IT THREAT EVOLUTION IN Q3 2016

David Emm, Roman Unuchek, Maria Garnaeva, Alexander Liskin,
Denis Makrushin, Fedor Sinitsyn

Content

Overview

Targeted attacks and malware campaigns

Dropping Elephant

Targeted attack campaigns don't need to be technically advanced in order to be successful. In July 2016 we reported on a group called Dropping Elephant (also known as 'Chinastrats' and 'Patchwork'). Using a combination of social engineering, old exploit code and some PowerShell-based malware this group was able to steal sensitive data from its victims.

This group, which has been active since November 2015, targets high profile diplomatic and economic organizations linked to China's foreign relations – an interest that is evident from the themes the attackers use to trap their victims.

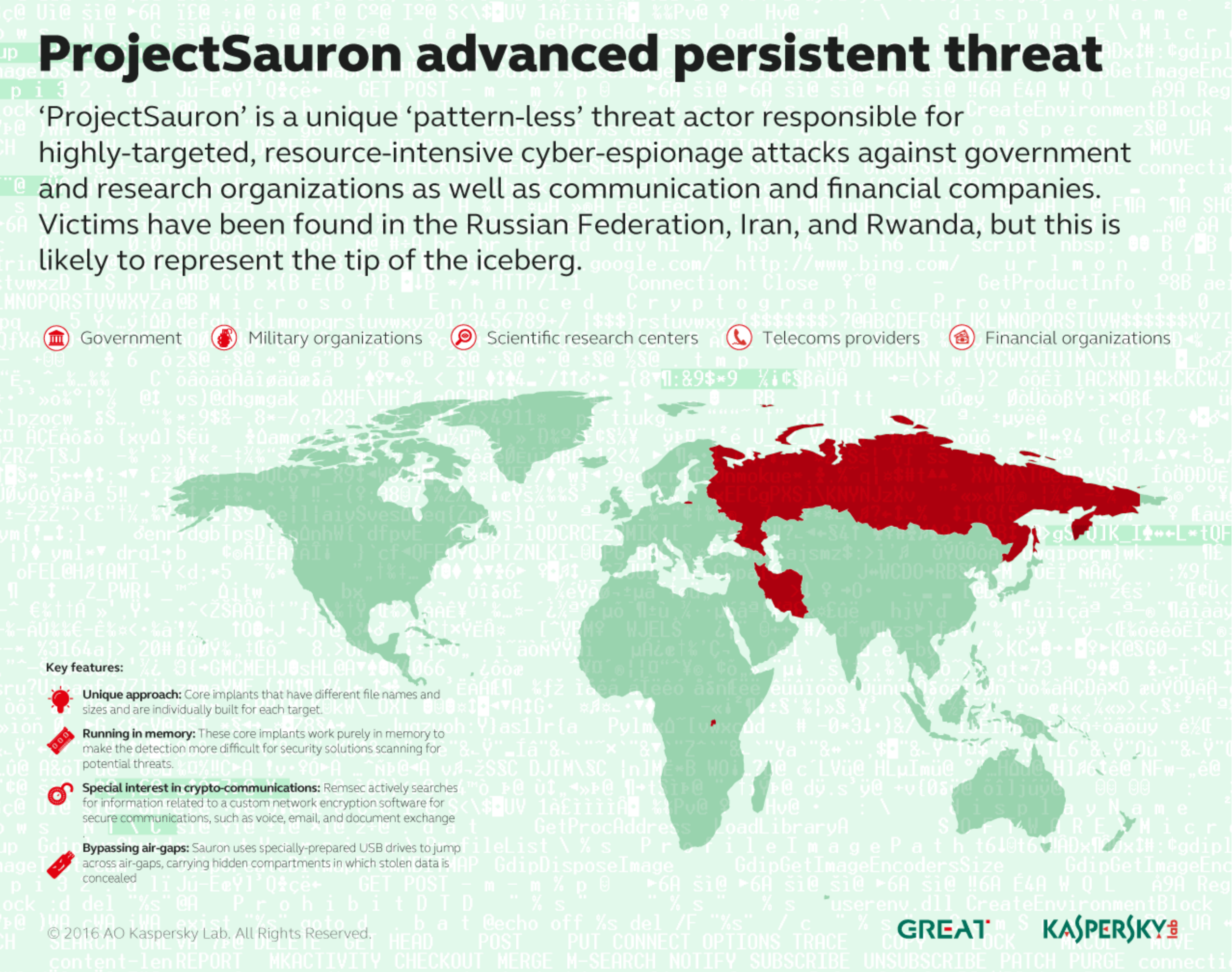
The attackers use a combination of spear-phishing e-mails and watering-hole attacks. The first involves sending a document with remote content. When the victim opens the document, a ping request is sent to the attackers' Command-and-Control (C2) server. The victim then receives a second spear-phishing e-mail, containing either a Word document or a PowerPoint file (these exploit old vulnerabilities – CVE-2012-0158 and CVE-2014-6352 respectively). Once the payload has been executed, a UPX-packed AutoIT executable is dropped on to the system: once executed, this downloads further components from the C2 server and the theft of data from the victim's computer begins.

The attackers also created a watering-hole website that downloads genuine news articles from legitimate websites. If a visitor wants to view the whole article, they are prompted to download a PowerPoint file: this reveals the rest of the document, but also asks the victim to download a malicious object. The attackers sometimes e-mail links to their watering-hole website. In addition, they maintain Google+, Facebook and Twitter accounts, to develop relevant search engine optimization (SEO) and to reach out to wider targets.

The success of the Dropping Elephant group is striking given that no zero-day exploits or advanced techniques were used to target high-profile victims – it's clear that by applying security updates and improving the security awareness of staff, the success of attacks like this can be prevented. At the start of the year we predicted that APT groups would invest less effort in developing sophisticated tools and make greater use of off-the-shelf malware. Dropping Elephant provides a further example of how low investment and use of ready-made toolsets can be very effective when combined with high quality social engineering.

ProjectSauron

In September, our Anti-Targeted Attack Platform flagged an anomaly in the network of a customer's organization. Further investigation led us to uncover ProjectSauron, a group that has been stealing confidential data from organizations in Russia, Iran and Rwanda – and probably other countries – since June 2011. We have identified more than 30 victims: the target organizations all play a key role in providing state services and come from government, military, scientific research, telecommunications and financial sectors.



ProjectSauron advanced persistent threat

'ProjectSauron' is a unique 'pattern-less' threat actor responsible for highly-targeted, resource-intensive cyber-espionage attacks against government and research organizations as well as communication and financial companies. Victims have been found in the Russian Federation, Iran, and Rwanda, but this is likely to represent the tip of the iceberg.

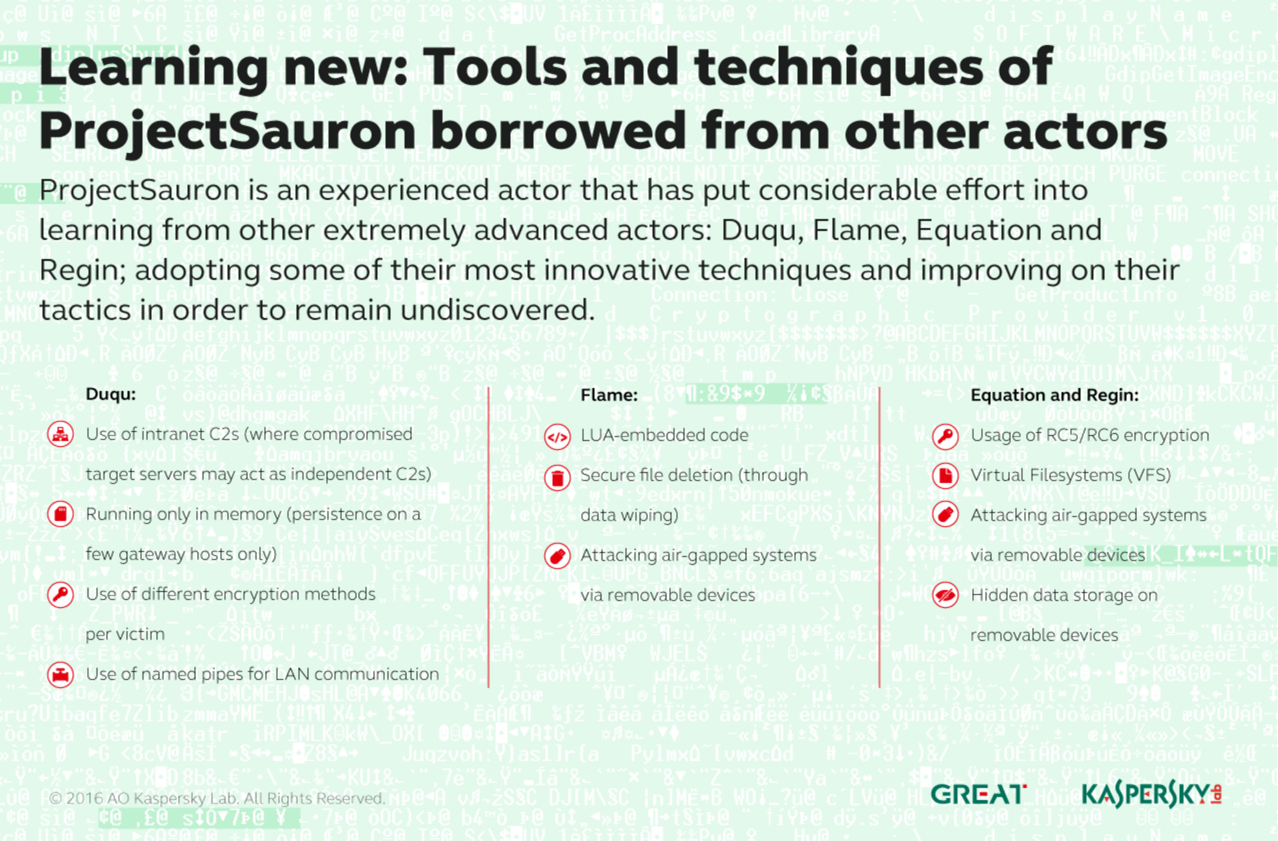
Government · Military organizations · Scientific research centers · Telecoms providers · Financial organizations

Key features:

- **Unique approach:** Core implants that have different file names and sizes and are individually built for each target.
- **Running in memory:** These core implants work purely in memory to make the detection more difficult for security solutions scanning for potential threats.
- **Special interest in crypto-communications:** Remsec actively searches for information related to a custom network encryption software for secure communications, such as voice, email, and document exchange
- **Bypassing air-gaps:** Sauron uses specially-prepared USB drives to jump across air-gaps, carrying hidden compartments in which stolen data is concealed

© 2016 AO Kaspersky Lab. All Rights Reserved.

ProjectSauron is particularly focused on obtaining access to encrypted communications, hunting for them using an advanced, modular cyber-espionage platform that incorporates a set of unique tools and techniques. The cost, complexity, persistence and the ultimate goal of the operation (i.e. stealing secret data from state-related organizations) suggest that ProjectSauron is a state-sponsored campaign. ProjectSauron gives the impression of an experienced threat group that has made a considerable effort to learn from other highly advanced attacks, including Duqu, Flame, Equation and Regin – adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered.



Learning new: Tools and techniques of ProjectSauron borrowed from other actors

ProjectSauron is an experienced actor that has put considerable effort into learning from other extremely advanced actors: Duqu, Flame, Equation and Regin; adopting some of their most innovative techniques and improving on their tactics in order to remain undiscovered.

Duqu:

- Use of intranet C2s (where compromised target servers may act as independent C2s)
- Running only in memory (persistence on a few gateway hosts only)
- Use of different encryption methods per victim
- Use of named pipes for LAN communication

Flame:

- LUA-embedded code
- Secure file deletion (through data wiping)
- Attacking air-gapped systems via removable devices

Equation and Regin:

- Usage of RC5/RC6 encryption
- Virtual Filesystems (VFS)
- Attacking air-gapped systems via removable devices
- Hidden data storage on removable devices

One of the most noteworthy features of ProjectSauron is the deliberate avoidance of patterns: the implants used by the group are customized for each victim and are never re-used. This makes the use of traditional Indicators of Compromise (IoC) almost useless. This approach, along with the use of multiple routes for the exfiltration of stolen data (such as legitimate e-mail channels and DNS) enables ProjectSauron to conduct well-hidden, long-term spying campaigns in targeted networks.

Key features of ProjectSauron:

- core implants that are unique for each victim;
- use of legitimate software update scripts;
- use of backdoors that download new modules or run commands in memory only;
- focus on information relating to custom network encryption software;
- use of low-level tools orchestrated by high-level LUA scripts (the use of LUA is very rare – previously seen only in Flame and Animal Farm attacks;
- use of specially prepared USB drives to jump across air-gapped networks, with hidden compartments for storing stolen data;
- use of multiple exfiltration mechanisms to conceal transfer of data in day-to-day traffic.

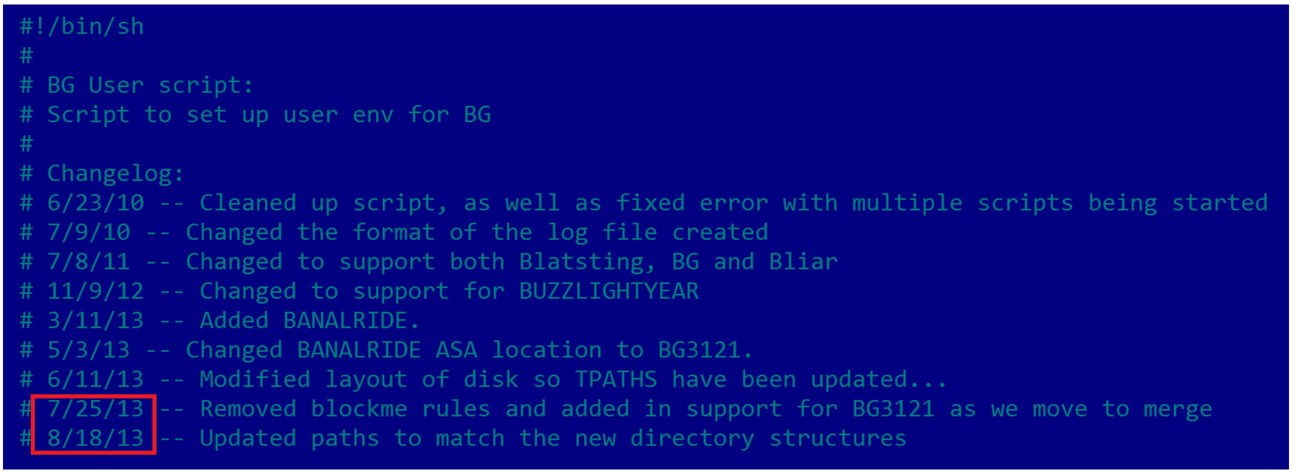
The method used to initially infect victims remains unknown.

The single use of unique methods, such as control server, encryption keys and more, in addition to the adoption of cutting-edge techniques from other major threats groups, is new. The only effective way to withstand such threats is to deploy multiple layers of security, with sensors to monitor for even the slightest anomaly in organizational workflow, combined with threat intelligence and forensic analysis. You can find further discussion of the methods available to deal with such threats here.

ShadowBrokers

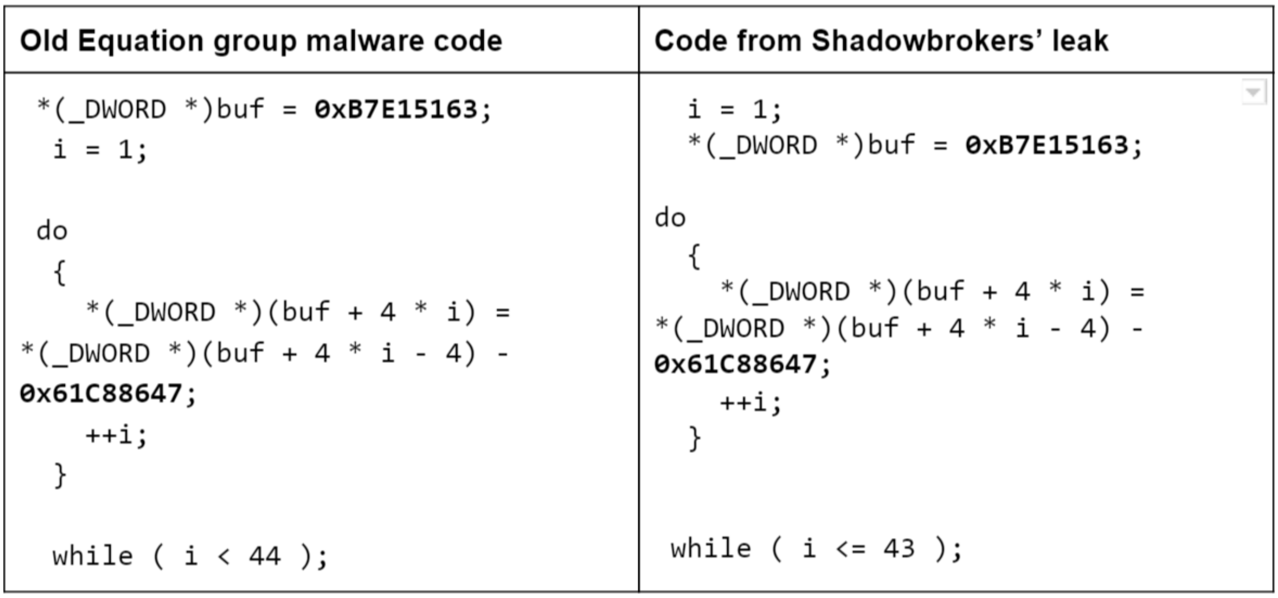
In August, a person or group going under the name 'ShadowBrokers' claimed to possess files belonging to the Equation group. They provided links to two PGP encrypted archives. They provided the password to the first for free, but 'auctioned' the second, setting the price at 1 million BTC (1/15th of the bitcoins in circulation).

Having uncovered the Equation group in February 2015, we were interested in examining the first archive. It contains almost 300MB of firewall exploits, tools and scripts, under cryptonyms such as BANANAUSURPER, BLATSTING and BUZZDIRECTION. Most of the files are at least three years old, with change entries pointing to August 2013 and the newest time-stamp dating to October 2013.



```
#!/bin/sh
#
# BG User script:
# Script to set up user env for BG
#
# Changelog:
# 6/23/10 -- Cleaned up script, as well as fixed error with multiple scripts being started
# 7/9/10 -- Changed the format of the log file created
# 7/8/11 -- Changed to support both Blatsting, BG and Bliar
# 11/9/12 -- Changed to support for BUZZLIGHTYEAR
# 3/11/13 -- Added BANALRIDE.
# 5/3/13 -- Changed BANALRIDE ASA location to BG3121.
# 6/11/13 -- Modified layout of disk so TPATHS have been updated...
# 7/25/13 -- Removed blockme rules and added in support for BG3121 as we move to merge
# 8/18/13 -- Updated paths to match the new directory structures
```

The Equation group makes extensive use of RC5 and RC6 encryption algorithms (these algorithms were designed by Ronald Rivest in 1994 and 1998 respectively). The free trove provided by ShadowBrokers includes 347 different instances of RC5 and RC6 implementations. The implementation is functionally identical with that found in the Equation malware – and has not been seen elsewhere.



Old Equation group malware code

```
 *(_DWORD *)buf = 0xB7E15163;
  i = 1;

 do
  {
    *(_DWORD *)(buf + 4 * i) =
*(_DWORD *)(buf + 4 * i - 4) -
0x61C88647;
    ++i;
  }

  while ( i < 44 );
```

Code from Shadowbrokers' leak

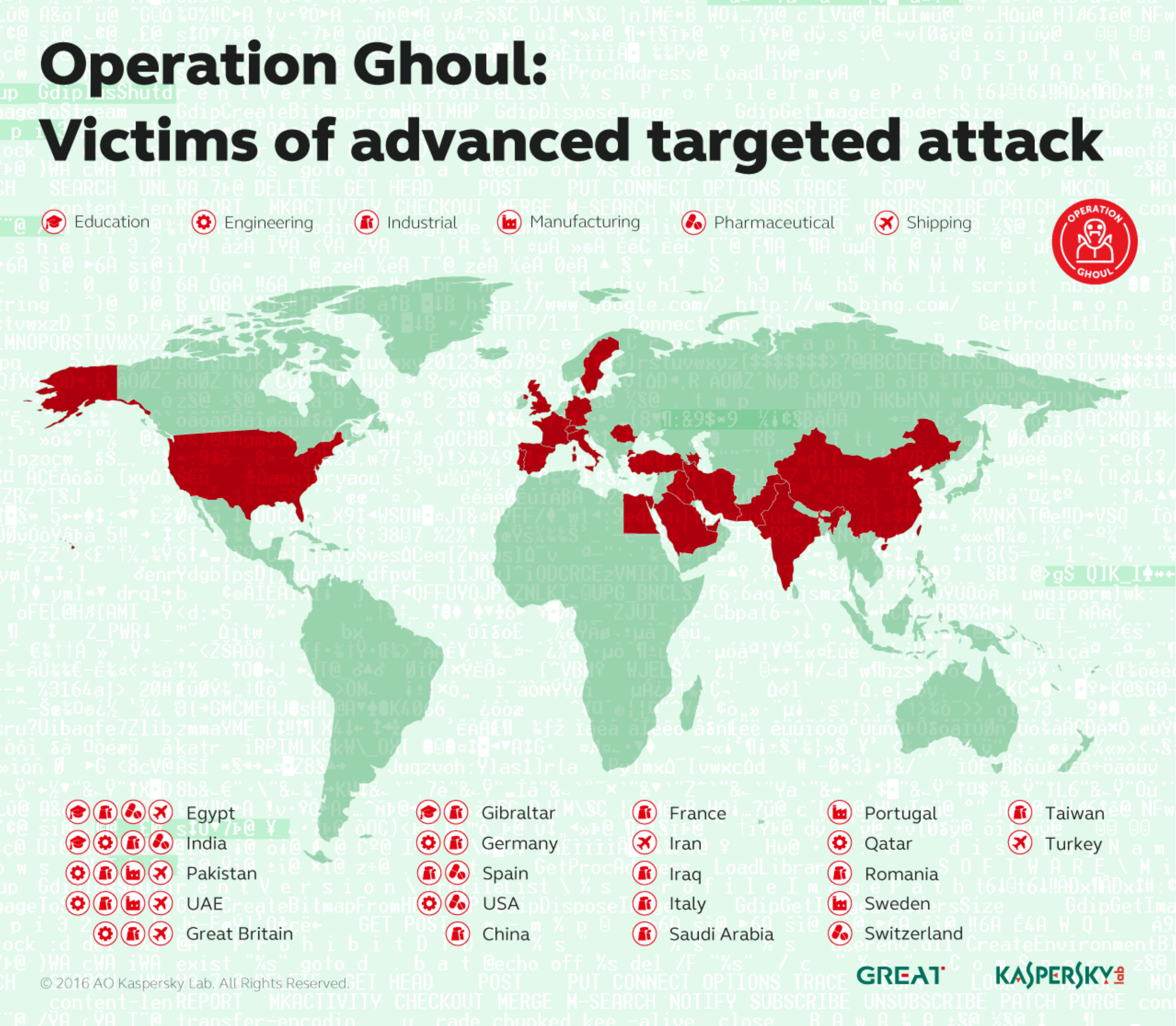
```
  i = 1;
  *(_DWORD *)buf = 0xB7E15163;

do
  {
    *(_DWORD *)(buf + 4 * i) =
*(_DWORD *)(buf + 4 * i - 4) -
0x61C88647;
    ++i;
  }


 while ( i <= 43 );
```

The code similarity makes us believe with a high degree of confidence that the tools from the ShadowBrokers leak are related to the malware from the Equation group.

Operation Ghoul

In June, we noticed a wave of spear-phishing e-mails with malicious attachments. The messages, sent mainly to top and middle level managers of numerous companies, appeared to be coming from a bank in the UAE. The messages claimed to offer payment advice from the bank and included an attached SWIFT document. But the archive really contained malware. Further investigation revealed that the June attacks were the most recent operation of a group that researchers had been tracking for more than a year, named Operation Ghoul by Kaspersky Lab.

The group successfully attacked more than 130 organizations from 30 countries, including Spain, Pakistan, UAE, India, Egypt, the United Kingdom, Germany and Saudi Arabia. Based on information obtained from the sink-hole of some C2 servers, the majority of the target organizations work in the industrial and engineering sectors. Others include shipping, pharmaceutical, manufacturing, trading and educational organizations.



The malware used by the Operation Ghoul group is based on the commercial spyware kit Hawkeye, sold openly on the Dark Web. Once installed, the malware collects interesting data from the victim's computer, including keystrokes, clipboard data, FTP server credentials, account data from browsers, messaging clients, e-mail clients and information about installed applications. This data is sent to the group's C2 servers.

The aim of the campaign seems to be financial profit – all the targeted organizations hold valuable data that can be sold on the black market.

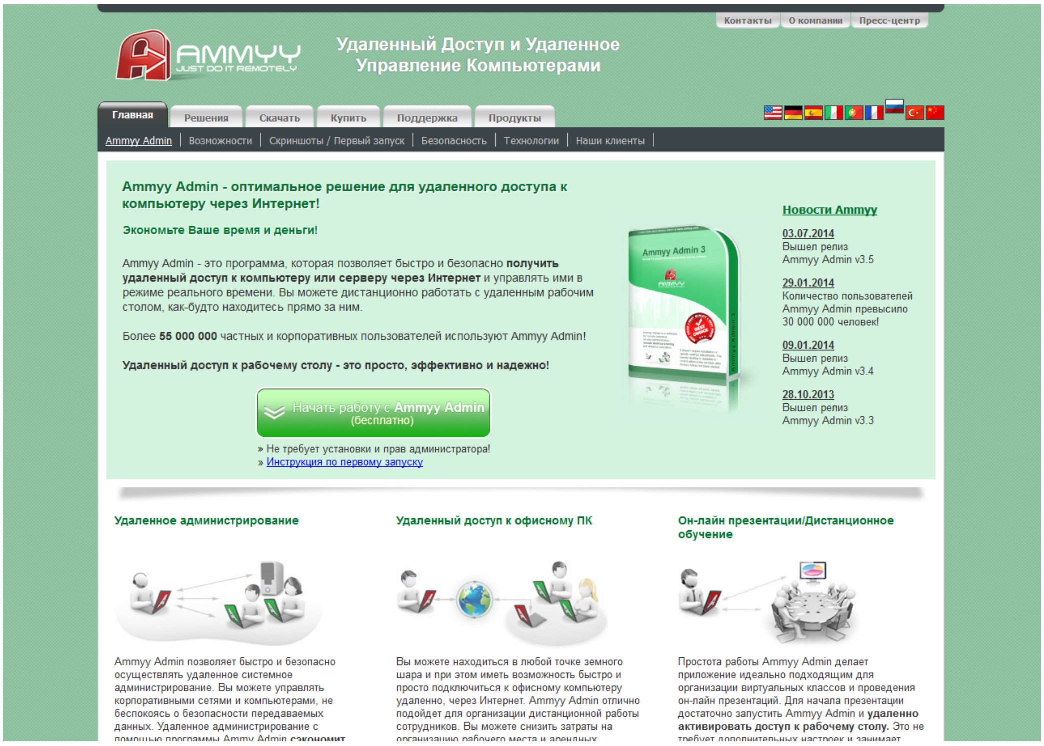
The continued success of social engineering as a way of gaining a foothold in target organizations highlights the need for businesses to make staff awareness and education a central component of their security strategy.

Malware stories

Lurk

In June 2016 we reported on the Lurk banking Trojan, used to systematically siphon money from the accounts of commercial organizations in Russia – among them, a number of banks. The police estimate the losses caused by this Trojan at around $45 million.

During our research into this Trojan, it became apparent that victims of Lurk had also installed the remote administration software, Ammyy Admin. While we didn't give it much thought at first, it became apparent that the official Ammyy Admin website had been compromised and was being used by the Lurk gang as part of a watering-hole attack: the Trojan was downloaded to victim's computers along with the legitimate software.



Ammyy Admin - оптимальное решение для удаленного доступа к компьютеру через Интернет!

Экономьте Ваше время и деньги!

Ammyy Admin - это программа, которая позволяет быстро и безопасно **получить удаленный доступ к компьютеру или серверу через Интернет** и управлять ими в режиме реального времени. Вы можете дистанционно работать с удаленным рабочим столом, как-будто находитесь прямо за ним.

Более **55 000 000** частных и корпоративных пользователей используют Ammyy Admin!

Удаленный доступ к рабочему столу - это просто, эффективно и надежно!

» Не требует установки и прав администратора!
» Инструкция по первому запуску

Новости Ammyy

03.07.2014
Вышел релиз
Ammyy Admin v3.5

29.01.2014
Количество пользователей
Ammyy Admin превысило
30 000 000 человек!

09.01.2014
Вышел релиз
Ammyy Admin v3.4

28.10.2013
Вышел релиз
Ammyy Admin v3.3

Удаленное администрирование

Ammyy Admin позволяет быстро и безопасно осуществлять удаленное системное администрирование. Вы можете управлять корпоративными сетями и компьютерами, не беспокоясь о безопасности передаваемых данных. Удаленное администрирование с помощью программы Ammy Admin **сэкономит**

Удаленный доступ к офисному ПК

Вы можете находиться в любой точке земного шара и при этом иметь возможность быстро и просто подключиться к офисному компьютеру удаленно, через Интернет. Ammyy Admin отлично подойдет для организации дистанционной работы сотрудников. Вы можете снизить затраты на организацию рабочего места и арендных

Он-лайн презентации/Дистанционное обучение

Простота работы Ammyy Admin делает приложение идеально подходящим для организации виртуальных классов и проведения он-лайн презентаций. Для начала презентации достаточно запустить Ammyy Admin и **удаленно активировать доступ к рабочему столу.** Это не требует дополнительных настроек и занимает

The dropper on the Ammyy Admin site started distributing a different Trojan on 1 June 2016, 'Trojan-PSW.Win32.Fareit': this was the day that the alleged creators of the Lurk Trojan were arrested. It seems that those responsible for the Ammyy Admin website breach were happy to sell their Trojan dropper to anyone who wanted to distribute malware from the compromised site.

The banking Trojan wasn't the only cybercriminal activity the Lurk group was involved in. The group also developed the Angler exploit kit, a set of malicious programs designed to exploit vulnerabilities in widespread software to install malware. This exploit kit was originally developed to provide a reliable and effective delivery channel for the group's malware. However, in 2013 the group started to rent out the kit to anyone who was willing to pay for it – probably to help pay for the group's huge network infrastructure and large number of 'staff'. The Angler exploit kit became one of the most powerful tools available on the criminal underground. Unlike the Lurk banking Trojan, which focused on victims in Russia, Angler has been used by attackers across the world – including the groups behind the CryptXXX and TeslaCrypt ransomware and the Neverquest banking Trojan (the latter was used against almost 100 banks). The operations of Angler were disrupted after the arrest of the alleged members of the Lurk group.

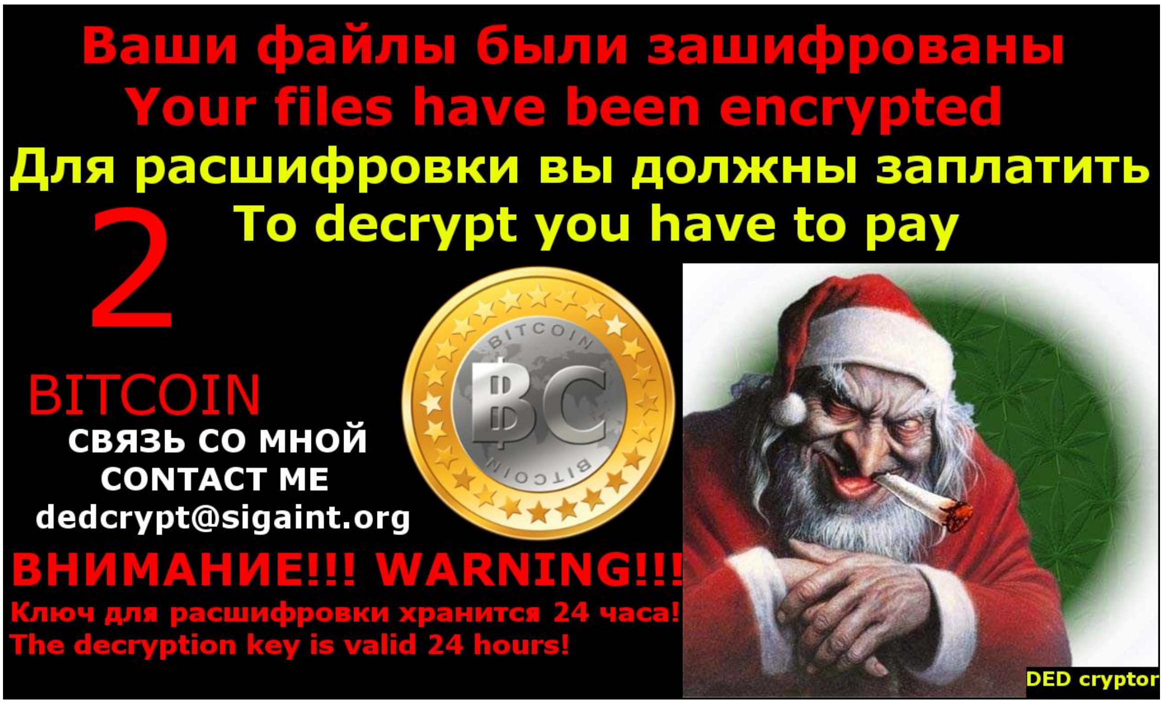
The group was involved in other side activities too. For more than five years, the group moved from developing very powerful malware for automated money theft with Remote Banking Services software, to sophisticated theft involving SIM-card swap fraud, to becoming hacking specialists familiar with the internal infrastructure of banks.

Kaspersky Lab provided assistance to the Russian police in the investigation into the group behind the Lurk Trojan. The arrests marked the culmination of a six-year investigation by our Computer Incidents Investigation Team. You can read about the investigation here.

Ransomware

Hardly a month goes by without reports of ransomware attacks in the media: for example, a recent report suggested that 28 NHS trusts in the UK have fallen victim to ransomware in the last 12 months. Most ransomware attacks are directed at consumers, but a significant proportion target businesses (around 13 per cent in 2015-16). The Kaspersky Lab IT Security Risks Survey 2016 indicated that around 42 per cent of small and medium businesses became victims of ransomware in the 12 months up to August 2016.

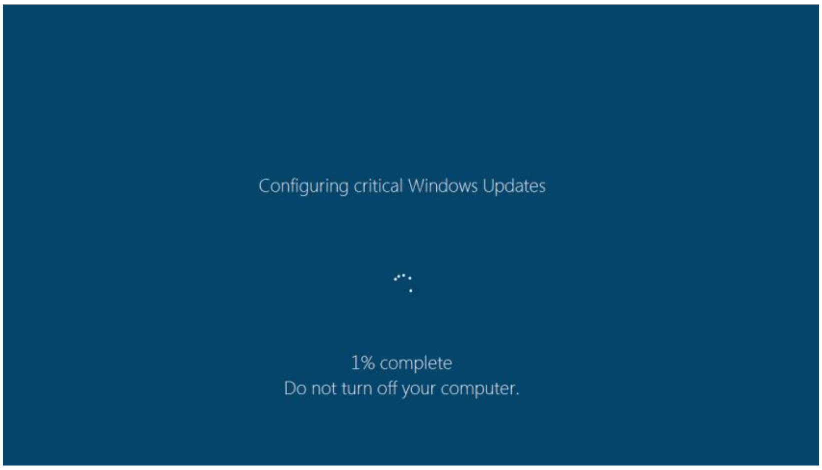
One recent ransomware campaign demanded a massive two bitcoins (around $1,300) as a ransom. The ransomware program, named Ded Cryptor, changes the wallpaper on the victim's computer to a picture of an evil-looking Santa Claus.



Ваши файлы были зашифрованы
Your files have been encrypted
Для расшифровки вы должны заплатить
To decrypt you have to pay
2
BITCOIN
СВЯЗЬ СО МНОЙ
CONTACT ME
dedcrypt@sigaint.org
ВНИМАНИЕ!!! WARNING!!!
Ключ для расшифровки хранится 24 часа!
The decryption key is valid 24 hours!

The modus operandi of this program (i.e. encrypted files, scary image, and ransom demand) is unremarkable, but the pre-history of this attack is interesting. It is based on the EDA2 open-source ransomware code, developed by Utku Sen as part of a failed experiment. Utku Sen, a security expert from Turkey, created a ransomware program and published the code online. He realized that cybercriminals would use the code to create their own cryptors, but hoped that this would help security researchers to understand how cybercriminals think and code, thereby making their own efforts to block ransomware more effective.

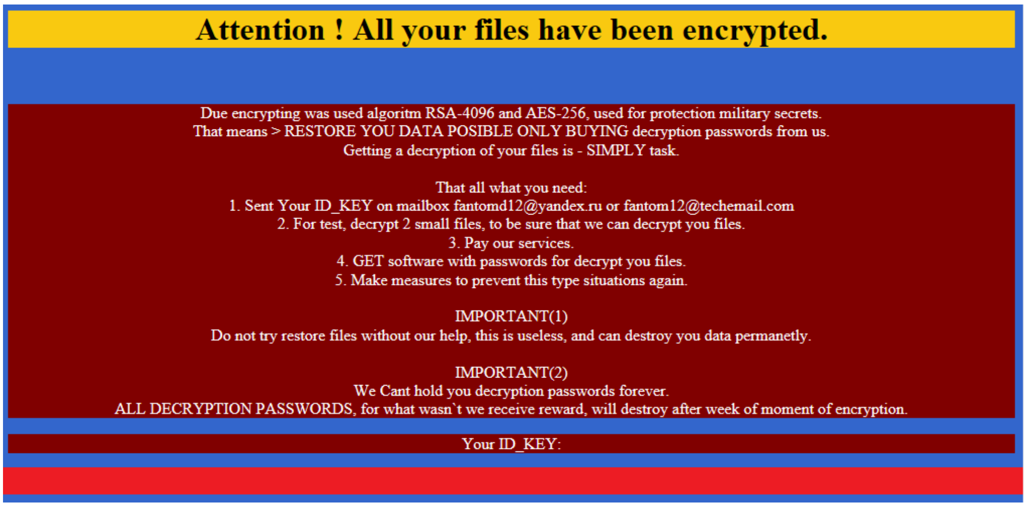
Ded Cryptor was just one of many ransomware programs spawned by EDA2. Another such program that we saw recently was Fantom. This was interesting not just because of its connection to EDA2, but because it simulates a genuine-looking Windows update screen



Configuring critical Windows Updates

1% complete
Do not turn off your computer.

This is displayed while Fantom is encrypting the victim's files in the background. The fake update program runs in full-screen mode, visually blocking access to other programs and distracting the victim from what's really happening. Once the encryption has been completed, Fantom displays a more typical message.



Attention ! All your files have been encrypted.

Due encrypting was used algoritm RSA-4096 and AES-256, used for protection military secrets.
That means > RESTORE YOU DATA POSIBLE ONLY BUYING decryption passwords from us.
Getting a decryption of your files is - SIMPLY task.

That all what you need:
1. Sent Your ID_KEY on mailbox fantomd12@yandex.ru or fantom12@techemail.com
2. For test, decrypt 2 small files, to be sure that we can decrypt you files.
3. Pay our services.
4. GET software with passwords for decrypt you files.
5. Make measures to prevent this type situations again.

IMPORTANT(1)
Do not try restore files without our help, this is useless, and can destroy you data permanetly.

IMPORTANT(2)
We Cant hold you decryption passwords forever.
ALL DECRYPTION PASSWORDS, for what wasn`t we receive reward, will destroy after week of moment of encryption.

Your ID_KEY:

There's no doubt that public awareness of the problem is growing, but it's clear that consumers and organizations alike are not doing enough to combat the threat; and cybercriminals are capitalising on this – this is clearly reflected in the growing number of ransomware attacks.

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.

If you do find yourself in a situation where your files are encrypted and you don't have a backup, ask your anti-malware vendor if they can help and check the No More Ransom website, to see if it holds the keys to decrypt your data. This is a joint initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky Lab and Intel Security – designed to help victims of ransomware retrieve their encrypted data without paying cybercriminals.

In a recent 'ask the expert' session, Jornt van der Wiel, an expert from Kaspersky Lab's Global Research and Analysis Team, provided useful insights into ransomware.

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 data leaks from the official forum of DotA 2, Yahoo 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. 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.

It's also a good idea to use two-factor authentication, where an online provider offers this feature – 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.

Given the potential impact of a security breach, it's hardly surprising to see regulatory authorities paying closer attention to the issue. The UK Information Commissioner's Office (ICO) recently issued a record fine of £400,000 to Talk Talk for the company's 'failure to implement the most basic cyber security measures', related to the attack on the company in October 2015. In the view of the ICO, the record fine 'acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue'.

The EU General Data Protection Regulation (GDPR), which comes into force in May 2018, will require companies to notify the regulator of data breaches, with significant fines for failure to secure personal data. You can find an overview of the regulation here.

We took a look back at the impact of the Ashley Madison breach, one year after the attack that led to the leak of customer data, offering some good tips to anyone who might be considering looking online for love (and good advice for managing any online account).

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.

Q3 figures

- According to KSN data, Kaspersky Lab solutions detected and repelled **171,802,109** malicious attacks from online resources located in 190 countries all over the world.
- **45,169,524** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **12,657,673** 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 **1,198,264** user computers.
- Crypto ransomware attacks were blocked on **821,865** computers of unique users.
- Kaspersky Lab's file antivirus detected a total of **116,469,744** unique malicious and potentially unwanted objects.
- Kaspersky Lab mobile security products detected:
    - **1,520,931** malicious installation packages;
    - **30,167** mobile banker Trojans (installation packages);
    - **37,150** mobile ransomware Trojans (installation packages).

Mobile threats

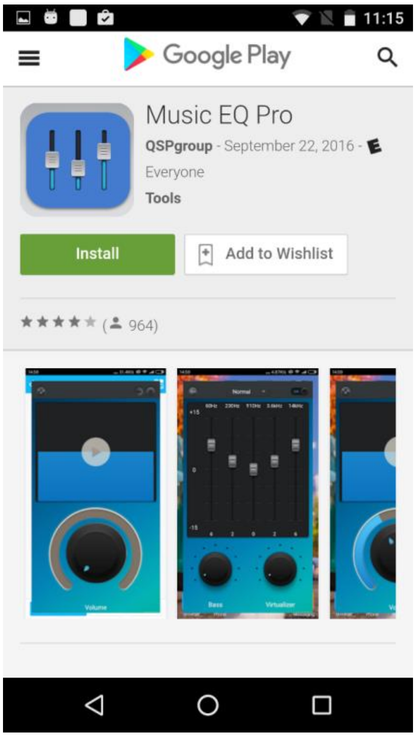
Q3 events

Pokémon GO: popular with users and hackers

One of the most significant events of the third quarter was the release of Pokémon GO. Of course, cybercriminals could not ignore such a popular new product and tried to exploit the game for their own purposes. This was primarily done by adding malicious code to the original app and spreading malicious versions via third-party stores. This method was used, for example, to spread Trojan-Banker.AndroidOS.Tordow, which exploits vulnerabilities in the system to obtain root access to a device. With root access, this Trojan protects itself from being deleted, and it can also steal saved passwords from browsers.

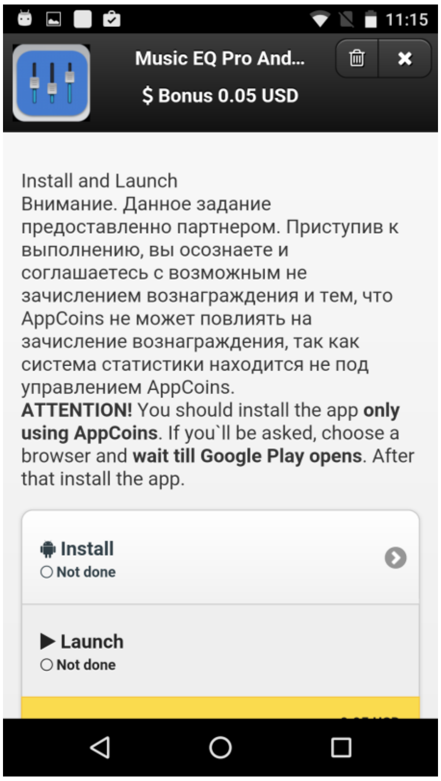
But perhaps the most notable case of Pokémon GO's popularity being used to infect mobile devices involved fraudsters publishing a guide for the game in the official Google Play store. The app turned out to be an advertising Trojan capable of gaining root access to a device by exploiting vulnerabilities in the system.

We later came across two more modifications of this Trojan, which were added to Google Play under the guise of different apps. According to Google Play data, one of them, imitating an equalizer, was installed between 100,000 and 500,000 times.


Music EQ Pro
QSPgroup - September 22, 2016 -
Everyone
Tools

Trojan.AndroidOS.Ztorg.ad in the official Google Play store

Interestingly, one of the methods used by the cybercriminals to promote the Trojan was a company that pays users for the installation of advertising apps.



Music EQ Pro And...

$ Bonus 0.05 USD

Install and Launch
Внимание. Данное задание предоставленно партнером. Приступив к выполнению, вы осознаете и соглашаетесь с возможным не зачислением вознаграждения и тем, что AppCoins не может повлиять на зачисление вознаграждения, так как система статистики находится не под управлением AppCoins.
ATTENTION! You should install the app **only using AppCoins**. If you`ll be asked, choose a browser and **wait till Google Play opens**. After that install the app.

Install
○ Not done

▶ **Launch**
○ Not done

Screenshot of the app that prompts the user to install the Trojan for 5 cents

According to this company's rules, it doesn't work with users whose devices have root access. The users may be looking to earn some money, but they end up with an infected device and don't actually receive any money, because after infection the device gains root access.

Ad with a Trojan

The most popular mobile Trojan in the third quarter of 2016 was Trojan-Banker.AndroidOS.Svpeng.q. During the quarter, the number of users attacked by it grew almost eightfold.

Over 97% of users attacked by Svpeng were located in Russia. The attackers managed to make the Trojan so popular by advertising it via Google AdSense – one of the most popular advertising networks on the Russian Internet. Many popular sites use it to display targeted advertising. Anyone can pay to register their ad on the network, and that was exactly what the attackers did.

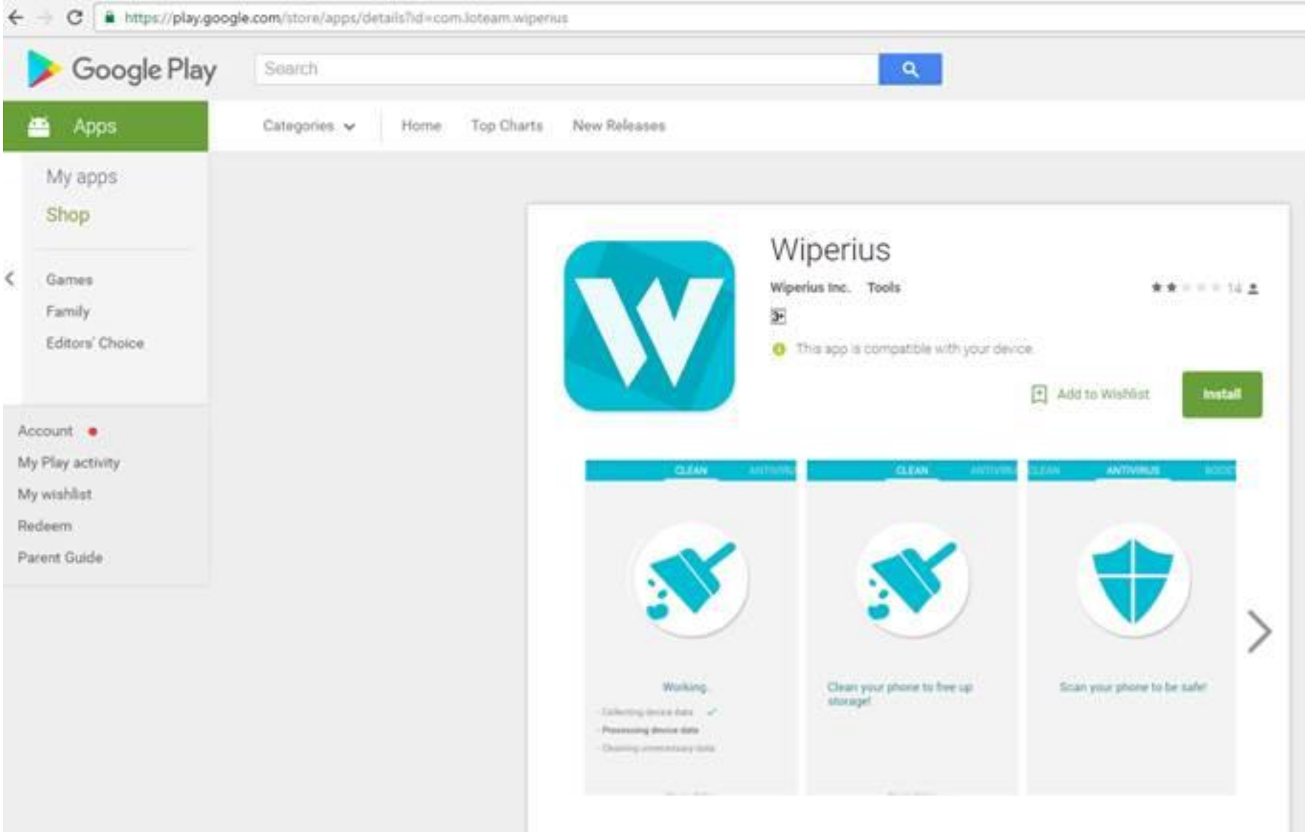
Along with the advert, however, they added the AdSense Trojan. When a user visited the page with the advert, Svpeng was downloaded to their device.

Bypassing protection mechanisms in Android 6

In our report for the second quarter of 2016 we mentioned the Trojan-Banker.AndroidOS.Asacub family that can bypass several system controls. Of special note this quarter is the Trojan-Banker.AndroidOS.Gugi family that has learned to bypass the security mechanisms introduced in Android 6 by tricking the user. The Trojan first requests rights to overlay other applications, and then uses those rights to trick the user into giving it privileges to work with text messages and to make calls.

Trojan ransomware in the Google Play store

In the third quarter, we registered the propagation of Trojan-Ransom.AndroidOS.Pletor.d, a mobile ransomware program, via Google Play. The Trojan imitated an app for servicing devices, including deleting unnecessary data, speeding up device performance and even antivirus protection.

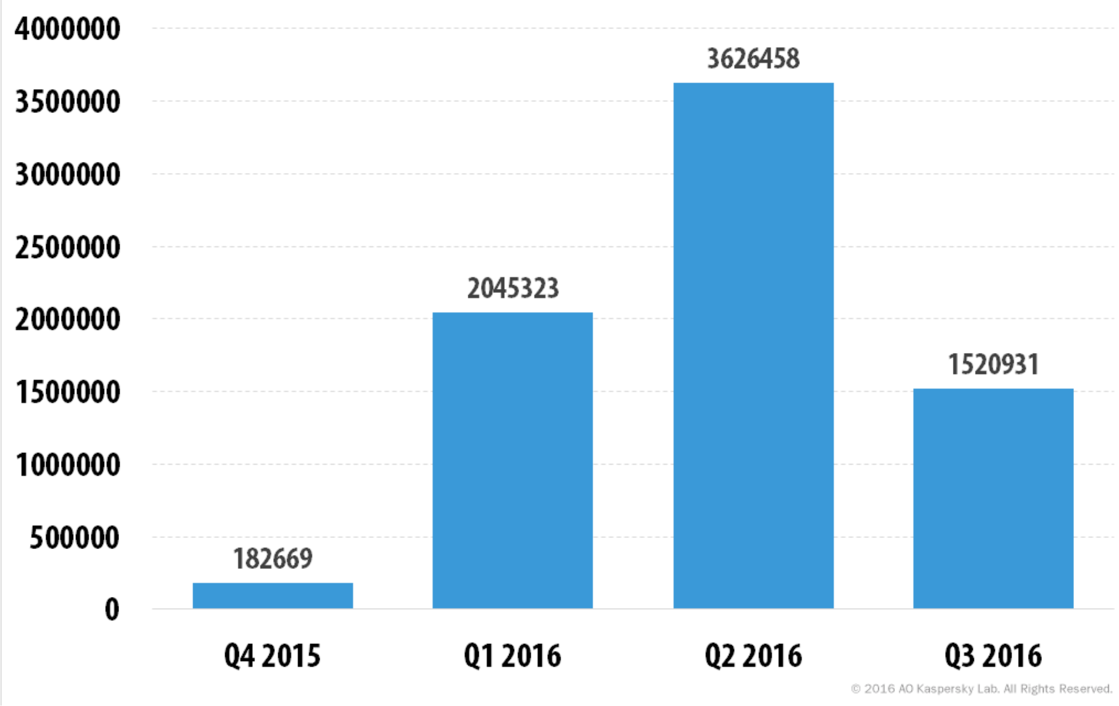


Trojan-Ransom.AndroidOS.Pletor.d in Google Play

The Trojan checks which country the device is located in, and if it is not Russia or Ukraine, it requests administrator rights and calls the command server. Earlier versions of this Trojan encrypted user data, but this modification doesn't possess such functionality. Instead, the Trojan blocks operation of the device by opening a window that covers all other open windows and demanding a ransom to unblock it.

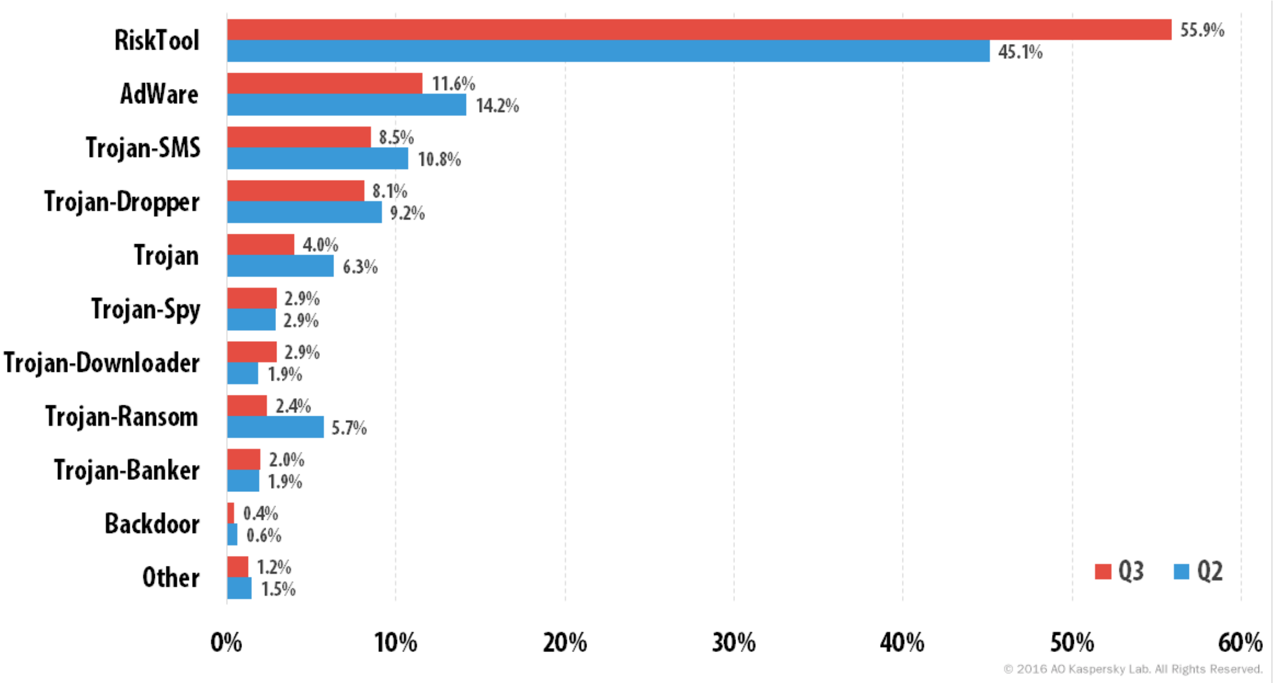
Mobile threat statistics

In Q3 2016, Kaspersky Lab detected **1,520,931** malicious installation packages, which is 2.3 times fewer than in the previous quarter.



Number of detected malicious installation packages (Q4 2015 – Q1 2016)

Distribution of mobile malware by type



Distribution of new mobile malware by type (Q2 2016 and Q3 2016)

In Q3 2016, RiskTool software, or legitimate applications that are potentially dangerous to users, topped the rating of malicious objects detected for mobile devices. Their share continued to grow from 45.1% in Q2 to 55.8% this quarter.

Due to the large number of RiskTool programs and the considerable increase in their overall share of the total flow of detected objects, the proportion of almost all other types of malicious programs decreased, even where the actual *number* of detected programs increased compared to the previous quarter.

The most affected was Trojan-Ransom – its share decreased from 5.72% to 2.37%. This was caused by a decline in activity by the Trojan-Ransom.AndroidOS.Fusob family (covered in more detail below).

At the same time, we registered a slight growth in the share of Trojan-Bankers – from 1.88% to 1.98%.

TOP 20 mobile malware programs

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

	Name	% of attacked users*
1	DangerousObject.Multi.Generic	78,46
2	Trojan-Banker.AndroidOS.Svpeng.q	11,45
3	Trojan.AndroidOS.Ztorg.t	8,03
4	Backdoor.AndroidOS.Ztorg.c	7,24
5	Backdoor.AndroidOS.Ztorg.a	6,55
6	Trojan-Dropper.AndroidOS.Agent.dm	4,91
7	Trojan.AndroidOS.Hiddad.v	4,55
8	Trojan.AndroidOS.Agent.gm	4,25
9	Trojan-Dropper.AndroidOS.Agent.cv	3,67
10	Trojan.AndroidOS.Ztorg.aa	3,61
11	Trojan-Banker.AndroidOS.Svpeng.r	3,44
12	Trojan.AndroidOS.Ztorg.pac	3,31
13	Trojan.AndroidOS.Iop.c	3,27
14	Trojan.AndroidOS.Muetan.b	3,17
15	Trojan.AndroidOS.Vdloader.a	3,14
16	Trojan-Dropper.AndroidOS.Triada.s	2,80
17	Trojan.AndroidOS.Muetan.a	2,77

18	Trojan.AndroidOS.Triada.pac	2,75
19	Trojan-Dropper.AndroidOS.Triada.d	2,73
20	Trojan.AndroidOS.Agent.eb	2,63

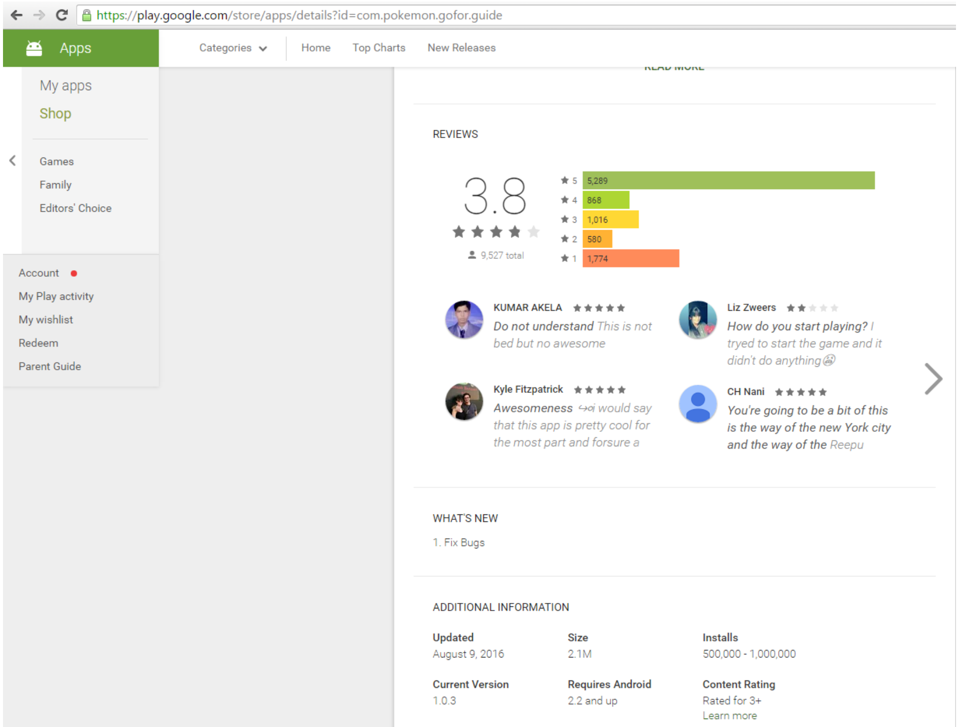
** Percentage of unique users attacked by the malware in question, relative to all users of Kaspersky Lab's mobile security product that were attacked.*

First place is occupied by DangerousObject.Multi.Generic (78.46%), the verdict used for malicious programs detected using 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.

In Q3 2016, 17 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.

With root access on the device, Trojans can do many different things without the user being aware, such as installing apps from Google Play, including paid apps.

It's worth noting that the Trojans from the Ztorg family, which occupied four places in the TOP 20, are often distributed via the official Google Play store. Since the end of 2015, we have registered more than 10 such cases (including a fake guide for Pokemon GO). Several times the Trojan notched up over 100,000 installations, and on one occasion it was installed more than 500,000 times.



https://play.google.com/store/apps/details?id=com.pokemon.gofor.guide

REVIEWS

3.8

9,527 total

★ 5	5,289
★ 4	868
★ 3	1,016
★ 2	580
★ 1	1,774

KUMAR AKELA ★★★★★
Do not understand This is not bed but no awesome

Liz Zweers ★★
How do you start playing? I tryed to start the game and it didn't do anything😩

Kyle Fitzpatrick ★★★★★
Awesomeness ↪oi would say that this app is pretty cool for the most part and forsure a

CH Nani ★★★★★
You're going to be a bit of this is the way of the new York city and the way of the Reepu

WHAT'S NEW

1. Fix Bugs

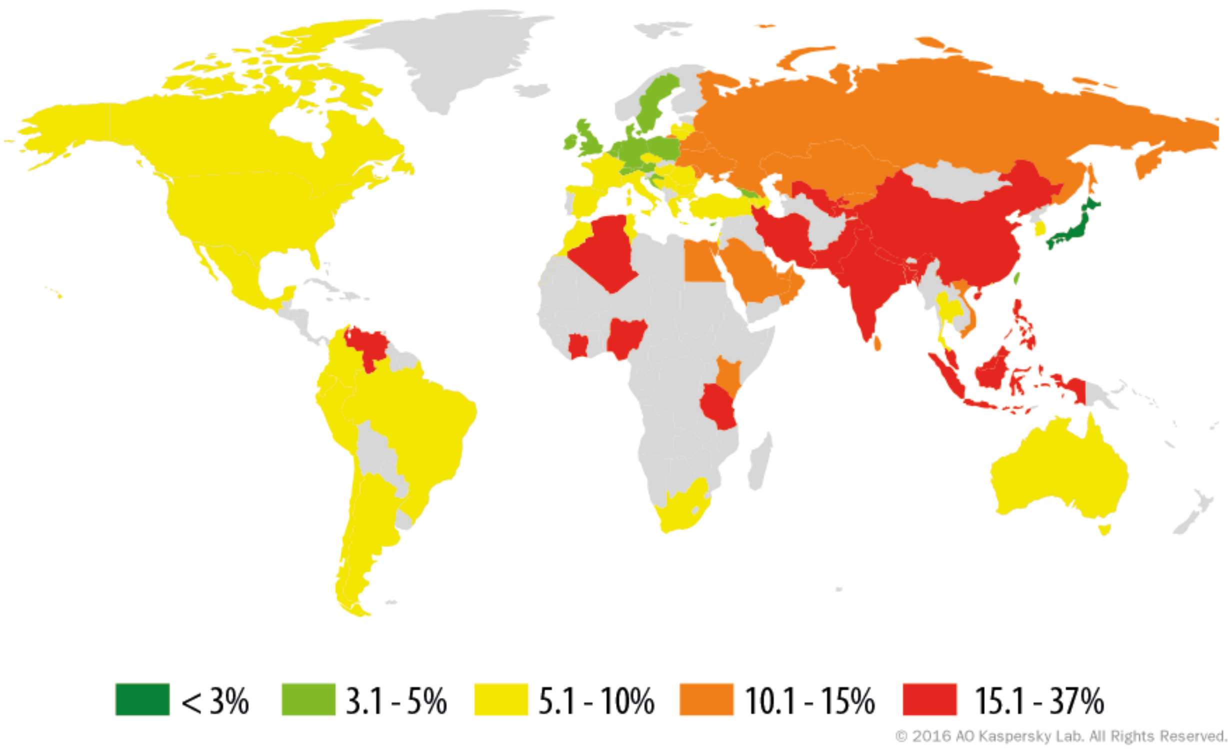
ADDITIONAL INFORMATION

Updated	Size	Installs
August 9, 2016	2.1M	500,000 - 1,000,000
Current Version	**Requires Android**	**Content Rating**
1.0.3	2.2 and up	Rated for 3+ Learn more

Trojan.AndroidOS.Ztorg.ad masquerading as a guide for Pokemon GO in Google Play

The ranking also included two representatives of the Trojan-Banker.AndroidOS.Svpeng mobile banker family. As we mentioned above, Svpeng.q became the most popular malware in the third quarter of 2016. This was down to the Trojan being distributed via the AdSense advertising network, which is used by a large number of sites on the Russian segment of the Internet.

The geography of mobile threats



The geography of attempted mobile malware infections in Q3 2016 (percentage of all users attacked)

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

	Country*	% of users attacked **
1	Bangladesh	**35,57**
2	Nepal	**31.54**
3	Iran	**31.38**
4	China	**26.95**
5	Pakistan	**26.83**
6	Indonesia	**26.33**
7	India	**24,35**

8	Nigeria	**22.88**
9	Algeria	**21,82**
10	The Philippines	**21.67**

** We eliminated countries from this rating where the number of users of Kaspersky Lab's mobile security product is relatively low (under 10,000).*
*** Percentage of unique users attacked in each country relative to all users of Kaspersky Lab's mobile security product in the country.*

Bangladesh topped the rating, with almost 36% of users there encountering a mobile threat at least once during the quarter. China, which came first in this rating two quarters in a row, dropped to fourth place.

The most popular mobile malware in all the countries of this rating (except China) was the same – advertising Trojans that mostly belonged to the Ztorg, Iop, Hiddad and Triada families. A significant proportion of attacks in China also involved advertising Trojans, but the majority of users there encountered Trojans from the Backdoor.AndroidOS.GinMaster and Backdoor.AndroidOS.Fakengry families.

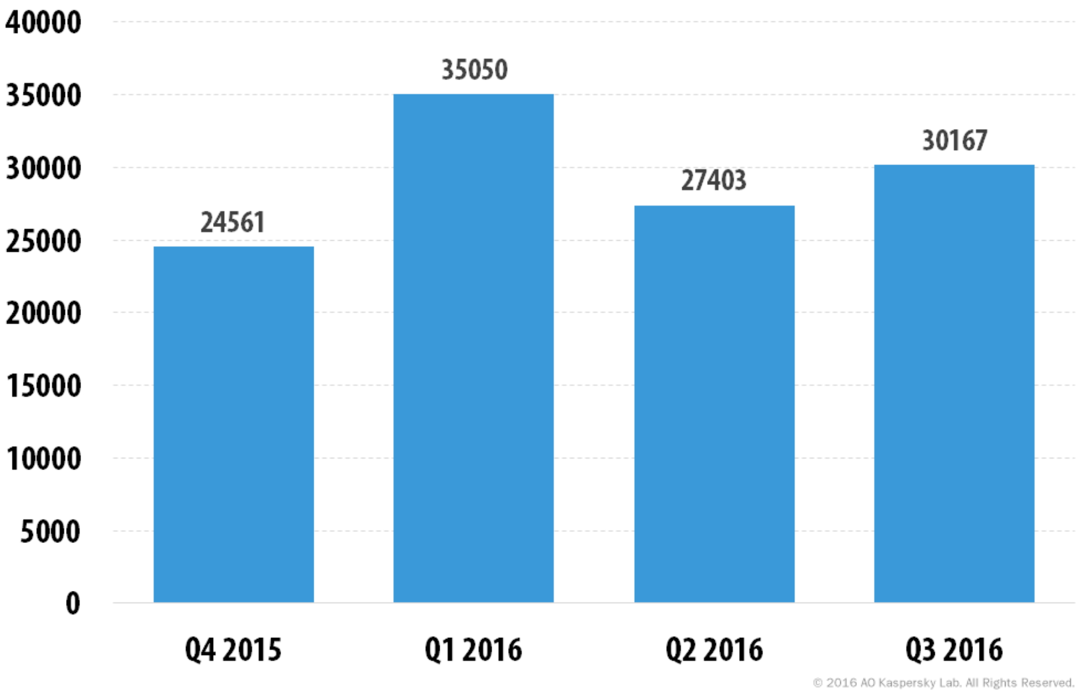
Russia (12.1%) came 24th in this rating, France (6.7%) 52nd, the US (5.3%) 63rd, Italy (5.1%) 65th, Germany (4.9%) 68th, and the United Kingdom (4.7%) 71st.

The situation in Germany and Italy has improved significantly: in the previous quarter, 8.5% and 6.2% of users in those countries respectively were attacked. This was due to a decline in activity by the Fusob family of mobile ransomware.

The safest countries were Austria (3.3%), Croatia (3.1%) and Japan (1.7%).

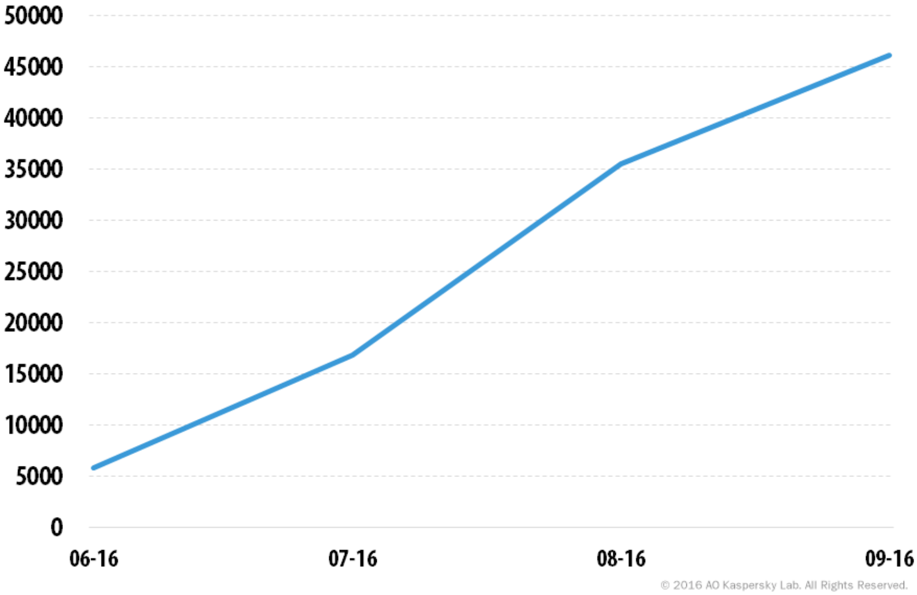
Mobile banking Trojans

Over the reporting period, we detected **30,167** installation packages for mobile banking Trojans, which is 1.1 times as many as in Q2.



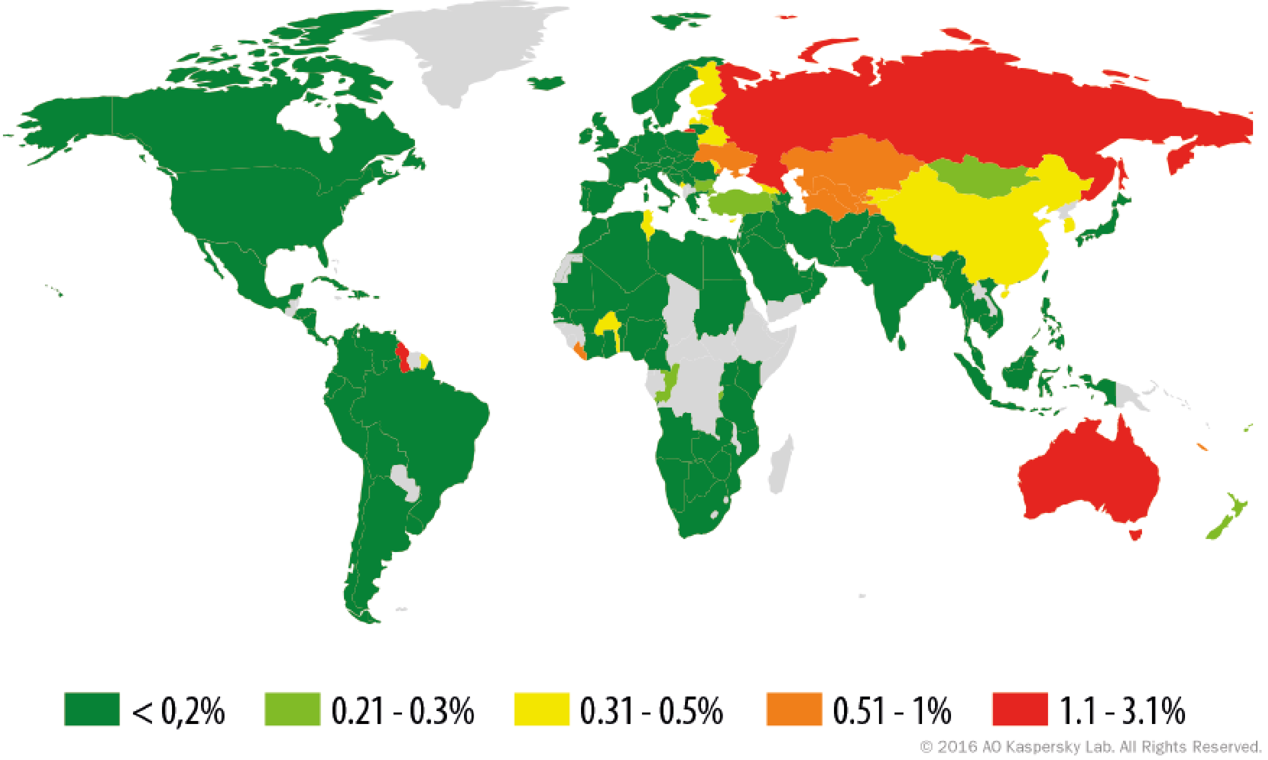
Number of installation packages for mobile banking Trojans detected by Kaspersky Lab solutions (Q4 2015 – Q3 2016)

Trojan-Banker.AndroidOS.Svpeng became the most popular mobile banking Trojan in Q3 due to its active distribution via the advertising network AdSense. More than half the users that encountered mobile banking Trojans in the third quarter faced Trojan-Banker.AndroidOS.Svpeng.q. It was constantly increasing the rate at which it spread – in September the number of users attacked by the Trojan was almost eight times greater than in June.



The number of unique users attacked by the Trojan-Banker.AndroidOS.Svpeng banking Trojan family (June-September 2016)

Over 97% of attacked users were in Russia. This family of mobile banking Trojans uses phishing windows to steal credit card data and logins and passwords from online banking accounts. In addition, fraudsters steal money via SMS services, including mobile banking.



Geography of mobile banking threats in Q3 2016 (percentage of all users attacked)

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

	Country*	% of users attacked**
1	Russia	3.12
2	Australia	1.42
3	Ukraine	0.95
4	Uzbekistan	0.60
5	Tajikistan	0.56
6	Kazakhstan	0.51
7	China	0.49
8	Latvia	0.47

9	Russia	0.41
10	Belarus	0.37

** We eliminated countries from this rating where the number of users of Kaspersky Lab's mobile security product is relatively low (under 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.*

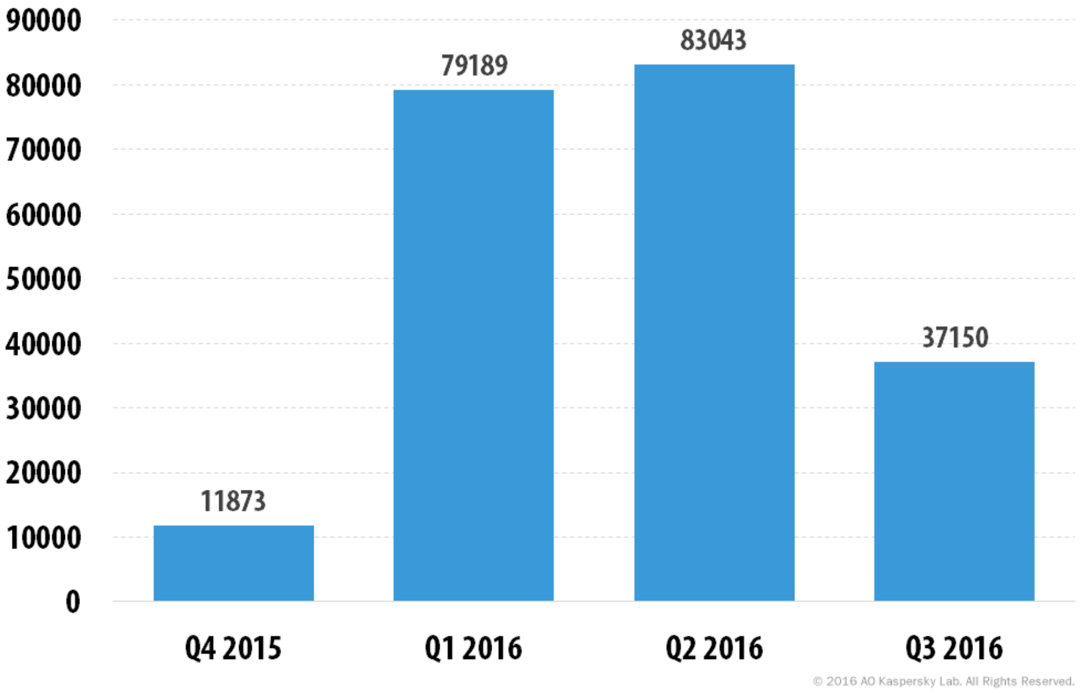
In Q3 2016, first place was occupied by Russia (3.12%) where the proportion of users that encountered mobile banker Trojans almost doubled from the previous quarter.

In second place again was Australia (1.42%), where the Trojan-Banker.AndroidOS.Acecard and Trojan-Banker.AndroidOS.Marcher families were the most popular threats.

The most widely distributed mobile banking Trojans in Q3 were representatives of the Svpeng, Faketoken, Regon, Asacub, Gugi and Grapereh families. In particular, the third quarter saw the Trojan-Banker.AndroidOS.Gugi family learn how to bypass protection mechanisms in Android by tricking users.

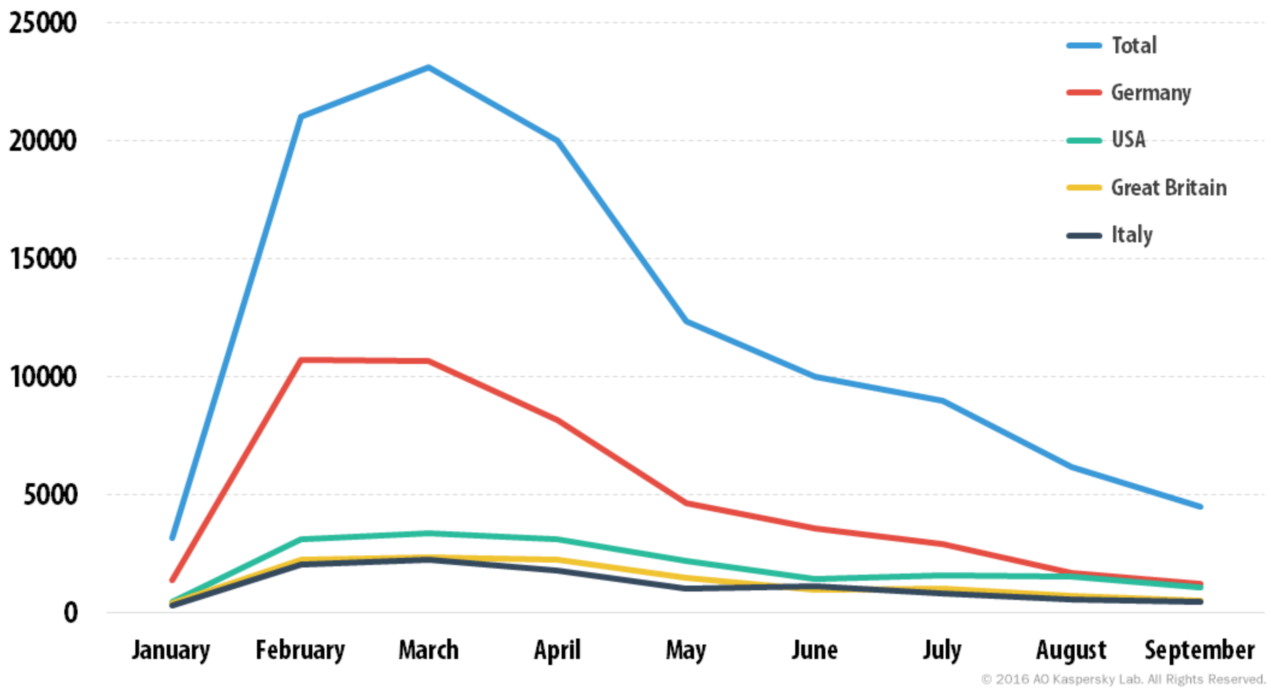
Mobile Ransomware

In Q3 2016, we detected **37,150** mobile Trojan-Ransomware installation packages.



Number of mobile Trojan-Ransomware installation packages detected by Kaspersky Lab (Q4 2015 – Q3 2016)

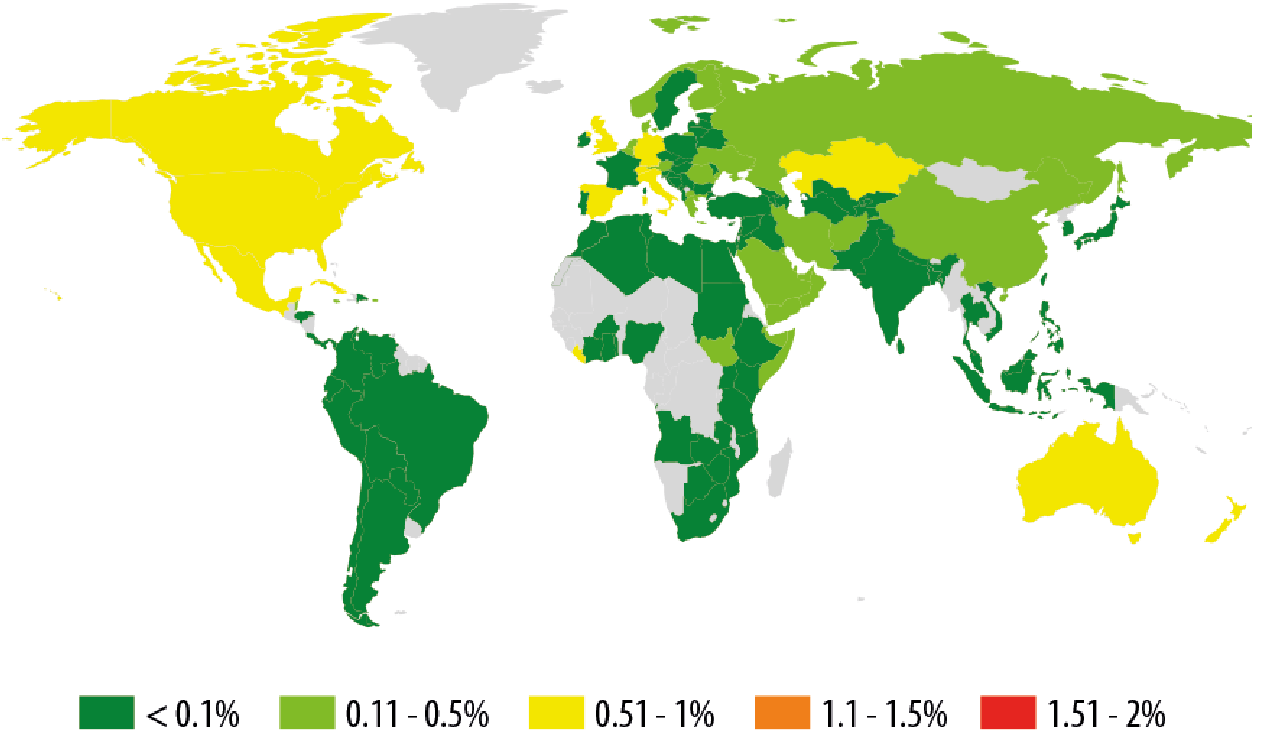
The sharp rise in the number of mobile Trojan-Ransomware installation packages in Q1 and Q2 of 2016 was caused by the active proliferation of the Trojan-Ransom.AndroidOS.Fusob family of Trojans. In the first quarter of 2016, this family accounted for 96% of users attacked by mobile ransomware; in Q2 it accounted for 85%. Its share in Q3 was 73%.



Number of users attacked by the Trojan-Ransom.AndroidOS.Fusob family, January-September 2016

The highest number of users attacked by the mobile Trojan-Ransomware family was registered in March 2016. Since then the amount of attacked users has been decreasing, especially in Germany.

Despite this, Trojan-Ransom.AndroidOS.Fusob.h remained the most popular mobile Trojan-Ransomware in the third quarter, accounting for nearly 53% of users attacked by mobile ransomware. Once run, the Trojan requests administrator privileges, collects information about the device, including GPS coordinates and call history, and downloads the data to a malicious server. After that, it may receive a command to block the device.



© 2016 AO Kaspersky Lab. All Rights Reserved.

Geography of mobile Trojan-Ransomware in Q3 2016 (percentage of all users attacked)

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

	Country*	% of users attacked **
1	Canada	0.95
2	USA	0.94
3	Kazakhstan	0.71
4	Germany	0.63
5	UK	0.61
6	Mexico	0.58
7	Australia	0.57
8	Spain	0,54
9	Italy	0.53
10	Switzerland	0.51

* *We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is relatively low (under 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 TOP 10 countries apart from Kazakhstan, the most popular Trojan-Ransom family was Fusob. In the US, the Trojan-Ransom.AndroidOS.Svpeng family was also popular. This Trojan family emerged in 2014 as a modification of the Trojan-Banker.AndroidOS.Svpeng family. These Trojans demand a ransom of $100-$500 from victims to unblock their devices.

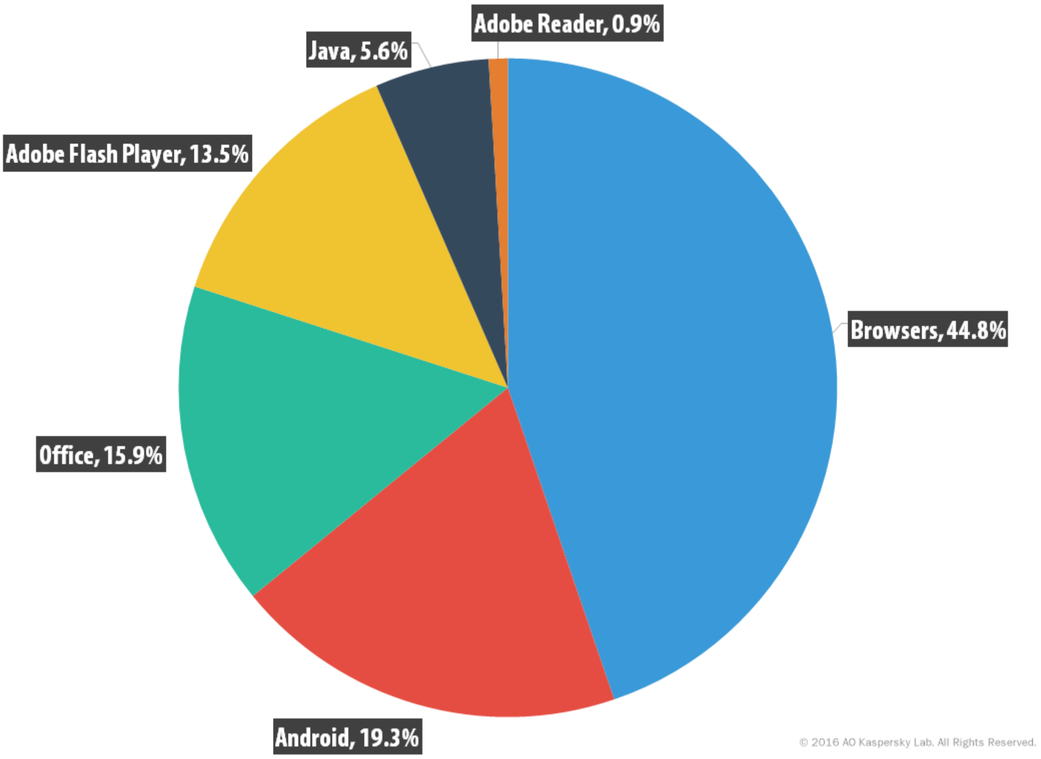
In Kazakhstan, the main threat to users originated from representatives of the Small mobile Trojan-Ransom family. This is a fairly simple ransomware program that blocks the operation of a device by overlaying all the windows with its own and demanding $10 to remove it.

Vulnerable apps exploited by cybercriminals

In Q3 2016, the Neutrino exploit kit departed the cybercriminal market, following in the wake of Angler and Nuclear which also left the market in the previous quarter.

RIG and Magnitude remain active. RIG was especially prominent – it has quickly filled the vacant niche on the exploit kit market.

This is the overall picture for the use of exploits this quarter:



Distribution of exploits used in attacks by the type of application attacked, Q3 2016

Exploits for different browsers and their components (45%) once again topped the rating, although their share decreased by 3 percentage points. They are followed by exploits for Android OS vulnerabilities (19%), whose share fell 5 p.p. in the third quarter. Exploits kits for Microsoft Office rounded off the top three. Their contribution actually saw an increase from 14% to 16% in Q3.

Exploits for Adobe Flash Player remained popular. In fact, their share more than doubled from 6% to 13%. This was caused by the aforementioned RIG exploit kit: its use in several campaigns saw the share of SWF exploits increase dramatically.

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 third quarter of 2016, Kaspersky Lab’s web antivirus detected **12,657,673** unique malicious objects (scripts, exploits, executable files, etc.) and **45,169,524** unique URLs were recognized as malicious by web antivirus components. Kaspersky Lab solutions detected and repelled **171,802,109** malicious attacks from online resources located in 190 countries all over the world.

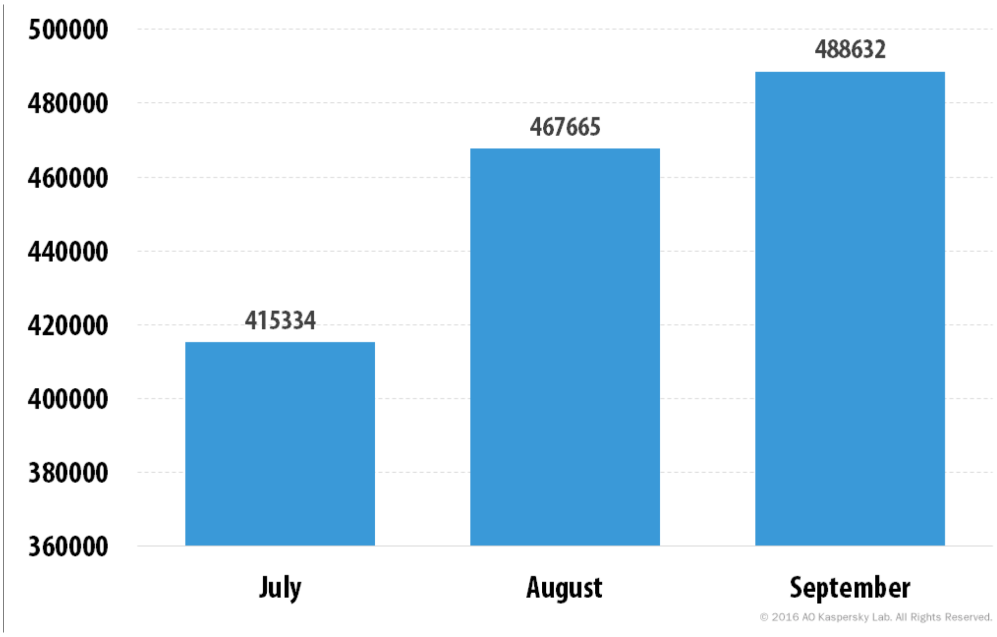
Online threats in the banking sector

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

Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **1,198,264** computers in Q3 2016. The number of users attacked by financial malware increased by 5.8% from the previous quarter (**1,132,031**).

The third quarter is traditionally holiday season for many users of online banking services in Europe, which means the number of online payments made by these users increases during this period. This inevitably sees an increase in financial risks.

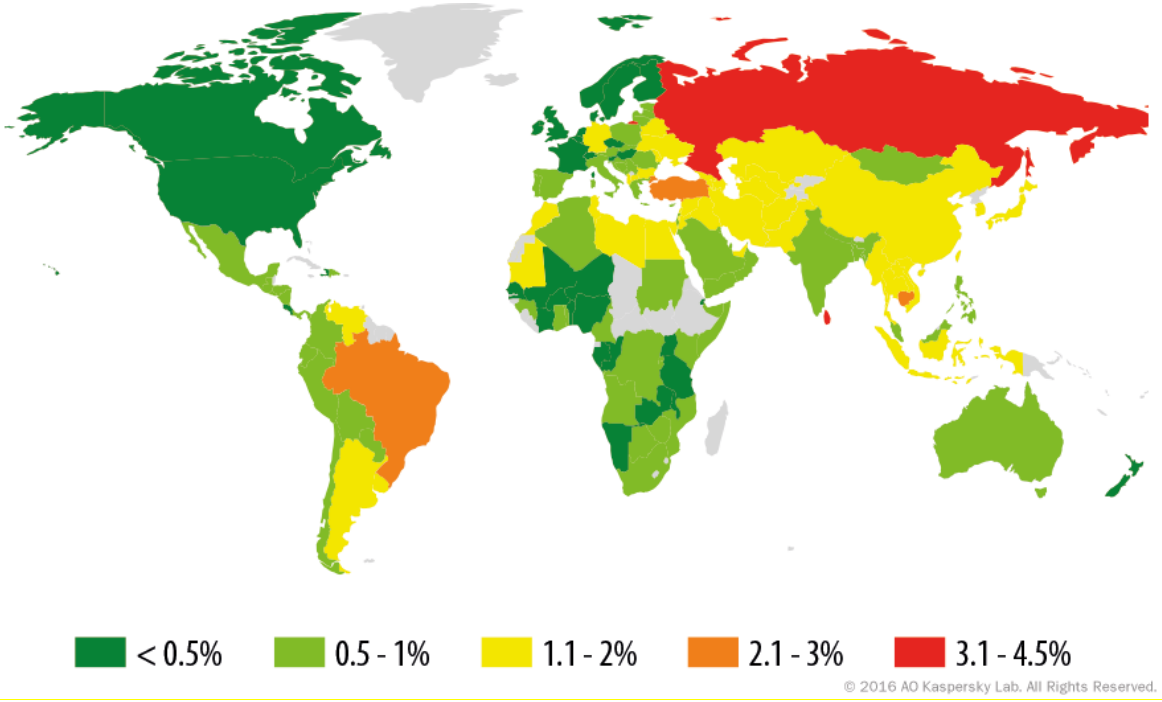
In Q3, the activity of financial threats grew month on month.



Number of users attacked by financial malware, Q3 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 in the country who encountered this type of threat during the reporting period, relative to all users of our products in that country.



Geography of banking malware attacks in Q3 2016 (percentage of attacked users)

TOP 10 countries by percentage of attacked users

	Country*	% of attacked users**
1	Russia	4.20
2	Sri Lanka	3.48
3	Brazil	2.86
4	Turkey	2.77
5	Cambodia	2.59
6	Ukraine	1.90
7	Venezuela	1.90
8	Vietnam	1.86
9	Argentina	1.86
10	Uzbekistan	1.77

These statistics are based on 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 (under 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.*

In the third quarter of 2016, Russia had the highest proportion of users attacked by banking Trojans. Representatives of the Trojan-Banker ZeuS (Zbot) family, which leads the way in terms of the number of attacked users worldwide, were especially active in Russia. This is unsurprising since Russian cybercriminals are allegedly behind the development of this malware. They know the specifics of Russia's online banking systems as well as the mentality of Russian users and take them into consideration when developing their malware. In Russia, the Gozi banking Trojan continues to proliferate. It displayed a burst of activity in the previous quarter after its developers joined forces with the creators of the Nymaim Trojan. Russia also topped the TOP 10 countries with the highest proportion of users attacked by mobile bankers.

Sri Lanka, a favorite destination with tourists, was a newcomer to the rating, going straight in at second. Financial threats were encountered by 3.48% of users in the country. Among them are likely to be foreigners who arrived in the country on holiday and used online banking services to make payments. The most active representatives of banking malware in the region were those from the Fsysna banker family. This family has previously been noted for attacks targeting customers of Latin American banks.

Brazil rounds off the top three for the second quarter in a row. In Q2, we forecast a surge of financial threat activity in Latin America and specifically in Brazil because of this summer's Olympic Games. However, the increase in the proportion of users attacked in Brazil was negligible: in the third quarter, 2.86% of users in Brazil encountered financial threats compared to 2.63% in Q2. At the same time, users in Argentina were subjected to a surge in malicious attacks, and as a result, the country ranked ninth.

The holiday season affected almost all countries in the TOP 10. In Russia, Ukraine and Uzbekistan, people traditionally have vacations at this time of the year, while other countries (Sri Lanka, Brazil, Turkey, Cambodia, etc.) are considered popular tourist destinations. Tourists tend to be active users of online banking systems, which in turn attracts cybercriminals and their banking malware.

The share of banking Trojan victims in Italy was 0.60%, in Spain it was 0.61%, while in Germany and the UAE the figures were 1.21% and 1.14% respectively.

The TOP 10 banking malware families

The table below shows the TOP 10 malware families used in Q3 2016 to attack online banking users (as a percentage of users attacked):

	Name*	% of attacked users**
1	Trojan-Spy.Win32.Zbot	34.58
2	Trojan.Win32.Qhost/Trojan.BAT.Qhost	9.48
3	Trojan.Win32.Fsysna	9.467
4	Trojan-Banker.Win32.Gozi	8.98
5	Trojan.Win32.Nymaim	8.32
6	Trojan-Banker.Win32.Shiotob	5.29
7	Trojan-Banker.Win32.ChePro	3.77
8	Trojan-Banker.Win32.BestaFera	3.31
9	Trojan-Banker.Win32.Banbra	2.79
10	Trojan.Win32.Neurevt	1.79

** 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.*

The undisputed leader of the rating is Trojan-Spy.Win32.Zbot. Its source codes have been publicly available since a leak and are now widely exploited as an easy-to-use tool for stealing user payment data. Unsurprisingly, this malware consistently tops this rating – cybercriminals regularly enhance the family with new modifications compiled on the basis of the source code and containing minor differences from the original.

The family of Qhost Trojans (verdicts Trojan.Win32.Qhost and Trojan.BAT.Qhost) came second. The functionality of this family's malicious programs is relatively simple: the Trojan modifies the content of the Host file (a special text file that contains a database of domain names that are used when transmitting to the network addresses of nodes) and as soon as specific resources are visited, the Trojan's malicious components are loaded to an infected workstation and used to steal payment information. The Trojan adds a number of records to the Host file preventing the user's browser from connecting to web-based apps and resources of popular antivirus vendors.

The Q3 rating also includes a new malware representative that has already demonstrated its capabilities in Sri Lanka – the Trojan.Win32.Fsysna family of banking Trojans. Members of this family, in addition to stealing payment data from infected workstations, are also used by cybercriminals to distribute spam. The Trojan uses an infected machine to redirect spam messages from the command center to a mail server. Some representatives of this family also possess Trojan cryptor functionality. Fsysna is kind of a 'Swiss army knife' used by cybercriminals to steal money.

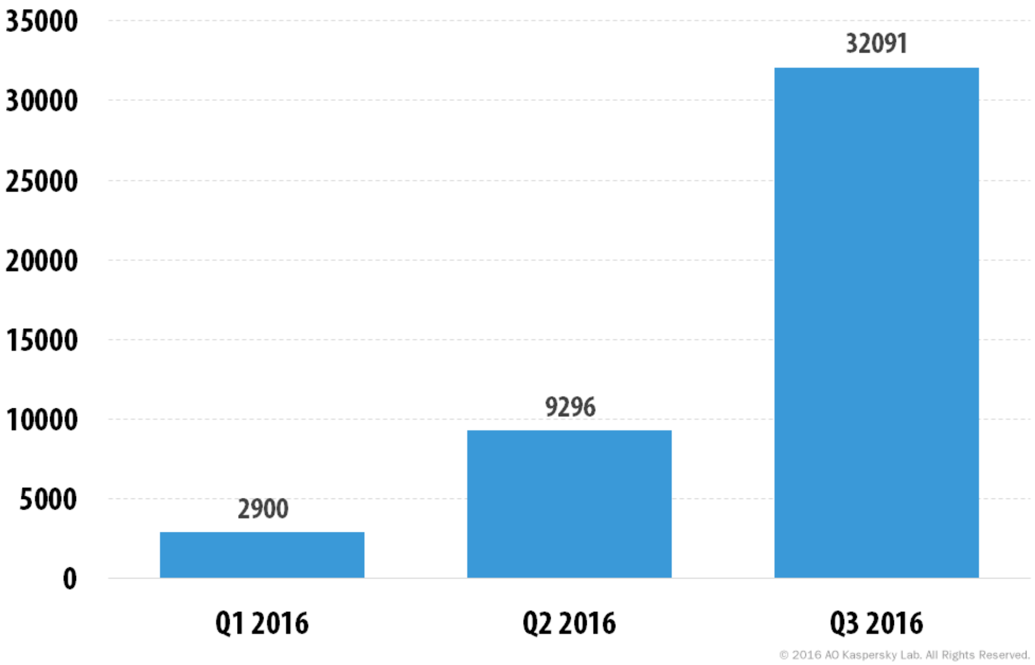
Q3 2016 saw a decline in the activity of the notorious financial threat Trojan-Spy.Win32.Lurk: the number of users attacked by this malware fell by 7.1%. Lurk was not included in the TOP 10 banking malware families, but it still poses a threat to users of online banking systems. The cybercriminal group behind this financial threat has been arrested (something we wrote about in a separate article), so we expect to see a further decrease in activity by this banking Trojan next quarter.

Ransomware Trojans

Cryptors are currently one of the biggest threats to users and companies. These malicious programs are becoming more and more popular in the cybercriminal world because they are capable of generating large profits for their owners.

A total of 21 new cryptor families and 32,091 new modifications were detected in Q3. We also added several existing cryptor families to our virus collection.

The number of new cryptor families added to our virus collection is slightly less than in the second quarter (25), but the number of newly created modifications increased 3.5 times compared to the previous quarter.



The number of newly created cryptor modifications, Q1 – Q3 2016

Malware writers are constantly trying to improve their creations. New ways to infect computers are always being sought, especially for attacks on companies, which cybercriminals see as far more profitable than attacks on standard users.

Remote launching of cryptors by cybercriminals

We are increasingly seeing incidents where cybercriminals crack passwords to gain remote access to a victim's system (usually an organization) and infect a compromised machine with Trojan ransomware. Examples of this in Q3 were Dcryptor and Xpan.

Dcryptor/Mamba

Trojan-Ransom.Win32.Dcryptor is known on the Internet under the pseudonym 'Mamba'. Infection is carried out manually. The fraudsters brute-force the passwords for remote access to the victim machine and run the Trojan, passing on the password for encryption as a command line argument.

During infection, the Trojan uses the legitimate DiskCryptor utility. As a result, it's not just individual files on network drives that are infected but entire hard drive sectors on the local machine. System boot is blocked: once the computer is started, a message appears on the screen demanding a ransom and displaying an email address for communicating with the attackers.

This Trojan reminds us of the notorious Petya/Mischa Trojan and continues the growing trend of cybercriminals looking for new ways to block access to data.

Xpan/TeamXRat ransomware

Trojan-Ransom.Win32.Xpan is yet another example of ransomware that is launched after attackers remotely penetrate a system. This Trojan is distributed by Brazilian cybercriminals. They brute-force the RDP password (the standard protocol for remote access to Windows computers) and infect the compromised system using the Xpan Trojan that encrypts files and displays a ransom demand.

Ransomware in scripting languages

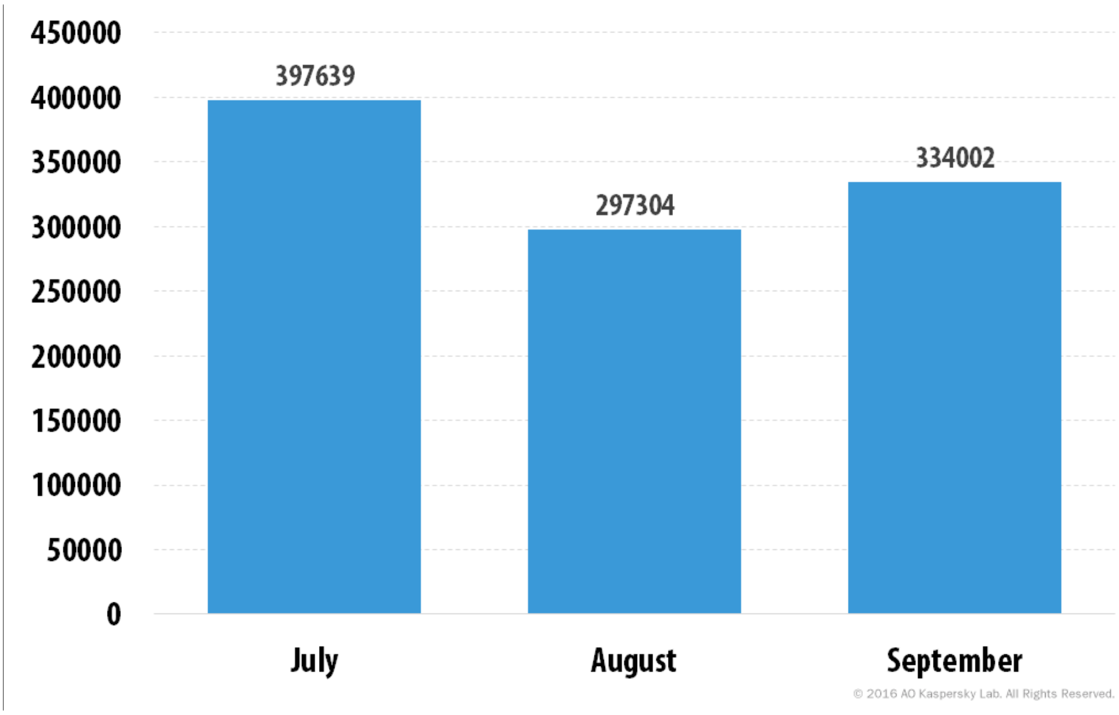
Another trend that has attracted our attention is the growing number of cryptors written in scripting languages. In the third quarter of 2016, we came across several new families written in Python:

- HolyCrypt (Trojan-Ransom.Python.Holy)
- CryPy (Trojan-Ransom.Python.Kpyna)
- Trojan-Ransom.Python.Agent

Another example that emerged in June was Stampado (Trojan-Ransom.Win32.Stampa) written in AutoIt, the automation language.

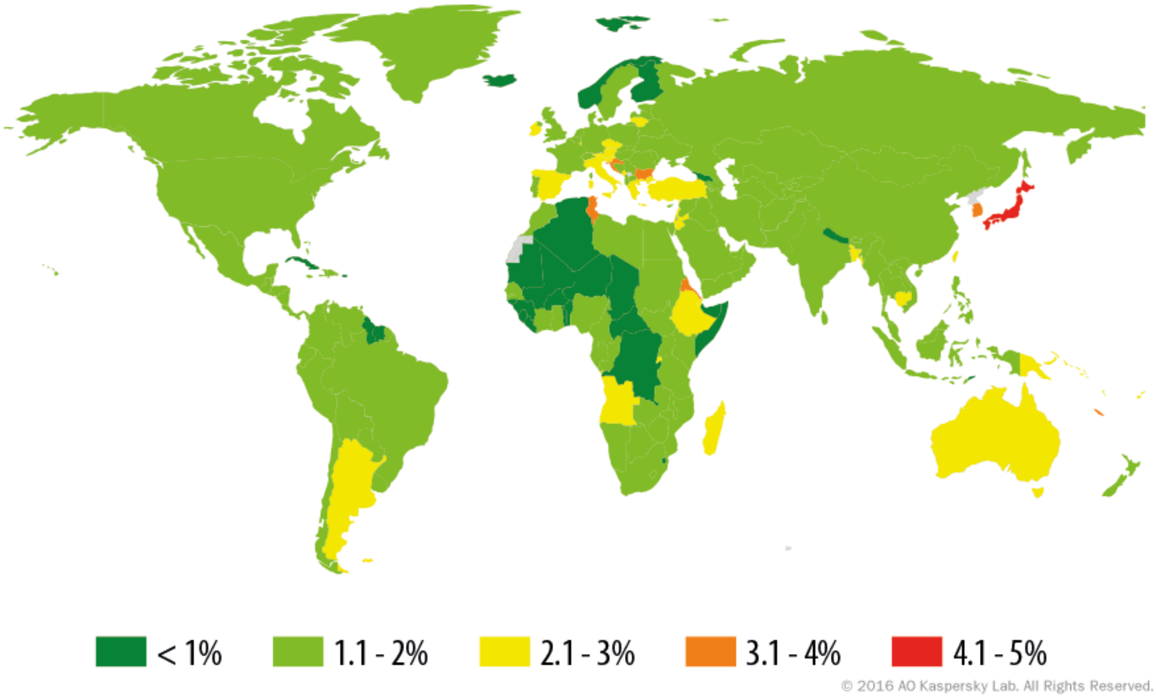
The number of users attacked by ransomware

In Q3 2016, 821,865 unique KSN users were attacked by cryptors – that is 2.6 times more than the previous quarter.



Number of unique users attacked by Trojan-Ransom cryptor malware (Q3 2016)

The largest contribution was made by representatives of the Trojan-Downloader.JS.Cryptoload family. These Trojan downloaders, written in JavaScript, were designed to download and install representatives of different cryptor families in the system.



Geography of Trojan-Ransom attacks in Q3 2016 (percentage of attacked users)

Top 10 countries attacked by cryptors

	Country*	% of users attacked by cryptors**
1	Japan	4.83
2	Croatia	3.71
3	Korea	3.36
4	Tunisia	3.22
5	Bulgaria	3.20
6	Hong Kong	3.14
7	Taiwan	3.03
8	Argentina	2.65
9	Maldives	2.63
10	Australia	2.56

** We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 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.*

As in the previous quarter, Japan topped this rating.

Newcomers to this Top 10 were Tunisia, Hong Kong, Argentina, and Australia, with Italy, Djibouti, Luxembourg, and the Netherlands all making way.

Top 10 most widespread cryptor families

	Name	Verdict*	% of attacked users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion/ Trojan-Ransom.NSIS.Onion	28.34
2	Locky	Trojan-Ransom.Win32.Locky	9.60
3	CryptXXX	Trojan-Ransom.Win32.CryptXXX	8.95
4	TeslaCrypt	Trojan-Ransom.Win32.Bitman	1.44
5	Shade	Trojan-Ransom.Win32.Shade	1.10
6	Cryakl	Trojan-Ransom.Win32.Cryakl	0.82
7	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.73
8	Cerber	Trojan-Ransom.Win32.Zerber	0.59
9	CryptoWall	Trojan-Ransom.Win32.Cryptodef	0.58
10	Crysis	Trojan-Ransom.Win32.Crusis	0.51

** 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.*

CTB-Locker once again occupied first place in the Q3. The top three also included the now infamous Locky and CryptXXX. Despite the fact that the owners of TeslaCrypt disabled their servers and posted a master key to decrypt files back in May 2016, it continues to make it into our rating (although its contribution dropped by 5.8 times in Q3)

Crysis

Crysis (verdict Trojan-Ransom.Win32.Crusis) was a newcomer to the TOP 10 in Q3. This Trojan was first detected in February 2016 and since then has undergone several code modifications.

Interestingly, the list of email addresses used for ransom demands by the distributors of Crysis partly matches the list associated with the Cryakl and Aura Trojans. Analysis of the executable files from these families, however, shows that they do not share the same code. It appears that these malicious programs are spread via a partner scheme, and because some distributors are distributing several different Trojans simultaneously they are using the same email address to communicate their ransom demands to the victims.

Polyglot/MarsJoke

This Trojan appeared in August 2016 (we recently published a detailed analysis of Polyglot/ MarsJoke). It is not included in the TOP 10, but it does have one interesting feature: the authors have tried to imitate the well-known CTB-Locker, which tops the rating for the second quarter in a row. Both the external and internal design of this piece of malware is very similar to the "original", but the cybercriminals made a mistake that allows files to be decrypted without paying a ransom.

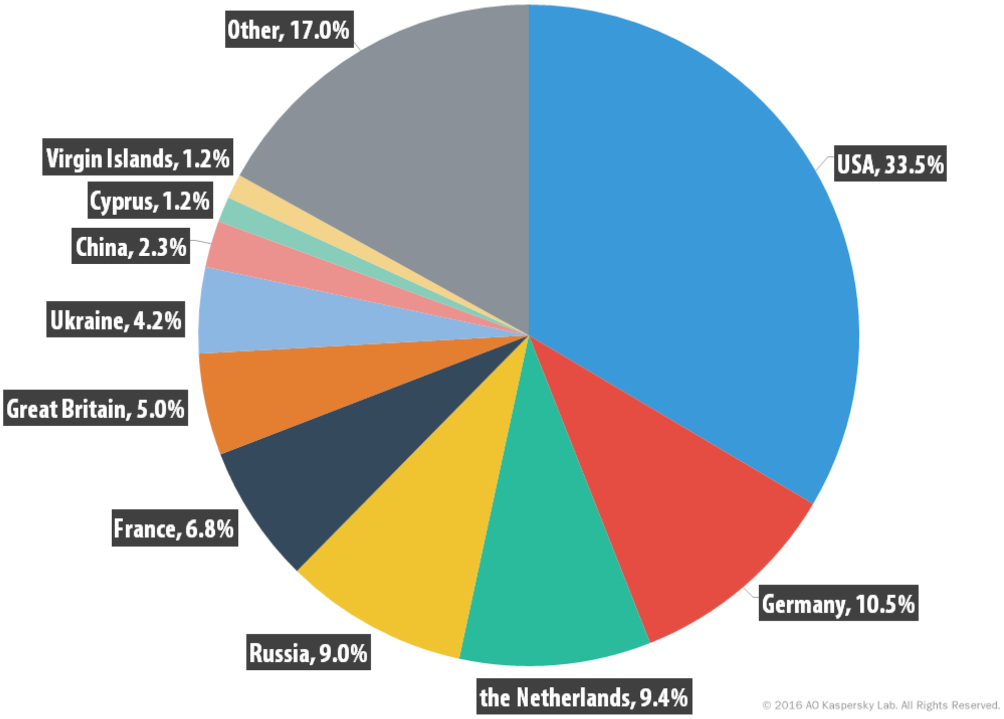
Top 10 countries where online resources are seeded with malware

The following statistics are based on the physical location of the online resources 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 Q3 2016, Kaspersky Lab solutions blocked **171,802,109** attacks launched from web resources located in 190 countries around the world. **45,169,524** unique URLs were recognized as malicious by web antivirus components.

83% 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, Q3 2016

The US (33.51%) remained top of this rating in Q3. Russia (9%) dropped from second to fourth, while Germany came second with a share of 10.5%. Canada left the Top 10, with Cyprus a newcomer in ninth place (1.24%).

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.

Please note that starting this quarter, this rating only includes attacks by malicious programs that fall under the ***Malware*** class. The rating does not include web antivirus module detections of potentially dangerous or unwanted programs such as RiskTool or adware.

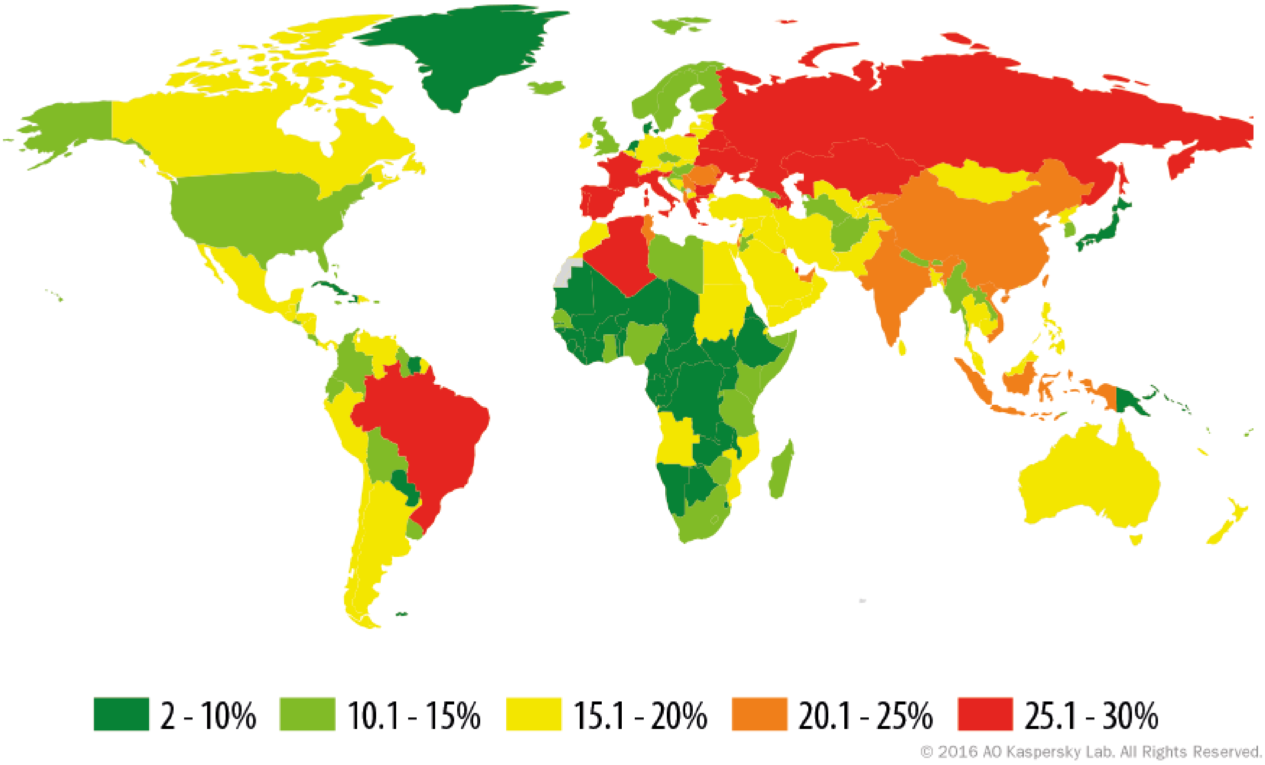
	Country*	% of users attacked **
1	Slovenia	30.02
2	Bulgaria	29.49
3	Armenia	29.30
4	Italy	29.21
5	Ukraine	28.18
6	Spain	28.15
7	Brazil	27.83
8	Belarus	27.06
9	Algeria	26.95
10	Qatar	26.42
11	Greece	26.10
12	Portugal	26.08
13	Russia	25.87
14	France	25.44
15	Kazakhstan	25.26
16	Azerbaijan	25.05
17	United Arab Emirates	24.97
18	Vietnam	24.73

19	China	24.19
20	Albania	23.23

These statistics are based on 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 (under 10,000 users).*
*** Unique users whose computers have been targeted **by Malware-class** attacks as a percentage of all unique users of Kaspersky Lab products in the country.*

On average, 20.2% of computers connected to the Internet globally were subjected to at least one **Malware-class** web attack during the quarter.



Geography of malicious web attacks in Q3 2016 (ranked by percentage of users attacked)

The countries with the safest online surfing environments included Croatia (14.21%), the UK (14.19%), Singapore (13.78%), the US (13.45%), Norway (13.07%), Czech Republic (12.80%), South Africa (11.98%), Sweden (10.96%), Korea (10.61%), the Netherlands (9.95%), Japan (9.78%).

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 Q3 2016, Kaspersky Lab's file antivirus detected **116,469,744** unique malicious and potentially unwanted objects.

Countries where users faced the highest risk of local infection

For each country, 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.

Please note that starting this quarter, the rating of malicious programs only includes ***Malware-class*** attacks. The rating does not include web antivirus module detections of potentially dangerous or unwanted programs such as RiskTool or adware.

	Country*	% of users attacked**
1	Vietnam	52.07
2	Afghanistan	52.00
3	Yemen	51.32
4	Somalia	50.78
5	Ethiopia	50.50
6	Uzbekistan	50.15
7	Rwanda	50,14
8	Laos	49.27
9	Venezuela	49.27
10	Philippines	47.69
11	Nepal	47.01
12	Djibouti	46.49
13	Burundi	46,17
14	Syria	45.97
15	Bangladesh	45.48
16	Cambodia	44.51
17	Indonesia	43.31

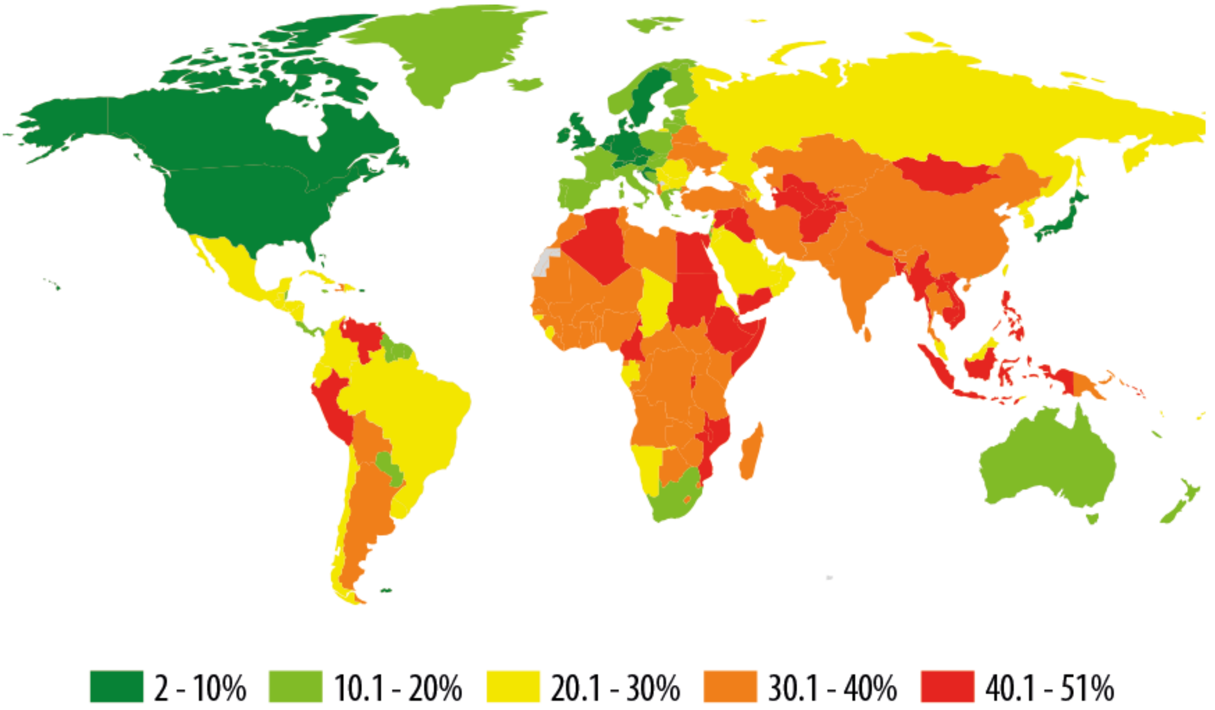
18	Tajikistan	43,01
19	Mozambique	42.98
20	Myanmar	42.85

These statistics are based on 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 (under 10,000 users).*

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

An average of 22.9% of computers globally faced at least one **Malware-class** local threat during the third quarter.



The safest countries in terms of local infection risks were: Spain (14.68%), Singapore (13.86%), Italy (13.30%), Finland (10.94%), Norway (10.86%), France (10.81%), Australia (10.77%), Czech Republic (9.89%), Croatia (9.70%), Ireland (9.62%), Germany (9.16%), the UK (9.09%), Canada (8.92%), Sweden (8.32%), the USA (8.08%), Denmark (6.53%), and Japan (6.53%).

For more info contact us at: intelreports@kaspersky.com
(Kaspersky Security Intelligence Service)

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