IT THREAT EVOLUTION Q2 2014

DAVID EMM

ROMAN UNUCHEK

VICTOR CHEBYSHEV

MARIA GARNAEVA

DENIS MAKRUSHIN

KASPERSKY lab

CONTENTS

Q2 2014 IN FIGURES

> According to KSN data, Kaspersky Lab products detected and neutralized a total of 995,534,410 threats in the second quarter of 2014.

> Kaspersky Lab solutions repelled 354,453,992 attacks launched from online resources located all over the world.

> Kaspersky Lab's web antivirus detected 57,133,492 unique malicious objects: scripts, web pages, exploits, executable files, etc.

> 145,386,473 unique URLs were recognized as malicious by web antivirus.

> 39% of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US and Germany.

> Kaspersky Lab's antivirus solutions detected 528,799,591 virus attacks on users' computers. A total of 114,984,065 unique malicious and potentially unwanted objects were identified in these incidents.

> In Q2 2014, 927,568 computers running Kaspersky Lab products were attacked by banking malware.

> A total of 3,455,530 notifications about attempts to infect those computers with financial malware were received.

OVERVIEW

TARGETED ATTACKS AND MALWARE CAMPAIGNS

'SOMEBODY'S POISONED THE WATER-HOLE'

In April, we reported a new Flash Player zero-day that we believe was used in watering-hole attacks from a compromised Syrian web site. The site (http://jpic.gov.sy), launched in 2011 by the Syrian Ministry of Justice, was designed to enable citizens to complain about law and order violations. We believe that this attack was developed to target Syrian dissidents complaining about the government.

We analyzed two new SWF exploits (both detected proactively by Kaspersky Lab products) in mid-April that didn't use any vulnerabilities that we already knew about – the vulnerability was later confirmed by Adobe as a new zero-day (CVE-2014-0515). This was located in the Pixel Bender component (no longer supported by Adobe) used for video and image processing. While the first exploit is fairly standard and was able to infect practically any unprotected computer, the second functions only on computers where the Adobe Flash Player 12 ActiveX and Cisco MeetingPlace Express add-ins are installed. The authors were counting on the developers not finding a vulnerability in that component in the hope that the exploit would remain active for longer. This suggests that the attackers were not targeting victims en masse.

It seems likely that victims were redirected to the exploits by means of an iframe or a script on the compromised site. When we published our blog on this zero-day, we had seen more than 30 detections on the computers of seven different people – all of them located in Syria.

We believe that this attack was carefully planned by high-caliber attackers, as evidenced by the use of professionally-written zero-day exploits used to compromise a single resource.

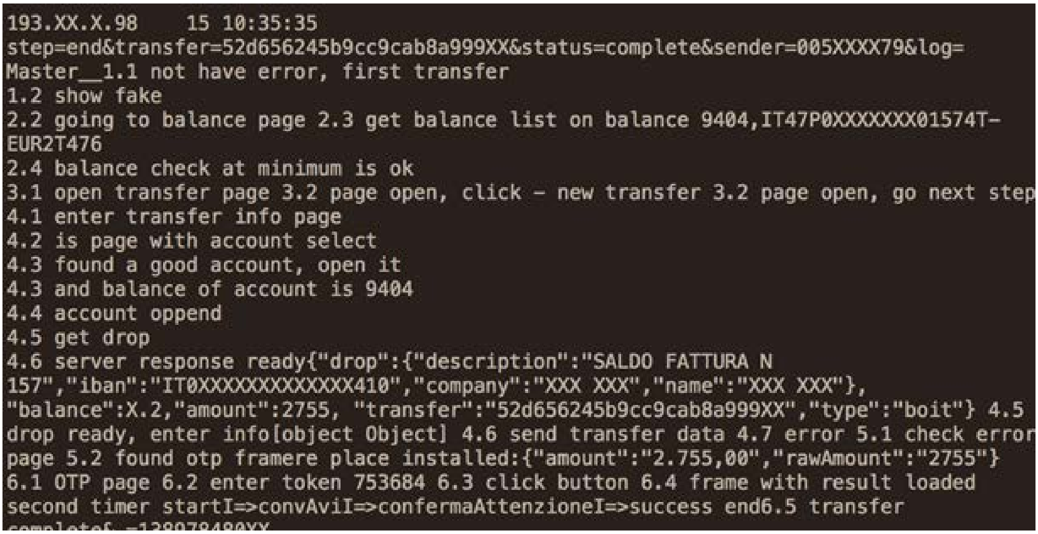
Technical details on the exploits can be found here.

THE ITALIAN (AND TURKISH) JOB

In June we reported on our research into an attack against the clients of a large European bank that resulted in the theft of half a million euros in just one week.

We uncovered the first signs of the campaign in January, when we discovered a suspicious server containing logs relating to financial fraud transactions – including details of the victims and sums of money that had been stolen. Further analysis revealed further information, showing the bank being targeted, the money mule system, operational details of the attack and JavaScript related to the command-and-control (C2) part of the campaign. It became clear that this was the server-side portion of a banking Trojan infrastructure. We named the C2 'luuuk' after the path in the administration panel used in the server – '/server/adm/luuuk'.

The campaign targeted customers of a single bank. 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.



```
193.XX.X.98    15 10:35:35
step=end&transfer=52d656245b9cc9cab8a999XX&status=complete&sender=005XXXX79&log=
Master__1.1 not have error, first transfer
1.2 show fake
2.2 going to balance page 2.3 get balance list on balance 9404,IT47P0XXXXXXX01574T-
EUR2T476
2.4 balance check at minimum is ok
3.1 open transfer page 3.2 page open, click - new transfer 3.2 page open, go next step
4.1 enter transfer info page
4.2 is page with account select
4.3 found a good account, open it
4.3 and balance of account is 9404
4.4 account oppend
4.5 get drop
4.6 server response ready{"drop":{"description":"SALDO FATTURA N
157","iban":"IT0XXXXXXXXXXXXXX410","company":"XXX XXX","name":"XXX XXX"},
"balance":X.2,"amount":2755, "transfer":"52d656245b9cc9cab8a999XX","type":"boit"} 4.5
drop ready, enter info[object Object] 4.6 send transfer data 4.7 error 5.1 check error
page 5.2 found otp framere place installed:{"amount":"2.755,00","rawAmount":"2755"}
6.1 OTP page 6.2 enter token 753684 6.3 click button 6.4 frame with result loaded
second timer startI=>convAviI=>confermaAttenzioneI=>success end6.5 transfer
complete{ =1389784800XX
```

Such injections are common in all variants of Zeus (Citadel, SpyEye, IceIX, etc.). We weren't able to identify the infection vector but banking Trojans use a variety of methods to infect victims, including spam and drive-by downloads. Following the publication of our post, researchers at Fox-IT InTELL sent us information potentially related to this campaign. This data indicated that the Luuuk server could be related to the ZeusP2P (aka Murofet), as we had originally suspected. However there was no definitive proof of this since the injected code couldn't be found on the server when we performed our analysis.

The attackers used stolen credentials to check the victim's account balance and perform malicious transactions automatically, probably operating in the background of a legitimate banking session. This is consistent with one of the malicious artefacts (a VNC server) that we found bound to the malicious server used by the attackers.

The stolen money was then transferred automatically to preset 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.

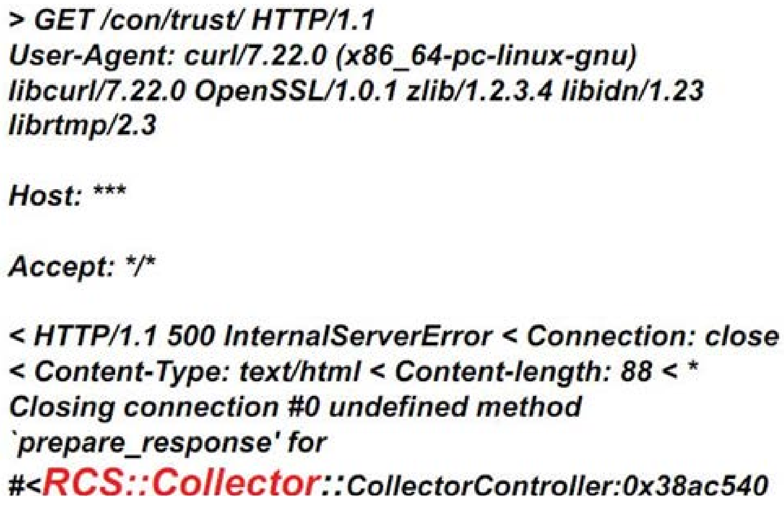
The attackers removed all the sensitive components on 22 January, two days after our investigation started. Based on the transaction activity, we believe that this represents an infrastructure change rather than a complete shutdown of the operation. Our analysis of attack indicates that the cybercriminals behind the campaign are highly professional and very active. They have also shown proactive operational security activities, changing tactics and removing traces when discovered.

When we first found the C2 server, we reported the matter to the bank concerned and to the appropriate law enforcement agencies. We are maintaining our contact with these agencies and continue to investigate the attack.

‘LEGAL’ SPYWARE GOES MOBILE

In June, we published the results of our latest research into the ‘legal’ software called Remote Control System (RCS) developed by the Italian company HackingTeam. It’s not the first time we’ve focused on this company’s software. However, there have been significant developments since our previous article on RCS.

First, we discovered a feature that can be used to fingerprint the RCS command-and-control (C2) servers. When a special request is sent to an RCS server, it responds with the following error message:



```
> GET /con/trust/ HTTP/1.1
User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu)
libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23
librtmp/2.3

Host: ***

Accept: */*

< HTTP/1.1 500 InternalServerError < Connection: close
< Content-Type: text/html < Content-length: 88 < *
Closing connection #0 undefined method
`prepare_response' for
#<RCS::Collector::CollectorController:0x38ac540
```

We were able to use this method to scan the entire IPv4 space, which enabled us to find all the IP addresses of RCS C2 servers across the globe. We found 326 in total, most of them located in the US, Kazakhstan and Ecuador. You can see the list here. 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.

Second, we discovered a number of mobile malware modules for Android, iOS, Windows Mobile and BlackBerry coming from HackingTeam. 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 an 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 optimiser/obfuscator, so it was difficult to analyse. 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'.You can find the full list of functions here.

This new data highlights the sophistication of such surveillance tools. Kaspersky Lab's 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.

MINIDUKE RE-LOADED

The beginning of 2014 saw the re-activation of MiniDuke, an APT campaign from early 2013. 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.

The targets of the new MiniDuke operation (known also as TinyBaron and CosmicDuke) include government, diplomatic, energy, military and telecom operators. But unusually, the list of victims includes those involved in the trafficking and reselling of illegal substances, including steroids and hormones. The reason for this isn't clear. It's possible that the customizable backdoor is available as so-called 'legal spyware'. But it may simply be that it's available in the underground market and has been purchased by various competitors in the pharmaceutical business to spy on each other.

The campaign targets countries across the world, including Austria, Belgium, France, Germany, Hungary, the Netherlands, Spain, Ukraine, and the USA.

One of the servers we analyzed contained a long list of victims dating back to April 2012. There were 265 different identifiers on the server, assigned to victims from 139 unique IPs: the geographical distribution of the victims included Georgia, Russia, the USA, the UK, Kazakhstan, India, Belarus, Cyprus, Ukraine and Lithuania.

Our analysis revealed that the attackers were expanding their field of operations, scanning IP ranges and servers in Azerbaijan, Ukraine and Greece.

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's components can be categorized according to their functions.

(1) Persistence. The malware is able to start via Windows Task Scheduler at a specific time, or when the screensaver is activated.

(2) Reconnaissance. 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 an individual victim. The malware is protected with a custom obfuscated loader which heavily consumes CPU resources for three to five minutes before executing the payload. This makes it hard to analyze. But it also drains the resources that security software needs to emulate the execution of the malware. 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 has been done deliberately to mislead researchers.

One of the more technically advanced parts of the malware relates to data storage. 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.

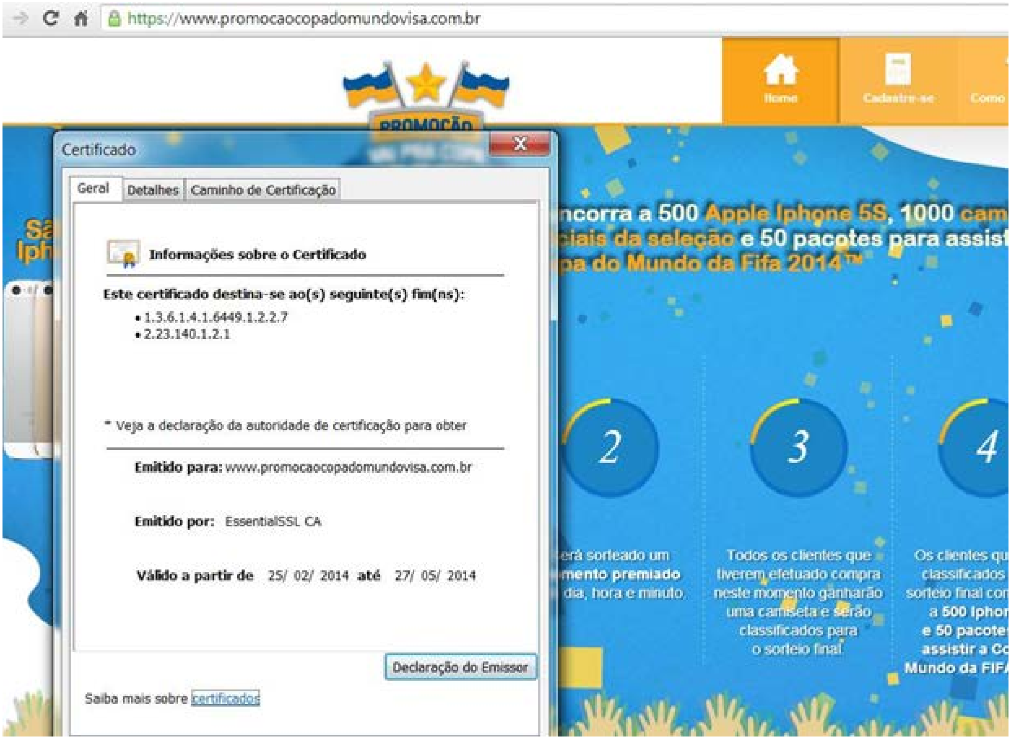
(3) Exfiltration. The malware implements several methods to transfer stolen data, including upload via FTP and three types of HTTP-based communication. When a file is uploaded to the C2 server it is split into small chunks (of around 3KB), which are compressed, encrypted and placed in a container to 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 be an overhead, the layers of additional processing ensures that very few researchers will get to the original data, and offers increased reliability against network errors.

As is the case with any APT, attribution is virtually impossible. While the attackers use English in several places, there are indications that it's not their native language. We found strings in a block of memory appended to the malware component used for persistence that suggest they may be Russian. This was true also of the use of Codepage 1251 in the webshell used by the attackers to compromise the C2 hosts this is commonly used to render Cyrillic characters. The same webshell was observed in the operations of another APT – Turla, Snake or Uroburos).

ONLINE FRAUDSTERS – THEIR [WORLD] CUP RUNNETH OVER!

Fraudsters are always on the lookout for opportunities to make money off the back of major sporting events and the FIFA World Cup is no different. In the run up to the tournament, we highlighted the various ways in which the scammers were trying to take advantage of unwary visitors to Brazil for football's major showcase event.

One obvious way for scammers to cash-in is through phishing attacks. It's common for phishers to compromise a legitimate site and host their page there. But Brazilian phishers have gone the extra mile to stage attacks that are very difficult for ordinary people to spot. They registered domains using the names of well-known local brands – including credit card companies, banks and online stores. However, the cybercriminals went one mile further still. Not only were the sites very professionally designed – they gave their sites an even greater feel of authenticity by buying SSL certificates from Certification Authorities such as Comodo, EssentialSSL, Starfield, Register.com and others. Clearly, a site with a 'legitimate' SSL certificate is likely to fool even security conscious consumers.



Informações sobre o Certificado

Este certificado destina-se ao(s) seguinte(s) fim(ns):

- 1.3.6.1.4.1.6449.1.2.2.7
- 2.23.140.1.2.1

* Veja a declaração da autoridade de certificação para obter

Emitido para: www.promocaocopadomundovisa.com.br

Emitido por: EssentialSSL CA

Válido a partir de 25/ 02/ 2014 até 27/ 05/ 2014

Saiba mais sobre certificados

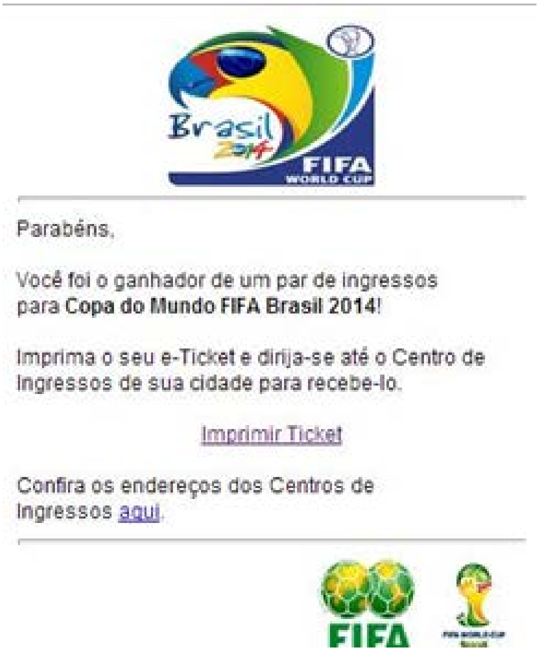
ncorra a 500 Apple Iphone 5S, 1000 cam
ciais da seleção e 50 pacotes para assist
pa do Mundo da Fifa 2014™

2
erá sorteado um
mento premiado
dia, hora e minuto.

3
Todos os clientes que
tiverem efetuado compra
neste momento ganharão
uma camiseta e serão
classificados para
o sorteio final.

4
Os clientes qu
classificados
sorteio final co
a 500 Iphon
e 50 pacote
assistir a Co
Mundo da FIF

They are also taking advantage of how easy it is to buy certificates in order to distribute digitally-signed malware. They start by sending messages offering free World Cup tickets, with a link that leads to a banking Trojan:



Parabéns,

Você foi o ganhador de um par de ingressos para **Copa do Mundo FIFA Brasil 2014**!

Imprima o seu e-Ticket e dirija-se até o Centro de Ingressos de sua cidade para recebe-lo.

Imprimir Ticket

Confira os endereços dos Centros de Ingressos aqui.

Some of these e-mails contain personal details, stolen from a breached database, to add credibility to the bogus offer.

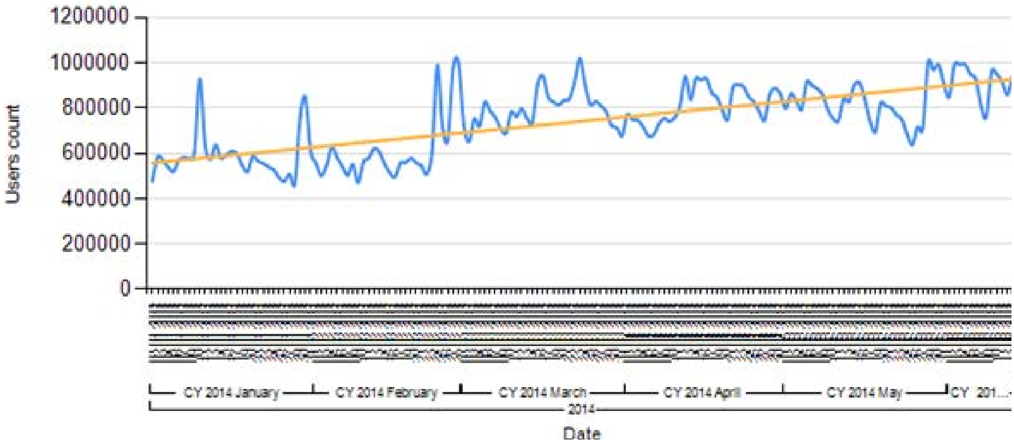
However, Brazilian cybercriminals aren't restricting their activities to phishing alone. We also reported how they were using malware installed on Point-of-Sale and PIN-pad devices in order to capture credit card data. These devices are connected to a computer via USB or serial port, to communicate with electronic funds transfer (EFT) software. The Trojans they use infect the computer and sniff the data transmitted through these ports. These PIN-pads are equipped with security features to ensure that security keys are erased if someone tries to tamper with the device. The PIN is encrypted as soon as it's entered – commonly using triple DES encryption. But Track 1 data (credit card number, expiry data, service code and CVV) and public CHIP data aren't encrypted on old, outdated devices – instead, they're sent in plain text to the computer via USB or serial port. This gives the cybercriminals all they need to clone the card.

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

Our report also highlighted the dangers of charging a mobile device using a USB port installed in a public place. Malicious AC/DC chargers can charge your device's battery, but they can also silently steal data from your device – or even install malware.

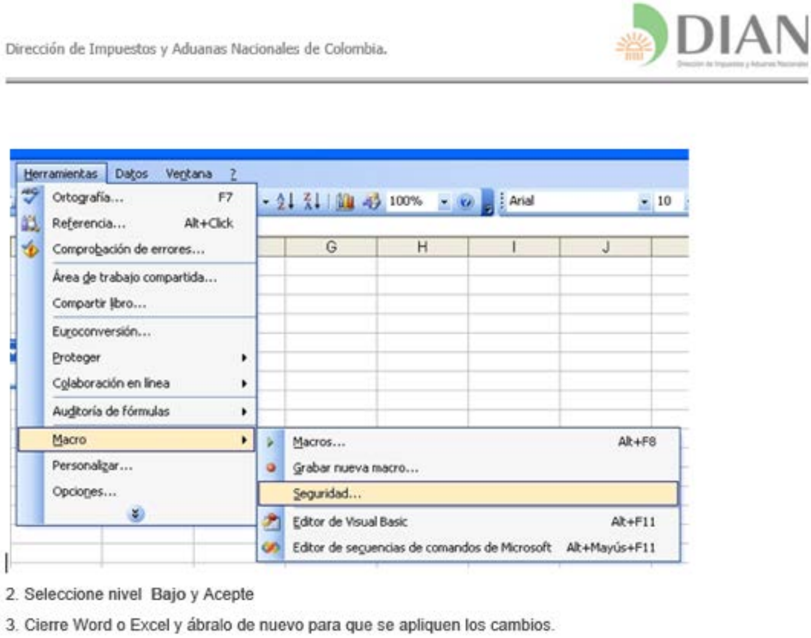
Punto de Energía
Energy Source
No olvide retirar su dispositivo
Remember to remove your device
Voltaje
Voltage
110V
USB
2.1 A
1.0 A

There's another way the fraudsters can make money from people, even if they're not looking for World Cup tickets. With a big audience all over the world, often in distant time zones, fans can find themselves away from their TV at the time they want to watch the game. That's when they start looking for a live online stream of the action. Unfortunately, searching for live broadcasts on the Internet can prove to be very expensive or result in your computer getting infected. That's because some of the advertisements you find when you search lead to fraudulent or malicious content. When you go to the web site, it asks you to download a special plugin so you can watch the online broadcast. But it turns out to be an adware program that may show you nothing, but will drain your computer's resources. Adware straddles the thin line between cybercrime and legitimate software. So it's little wonder that our statistics show ongoing detections of this type of software. You can find our full report here.



PAY THE TAXMAN – BUT AVOID THE PHISHERS

Phishers don't just try to exploit major sporting events. They also base the campaigns around more mundane aspects of life. In May, [many people in Colombia received an e-mail accusing them of tax evasion and fraud](). To add a further 'edge' to the communication, the cybercriminals claimed that this was the third notification about the matter. The e-mail contained a link that led to an infected Word document. Microsoft Office blocks embedded macros, so the attackers included instructions on how the victim should enable macros.



Dirección de Impuestos y Aduanas Nacionales de Colombia.

2. Seleccione nivel Bajo y Acepte

3. Cierre Word o Excel y ábralo de nuevo para que se apliquen los cambios.

If the victim clicks on the document, another malicious file is downloaded to their computer, from a hacked server in Ecuador. This is designed to steal passwords for online games, PayPal, file-sharing systems, social networks (including Facebook and Twitter), online bank accounts and more.

The use of scare tactics in general, and fake communications from tax authorities in particular, are common methods used by phishers around the world.

In April, we published an in-depth report on financial cybercrime, based on data from the Kaspersky Security Network. You can read the report on phishing here.

MALWARE STORIES: LOADING EARLY – THE USE OF BOOTKITS BY CYBERCRIMINALS

When malware writers are developing their code one of their key objectives is to load their malicious content as early as possible in the boot process. This gains the maximum possible control over the system. Bootkits represent the most advanced technology in this area, allowing malicious code to start before the operating system itself loads. This technology has been implemented in numerous malicious programs. Notable examples include XPAJ and TDSS, but there are many others, including targeted attack campaigns such as The Mask.

Bootkits have evolved over the years from proof-of-concept to mass distribution, as we explained here. They have now effectively become open-source software, thanks to the publication of the source-code for the Carberp banking Trojan – the Cidox bootkit was used to protect Carberp and its source-code was published alongside that of Carberp.

It’s clear that the evolution of bootkits must be seen within the overall context of the cat-and-mouse battle between malware writers and anti-malware researchers. They are always looking for new ways to evade detection; we’re continually investigating ways to make protection of our customer more effective. Our report also looks at the security benefits offered by UEFI (Unified Extensible Firmware Interface), as well as how malware writers might try to subvert it.

WEB SECURITY AND DATA BREACHES: WINDOWS XP – UNSUPPORTED, BUT STILL OUT THERE

Support for Windows XP ended on 8 April: this means no new security updates, non-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 for the period since 8 April 2014 indicate that about 18 per cent of infections are on machines running Windows XP. This is a lot of people wide open to attack now that security patches have dried up: effectively, every vulnerability discovered since then 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 un-patched 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 doesn't support Windows XP.

Switching to a newer operating system might seem like a straightforward decision. But although Microsoft gave plenty of notice about the end of support, it's not so difficult to see why migration to a new operating system might be problematic 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 support for XP.

So if you don't switch right now, can you stay secure? Will your anti-virus software protect you?

Certainly it 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.

At best, you should see this as a stop-gap, while you finalize your migration strategy. Malware writers will undoubtedly target Windows XP while significant numbers of people continue to run it, since an un-patched 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 alike. But the potential risk of using an increasingly insecure operating system is likely to outweigh the inconvenience and cost.

MOBILE THREATS

THE QUARTER IN FIGURES

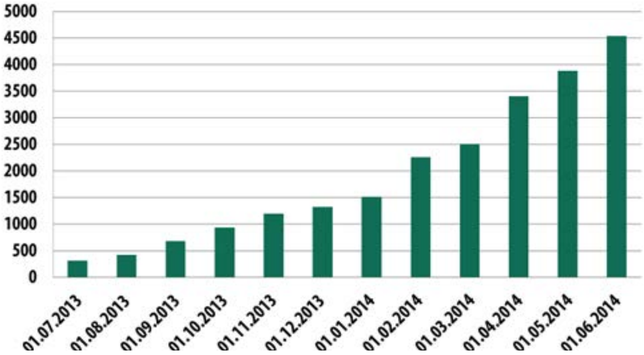
In the second quarter of 2014 the following were detected:

- 727,790 installation packages;
- 65,118 new malicious mobile programs;
- 2,033 mobile banking Trojans.

The sum total of malicious mobile objects detected was 1.7 times lower than in the first quarter. We link this with the start of the holiday season. In June we noticed a reduction in attempts to infect mobile devices using Trojans.

MOBILE BANKING TROJANS

Although the total number of threats decreased in the second quarter, we detected 2033 mobile banking Trojans in this period, 1.7 times more than last quarter. From the beginning of 2014 the number of banking Trojans has increased by almost a factor of four, and over a year (from July 2012) - 14.5 times.

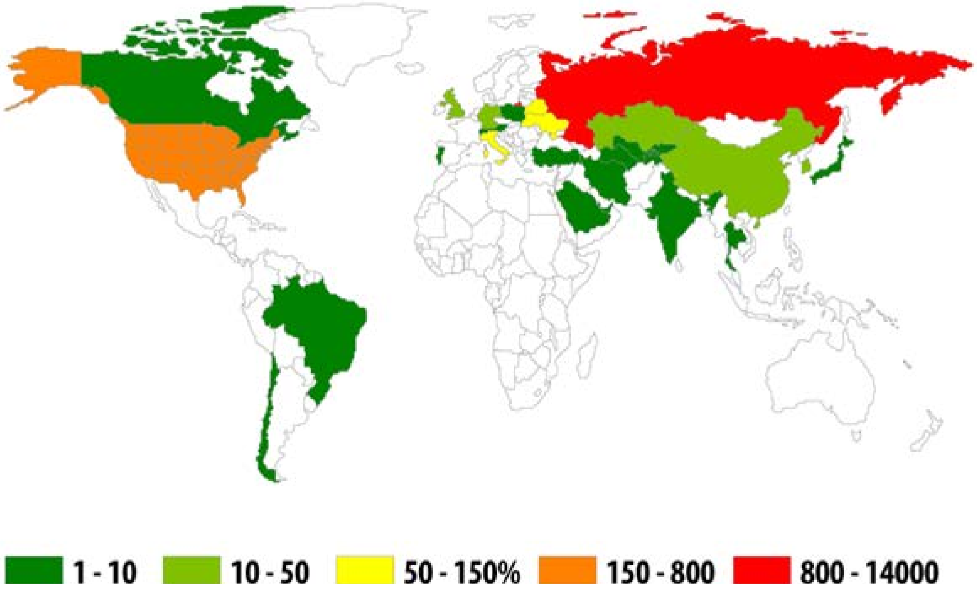


Number of mobile banking Trojans detected, Q2 2014

This growth reflects two factors:

- the interest of cybercriminals in “big” money;
- active countermeasures from antivirus companies.

We note that the geography of infection by mobile banking Trojans has changed:



The geography of infection by mobile banking Trojans in the first quarter of 2014

THE TOP 10 COUNTRIES ATTACKED BY BANKING TROJANS

	COUNTRY	NUMBER OF ATTACKS	% OF ALL ATTACKS
1	Russia	13800	91.7%
2	USA	792	5.3%
3	Ukraine	136	0.9%
4	Italy	83	0.6%
5	Belarus	68	0.5%

6	Republic of Korea	30	0.2%
7	Kazakhstan	25	0.2%
8	China	19	0.1%
9	United Kingdom	17	0.1%
10	Germany	12	0.1%

As before, Russia is in the first place in the rating but in the second place is the USA, and by a big margin over all other countries. Kazakhstan, which was in second place in this rating in the first quarter, is now in seventh place.

NEW DEVELOPMENTS FROM THE VIRUS WRITERS

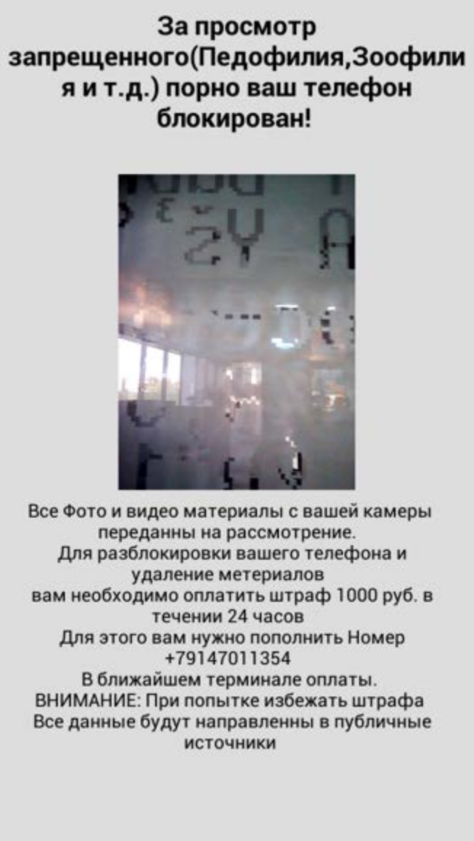
FIRST MOBILE ENCRYPTOR

In the middle of May an announcement appeared on one of the virus writing forums offering a unique Trojan-encryptor for sale at $5000, working on the Android OS. On 18 May we detected the first mobile encryptor in the wild. This malware was detected by Kaspersky Lab as Trojan-Ransom.AndroidOS.Pletor.a.

After the Trojan is started it uses the AES encryption algorithm to encrypt the contents of the memory card of the smartphone, including media files and documents. Immediately after the start of the encryption Pletor displays a ransom demand on the screen. To receive money from the user the QIWI VISA WALLET, MoneXy system or standard transfer of money to a telephone number are used.

By the end of the second quarter we had managed to identify more than 47 versions of the Trojan. They all contain the key necessary to decipher all the files.

For communication with the cybercriminals one version of the Trojan uses the TOR network, others HTTP and SMS. Trojans from this second group show the user a video image of himself in the window with the demand for money, transmitted in real time using the frontal camera of the smartphone.



За просмотр
запрещенного(Педофилия,Зоофили
я и т.д.) порно ваш телефон
блокирован!

Все Фото и видео материалы с вашей камеры
переданны на рассмотрение.
Для разблокировки вашего телефона и
удаление метериалов
вам необходимо оплатить штраф 1000 руб. в
течении 24 часов
Для этого вам нужно пополнить Номер
+79147011354
В ближайшем терминале оплаты.
ВНИМАНИЕ: При попытке избежать штрафа
Все данные будут направленны в публичные
источники

We note that the virus writers use the same social engineering mechanisms as the creators of early encryptors for Windows: the telephone is supposedly blocked for accessing prohibited pornographic content and all the photos and videos on the phone are “transferred for examination”. In addition for non-payment of the “fine” the blackmailers threaten to send all the data to “public sources”.

Pletor is targeted at citizens of Russia and Ukraine and the messages are in Russian and the ransom is demanded in rubles or hryvnia (the sum is the equivalent of about 300 euros). However we have found instances of this malware in 13 countries - mostly on the territory of the former USSR.

DISABLER EVOLUTION

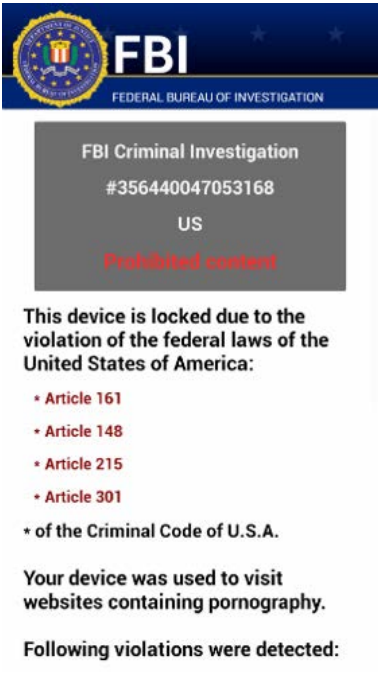
In terms of attack technique there is a clear tendency towards development of ransom-disablers. Here also cybercriminals are adopting methods of frightening their victims that were used by the creators of Windows malware.

The first version of the Svpeng mobile malware, which has Trojan-ransom capability, was detected at the beginning of 2014. The Trojan blocks the phone, allegedly because its owner has viewed child pornography. To unblock the mobile device the cybercriminals demand payment of a “fine” of 500 dollars.

In early June we discovered a new version of Svpeng aimed mostly at users in the USA. However users in the UK, Switzerland, Germany, India and Russia were also attacked.

This version of Svpeng completely blocks the mobile device so that the user can not even access the switch off/reboot menu. The smartphone can only be turned off by a long push on the off button but the Trojan starts immediately after it is switched on again.

At the same time the cybercriminals have used a time-tested social engineering trick. When it starts the Trojan imitates the scanning of the telephone and apparently finds forbidden content. To frighten the user the window announcing the “find” bears the FBI logo.



FBI Criminal Investigation
#356440047053168
US
Prohibited content

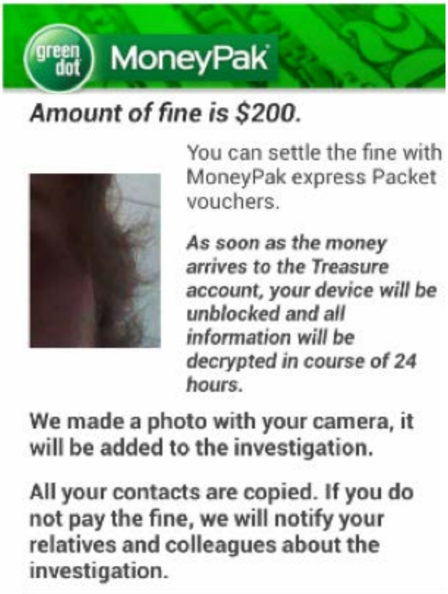
This device is locked due to the violation of the federal laws of the United States of America:

- Article 161
- Article 148
- Article 215
- Article 301

* of the Criminal Code of U.S.A.

Your device was used to visit websites containing pornography.

Following violations were detected:



Amount of fine is $200.

You can settle the fine with MoneyPak express Packet vouchers.

As soon as the money arrives to the Treasure account, your device will be unblocked and all information will be decrypted in course of 24 hours.

We made a photo with your camera, it will be added to the investigation.

All your contacts are copied. If you do not pay the fine, we will notify your relatives and colleagues about the investigation.

The Trojan blocks the phone and demands the payment of 200 dollars to unblock it. The creators of the Trojan use MoneyPak vouchers to receive the money.

In this window Svpeng shows a photograph of the user, taken using the frontal camera, which is reminiscent of Trojan-Ransom.AndroidOS.Pletor.a which we discussed above, except that Pletor transmits a video image.

By the end of the second quarter we had managed to find 64 versions of the new Svpeng. Each version mentions the Cryptor class, although no use of this class was detected. Perhaps the criminals intend in future to use the malware to encrypt users' data and demand a ransom for decrypting it.

NOT ONLY ANDROID

As earlier, the main target of cybercriminals is the Android platform. More than 99% of new mobile malware is aimed at Android.

However this doesn't mean we can forget about other mobile platforms. Thus, in the second quarter of 2014 new malware objects appeared for the Apple iOS platform (but only for "jailbroken" devices). Along with their malware cybercriminals have used the protective functions of iOS for evil aims. An attack on Apple ID allowed the wrongdoers to completely block a device and demand money from their victim to restore its functionality.

The exposure of Hacking Team also came with a sting in the tail, as it was revealed that their arsenal contained modules for attacking "jailbroken" iOS devices.

The platform Windows Phone was not left out either. Here the virus writers had not come up with any technical innovations but took the route of inserting false applications without any useful function whatsoever in the official paid app store. And our brand was not unscathed: the crooks also used the trademark and logo of Kaspersky Lab.

In this way two vulnerabilities were revealed in the Windows Phone Store at once:

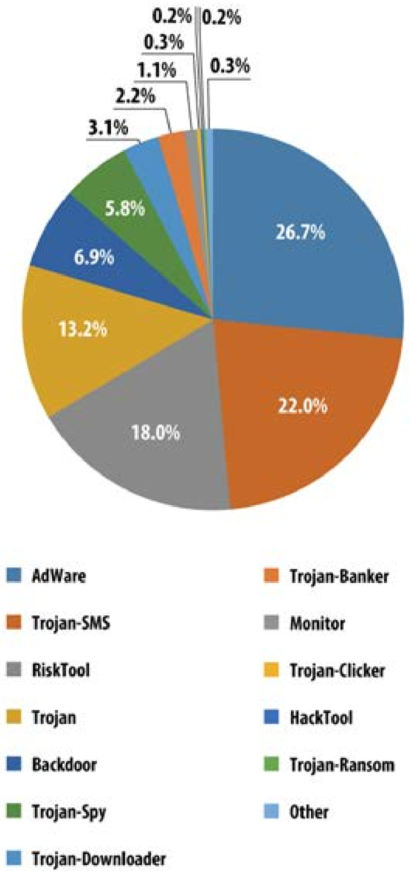
- the lack of checks that brand names are being properly used;
- the lack of checks of functionality.

The same publishers' false apps also appeared on Google Play.

MOBILE THREATS: STATISTICS

The sum total of malicious mobile objects detected was 1.7 times lower than in the first quarter: 727,790 installation packages, 65,118 new mobile malware programs, 2033 mobile banking Trojans. Probably the reduction in activity is down to the start of the holiday season.

DISTRIBUTION OF MOBILE THREATS BY TYPE



Distribution of mobile threats by type, Q2 2014

The rating of malware objects for mobile devices for the second quarter of 2014 was headed by potentially unwanted advertising applications (27%). Holding on to their position are SMS-Trojans with 22%. Whilst the figures for these two types of mobile threats have more or less remained unchanged over the quarter RiskTool has risen from fifth to third place, its share in the flow of mobile malware detected has risen from 8.6% to 18%. These are legal applications that are potentially dangerous for the user - careless use by the smartphone user or a malicious attacker could lead to financial loss.

TOP 20 MALICIOUS MOBILE PROGRAMS

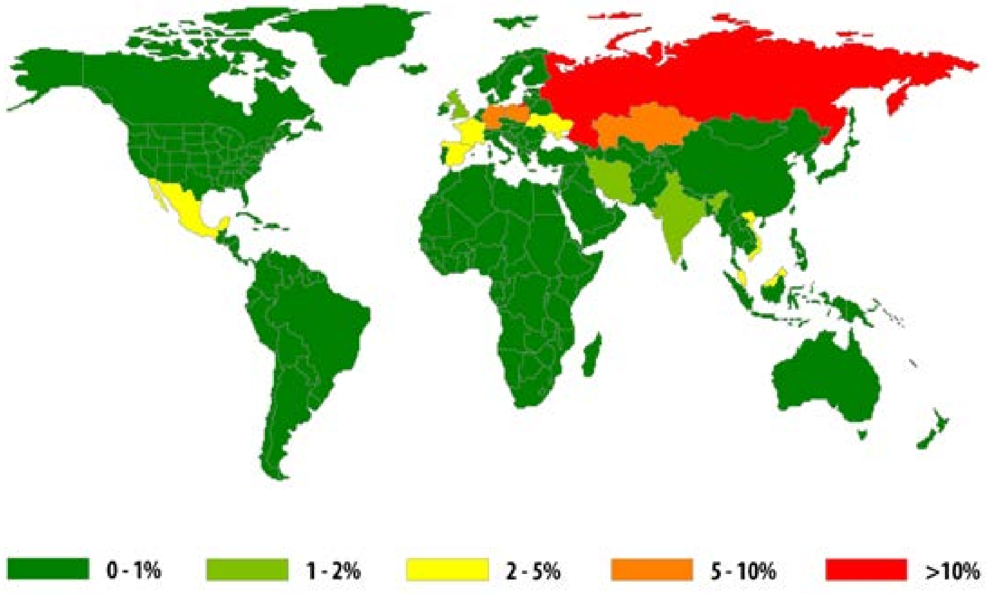
	NAME	% OF ATTACKS*
1	Trojan-SMS.AndroidOS.Stealer.a	25.42%
2	RiskTool.AndroidOS.SMSreg.gc	6.37%
3	RiskTool.AndroidOS.SMSreg.hg	4.82%
4	Trojan-SMS.AndroidOS.FakeInst.a	4.57%
5	Trojan-SMS.AndroidOS.Agent.ao	3.39%
6	AdWare.AndroidOS.Viser.a	3.27%
7	Trojan-SMS.AndroidOS.Opfake.a	2.89%
8	Trojan-SMS.AndroidOS.Erop.a	2.76%
9	Trojan-SMS.AndroidOS.FakeInst.ff	2.76%
10	Trojan-SMS.AndroidOS.Agent.en	2.51%
11	Trojan-SMS.AndroidOS.Agent.ev	2.43%
12	RiskTool.AndroidOS.SMSreg.eh	2.41%
13	Trojan-SMS.AndroidOS.Opfake.bw	1.96%
14	Trojan-SMS.AndroidOS.Opfake.bo	1.53%
15	RiskTool.AndroidOS.MimobSMS.a	1.48%
16	Trojan-SMS.AndroidOS.Skanik.a	1.35%
17	Trojan-SMS.AndroidOS.Agent.mw	1.33%
18	RiskTool.AndroidOS.SMSreg.ey	1.31%
19	Trojan-SMS.AndroidOS.Agent.ks	1.24%
20	Trojan-SMS.AndroidOS.Agent.ay	1.21%

** The percentage of all attacks recorded on the mobile devices of unique users.*

In the TOP 20 detected threats SMS Trojans dominate as before, these malicious programs occupied 15 places in the rating.

Throughout the second quarter, against a background of a reduced number of attacks, we observed a steady growth in attempts to attack users with the Trojan Trojan-SMS.AndroidOS.Stealer.a. This malware took first place in the rating with over 25% of all attacks. The wrongdoers were especially active in April, when attempts at Stealer infection were almost twice as frequent as in May or March. And in June the attempts at infection with this Trojan were 7 times more frequent than those of its nearest competitor.

THE GEOGRAPHY OF THREATS



Map of mobile malware infection attempts

(percentage of all attacks on unique users)

There have been some slight changes in the territorial distribution of attacks. And so we see Germany in the second place, while India, which was in the second place in the first quarter, has fallen out of the TOP 10 altogether. Kazakhstan hung on to third place and Ukraine moved from fourth to fifth to make way for Poland, which climbed from tenth into fourth place.

TOP 10 ATTACKED COUNTRIES:

	COUNTRY	% OF ATTACKS
1	Russia	46.96%
2	Germany	6.08%
3	Kazakhstan	5.41%
4	Poland	5.02%
5	Ukraine	3.72%
6	Malaysia	2.89%
7	Vietnam	2.74%
8	France	2.32%
9	Spain	2.28%
10	Mexico	2.02%

Users install a lot of apps on their mobile devices and it should be noted that in different countries the percentage of malicious apps among the apps installed by users varies.

TOP 10 COUNTRIES BY RISK OF INFECTION

	COUNTRY*	% OF MALICIOUS APPS
1	Vietnam	2.31%
2	Greece	1.89%
3	Poland	1.89%
4	Kazakhstan	1.73%
5	Uzbekistan	1.51%
6	Armenia	1.24%
7	Serbia	1.15%
8	Morocco	1.09%

9	Czech Republic	1.03%
10	Romania	1.02%

**We have excluded countries where there were less than 100,000 downloads*

Although Russia takes first place in terms of recorded attacks it is not the country with the greatest chance of infection with mobile malware. In this respect Vietnam is in the lead; there 2.31% of all apps that users attempted to install were malicious.

Below for comparison we show the risk levels of infection for another 15 countries from various regions of the world:

COUNTRY	% OF MALICIOUS APPS
China	0.94%
France	0.85%
Russia	0.74%
Mexico	0.58%
Spain	0.55%
India	0.41%
Germany	0.19%
UK	0.18%
Argentina	0.13%
Brazil	0.12%
Italy	0.11%
USA	0.09%
Peru	0.07%
Hong Kong	0.06%
Japan	0.02%

In France 0.85% of apps that users were interested in turned out to be malicious, in Russia 0.74%, in Germany 0.19%, in the UK 0.18%, in the USA 0.09% and in Japan only 0.02%.

STATISTICS

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

ONLINE THREATS IN THE BANKING SECTOR

KEY EVENTS IN Q2

One of the biggest events in Q2 was the appearance of the OpenSSL vulnerability capable of providing unauthorized access to users' secret keys, names and passwords as well as content that is transferred in an encrypted form.

The Heartbleed vulnerability is exploited in the OpenSSL cryptographic library used in various software products including banking software. It took several hours for an official patch to emerge, and then there was a long installation procedure, leading to leakage of customer payment data and other valuable information in various spheres of business. Following the spread of this information and those subsequent leaks, we can expect a spike in the number of fraudulent transactions. This is yet another wake-up call, highlighting the need for financial organizations and their customers to stay on top of security for all e-payment data.

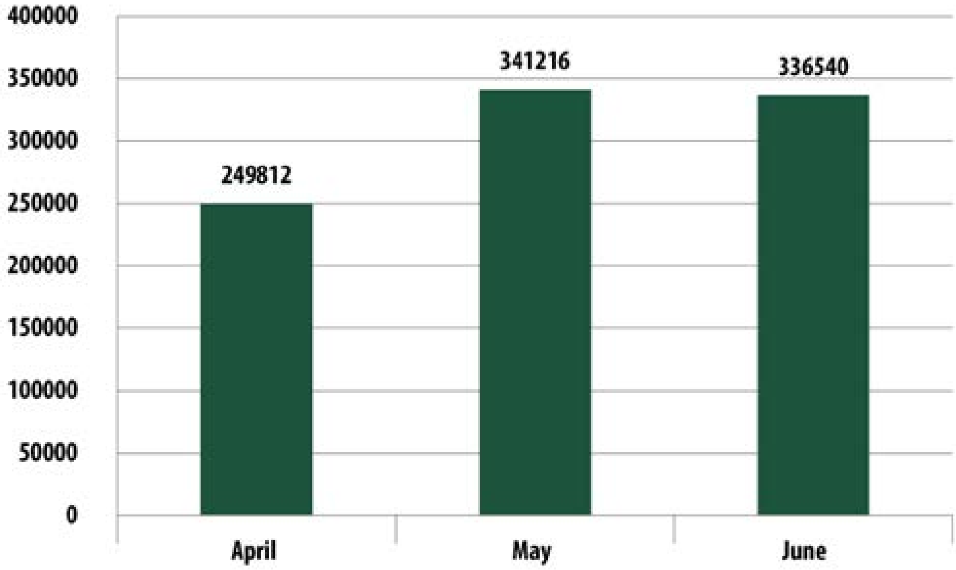
The second quarter of 2014 saw the appearance of a new banking Trojan, Pandemiya, which uses commonly seen malware methods like a web-inject attack to steal payment information.

Q2 also saw an international law enforcement operation to seize control over the Gameover ZeuS botnet. The FBI put the developer of the banking Trojan ZeuS on its international wanted list.

Not surprisingly the 2014 World Cup in Brazil attracted the attention of fraudsters. According to this quarter's results, Brazilian users were attacked by banking malware more frequently than in other countries. Malicious content was detected, for instance, that spread in the guise of adverts and exploited the excitement surrounding this summer's main sporting event.

THE NUMBER OF COMPUTERS ATTACKED BY FINANCIAL MALWARE

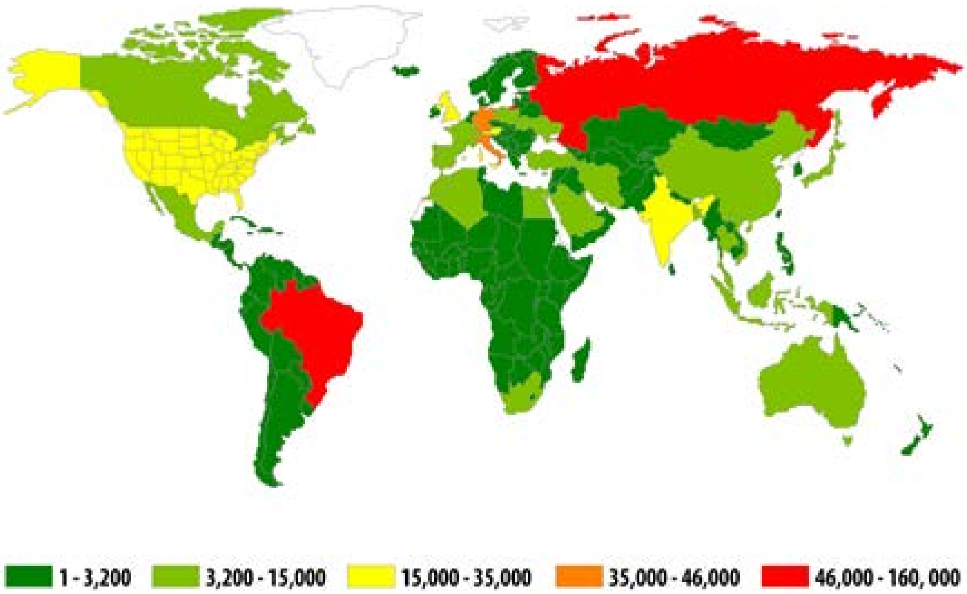
During the reporting period, Kaspersky Lab solutions blocked 927,568 attacks on user computers attempting to launch malware capable of stealing money from online banking accounts. This figure represents a 36.6% increase compared to April.



The number of computers attacked by financial malware, Q2 2014

A total of 3,455,530 notifications of malicious activity by programs designed to steal money via online access to bank accounts were registered by Kaspersky Lab security solutions in Q2 2014.

THE GEOGRAPHY OF ATTACKS



The geography of banking malware attacks in Q2 2014

(by number of attacked users in the country)

THE TOP 20 COUNTRIES BY THE NUMBER OF ATTACKED USERS:

	COUNTRY	NUMBER OF USERS
1	Brazil	159,597
2	Russia	50,003
3	Italy	43,938
4	Germany	36,102
5	USA	34,539

6	India	27,447
7	UK	25,039
8	Austria	16,307
9	Vietnam	14,589
10	Algeria	9,337

Brazil traditionally tops the rating of the countries where users are attacked by banking malware most often.

Brazil is often at the top of this list because financial malware has always been widely used by criminals here. In Q2 2014, the FIFA World Cup generated even more opportunities for attacks: thousands of fans visited the country and used online banking systems while they were there. Kaspersky Lab experts have examined the security of Wi-Fi networks and made a list of recommendations for those who do not want to risk compromising their payment information in Brazil.

THE TOP 10 BANKING MALWARE FAMILIES

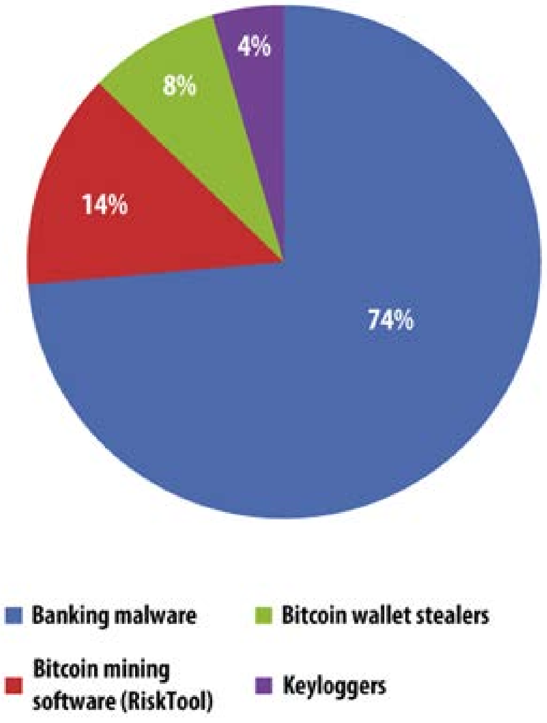
The table below shows the programs most commonly used in Q2 2014 to attack online banking users, based on the number of reported infection attempts:

	VERDICT*	NUMBER OF USERS	NUMBER OF NOTIFICATIONS
1	Trojan-Spy.Win32.Zbot	559,988	2,353,816
2	Trojan-Banker.Win32.Lohmys	121,675	378,687
3	Trojan-Banker.Win32.ChePro	97,399	247,467
4	Trojan-Spy.Win32.Spyeyes	35,758	99,303
5	Trojan-Banker.Win32.Agent	31,234	64,496
6	Trojan-Banker.Win32.Banbra	21,604	60,380
7	Trojan-Banker.Win32.Banker	22,497	53,829
8	Trojan-Banker.Win32.Shiotob	13,786	49,274
9	Backdoor.Win32.Clampi	11,763	27,389
10	Backdoor.Win32.Shiz	6,485	17,268

Zeus (Trojan-Spy.Win32.Zbot) remained the most widespread banking Trojan. According to Kaspersky Lab's research, the program was involved in 53% of malware attacks affecting online banking clients.

Nine out of 10 malware families represented in the table work by injecting a 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. As well as web injections, four of the 10 entries also make use of keylogging technology, which suggests this method of stealing information is still effective when carrying out attacks on online banking customers.

Financial threats are not restricted to banking malware that attacks the customers of online banking.

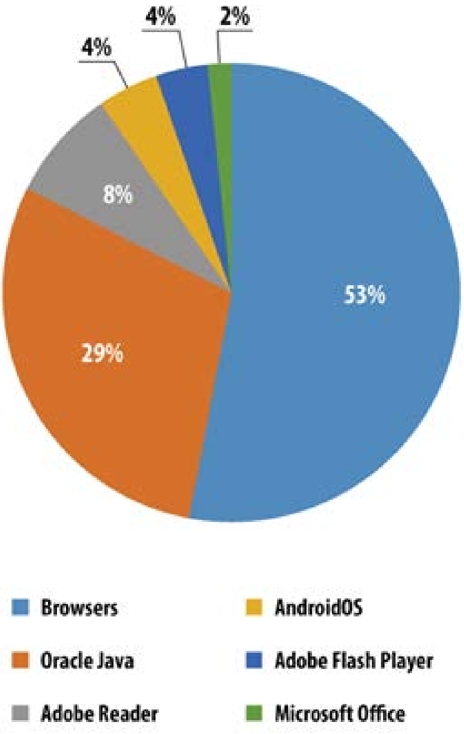


Distribution of attacks targeting user money by malware type, Q2 2014

As well as banking Trojans that modify HTML pages in the browser, there are other methods of stealing e-money, such as Bitcoin wallet theft. Fraudsters are also happy to use computing resources to generate crypto currency: Bitcoin miners account for 14% of all financial attacks. Criminals also use keyloggers to collect user credentials for online banking and payment systems in another bid to access bank accounts.erate crypto currency: Bitcoin miners account for 14% of all financial attacks. Criminals also use keyloggers to collect user credentials for online banking and payment systems in another bid to access bank accounts.

VULNERABLE APPLICATIONS USED BY FRAUDSTERS

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



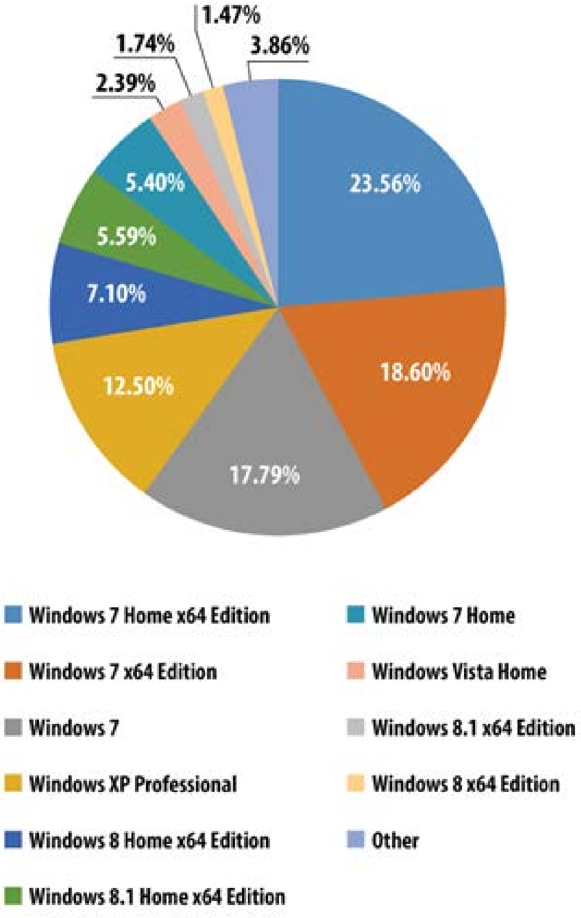
The distribution of exploits used by fraudsters, by type of application attacked, Q2 2014

Of all registered attempts to use vulnerabilities, 53% involved vulnerabilities in browsers. Almost every exploit pack includes an exploit for Internet Explorer.

Java exploits are in second place. Java vulnerabilities are used in drive-by attacks via the Internet and new Java exploits are part of many exploit packs. In 2013, 90.5% all of registered attempts to use vulnerabilities exploited vulnerabilities in Oracle Java. At the beginning of 2014 the popularity of Java exploits began to decrease. In Q1 of this year, 54% of attempts to use vulnerabilities targeted

Java; in the second quarter the figure was just 29%. This decline in popularity may reflect the fact that no new Java vulnerabilities have been made public for almost a year.

Next come Adobe Reader exploits. These vulnerabilities are also exploited in drive-by attacks via the Internet and PDF exploits are part of many exploit packs.



The distribution of Windows OS installed on user computers by version, Q2 2014

65.35% of KSN participants use various versions of Windows 7 and 12.5% use Windows XP.

ONLINE THREATS (WEB-BASED ATTACKS)

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

THE TOP 20 MALICIOUS OBJECTS DETECTED ONLINE

In the second quarter of 2014, Kaspersky Lab's web antivirus detected 57,133,492 unique malicious objects: scripts, web pages, exploits, executable files, etc.

We identified the 20 most active malicious programs involved in online attacks launched against user computers. These 20 accounted for 97% of all attacks on the Internet.

	NAME*	% OF ALL ATTACKS**
1	Malicious URL	72.94%
2	Trojan.Script.Generic	11.86%
3	Trojan-Downloader.Script.Generic	5.71%
4	Trojan.Script.Iframer	2.08%
5	Adware.Win32.Amonetize.heur	1.00%
6	AdWare.Script.Generic	0.88%
7	AdWare.Win32.Agent.aiyc	0.76%
8	AdWare.Win32.Yotoon.heur	0.25%
9	Trojan.Win32.AntiFW.b	0.23%
10	AdWare.Win32.Agent.allm	0.19%
11	AdWare.Win32.AirAdInstaller.aldw	0.17%
12	Trojan.Win32.Generic	0.15%
13	Trojan-Downloader.Win32.Generic	0.14%
14	Trojan.Win32.Vague.cg	0.11%
15	Trojan.Win32.Invader	0.11%
16	AdWare.Win32.BetterSurf.b	0.10%
17	AdWare.Win32.Lollipop.qp	0.08%

18	Exploit.Script.Blocker	0.08%
19	AdWare.Win32.Lollipop.agzn	0.08%
20	Trojan.JS.Small.aq	0.07%

** These statistics represent detection verdicts of 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 mostly comprises verdicts assigned to objects used in drive-by attacks and to adware programs. The number of positions occupied by adware verdicts rose from nine to 11 in the second quarter of 2014.

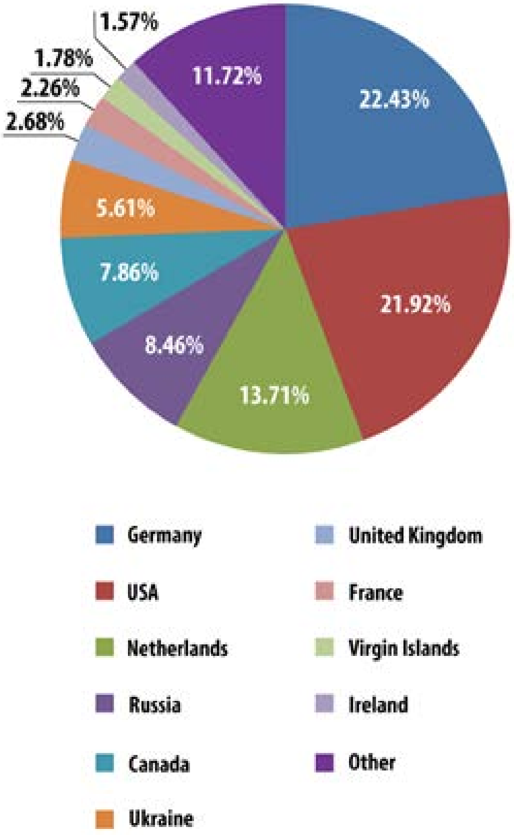
The Trojan.JS.Small.aq verdict is in twentieth place. This is assigned to a script that a malicious browser extension inserts in web pages of specific sites in order to display intrusive advertising.

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 antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host might become a source of one or more web attacks.

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

In Q2 2014, Kaspersky Lab solutions blocked 354,453,992 attacks launched from web resources located in various countries around the world. 88.3% of the online resources used to spread malicious programs are located in 10 countries. This is 4.9 percentage points more than in the previous quarter.



The distribution of online resources seeded with malicious programs in Q2 2014

The Top 10 rating of countries where online resources are seeded with malware remained largely unchanged from the previous quarter although there was some movement within that group. Germany rose from fourth to first place: its share increased by almost 12 percentage points. Russia dropped from second to fourth following a decline in its share of 2.5 percentage points. Canada climbed from tenth to fifth after its contribution grew by 6.29 percentage points.

COUNTRIES WHERE USERS FACE THE GREATEST RISK OF ONLINE INFECTION

In order to assess in which countries users face cyber threats most often, 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 in which computers work in different countries.

	COUNTRY*	% OF UNIQUE USERS **
1	Russia	46.53%
2	Kazakhstan	45.35%
3	Armenia	42.26%
4	Ukraine	41.11%
5	Azerbaijan	40.94%
6	Vietnam	39.59%
7	Belorussia	37.71%
8	Moldova	36.65%
9	Mongolia	33.86%
10	Kyrgyzstan	33.71%
11	Algeria	32.62%
12	Tajikistan	32.44%
13	Georgia	31.38%
14	Croatia	29.46%
15	Turkey	29.31%
16	Uzbekistan	29.20%
17	Qatar	28.76%
18	Tunisia	28.67%
19	Iran	28.35%
20	Spain	28.05%

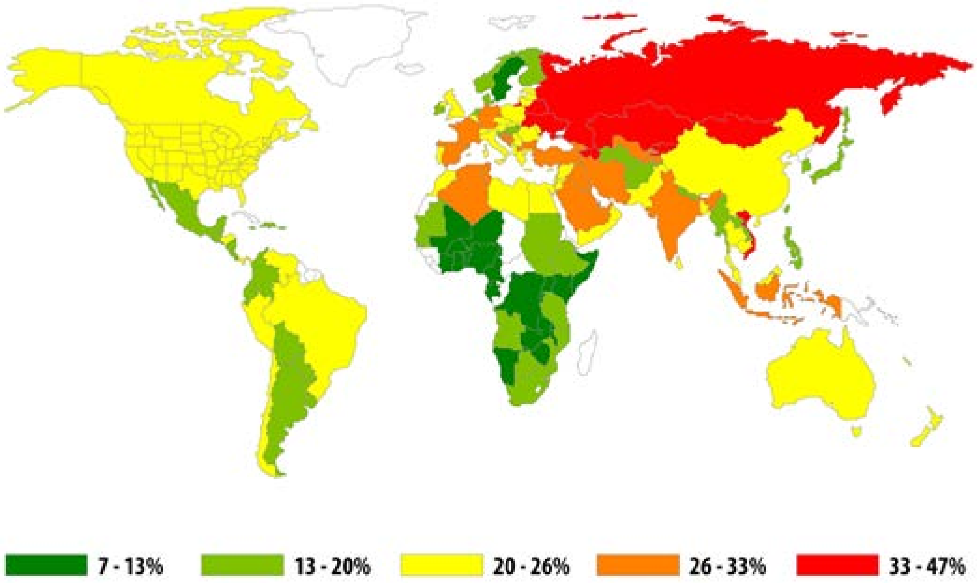
These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

** 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.*

In Q2 2014, Vietnam was replaced at the top of the rating by Russia. Tunisia (18th place) and Iran (19th place) were newcomers to the rating. Lithuania and Greece dropped out of the Top 20.

The countries with the safest online surfing environments are Singapore (10.4%), Sweden (12.8%), Japan (13.3%), Finland (16.3%), South Africa (16.9%), Ecuador (17.1%), Norway (17.5%), the Netherlands (17.5%), Hong Kong (17.7%) and Argentina (17.9%).



On average, 29.5% of computers connected to the Internet were subjected to at least one web attack during the past three months.

LOCAL THREATS

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

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

In Q2 2014, Kaspersky Lab's antivirus solutions successfully blocked 528,799,591 malware attacks on user computers. In these incidents, a total of 114,984,065 unique malicious and potentially unwanted objects were detected.

THE TOP 20 MALICIOUS OBJECTS DETECTED ON USER COMPUTERS

	NAME*	% OF UNIQUE ATTACKED USERS **
1	DangerousObject.Multi.Generic	17.69%
2	Trojan.Win32.Generic	15.59%
3	AdWare.Win32.Agent.ahbx	14.81%
4	Adware.Win32.Amonetize.heur	13.31%
5	Trojan.Win32.AutoRun.gen	6.13%
6	Worm.VBS.Dinihou.r	5.95%
7	Virus.Win32.Sality.gen	4.94%
8	AdWare.Win32.BetterSurf.b	4.29%
9	AdWare.Win32.Yotoon.heur	4.01%
10	AdWare.Win32.Agent.aknu	3.64%
11	AdWare.Win32.Agent.aljb	3.57%
12	Worm.Win32.Debris.a	3.29%
13	AdWare.Win32.Skyli.a	2.90%
14	Trojan.Win32.Starter.lgb	2.74%
15	AdWare.Win32.Agent.heur	2.64%
16	AdWare.Win32.Agent.aljt	2.30%

17	Trojan.Win32.AntiFW.b	2.27%
18	AdWare.JS.MultiPlug.c	2.21%
19	Worm.Script.Generic	1.99%
20	Virus.Win32.Nimnul.a	1.89%

** 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 that have 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.*

This ranking usually includes verdicts given to adware programs, worms spreading on removable media, and viruses.

The proportion of viruses in this Top 20 continues to decline slowly, but steadily. In Q2 2014, viruses were represented by the verdicts Virus.Win32.Sality.gen and Virus.Win32.Nimnul.a, with a total share of 6.83%. In Q1 2014, that figure was 8%.

COUNTRIES WHERE USERS FACE THE HIGHEST RISK OF LOCAL INFECTION

	COUNTRY	% UNIQUE USERS*
1	Vietnam	58.42%
2	Mongolia	55.02%
3	Algeria	52.05%
4	Yemen	51.65%
5	Bangladesh	51.12%
6	Pakistan	50.69%
7	Nepal	50.36%
8	Afghanistan	50.06%
9	Iraq	49.92%
10	Egypt	49.59%

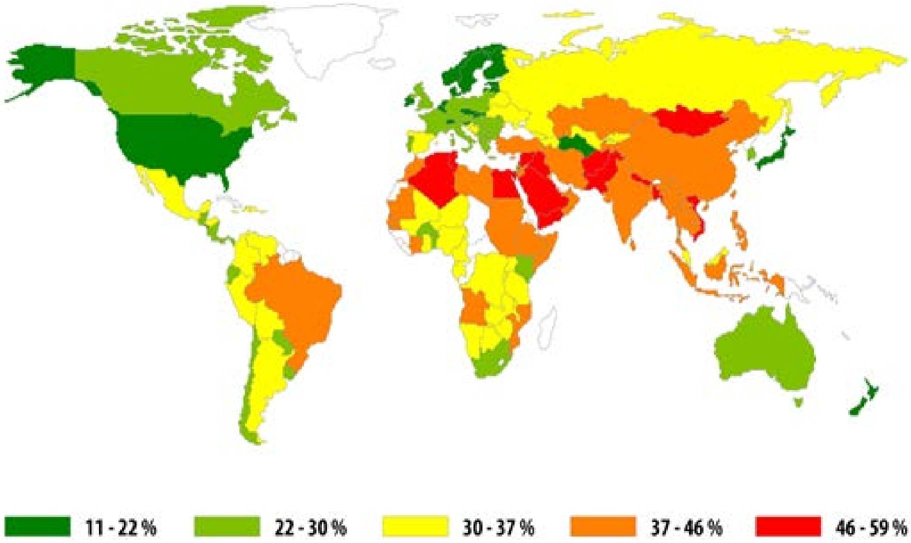
11	Tunisia	46.75%
12	Syria	46.29%
13	Saudi Arabia	46.01%
14	Ethiopia	45.94%
15	Iran	45.40%
16	Laos	45.20%
17	Turkey	44.98%
18	India	44.73%
19	Cambodia	44.53%
20	Djibouti	44.52%

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

** 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 20 in this category continues to be dominated by countries in Africa, the Middle East, and South East Asia. Vietnam ranks first, as was the case in Q1 2014, while Mongolia remains in second. Nepal fell to seventh place. Saudi Arabia, Ethiopia, and Turkey are new entries in this ranking. Morocco, Myanmar and Sudan dropped out of the top 20.



The safest countries in terms of local infection risks are: Japan (11%), Sweden (13.8%), Denmark (15.3%), Finland (16.4%), Singapore (16.8%), the Netherlands (17.1%), the Czech Republic (18.3%), Norway (19.1%) and Hong Kong (19.2%).

An average of 32.8% of computers were subjected to at least one local threat during the past year.