# IT THREAT EVOLUTION Q3 2014

DAVID EMM

MARIA GARNAEVA

VICTOR CHEBYSHEV

ROMAN UNUCHEK

DENIS MAKRUSHIN

ANTON IVANOV

KASPERSKY lab

# CONTENTS

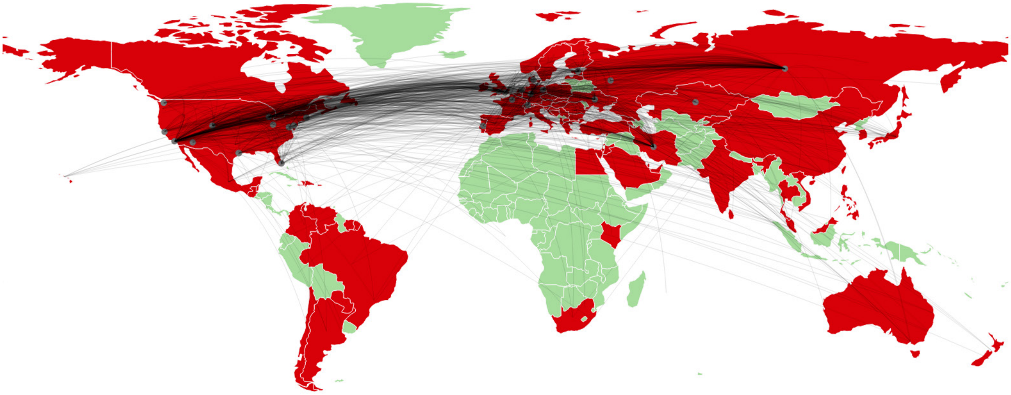
# OVERVIEW

## TARGETED ATTACKS AND MALWARE CAMPAIGNS

### ON THE TRAIL OF THE YETI

In July we published our in-depth analysis into a targeted attack campaign that we dubbed 'Crouching Yeti'. This campaign is also known as 'Energetic Bear'.

This campaign, which has been 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 organisations – mostly in the United States, Spain, Japan, Germany, France, Italy, Turkey, Ireland, Poland and China.



The list of victims suggests that the attackers behind Crouching Yeti are pursuing strategic targets. Nevertheless, the attackers have also shown an interest in not-so-obvious institutions too.

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 organisations and steal confidential data, including intellectual property and other strategic information. 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. First, they use a legitimate software installer, re-packaged to include a malicious DLL file. Such modified self-extracting archive files could be uploaded directly to a compromised server, or they could be sent directly to someone within the target organisation by e-mail. Second, they use spear-phishing to deliver a malicious XDP (XML Data Package) file containing a Flash exploit (CVE-2011-0611). Third, they use watering-hole attacks. Hacked web sites use several exploits (CVE-2013-2465, CVE-2013-1347, and CVE-2012-1723) to redirect visitors to malicious JAR or HTML files hosted on other sites maintained by the attackers. The term 'watering-hole' is applied to a web site that is likely to be visited by potential victims. These web sites are compromised in advance by the attackers – the site is injected to install malware on the computers of anyone visiting the compromised site.

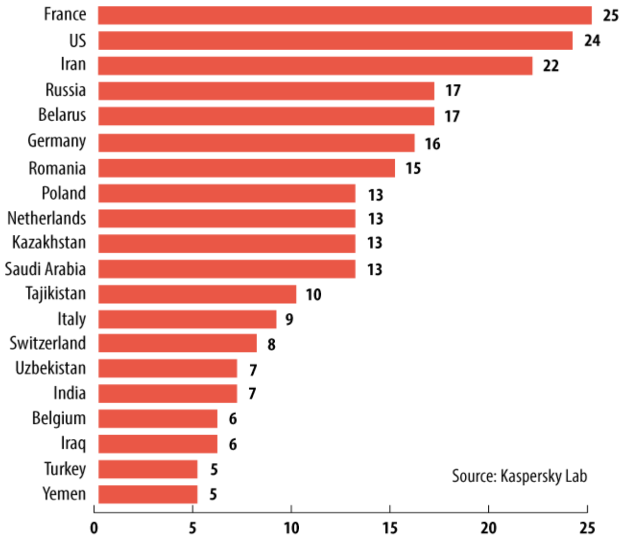
One malicious program used by the attackers, the Havex Trojan, includes special modules to collect data from specific industrial IT environments. The first of these is the OPC scanner module. This module is designed to collect the extremely detailed data about the OPC servers running in the local network. OPC (Object Linking and Embedding (OLE) for Process Control) servers are typically used where multiple industrial automation systems are operating. This module is accompanied by a network scanning tool. This module scans the local network, looks for all computers listening on ports related to OPC/SCADA (Supervisory Control and Data Acquisition) software, and tries to connect to such hosts in order to identify which potential OPC/SCADA system is running. It then transmits all the data it finds to the Command-and-Control (C2) servers used by the attackers to manage the campaign.

While analysing the code, we looked for clues that might point to the identity of the attackers.

A timestamp analysis of 154 files revealed that most of the samples were compiled between 06:00 and 16:00 UTC. This could match any country in Europe. We also looked at the language used by the attackers. The malware contains strings in English (written by non-native English speakers). There were also some clues pointing indicating possible French and Swedish speaker. But unlike several other researchers who looked at Crouching Yeti, we didn't find anything that would enable us to conclude with certainty that the attackers are of Russian origin. There's a lack of Cyrillic content (or transliteration) across the 200 malicious binaries and related operational content – in contrast to what we found when looking at earlier targeted attack campaigns, including Red October, MiniDuke, CosmicDuke, the Snake and TeamSpy.

## AN EPIC TALE OF CYBER-ESPIONAGE

For more than a year Kaspersky Lab has been researching a sophisticated cyber-espionage campaign that we call 'Epic Turla'. This campaign, which dates back to 2012, targets government institutions, embassies, military, research and educational organizations and pharmaceutical companies. Most of the victims are located in the Middle East and Europe, although we have seen victims elsewhere, including the United States. Altogether, we have found several hundred victim's IP addresses in more than 45 countries.



Source: Kaspersky Lab

*The Epic Turla Operation: distribution of the top 20 affected countries by victim IP*

When we published our initial research into this campaign, it was unclear how victims of the attack were becoming infected. In in our latest research, published in August, we outlined the infection mechanisms used by Epic Turla and how they fit within the structure of the overall campaign.

The attackers use social engineering tricks to infect their victims –specifically spear-phishing and watering-hole attacks.

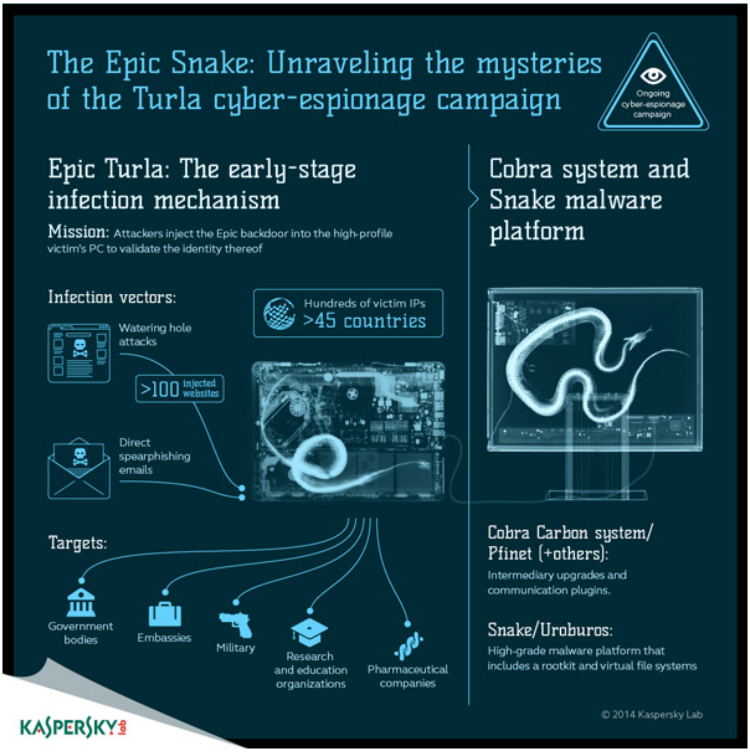
Some of the spear-phishing e-mails include zero-day exploits. The first of these, affecting Adobe Acrobat Reader (CVE-2013-3346), allows the attackers to arbitrarily execute code on the victim's computer. The second, a privilege escalation vulnerability in Windows XP and Windows Server 2003 (CVE-2013-5065), provides the Epic Turla backdoor with administrator rights on the victim's computer. In addition, the attackers trick their victims into running malware installers with an SCR extension – sometimes packed using RAR. When the unsuspecting victims open an infected file, a backdoor is installed on their computer, giving the attackers full control.

The cybercriminals behind Epic Turla also use watering-hole attacks that deploy a Java exploit (CVE-2012-1723), Adobe Flash exploits and Internet Explorer exploits. There are others that use social engineering to 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. We have seen more than 100 injected web sites. Unsurprisingly, the choice of web sites reflects the specific interests of the attackers (as well as the interests of the victims). For example, many infected Spanish web sites belong to local governments.

Once the computer is infected, the Epic Turla backdoor (known also as 'WorldCupSec', 'TadjMakhal', 'Wipbot' and 'Tadvig') immediately connects to the C2 server to send a pack containing the victim's system information. Based on the summary information sent to the C2 server, the attackers deliver pre-configured batch files containing a series of commands to be executed on the infected computer. The attackers also upload custom lateral movement tools (including a specific keylogger and RAR archiver), as well as standard utilities such as a DNS query tool from Microsoft.

Our analysis revealed that the Epic Turla backdoor is just the first stage of a wider infection process. It is used to deploy a more sophisticated backdoor known as the 'Cobra/Carbon system' (named 'Pfinet' by some anti-malware products). After some time, the attackers went further, using the Epic Turla implant to update the Carbon configuration file with a different set of C2 servers. 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.

Here's an overview of the whole Epic Turla cyber-espionage campaign:


The Epic Snake: Unraveling the mysteries of the Turla cyber-espionage campaign
Ongoing 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
Infection vectors:
Watering hole attacks
>100 injected websites
Direct spearphishing emails
Hundreds of victim IPs >45 countries
Targets:
Government bodies
Embassies
Military
Research and education organizations
Pharmaceutical companies
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
KASPERSKY lab

Attributing these attacks is always very difficult. However, some aspects of the code tell us something about the attackers. It's clear that they are not native English speakers. They commonly misspell words and phrases, such as:

- 'Password it's wrong!'
- 'File is not exists'
- 'File is exists for edit'

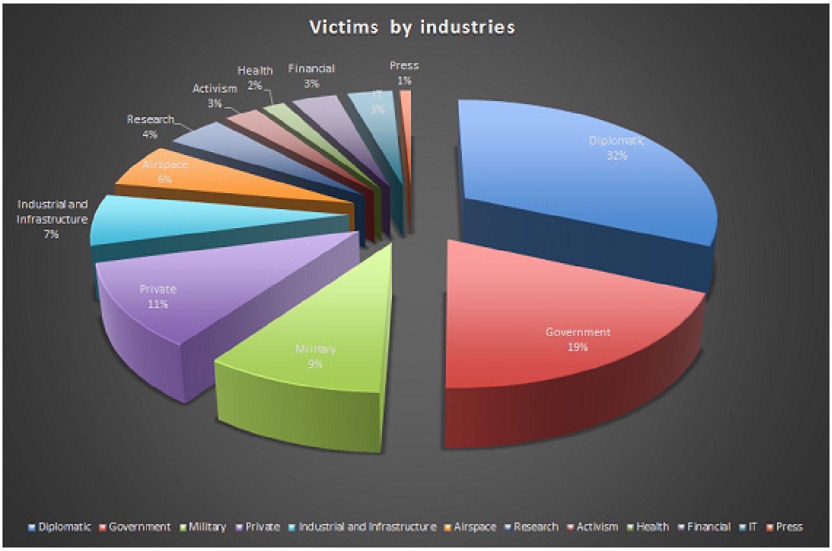
There are also other indicators that hint at the origin of the attackers. For example, some of the backdoors have been compiled on a system with the Russian language. In addition, the internal name of one of the Epic Turla backdoors is 'Zagruzchik.dll', which means 'bootloader' or 'load program' in Russian. Finally, the Epic Turla 'mother ship' control panel sets the code page to 1251, which is used for Cyrillic characters.

## NETTRAVELER GETS A BIRTHDAY MAKEOVER

We have discussed this targeted attack campaign, which has now been active for 10 years, on several occasions.

Earlier this year we observed an increase in the number of attacks on Uyghur and Tibetan activists, using an updated version of the NetTraveler backdoor. The attackers use spear-phishing e-mails to lure their victims: e-mails include a Microsoft Word document that contains the CVE-2012-0158 exploit. This drops the main module ('net.exe') onto the computer, which in turn installs a number of other files, including the main C2 module. This module is registered as a service ('Windowsupdata') by means of a Windows batch file called 'dot.bat'. The format of the malware configuration file has also been updated and it's clear that the attackers have taken steps to try and conceal the configuration (but the encryption they used is weak).

The focus of the attackers has changed over time. For much of its existence, the main targets of NetTraveler were diplomatic, government and military organisations. More recently, its cyber-espionage activities have focused more on organisations involved in space exploration, nano-technology, energy production, nuclear power, lasers, medicine and communications.



A focus on Uyghur and Tibetan activists remains a core part of the attackers' activities.

## THE SYRIAN MALWARE HOUSE OF CARDS

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. Kaspersky Lab’s Global Research and Analysis Team analysed the recent increase in malware activity in Syria.

The people behind these attacks use social engineering tricks to lure their victims into opening infected files. They use e-mail, Skype messages, Facebook posts and YouTube videos.

They use a variety of ‘hooks’ – preying on their victims’ trust in social networking forums, their curiosity about news related to the conflict in Syria, their fear of the government and their lack of technical awareness.

Examples include a disturbing video on YouTube showing injured victims of recent bombings that also invites people to download a malicious program from a public file-sharing web site. We also found a set of compressed files on a popular social networking site which, when extracted, revealed a database containing a list of activists and wanted individuals in Syria. The download link for this database application was included in the information section of a video published on 9 November 2013. The attackers also make use of fake security solutions to trick their victims – including a fake anti-virus program called ‘Ammazon Internet Security’ and a Trojanised version of a legitimate network monitoring tool, Total Network Monitor. They don’t just spread fake security applications – we’ve also seen fake versions of the Whatsapp and Viber instant messaging apps.

The attackers use a number of well-known remote administration tools (RATs), malicious programs that allow a remote ‘operator’ to control a compromised computer as if they had physical access to it. These tools are widely used in cybercrime attacks of all kinds and even in some state-sponsored attacks. The RATs used in this campaign include ‘ShadowTech’, ‘Xtreme’, ‘NjRAT’,’ Bitcoment’, ‘Dark Comet’ and ‘Blackshades’. The malware is used to monitor the victims, to gather information and, in some cases, to try and shut down their operations.

The victims of these attacks are not only located in Syria. The attacks have also been seen in Turkey, Saudi Arabia, Lebanon, Palestine, 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.

The number of attacks has grown markedly over the last year. In addition, it's clear that the groups involved in the attacks are well organised. 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.

You can find our full report on this malware here.

## MALWARE STORIES

### SHYLOCK – A POUND OF *YOUR* FLESH

Earlier this year Kaspersky Lab contributed to an alliance of law enforcement and industry organizations, co-ordinated by the United Kingdom National Crime Agency (NCA), to disrupt the infrastructure behind the Shylock Trojan. This partnership shows how global cooperation on cybercrime can produce positive results.

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 such as Zeus, SpyEye and Carberp, 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.

The Trojan injects fake data entry fields into web pages when they load on the victim's browser. Victims are typically tricked into running the malware by clicking on malicious links. Shylock then seeks to access funds held in business or personal bank accounts, and transfers them to accounts under the control of the attackers.

The focus of the cybercriminals changed over time. When Shylock first appeared, it was aimed mainly at victims in the UK and, during the course of 2012, spread to other countries in Europe and to the United States. By the end of 2013, the cybercriminals were more focused on developing markets such as Brazil, Russia and Vietnam. You can find more information, including data on the spread of the malware, here.

All banking Trojans, Shylock included, target bank customers, hoping to take advantage of what is often the least protected element of any financial transaction – i.e. the human. That's why it's important that security starts at home – we all need to secure our computers effectively.

## YOUR MONEY OR YOUR FILE(S)!

The number of ransomware programs has been growing in recent years – not all of them focused on computers running Windows. Some, including the ones targeting Android devices, tend to simply block access to the device and demand a ransom payment in order to unlock the device.

But many ransomware programs go further than this, encrypting data on the victim's computer. One recent example is ZeroLocker.

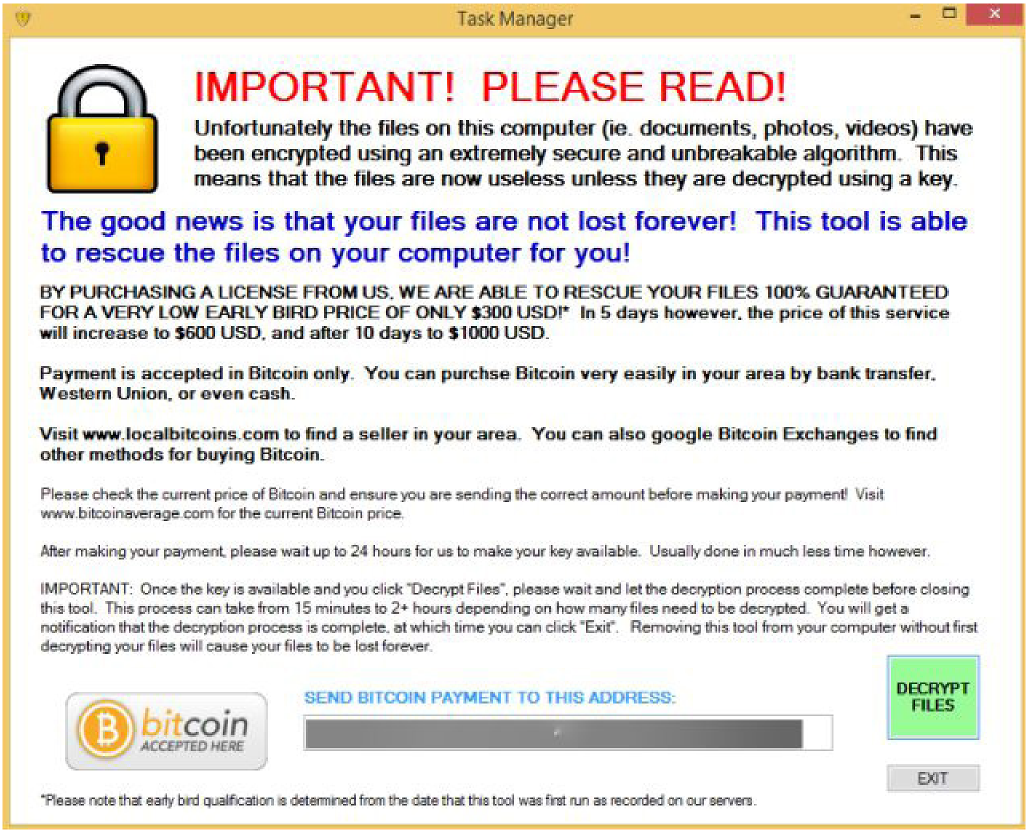
Unlike most ransomware programs, which encrypt a pre-defined list of file types, ZeroLocker encrypts nearly all the files on the victim's computer and adds the extension '.encrypt' to encrypted files. ZeroLocker doesn't encrypt files located in directories containing the words 'Windows', 'WINDOWS', 'Program Files', 'ZeroLocker' or 'Destroy' and doesn't encrypt files larger than 20MB in size.

ZeroLocker generates a 160-bit AES key to encrypt all files. The key space is somewhat limited because of the way the key is generated, but it's still large enough to make general brute –forcing unfeasible. After encrypting files, the malware runs the 'cipher.exe' utility to remove all unused data from the drive, making file recovery much more difficult. The encryption key, together with a CRC32 of the computer's MAC address, and the associated Bitcoin wallet, is sent to the server used by the cybercriminals. There's an indication that the C2 configuration contains some errors that might prevent successful decryption – another reason why paying the ransom is a bad idea.

The encryption key, along with other information, is sent by means of a GET request, rather than a POST. This results in a 404 error on the server. This could mean that the server isn't storing the information, suggesting that the victims will probably not get their files back, even if they pay the ransom.

Several other URLs that the malware tries to get also result in 404 errors. This suggests that the operation may still be in its infancy. If and when these errors are fixed, we may see ZeroLocker deployed on a larger scale.

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.



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

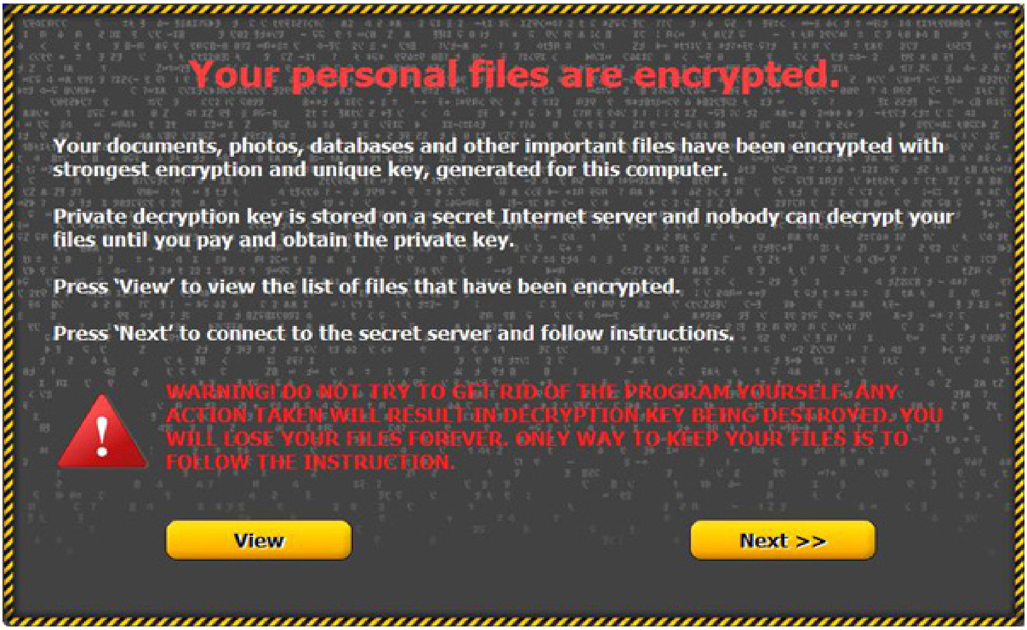
IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS: [redacted]

*Please note that early bird qualfication is determined from the date that this tool was first run as recorded on our servers.

There's a Bitcoin wallet hard-coded inside the binary, but the malware tries to fetch a new wallet address from the C2 server, probably to make it harder to trace how successful the operation is and where the money goes. None of the Bitcoin wallet addresses we looked at had any transactions associated with them. Since the C2 server provides Bitcoin wallet information, it's possible that the attackers are able to use a unique wallet for each victim.

Another ransomware program that we analysed recently is Onion. This malicious program uses the tried-and-tested method used by other recent ransomware programs – encrypting the victim's data and demanding a ransom payment in Bitcoin.



Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

However, it also breaks new ground. First, Onion uses the anonymous Tor network to hide its C2 servers. This makes it harder to track down the cybercriminals behind the malware. Other malware has used Tor in the past, but this Trojan stands apart because it 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. Further details can be found in our report on the Onion Trojan.

These things combined make the Onion Trojan technically advance and very dangerous.

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.

## WHY ONE OF OUR SECURITY RESEARCHERS HACKED HIS OWN HOME

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 as hackers and researchers probe the technologies integrated into cars, hotels, home alarm systems and refrigerators and more – looking for vulnerabilities .

Sometimes the Internet of things can seem remote. But it's often closer than we think. The modern home today is likely to have a handful of devices connected to the local network that aren't traditional computers, tablets or cellphones – devices such as a smart TV, a printer, a gaming console, a network storage device or some kind of media player/satellite receiver.

One of our security researchers, David Jacoby, investigated his own home, to determine whether it was really cyber-secure. He looked at several devices, including network-attached storage (NAS) devices, smart TV, router and satellite receiver, to see if they were vulnerable to attack. The results were striking. David found 14 vulnerabilities in the network-attached storage devices, one in the smart TV and several potentially hidden remote control functions in the router.

The most severe vulnerabilities were found in the network-attached storage devices. Several of them would allow an attacker to remotely execute system commands with the highest administrative privileges. The tested devices also had weak default passwords, stored passwords in plain text and included configuration files with the wrong permissions. The default administrator password for one of the devices contained just one digit!  And another device even shared the entire configuration file, containing encrypted passwords, with everyone on the network!

David was also able to upload a file to an area of storage memory that's inaccessible to an ordinary user.  If an attacker uploaded a malicious file to this area, the compromised device would become a source of infection for other devices connecting to this NAS – a home PC, for example – and could even serve as a DDoS (Distributed Denial of Service) bot in a botnet. On top of this, the only way to delete this file was by using the same vulnerability –even for a technical specialist this is no simple task.

When David looked at his smart TV, he discovered that communication between the TV and the TV vendor's servers isn't encrypted – potentially opening the way for a Man-in-the-Middle attack that could result in an unsuspecting consumer transferring money to fraudsters while trying to buy content via the TV.  As a proof of concept exercise, David was able to replace one of the icons on the smart TV graphic interface with a picture.  Normally the widgets and thumbnails are downloaded from the TV vendor's servers but since the connection isn't encrypted, this information could be modified by a third party.  He also discovered that the smart TV is able to execute Java code that, in combination with the ability to intercept the exchange of traffic between the TV and Internet, could result in exploit-driven malicious attacks.

The DSL router, used to provide wireless Internet access for all other home devices, contained several dangerous features hidden from its owner.  Some of these hidden functions could potentially give an attacker remote access to any device in a private network.  What's more, sections of the router's web interface called 'Web Cameras', 'Telephony Expert Configure', 'Access Control', 'WAN-Sensing' and 'Update' are 'invisible' and cannot be adjusted by the owner of the device.  They can only be accessed by exploiting a rather generic vulnerability that makes it possible to travel between sections of the interface (these are basically web pages, each with its own alphanumeric address) by brute-forcing the numbers at the end of the address.  Originally these functions were implemented for the convenience of the owner of the device:  the remote access function makes it fast and easy for an ISP (Internet Service Provider) to troubleshoot and resolve technical problems on the device. But this convenient feature could become a security risk if the controls fell into the wrong hands.

In line with our policy of responsible disclosure, Kaspersky Lab hasn't disclosed the names of vendors whose products were investigated as part of this research. All vendors were informed about the existence of the vulnerabilities and Kaspersky Lab specialists work closely with vendors to help them remediate any vulnerabilities discovered.

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).

You can find some advice on how to reduce the risk of attack in this summary of David Jacoby's article.

## WEB SECURITY AND DATA BREACHES: SHELLSHOCK

In September, the information security world faced a red alert following the discovery of the 'Bash' vulnerability (also known as 'ShellShock'). Bash, a Unix shell written in 1989, is the default shell on Linux and Mac OS X. The flaw (CVE-2014-6271) allows an attacker to remotely attach a malicious file to a variable that is executed when the Bash command interpreter is invoked. The high impact of this vulnerability, coupled with the ease with which it can be exploited, make it very powerful. Some have compared it to the 'Heartbleed' vulnerability. However, Bash is much easier to exploit than Heartbleed and, whereas Heartbleed only allowed an attacker to steal data from the memory of a vulnerable computer, Shellshock could provide full system control.

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 is possible that the vulnerability could have an impact on a Windows-based infrastructure.

Nor is the problem 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 – as discussed above.

You can find guidance on how to update vulnerable systems here.

# STATISTICS

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

## Q3 IN FIGURES

> According to KSN data, Kaspersky Lab products detected and neutralized a total of 1,325,106,041 threats in the third quarter of 2014.

> Kaspersky Lab solutions repelled 367,431,148 attacks launched from online resources located all over the world

> Kaspersky Lab's web antivirus detected 26,641,747 unique malicious objects: scripts, web pages, exploits, executable files, etc.

> 107,215,793 unique URLs were recognized as malicious by web antivirus components.

> 33% of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US.

> Kaspersky Lab's antivirus solutions detected a total of 116,710,804 unique malicious and potentially unwanted objects.

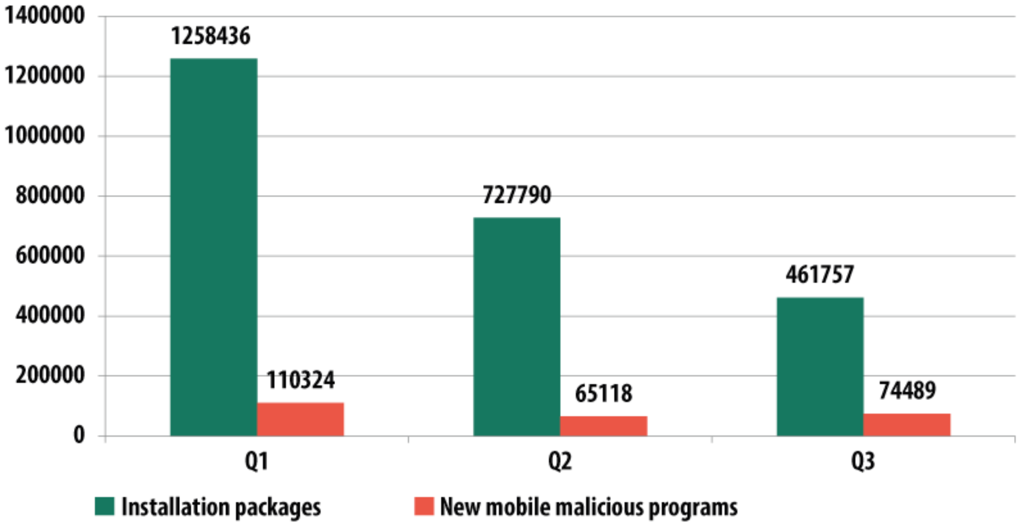
> Kaspersky Lab mobile security products detected

- 461,757 installation packages;
- 74,489 new malicious mobile programs;
- 7,010 mobile banking Trojans.

## MOBILE THREATS

In Q3 2014 Kaspersky Lab mobile security products detected 74,489 new malicious mobile programs, 14.4% more than in the second quarter.

At the same time, fewer installation packages were detected.

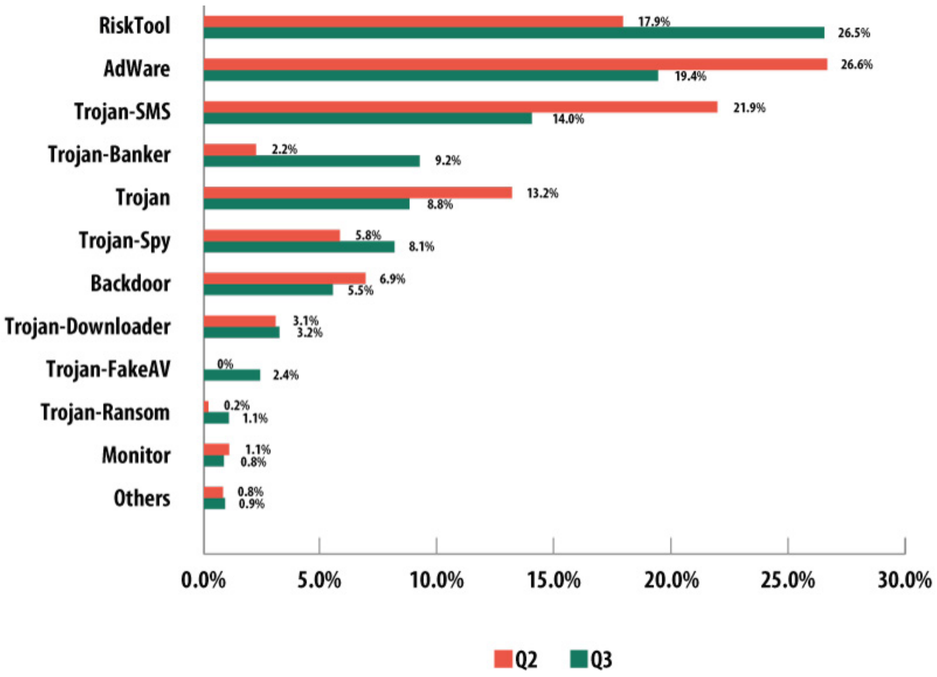


*Number of installation packages and new malicious mobile programs detected in Q1-Q3 2014*

In the first half of 2014, there were a little more than 11 malicious installation packages on the average associated with each malicious program but in Q3 there were 6.2 million.

Using multiple installation packages for one mobile malicious program is typical of SMS-Trojan distributors. For example, attackers have used up to 70,000 packets for one version of Stealer.a. The decrease in the number of malicious installation packages is probably related to the reduced proportion of this malware in the flow of new mobile malicious programs decreased (see below).

## DISTRIBUTION OF MOBILE THREATS BY TYPE



*Distribution of mobile threats by type in Q2 and Q3 2014*

The rating of malware objects for mobile devices for the third quarter of 2014 was headed by RiskTool. This claimed 26.5% of detections, a rise of 8.6 percentage points. These are legal applications that are potentially dangerous for the user – if they are used carelessly, or manipulated by a cybercriminal they could lead to financial losses.

Second came Adware, potentially unwanted advertising applications (19.4%); their contribution went down 7.9 pp.

SMS-Trojans were in 3rd place: their share declined by 7.2pp from the previous quarter.

In Q3, while Adware and SMS-Trojans were less widely seen, we observed a sharp rise in the percentage of banking Trojans: their share in the flow of mobile malware has risen from 2.2% to 9.2% which placed this category 4th in the rating.

## TOP 20 MALICIOUS MOBILE PROGRAMS

| | NAME | % OF ATTACKS* |
|---|---|---|
| 1 | Trojan-SMS.AndroidOS.Stealer.a | 15.63% |
| 2 | RiskTool.AndroidOS.SMSreg.gc | 14.17% |
| 3 | AdWare.AndroidOS.Viser.a | 10.76% |
| 4 | Trojan-SMS.AndroidOS.FakeInst.fb | 7.35% |
| 5 | RiskTool.AndroidOS.CallPay.a | 4.95% |
| 6 | Exploit.AndroidOS.Lotoor.be | 3.97% |
| 7 | DangerousObject.Multi.Generic | 3.94% |
| 8 | RiskTool.AndroidOS.MimobSMS.a | 3.94% |
| 9 | Trojan-SMS.AndroidOS.Agent.ao | 2.78% |
| 10 | AdWare.AndroidOS.Ganlet.a | 2.51% |
| 11 | Trojan-SMS.AndroidOS.OpFake.a | 2.50% |
| 12 | RiskTool.AndroidOS.SMSreg.de | 2.36% |
| 13 | Trojan-SMS.AndroidOS.FakeInst.ff | 2.14% |
| 14 | Trojan-SMS.AndroidOS.Podec.a | 2.05% |
| 15 | Trojan-SMS.AndroidOS.Erop.a | 1.53% |
| 16 | RiskTool.AndroidOS.NeoSMS.a | 1.50% |
| 17 | Trojan.AndroidOS.Agent.p | 1.47% |
| 18 | Trojan-SMS.AndroidOS.OpFake.bo | 1.29% |
| 19 | RiskTool.AndroidOS.SMSreg.hg | 1.19% |
| 20 | Trojan-Ransom.AndroidOS.Small.e | 1.17% |

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

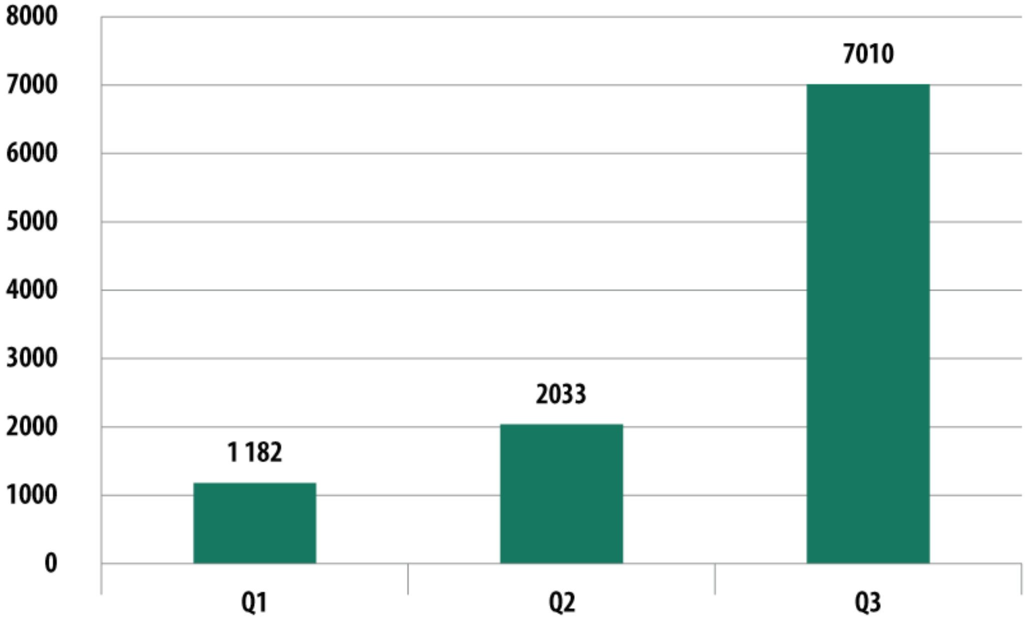
The top 20 is no longer so heavily dominated by SMS Trojans: in Q2 2014 these malicious programs occupied 15 places in the rating while in Q3 there were only 8. Trojan-SMS.AndroidOS.Stealer.a topped the previous quarter's rating with 25.42% of all attacks but in Q3 it accounted for only 16.63% of attacks.

RiskTool representatives occupied 6 positions in the Top 20, with RiskTool.AndroidOS.SMSreg.gc (14.17%) in second place.

7th came DangerousObject.Multi.Generic (3.94%), demonstrating how new malicious applications are detected by Kaspersky Security Network cloud technologies that enable our product to quickly respond to new unknown threats.

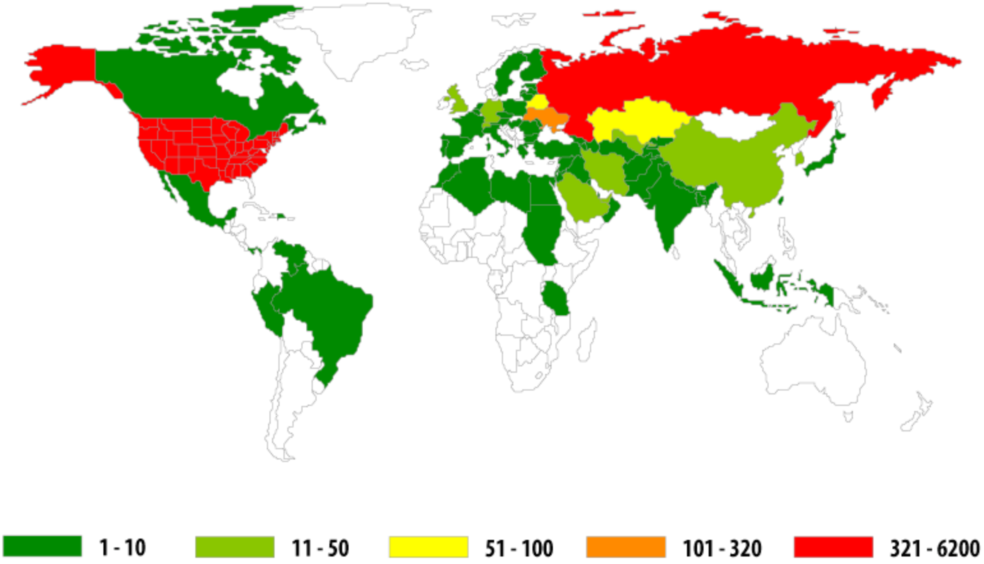
## MOBILE BANKING TROJANS

In the third quarter, we detected 7010 mobile banking Trojans, 3.4 times more than last quarter.



*Number of mobile banking Trojans detected, Q1-Q3 2014*

The number of countries attacked by banking Trojans also increased: in Q2 mobile banking Trojan attacks were detected in 31 countries while in Q3 there were 70.



*The geography of mobile banking threats, Q3 2014 (the number of attacked users)*

## THE TOP 10 COUNTRIES ATTACKED BY BANKING TROJANS

| | COUNTRY | % OF ALL ATTACKS* |
|---|---|---|
| 1 | Russia | 83.85% |
| 2 | USA | 7.09% |
| 3 | Ukraine | 1.79% |
| 4 | Belarus | 1.18% |
| 5 | Kazakhstan | 0.92% |
| 6 | Republic of Korea | 0.68% |
| 7 | Germany | 0.62% |
| 8 | China | 0.50% |
| 9 | UK | 0.50% |
| 10 | Saudi Arabia | 0.35% |

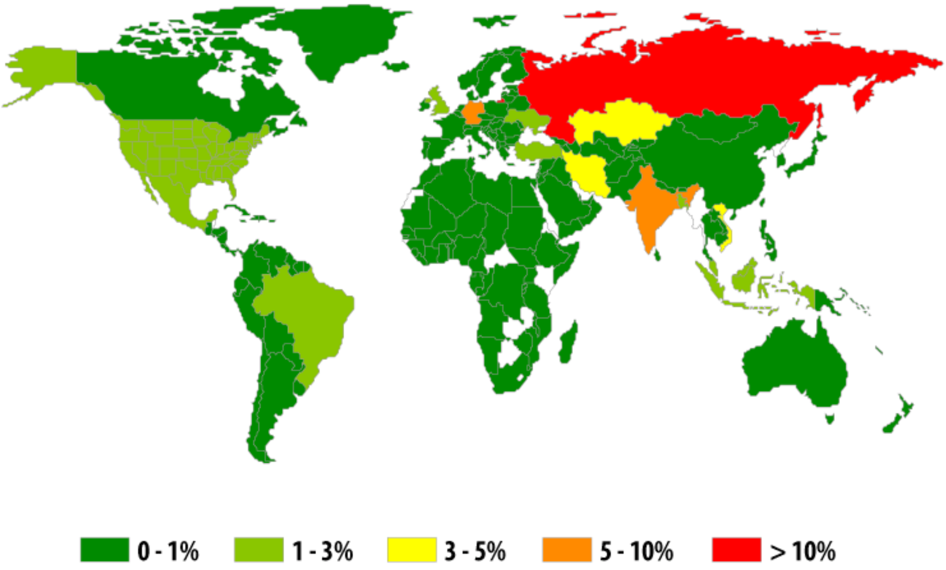
** The percentage of users attacked per country*

Italy dropped out of the Top 10 while Saudi Arabia appeared in 10th place.

Russia maintained its traditional lead here, although it was 7.85pp on before. At the same time the contribution of the other Top 10 members grew slightly: mobile cybercriminals are gradually extending their area of activity.

## THE GEOGRAPHY OF MOBILE THREATS

In Q3 2014 mobile malicious attacks were detected at least once in 205 countries.



*The geography of infection by mobile banking Trojans, Q3 2014 (the percentage of all attacked users)*

### THE TOP 10 OF ATTACKED COUNTRIES

| | COUNTRY | % OF ATTACKS* |
|---|---|---|
| 1 | Russia | 44.0% |
| 2 | India | 7.6% |
| 3 | Germany | 5.6% |
| 4 | Iran | 3.4% |

| | | |
|---|---|---|
| 5 | Vietnam | 3.1% |
| 6 | Kazakhstan | 3.1% |
| 7 | Ukraine | 2.7% |
| 8 | Malaysia | 1.9% |
| 9 | Brazil | 1.7% |
| 10 | USA | 1.7% |

** The percentage of users attacked per country*

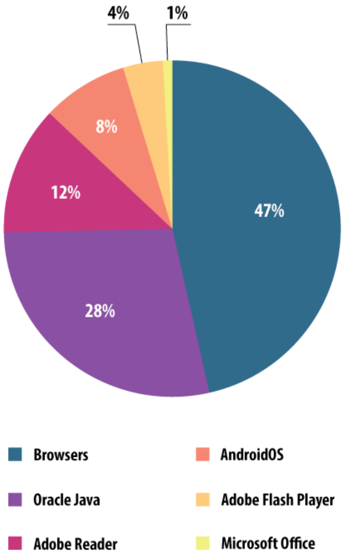
Russia remained the most heavily targeted nation with 44% of all attacks. India (7.6%) returned to second place. For the first time in 2014 Iran (3.4%) and the USA (1.7%) entered the Top 10 while Poland, France, Spain and Mexico were the Q3 outsiders.

## 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 Internet attacks and when compromising local applications, including those installed on mobile devices.

Of all registered attempts to use vulnerabilities, 47% 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 although no new Java vulnerabilities have been made public for almost a year. In Q3 of this year, 28% of attempts to use vulnerabilities targeted Java; in the first quarter the figure was 29%.



*The distribution of web-exploits used by fraudsters, by type of application attacked, Q3 2014*

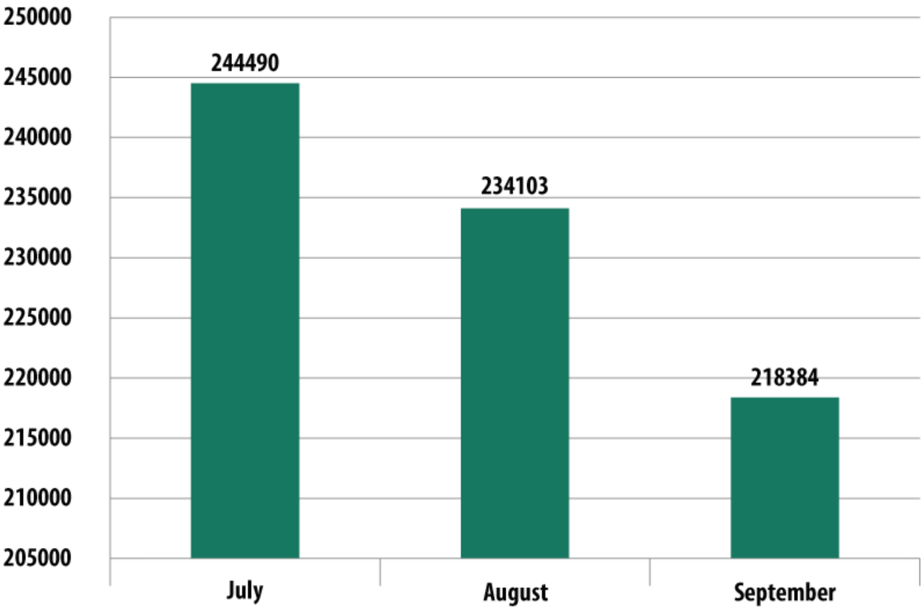
Next come Adobe Reader exploits (12%). These vulnerabilities are also exploited in drive-by attacks via the Internet and PDF exploits feature in many exploit packs.

## 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.

### ONLINE THREATS IN THE BANKING SECTOR

During the reporting period, Kaspersky Lab solutions blocked 696,977 attacks that attempted to launch malware capable of stealing money from online banking accounts. This figure represents a 24.9% decrease compared to Q2 (927,568).

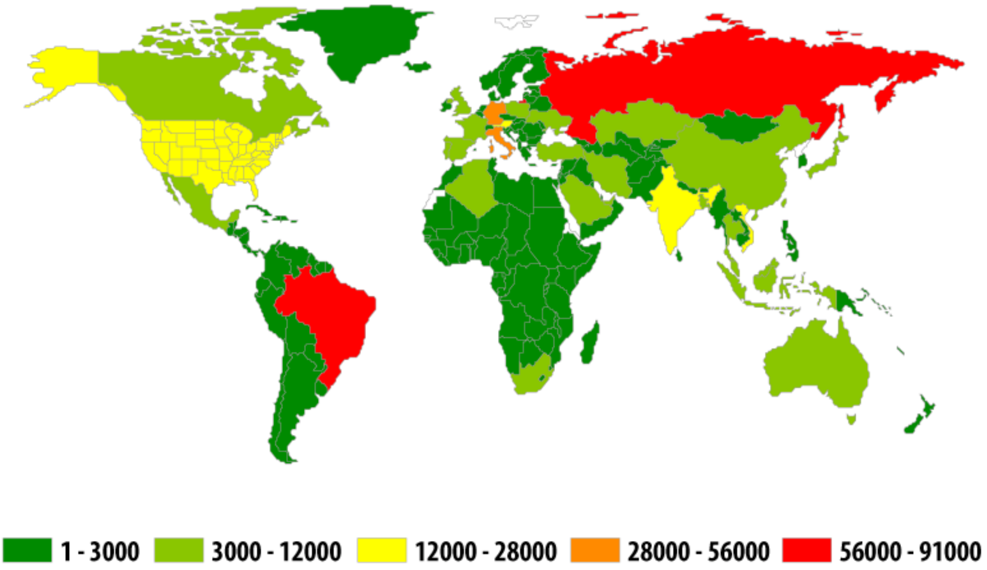


*The number of computers attacked by financial malware, Q3 2014*

The number of attacks gradually declined throughout the quarter: in June 244,490 attacks were blocked while in September this figure was 218,384 (-11%).

A total of 2,466,952 notifications of malicious activity by programs designed to steal money via online access to bank accounts were registered by Kaspersky Lab security solutions in Q3 2014.

### THE GEOGRAPHY OF ATTACKS



*The geography of banking malware attacks in Q2 2014 (by number of attacked users in the country)*

### THE TOP 10 COUNTRIES BY THE NUMBER OF ATTACKED USERS:

| COUNTRIES | NUMBER OF USERS |
|---|---|
| Brazil | 90176 |
| Russia | 57729 |
| Germany | 55225 |
| Italy | 32529 |
| India | 24975 |

| | |
|---|---|
| USA | 22340 |
| Austria | 22013 |
| Vietnam | 13495 |
| UK | 11095 |
| China | 9060 |

Brazil remained the country where users are most often attacked by banking malware, even if its share was down one third. Russia stayed in second place. Italy dropped to 4th position while Germany rose to 3rd place: the number of attacked users in this country grew by 1.5 times.

### THE TOP 10 BANKING MALWARE FAMILIES

The table below shows the programs most commonly used to attack online banking users in Q3 2014, based on the number of reported infection attempts:

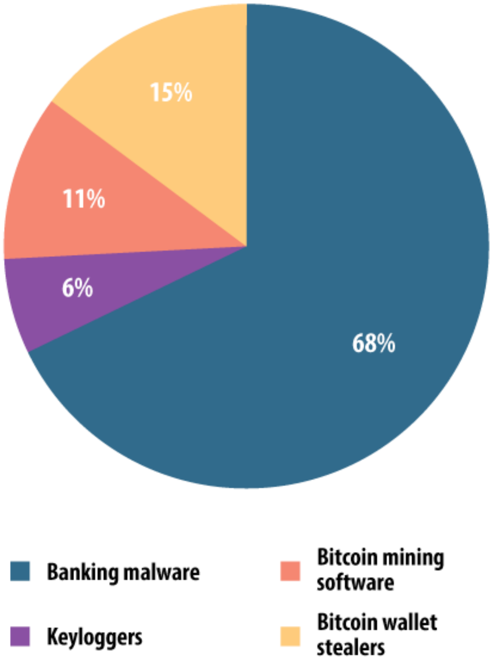
| VERDICT | NUMBER OF NOTIFICATIONS | NUMBER OF USERS |
|---|---|---|
| Trojan-Spy.Win32.Zbot | 1381762 | 285559 |
| Trojan-Banker.Win32.ChePro | 322928 | 92415 |
| Trojan-Banker.Win32.Shiotob | 123150 | 24839 |
| Trojan-Banker.Win32.Agent | 49563 | 23943 |
| Trojan-Banker.HTML.PayPal | 117692 | 21138 |
| Trojan-Spy.Win32.SpyEyes | 73496 | 19113 |
| Trojan-Banker.Win32.Lohmys | 47188 | 16619 |
| Trojan-Banker.Win32.Banker | 39892 | 12673 |
| Trojan-Banker.Win32.Banbra | 20563 | 9646 |
| Backdoor.Win32.Sinowal | 18921 | 8189 |

Zeus (Trojan-Spy.Win32.Zbot) remained the most widespread banking Trojan although the number of attacks involving this malicious the program, as well as the number of attacked users, nearly halved compared with the previous quarter.

In Q3, 3rd place was occupied by Trojan-Banker.Win32.Shiotob. This malicious program is most often spread via spam messages and is designed to monitor traffic in order to intercept payment data. Nine out of 10 malware families represented in the table work by injecting random HTML code into the web page displayed by the browser and intercepting any payment data entered by the user in the original or inserted web forms.

Financial threats are not restricted to malware that attacks online banking services.

Bitcoin wallet theft was the second most frequently used method of stealing e-money: its popularity grew from 8% in the previous quarter to 15% in Q3. Yet another threat related to crypto currency is Bitcoin mining software (11%) which uses computing resources to generate bitcoins.



*Distribution of attacks targeting user money by malware type, Q3 2014*

## THE TOP 20 MALICIOUS OBJECTS DETECTED ONLINE

In the third quarter of 2014, Kaspersky Lab's web antivirus detected 26,641,747 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 96.2% of all attacks on the Internet.

## THE TOP 20 MALICIOUS OBJECTS DETECTED ONLINE

| | NAME* | % OF ALL ATTACKS** |
|---|---|---|
| 1 | Malicious URL | 59.83% |
| 2 | AdWare.Script.Generic | 14.46% |
| 3 | Trojan.Script.Generic | 13.13% |
| 4 | Trojan.Script.Iframer | 1.77% |
| 5 | AdWare.Win32.Agent.fflm | 1.23% |
| 6 | Trojan-Downloader.Script.Generic | 1.02% |
| 7 | AdWare.Win32.Agent.allm | 1.02% |
| 8 | AdWare.JS.Agent.ao | 0.78% |
| 9 | AdWare.JS.Agent.an | 0.55% |
| 10 | AdWare.Win32.Agent.aiyc | 0.32% |
| 11 | AdWare.Win32.OutBrowse.g | 0.32% |
| 12 | Trojan.Win32.Generic | 0.30% |
| 13 | AdWare.Win32.Amonetize.bcw | 0.23% |
| 14 | AdWare.Win32.Amonetize.cmg | 0.18% |
| 15 | AdWare.Win32.Yotoon.heur | 0.18% |
| 16 | Trojan-Downloader.Win32.Generic | 0.15% |
| 17 | AdWare.Win32.Amonetize.cmd | 0,14% |
| 18 | Trojan-Dropper.Win32.Agent.lefs | 0.12% |
| 19 | AdWare.Win32.Linkun.j | 0.11% |
| 20 | AdWare.Win32.Amonetize.aik | 0.09% |

** 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.*

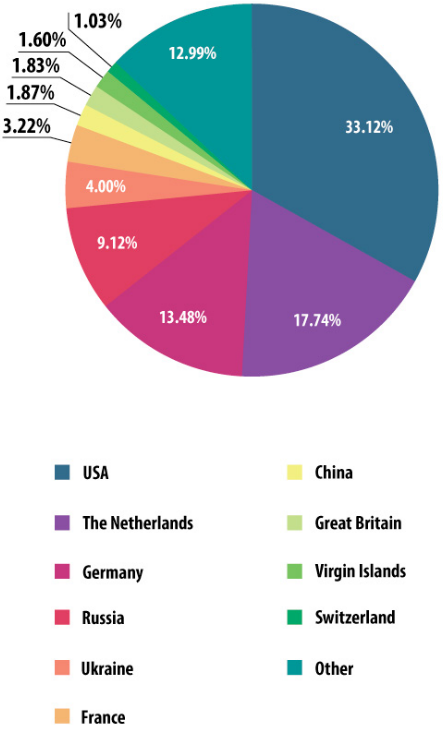
As is often the case, the Top 20 is largely made up of objects used in drive-by attacks, as well as adware programs. 59.8% of all verdicts fell on links from these black lists.

## 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 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 domain names are matched up against actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In Q3 2014, Kaspersky Lab solutions blocked 367,431,148 attacks launched from web resources located in various countries around the world. 87% of the online resources used to spread malicious programs are located in 10 countries. This is 1.3 percentage points less than in the previous quarter.



*The distribution of online resources seeded with malicious programs in Q3 2014*

The Top 10 rating of countries where online resources are seeded with malware saw major changes from the previous quarter: Canada (-7 pp) and Ireland  (-0.7 pp) dropped out of the Top 10. China reentered the Top 10 with 1.87% and settled in 7th. Switzerland (1.03%) was Q3's other newcomer.

The most significant changes happened to the USA, which climbed to the top of the rating with a +11.2pp swing, and Germany (-9 pp), which dropped from 1st to 3rd place.

## 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 | 46.68% |
| 2 | Kazakhstan | 45.92% |
| 3 | Azerbaijan | 43.50% |
| 4 | Armenia | 41.64% |
| 5 | Ukraine | 40.70% |
| 6 | Iran | 39.91% |
| 7 | Vietnam | 38.55% |
| 8 | Belarus | 38.08% |
| 9 | Moldova | 36.64% |
| 10 | Algeria | 36.05% |
| 11 | Tadjikistan | 36.05% |
| 12 | Kyrgyzstan | 33.59% |
| 13 | Mongolia | 33.59% |
| 14 | Qatar | 30.84% |
| 15 | Uzbekistan | 29.22% |
| 16 | Georgia | 29.17% |
| 17 | Turkey | 28.91% |
| 18 | UAE | 28.76% |
| 19 | Indonesia | 28.59% |
| 20 | Germany | 28.36% |

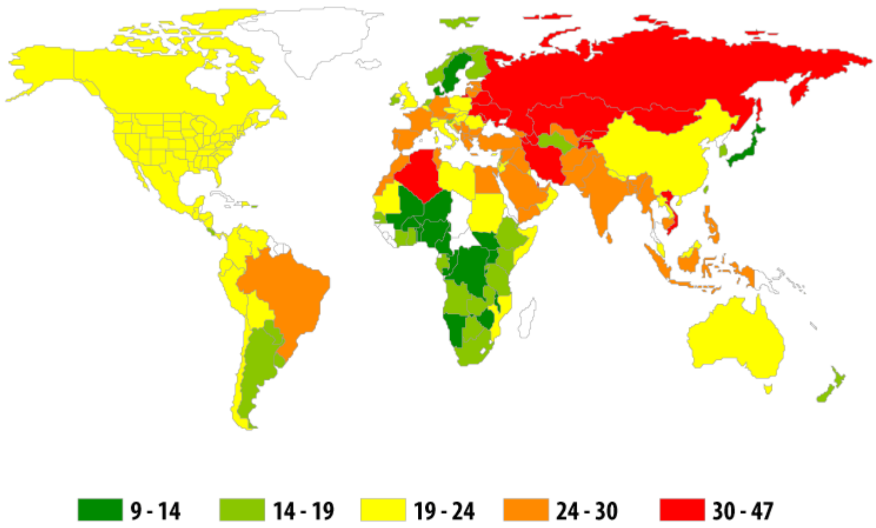
*These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.*

**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 the third quarter of 2014 Croatia, Tunisia and Spain dropped out of the Top 20. The newcomers of the rating were UAE (28.76%), Indonesia (28.59%) and Germany (28.36%) which occupied the last three positions in the chart.

The countries with the safest online surfing environments were Sweden (12.4%), Denmark (13.2%), Japan (13.3%), South Africa (16.0%), Finland (16.1%), and the Netherlands (16.6%).



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 antivirus scans of files on the hard drive at the moment they are created or accessed, and the results of scanning various removable data storages.

In Q3 2014, Kaspersky Lab's antivirus solutions detected 116,710,804 unique malicious and potentially unwanted objects.

## THE TOP 20 MALICIOUS OBJECTS DETECTED ON USER COMPUTERS

| | NAME* | % OF UNIQUE ATTACKED USERS** |
|---|---|---|
| 1 | Trojan.Win32.Generic | 18.95% |
| 2 | DangerousObject.Multi.Generic | 18.39% |
| 3 | AdWare.MSIL.Kranet.heur | 11.61% |
| 4 | AdWare.Win32.Agent.ahbx | 5.77% |
| 5 | Trojan.Win32.AutoRun.gen | 4.81% |
| 6 | AdWare.Win32.Kranet.heur | 4.68% |
| 7 | AdWare.NSIS.Zaitu.heur | 4.51% |
| 8 | Worm.VBS.Dinihou.r | 4.51% |
| 9 | Virus.Win32.Sality.gen | 4.08% |
| 10 | AdWare.Win32.Yotoon.abs | 4.03% |
| 11 | AdWare.Win32.IBryte.dolh | 3.14% |
| 12 | AdWare.Win32.Agent.aljt | 3.12% |
| 13 | AdWare.Win32.Agent.allm | 3.11% |
| 14 | AdWare.Win32.Yotoon.heur | 3.10% |
| 15 | Adware.Win32.Amonetize.heur | 2.86% |
| 16 | AdWare.Win32.Agent.heur | 2.80% |
| 17 | WebToolbar.JS.Condonit.a | 2.59% |
| 18 | Worm.Win32.Debris.a | 2.56% |
| 19 | AdWare.Win32.Kranet.c | 2.55% |
| 20 | Trojan.Script.Generic | 2.51% |

**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: in Q3 they occupied thirteen places in the Top 20.

Worms distributed via removable media were 8th and 18th in the ranking.

Viruses were represented by only one verdict Virus.Win32.Sality.gen which came 9th in the Top 20.

Q3 2014 saw a considerable increase in the number of Kaspersky Lab's file antivirus detections of adware programs and components that actively participate in distributing these programs and evading antivirus detection.

## COUNTRIES WHERE USERS FACE THE HIGHEST RISK OF LOCAL INFECTION

| | COUNTRY* | % OF UNIQUE USERS** |
|---|---|---|
| 1 | Vietnam | 61.89% |
| 2 | Bangladesh | 55.01% |
| 3 | Mongolia | 54.13% |
| 4 | Nepal | 53.08% |
| 5 | Algeria | 51.71% |
| 6 | Cambodia | 51.26% |
| 7 | Afghanistan | 50.59% |
| 8 | Laos | 50.55% |
| 9 | Yemen | 50.38% |
| 10 | Pakistan | 50.35% |
| 11 | Egypt | 49.65% |
| 12 | India | 49.44% |
| 13 | Iraq | 49.33% |
| 14 | Iran | 48.85% |
| 15 | Ethiopia | 47.87% |
| 16 | Myanmar | 46.71% |
| 17 | Sri Lanka | 46.67% |
| 18 | Syria | 46.24% |
| 19 | Qatar | 46.03% |
| 20 | Tunisia | 45.36% |

*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.*

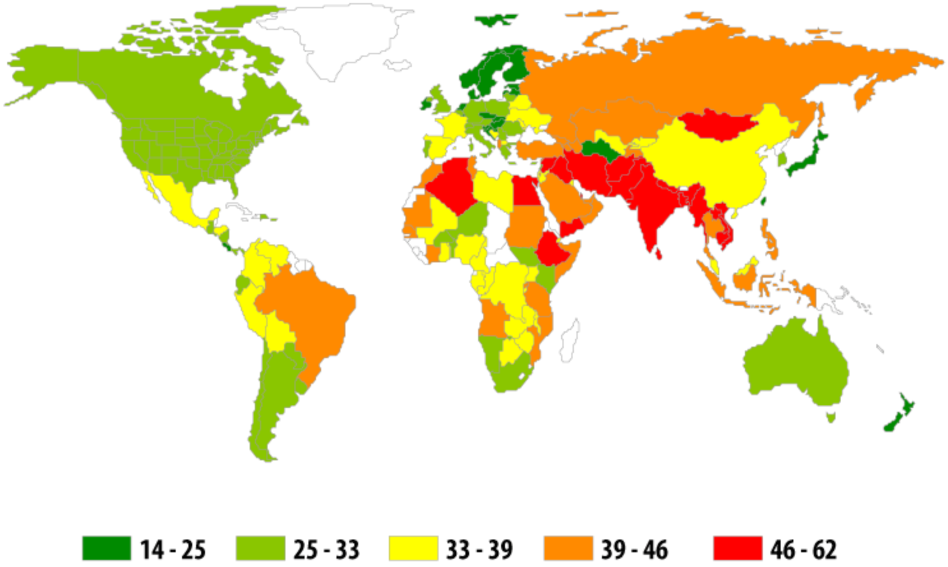
***The percentage of unique users in the country with computers that blocked local threats as a percentage of all unique users of Kaspersky Lab products.*

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 Q2 2014 (61.89%).

Mongolia (54.13%) moved down one step to third place, giving way to Bangladesh which ranked second with 55.01% of unique users in the country with computers that blocked local threats.

Qatar (46.03%) was Q3's newcomer. Myanmar (46.71%) and Sri Lanka (46.67%) reentered the Top 20 while Saudi Arabia, Turkey and Djibouti left the rating.

In the third quarter of 2014 local threats were detected on 44.4% of computers in Russia.



The safest countries in terms of local infection risks are: Japan (15%), Sweden (16.4%), Denmark (16.5%), Finland (18%), and Singapore (19.7%).

An average of 37.2% of computers faced at least one local threat during the quarter, which is 4.4 pp more than in Q2 2014.