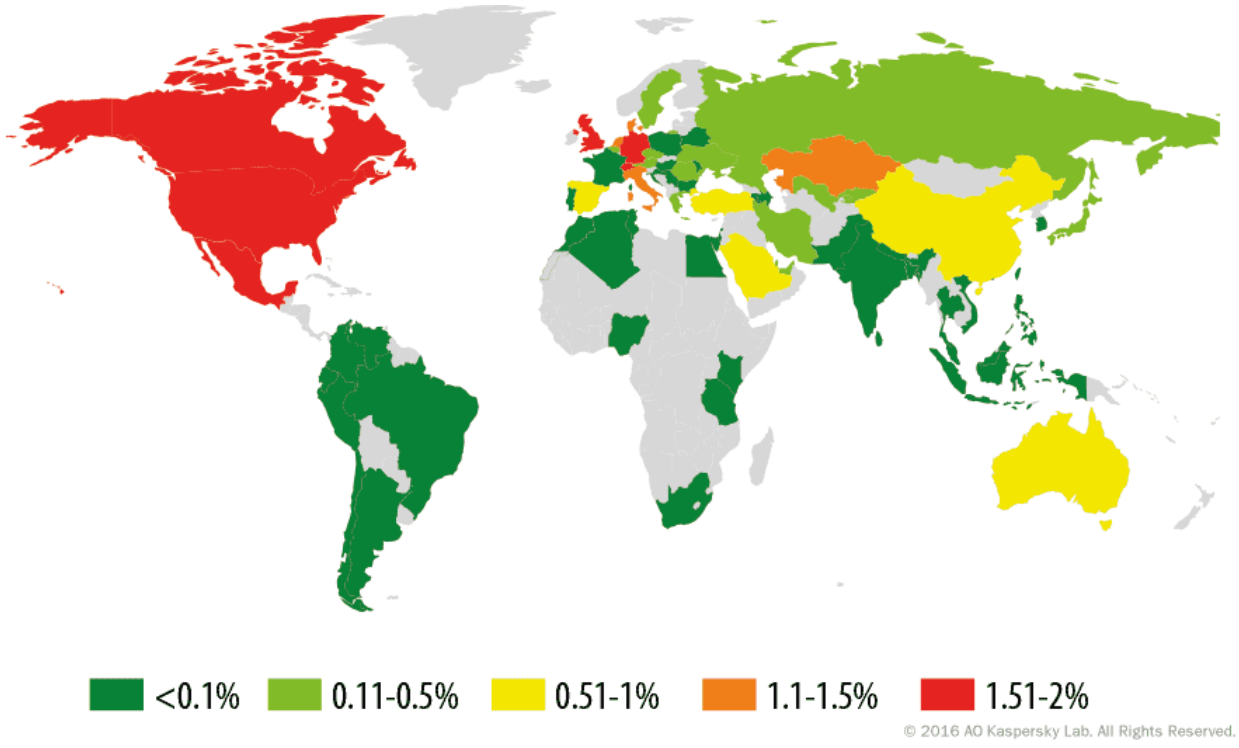


Number of mobile Trojan-Ransomware installation packages detected by Kaspersky Lab (Q3 2015 – Q2 2016)

The sharp rise in the number of mobile Trojan-Ransomware installation packages in 2016 was caused by the active proliferation of the Trojan-Ransom.AndroidOS.Fusob family of Trojans. In the first quarter of 2016, this family accounted for 96% of users attacked by mobile ransomware. In Q2 its share was 85%.

Trojan-Ransom.AndroidOS.Fusob.h became the most popular mobile Trojan-Ransomware in the second quarter – it accounted for nearly 60% of users attacked by mobile ransomware. Once run, the Trojan requests administrator privileges, collects information about the device, including the GPS coordinates and call history, and downloads the data to a malicious server. After that, it may get a command to block the device. In the second quarter we registered a growth in the number of installation packages related to Trojan-Ransom.AndroidOS.Congur.b: their share grew from 0.8% to 8.8%. This Trojan, targeting Chinese-speaking users, changes the system password (PIN), or installs it if no password was installed earlier, thus making it impossible to use the device. The notification containing the ransom demand is displayed on the screen of the blocked device.

Germany, the US and Russia had the highest number of users attacked by Trojan-Ransomware this quarter:



Geography of mobile Trojan-Ransomware in Q2 2016 (percentage of all users attacked)

To assess the risk of a mobile banker Trojan infection in each country, and to compare it across countries, we created a country ranking according to the percentage of users attacked by mobile Trojan-Ransomware.

TOP 10 counties attacked by mobile Trojan-Ransomware (ranked by percentage of users attacked)

	Country*	% of users attacked **
1	Canada	2.01
2	Germany	1.89
3	US	1.66
4	Switzerland	1.63
5	Mexico	1.55
6	UK	1.51
7	Denmark	1.35
8	Italy	1.35
9	Kazakhstan	1,35
10	Netherlands	1.15

** We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.*

*** Percentage of unique users in each country attacked by mobile Trojan-Ransomware, relative to all users of Kaspersky Lab's mobile security product in the country.*

In all the countries of the TOP 10, except for Kazakhstan, the most popular Trojan-Ransom family was Fusob. In the US, the Trojan-Ransom.AndroidOS.Svpeng family was also popular. These Trojans demand a ransom of $100-500 from victims to unblock their devices.

In Kazakhstan and Uzbekistan, the main threat to users originated from representatives of the Small mobile Trojan-Ransom family. This is a fairly simple ransomware program that blocks operation of a device by overlaying all the windows on the device with its own window and demanding $10 to unblock it.

Vulnerable applications exploited by cybercriminals

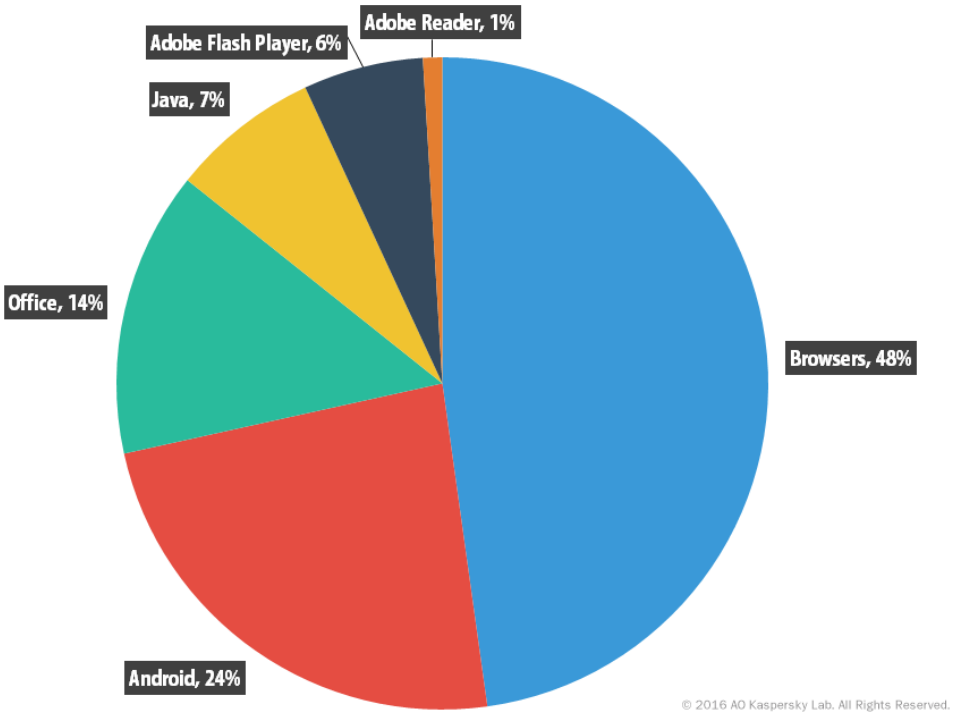
In Q2 2016, exploits for Adobe Flash Player remained popular. During the reporting period two new vulnerabilities were discovered in this software:

- CVE-2016-4117
- CVE-2016-4171

An exploit for CVE-2016-4117 was added to the Magnitude and Neutrino exploit kits. The CVE-2016-4171 vulnerability was used by the ScarCruft group to carry out targeted attacks. We wrote a more detailed account of this group's activities in a blog published in mid-June.

The main event this quarter was the demise of the long-term market leaders – the Angler and Nuclear exploit kits. Angler's departure resulted in market players shifting to other kits to distribute malware. In particular, we registered a dramatic growth in the popularity of the Neutrino exploit kit.

This is how the overall picture for the use of exploits in the second quarter looks:



Distribution of exploits used in attacks by the type of application attacked, Q2 2016

The chart shows that despite the exit of the market leaders the breakdown of exploits was almost unchanged from the previous quarter: the proportion of exploits for Microsoft Office (14%) and Java (7%) fell by 1 p.p., while the share for Android grew 2 p.p. and reached 24%. This suggests that demand for exploit kits has been spread among the remaining players: RIG, Magnitude and Neutrino. The latter was the undisputed leader this quarter in terms of the number of attempts to download malware.

Online threats (Web-based attacks)

The statistics in this section were derived from web antivirus components that protect users from attempts to download malicious objects from a malicious/infected website. Malicious websites are created deliberately by malicious users; infected sites include those with user-contributed content (such as forums), as well as compromised legitimate resources.

In the second quarter of 2016, Kaspersky Lab's web antivirus detected **16,119,489** unique malicious objects: scripts, exploits, executable files, etc. **54,539,948** unique URLs were recognized as malicious by web antivirus components.

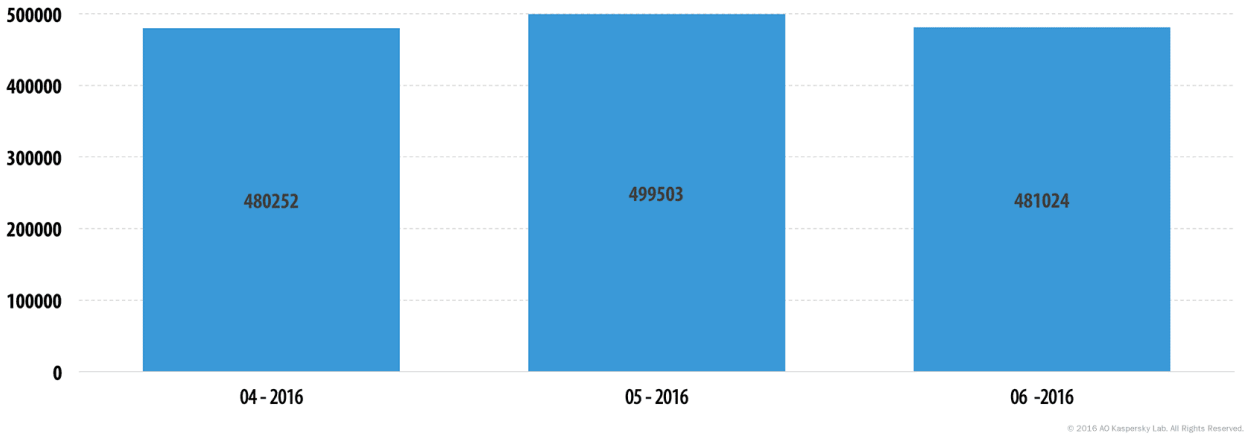
Online threats in the banking sector

These statistics are based on the detection verdicts of Kaspersky Lab products, received from users of Kaspersky Lab products who have consented to provide their statistical data.

Number of users attacked by malware targeting finances

Due to the constant emergence of new representatives of banking Trojans and functional changes in existing banking Trojans, in the second quarter of 2016 we have significantly updated the list of verdicts classed as banking risks. This means the number of financial malware victims has changed significantly compared to the data published in previous quarters. As a comparison, we have recalculated the statistics for the previous quarter, taking into account all the malware from the updated list.

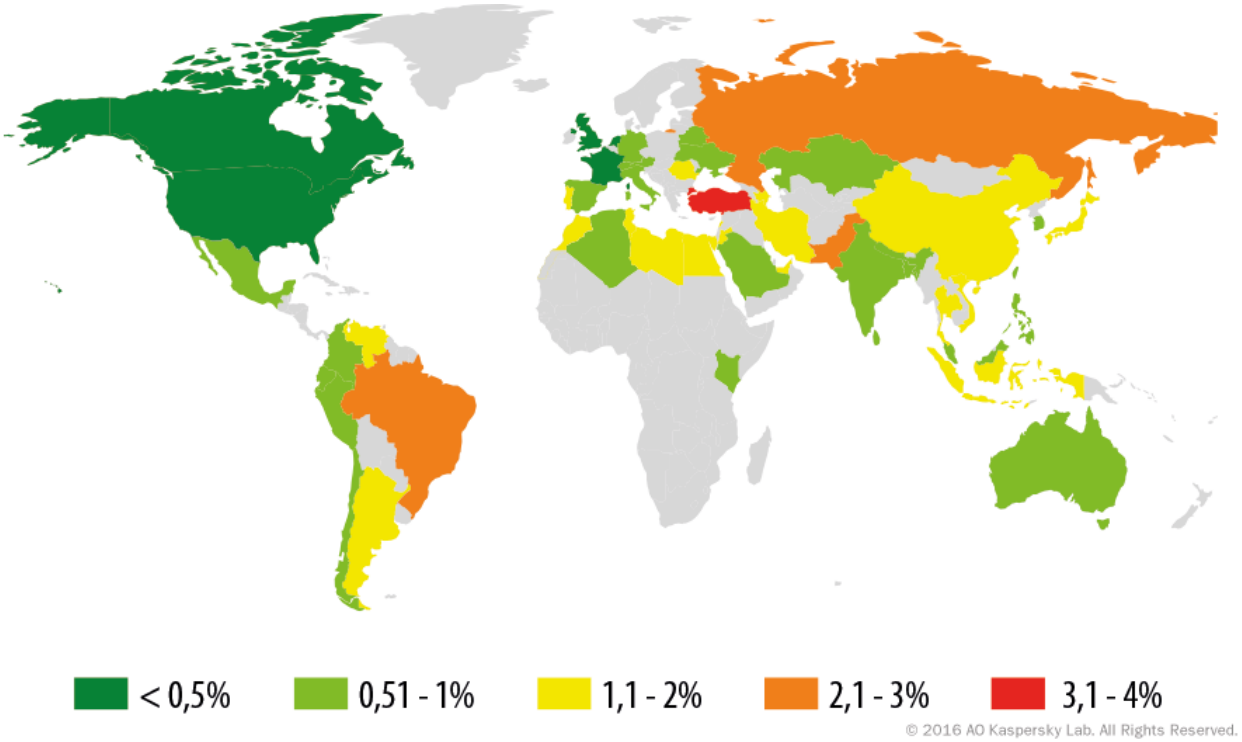
Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **1,132,031** computers in Q2 2016. The quarter saw an increase in financial malware activity: the figure for Q2 is 15.6% higher than that for the previous quarter (979, 607).



Number of users attacked by malware targeting finances, Q2 2016

Geography of attacks

To evaluate and compare the risk of being infected by banking Trojans worldwide, we calculate the percentage of Kaspersky Lab product users who encountered this type of threat during the reporting period in the country, relative to all users of our products in the county.



Geography of banking malware attacks in Q2 2016 (percentage of attacked users)

TOP 10 countries by percentage of attacked users

	Country*	% of attacked users**
1	Turkey	3.45
2	Russia	2.92
3	Brazil	2.63
4	Pakistan	2.60
5	Venezuela	1.66
6	Tunisia	1.62
7	Japan	1.61
8	Singapore	1.58

9	Libya	1.57
10	Argentina	1.48

These statistics are based on the detection verdicts returned by the antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

** We excluded those countries in which the number of Kaspersky Lab product users is relatively small (less than 10,000).*

*** Unique users whose computers have been targeted by banking Trojan attacks as a percentage of all unique users of Kaspersky Lab products in the country.*

The highest percentage of Kaspersky Lab users attacked by banking Trojans was in Turkey. One of the reasons for the growth in financial threats there was a burst of activity by the Gozi banking Trojan whose developers have joined forces with the creators of the Nymaim Trojan.

In Russia, 2.92% of users encountered a banking Trojan at least once in Q2, placing it second in this ranking.

Brazil rounds off the top three. We expect a surge in financial threats in Latin America in the next quarter due to the Olympic Games in Brazil. This event is just too tempting for cybercriminals to ignore – they regularly use the theme of major sporting events in their attacks to lure potential victims.

The top five countries where users were least affected by banking Trojans were Canada (0.33%), the US (0.4%), the UK (0.4%), France (0.43%) and the Netherlands (0.5%).

The percentage of banking Trojan victims in Italy was 0.62%, in Spain it was 0.83%, while in Germany the figure was 1.03%.

The TOP 10 banking malware families

The table below shows the top 10 malware families most commonly used in Q2 2016 to attack online banking users (as a percentage of users attacked):

	Name*	% of attacked users**
1	Trojan-Spy.Win32.Zbot	15.72
2	Trojan-Banker.Win32.Gozi	3.28
3	Trojan.Win32.Qhost	2.35
4	Trojan-Banker.Win32.Shiotob	2.27
5	Trojan-Banker.Win32.BestaFera	2.12
6	Trojan.Win32.Nymaim	1.98

7	Trojan-Banker.Win32.ChePro	1.90
8	Trojan-Banker.Win32.Banbra	1.77
9	Trojan.Win32.Neurevt	0.67
10	Backdoor.Win32.Shiz	0.66

** The detection verdicts of Kaspersky Lab products, received from users of Kaspersky Lab products who have consented to provide their statistical data.*

*** Unique users whose computers have been targeted by the malware in question as a percentage of all users attacked by financial malware.*

Trojan-Spy.Win32.Zbot in first place is a permanent fixture in the leading positions of this ranking, and it is no coincidence: the source codes of this Trojan became publicly available back in 2012. This has resulted in the emergence of new banking Trojans that have adopted fragments of the Zbot code.

The second quarter of 2016 saw a surge in malicious activity by Trojan.Win32.Nymaim. As a result, this Trojan made it into the top 10 for the first time, going straight in at sixth place. Nymaim was initially designed to block access to valuable data and then demand a ransom (ransomware) to unblock it, but the latest version now also includes banking Trojan functionality for stealing financial information. This can be explained by the fact that the creators of Nymaim and Gozi (which also appears in the Q2 TOP 10 financial risks) have joined forces. Nymaim's source code now includes fragments of Gozi code that provide attackers with remote access to infected computers.

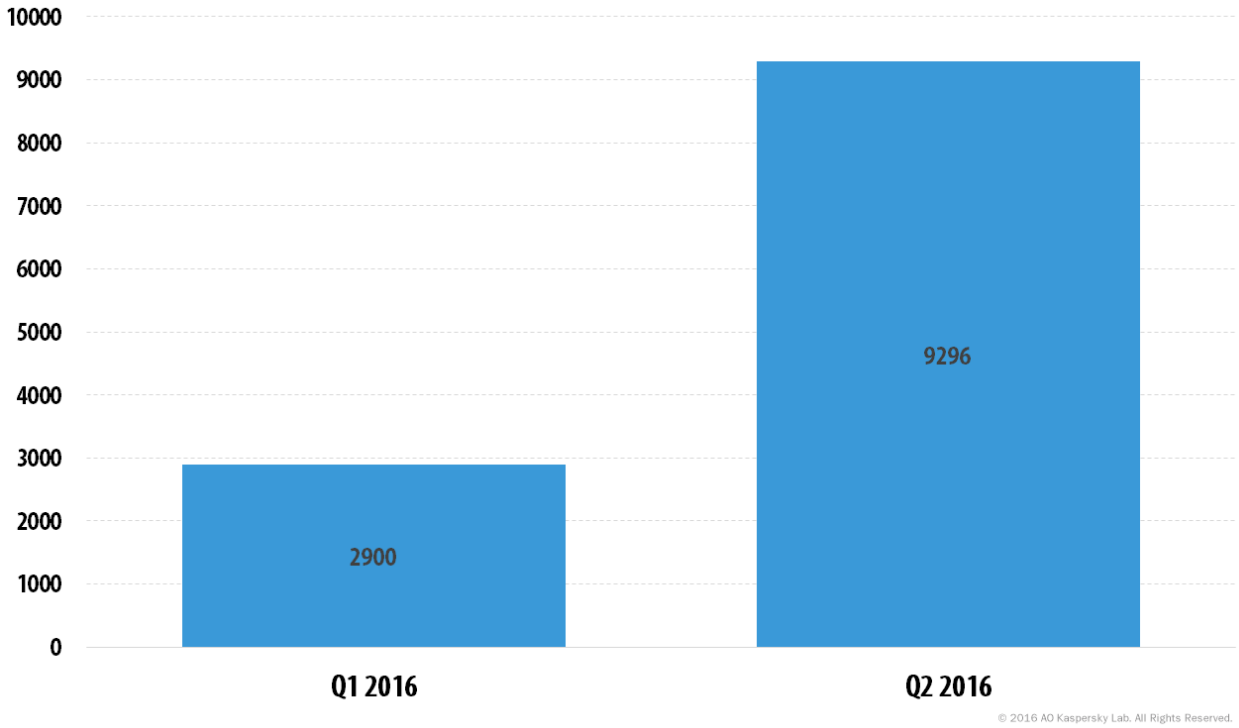
A permanent resident in this ranking and one of the reasons financial threats are so prominent in Brazil is the Trojan-Banker.Win32.ChePro family. This banking malware lets cybercriminals take screenshots, register keystrokes, and read the contents of the clipboard, i.e., it possess functionality capable of attacking almost any online banking system. Criminals are trying to implement new techniques to avoid detection for as long as possible. Some of the Trojans from this family use geolocation or ask for the time zone and the Windows version from the system in order to infect users in a particular region.

Yet another newcomer to the top 10 most active financial threats in Q2 was the Trojan.Win32.Neurevt family. Representatives of this family were first discovered in 2013 and are used by cybercriminals not only to steal user payment data in online banking systems but also to send out spam (some versions, for example, sent spam messages on Skype) and implement DDoS attacks (with the addition of functionality capable of performing the Slowloris HTTP flooding scenario).

Ransomware Trojans

The overall number of cryptor modifications in our virus collection to date is approximately 26,000. A total of 28 new cryptor families and **9,296** new modifications were detected in Q2.

The following graph shows the rise in the number of newly created cryptor modifications over the last two quarters.



Number of Trojan-Ransom cryptor modifications (Q1 2016 vs Q2 2016)

Some of the more high-profile or unusual Trojans detected in Q2 2016 are listed below:

- **CryptXXX (Trojan-Ransom.Win32.CryptXXX)**

  This cryptor has been widely distributed via exploit kits since April 2016. Its earlier versions contained gaps in the file encryption algorithm which allowed Kaspersky Lab to release a utility to decrypt them. Unfortunately, the attackers have made adjustments to subsequent versions, making it impossible to decrypt the files affected by later CryptXXX modifications.

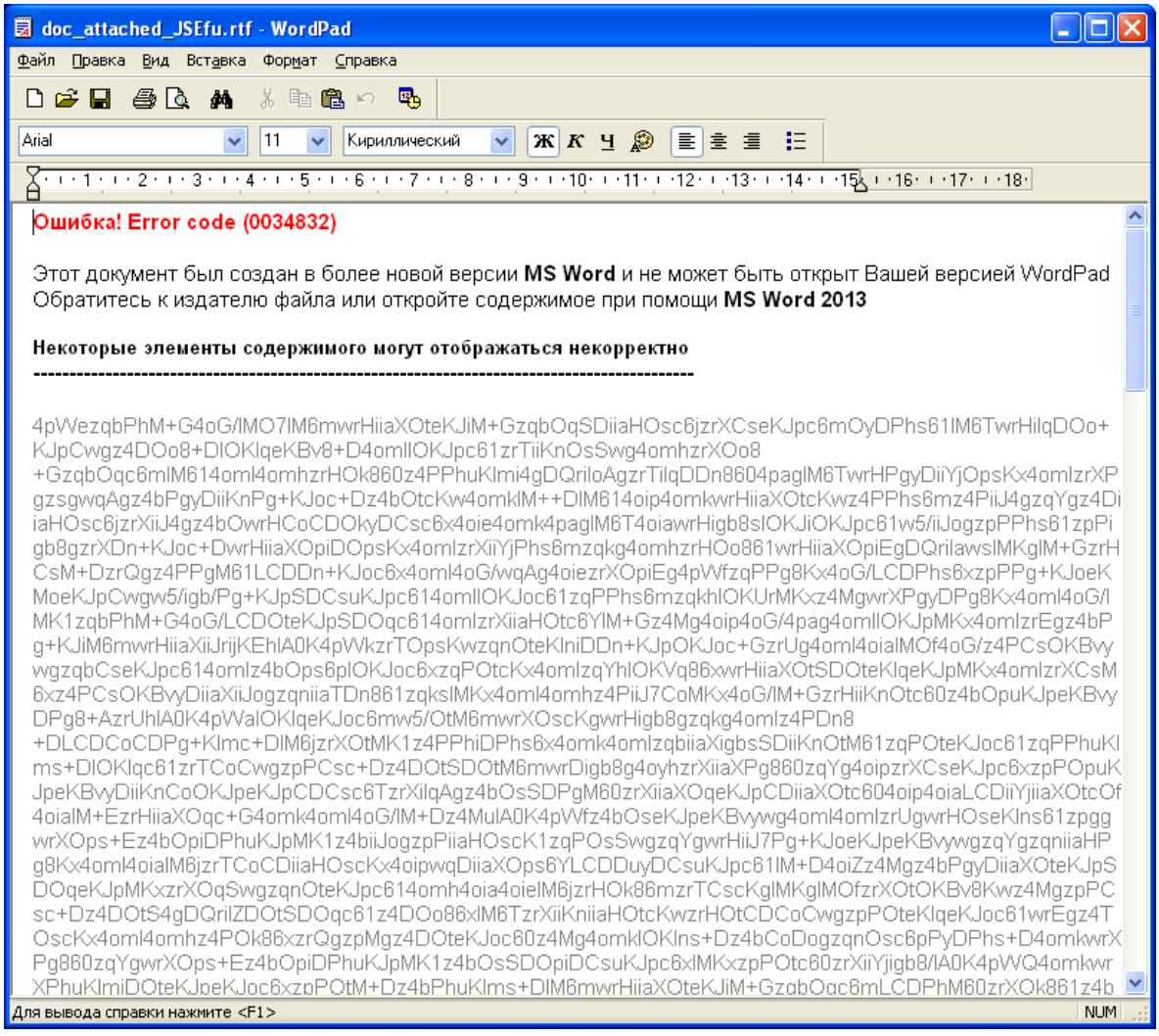
- **ZCryptor (Trojan-Ransom.MSIL.Zcryptor)**

  This malware combines cryptor functionality and a worm distribution method. Trojan ransomware does not usually include tools for self-propagation, and ZCryptor just happens to be an exception to this rule. Like a classic worm, while infecting, it creates copies of its body on removable media and generates the autorun.inf file to implement the automatic launch of

its executable file once the media is connected to another system (if, of course, autorun is not disabled).

- **RAA (Trojan-Ransom.JS.RaaCrypt)**

  Sometimes we come across cryptors that differ from their peers in terms of functionality, and sometimes an unusual implementation will catch the attention of an analyst. In the case of RAA, the choice of programming language was curious: it was written entirely in JavaScript. The whole body of the program was included in a single .js file delivered to the victim as an attachment in a spam message. When run, it displays a fake error message, and in the meantime, encrypts the user's files.



- **Bart (Trojan-Ransom.Win32.Bart)**

  This cryptor puts the victim's files in password-protected ZIP archives; and it creates passwords using the Diffie-Hellman algorithm on an elliptic curve. The design of the ransom note and the payment site is an exact copy of that used by the notorious Locky.

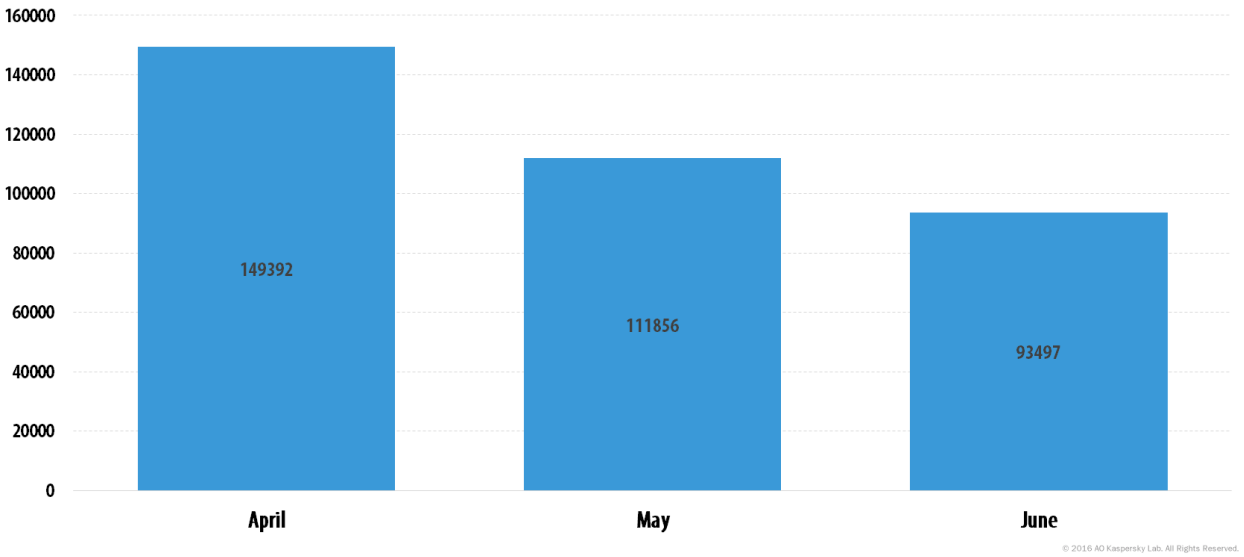
- **Satana (Trojan-Ransom.Win32.Satan)**

  This is a combination of MBR blocker and file cryptor, probably inspired by similar functionality in the notorious Petya + Mischa Trojans. Satana, unlike Petya, does not encrypt MFT; in fact, its MBR module is obviously incomplete because the process of checking the password entered by the victim results in nothing more than a continuous cycle. Below is a fragment of the code demonstrating this.

```
000007C2
000007C2
000007C2                        ; Attributes: noreturn
000007C2
000007C2                        check_hash proc near
000007C2 BE 00 28               mov     si, 2800h
000007C5 B9 08 00               mov     cx, 8
000007C8 E8 DA FF               call    calc_correct_hash
000007CB 00 E0                  add     al, ah
000007CD 3A 06 00 29            cmp     al, sum
```

```
000007D1
000007D1                        endless:
000007D1 EB FE                  jmp     short endless
000007D1                        check_hash endp
000007D1
```

The number of users attacked by ransomware



Number of users attacked by Trojan-Ransom cryptor malware (Q2 2016)

In Q2 2016, 311,590 unique users were attacked by cryptors, which is 16% less than the previous quarter. Approximately 21% of those attacked were in the corporate sector.

It is important to keep in mind that the real number of incidents is several times higher: the statistics reflect only the results of signature-based and heuristic detections, while in most cases Kaspersky Lab products detect encryption Trojans based on behavior recognition models and issue the Generic verdict, which does not distinguish the type of malicious software.

Top 10 countries attacked by cryptors

	Country*	% of users attacked by cryptors **
1	Japan	2.40
2	Italy	1.50
3	Djibouti	1.46
4	Luxembourg	1.36
5	Bulgaria	1.34
6	Croatia	1.25
7	Maldives	1.22
8	Korea	1.21
9	Netherlands	1.15
10	Taiwan	1.04

** We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 10,000).*

*** Unique users whose computers have been targeted by ransomware as a percentage of all unique users of Kaspersky Lab products in the country.*

In Q2, half of the top 10 were European countries – one less than the previous quarter.

Japan, which came ninth in Q1, topped the ranking of countries attacked by cryptors with 2.40%: the most widespread cryptor families in the country were Teslacrypt, Locky and Cryakl.

Newcomers to this ranking were Djibouti (1.46%), Korea (1.21%) and Taiwan (1.04%).

Top 10 most widespread cryptor families

	Name*	Verdict*	% of attacked users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	14.59
2	Teslacrypt	Trojan-Ransom.Win32.Bitman	8.36
3	Locky	Trojan-Ransom.Win32.Locky	3.34
4	Shade	Trojan-Ransom.Win32.Shade	2.14
5	Cryrar/ ACCDFISA	Trojan-Ransom.Win32.Cryrar	2.02
6	Cryptowall	Trojan-Ransom.Win32.Cryptodef	1.98
7	Cryakl	Trojan-Ransom.Win32.Cryakl	1.93
8	Cerber	Trojan-Ransom.Win32. Zerber	1.53
9	Scatter	Trojan-Ransom.BAT.Scatter/ Trojan-Downloader.JS.Scatter/ Trojan-Dropper.JS.Scatter/ Trojan-Ransom.Win32.Scatter	1.39
10	Rakhni	Trojan-Ransom.Win32.Rakhni/ Trojan-Downloader.Win32.Rakhni	1.13

** These statistics are based on detection verdicts received from users of Kaspersky Lab products who have consented to provide their statistical data.*

*** Unique users whose computers have been targeted by a specific Trojan-Ransom family as a percentage of all users of Kaspersky Lab products attacked by Trojan-Ransom malware.*

First place in Q2 was occupied by the CTB-Locker (Trojan-Ransom.Win32/NSIS.Onion) family. In second place was the TeslaCrypt family represented by one verdict: Trojan-Ransom.Win32.Bitman. The Trojan-Ransom.JS.Cryptoload verdict, which in the past downloaded malware and was associated with TeslaCrypt, is no longer characteristic of this family only. TeslaCrypt was earlier a major contributor to the statistics, but fortunately ceased to exist in May 2016 – the owners disabled their servers and posted a master key to decrypt files.

Cerber and Cryrar are the only changes to this ranking compared to the previous quarter.

The Cerber cryptor spreads via spam and exploit kits. The cryptor's site on the Tor network is translated into lots of languages. Cerber's special features include the following:

- It explores the infected system meticulously: checks for the presence of an antivirus, if it is running under a virtual machine (Parallels, VmWare, QEMU, VirtualBox) or Wine, checks for

utilities from various researchers and analysts (it does this by searching for certain processes and files on the disk drive), it even has a blacklist of system drive serial numbers.

- It checks the keyboard layout and the IP address of the infected system. If it detects that the machine is located in a CIS country, it stops infecting it.
- It attempts to bypass antivirus protection by terminating their processes, interrupting services, deleting files.
- In addition to notifying users about encryption in the form of TXT and HTML files, as is the case with other families, it also runs the VBS script which reproduces the following voice message: "Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!"

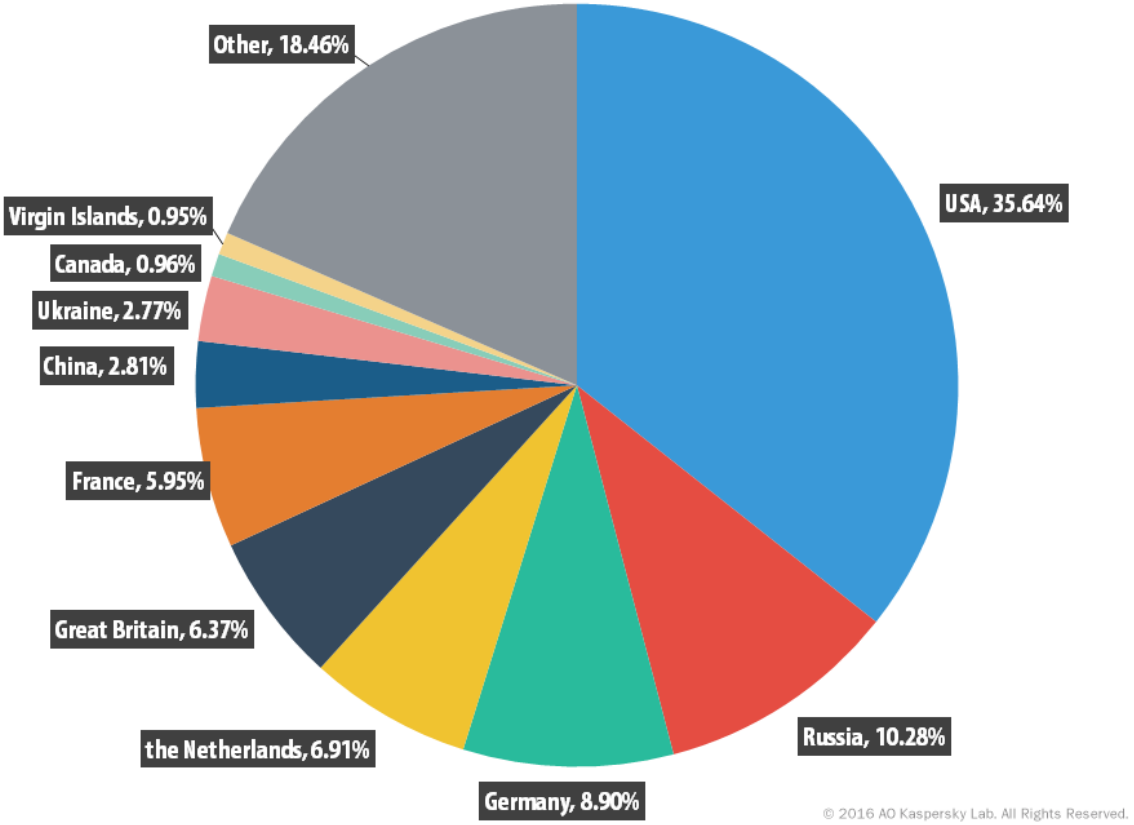
The Cryrar cryptor also known as the Anti Cyber Crime Department of Federal Internet Security Agency (ACCDFISA), Anti-Child Porn Spam Protection, etc. first appeared back in 2012. It has the distinctive feature of placing the victim's files in password-protected self-extracting RAR archives. According to KSN statistics, it shows no signs of conceding its position to newer rivals.

Top 10 countries where online resources are seeded with malware

The following statistics are based on the physical location of the online resources that were used in attacks and blocked by our antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host could be the source of one or more web attacks.

In order to determine the geographical source of web-based attacks, domain names are matched against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In Q2 2016, Kaspersky Lab solutions blocked **171,895,830** attacks launched from web resources located in 191 countries around the world. **54,539,948** unique URLs were recognized as malicious by web antivirus components. 81% of notifications about blocked web attacks were triggered by attacks coming from web resources located in 10 countries.



Distribution of web attack sources by country, Q2 2016

The US (35.44%) returned to the top of this ranking in the second quarter. Russia (10.28%) moved up one place to second. The previous quarter's leader, the Netherlands, dropped to fourth place after its share fell by 17.7 percentage points. Germany completed the Top 3 with a share of 8.9%. Bulgaria left the Top 10, while Canada was a newcomer in ninth place with 0.96%.

Countries where users faced the greatest risk of online infection

In order to assess the risk of online infection faced by users in different countries, we calculated the percentage of Kaspersky Lab users in each country who encountered detection verdicts on their machines during the quarter. The resulting data provides an indication of the aggressiveness of the environment in which computers work in different countries.

	Country*	% of unique users attacked**
1	Azerbaijan	32.10
2	Russia	30.80

3	China	29.35
4	Slovenia	27.54
5	Ukraine	27.46
6	Kazakhstan	27.03
7	Vietnam	26.02
8	Algeria	25.63
9	Armenia	25.09
10	Belarus	24.60
11	Brazil	24.05
12	France	22.45
13	Moldova	22.34
14	Kyrgyzstan	22.13
15	Bulgaria	22.06
16	Italy	21.68
17	Chile	21.56
18	Qatar	20.10
19	India	20.00
20	Portugal	19.84

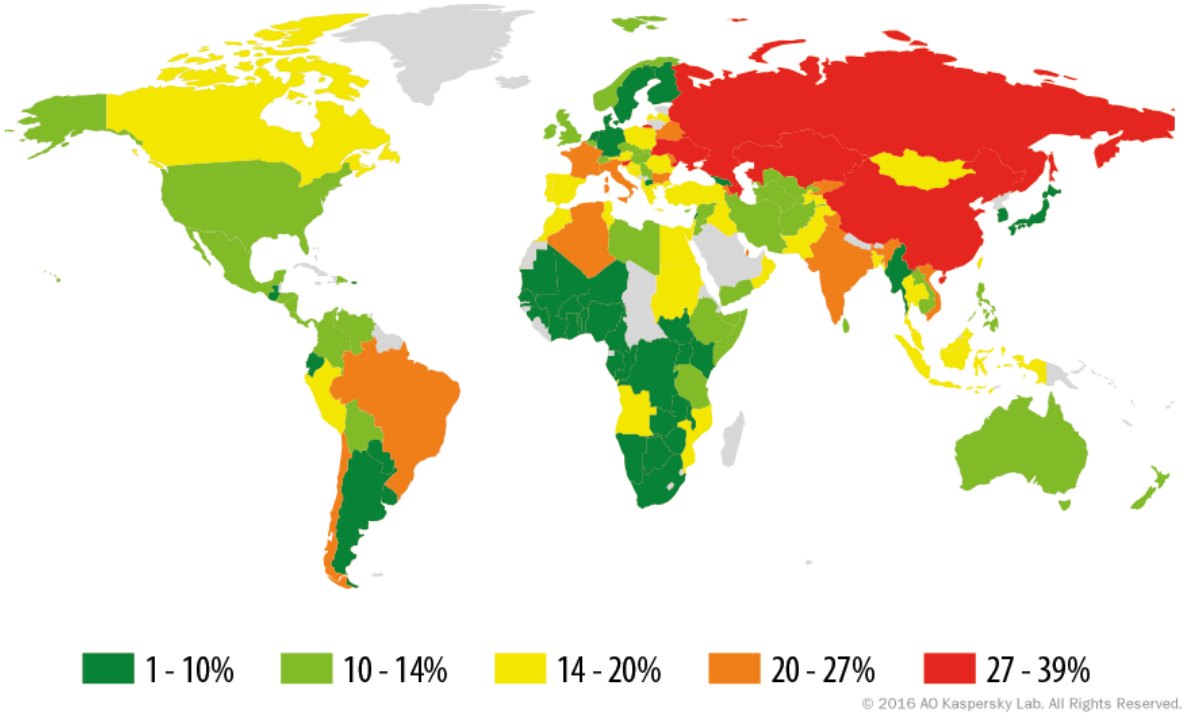
These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

** These calculations excluded countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).*

*** Unique users whose computers have been targeted by web attacks as a percentage of all unique users of Kaspersky Lab products in the country.*

In Q2, Azerbaijan moved up from fourth to first place and became the new leader of this ranking with 32.1%. Russia (30.8%) dropped from first to second, while Kazakhstan (27.03%) fell from second to sixth place.

Since the previous quarter, Spain, Lithuania, Croatia and Turkey have all left the TOP 20. The newcomers to this ranking were Bulgaria (22.06%), Chile (21.56%), Qatar (20.10%) and Portugal (19.84%).



The countries with the safest online surfing environments included Canada (15%), Romania (14.6%), Belgium (13.7%), Mexico (13.2%), the US (12.8%), Switzerland (12. 4%), New Zealand (12.1%), Czech Republic (12%), Argentina (9.9%), Japan (9.5%), the Netherlands (8.3), Sweden (8.2%) and Germany (8%).

On average, 19.4% of computers connected to the Internet globally were subjected to at least one web attack during the three months. This is a fall of 1.8 p.p. compared to Q1 2016.

Local threats

Local infection statistics for user computers are a very important indicator: they reflect threats that have penetrated computer systems by infecting files or removable media, or initially got on the computer in an encrypted format (for example, programs integrated in complex installers, encrypted files, etc.).

Data in this section is based on analyzing statistics produced by antivirus scans of files on the hard drive at the moment they were created or accessed, and the results of scanning removable storage media.

In Q2 2016, Kaspersky Lab's file antivirus detected **249,619,379** unique malicious and potentially unwanted objects.

Countries where users faced the highest risk of local infection

For each of the countries, we calculated the percentage of Kaspersky Lab product users on whose computers the file antivirus was triggered during the quarter. These statistics reflect the level of personal computer infection in different countries.

Top 20 countries with the highest levels of computer infection

	Country*	% of unique users attacked**
1	Somalia	65.80
2	Vietnam	63.33
3	Tajikistan	62.00
4	Russia	61.56
5	Kyrgyzstan	60.80
6	Bangladesh	60.19
7	Afghanistan	60.00
8	Armenia	59,74
9	Ukraine	59.67
10	Nepal	59.66
11	Ethiopia	59.63
12	Laos	58.43
13	Kazakhstan	57.72
14	Rwanda	57.33
15	Djibouti	56.07
16	Yemen	55.98
17	Venezuela	55.76
18	Algeria	55.58
19	Cambodia	55.56
20	Iraq	55.55

These statistics are based on the detection verdicts returned by on-access and on-demand antivirus modules, received from users of Kaspersky Lab products who have consented to provide their statistical data. The data

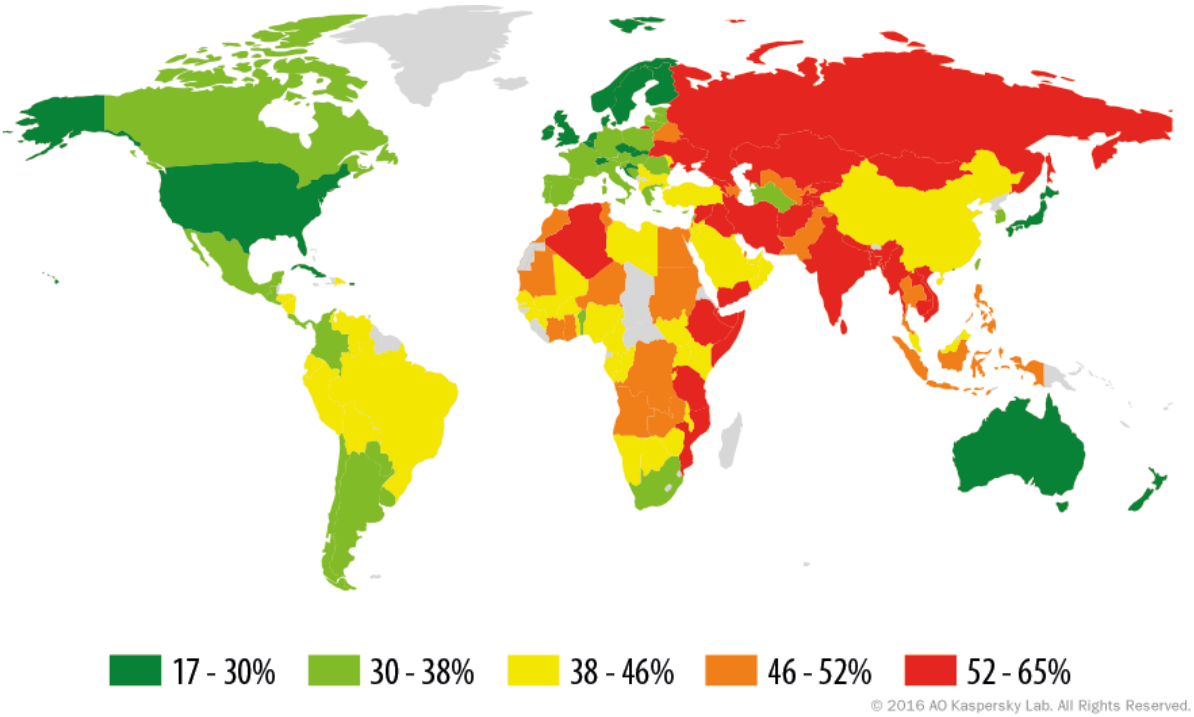
include detections of malicious programs located on users' computers or on removable media connected to the computers, such as flash drives, camera and phone memory cards, or external hard drives.

** These calculations exclude countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).*

*** The percentage of unique users in the country with computers that blocked local threats as a percentage of all unique users of Kaspersky Lab products.*

Somalia remained the leader of this ranking in Q2 2016 with 65.8%. Yemen (55.98%) fell from second to sixteenth place, while Vietnam (63.33%) jumped from eighth to second. Tajikistan (62%) rounded off the TOP 3. Russia moved up one place from fifth to fourth, although the figure for that country declined by 2.62 percentage points to 61.56%.

Newcomers to this ranking are Djibouti in fifteenth place (56.07%), Venezuela in seventeenth (55.76%), and Cambodia in nineteenth (55.56%).



The safest countries in terms of local infection risks were Croatia (29%), Singapore (28.4%), Germany (28.1%), Norway (27.6%), the US (27.1%), Switzerland (26.3%), Japan (22.1%), Denmark (21.4%) and Sweden (21.3%).

An average of 43.3% of computers globally faced at least one local threat during Q2 2016, which is 1.2 p.p. less than in the previous quarter.

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