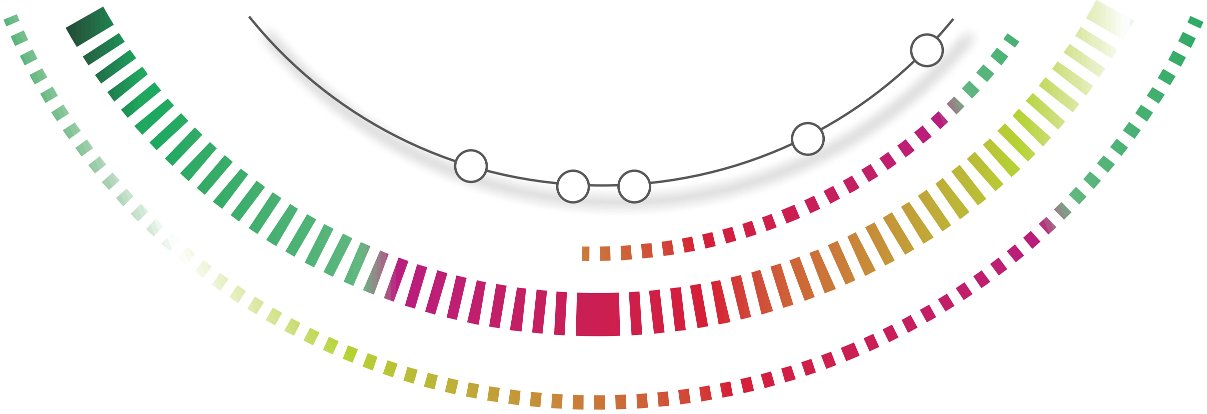
KASPERSKY SECURITY BULLETIN 2014

KASPERSKY lab



CONTENT

PREDICTIONS 2015

GREAT

(Global Research and Analysis Team)

CYBER-CRIMINALS MERGE WITH APT

In 2015, we expect to see another stage in the evolution of cyber-criminal activity with the adoption of APT tactics and techniques in financially motivated online criminal activity.

During a recent investigation, we discovered an attack in which an accountant's computer was compromised and used to initiate a large transfer with a financial institution. It represented the emergence of an interesting trend: targeted attacks directly against banks.

We are seeing an upsurge in malware incidents where banks are being breached using methods coming directly from the APT playbook. Once the attackers got into the banks' networks, they siphon enough information to allow them to steal money directly from the bank in several ways:

— Remotely commanding ATMs to dispose cash.

— Performing SWIFT transfers from various customers accounts,

— Manipulating online banking systems to perform transfers in the background.

Such attacks are an indication of a new trend that is embracing APT style attacks in the cybercriminal world.

APT GROUPS FRAGMENT, DIVERSIFY ATTACKS

The naming-and-shaming of APT groups in 2014 led to the public exposure and indictment of a hacking group that allegedly carried out cyber-espionage against U.S. businesses.

As security research teams continue to push for exposure of nation-state APT crews, we expect to see a shift in 2015 where the bigger, noisy APT groups splinter into smaller units, operating independently of each other. This in turn will result in a more widespread attack base, meaning more companies will be hit, as the smaller groups diversify their attacks. At the same time it means that bigger companies that were previously compromised by two or three major APT groups (eg. Comment Crew and Webky) will see more diverse attacks, coming from more sources.

OLD CODE, NEW (DANGEROUS) VULNERABILITIES

Recent allegations of deliberate tampering and accidental failures in crypto implementations (“goto fail”), and critical vulnerabilities in essential software (Shellshock, Heartbleed, OpenSSL) have left the community suspicious of unaudited software. The reaction has been to either launch independent audits of key software or have security researchers poke them in search of critical vulnerabilities (tantamount to an unofficial audit). This means that 2015 will be another year of new, dangerous vulnerabilities appearing in old code, exposing the Internet infrastructure to menacing attacks.

ESCALATION OF ATM AND POS ATTACKS

Attacks against cash machines (ATM) seemed to explode this year with several public incidents and a rush by law enforcement authorities globally to respond to this crisis. A corollary of this publicity is an awareness that ATMs are ripe for the taking and cybercriminals are sure to notice. As most of these systems are running Windows XP and also suffer from frail physical security, they are incredibly vulnerable by default and, as the impersonal gatekeepers of the financial institutions’ cash, cybercriminals are bound to come knocking here first.

In 2015, we expect to see further evolution of these ATM attacks with the use of APT techniques to gain access to the “brain” of cash machines. The next stage will see attackers compromising the networks of banks and using that level of access to manipulate ATM machines in real time.

MAC ATTACKS: OS X BOTNETS

Despite efforts by Apple to lock down the Mac operating system, we continue to see malicious software being pushed via torrents and pirated software packages. The increasing popularity of Mac OS X devices is turning heads in the criminal world, making it more appealing to develop malware for this platform. The closed-by-default ecosystem makes it harder for this malware to successfully take hold of the platform, but there remains a subsection of users who'll gladly disable Mac OS X security measures – especially people who use pirated software. This means that those looking to hijack OS X systems for a variety of reasons know that they simply need to bundle their malware with desirable software (probably in the form of a key generator) to enjoy widespread success. Due to widespread beliefs about the security of the OS X platform, these systems are also unlikely to have an antimalware solution installed that will flag the infection so once the malware is installed, so it's likely to go unnoticed for a very long time.

ATTACKS AGAINST TICKETING MACHINES

Incidents such as the NFC hack on Chilean public transport show an interest in abusing public resources such as transportation systems. Some hackers won't be looking to turn a profit from these types of attacks and will be satisfied to get some free rides and 'stick it to the man' by sharing this ability with others. However, ticketing systems are being shown to be vulnerable (many of them running Windows XP) and in many cities handle credit card transaction data directly. We expect to see bolder attacks on these systems to either game the system or steal credit card data for themselves.

ATTACKS AGAINST VIRTUAL PAYMENT SYSTEMS

Conventional wisdom tells us that cybercriminals are looking to monetize their daring exploits as simply and efficiently as possible. What better target than virtual payment systems in their infancy? As some countries like Ecuador rush to adopt virtual payment systems, we expect criminals to leap at every opportunity to exploit these. Whether social engineering the users, attacking the endpoints (cellphones in many cases), or hacking the banks directly, cybercriminals will jump all over directly monetized attacks and virtual payment systems will end up bearing the brunt.

These fears can also be extended to the new Apple Pay, which uses NFC (Near Field Communications) to handle wireless consumer transactions. This is a ripe market for security research and we expect to the appearance of vulnerability warnings about weaknesses in Apple Pay, virtual wallets and other virtual payment systems.

APPLE PAY

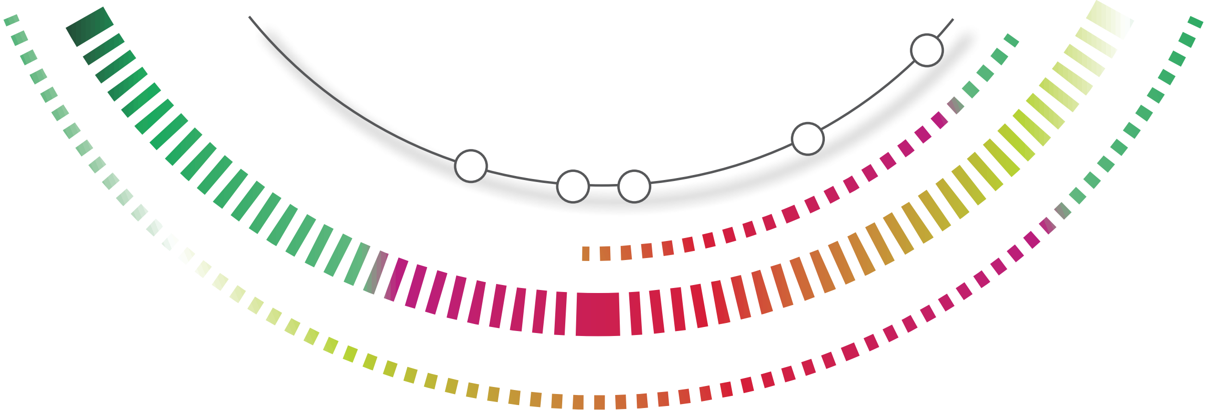
Previous attacks have focused on NFC payment systems but, thanks to limited adoption, these have reaped limited rewards. Apple Pay is bound to change that. The enthusiasm over this new payment platform is going to drive adoption through the roof and that will inevitably attract many cybercriminals looking to reap the rewards of these transactions. Apple's design possesses and increased focus on security (like virtualized transaction data) but we'll be very curious to see how hackers will exploit the features of this implementation.

COMPROMISING THE INTERNET OF THINGS

Attacks against the Internet of Things (IoT) have been limited to proof-of-concepts and (sometimes overhyped) warnings that smart televisions and refrigerators will be targeted by hackers to create botnets or launch mischievous attacks.

As more and more of these connected devices become available, we expect to see a wider discussion about security and privacy, especially among businesses in this space. In 2015, there will surely be in-the-wild attacks against networked printers and other connected devices that can help an advanced attacker to maintain persistence and lateral movement within a corporate network. We expect to see IoT devices form part of an APT group's arsenal, especially at high-value targets where connectivity is being introduced to the manufacturing and industrial processes.

On the consumer side, IoT attacks will be limited to demonstrations of weaknesses in protocol implementations and the possibility of embedding advertising (adware/spyware?) into smart TV programming.



OVERALL STATISTICS FOR 2014

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

The data presented covers the period from November 2013 to October 2014.

Maria **GARNAEVA**
Victor **CHEBYSHEV**
Denis **MAKRUSHIN**
Roman **UNUCHEK**
Anton **IVANOV**

THE YEAR IN FIGURES

- According to KSN data, Kaspersky Lab products detected and neutralized a total of **6,167,233,068** threats during the reported period.
- A total of **3,693,936** attempts to infect Mac OS X- based computers were blocked by Kaspersky Lab products.
- Kaspersky Lab solutions blocked **1,363,549** attacks on Android-based devices.
- Kaspersky Lab solutions repelled **1,432,660,467** attacks launched from online resources located all over the world.
- To carry out their attacks, cybercriminals used **9,766,119** unique hosts.
- **44%** of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US and Germany.
- **38%** of user computers were subjected to at least one web attack over the year.
- A total of **1,910,520** attempts to launch banking malware on user computers were neutralized in 2014.
- Kaspersky Lab's web antivirus detected **123,054,503** unique malicious objects: scripts, exploits, executable files, etc.
- Kaspersky Lab's antivirus solutions detected a total of **1,849,949** unique malicious and potentially unwanted objects.

MOBILE THREATS

During the reporting period Kaspersky Lab detected the following:

- **4,643,582** malicious installation packets
- **295,539** new malicious mobile programs
- **12,100** mobile banking Trojans

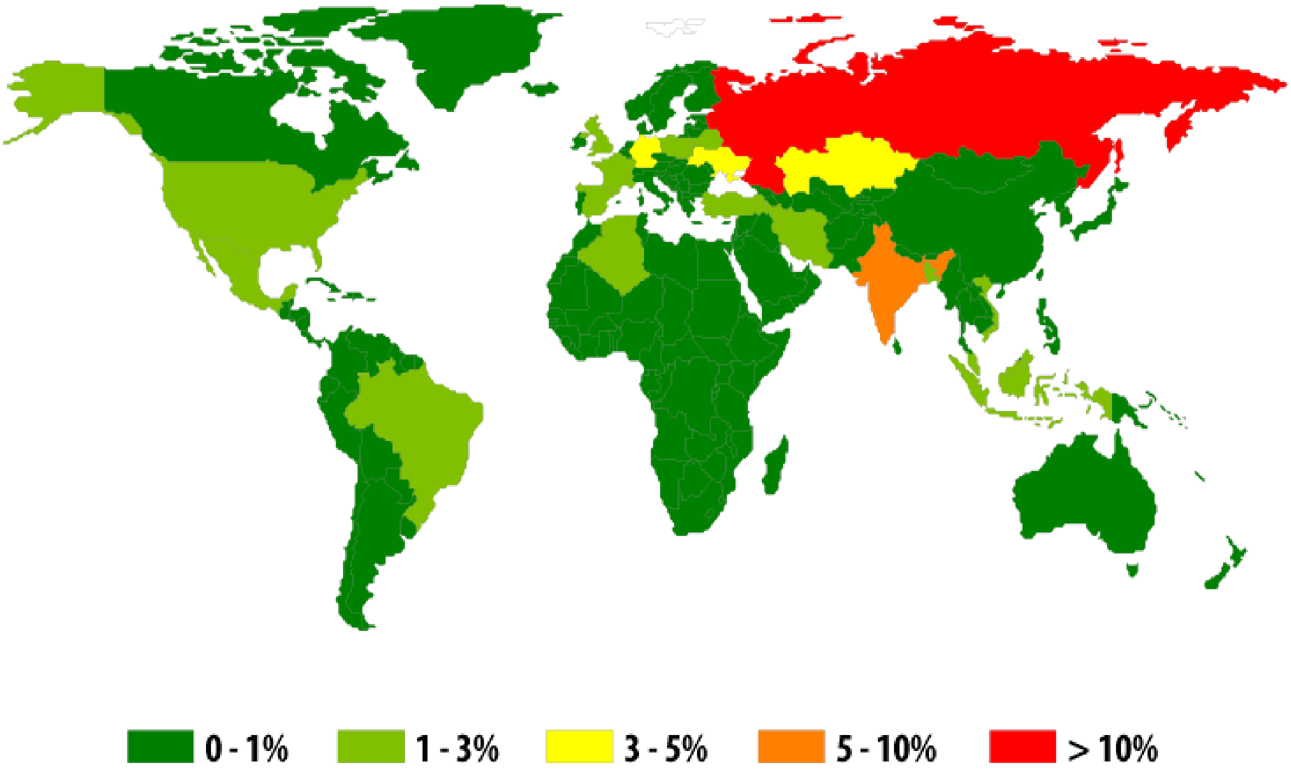
Overall from the beginning of November 2013 to the end of October 2014 Kaspersky Lab warded off **1,363,549** unique attacks. For the same period in 2012-2013 the figure was **335,000** unique attacks. There were four times as many attacks on Android devices compared with the previous 12 months.

19% of Android users encountered a mobile threat at least once during the year - nearly one in five users.

53% of Android-attacks used mobile Trojans designed to steal the user’s money (SMS Trojans and banking Trojans).

Geography of mobile threats

Attacks by malicious mobile software were recorded in more than **200** countries.



© Kaspersky Lab

Percentage from total number of attacked users

TOP 10 countries by number of attacked users

	Country	% of attacked users*
1	Russia	45.7%
2	India	6.8%
3	Kazakhstan	4.1%
4	Germany	4.0%
5	Ukraine	3.0%
6	Vietnam	2.7%
7	Iran	2.3%
8	UK	2.2%
9	Malaysia	1.8%
10	Brazil	1.6%

** Percentage of attacked users in the country from total number of attacked users*

Russia maintained its leading position in terms of the number of users attacked.

The number of recorded attacks greatly depends on the number of users in a country. To evaluate the danger of infection by mobile malware in various countries we counted the percentage of malicious applications among the total number applications that users tried to install. This method produced very different results from those shown above.

TOP 10 countries by risk of infection

	Country*	**% of malicious applications**
1	Vietnam	2.34%
2	Poland	1.88%
3	Greece	1.70%
4	Kazakhstan	1.62%
5	Uzbekistan	1.29%
6	Serbia	1.23%
7	Armenia	1.21%
8	Czech Republic	1.02%
9	Morocco	0.97%
10	Malaysia	0.93%

** Countries where the number of downloaded applications was less than 100,000 were excluded from these results*

Vietnam leads this rating: **2.34%** of all applications that users tried to download were malicious.

Russia, which suffered by far the most attacks, was only 22nd in terms of risk of infection with **0.69%**.

In Spain the risk of infection was **0.54%**, in Germany **0.18%** and in the UK **0.16%**, in Italy 0.09% and in the USA **0.07%**. The situation is best of all in Japan, where only 0.01% of all applications that users tried to install proved to be malicious.

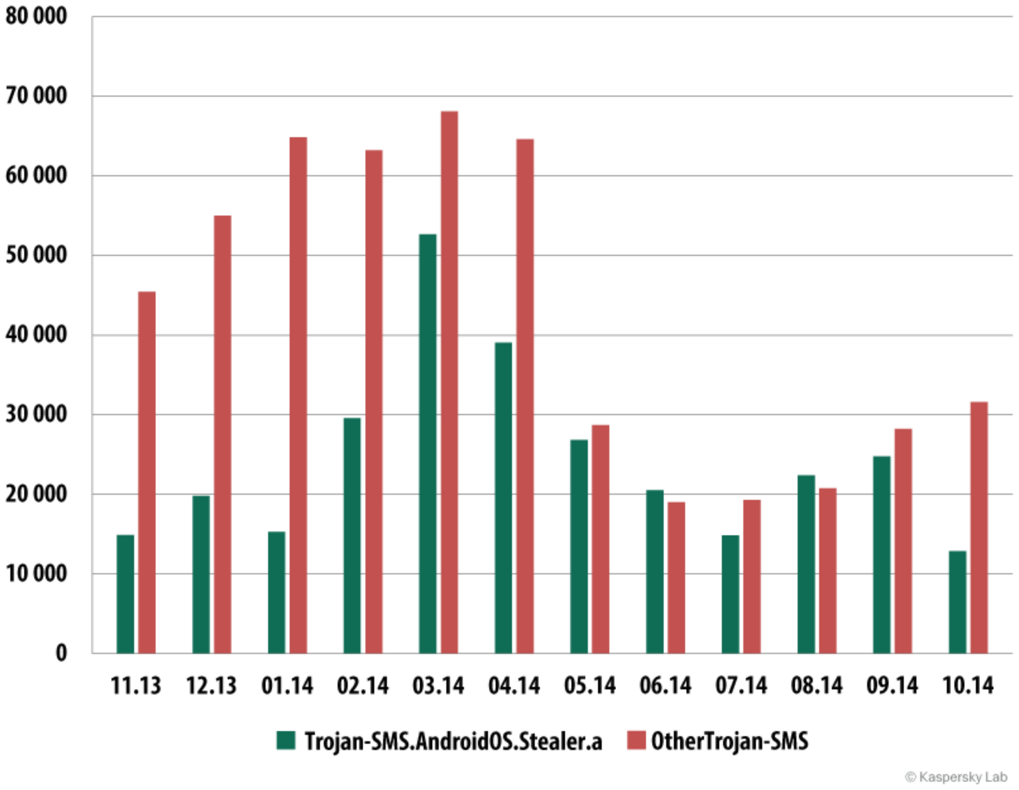
TOP 20 mobile threats of 2014

	Name	% of attacks
1	Trojan-SMS.AndroidOS.Stealer.a	18.0%
2	RiskTool.AndroidOS.MimobSMS.a	7.1%
3	DangerousObject.Multi.Generic	6.9%
4	RiskTool.AndroidOS.SMSreg.gc	6.7%
5	Trojan-SMS.AndroidOS.OpFake.bo	6.4%
6	AdWare.AndroidOS.Viser.a	5.9%
7	Trojan-SMS.AndroidOS.FakeInst.a	5.4%
8	Trojan-SMS.AndroidOS.OpFake.a	5.1%
9	Trojan-SMS.AndroidOS.FakeInst.fb	4.6%
10	Trojan-SMS.AndroidOS.Erop.a	4.0%
11	AdWare.AndroidOS.Ganlet.a	3.8%
12	Trojan-SMS.AndroidOS.Agent.u	3.4%
13	Trojan-SMS.AndroidOS.FakeInst.ff	3.0%
14	RiskTool.AndroidOS.Mobogen.a	3.0%
15	RiskTool.AndroidOS.CallPay.a	2.9%
16	Trojan-SMS.AndroidOS.Agent.ao	2.5%
17	Exploit.AndroidOS.Lotoor.be	2.5%
18	Trojan-SMS.AndroidOS.FakeInst.ei	2.4%
19	Backdoor.AndroidOS.Fobus.a	1.9%
20	Trojan-Banker.AndroidOS.Faketoken.a	1.7%

10 out of the 20 programs in this rating are SMS Trojans from the following families: Stealer, OpFake, FakeInst, Agent and Erop.

Trojan-SMS.AndroidOS.Stealer. a were among the most widespread families throughout the year and finished up on top of the annual ranking by a considerable margin.

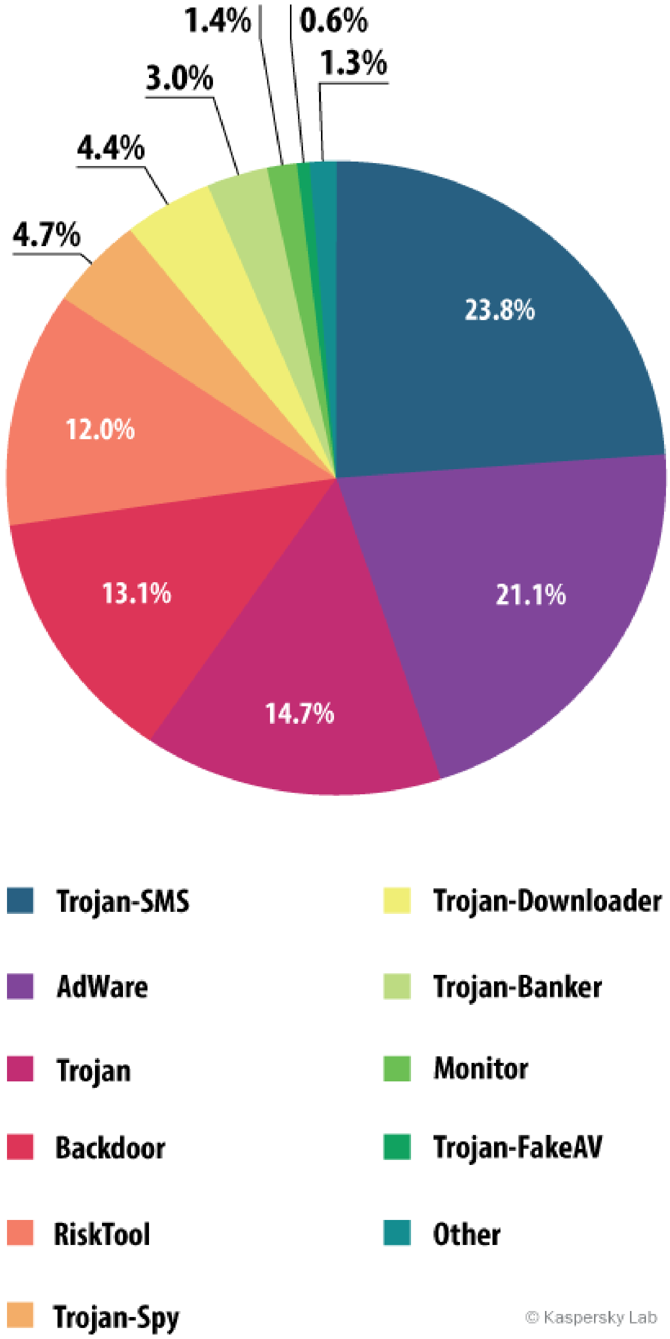
This SMS Trojan spread very actively. After May 2014 the number of Stealer attacks matched the total number of attacks involving all other SMS Trojans.



The number of users attacked with Trojan-SMS.AndroidOS.Stealer.a and all other SMS Trojans (November 2013 - October 2014)

Reduction in attacks by SMS Trojans

As before, SMS Trojans are the single biggest component in the flow of mobile malware; in our figures they have **23.9%** of the total.

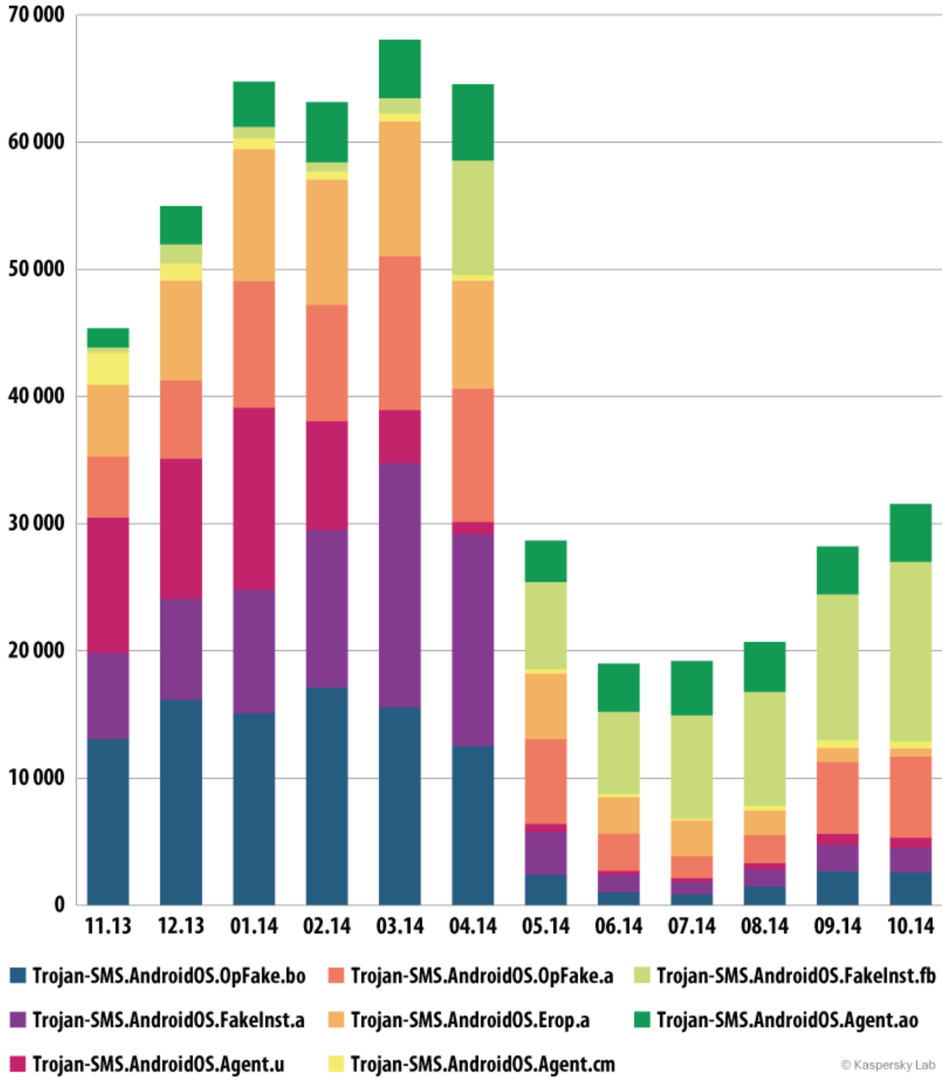


© Kaspersky Lab

Distribution of mobile threats by type (Kaspersky Lab collection)

However, as the above diagram shows, in the second half of 2014 there were fewer attacks with SMS Trojans. As a result for the year their amount reduced by **12.3%**.

Let's look in a bit more detail at the change in distribution of the SMS Trojans that are most popular with cybercriminals (other than Stealer.a).



Number of users attacked by popular SMS Trojans
(November 2013 — October 2014)

May saw a sharp fall in the number of SMS Trojans detected in Russia, where attacks with the use of SMS Trojans are particularly widespread. The fall was caused by a change in the way paid messages work in Russia. In May 2014 mobile operators in Russia were forced to use an Advice of Charge (AoC) mechanism. Now when a mobile device sends a message to a paid number the operator must inform the device owner of the cost of the service and get confirmation of the payment.

As a result, SMS Trojans are less profitable and their criminal nature is clearly exposed. Now the only way to make a profit is to use Trojans that can send an SMS to a premium rate number and then intercept the operator's request and return a confirmation on behalf of the user.

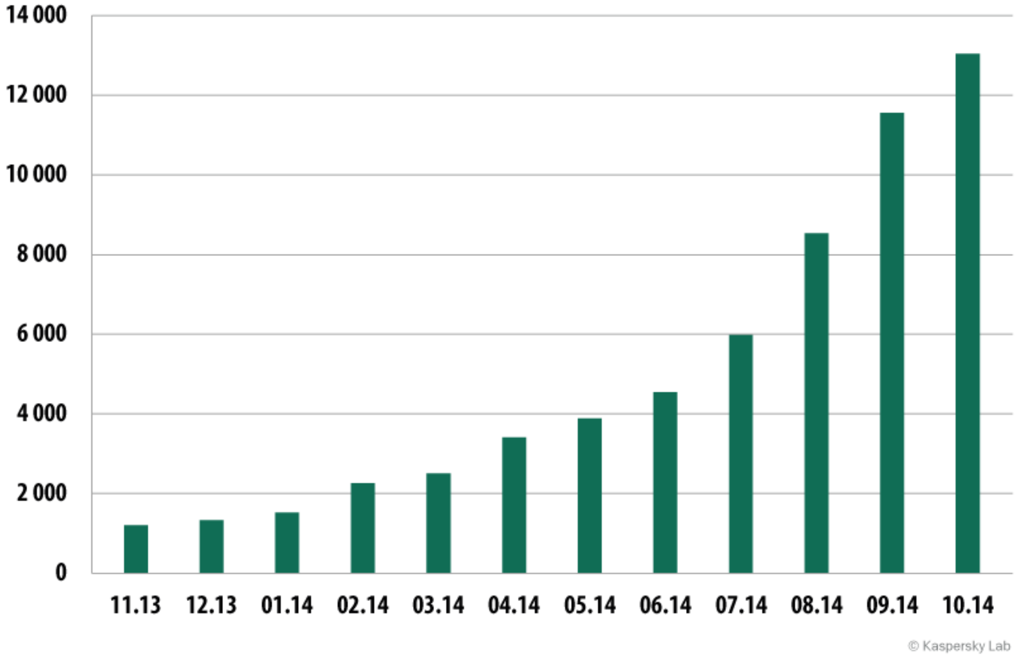
As a result partners in several semi-legal programs, which had earlier distributed applications with SMS Trojan functionality, left this business. Their operating model had been based on badly explained conditions for the provision of paid services, or subscription and service charges that were simply not indicated.

We can assume that Russian creators of SMS Trojans who found themselves out of work will have to look for new projects. Some of them might switch to attacking users in other countries and some to working on more serious malware such as banking programs. Hopefully at least some of them will turn their backs on the underworld and will put their skills to lawful use.

The changes in distribution patterns are clearly visible with once-popular SMS trojans like OpFake.bo, FakeInst.a and OpFake.a. They used to be seen in **10-20,000** attacks a month; now the numbers are **1-2,000**.

Mobile banking Trojans

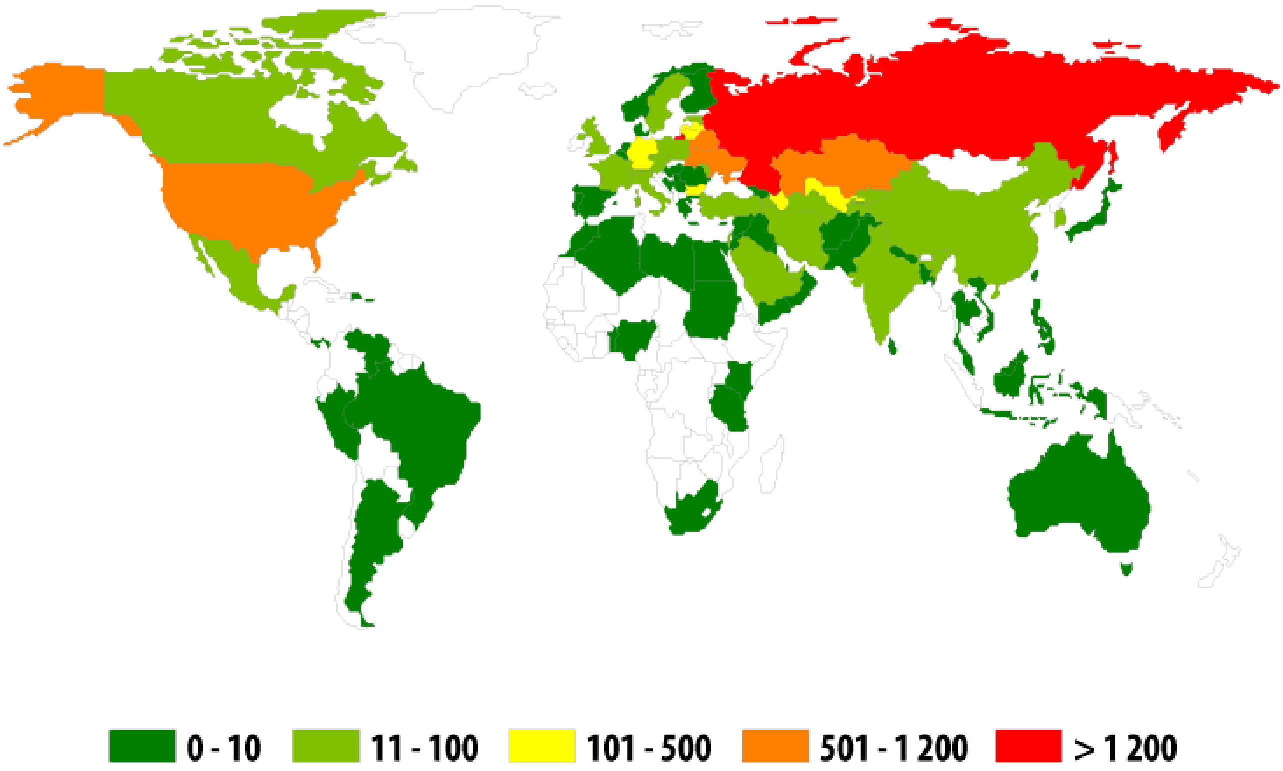
During the period in question we detected **12,100** mobile banking Trojans — nine times as many as than in 2013.



Number of mobile banking Trojans in the Kaspersky Lab collection (November 2013 — October 2014)

45,032 users were attacked with mobile banking Trojans at least once in the course of the year.

And the number of countries under attack is growing: at least one attack using a mobile banking Trojan was recorded in **90** different countries worldwide.



© Kaspersky Lab

Geography of mobile banking threats
(number of attacked users in the period November 2013 — October 2014)

TOP 10 countries for banking Trojan attacks

	Country	**Number of attacked users**	**% of all attacks***
1	Russia	39,561	87.85%
2	Kazakhstan	1,195	2.65%
3	Ukraine	902	2.00%
4	USA	831	1.85%
5	Belorus	567	1.26%
6	Germany	203	0.45%
7	Lithuania	201	0.45%
8	Azeraijan	194	0.43%
9	Bulgaria	178	0.40%
10	Uzbekistan	125	0.28%

** Perentage of attacked users in each country from the total all attacked users*

Russia has retained its place as the leader in this rating.

THREATS DESIGNED FOR MAC OS X

In 2014 Kaspersky Lab security products designed to protect Mac OS X-based computers blocked **3,693,936** infection attempts.

Kaspersky Lab experts detected **1,499** new malicious programs for Mac OS X, **200** samples more than in the previous year.

Every second user of Kaspersky Lab products was exposed to a malicious attack.

An average Mac user encountered **9** threats during the year.

TOP 20 threats designed for Mac OS X

	Name	% of attacks*
1	AdWare.OSX.Geonei.b	9.04%
2	Trojan.Script.Generic	5.85%
3	Trojan.OSX.Vsrch.a	4.42%
4	Trojan.Script.Iframer	3.77%
5	AdWare.OSX.Geonei.d	3.43%
6	DangerousObject.Multi.Generic	2.40%
7	AdWare.OSX.Vsrch.a	2.18%
8	Trojan.Win32.Generic	2.09%
9	AdWare.OSX.FkCodec.b	1.35%
10	Trojan.OSX.Yontoo.i	1.29%
11	Trojan-PSW.Win32.LdPinch.ex	0.84%
12	AdWare.Win32.Yotoon.heur	0.82%
13	Trojan.OSX.Yontoo.j	0.80%
14	Exploit.Script.Generic	0.76%
15	AdWare.OSX.Bnodlero.a	0.58%
16	AdWare.JS.Agent.an	0.57%
17	Trojan.OSX.Yontoo.h	0.52%
18	Exploit.PDF.Generic	0.51%
19	AdWare.Win32.MegaSearch.am	0.50%
20	Trojan.Win32.AutoRun.gen	0.43%

** The percentage of users attacked by the malicious program of all attacked users.*

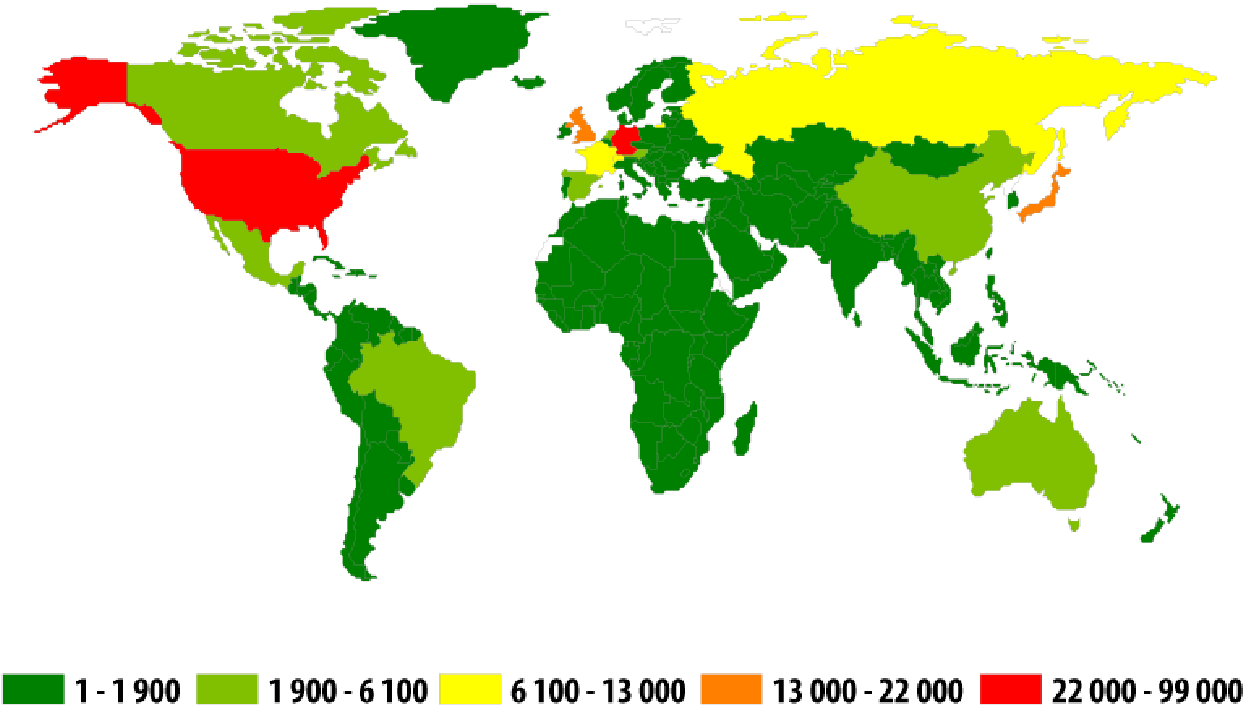
Almost half of our TOP 20 programs, including the one in first place, were occupied by AdWare programs. As a rule, these malicious programs arrive on users' computers alongside legitimate programs if they are downloaded from a software store rather than from the official website of the developer. These legitimate programs might become a carrier for the AdWare-module: once installed on the user's computer it can add advertising links to browser bookmarks, change the default search engine, add contextual advertising, etc.

Interestingly, 8th place is occupied by Trojan.Win32.Generic which affects Windows OS. This is probably because this particular Trojan can penetrate into virtual machines that run under Windows.

In 2014 the experts detected several interesting malicious programs for Mac OS X that should be mentioned separately.

- **Backdoor.OSX.Callme** – a backdoor that provides the fraudster with remote access to the system and at the same time steals contact lists, apparently, to find new victims. It is distributed in the body of a specially designed MS Word document: when run it installs the backdoor via the vulnerability in the system.
- **Backdoor.OSX.Laoshu** – a malicious program which makes screenshots every minute. This backdoor is signed by the trusted certificate of the developer which means the creators of the program were about to place it in the AppStore.
- Backdoor.OSX.Ventir – a multi-module Trojan spy with a hidden remote control function. It includes the keystrokes interception driver logkext, the source code for which is publicly available.
- Trojan.OSX.IOSinfector – used to install the mobile version of Trojan-Spy.IPhoneOS.Mekir (OSX/Crisis).
- Trojan-Ransom.OSX.FileCoder – the first file coder for OS X. It is a conditionally working prototype produced by an author who, for whatever reason, decided to abandon malware development.
- Trojan-Spy.OSX.CoinStealer – the first malicious program designed to steal bitcoins for OS X. It imitates different bitcoin utilities built from open source code while it installs a malicious browser extension and/or a patched version of bitcoin-qt.
- Trojan-Downloader.OSX.WireLurker – an unusual piece of malware designed to steal victims' data. It attacks not only Mac-based computers but iOS-based devices connected to them. There is also a Windows-based version of this malicious program. It is distributed via a well-known Chinese store that sells apps for OS X and iOS.

The geography of threats



© Kaspersky Lab

The geography of attacks on Mac OS X users in 2014
(based on the number of all attacked users)

The TOP 10 of countries under attack

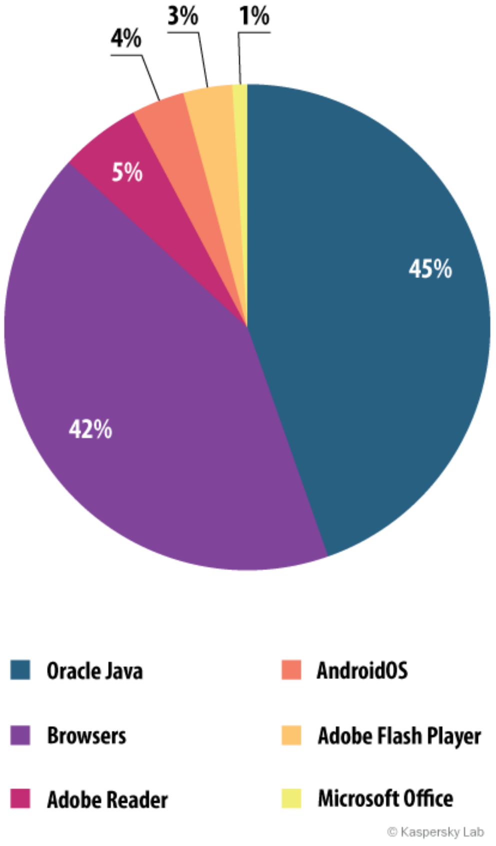
	Country	Number of attacked users	% Of attacks*
1	USA	98,077	39.14%
2	Germany	31,466	12.56%
3	Japan	13,808	5.51%
4	UK	13,763	5.49%
5	Russia	12,207	4.87%
6	France	9,239	3.69%
7	Switzerland	6,548	2.61%
8	Canada	5,841	2.33%
9	Brazil	5,558	2.22%
10	Italy	5,334	2.13%

** The percentage of users attacked per country*

The **USA** (39.14%) tops this rating, perhaps because of the popularity of Apple computers in the country. **Germany** (12.56%) came second followed by **Japan** (5.51%).

VULNERABLE APPLICATIONS USED BY FRAUDSTERS

The graph of vulnerable applications shown below is based on information about the exploits blocked by our products. These exploits were used by hackers in Internet attacks and when compromising local applications, including those installed on mobile devices.



The distribution of exploits used by fraudsters, by type of application attacked, 2014

In 2014, the fraudsters most often exploited Oracle Java vulnerabilities. However, the popularity of Java vulnerabilities declined steadily throughout the year, and its overall share was less than half of last year’s figure – **45%** against **90.5%** 12 months ago. This might be due to the closure of old vulnerabilities and a lack of information about any new ones.

Second place was occupied by the Browsers category (**42%**) which includes exploits for Internet Explorer, Google Chrome, Mozilla Firefox, etc. According to the quarterly ratings, for much of 2014 this was the leading category but it didn't quite outstrip the large number of Java exploits in late 2013 and early 2014.

Adobe Reader exploits were in third place (5%). These vulnerabilities are exploited in drive-by attacks via the Internet, and PDF exploits form part of many exploit packs.

During the year, we saw a decrease in the number of attacks using exploit packs. There may be several reasons for this, including the arrests of some of their developers. In addition, many exploit packs have stopped attacking computers protected by Kaspersky Lab products (exploit packs check the victim computer and halt the attack if a Kaspersky Lab solution is installed on it). Despite this, exploitation of vulnerabilities remains one of the main ways to deliver malicious software on the user's computer.

ONLINE THREATS (WEB-BASED ATTACKS)

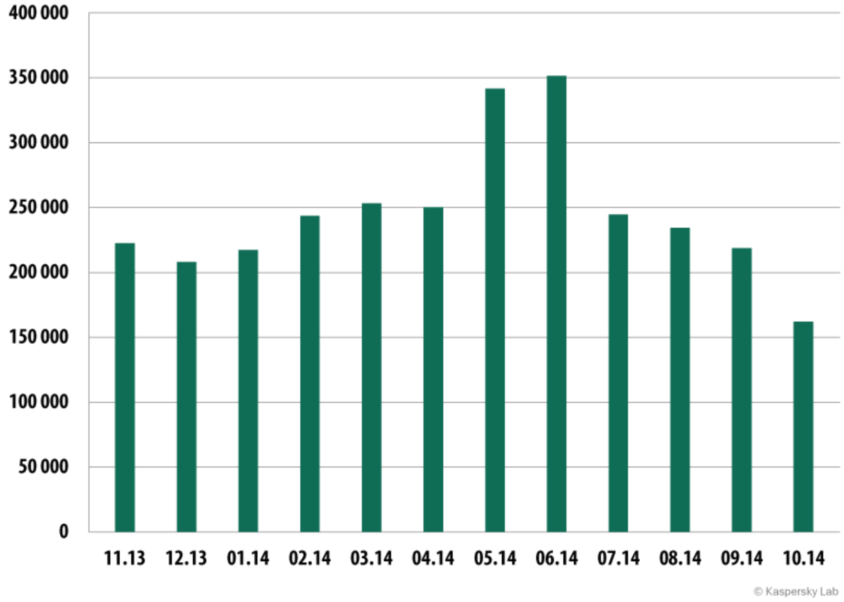
The statistics in this section were derived from web antivirus components that protect Windows users when malicious code attempts to download from a malicious/infected website. Malicious websites are deliberately created by cybercriminals; infected sites include those with user-contributed content (such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

In 2014, there were **1,432,660,467** attacks launched from online resources located all over the world. It means that Kaspersky Lab products protected users an average **of 3,925,097** times per day during their Internet sessions.

The main attack method - via exploit packs - gives attackers an almost guaranteed opportunity to infect the user computer if it is not protected with a security solution and if it has at least one popular and vulnerable (not updated) application installed.

Online threats in the banking sector

During the reporting period, Kaspersky Lab solutions blocked **1,910,520** attacks attempting to launch malware capable of stealing money from online banking accounts.

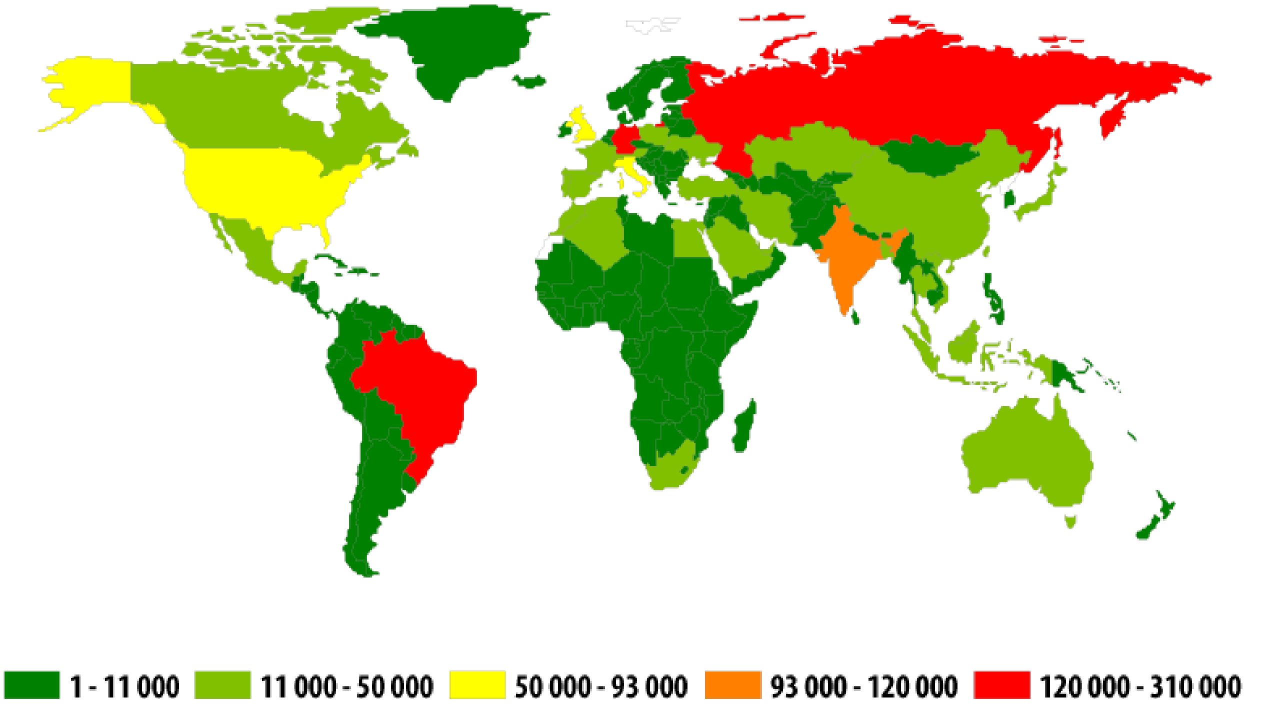


The number of computers attacked by financial malware, November 2013-October 2014

Noticeably, the number of attacks grew considerably in May and June 2014. This might have been be caused by an increase in online banking activity at the beginning of the holiday season as well as by the main sport event of the year – the World Cup-2014 in Brazil – where cybercriminals used financial malware to steal tourists' payment data.

A total of **16,552,498** notifications of malicious activity by programs designed to steal money via online access to bank accounts were registered by Kaspersky Lab security solutions in 2014.

The geography of attacks



© Kaspersky Lab

The geography of banking malware attacks in 2014

The TOP 20 countries by the number of attacked users

	Country	Number of attacked users
1	Brazil	299,830
2	Russia	251,917
3	Germany	155,773
4	India	98,344
5	USA	92,224
6	Italy	88,756
7	UK	54,618

	Country	Number of attacked users
8	Vietnam	50,040
9	Austria	44,445
10	Algeria	33,640

The TOP 10 banking malware families

The table below shows the programs most commonly used in 2014 to attack online banking users, based on the number of reported infection attempts:

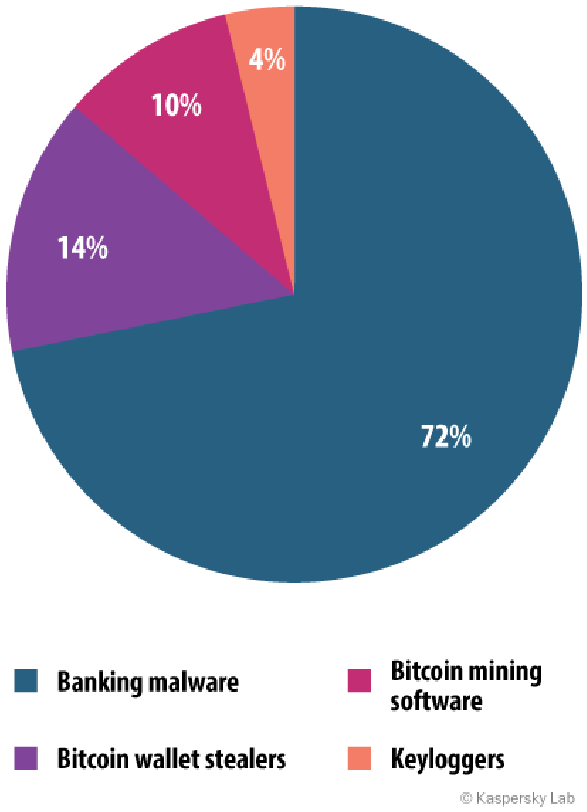
	Name	Number of attacked users
1	Trojan-Spy.Win32.Zbot	742,794
2	Trojan-Banker.Win32.ChePro	192,229
3	Trojan-Banker.Win32.Lohmys	121,439
4	Trojan-Banker.Win32.Shiotob	95,236
5	Trojan-Banker.Win32.Agent	83,243
6	Trojan-Banker.AndroidOS.Faketoken	50,334
7	Trojan-Banker.Win32.Banker	41,665
8	Trojan-Banker.Win32.Banbra	40,836
9	Trojan-Spy.Win32.SpyEyes	36,065
10	Trojan-Banker.HTML.Agent	19,770

Zeus (Trojan-Spy.Win32.Zbot) remained the most widespread banking Trojan. It kept its leading position in quarterly ratings so its 1st place in the TOP 10 for 2014 is not a surprise. Second came Trojan-Banker.Win32.ChePro, followed by Trojan-Banker.Win32.Lohmys. Both families have the same functionality and are spread via spam messages with a theme related to online banking (for example, an invoice from an online banking service). The email includes a Word document with the attached picture: clicking on the picture launches malicious code execution.

Trojan-Banker.Win32.Shiotob was in 4th place. This malicious program is most often spread via spam messages and is designed to monitor traffic in order to intercept payment data.

The majority of the Top 10 malicious programs work by injecting random 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.

Although three quarters of attacks targeting users' money were carried out with the help of banking malware these are not the only financial threats.



Distribution of attacks targeting user money by malware type, 2014

Bitcoin wallet theft was the second most popular banking threat (14%). Yet another threat related to crypto currency is Bitcoin mining software (10%) which uses computing resources to generate bitcoins.

The TOP 20 malicious objects detected online

In 2014, Kaspersky Lab's web antivirus detected **123,054,503** unique malicious objects: scripts, exploits, executable files, etc.

We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2014. These 20 accounted for **95.8%** of all online attacks.

	Name*	**% of all attacks****
1	Malicious URL	73.70%
2	Trojan.Script.Generic	9.10%
3	AdWare.Script.Generic	4.75%
4	Trojan.Script.Iframer	2.12%
5	Trojan-Downloader.Script.Generic	2.10%

	Name*	% of all attacks**
6	AdWare.Win32.BetterSurf.b	0.60%
7	AdWare.Win32.Agent.fflm	0.41%
8	AdWare.Win32.Agent.aiyc	0.38%
9	AdWare.Win32.Agent.allm	0.34%
10	Adware.Win32.Amonetize.heur	0.32%
11	Trojan.Win32.Generic	0.27%
12	AdWare.Win32.MegaSearch.am	0.26%
13	Trojan.Win32.AntiFW.b	0.24%
14	AdWare.JS.Agent.an	0.23%
15	AdWare.Win32.Agent.ahbx	0.19%
16	AdWare.Win32.Yotoon.heur	0.19%
17	AdWare.JS.Agent.ao	0.18%
18	Trojan-Downloader.Win32.Generic	0.16%
19	Trojan-Clicker.JS.Agent.im	0.14%
20	AdWare.Win32.OutBrowse.g	0.11%

** 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 web attacks recorded on the computers of unique users.*

As is often the case, the TOP 20 is largely made up of objects used in drive-by attacks, as well as adware programs. **73.7%** of all verdicts identified links from these black lists.

Noticeably, in 2014 there was an increase in the number of advertising programs in the TOP 20, up from 5 to 12 compared to the previous year and accounting for **8.2%** of all malicious objects detected online (+7.01 percentage points). The growth in the amount of advertising programs, along with their aggressive distribution schemes and their efforts to counteract anti-virus detection, has become the trend of 2014.

The Trojan-Clicker.JS.Agent.im verdict is also connected to advertising and all sorts of “potentially unwanted” activities. This is how scripts placed on Amazon Cloudfront to redirect users to pages with advertising content are detected. Links to these scripts are inserted by adware and various extensions for browsers, mainly on users’ search pages. The scripts can also redirect users to malicious pages containing recommendations to update Adobe Flash and Java - a popular method of spreading malware.

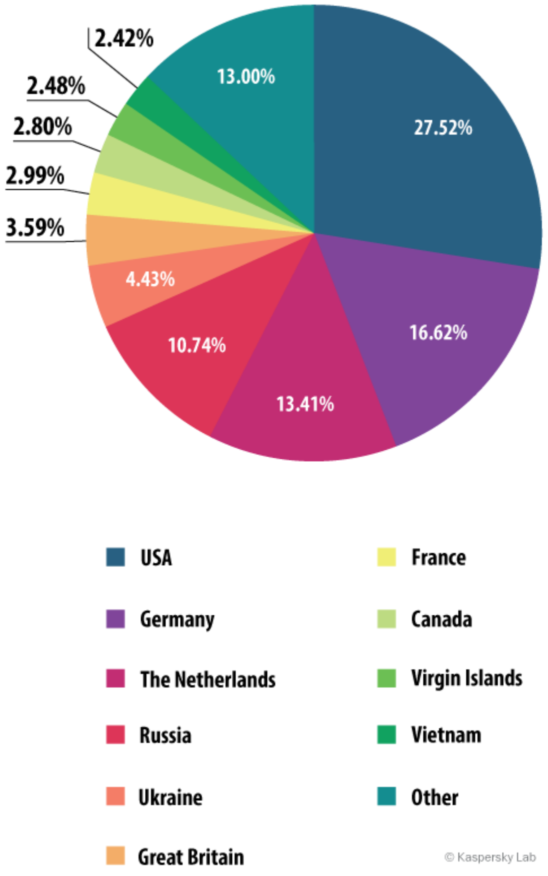
The TOP 10 countries where online resources are seeded with malware

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

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

In 2014, Kaspersky Lab solutions blocked **1,432,660,467**attacks launched from web resources located in various countries around the world. To carry out their attacks, the fraudsters used **9,766,119** unique hosts, **838,154** hosts or **8%** fewer than in 2013.

87% of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries. This is 5 percentage points more than in the previous year.



The distribution of online resources seeded with malicious programs in 2014

In 2014, the TOP 10 rating of countries where online resources are seeded with malware remained largely unchanged from the previous year. However four countries changed places: Germany and Russia swapped, with the Germans climbing to 2nd and Russia dropping to fourth. Ukraine overtook Britain to move up to 5th.

44% of all web attacks came from resources located in the USA and Germany.

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 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.

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

	Country*	% of unique users**
1	Russia	53.81%
2	Kazakhstan	53.04%
3	Azerbaijan	49.64%
4	Vietnam	49.13%
5	Armenia	48.66%
6	Ukraine	46.70%
7	Mongolia	45.18%
8	Belarus	43.81%
9	Moldova	42.41%
10	Kyrgyzstan	40.06%
11	Germany	39.56%
12	Algeria	39.05%
13	Qatar	38.77%
14	Tadjikistan	38.49%
15	Georgia	37.67%
16	Saudi Arabia	36.01%
17	Austria	35.58%
18	Lithuania	35.44%

	Country*	**% of unique users****
19	Sri Lanka	35.42%
20	Turkey	35.40%

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

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

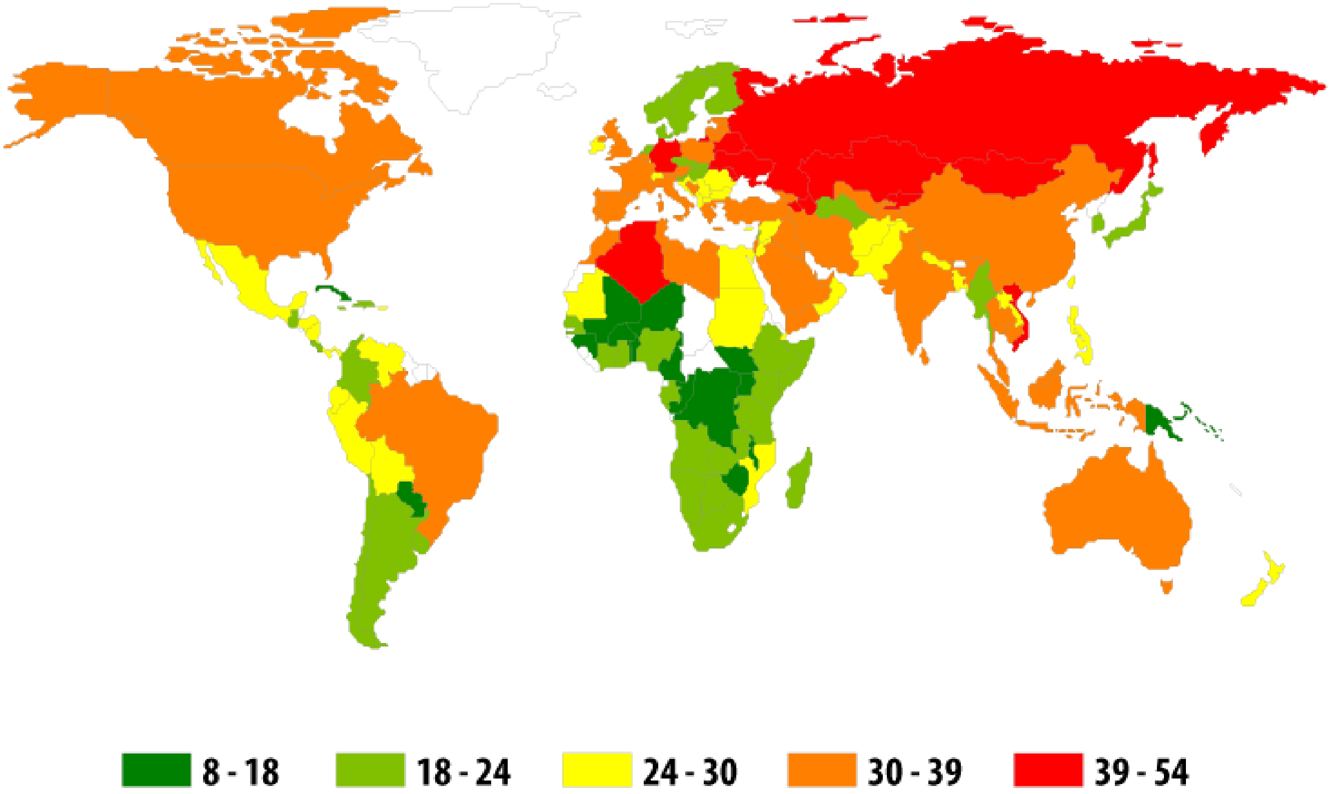
The year 2014 saw a change of leader in the TOP 20: the rating was topped by Russia where **53.81%** of users faced the risk of online infection.

Last year's leader, Azerbaijan, fell to 3rd position (49.64%).

Uzbekistan, Malaysia, Greece and Italy dropped out of the TOP 20. Among the newcomers were Mongolia, Qatar, Saudi Arabia, Turkey and Lithuania.

All countries can be divided into three groups expressing different levels of infection risk.

1. The high risk group (over 41%). In 2014, this group includes nine countries from the TOP 20, compared to **15** countries in 2013.
2. The risk group (21-40%). This group includes **111** countries; among them are Kyrgyzstan (40.1%), Germany (39.6%), Qatar (38.8%), Tajikistan (38.5%), Georgia (37.7), Saudi Arabia (36%), Turkey (35. 4%), France (34.9%), India (34.8%), Spain (34.4%), USA (33.8%), Canada (33.4%), Australia (32.5%), Brazil (32.1%), Poland (31.7%), Italy (31.5%), Israel (30.2%), China (30.1%), the UK (30%), Egypt (27.8%), Mexico (27.5%), the Philippines (27.2%), Croatia (26.2%), Pakistan (26.1%), Romania (25.7%), Japan (21. 2%), Argentina (21. 1%).
3. The low risk group (0-20.9%). The **39** countries with the safest online surfing environments include Sweden (19.5%), Denmark (19.2%), Uruguay (19.5%) and a number of African countries.



© Kaspersky Lab

In 2014, **38.3%** of computers were attacked at least once while their owners were online.

On average, the risk of being infected while surfing the Internet decreased by 3.3 percentage points over the year. This may be caused several factors:

- Firstly, developers of browsers and search engines realized the necessity of securing their users and started to contribute to the fight against malicious sites
- Secondly, many exploit packs have started to check if Kaspersky Lab's product is installed on the user's computer. If it is, the exploits do not even try to attack the computer.
- Thirdly, users using more and more mobile devices and tablets to surf the Internet.

In addition, the number of attacks using exploit packs slightly decreased: arresting the developers of these packs was not in vain. However there are no grounds to expect some drastic change in the situation with exploits: they are still the main technique used to deliver malware, including for targeted attacks. The Internet remains the major source of malware for users in most countries.

LOCAL THREATS

Local infection statistics for user computers are a very important indicator. This data points to threats that have penetrated the Windows operating system through something other than the Internet, email, or network ports.

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.

The TOP 20 malicious objects detected on user computers

In 2014, Kaspersky Lab's antivirus solutions detected **1,849,949** unique malicious and potentially unwanted objects.

	Name	% of unique attacked users*
1	DangerousObject.Multi.Generic	26.04%
2	Trojan.Win32.Generic	25.32%
3	AdWare.Win32.Agent.ahbx	12.78%
4	Trojan.Win32.AutoRun.gen	8.24%
5	Adware.Win32.Amonetize.heur	7.25%
6	Virus.Win32.Sality.gen	6.69%
7	Worm.VBS.Dinihou.r	5.77%
8	AdWare.MSIL.Kranet.heur	5.46%
9	AdWare.Win32.Yotoon.heur	4.67%
10	Worm.Win32.Debris.a	4.05%
11	AdWare.Win32.BetterSurf.b	3.97%
12	Trojan.Win32.Starter.lgb	3.69%
13	Exploit.Java.Generic	3.66%
14	Trojan.Script.Generic	3.52%
15	Virus.Win32.Nimnul.a	2.80%
16	Trojan-Dropper.Win32.Agent.jkcd	2.78%
17	Worm.Script.Generic	2.61%
18	AdWare.Win32.Agent.aljt	2.53%

	Name	% of unique attacked users*
19	AdWare.Win32.Kranet.heur	2.52%
20	Trojan.WinLNK.Runner.ea	2.49%

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.

** The proportion of individual users on whose computers the antivirus module detected these objects 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 1st place (26.04%). 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 includes the information about the object. In fact, this is how the latest malware is detected.

The notorious worm Net-Worm.Win32.Kido dropped out of the TOP 20. In general the proportion of viruses continues to decrease: for example, last year Virus.Win32.Sality.gen affected **13.4%** of users while in 2014 – only **6.69%**.

Both this rating and the rating of web detections show that advertising programs are becoming more common. In 2014, the number of users who encountered adware doubled from the previous year and reached **25,406,107**. At the same time advertising programs are becoming both more intrusive and more dangerous. Some of them "cross the border" into the category of potentially unwanted programs and are assigned a "harsher" verdict. For example, Trojan-Dropper.Win32.Agent.jkcd (16th place), in addition to displaying ads and changing search results, can download malware on the computer.

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 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.

The TOP 20 countries by the level of infection

	Country*	%**
1	Vietnam	69.58%
2	Mongolia	64.24%

	Country*	**%****
3	Nepal	61.03%
4	Bangladesh	60.54%
5	Yemen	59.51%
6	Algeria	58.84%
7	Iraq	57.62%
8	Laos	56.32%
9	India	56.05%
10	Cambodia	55.98%
11	Afghanistan	55.69%
12	Egypt	54.54%
13	Saudi Arabia	54.37%
14	Kazakhstan	54.27%
15	Pakistan	54.00%
16	Syria	53.91%
17	Soudan	53.88%
18	Sri Lanka	53.77%
19	Myanma	53.34%
20	Turkey	52.94%

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.

** When calculating, we excluded countries where there are fewer than 10,000 Kaspersky Lab users.*

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

The TOP 4 countries for risk of local infection remained largely unchanged from the previous year: Vietnam was in 1st position; Mongolia and Bangladesh changed places – Bangladesh moved down from 2nd to 4th position while Mongolia climbed from 4th to 2nd place.

Djibouti, Maldives, Mauritania, Indonesia, Rwanda and Angola left the TOP 20. The newcomers were Yemen, Saudi Arabia, Kazakhstan, Syria, Myanmar and Turkey.

Within the TOP 20 countries at least one malicious object was found on an average of **58.7%** of computers, hard drives or removable media belonging to KSN users. The 2013 figure was **60.1%**.

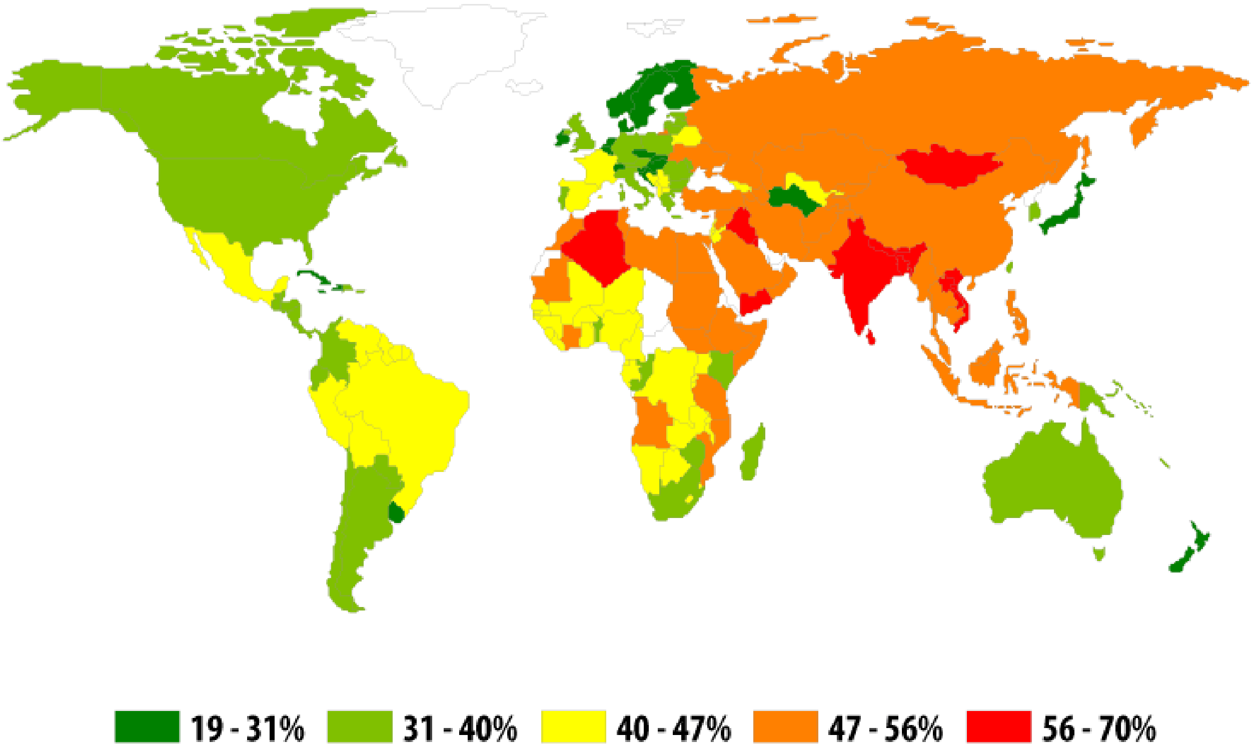
Countries can be divided into four risk categories for local threats.

1. Maximum risk (over 60%): four countries including Vietnam (69.6%), Mongolia (64.2%), Nepal (61.0%) and Bangladesh (60.5%).

2. High risk (41-60%): 83 countries including India (56.0%), Kazakhstan (54.3%), Turkey (52.9%), Russia (52.0%), China (49.7%), Brazil (46.5%), Belarus (45.3%), Mexico (41.6%), the Philippines (48.4%).

3. Moderate local infection rate (21-40.99%): 70 countries including Spain (40.9%), France (40.3%), Poland (39.5%), Lithuania (39.1%), Greece (37.8%), Portugal (37.7%), Korea (37.4%), Argentina (37.2%), Italy (36.6%), Austria (36.5%), Australia (35.3%), Canada (34.8%), Romania (34. 5%), the US (34.4%), the UK (33.8%), Switzerland (30.8%), Hong Kong (30.4%), Ireland (29.7%), Uruguay (27.8%), the Netherlands (26.4%), Norway (25.1%), Singapore (23.5%), Japan (22.9%), Sweden (23%), Denmark (21.3%)

4. Low local infection rate (0-20.99%): 3 countries including Finland (20%), Cuba (19.1%) and Seychelles (19%).



© Kaspersky Lab

The 10 safest countries were:

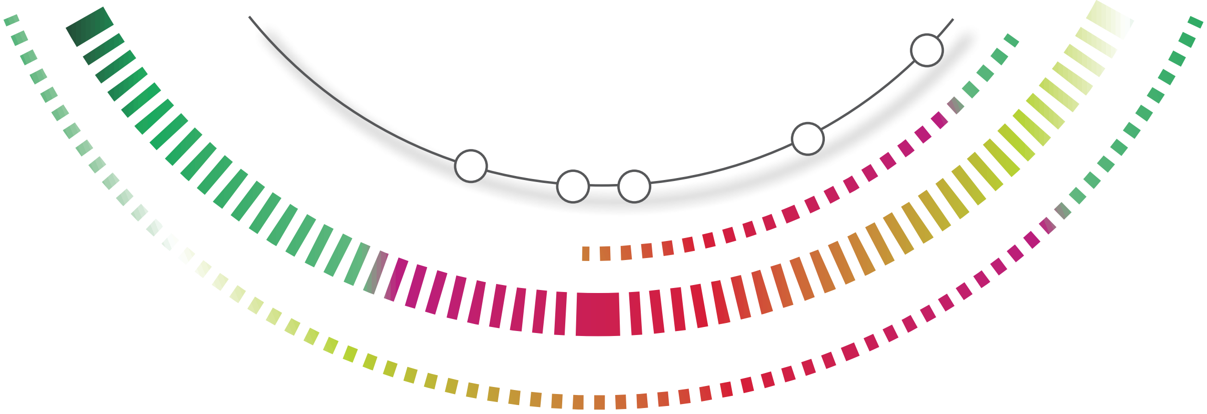
	Country	%*
1	Seychelles	19.03%
2	Cuba	19.08%
3	Finland	20.03%
4	Denmark	21.34%
5	Japan	22.89%

	Country	%*
6	Sweden	22.98%
7	Czech Republic	23.13%
8	Singapore	23.54%
9	Martinique	25.04%
10	Norway	25.13%

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

In 2014, three new countries appeared in this TOP 10 — Martinique, Singapore and Sweden. Slovakia, Slovenia and Malta dropped out of the rating.

On average, **23%** of user machines were attacked at least once during the year. This is 4.2 percentage points more than last year.



KEY EVENTS THAT HAVE DEFINED THE THREAT LANDSCAPE IN 2014

The end of the year is traditionally a time for reflection – for taking stock of our lives before considering what lies ahead. We'd like to offer our customary retrospective of the key events that shaped the threat landscape in 2014.

David Emm

1

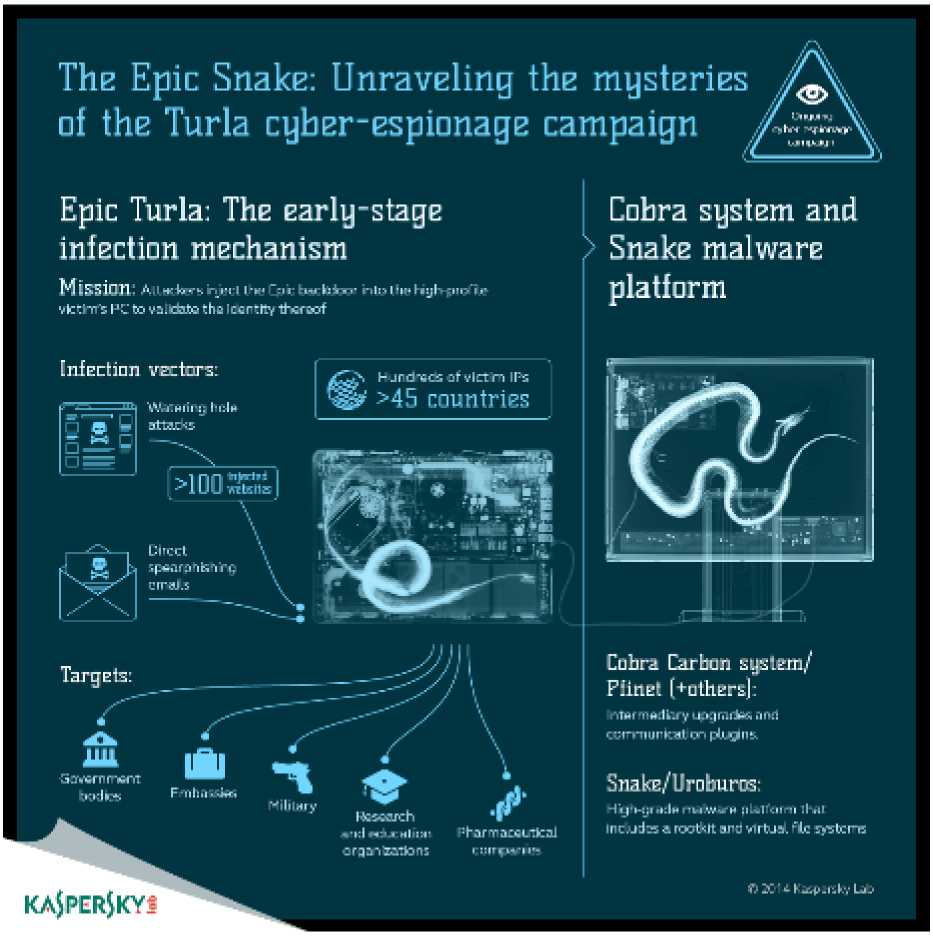
TARGETED ATTACKS AND MALWARE CAMPAIGNS

Targeted attacks are now an established part of the threat landscape, so it's no surprise to see them feature in our yearly review.

The complex cyber-espionage campaign called 'Careto' or 'The Mask' (Careto is Spanish slang for 'ugly face' or 'mask') was designed to steal sensitive data from specific organizations. The victims of the attack included government agencies, embassies, energy companies, research institutions, private equity firms and activists from 31 countries around the world. Careto included a sophisticated backdoor Trojan capable of intercepting all communication channels and of harvesting all kinds of data from infected computers – including encryption keys, VPN configurations, SSH keys, RDP files and some unknown file types that could be related to bespoke military/government-level encryption tools. The code was highly modular, allowing the attackers to add new functionality at will. There are versions of the backdoor for Windows and Mac OS X and we also found references in some modules indicating that there might be versions for Linux, iOS and Android. As with any sophisticated campaign of this sort, attribution is difficult. Use of the Spanish language in the code doesn't help, since Spanish is spoken in many parts of the world. Also, it's possible that its use is an intentional piece of misdirection. However, the very high degree of professionalism of the group behind this attack is unusual for cybercriminal groups – one indicator that Careto could be a state-sponsored campaign. Like previous targeted attack campaigns, the roots of Careto stretch back well before the threat first came to light: we believe that the attackers have been active since 2007.

Early in March there was widespread discussion among security researchers about a cyber-espionage campaign called ‘Epic Turla’. Researchers at G DATA believed the malware may have been created by Russian special services; while research carried out by BAE Systems linked it to malware identified as ‘Agent.btz’ that dates back to 2007 and was used in 2008 to infect the local networks of US military operations in the Middle East. Our initial analysis of Epic Turla focused on the malware’s use of USB flash drives to store stolen data that can’t be sent directly over the Internet to the attackers’ Command-and-Control (C2) server. The worm writes a file called ‘thumb.dd’ to all USB flash drives connected to an infected computer. If the flash drive is subsequently inserted into another computer, the ‘thumb.dd’ file is copied to the new computer. Epic Turla isn’t the only malware that is aware of ‘thumb.dd’. This is one of the files in the ‘USB Stealer module’ in Red October. Looking back further, Gauss and miniFlame were aware of ‘thumb.dd and looked for the file on USB flash drives. You can find a chart showing the points of comparison here. We think it’s likely that there are tens of thousands of USB flash drives around the world containing files called ‘thumb.dd’ created by this malware.

In our subsequent analysis of Epic Turla we explained how the attackers use social engineering to spread the malware and highlighted the overall structure of the campaign. The attackers use spear-phishing emails to trick their victims into installing a backdoor on their computer. Some of these include zero-day exploits – one affecting Adobe Acrobat Reader and the other a privilege escalation vulnerability in Windows XP and Windows Server 2003. They also use watering-hole attacks that deploy a Java exploit, Adobe Flash exploits and Internet Explorer exploits, or trick victims into running fake 'Flash Player' malware installers. Depending on the IP address of the victim, the attackers serve Java or browser exploits, signed fake Adobe Flash Player software or a fake version of Microsoft Security Essentials. Unsurprisingly, the choice of web sites reflects the specific interests of the attackers (as well as the interests of the victims). However, our analysis showed that the Epic Turla backdoor is just the first stage of the infection. It is used to deploy a more sophisticated backdoor known as the 'Cobra/Carbon system' (named 'Pfinet' by some anti-malware products). The unique knowledge to operate these two backdoors indicates a clear and direct connection between them: one is used to gain a foothold and validate the high-profile victim. If the victim proves to be of interest to the attackers, the compromised computer is upgraded to the full Carbon system. You can find an overview of the Epic Turla campaign here:



The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign

Epic Turla: The early-stage infection mechanism

Mission: Attackers inject the Epic backdoor into the high-profile victim's PC to validate the identity thereof

Cobra system and Snake malware platform

Cobra Carbon system/ Pfinet (+others): Intermediary upgrades and communication plugins.

Snake/Uroburos: High-grade malware platform that includes a rootkit and virtual file systems

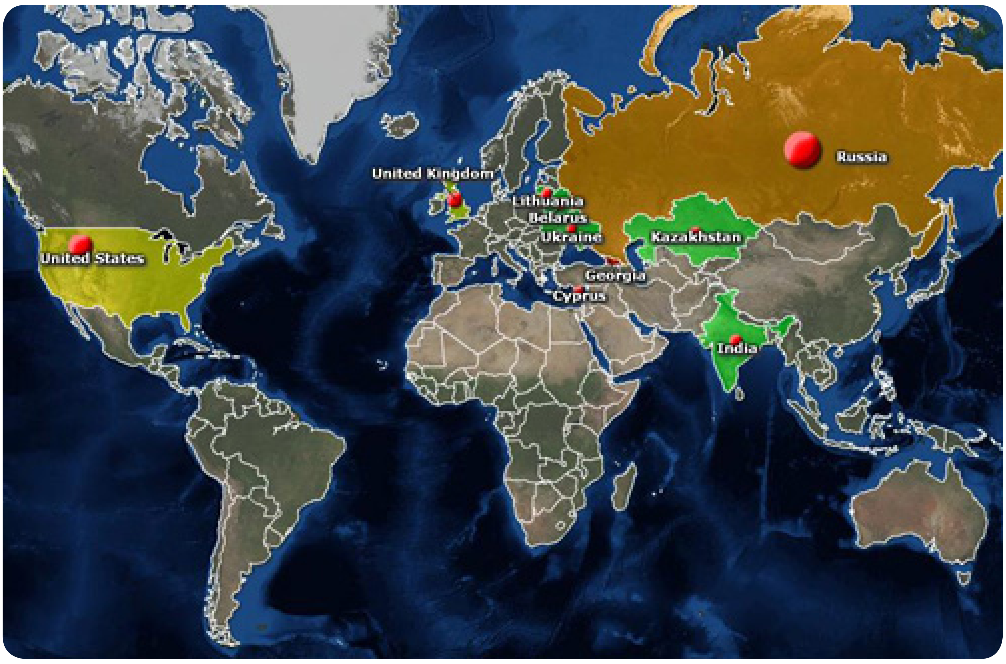
© 2014 Kaspersky Lab

In June we reported on our research into an attack on the clients of a large European bank that resulted in the theft of half a million euros in just one week. We named this 'Luuuk', after the path in the administration panel used in the C2 server. Although we were unable to obtain the malware used to infect the victims, we believe the criminals used a banking Trojan that performed 'Man-in-the-Browser' operations to steal the victims' credentials through a malicious web injection. Based on the information available in some of the log files, the malware stole usernames, passwords and one-time passcodes (OTP) in real time. The attackers used the stolen credentials to check the victim's account balance and perform malicious transactions automatically, probably operating in the background of a legitimate banking session. The stolen money was then transferred automatically to pre-defined money mule accounts. The classification of pre-defined money mules used by the attackers was very interesting. There were four different money mule groups, each defined by the amount of money the mules in the group could accept – probably a reflection of the level of trust between them. We identified 190 victims in total, most of them located in Italy and Turkey. The sums stolen from each victim ranged from €1,700 to €39,000; and amounted to €500,000.

Although the attackers removed all sensitive components soon after our investigation started, we believe that this represents a change of infrastructure rather than a complete shutdown of the operation. The cybercriminals behind the campaign are highly professional and very active. They have also shown proactive operational security activities, changing tactics and removing traces when discovered. The investigation into this campaign, which we reported to the bank concerned and to the appropriate law enforcement agencies, is ongoing.

The end of June saw the re-activation of a targeted attack campaign from early 2013, called 'MiniDuke'. The original campaign stood out for several reasons. It included a custom backdoor written in the 'old school' Assembler programming language. The attack was managed using an unusual command-and-control (C2) infrastructure: it made use of multiple redundancy paths, including Twitter accounts. The developers transferred their updated executables hidden inside GIF files.

Targets of the new operation, known as 'CosmicDuke', or 'TinyBaron', include government, diplomatic, energy, military and telecom operators. But unusually the list of victims also includes those involved in the trafficking and reselling of illegal substances, including steroids and hormones. It's not clear why: maybe the customizable backdoor was made available as so-called 'legal spyware', or it was available in the underground market and was purchased by various rivals in the pharmaceutical business to spy on each other.



Victim geography (Miniduke and CosmicDuke)

The malware spoofs popular applications designed to run in the background - including file information, icons and even file size. The backdoor itself is compiled using 'BotGenStudio' - a customizable framework that allows the attackers to enable and disable components when the bot is constructed. The malware not only steals files with specific extensions, but also harvests passwords, history, network information, address books, information displayed on the screen (screenshots are made every five minutes) and other sensitive data. Each victim is assigned a unique ID, making it possible to push specific updates to individual victims.

The malware is protected with a custom obfuscated loader which heavily consumes CPU resources for 3-5 minutes before passing execution to the payload. This makes it hard to analyze. But it also drains the resources needed by security software to emulate the malware's execution. On top of its own obfuscator, the malware makes heavy use of encryption and compression based on the RC4 and LZRW algorithms. They are implemented slightly differently to the standard versions - we believe that this is done deliberately to mislead researchers. The internal configuration of the malware is encrypted, compressed and serialized as a complicated registry-like structure, which has various record types including strings, integers and internal references. Stolen data uploaded to the C2 server is split into small chunks (of around 3KB), which are compressed, encrypted and placed in a container to be uploaded to the server. If it's a large file, it may be placed into several hundred different containers that are all uploaded independently. It's likely that these data chunks are parsed, decrypted, unpacked, extracted and reassembled on the attacker's side. While this method might add an overhead, the layers of additional processing ensure that very few researchers will get to the original data. This method also offers increased reliability against network errors.

In July we published an in-depth analysis of a targeted attack campaign that we dubbed 'Crouching Yeti' – also known as 'Energetic Bear', because researchers from CrowdStrike had suggested that the attackers were located in Russia: we don't think there's enough evidence to confirm this one way or the other. This campaign, active since late 2010, has so far targeted the following sectors: industrial/machinery, manufacturing, pharmaceutical, construction, education and information technology. So far there have been more than 2,800 victims worldwide, and we have been able to identify 101 different victim organizations – mostly in the United States, Spain, Japan, Germany, France, Italy, Turkey, Ireland, Poland and China.

The attackers behind Crouching Yeti use various types of malware (all designed to infect systems running Windows) to infiltrate their victims, extend their reach within the target organizations and steal confidential data, including intellectual property and other strategic information. The malware used includes special modules to collect data from specific industrial IT environments. Infected computers connect to a large network of hacked web sites that host malware modules, hold information about victims and send commands to infected systems. The attackers use three methods to infect their victims. These include a legitimate software installer re-packaged to include a malicious DLL file; spear-phishing e-mails; and watering-hole attacks.

Technology is now an integral part of our lives, so it's hardly surprising to see a cyber-dimension to conflicts around the world. This is especially true of the Middle East, where geo-political conflicts have intensified in recent years. In August we reported on the increase in malware activity in Syria from early 2013. The victims of these attacks are not only located in Syria: the malware has also been seen in Turkey, Saudi Arabia, Lebanon, Palestine, the United Arab Emirates, Israel, Morocco, France and the United States. We were able to track the C2 servers of the attackers to IP addresses in Syria, Russia, Lebanon, the United States and Brazil. In total, we found 110 files, 20 domains and 47 IP addresses associated with the attacks.

It’s clear that the groups involved in the attacks are well organized. So far the attackers have made use of established malware tools rather than developing their own (although they use a variety of obfuscation methods to bypass simple signature-based detection). However, we think it’s likely that the number and sophistication of malware used in the region is likely to increase.

In November we published our analysis of the ‘Darkhotel’ APT, a campaign that has been operating for almost a decade, targeting thousands of victims across the globe. 90 per cent of the infections we have seen are in Japan, Taiwan, China, Russia and Hong Kong, but we have also seen infections in Germany, the USA, Indonesia, India, and Ireland.

The campaign employs varying degrees of targeting. First, they use spear-phishing e-mails and zero-day exploits to infiltrate organizations from different sectors, including Defense Industrial Base (DIB), government and Non-Governmental Organizations (NGOs). Second, they spread malware indiscriminately via Japanese P2P (peer-to-peer) file-sharing sites. Third, they specifically target business executives who are traveling overseas and staying at hotels in a number of countries: using a two-step infection process, the attackers first identify their victims and then download further malware to the computers of more significant targets, designed to steal confidential data from the infected computer.

2

OUR HOMES AND OTHER VULNERABILITIES

Exploiting unpatched vulnerabilities remains one of the key mechanisms used by cybercriminals to install malicious code on victims' computers. This relies on the existence of vulnerabilities in widely-used software and the failure of individuals or businesses to patch applications.

This year vulnerabilities were discovered in two widely-used open source protocols, known as 'Heartbleed' and 'Shellshock' respectively. Heartbleed, a flaw in the OpenSSL encryption protocol, lets an attacker read the contents of the memory, and intercept personal data, on systems using vulnerable versions of the protocol. OpenSSL is widely-used to secure Internet-based communications, including web, e-mail, instant messaging and Virtual Private Networks (VPN), so the potential impact of this vulnerability was huge. As often happens when there's a risk that personal data might have been exposed, there was a rush to change passwords. Of course, this could only be effective once an online provider had taken steps to patch OpenSSL and thereby secure their systems – otherwise any new password would be just at risk from attackers trying to exploit the vulnerability. We offered some perspectives on the impact of the flaw two months after its disclosure.

In September, the information security world faced a red alert following the discovery of the Shellshock vulnerability (also known as 'Bash'). The flaw allows an attacker to remotely attach a malicious file to a variable that is executed when the Bash command interpreter is invoked (Bash is the default shell on Linux and Mac OS X systems). The high impact of this vulnerability, coupled with the ease with which it could be exploited, caused considerable concern. Many people compared it to Heartbleed. However, unlike Heartbleed, Shellshock provided full system control – not just the ability to steal data from the memory. It didn't take long for attackers to try and take advantage of the vulnerability – we discussed some early examples soon after it was discovered. In most cases attackers remotely attacked web servers hosting CGI (Common Gateway Interface) scripts that have been written in Bash or pass values to shell scripts. However, it remains possible that the vulnerability could have an impact on a Windows-based infrastructure. Unfortunately, the problem wasn't confined only to web servers. Bash is widely used in the firmware of devices that now take for granted in our everyday lives. This includes routers, home appliances and wireless access points. Some of these devices can be difficult or impossible to patch.

The Internet is becoming woven into the fabric of our lives – literally, in some cases, as connectivity is embedded into everyday objects. This trend, known as the 'Internet of Things', has attracted more and more attention. It can seem very futuristic, but the Internet of Things is actually closer than you may think. The modern home today is likely to have a handful of devices connected to the local network that aren't traditional computers – devices such as a smart TV, a printer, a games console, a network storage device or some kind of media player/satellite receiver.

One of our security researchers investigated his own home, to determine whether it was really cyber-secure. He looked at several pieces of household kit, including network-attached storage (NAS) devices, smart TV, router and satellite receiver, to see if they were vulnerable to attack. The results were striking. He found 14 vulnerabilities in the network-attached storage devices, one in the smart TV and several potentially hidden remote control functions in the router. You can read the full details here. It's important that we all understand the potential risks associated with using network devices – this applies to individuals and businesses alike. We also need to understand that our information is not secure just because we use strong passwords or run software to protect against malicious code. There are many things over which we have no control, and to some degree we are in the hands of software and hardware vendors. For example, not all devices include automated update checks – sometimes consumers are required to download and install new firmware. This is not always an easy task. Worse still, it's not always possible to update a device (most devices investigated during this research had been discontinued more than a year before).

3

THE CONTINUING EXPONENTIAL GROWTH OF MOBILE MALWARE

We have seen dramatic growth in the numbers of mobile malware in recent years. In the period from 2004-13 we analyzed almost 200,000 mobile malware code samples. In 2014 alone we analyzed a further 295,539 samples. However, this doesn't give the whole picture. These code samples are re-used and re-packaged: in 2014 we saw 4,643,582 mobile malware installation packs (on top of the 10,000,000 installation packs we had seen in the period 2004-13). The number of mobile malware attacks per month increased tenfold – from 69,000 per month in August 2013 to 644,000 in March 2014 (see Mobile Cyber Threats, Kaspersky Lab and INTERPOL Joint Report, October 2014).

53 per cent of all mobile malware detections are now related to malware capable of stealing money. One of the more notable examples is Spveng, designed to steal money from customers of three of Russia's biggest banks. The Trojan waits until a customer opens an online banking app and replaces it with its own, to try and obtain the customer's login details. It also tries to steal credit card data by displaying its own window over the Google Play app and asking for card details. Another is Waller which, in addition to behaving like a typical SMS Trojan, steals money from QIWI wallets on infected devices.

Cybercriminals have also diversified their efforts to make money from their victims, using methods that have been well-established on desktops and laptops. This includes ransomware Trojans. Fake anti-virus apps are another example of an established approach now being applied to mobile devices. Finally, this year saw the appearance of the first Trojan that is managed through a C2 server hosted in the Tor network. The Torec backdoor is a modification of the commonly-used Tor client, Orbot. The benefit, of course, is that the C2 server can't be shut down.

Until recently, nearly all malware targeting iOS was designed to exploit 'jailbroken' devices.

However, the recent appearance of the 'WireLurker' malware has shown that iOS is not immune from attack.

Mobile devices are now integrated into the fabric of our lives, so it's hardly surprising that the development of mobile malware is underpinned by a cybercrime business that includes malware writers, testers, app designers, web developers and botnet managers.

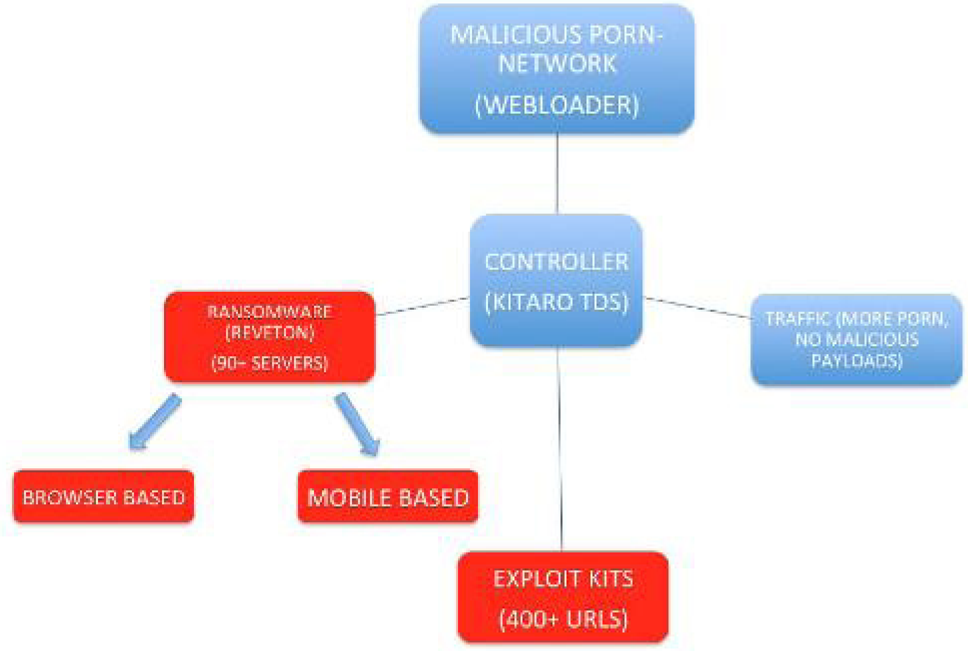
4

YOUR MONEY OR YOUR FILE(S)

The number of ransomware programs has been growing in recent years. Some simply block access to the victim's computer and demand a ransom payment in order to restore normal access. But many go further than this, encrypting data on the computer. One recent example is 'ZeroLocker'. ZeroLocker encrypts nearly all the files on the victim's computer and adds the extension '.encrypt' to encrypted files (although it doesn't encrypt files located in directories containing the words 'Windows', 'WINDOWS', 'Program Files', 'ZeroLocker' or 'Destroy' and doesn't encrypt files larger than 20MB in size). The Trojan uses a 160-bit AES key to encrypt files. Once the files are encrypted, it runs the 'cipher.exe' utility to remove all unused data from the drive. Both these things make file recovery very difficult. The cybercriminals behind ZeroLocker demand an initial $300 worth of Bitcoins to decrypt the file. If the victim does not pay promptly the fee increases to $500 and $1,000 as time goes on.

Another ransomware program that we analyzed this year is Onion. Not only does this Trojan use the Tor network to hide its C2 servers, but it also supports full interaction with Tor without any input from the victim. Other programs like this communicate with the Tor network by launching (sometimes by injecting code into other processes) the legitimate 'tor.exe' file. By contrast Onion implements this communication as part of the malware code itself. Onion also uses an unorthodox cryptographic algorithm that makes file decryption impossible, even if traffic between the Trojan and the C2 server is intercepted. This Trojan not only uses asymmetric encryption, it also uses a cryptographic protocol known as ECDH (Elliptic Curve Diffie-Hellman). This makes decryption impossible without the master private key – which never leaves the cybercriminals' controlled server.

This year the use of ransomware programs has been extended to devices running Android. The first version of Svpeng, for example, discovered early in 2014, blocks the phone, claiming that the victim was viewing child pornography and demanding a 'fine' of $500 to unlock the phone. A subsequent modification of this malware, discovered in June 2014, completely blocks the device, so that it can only be turned off by pressing down the 'Off' button for a long time – and the Trojan loads again as soon as the device has been switched on again. This version was aimed mainly at victims in the US, but we also saw victims in the UK, Switzerland, Germany, India and Russia. This version demands a payment of $200 to unblock the phone, payment to be made using MoneyPak vouchers. The ransom demand screen displays a photograph of the victim, taken using the frontal camera. Another Trojan, called 'Koler', discovered in May 2014, uses the same approach – blocking access to the device and demanding a ransom payment of between $100 and $300 to unblock the phone. Like Svpeng, this Trojan displays a message claiming to be from the police – it targets victims in more than 30 countries around the world, using local 'police' messages.


MALICIOUS PORN-NETWORK (WEBLOADER)
CONTROLLER (KITARO TDS)
RANSOMWARE (REVETON) (90+ SERVERS)
TRAFFIC (MORE PORN, NO MALICIOUS PAYLOADS)
BROWSER BASED
MOBILE BASED
EXPLOIT KITS (400+ URLS)

Koler's distribution infrastructure

The first Android Trojan to encrypt data, called 'Pletor', appeared in May 2014. This Trojan uses the AES encryption algorithm to encrypt the contents of the phone's memory card and then displays a ransom demand on the screen, payable using the victim's QIWI Visa wallet, MoneXy or standard transfer of money to a telephone number. This Trojan mainly targets victims in Russia and Ukraine (although we have seen victims in other former Soviet republics) and demands the equivalent of around $300 in rubles or hryvnia.

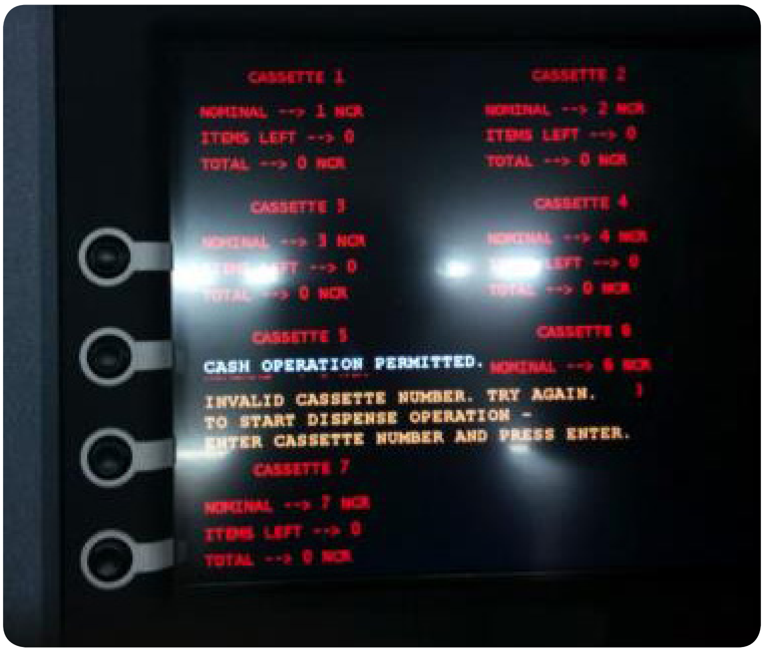
Ransomware operations rely on their victims paying up. Don't do it! Instead, make regular backups of your data. That way, if you ever fall victim to a ransomware program (or a hardware problem that stops you accessing your files) you will not lose any of your data.

5

CHA-CHING!
USING MALWARE TO GET MONEY FROM ATMS

Malware for ATMs is not new. The first malware of this kind, called 'Skimer', was found in 2009 – this targeted ATMs in Eastern Europe running a Windows-based operating system. This used undocumented functions to print details of cards inserted in the infected machine and to open cassettes using a master card command. We saw further ATM malware in Brazil, in 2010 ('SPSniffer'): this collected PIN numbers in outdated ATMs using PIN pads that weren't using strong cryptographic protection. Then last year we saw a further family of ATM malware ('Atmer'), designed to steal money from ATMs in Mexico.

This year, at the request of a financial institution, we carried out a forensic investigation into a new attack on ATMs in Asia, Europe and Latin America. The operation was in two stages. The cybercriminals gain physical access to the ATMs and use a bootable CD to install the malware, called 'Tyupkin'; then they reboot the machine to load the malware, putting them in control of the ATM. The malware then runs in an infinite loop, waiting for a command.



```
     CASSETTE 1                      CASSETTE 2
NOMINAL --> 1 NCR               NOMINAL --> 2 NCR
ITEMS LEFT --> 0                ITEMS LEFT --> 0
TOTAL --> 0 NCR                 TOTAL --> 0 NCR

     CASSETTE 3                      CASSETTE 4
NOMINAL --> 3 NCR               NOMINAL --> 4 NCR
ITEMS LEFT --> 0                ITEMS LEFT --> 0
TOTAL --> 0 NCR                 TOTAL --> 0 NCR

     CASSETTE 5                      CASSETTE 6
CASH OPERATION PERMITTED.       NOMINAL --> 6 NCR

INVALID CASSETTE NUMBER. TRY AGAIN.
TO START DISPENSE OPERATION -
ENTER CASSETTE NUMBER AND PRESS ENTER.
     CASSETTE 7
NOMINAL --> 7 NCR
ITEMS LEFT --> 0
TOTAL --> 0 NCR
```

To make the scam less obvious, the malware only accepts commands at specific times on Sunday and Monday nights. The attackers can then enter a combination of digits on the ATM keyboard, make a call to the malware operators, enter a further set of numbers and then collect the cash dispensed by the ATM.

Video Footage obtained from security cameras at the infected ATMs showed the methodology used to access cash from the machines. A unique digit combination key based on random numbers is freshly generated for every session: this ensures that no one outside the gang can accidentally profit from the fraud. Then the malicious operator receives instructions by phone from another member of the gang who knows the algorithm and is able to generate a session key based on the number shown: this ensures that the mules collecting the cash do not try to go it alone. When the correct key is entered, the ATM shows how much money is available in each cash cassette, inviting the operator to choose which cassette to rob. Then it dispenses 40 bank notes at a time from the chosen cassette.

The upswing in ATM attacks in recent years is a natural evolution from the more well-established method of using physical skimmers to capture data from cards used in ATMs that have been tampered with. Unfortunately, many ATMs run operating systems with known security weaknesses. This makes physical security even more important; and we would urge all banks to review the physical security of their ATMs.

6

WINDOWS XP: FORGOTTEN BUT NOT GONE?

Support for Windows XP ended on 8 April: this means no new security updates, no security hotfixes, free or paid assisted support options or online technical content updates. Sadly, there are still a lot of people running Windows XP – our data suggests that Windows XP accounts for around 18 per cent of infections. This is a lot of people wide open to attack now that security patches have dried up. Effectively, every vulnerability discovered since April is a zero-day vulnerability – that is, one for which there is no chance of a patch. This problem will be compounded as application vendors stop developing updates for Windows XP. Every unpatched application will become yet another potential point of compromise, further increasing the potential attack surface. In fact, this process has already started: the latest version of Java no longer supports Windows XP.

It might seem that the simple and obvious solution is to upgrade to a newer operating system. But even though Microsoft gave plenty of notice about the end of support, it's not difficult to see why migration to a new operating system might be difficult for some businesses. On top of the cost of switching, it may also mean investing in new hardware and even trying to replace a bespoke application developed specifically for the company – one that will not run on a later operating system. So it's no surprise see some organizations paying for continued XP support.

Of course, an anti-virus product will provide protection. But this only holds good if by 'anti-virus' we mean a comprehensive Internet security product that makes use of proactive technology to defend against new, unknown threats – in particular, functionality to prevent the use of exploits. A basic anti-virus product, based largely on signature-based scanning for known malware, is insufficient. Remember too that, as times goes by, security vendors will implement new protection technologies that may well not be Windows XP-compatible.

Anyone still running Windows XP should see this as a stop-gap, while they finalize a migration strategy. Malware writers will undoubtedly target Windows XP while significant numbers of people continue to run it, since an unpatched operating system will offer them a much bigger window of opportunity. Any Windows XP-based computer on a network offers a weak point that can be exploited in a targeted attack on the company – if compromised this will become a stepping-stone into the wider network.

There's no question that switching to a newer operating system is inconvenient and costly - for individuals and businesses. But the potential risk of using an increasingly insecure operating system is likely to outweigh the inconvenience and cost.

7

BENEATH THE LAYERS OF THE ONION

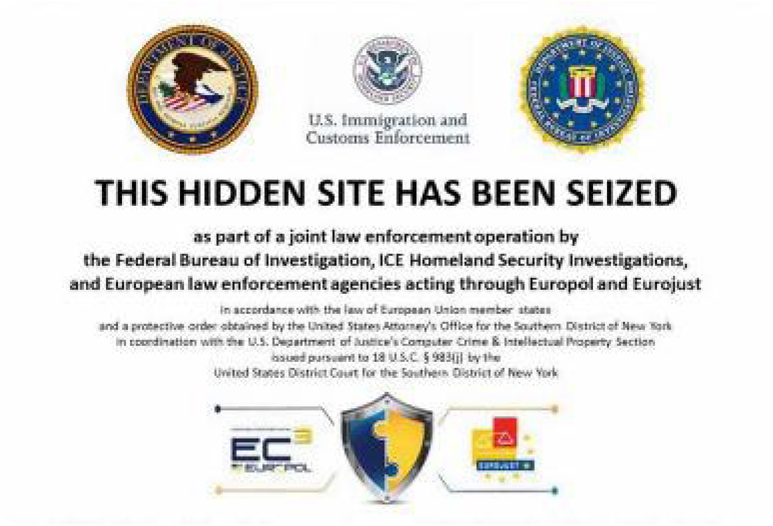
Tor (short for The Onion Router) is software designed to allow someone to remain anonymous when accessing the Internet. It has been around for some time, but for many years was used mainly by experts and enthusiasts. However, use of the Tor network has spiked this year, in large part because of growing concerns about privacy. Tor has become a helpful solution for those who, for any reason, fear surveillance and the leakage of confidential information. However, our investigations highlighted the fact that Tor is also attractive for cybercriminals, who value the anonymity it offers.

We started seeing cybercriminals actively using Tor to host their malicious infrastructure in 2013. In addition to malware, we found many related resources, including C2 servers, administration panels and more. By hosting their servers in the Tor network, cybercriminals make them harder to identify, blacklist and eliminate. There's also a Tor-based underground marketplace, including the buying and selling of malware and stolen personal data – typically paid for using the crypto-currency Bitcoin, enabling cybercriminals to remain untraceable. Tor allows cybercriminals to conceal the operation of the malware they use, to trade in cybercrime services and launder their illegal profits.

In July we published our analysis of a ransomware Trojan, called 'Onion' that broke new ground in its use of Tor.

Developers of Android-based malware have also started to use Tor. The Torec Trojan, a malware variation of the popular Orbot Tor client, uses a domain in the .onion pseudo zone as a C2 server. Some modifications of the Pletor ransomware Trojan also use the Tor network to communicate with the cybercriminals managing the scam.

Cybercriminals can't always operate with impunity, despite using Tor, as demonstrated by the recent global law enforcement operation against a number of Tor-based cybercrime services ('Operation Onymous').



U.S. Immigration and Customs Enforcement

THIS HIDDEN SITE HAS BEEN SEIZED

as part of a joint law enforcement operation by
the Federal Bureau of Investigation, ICE Homeland Security Investigations,
and European law enforcement agencies acting through Europol and Eurojust

In accordance with the law of European Union member states
and a protective order obtained by the United States Attorney's Office for the Southern District of New York
in coordination with the U.S. Department of Justice's Computer Crime & Intellectual Property Section
issued pursuant to 18 U.S.C. § 983(j) by the
United States District Court for the Southern District of New York

This begs the question of how the police agencies involved were able to compromise a supposedly ‘impenetrable’ network – because, in theory at least, there’s no way of knowing the physical location of a web server behind a hidden service that someone visits. However, there are ways to compromise a hidden service that don’t involve attacking the Tor architecture itself, as we discussed here. A Tor-based service can only remain secure if it’s properly configured, if it’s free from vulnerabilities or configuration errors and the web application doesn’t have any flaws.

8

THE GOOD, THE BAD AND THE UGLY

Unfortunately, software isn't neatly divided between good and bad programs. There's always the risk that software developed for legitimate purposes might be misused by cybercriminals. At the Kaspersky Security Analyst Summit 2014 in February we outlined how improper implementation of anti-theft technologies residing in the firmware of commonly used laptops and some desktop computers could become a powerful weapon in the hands of cybercriminals. Our research started when a Kaspersky Lab employee experienced repeated system process crashes on one of his personal laptops, related to instability in modules belonging to the Computrace software developed by Absolute Software. Our colleague hadn't installed the software and didn't even know it was present on the laptop. This caused us concern because, according to an Absolute Software white paper, the installation should be done by the owner of the computer or their IT service. On top of this, while most pre-installed software can be permanently removed or disabled by the owner of the computer, Computrace is designed to survive a professional system cleanup and even a hard disk replacement. Moreover, we couldn't simply dismiss this as a one-off occurrence because we found similar indications of Computrace software running on personal computers belonging to some of our researchers and some enterprise computers. As a result, we decided to carry out an in-depth analysis.

When we first looked at Computrace, we mistakenly thought it was malicious software, because it uses so many tricks that are popular in current malware. Indeed, in the past this software has been detected as malware although at present most anti-malware companies whitelist Computrace executables.

We believe that Computrace was designed with good intentions. However, our research shows that vulnerabilities in the software could allow cybercriminals to misuse it. In our view, strong authentication and encryption must be built into such a powerful tool. We found no evidence that Computrace modules had been secretly activated on the computers we analyzed. But it's clear that there are a lot of computers with activated Computrace agents. We believe that it's the responsibility of manufacturers, and Absolute Software, to notify these people and explain how they can deactivate the software if they don't wish to use it. Otherwise, these orphaned agents will continue to run unnoticed and will provide opportunities for remote exploitation.

In June, we published the results of our research into a piece of 'legal' software called Remote Control System (RCS) developed by the Italian company HackingTeam. We discovered a feature that can be used to fingerprint its C2 servers. This allowed us to scan the entire IPv4 space and find all the IP addresses of RCS C2 servers across the globe. We found 326 in total, the greatest number of them located in the US, Kazakhstan and Ecuador. Several IPs were identified as 'government'-related, based on their WHOIS information. Of course, we can't be sure that the servers located in a specific country are being used by law enforcement agencies in that country, but this would make sense: after all, it would avoid cross-border legal problems and avoid the risk of servers being seized by others. We also found a number of mobile malware modules coming from HackingTeam, for Android, iOS, Windows Mobile and BlackBerry. They are all controlled using the same configuration type – a good indication that they are related and belong to the same product family. Unsurprisingly, we were particularly interested in those relating to Android and iOS, because of the popularity of those platforms.

The modules are installed using infectors – special executables for either Windows or Mac OS that run on already-infected computers. The iOS module supports only 'jailbroken' devices. This does limit its ability to spread, but the method of infection used by RCS means that an attacker can run a jailbreaking tool (such as Evasi0n) from the infected computer to which the phone is connected – as long as the device isn't locked. The iOS module allows an attacker to access data on the device (including e-mail, contacts, call history, cached web pages), to secretly activate the microphone and to take regular camera shots. This gives complete control over the whole environment in and around a victim's computer.

The Android module is protected by the DexGuard optimizer/obfuscator, so it was difficult to analyze. But we were able to determine that it matches the functionality of the iOS module, plus offering support for hijacking information from the following applications: 'com.tencent.mm', 'com,google,android,gm', 'android,calendar', 'com,facebook', 'jp,naver,line,android' and 'com,google.android,talk'.

This new data highlighted the sophistication of such surveillance tools. Our policy in relation to such tools is very clear. We seek to detect and remediate any malware attack, regardless of its origin or purpose. For us, there's no such thing as 'right' or 'wrong' malware; and we've issued public warnings about the risks of so-called 'legal' spyware in the past. It's imperative that these surveillance tools don't fall into the wrong hands – that's why the IT security industry can't make exceptions when it comes to detecting malware.

PRIVACY AND SECURITY

The ongoing tension between privacy and security has continued to make headlines.

Among the usual steady stream of security breaches this year, it’s not really surprising that the incident that attracted most attention was the theft and subsequent publication of explicit photographs of various Hollywood celebrities. This story highlights the dual responsibility of providers and individuals in securing data stored online. It seems that the theft was made possible by a loophole in iCloud security: the ‘Find My iPhone’ interface lacked any limitation on the number of password attempts, allowing attackers to brute-force the passwords of the victims. Apple closed up this loophole soon afterwards. However, the attack would not have been possible had the victims not used weak passwords. We increasingly live our lives online. But many of us fail to consider the implications of storing personal data online. The security of a cloud service depends on the provider. The moment we entrust our data to a third-party service, we automatically lose some control over it. It’s important to cherry-pick the data we store in the cloud and decide what data is automatically moved from our devices to the cloud.

The issue of passwords is one that keeps surfacing. If we choose a password that is too easy to guess, we leave ourselves wide open to identify theft. The problem is compounded if we recycle the same password across multiple online accounts – if one account is compromised, they’re all at risk! This is why many providers, including Apple, Google and Microsoft, now offer two-factor authentication – i.e. requiring customers to enter a code generated by a hardware token, or one sent to a mobile device, in order to access a site, or at least in order to make changes to account settings. Two-factor authentication certainly enhances security – but only if it’s required, rather than just being an option.

There’s always a trade-off between security and ease of use. In an effort to strike this balance, Twitter recently launched its Digits service. Customers no longer need to create a username and password combination in order to sign in to an app. Instead, they simply enter their phone number. They receive a one-time passcode to confirm each transaction – this code is read automatically by the app. Twitter is effectively making itself a go-between, verifying the identity of the customer for the app provider. There are several benefits. Consumers no longer have to worry about creating a login and password combination to set up an account with an app provider; and they don’t need to have an e-mail address. App developers don’t need to create their own framework for verifying logins; and they won’t lose potential customers who don’t use e-mail. Twitter gets more visibility into what its customers are interested in. In addition, the fact that no passwords are stored on the app provider’s server is also a plus: a breach of an app provider’s server will not result in the loss of personal data belonging to customers. However, if someone loses their device, or if it’s stolen, the number verification will still work – and anyone with access to the device will be able to access an app in the same way as the legitimate owner. That said, it doesn’t represent a step backwards in security compared to the traditional username and password method. Currently, mobile apps don’t force a login each time an app is run anyway, so if someone steals a phone, and the owner isn’t using a PIN, passcode or fingerprint, the thief has access to everything – e-mail, social networks and apps. In other words, security is dependent on a single-point-of-failure – the PIN, passcode or fingerprint used to access the device itself.

In response to increasing concerns about privacy, the developers of the ‘pwnedlist.com’ web site created an easy to use interface where people can check to see if their e-mail addresses and passwords have been stolen and published online. This year they have made this a chargeable service.

The response of both Apple and Google to growing fears about loss of privacy was to enable default encryption of data on iOS and Android devices, something that some law enforcement agencies believe plays into the hands of cybercriminals – making it easier for them to evade detection.

10

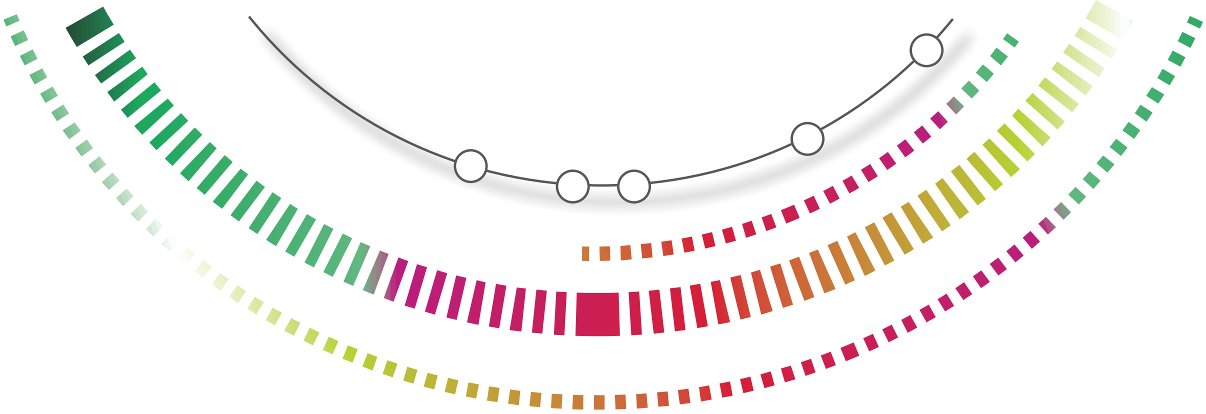
INTERNATIONAL LAW ENFORCEMENT: CO-OPERATION BRINGS RESULTS

Cybercrime has become an established part of life, on the back of the ever-increasing online activities we engage in. It's tempting to imaging that cybercriminals are able to operate with impunity, but the actions of law enforcement agencies can have a significant impact on their activities. International co-operation is particularly important, given the global nature of cybercrime. This year there have been some notable police successes.

In June 2014 an operation involving law enforcement agencies of several countries, including the UK's NCA (National Crime Agency) and the FBI, was able to take down the global network of computers responsible for managing the 'GameoverZeus' botnet. The police operation ('Operation Tovar') disrupted the communications underlying the botnet, thereby preventing the cybercriminals from controlling it. GameoverZeus was one of the largest operating botnets based on the code of the Zeus banking Trojan. In addition to infecting computers with the Zeus Trojan and stealing login credentials for online e-mail accounts, social networks, online banking and other online financial services, the botnet also distributed the 'Cryptolocker' ransomware program. The police campaign offered victims a breathing-space in which to clean their computers.

Earlier this year Kaspersky Lab contributed to an alliance of law enforcement and industry organizations, co-ordinated by the NCA, to disrupt the infrastructure behind the 'Shylock' Trojan. The Shylock banking Trojan, so-called because its code contains excerpts from Shakespeare's The Merchant of Venice, was first discovered in 2011. Like other well-known banking Trojans Shylock is a man-in-the-browser attack designed to steal banking login credentials from the computers of bank customers. The Trojan uses a pre-configured list of target banks, located in different countries around the world.

In November, Operation Onymous resulted in the take-down of dark markets running within the Tor network.



►A LOOK INTO THE APT CRYSTAL BALL

Over the past years, Kaspersky's Global Research and Analysis Team (GReAT) has shed light on some of the biggest APT campaigns, including RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/Mask and others. While studying these campaigns we have also identified a number of 0-day exploits, including the most recent CVE-2014-0546. We were also among the first to report on emerging trends in the APT world, such as cyber mercenaries who can be contracted to launch lightning attacks or more recently, attacks through unusual vectors such as hotel Wi-Fi. Over the past years, Kaspersky Lab's GReAT team has monitoring more than 60 threat actors responsible for cyber-attacks worldwide, organizations which appear to be fluent in many languages such as Russian, Chinese, German, Spanish, Arabic, Persian and others.

By closely observing these threat actors, we put together a list of what appear to be the emerging threats in the APT world. We think these will play an important role in 2015 and deserve special attention, both from an intelligence point of view but also with technologies designed to stop them.

Costin Raiu

1

THE MERGER OF CYBER-CRIME AND APT

For many years, cyber-criminal gangs focused exclusively on stealing money from end users. An explosion of credit card theft, hijacking of electronic payment accounts or online banking connections led to consumer losses in the worth hundreds of millions of dollars. Maybe this market is no longer so lucrative, or maybe the cybercriminal market is simply overcrowded, but it now seems like there is a struggle being waged for ‘survival’. And, as usual, that struggle is leading to evolution.

What to expect: In one incident we recently investigated attackers compromised an accountant’s computer and used it to initiate a large transfer with their bank. Although it might seem that this is nothing very unusual, we see a more interesting trend: **Targeted attacks directly against banks, not their users.**

In a number of incidents investigated by Kaspersky Lab experts from the Global Research and Analysis Team, several banks were breached using methods straight out of the APT playbook. Once the attackers got into the banks’ networks, they collected enough information to enable them to steal money directly from the bank in several ways:

- Remotely commanding ATMs to dispense cash.
- Performing SWIFT transfers from various customer accounts,
- Manipulating online banking systems to perform transfers in the background.

These attacks are an indication of a new trend that is embracing APT style attacks in the cybercriminal world. As usual, cybercriminals prefer to keep it simple: they now attack the banks directly because that’s where they money is. We believe this is a noteworthy trend that will become more prominent in 2015.

2

FRAGMENTATION OF BIGGER APT GROUPS

2014 saw various sources expose APT groups to the public eye. Perhaps the best-known case is the FBI indictment of five hackers on various computer crimes:

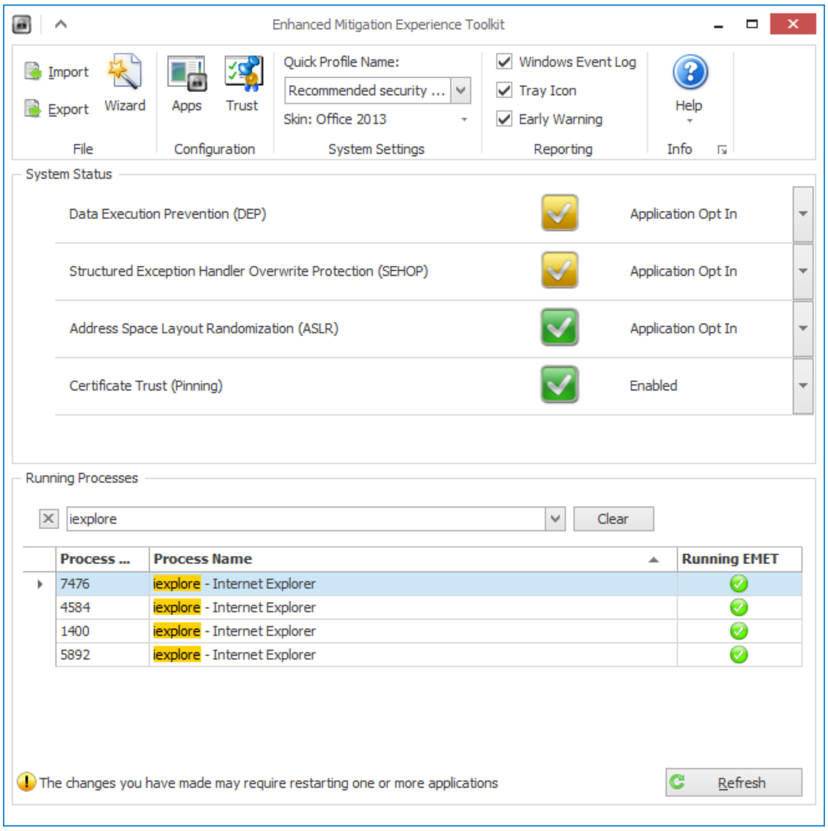
This public "naming and shaming" means we expect some of the bigger and "noisier" APT groups to shatter and break into smaller units, operating INDEPENDENTLY.

What to expect: This will result in a more widespread attack base, meaning more companies will be hit, as smaller groups diversify their attacks. At the same time, it means that bigger companies that were previously compromised by two or three major APT groups (eg. Comments Crew and Wekby) will see more varied attacks from a wider range of sources.

3

EVOLVING MALWARE TECHNIQUES

As computers become more sophisticated and powerful, operating systems also become more complex. Both Apple and Microsoft have spent a lot of time improving the security posture of their respective operating systems. Additionally, special tools such as Microsoft's EMET are now available to help thwart targeted attacks against software vulnerabilities.



Quick Profile Name: Recommended security ...

Skin: Office 2013

☑ Windows Event Log
☑ Tray Icon
☑ Early Warning

System Status

Data Execution Prevention (DEP)	✓	Application Opt In
Structured Exception Handler Overwrite Protection (SEHOP)	✓	Application Opt In
Address Space Layout Randomization (ASLR)	✓	Application Opt In
Certificate Trust (Pinning)	✓	Enabled

Running Processes

iexplore

Process ...	Process Name	Running EMET
7476	iexplore - Internet Explorer	✓
4584	iexplore - Internet Explorer	✓
1400	iexplore - Internet Explorer	✓
5892	iexplore - Internet Explorer	✓

The changes you have made may require restarting one or more applications

With Windows x64 and Apple Yosemite becoming more popular, we expect APT groups to update their toolsets with more powerful backdoors and technologies to evade security solutions.

What to expect: Today, we are already seeing APT groups constantly deploying malware for 64-bit systems, including 64-bit rookits. In 2015, we expect to see more sophisticated malware implants, enhanced evasion techniques and more use of virtual file systems (such as those from Turla and Regin) to conceal precious tools and stolen data.

While we see these increases in advanced techniques, some attackers are moving in the opposite direction. While minimizing the number of exploits and amount of compiled code they introduce to compromised networks altogether, their work continues to require sophisticated code or exploit introduction at a stable entry into the enterprise, script tools and escalation of privilege of all sorts, and stolen access credentials at victim organizations.

As we saw with BlackEnergy 2 (BE2), attackers will actively defend their own presence and identity within victim networks once discovered. Their persistence techniques are becoming more advanced and expansive. These same groups will step up the amount and aggression of destructive last effort components used to cover their tracks, and they include more *nix support, networking equipment, and embedded OS support. We have already seen some expansion from BE2, Yeti, and Winnti actors.

4

NEW METHODS OF DATA EXFILTRATION

The days when attackers would simply activate a backdoor in a corporate network and start siphoning terabytes of information to FTP servers around the world are long gone. Today, more sophisticated groups use SSL on a regular basis alongside custom communication protocols.

Some of the more advanced groups rely on backdooring networking devices and intercepting traffic directly for commands. Other techniques we have seen include exfiltration of data to cloud services, for instance via the WebDAV protocol (facilitates collaboration between users in editing and managing documents and files stored on web servers).

These in turn have resulted in many corporations banning public cloud services such as Dropbox from their networks. However, this remains an effective method of bypassing intrusion detection systems and DNS blacklists.

What to expect: In 2015, more groups to adopt use of cloud services in order to make exfiltration stealthier and harder to notice.

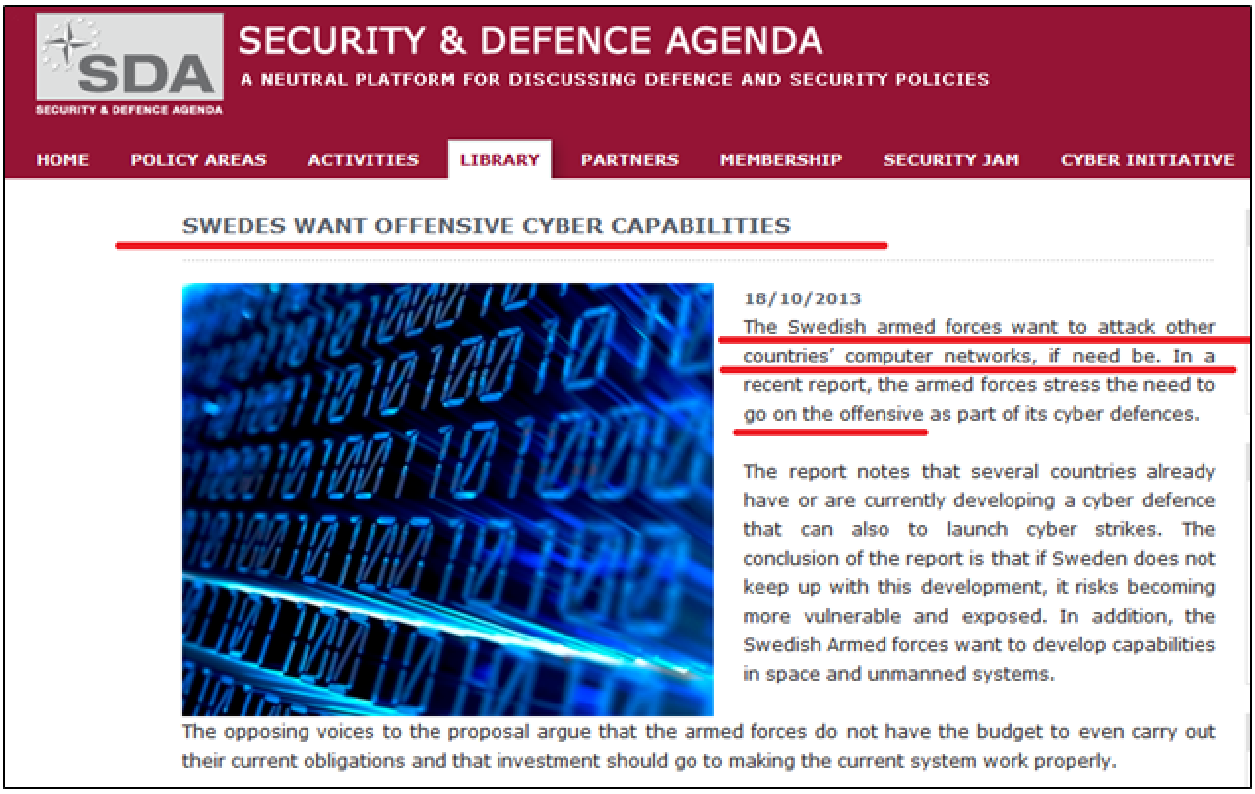
5

NEW APTS FROM UNUSUAL PLACES AS MORE COUNTRIES JOIN THE CYBER ARMS RACE

In February 2014, we published research into Careto/Mask, an extremely sophisticated threat actor that appears to be fluent in Spanish, a language rarely seen in targeted attacks. In August, we also released a report on Machete, another threat actor using the Spanish language.

Before that, we were accustomed to observing APT actors and operators that are fluent in relatively few languages. Additionally, many professionals do not use their native language, preferring instead to write in perfect English.

In 2014, we observed a lot of nations around the world publicly expressing an interest in developing APT capabilities:



SECURITY & DEFENCE AGENDA

A NEUTRAL PLATFORM FOR DISCUSSING DEFENCE AND SECURITY POLICIES

SWEDES WANT OFFENSIVE CYBER CAPABILITIES

18/10/2013

The Swedish armed forces want to attack other countries' computer networks, if need be. In a recent report, the armed forces stress the need to go on the offensive as part of its cyber defences.

The report notes that several countries already have or are currently developing a cyber defence that can also to launch cyber strikes. The conclusion of the report is that if Sweden does not keep up with this development, it risks becoming more vulnerable and exposed. In addition, the Swedish Armed forces want to develop capabilities in space and unmanned systems.

The opposing voices to the proposal argue that the armed forces do not have the budget to even carry out their current obligations and that investment should go to making the current system work properly.

What to expect: Although we haven't yet seen APT attacks in Swedish, we do predict that more nations will join the "cyber-arms" race and develop cyber-espionage capabilities.

6

USE OF FALSE FLAGS IN ATTACKS

Attackers make mistakes. In the vast majority of the cases we analyze, we observe artifacts that provide clues about the language spoken by the attackers. For instance, in the case of RedOctober and Epic Turla, we concluded that the attackers were probably fluent in the Russian language. In the case of NetTraveler we came to the conclusion that attackers were fluent in Chinese.

In some cases, experts observe other meta features that could point toward the attackers. For example, performing file timestamp analysis of the files used in an attack may lead to the conclusion in what part of the world most of the samples were compiled.

However attackers are beginning to react to this situation. In 2014 we observed several "false flag" operations where attackers delivered "inactive" malware commonly used by other APT groups. Imagine a threat actor of Western origin dropping a malware commonly used by a "Comment Crew," a known Chinese threat actor. While everyone is familiar with the "Comment Crew" malware implants, few victims could analyze sophisticated new implants. That can easily mislead people into concluding that the victim was hit by the Chinese threat actor.

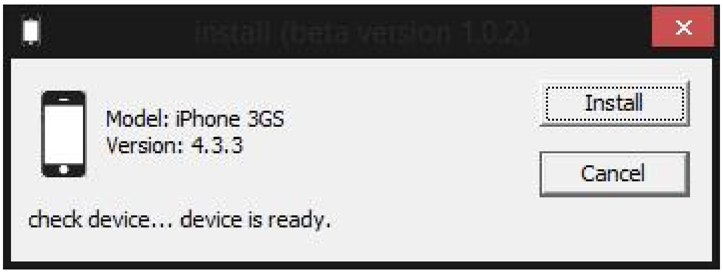
What to expect: In 2015, with governments increasingly keen to "name and shame" attackers, we believe that APT groups will also carefully adjust their operations and throw false flags into the game.

7

THREAT ACTORS ADD MOBILE ATTACKS TO THEIR ARSENAL

Although APT groups have been observed infecting mobile phones, this hasn't yet become a major trend. Perhaps the attackers wish to get data that isn't usually available on mobiles, or maybe not all of them have access to the technologies that can infect Android and iOS devices.

In 2014 we saw several new APT tools designed for infecting mobiles, for instance Hacking Team's Remote Control System mobile modules.



Model: iPhone 3GS
Version: 4.3.3

check device... device is ready.

Additionally, during the Hong Kong protests in October 2014, attacks were seen against Android and iOS users which appear to be connected to APT operations.

Although a mobile phone might not have valuable documents and schematics, or geopolitical expansion plans for next 10 years, they can be a valuable source of contacts as well as listening points. We observed this with the RedOctober group, which had the ability to infect mobile phones and turn them into “Zakladka's”, mobile bugs.

What to expect: In 2015, we anticipate more mobile-specific malware, with a focus on Android and jailbroken iOS.

8

APT+BOTNET: PRECISE ATTACK + MASS SURVEILLANCE

In general, APT groups are careful to avoid making too much noise with their operations. This is why the malware used in APT attacks is much less widespread than common crimeware such as Zeus, SpyEye and Cryptolocker.

In 2014 we observed two APT groups (Animal Farm and Darkhotel) using botnets in addition to their regular targeted operations. Of course, botnets can prove to be a vital asset in cyberwar and can be used to DDoS hostile countries; this has happened in the past. We can therefore understand why some APT groups might want to build botnets in addition to their targeted operations.

In addition to DDoS operations, botnets can also offer another advantage - mass surveillance apparatus for a “poor country”. For instance, Flame and Gauss, which we discovered in 2012, were designed to work as a mass surveillance tool, automatically collecting information from tens of thousands of victims. The information would have to be analyzed by a supercomputer, indexed and clustered by keywords and topics; most of it would probably be useless. However, among those hundreds of thousands of exfiltrated documents, perhaps one provides key intelligence details, that could make a difference in tricky situations.

What to expect: In 2015 more APT groups will embrace this trend of using precise attacks along with noisy operations and deploy their own botnets.

9

TARGETING OF HOTEL NETWORKS

The Darkhotel group is one of the APT actors known to have targeted specific visitors during their stay in hotels in some countries. Actually, hotels provide an excellent way of targeting particular categories of people, such as company executives. Targeting hotels is also highly lucrative because it provides intelligence about the movements of high profile individuals around the world.

Compromising a hotel reservation system is an easy way to conduct reconnaissance on a particular target. It also allows the attackers to know the room where the victim is staying, opening up the possibility of physical attacks as well as cyber-attacks.

It isn't always easy to target a hotel. This is why very few groups, the elite APT operators, have done it in the past and will use it as part of their toolset.

What to expect: In 2015, a few other groups might also embrace these techniques, but it will remain beyond the reach of the vast majority of APT players.

10

COMMERCIALIZATION OF APT AND THE PRIVATE SECTOR

Over the last few years, we published extensive research into malware created by companies such as HackingTeam or Gamma International, two of the best known vendors of “legal spyware”. Although these companies claim to sell their software only to “trusted government entities”, public reports from various sources, including Citizen Lab, have repeatedly shown that spyware sales cannot be controlled. Eventually, these dangerous software products end up in the hands of less trustworthy individuals or nations, who can use them for cyber-espionage against other countries or their own people.

The fact is that such activities are highly profitable for the companies developing the cyber-espionage software. They are also low risk because – so far – we have not seen a single case where one of these companies was convicted in a cyber-espionage case. The developers of these tools are usually out of the reach of the law, because the responsibility falls with the tool users, not the company that develops and facilitates the spying.

What to expect: It’s a high-reward, low risk business that will lead to the creation of more software companies entering the “legal surveillance tools” market. In turn, these tools will be used for nation-on-nation cyber-espionage operations, domestic surveillance and maybe even sabotage.

11

CONCLUSIONS

In general, 2014 was a rather sophisticated and diverse year for APT incidents. We discovered several zero-days, for instance CVE-2014-0515 which was used by a group we call “Animal Farm”. Another zero-day we discovered was CVE-2014-0487, used by the group known as DarkHotel. In addition to these zero-days, we observed several new persistence and stealth techniques, which in turn resulted in the development and deployment of several new defense mechanisms for our users.

If we can call 2014 “sophisticated”, the word for 2015 will be “elusive”. We believe that more APT groups will become concerned with exposure and they will take more advanced measures to hide from discovery.

Finally, some of them will deploy false flag operations. We anticipate these developments and, as usual, will document them thoroughly in our reports.

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