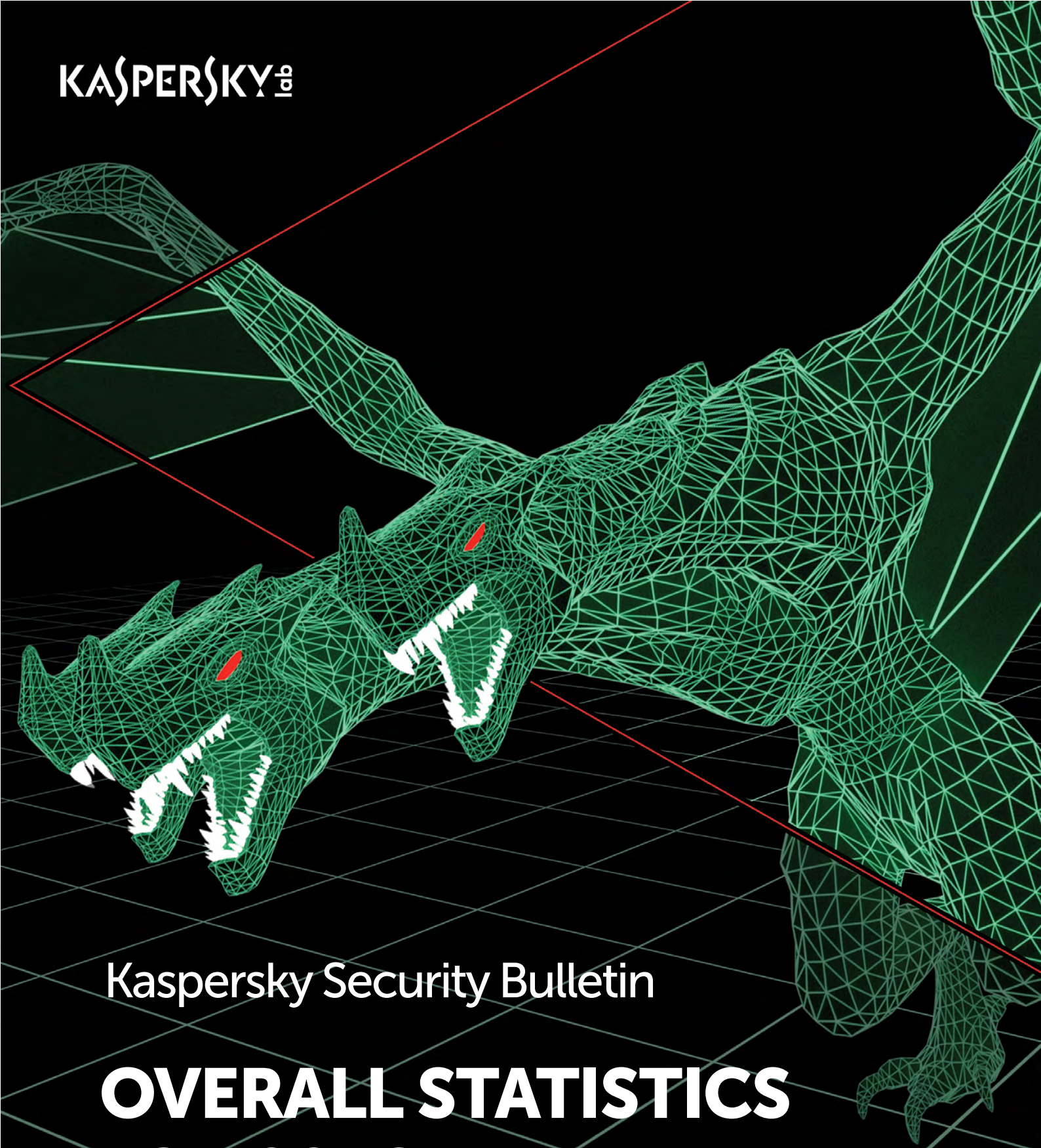
KASPERSKY lab



Kaspersky Security Bulletin

OVERALL STATISTICS FOR 2016

Maria Garnaeva, Fedor Sinitsyn, Yury Namestnikov,
Denis Makrushin, Alexander Liskin

GREAT

CONTENTS

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.

THE YEAR IN FIGURES

- **31.9%** of user computers were subjected to at least one **Malware-class** web attack over the year.
- Kaspersky Lab solutions repelled **758,044,650** attacks launched from online resources located all over the world.
- **261,774,932** unique URLs were recognized as malicious by web antivirus components.
- **29.1%** of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US.
- Kaspersky Lab's web antivirus detected **69,277,289** unique malicious objects.
- **1,445,434** computers of unique users were targeted by encryptors.
- Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **2,871,965** devices.
- Kaspersky Lab's file antivirus detected a total of **4,071,588** unique malicious and potentially unwanted programs.

Mobile threat statistics can be found in the report 'Mobile malware evolution 2016'.

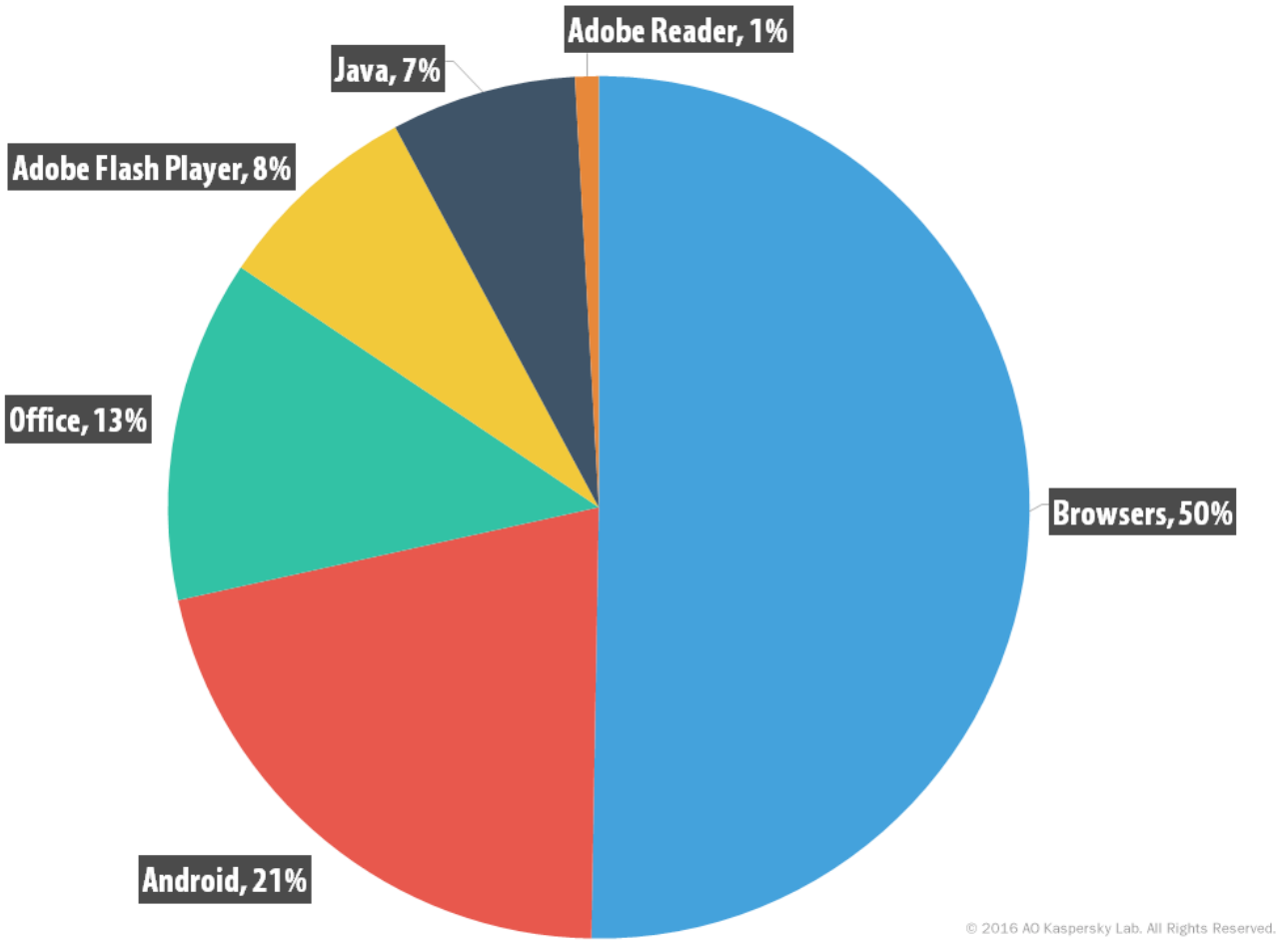
VULNERABLE APPLICATIONS USED IN CYBERATTACKS

2016 saw many of the major players leave the exploit kit market. In Q2, such giants as Angler and Nuclear disappeared after years of dominating the market. This meant cybercriminals had to switch to other exploit kits, and the same quarter saw a dramatic rise in the use of Neutrino. However, that exploit kit also left the market in Q3. As of late 2016, the Rig and Magnitude exploit kits remain in active use; Rig has occupied the niche left vacant by Neutrino, and we've seen it being used more and more often.

During 2016, just like in 2015, exploits for Adobe Flash Player vulnerabilities have been in high demand. Four such vulnerabilities made it into our list of vulnerabilities most often exploited by cybercriminals:

- CVE-2015-8651 (Adobe Flash)
- CVE-2016-1001 (Adobe Flash)
- CVE-2016-0034 (Microsoft Silverlight)
- CVE-2015-2419 (Internet Explorer)
- CVE-2016-4117 (Adobe Flash)
- CVE-2016-4171 (Adobe Flash)

Because the market has been dominated by exploit kits that typically target vulnerabilities in Adobe Flash Player, the proportion of Flash exploits has grown considerably compared to last year, from 3% to 8%.



Distribution of exploits used in cyberattacks, by type of application attacked*, 2016

* Vulnerable applications are ranked based on Kaspersky Lab product reports of blocked exploits used by cybercriminals both in web-borne attacks and in compromised local applications, including those on users' mobile devices.

2016 has also seen a substantial rise in the proportion of exploits for Microsoft Office application vulnerabilities, from 4% last year to 13% this year. The reason for this was a surge in malicious spam containing Microsoft Office exploits. However, there was a decline in this type of such spam towards the end of the year.

The proportion of exploits targeting the Android operating system is 21%, or a 7 p.p. increase year on year. This growth is mostly due to the increasing number of emerging exploits that enable root privilege escalation on a mobile device.

Overall, we saw a long-term trend continue in 2016: Adobe Flash Player, Microsoft Office and Internet Explorer exploits are still a favorite with cybercriminals. In the pie chart above, Internet Explorer exploits are classified as 'Browsers' (50% of all exploits), as are detections of landing pages that distribute exploits.

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 2016, Kaspersky Lab's web antivirus detected **69,277,289** unique malicious objects (scripts, exploits, executable files, etc.) and **261,774,932** unique URLs were recognized as malicious by web antivirus components. Kaspersky Lab solutions detected and repelled **758,044,650** malicious attacks launched from online resources located in 212 countries all over the world.

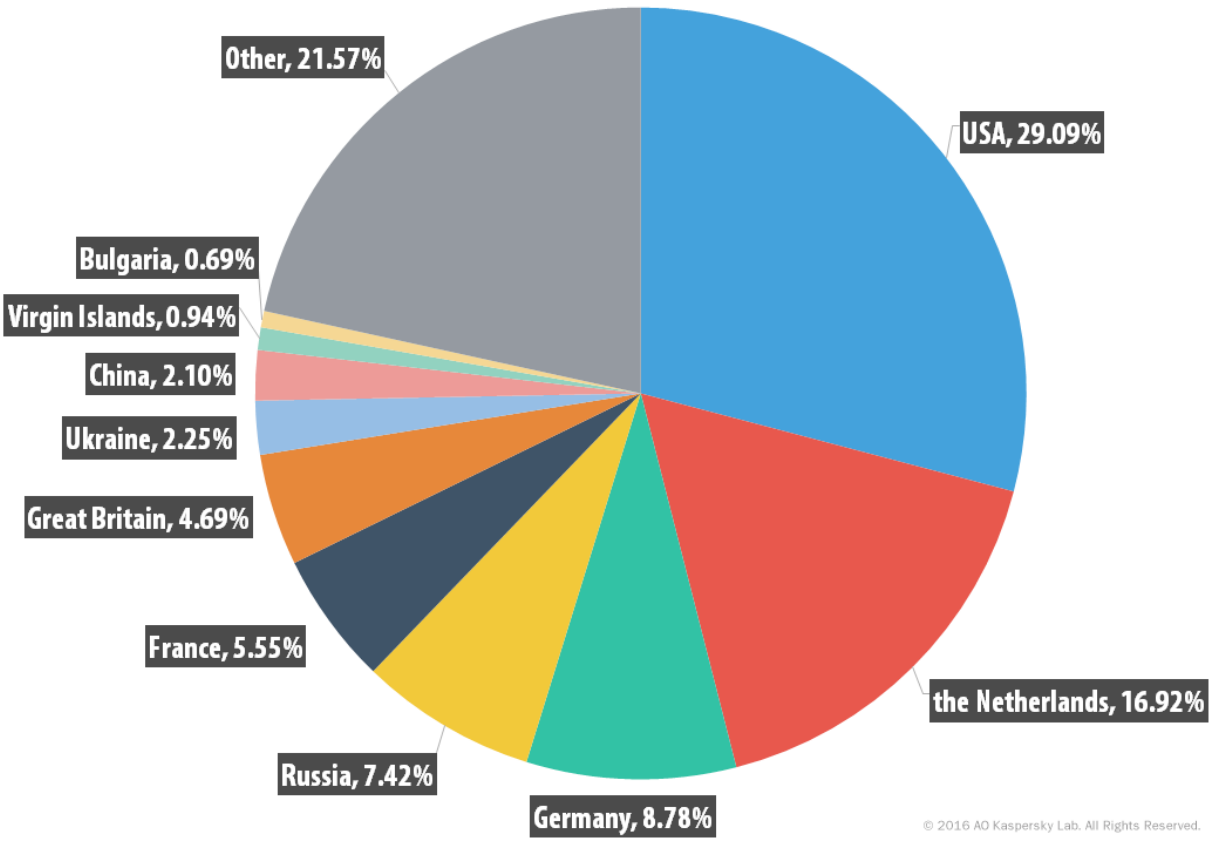
TOP 10 countries where online resources are seeded with malware

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 2016, Kaspersky Lab solutions blocked **758,044,650** attacks launched from web resources located in various countries around the world. To carry out their attacks, cybercriminals used 3,014,685 unique hosts.

78% of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries.



Distribution of web attack sources by country (November 2015 — October 2016)

The top nine countries where online resources are seeded with malware remained unchanged from the previous year. The Netherlands and Germany swapped places, as did China and the Virgin Islands. Sweden left the Top 10, and was replaced by the newcomer Bulgaria in 10th place.

TOP 20 verdicts detected online

Throughout 2016, Kaspersky Lab's web antivirus detected **69,277,289** unique malicious objects (samples composing unique hash including scripts, exploits, executable files, etc.).

During the year, advertising programs and their components were registered on 15.6% of user computers where our web antivirus was triggered.

We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2016.

These 20 programs accounted for 96.6% of all online attacks.

	Name*	% of all attacks**
1	Malicious URL	77.26
2	Trojan-Clicker.HTML.Iframe.dg	8.15
3	Trojan.Script.Generic	6.74
4	Trojan.Script.Iframer	3.14
5	Trojan-Downloader.Script.Generic	0.35
6	Exploit.Script.Generic	0.20
7	Packed.Multi.MultiPacked.gen	0.15
8	Trojan.JS.FBook.bh	0.13
9	Exploit.Script.Blocker	0.11
10	Trojan-Downloader.JS.Iframe.div	0.11
11	Trojan.JS.Redirector.ns	0.09
12	Trojan-Dropper.VBS.Agent.bp	0.08
13	Trojan-Downloader.JS.Agent.hjc	0.08
14	Trojan.JS.Iframe.ako	0.07
15	Trojan.Win32.Generic	0.06
16	Trojan.Win32.Generic	0.06
17	Trojan.JS.Agent.ckf	0.05
18	Trojan-Spy.HTML.Fraud.gen	0.05
19	Trojan.Win32.Invader	0.04
20	Exploit.SWF.Agent.gen	0.04

* These statistics represent detection verdicts from the web antivirus module. Information was provided by users of Kaspersky Lab products who consented to share their local data.

** The percentage of all malware web attacks recorded on the computers of unique users.

As is often the case, this TOP 20 is largely made up of objects used in drive-by attacks. They are heuristically detected as Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic, etc.

Malicious URL in first place is the verdict identifying links from our black list (links to web pages containing redirects to exploits, sites with exploits and other malicious programs, botnet control centers, extortion websites, etc.).

The Trojan.JS.FBook.bh script retrieves a link from a certain C&C address in order to update the user's status on Facebook, adding the link to a status and tagging all the user's friends. The link leads to the installation of a web browser extension that gains access to the user's Facebook account, meaning it can then perform a variety of actions on behalf of the user, including implementing this propagation scheme.

Trojan-Downloader.JS.Agent.hjc is a 'dynamic' clicker that accesses a C&C in order to read a configuration file; this file contains a link that will be included in iframe and will be visited when the user clicks on the website.

Trojan-Spy.HTML.Fraud.gen is a verdict for a phishing HTML page mimicking a web marketplace or a bank web page and is included in a phishing web email.

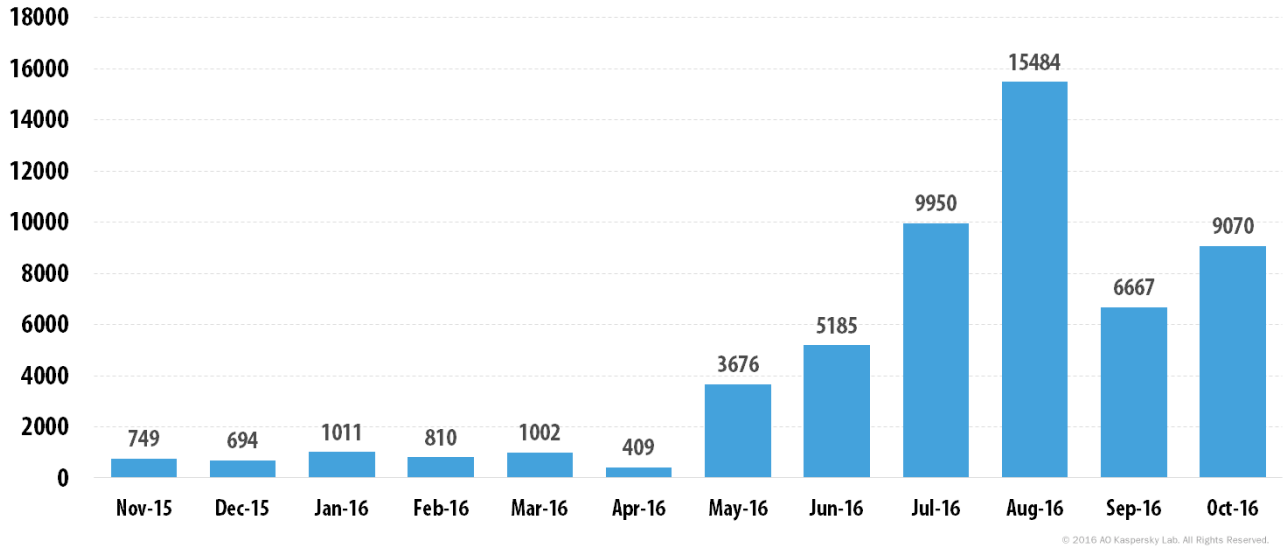
Crypto-ransomware

The crypto-ransomware threat continues to grow, with both the number of new families and new modifications rising in the second half of the year. New Trojans keep appearing at a disturbing rate, and while most of them turn out to be low-effort, low-reach experiments by unqualified developers, some, like Locky, Cerber and CryptXXX, have become major new threats to both individuals and businesses.

Meanwhile, older Trojans such as CTB-Locker, CryptoWall, TorrentLocker continue operating, and the criminals behind them have little desire to see their campaigns shut down like TeslaCrypt.

The number of detected crypto-ransomware modifications

During the year, we detected more than **54,000 modifications** of crypto-ransomware and discovered a more than **62 new families**.

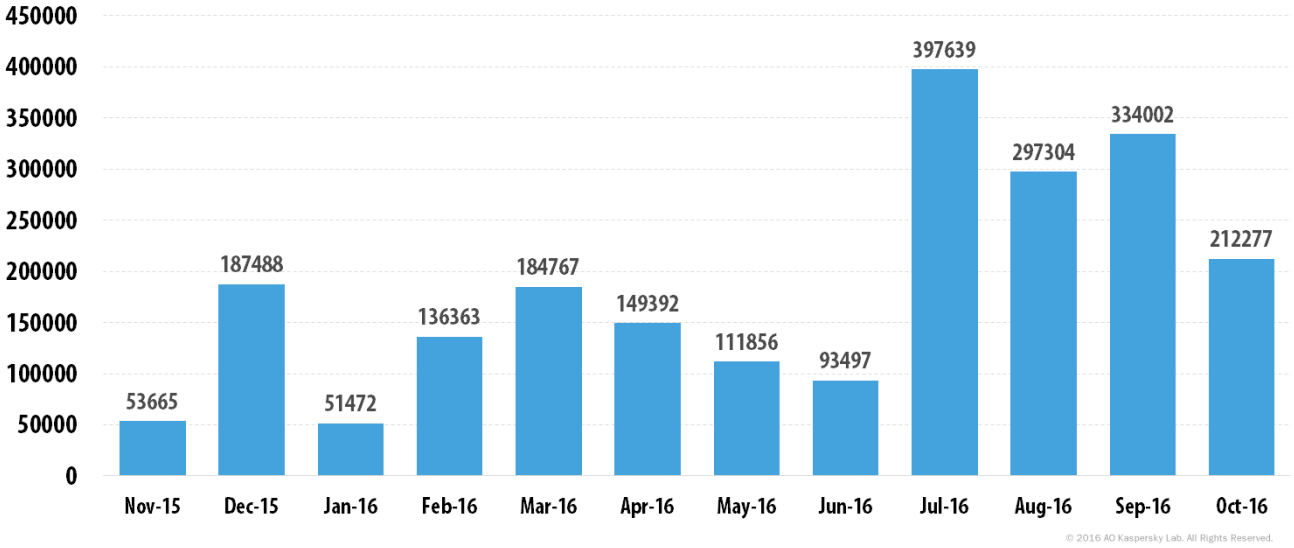


Number of new crypto-ransomware modifications (November 2015 – October 2016)

The overall number of encryptor modifications in our Virus Collection to date is at least **65,000**.

The number of users attacked by encryptors

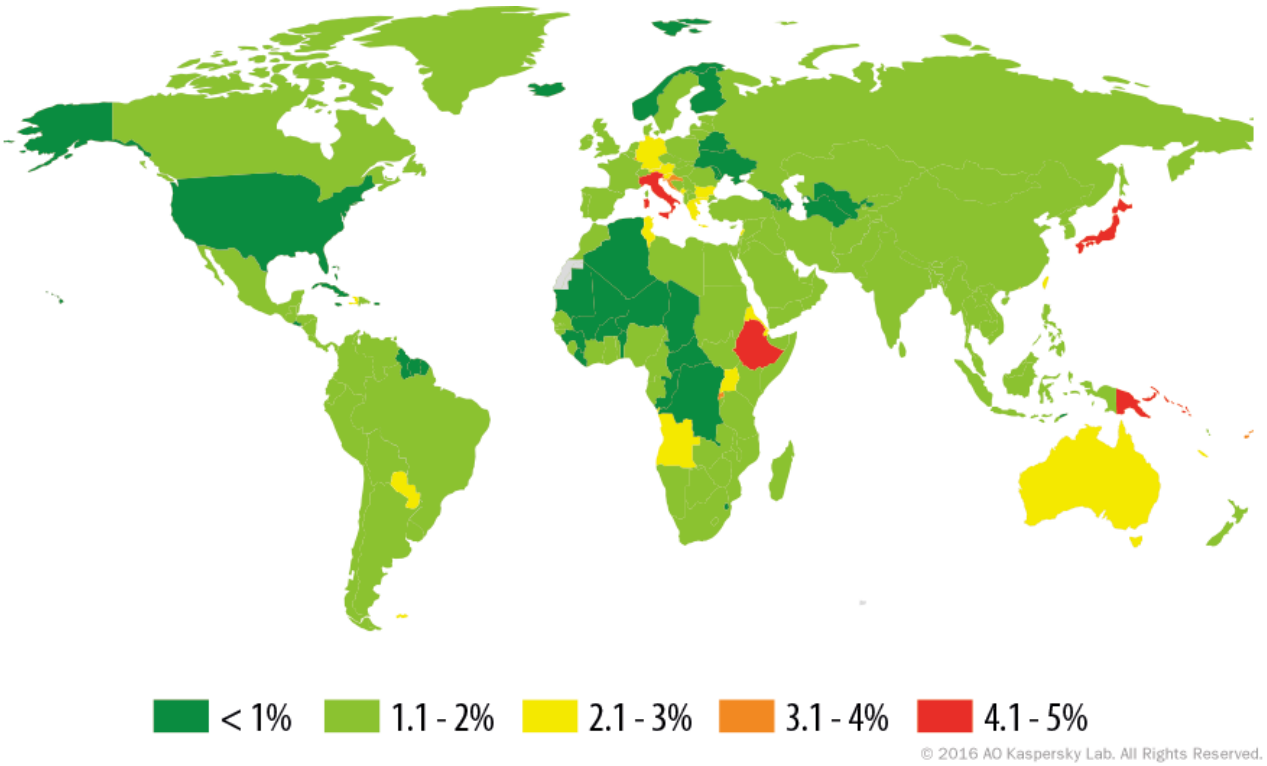
In 2016, **1,445,434 unique KSN users** were attacked by encryptors.



Number of users attacked by crypto-ransomware (November 2015 — October 2016)

It is important to keep in mind that the real number of incidents is higher: the statistics reflect only the results of signature-based and heuristic detections, while in the case of new and unknown malware samples Kaspersky Lab products detect encryption Trojans based on behavior recognition models.

Geography of attacks



Geography of crypto-ransomware attacks in 2016 (percentage of targeted users)

TOP 10 countries attacked by encryptors

	Country*	% of users attacked by encryptors**
1	Japan	4.46
2	Italy	4.17
3	Croatia	3.23
4	Luxembourg	3.15
5	Bulgaria	2.86
6	Uganda	2.55
7	Tunisia	2.54
8	Austria	2.45
9	Hong Kong	2.43
10	Lebanon	2.39

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 50,000).

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

TOP 10 most widespread encryptor families

	Name	Verdict*	% of attacked users**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25.32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7.07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6.54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2.85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2.79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2.36
7	Shade	Trojan-Ransom.Win32.Shade	1.73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1.26
9	Crysis	Trojan-Ransom.Win32.Crusis	1.15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0.90

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

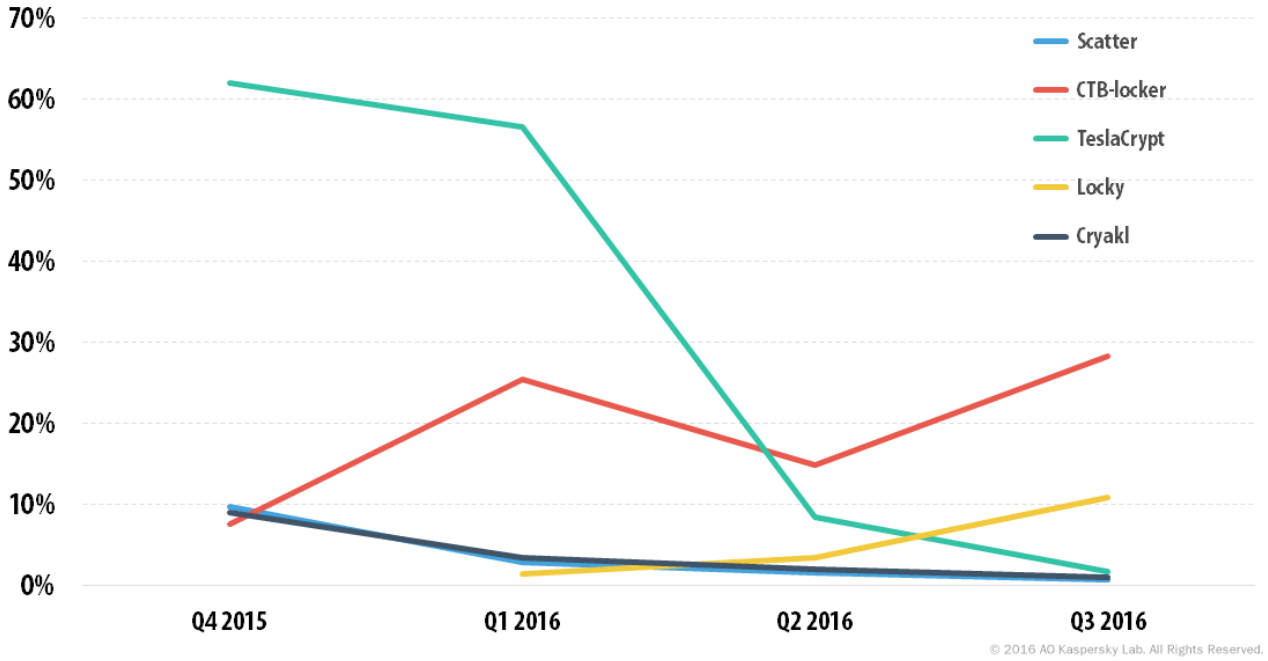
** Unique users whose computers have been targeted by a specific crypto-ransomware family as a percentage of all users of Kaspersky Lab products attacked by crypto-ransomware.

Most of the top 10 is occupied by notorious Trojans released in previous years: CTB-Locker, CryptoWall, Shade, Cryakl, TeslaCrypt, Scatter, Cryrar.

However, two new encryptors that emerged in 2016 — Locky and Crysis — are already among the most widespread.

The new crypto-ransomware Trojans that we have been discovering throughout 2016 are remarkably similar to their predecessors. The standard encryption schemes most commonly employed by ransomware are already known and criminals don't have to come up with new, unorthodox approaches when creating new Trojans. Ransomware programmers now tend to use time-tested approaches when implementing file encryption and mainly focus their efforts on new anti-reverse and detection evasion techniques.

At the same time, we have discovered many new encryptors clearly created by 'unqualified' developers. These families are usually characterized by low-quality code, lots of errors and flaws in the cryptography, the use of unsophisticated algorithms and approaches, and sometimes even grammatical errors in the ransom notes. The samples seldom become widespread, but the number of these new families of 'amateur' ransomware cannot go unnoticed. Obviously, the desire for easy money through extortion, and the extensive media coverage of ransomware is attracting more and more criminals that specialize in other types of fraud.



Top 5 most widespread crypto-ransomware families, by quarter (percentage of targeted users)

There was a rapid decline in the percentage of users affected by Teslacrypt, which is to be expected after it was shutdown in Q2 2016.

Locky, which first appeared in Q1 2016, on the contrary, is on the rise; CTB-Locker continues to lead the way after the demise of Teslacrypt; Cryakl and Scatter, both of which target mainly Russian-speaking countries, have been steadily losing ground.

Crypto-ransomware and the corporate sector

In 2016, about 22.6% of users attacked by crypto-ransomware were in the corporate sector. The 10 most widespread encryptor families are mostly the same as those shown in the rating above. However, there is one exception that should be noted: Trojan-Ransom.Win32.Rakhni, which targeted 2.42% of all corporate users attacked by crypto-ransomware in 2016.

Trojan-Ransom.Win32.Rakhni propagates with the help of Trojan-Downloader.Win32.Rakhni. This downloader is an executable file that is embedded into a .docx document, which is typically spread as an attachment in spam emails. The criminals behind Rakhni clearly target the corporate sector (namely, HR departments) in Russian-speaking countries, because the docx is usually made to look like a job application form (e.g. 'Резюме Жанна.docx'). When the victim opens the .docx file, they see a PDF reader icon, and if they click on it, the malicious downloader is executed. To avoid raising any immediate suspicions, the Trojan shows what appears to be a perfectly plausible resume.

Менеджер по работе с клиентами

Общая информация

Заработная плата:	**от 35 000 руб.**
Характер работы:	На территории работодателя
График работы:	Полный рабочий день
Образование:	Высшее
Опыт работы:	11 лет 2 месяца
Возраст:	28 лет (11 февраля 1988)

Опыт работы 11 лет 9 месяцев

Период работы:	сентябрь 2008 — по настоящее время
Должность:	**Менеджер отдела прямых продаж**
Компания:	ООО "Протек"
Обязанности:	Оптово-розничная продажа дверей стратегическое планирование и развитие продаж; составление бюджетов продаж и расходов отдела; анализ эффективности работы отдела; разработка мероприятий по увеличению объемов продаж отдела; оперативное управление отделом: организация работы, координация, контроль выполнения плана продаж, составление отчетов; контроль дебиторской задолженности, работа с просроченной задолженностью;
Период работы:	август 2007 — сентябрь 2008 (1 год 2 месяца)
Должность:	**Специалист по документообороту**
Компания:	ООО Биокад
Обязанности:	Прием и распределение тел звонков, работа с оргтехникой, архивация документов, деловая переписка, организация и планирование деловых встреч руководителей, контроль исполнения приказов и распоряжений.
Период работы:	январь 2005 — август 2007 (2 года 8 месяцев)
Должность:	**Ассистент менеджера**
Компания:	ООО ПКФ Эрион
Обязанности:	Ведение делопроизводства, оформление документов при закупке/продаже товаров.

Образование

Образование:	Высшее
Окончание:	2010 год
Учебное заведение:	МЭСИ
Факультет:	Менеджмент организации
Специальность:	Менеджер по конкурентоспособности

Дополнительная информация

Иностранные языки:	Английский (Базовый)
Водительские права:	Категория B
Владение компьютером:	Эксперт
Возможность командировок:	Есть
Навыки и умения:	Высокие коммуникативные навыки, хорошие аналитические способности, умение работать в команде и с большим объемом информации, знание 1С программы "Управление торговлей 8.0"

Resume shown to the victim by Trojan-Downloader.Win32.Rakhni

Meanwhile, the Trojan is proceeding to download the main payload – the encryptor Trojan-Ransom.Win32.Rakhni — that encrypts files and displays the ransom demands.

KSN data proves that the criminals behind Rakhni are not really interested in infecting individuals and that they clearly know how to target companies: this family is not in the overall TOP 10, but is among the most widespread in the corporate sector.

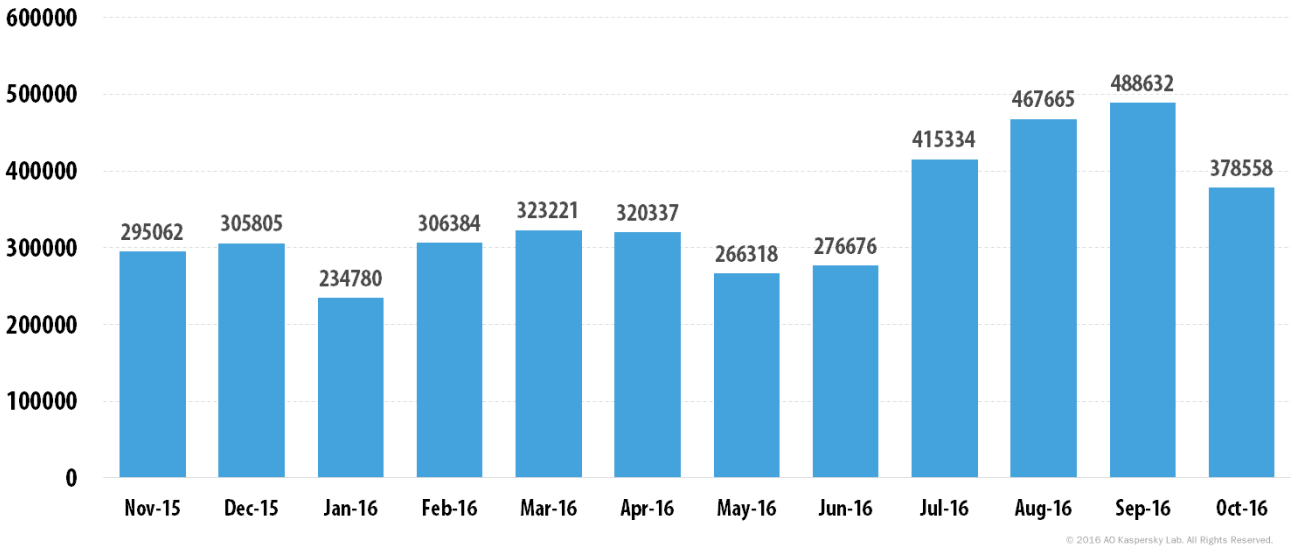
Online threats in the banking sector

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.

The annual statistics for 2016 are based on data received between November 2015 and October 2016.

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 data published for previous years. As a comparison, we have recalculated the statistics for the previous year, taking into account all the malware from the updated list.

In 2016, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking channels on **2,871,965 devices**. This number is 46% higher than in 2015 (1,966,324).

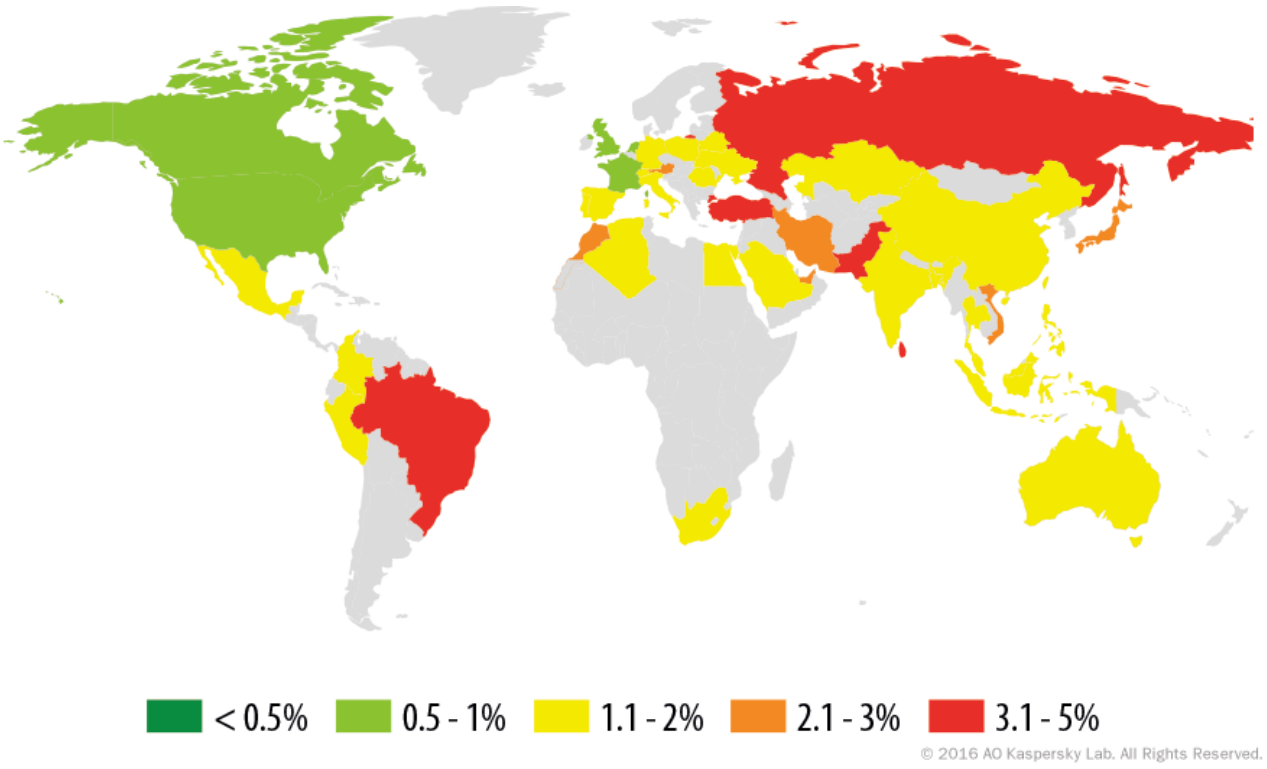


The number of users targeted by financial malware, November 2015 — October 2016

From the end of 2015, we witnessed a fall in the number of attacked devices, which was due to the suspension of activities by the Dyre (Dyreza) botnet. However, by the middle of 2016, the number of attacks began increasing gradually, and in September 2016, the monthly number of attacked devices exceeded the maximum monthly indicators for both 2014 and 2015, due to an increase in the number of attacks on mobile banking users, mostly Android device owners.

Geography of attacks

In order to evaluate the popularity of financial malware among cybercriminals and the risk of user computers around the world being infected by banking Trojans, we calculate the percentage of Kaspersky Lab 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 2016 (percentage of targeted users)

TOP 10 countries attacked by banking Trojans

	Country*	% attacked users**
1	Russian Federation	4.8
2	Brazil	4.7
3	Turkey	4.5
4	Sri Lanka	4.5
5	Pakistan	3.8
6	Austria	2.6
7	Vietnam	2.4
8	United Arab Emirates	2.3
9	Japan	2.2
10	Morocco	2.2

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 50,000 and less than 7,000 banking malware notifications).

** Unique users whose computers have been targeted by banking Trojans as a percentage of all unique users

The Russian federation leads this rating. Of all the Kaspersky Lab users attacked by malware in the country, 4.8% were targeted at least once by banking Trojans throughout the year. This reflects the popularity of financial threats in relation to all threats in the country.

4.7% of users attacked in Brazil encountered a banking Trojan at least once in 2016. The figure for Turkey was 4.5%, in Germany it was 2%, 1.7% in Switzerland and 1% in France.

TOP 10 banking malware programs

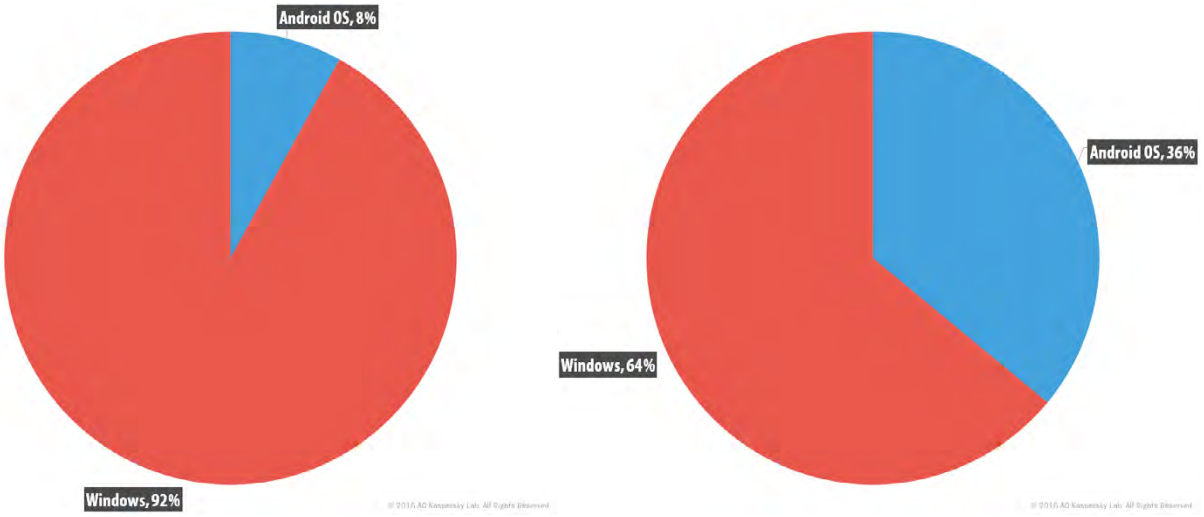
The table below shows the 10 malware programs most commonly used in 2016 to attack online and mobile banking users (as a percentage of targeted users):

	Name*	% users attacked**
1	Trojan-Banker.AndroidOS.Svpeng.q	8.8
2	Trojan-Banker.Win32.Gozi.gr	5.7
3	Trojan.BAT.Qhost.abp	4.5
4	Trojan-Spy.Win32.Zbot.pef	3.5
5	Trojan-Banker.AndroidOS.Agent.ai	2.8
6	Trojan-Spy.Win32.Zbot.vho	2.5
7	Trojan-Banker.AndroidOS.Asacub.e	1.9
8	Trojan-Banker.AndroidOS.Svpeng.r	1.8
9	Trojan.Win32.Qhost.afes	1.4
10	Trojan-Banker.AndroidOS.Hqwar.t	1.2

* These statistics are based on the detection verdicts returned by Kaspersky Lab's 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 malicious program, as a percentage of all unique users targeted by financial malware attacks.

Five of the top 10 banking Trojans attempt to steal mobile banking data from devices running Android OS. Compared to 2015, the proportion of attacks targeting Android rose 4.5 times. This shows that cybercriminals are keeping track of user behavior and switching from targeting Internet banking websites to spoofing mobile banking applications.



Proportion of devices targeted by financial malware, 2015–2016

The majority of the top 10 malicious programs for Windows work by injecting HTML code in the web page displayed by the browser and intercepting any payment data entered by the user in the original or inserted web forms. While mobile banking Trojans attempt to display a phishing window that covers the original mobile banking app window and grab one-time authentication codes by controlling incoming SMS messages.

First place in the rating is occupied by Trojan-Banker.AndroidOS.Svpeng.q. This is primarily down to how the malware spreads — via the Google AdSense advertising network, which is used by many web portals, including major news sites to display targeted advertising to users. Apparently, the authors of the Svpeng Trojan placed malicious ads on this network. The Trojan downloads itself as soon as an infected ad is loaded, regardless of whether the user tapped on it or not. The Svpeng family of banking Trojans has been known to Kaspersky Lab since 2013 and has a wide range of malicious functions. After being installed and launched, it disappears from the list of installed apps and requests the device's admin rights (to make it harder for antivirus software or the user to remove it). Svpeng can steal information about the user's bank cards via phishing windows, intercept, delete, and send text messages — all of which is necessary for attacks on remote banking systems that use SMS for one-time authentication codes.

A representative from the Trojan-Banker.Win32.Gozi family is in second place. It uses the technique of injecting code into working processes of popular web browsers to steal billing information entered on internet banking websites. Some samples of this family can infect the MBR (Master Boot Record) and maintain a presence in the operating system, even if it has been reset. The first versions of this Trojan appeared 10 years ago and during that time, the Trojan has changed significantly. This year the creators of Gozi, in addition to stealing banking data, turned to extortion via Trojan encryptors. We discovered that the code of Trojan Nymaim contains fragments from the Gozi banker that provide remote access to infected computers. This means that if the ransomware victim uses Internet banking, then the criminals not only extort money but also steal any available funds from the victim's bank account.

For a long time the Zbot Trojan family was an ever-present in the TOP 3, but with the emergence of mobile banking Trojans in this rating the situation has changed. It should be noted, however, that Zbot has not disappeared — it is in fourth place — and is used as a basis for a huge number of other banking Trojans, including Citadel, Kins and ZeusVM.

Third and ninth places are occupied by representatives of the Trojan Qhost family. This is one of the most basic banking Trojan families, though this has no bearing on its effectiveness. These two representatives modify the contents of the Host file on a victim's computer so that all requests to a bank's site go through a malicious server from which it is possible to 'break into the conversation' and replace the data that the user sees in the browser, as well as the data sent to the bank.

Countries where users face the greatest risk of online infection

In order to assess the countries in which users most often face cyber threats, we calculated how often Kaspersky Lab users encountered detection verdicts on their machines in each country. The resulting data characterizes the risk of infection that computers are exposed to in different countries across the globe, providing an indicator of the aggressiveness of the environment facing computers in different parts of the world.

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.

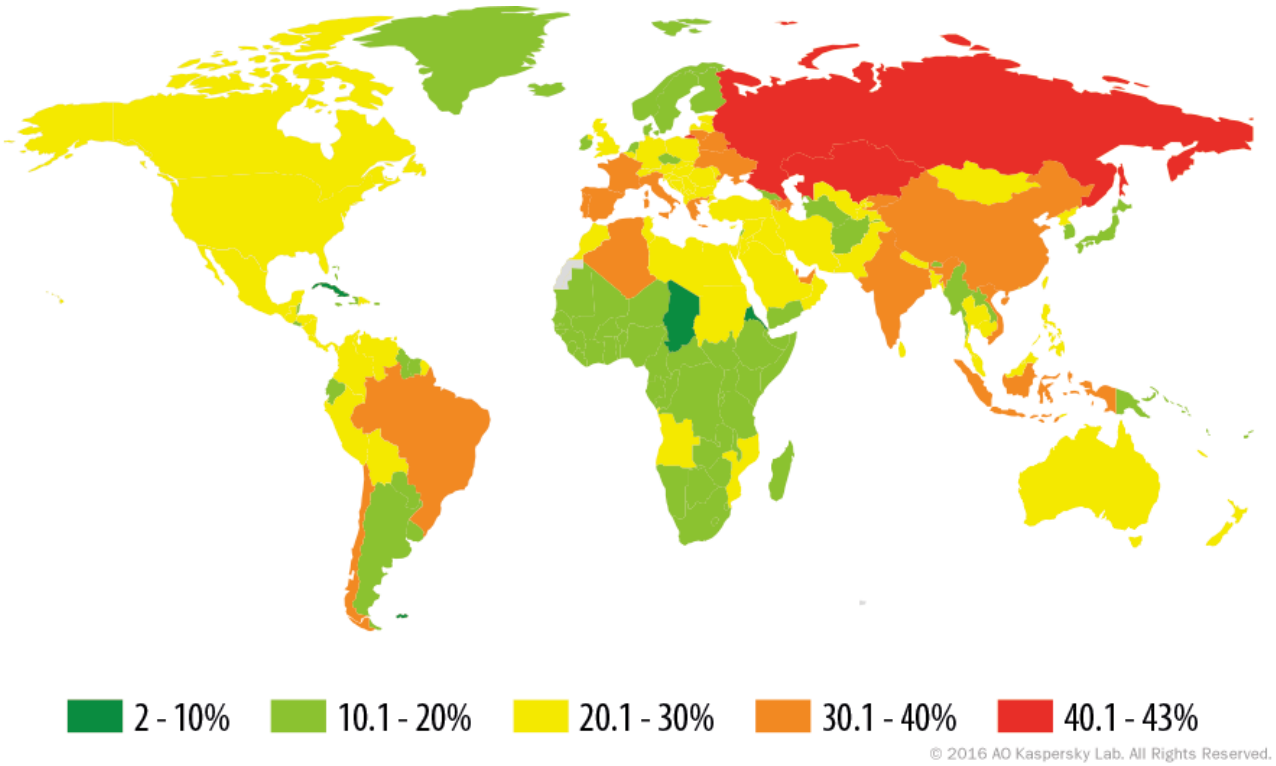
The TOP 20 countries where users face the greatest risk of online infection

	Country*	% of unique users**
1	Russia	42.15
2	Kazakhstan	41.22
3	Italy	39.92
4	Ukraine	39.00
5	Brazil	38.83
6	Azerbaijan	38.81
7	Spain	38.21
8	Belarus	38.04
9	Algeria	37.11
10	Vietnam	36.77
11	China	36.53
12	Portugal	35.86
13	France	34.74
14	Armenia	33.01
15	Greece	32.99
16	Chile	32.82
17	India	32.61
18	Qatar	32.53
19	Indonesia	32.30
20	Moldova	31.42

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.

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 50,000).

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



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

The countries can be divided into three groups that reflect the different levels of infection risk.

1. **The high risk group (40% and higher)**
   In 2016, this group includes the first two countries from the TOP 20 — Russia and Kazakhstan.

2. **The medium risk group (20-39.9%)**
   This group includes 105 countries; among them are Turkey (29.3%), Canada (29.5%), Poland (28.7%), Romania (27.4%), Mexico (26.8%), Australia (26.2%), Germany (26.2%), Belgium (25.3%), Austria (24.8%), the US (24%), Switzerland (23.6%), the UK (22.13%), Hungary (21.3%), Ireland (20%).

3. **The low risk group (0-19.9%)**
   The countries with the safest online surfing environments include the Czech Republic (19.6%), Argentina (19.5%), Japan (17.7%), Norway (15.9%), Sweden (15.2%), Georgia (14.6%), the Netherlands (14.5%), Denmark (12.2%).

In 2016, **31.9%** of computers were subject to at least one **Malware-class** web attack while online.

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.). In addition, these statistics include objects detected on user computers after the first scan of the system by Kaspersky Lab's file antivirus.

This section contains an analysis of the statistical data obtained based on antivirus scans of files on the hard drive at the moment they are created or accessed, and the results of scanning various removable data storages.

In 2016, Kaspersky Lab's antivirus solutions detected **4,071,588** unique malicious and potentially unwanted programs (i.e. unique programs are those who have a unique verdict).

TOP 20 verdicts detected on user computers

For this rating we identified the 20 most frequently detected threats on user computers in 2016. This rating does not include the Adware and Riskware classes of program.

	Name*	% of unique attacked users**
1	DangerousObject.Multi.Generic	42.32
2	Trojan.Win32.Generic	9.23
3	Trojan.WinLNK.Agent.gen	7.78
4	Trojan.WinLNK.StartPage.gena	6.25
5	Trojan.Script.Generic	5.86
6	Trojan.Win32.AutoRun.gen	4.78
7	Virus.Win32.Sality.gen	4.34
8	Trojan.WinLNK.Runner.jo	4.17
9	Worm.VBS.Dinihou.r	3.58
10	Trojan.WinLNK.Agent.ew	3.13
11	Trojan.Win32.Starter.yy	2.93
12	Trojan-Downloader.Script.Generic	2.80
13	Trojan.Win32.Autoit.cfo	2.27
14	Trojan.Win32.Wauchos.a	2.03
15	Virus.Win32.Nimnul.a	2.02
16	Trojan-Proxy.Win32.Bunitu.avz	1.90
17	Worm.Win32.Debris.a	1.83
18	Trojan.Win32.Hosts2.gen	1.80
19	Trojan-Dropper.VBS.Agent.bp	1.34
20	Trojan.WinLNK.StartPage.ab	1.26

These statistics are compiled from malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who consented to submit their statistical data.

* Malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who consented to submit their statistical data.

** The proportion of individual users on whose computers the file antivirus detected these programs as a percentage of all individual users of Kaspersky Lab products on whose computers a malicious program was detected.

The DangerousObject.Multi.Generic verdict, which is used for malware detected with the help of cloud technologies, is in first place (42.32%). Cloud technologies work when the antivirus databases do not yet contain either signatures or heuristics to detect a malicious program, but the company's cloud antivirus database already has information about the object. In fact, this is how the very latest malware is detected.

The proportion of viruses continues to decrease: for example, last year Virus.Win32.Sality.gen affected 5.53% of users, while in 2016 the figure was only 4.34%. For Virus.Win32.Nimnul these figures were 2.37% in 2015 and 2.02% in 2016. The Trojan-Dropper.VBS.Agent.bp verdict, 19th in this rating, is a VBS script that extracts Virus.Win32.Nimnul from itself and saves in to the disk.

In addition to heuristic verdicts and viruses, the TOP 20 includes verdicts for worms spread on removable media and their components. Their presence in this rating is due to the nature of their distribution and creation of multiple copies. A worm can continue to self-proliferate for a long time even if its management servers are no longer active.

For example, Trojan.Win32.Wauchos.a, a new verdict in this rating, is a component of the Worm.Win32.Debris family that installs the Trojan on removable drives. This Trojan is able to load other malware from C&C servers and was recorded loading new versions of Worm.Win32.Debris.

Trojan-Proxy.Win32.Bunitu.avz is not a typical verdict for this rating as it belongs to the Trojan-Proxy class and doesn't have a self-replicating mechanism.

The majority of the Trojan.Win32.Hosts2.gen samples this year are made up of host files that block access to antivirus sites and servers.

Countries where users face the highest risk of local infection

For each country, we calculated the number of file antivirus detections the users faced during the year. The data includes malicious programs located on user computers or on removable media connected to the computers, such as flash drives, camera and phone memory cards, or external hard drives. This statistic reflects the level of infected personal computers in different countries around the world.

The TOP 20 countries by level of infection

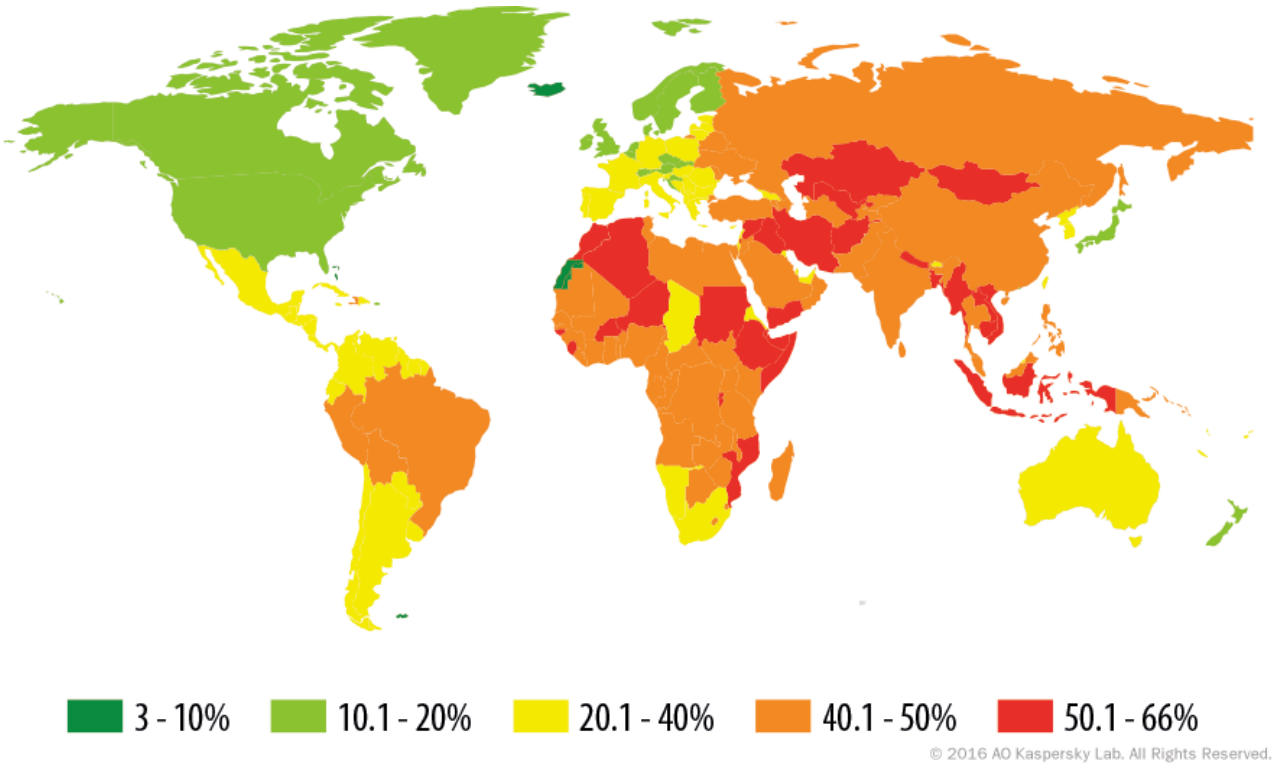
	Country*	% of unique users**
1	Vietnam	65.69
2	Somalia	63.90
3	Afghanistan	61.05
4	Rwanda	60.17
5	Algeria	59.80
6	Lao	58.90
7	Ethiopia	57.75
8	Bangladesh	57.39
9	Nepal	57.35
10	Mongolia	56.89
11	Cambodia	55.90
12	Indonesia	55.51
13	Mozambique	54.95
14	Uzbekistan	54.03
15	Iraq	53.97
16	Syria	53.44
17	Morocco	53.39
18	Myanmar	53.11
19	Kazakhstan	53.02
20	Niger	52.96

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

* When calculating, we excluded countries where there are fewer than 50,000 Kaspersky Lab users.

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

In the TOP 20 countries, at least one malicious program was found on an average of 36.8% of computers, hard drives or removable media belonging to KSN users.



Geography of malicious local infection in 2016 (ranked by percentage of targeted users)

The countries can be divided into several risk categories that reflect the level of local threats.

- **Maximum risk (over 60%):** four countries from the TOP 20.
- **High risk (41–60%):** countries include Iran (51.9%), India (50.4%), Belarus (48.7%), China (48.6%), Ukraine (47.9%), Saudi Arabia (44.04%), Russia (43.6%), Turkey (42%), Brazil (41.3%).
- **Moderate local infection rate (21–40.99%):** countries include Moldova (40.8%), Armenia (40.4%), Mexico (39.1%), South Africa (30.5%), Serbia (28.6%), Poland (29%), Bulgaria (27.4%), Spain (27%), Greece (26.2%), Italy (24.8%), Israel (24.8%), Hungary (23.4%), France (21.1%).

The 10 safest countries were:

	Country	% of unique users*
1	Denmark	10.4
2	Sweden	13.0
3	Netherlands	13.9
4	Japan	13.9
5	Norway	14.5
6	Ireland	15.1
7	Czech republic	15.2
8	Switzerland	15.75
9	United States	16.48
10	New Zealand	16.78

On average, 16% of user computers were attacked at least once throughout the year in the 10 safest countries.

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