KASPERSKY SECURITY BULLETIN 2013

KASPERSKY LAB
GLOBAL RESEARCH
AND ANALYSIS TEAM
(GREAT)

KASPERSKY lab

CONTENTS

MALWARE EVOLUTION. THE TOP SECURITY STORIES OF 2013 4

> 1. New “old” cyber-espionage campaigns 5
> 2. Cyber-mercenaries: a new emerging trend 8
> 3. Hacktivism and leaks 9
> 4. Ransomware 10
> 5. Mobile malware and app store (in)security 11
> 6. Watering-hole attacks 13
> 7. The need to re-forge the weakest link in the security chain 14
> 8. Privacy loss: Lavabit, Silent Circle, NSA and the loss of trust 15
> 9. Vulnerabilities and zero-days 17
> 10. The ups and downs of cryptocurrencies — how the Bitcoins rule the world 18
> Conclusions and looking forward: “2014, the year of trust” 20

CORPORATE THREATS 22

> The motives 23
> Target organizations 24
> Preparing an attack 24
> Intrusion techniques 25
> Technologies 27
> What gets stolen 29
> The rise of the cybermercenaries 30
> Consequences of high-profile disclosures 30

OVERALL STATISTICS FOR 2013 32

> 2013 in figures 32
> Mobile Threats 33
> Vulnerable applications exploited by cybercriminals 37
> Online threats (attacks via the web) 38
> Local threats 45

FORECASTS **50**
> Mobile threats 50
> Attacks on Bitcoin 50
> The problems of protecting privacy 51
> Attacks on cloud storage facilities 51
> Attacks on software developers 52
> Cyber-mercenaries 52
> Fragmentation of the Internet 53
> The pyramid of cyber-threats 54

MALWARE EVOLUTION. THE TOP SECURITY STORIES OF 2013

Costin Raiu, David Emm

Once again, it's time for us to deliver our customary retrospective of the key events that have defined the threat landscape in 2013. Let's start by looking back at the things we thought would shape the year ahead, based on the trends we observed in the previous year.

> Targeted attacks and cyber-espionage

> The onward march of 'hacktivism'

> Nation-state-sponsored cyber-attacks

> The use of legal surveillance tools

> Cloudy with a chance of malware

> Vulnerabilities and exploits

> Cyber extortion

> Who do you trust?

> Mac OS malware

> Mobile malware

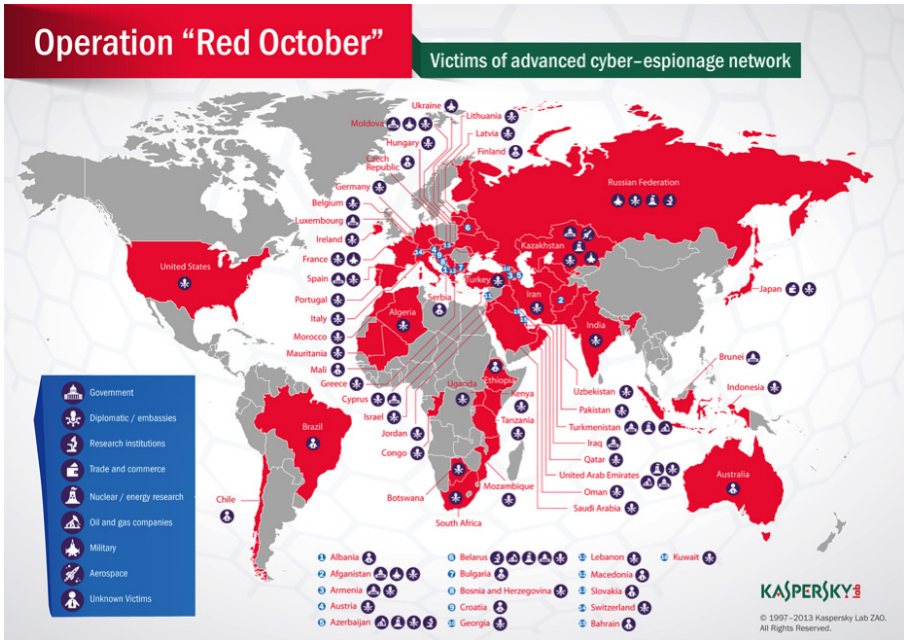
> Dude, where's my privacy?!

If we now focus on the highlights on 2013, you can judge for yourself how well we did in predicting the future.

Here's our shortlist of the top security stories of 2013.

1. NEW "OLD" CYBER-ESPIONAGE CAMPAIGNS

In any retrospective of top stories of 2013 you might expect to read about incidents that occurred this year. But it's not quite that straightforward when looking at targeted attacks. Often, the roots of the attack reach back in time from the point at which they become known and are analyzed and reported. You might remember, for example, that this was the case with Stuxnet — the more we analyzed it, the further back we had to place its date of origin. It's true also of some of the major cyber-espionage campaigns we've seen this year.



RedOctober victims map

Red October is a cyber-espionage campaign that has affected hundreds of victims around the world — including diplomatic and government agencies, research institutions, energy and nuclear groups and trade and aerospace organizations. The malware is highly sophisticated — among other things, it includes a 'resurrection mode' that enables the malware to re-infect computers. The code is highly modular, allowing the attackers to tweak the code easily for each specific target. Interestingly, Red October didn't just harvest information from traditional endpoints, but also from mobile devices connected to the victims' networks — a clear recognition by cybercriminals that mobile devices are

a core component of today's business environment and contain valuable information. We published the results of our analysis in January 2013, but it's clear that the campaign dates back to 2008.

In February, we published our analysis of MiniDuke, designed to steal data from government agencies and research institutions. Our analysis uncovered 59 high profile victim organizations in 23 countries, including Ukraine, Belgium, Portugal, Romania, the Czech Republic, Ireland, Hungary and the US. Like many targeted attacks, MiniDuke combined the use of 'old school' social engineering tactics with sophisticated techniques. For example, MiniDuke included the first exploit capable of bypassing the Adobe Acrobat Reader sandbox. In addition, compromised endpoints received instructions from the command-and-control server via pre-defined Twitter accounts (and used Google search as a fallback method).

We learned of a wave of attacks in March that targeted top politicians and human rights activists in CIS countries and Eastern Europe. The attackers used the TeamViewer remote administration tool to control the computers of their victims, so the operation became known as 'TeamSpy'. The purpose of the attacks was to gather information from compromised computers. Though not as sophisticated as Red October, NetTraveler and other campaigns, this campaign was nevertheless successful — indicating that not all successful targeted attacks need to build code from scratch.

NetTraveler (also known as "NetFile"), which we announced in June, is another threat that, at the time of discovery, had long been active — in this case, since 2004.

This campaign was designed to steal data relating to space exploration, nano-technology, energy production, nuclear power, lasers, medicine and telecommunications. NetTraveler was successfully used to compromise more than 350 organizations across 40 countries — including Mongolia, Russia, India, Kazakhstan, Kyrgyzstan, China, Tajikistan, South Korea, Spain and Germany. The targets were from state and private sector organizations that included government agencies, embassies, oil and gas companies, research centers, military contractors and activists.

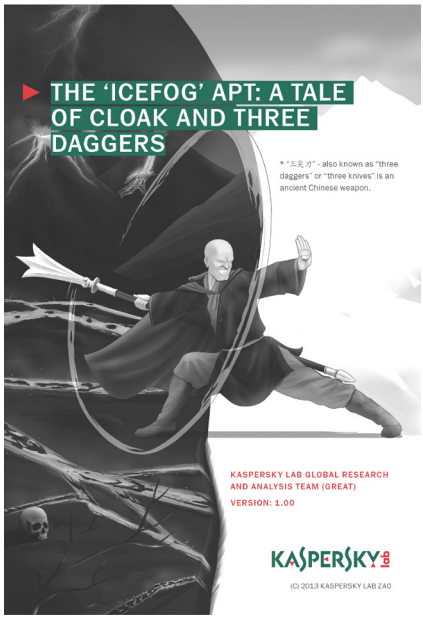
If your organization has never suffered an attack, it's easy to tell yourself that 'it won't happen to me', or to imagine that most of what we hear about malware is just hype. It's easy to read the headlines and draw the conclusion that targeted attacks are a problem only for large organizations. But not all attacks involve high profile targets, or those involved in 'critical infrastructure' projects. In truth, any organization can become a victim. Every organization holds data that could be of value to cybercriminals, or they can be used as a 'stepping-stones' to reach other companies. This point was amply illustrated by the Winnti and Icefog attacks.

In April we published a report on the cybercrime group 'Winnti'. This group, active since 2009, focuses on stealing digital certificates signed by legitimate software vendors, as well as intellectual property theft (including theft of source code for online game projects). The Trojan used by the group is a DLL library compiled for 64-bit Windows environments. It uses a properly signed driver and operates as a fully-functional Remote Administration Tool — giving the attackers full control over the compromised computer. In total, we found that more than 30 companies in the online gaming industry fell victim to the group's activities — mostly in South-East Asia, but also affecting companies in Germany, the US, Japan, China, Russia, Brazil, Peru, Belarus and the UK. This group is still active.

The Icefog attacks that we announced in September (discussed in the next section of this report) were focused on the supply chain and, as well assensitive data from within the target networks, also gathered e-mail and network credentials to resources outside the target networks.

2. CYBER-MERCENARIES: A NEW EMERGING TREND

On the face of it, Icefog seems to be a targeted attack like any other. It's a cyber-espionage campaign, active since 2011, focused mainly in South Korea, Taiwan and Japan, but also in the US, Europe and China. Similarly, the attackers use spear-phishing e-mails — containing either attachments or links to malicious web sites – to distribute the malware to their victims. As with any such attack, it's difficult to say for sure how many victims there have been, but we have seen several dozen victims running Windows and more than 350 running Mac OSX (most of the latter are in China).



However, there are some key distinctions from other attacks that we've discussed already. First, Icefog is part of an emerging trend that we're seeing – attacks by small groups of cyber-mercenaries who conduct small hit-and-run attacks. Second, the attackers specifically targeted the supply chain – their would-be victims include government institutions, military contractors, maritime and ship-building groups, telecommunications operators, satellite operators, industrial and high technology companies and mass media. Third, their campaigns rely on custom-made cyber-espionage tools for Windows and Mac OSX and they directly control the compromised computers; and in addition to Icefog, we have noticed that they use backdoors and other malicious tools for lateral movement within the target organizations and for exfiltration of data.

The Chinese group 'Hidden Lynx', whose activities were reported by researchers at Symantec in September , fall into the same category – 'guns-for-hire' performing attacks to order using cutting-edge custom tools. This group was responsible for, among others, an attack on Bit9 earlier this year.

Going forward, we predict that more of these groups will appear as an underground black market for "APT" services begins to emerge.

3. HACKTIVISM AND LEAKS

Stealing money – either by directly accessing bank accounts or by stealing confidential data – is not the only motive behind security breaches. They can also be launched as a form of political or social protest, or to undermine the reputation of the company being targeted. The fact is that the Internet pervades nearly every aspect of life today. For those with the relevant skills, it can be easier to launch an attack on a government or commercial web site than it is to co-ordinate a real-world protest or demonstration.

One of the weapons of choice for those who have an ax to grind is the DDoS (Distributed Denial of Service) attack. One of the biggest such attacks in history (some would say *the* biggest) was directed at Spamhaus in March. It's estimated that, at its peak, the attack reached a throughput of 300gbps. One organization suspected of launching it was called Cyberbunker. The conflict between this organization and Spamhaus dates back to 2011, but reached a peak when Cyberbunker was blacklisted by Spamhaus a few weeks before the incident. The owner of Cyberbunker denied responsibility, but claimed to be a spokesperson for those behind it. The attack was certainly launched by someone capable of generating huge amounts of traffic. To mitigate this, Spamhaus was forced to move to CloudFlare, a hosting and service provider known for dissipating large DDoS attacks. While some of the 'it's the end of the world as we know it' headlines might have overstated the effects of this event, the incident highlights the impact that a determined attacker can have.

While the attack on Spamhaus appears to have been an isolated incident, ongoing hacktivist activities by groups who have been active for some time have continued this year. This includes the 'Anonymous' group. This year it has claimed responsibility for attacks on the US Department of Justice, MIT (Massachusetts Institute of Technology) and the web sites of various governments – including Poland, Greece, Singapore, Indonesia and Australia (the last two incidents involved an exchange between Anonymous groups in their respective countries). The group also claims to have hacked the wi-fi network of the British parliament during protests in Parliament Square during the first week of November.

Those claiming to be part of the 'Syrian Electronic Army' (supporters of Syria's president, Bashar-al-Assad) have also been active throughout the year. In April, they claimed responsibility for hacking the Twitter account of Associated Press and sending a false tweet reporting explosions at the White House – which wiped $136 billion off the DOW. In July the group compromised the Gmail accounts of three White House employees and the Twitter account of Thomson Reuters.

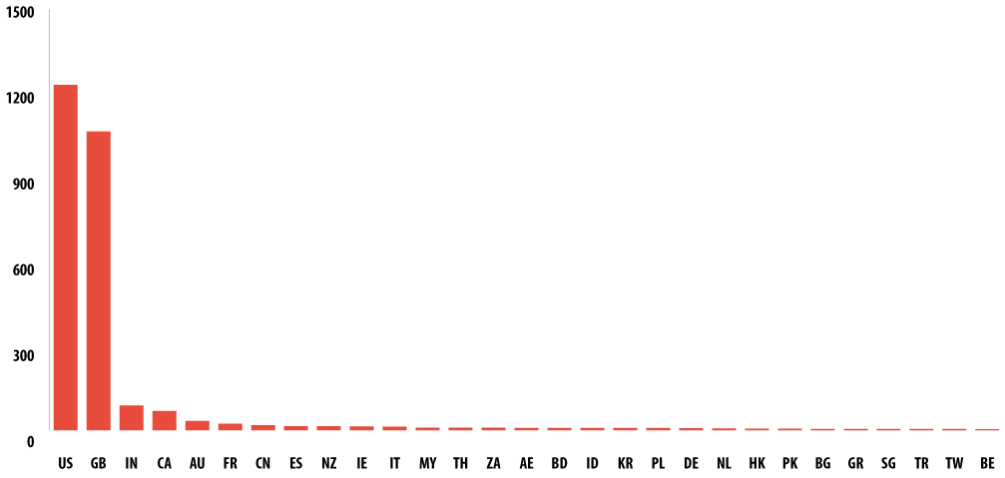
It's clear that our dependence on technology, together with the huge processing power built into today's computers, means that we're potentially vulnerable to attack by groups of people with diverse motives. So it's unlikely that we'll see an end to the activities of hacktivists or anyone else choosing to launch attacks on organizations of all kinds.

4. RANSOMWARE

The methods used by cybercriminals to make money from their victims are not always subtle. 'Ransomware' programs operate like a computer-specific 'denial-of-service' attack – they block access to a computer's file system, or they encrypt data files stored on the computer. The modus operandi can vary. In areas where levels of software piracy are high, for example, ransomware Trojans may claim to have identified unlicensed software on the victim's computer and demand payment to regain access to the computer. Elsewhere, they purport to be pop-up messages from police agencies claiming to have found child pornography or other illegal content on the computer and demanding a fine. In other cases, there's no subterfuge at all – they simply encrypt the data and warn you that you must pay in order to recover your data. This was the case with the Cryptolocker Trojan that we analyzed in October.

Cryptolocker downloads an RSA public key from its command-and-control (C2) server. A unique key is created for each new victim and only the authors have access to the decryption keys. To connect to the C2 server, Cryptolocker uses a domain generation algorithm that products 1,000 unique candidate domain names every day. The cybercriminals give their victims only three days to pay up – and they reinforce their message with scary wallpaper that warns them that if they don't pay up in time their data will be gone forever. They accept different forms of payment, including Bitcoin. The most affected countries are the UK and US, distantly followed by India, Canada and Australia.

In this case there's little difficulty in removing the malicious application, or even rebuilding the infected computer. But the data may potentially be lost forever. Sometimes in the past, we've been able decrypt the hijacked data. But that isn't always possible if the encryption is very strong, as with some of the Gpcode variants. It is also true of Cryptolocker. That's why it's essential that individuals and businesses always make regular backups. If data is lost – for any reason – an inconvenience doesn't turn into a disaster.



Victims count per country – TOP 30

Cryptolocker wasn't the only extortion program that made the headlines this year. In June we saw an Android app called 'Free Calls Update' – a fake anti-malware program designed to scare its victims into paying money to remove non-existent malware from the device. Once installed, the app tries to gain administrator rights: this allows it to turn wi-fi and 3G on and off; and prevents the victim from simply removing the app. The installation file is deleted afterwards, in a ploy to evade detection by any legitimate anti-malware program that may be installed. The app pretends to identify malware and prompts the victim to buy a license for the full version to remove the malware. While the app is browsing, it displays a warning that malware is trying to steal pornographic content from the phone.

5. MOBILE MALWARE AND APP STORE (IN)SECURITY

The explosive growth in mobile malware that began in 2011 has continued this year. There are now more than 148,427 mobile malware modifications in 777 families. The vast majority of it, as in recent years, is focused on Android – 98.05% of mobile malware found this year targets this platform. This is no surprise. This platform ticks all the boxes for cybercriminals: it's widely-used, it's easy to develop for and people using Android devices are able to download programs (including malware) from wherever they choose. This last factor is important: cybercriminals are able to exploit the fact that people download apps from Google Play, from other marketplaces, or from other web sites. It's also what makes it possible for cybercriminals to create their own fake web

sites that masquerade as legitimate stores. For this reason, there is unlikely to be any slowdown in development of malicious apps for Android.

The malware targeting mobile devices mirrors the malware commonly found on infected desktops and laptops – backdoors, Trojans and Trojan-Spies. The one exception is SMS-Trojan programs – a category exclusive to smartphones.

The threat isn't just growing in volume. We're seeing increased complexity too. In June we analyzed the most sophisticated mobile malware Trojan we've seen to-date, a Trojan named Obad. This threat is multi-functional: it sends messages to premium rate numbers, downloads and installs other malware, uses Bluetooth to send itself to other devices and remotely performs commands at the console. This Trojan is also very complex. The code is heavily obfuscated and it exploits three previously unpublished vulnerabilities. Not least among these is one that enables the Trojan to gain extended Device Administrator privileges – but without it being listed on the device as one of the programs that has these rights. This makes it impossible for the victim to simply remove the malware from the device. It also allows the Trojan to block the screen. It does this for no more than 10 seconds, but that's enough for the Trojan to send itself (and other malware) to nearby devices – a trick designed to prevent the victim from seeing the Trojan's activities.

Obad also uses multiple methods to spread. We've already mentioned the use of Bluetooth. In addition, it spreads through a fake Google Play store, by means of spam text messages and through redirection from cracked sites. On top of this, it's also dropped by another mobile Trojan – Opfake.

The cybercriminals behind Obad are able to control the Trojan using pre-defined strings in text messages. The Trojan can perform several actions. including sending text messages, pinging a specified resource, operating as a proxy server, connecting to a specified address, downloading and installing a specified file, sending a list of apps installed on the device, sending information on a specific app, sending the victim's contacts to the server and performing commands specified by the server.

The Trojan harvests data from the device and sends it to the command-and-control server – including the MAC address of the device, the operating name, the IMEI number, the account balance, local time and whether or not the Trojan has been able to successfully obtain Device Administrator rights. All of this data is uploaded to the Obad control-and-command server: the Trojan first tries

to use the active Internet connection and, if no connection is available, searches for a nearby Wi-Fi connection that doesn't require authentication.

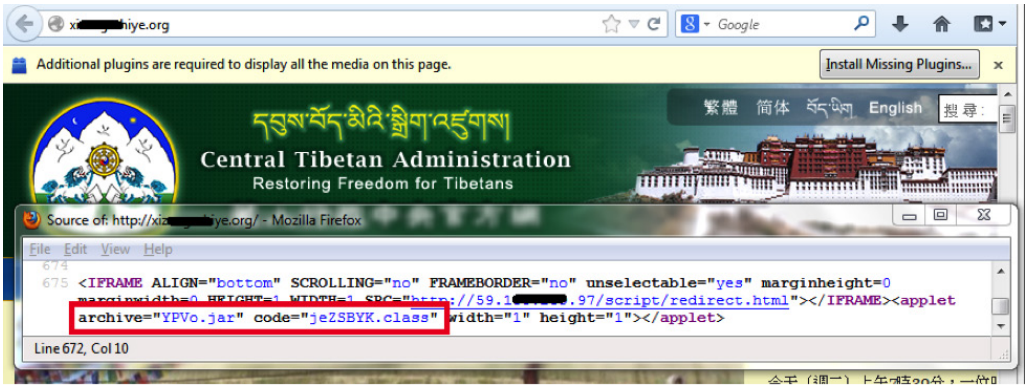
6. WATERING-HOLE ATTACKS

You might be familiar with the terms 'drive-by download' and spear-phishing. The former is where cybercriminals look for insecure web sites and plant a malicious script into HTTP or PHP code on one of the web pages. This script may directly install malware onto the computer of someone who visits the site, or it may use an IFRAME to redirect the victim to a malicious site controlled by the cybercriminals. The latter is a targeted form of phishing, often used as the starting-point for a targeted attack. An e-mail is directed to a specific person within a target organization, in the hope that they will click on a link or launch an attachment that runs the attacker's code and helps them to gain an initial foothold within the company.

When you combine the two approaches (drive-by downloads and spear-phishing) you end up with what's called a 'watering-hole' attack. The attackers study the behavior of people who work for a target organization, to learn about their browsing habits. Then they compromise a web site that is frequently used by employees – preferably one that is run by a trusted organization that is a valuable source of information. Ideally, they will use a zero-day exploit. So when an employee visits a web page on the site, they are infected – typically a backdoor Trojan is installed that allows the attackers to access the company's internal network. In effect, instead of chasing the victim, the cybercriminal lies in wait at a location that the victim is highly likely to visit – hence the watering-hole analogy.

It's a method of attack that has proved successful for cybercriminals this year. Hard on the heels of our report on the Winnti attacks, we found a Flash Player exploit on a care-giver web site that supports Tibetan refugee children, the 'Tibetan Homes Foundation'. It turned out that this web site was compromised in order to distribute backdoors signed with stolen certificates from the Winnti case. This was a classic case of a watering-hole attack – the cybercriminals had researched the preferred sites of their victims and compromised them in order to infect their computers. We saw the technique used again in August, when code on the Central Tibetan Administration web site started to redirect Chinese-speaking visitors to a Java exploit that dropped a backdoor used as part of a targeted attack.

Then in September we saw further watering-hole attacks directed against these groups as part of the NetTraveler campaign.



It's important to note that the watering-hole attack is just one method used by cybercriminals, rather than a replacement for spear-phishing and other methods. And the attacks mentioned above are just part of a series of attacks on Tibetan and Uyghur sites stretching back over two years or more.

Finally, all of these attacks are further testimony to the fact that you don't need to be a multi-national corporation, or other high-profile organization, to become the victim of a targeted attack.

7. THE NEED TO RE-FORGE THE WEAKEST LINK IN THE SECURITY CHAIN

Many of today's threats are highly sophisticated. This is especially true for targeted attacks, where cybercriminals develop exploit code to make use of unpatched application vulnerabilities, or create custom modules to help them steal data from their victims. However, often the first kind of vulnerability exploited by attackers is the human one. They use social engineering techniques to trick individuals who work for an organization into doing something that jeopardizes corporate security. People are susceptible to such approaches for various reasons. Sometimes they simply don't realize the danger. Sometimes they're taken in by the lure of 'something for nothing'. Sometimes they cut corners to make their lives easier – for example, using the same password for everything.

Many of the high profile targeted attacks that we have analyzed this year have started by 'hacking the human'. Red October, the series of attacks on Tibetan and Uyghur activists, MiniDuke, NetTraveler and Icefog all employed spear-phishing to get an initial foothold in the organizations they targeted. They frame their approaches to employees using data that they're able to gather from a company web site, public forums and by sifting through the various snippets of information that people post in social networks. This helps them to generate e-mails that look legitimate and catch people off-guard.

Of course, the same approach is also adopted by those behind the mass of random, speculative attacks that make up the majority of cybercriminal activities – the phishing messages sent out in bulk to large numbers of consumers.

Social engineering can also be applied at a physical level; and this dimension of security is sometimes overlooked. This was highlighted this year in the attempts to install KVM switches in the branches of two British banks. In both cases, the attackers masqueraded as engineers in order to gain physical access to the bank and install equipment that would have let them monitor network activity. You can read about the incidents here and here.

The issue was also highlighted by our colleague, David Jacoby, in September: he conducted a small experiment in Stockholm to see how easy it would be to gain access to business systems by exploiting the willingness of staff to help a stranger in need. You can read David's report here.

Unfortunately, companies often ignore the human dimension of security. Even if the need for staff awareness is acknowledged, the methods used are often ineffective. Yet we ignore the human factor in corporate security at our peril, since it's all too clear that technology alone can't guarantee security. Therefore it's important for all organizations to make security awareness a core part of their security strategy.

8. PRIVACY LOSS: LAVABIT, SILENT CIRCLE, NSA AND THE LOSS OF TRUST

No ITSec overview of 2013 would be complete without mentioning Edward Snowden and the wider privacy implications which followed up to the publication of stories about Prism, XKeyscore and Tempora, as well as other surveillance programs.

Perhaps one of the first visible effects was the shutdown of the encrypted Lavabit e-mail service. We wrote about it here. Silent Circle, another encrypted e-mail provider, decided to shut down their service as well, leaving very few options for private and secure e-mail exchange. The reason why these two services shut down was their inability to provide such services under pressure from Law Enforcement and other governmental agencies.

Another story which has implications over privacy is the NSA sabotage of the elliptic curve cryptographic algorithms released through NIST. Apparently, the NSA introduced a kind of "backdoor" in the Dual Elliptic Curve Deterministic Random Bit Generation (or Dual EC DRBG) algorithm. The "backdoor" supposedly allows certain parties to perform easy attacks against a particular encryption protocol, breaking supposedly secure communications. RSA, one of the major encryption providers in the world noted that this algorithm was default in its encryption toolkit and recommended all their customers to migrate away from it. The algorithm in question was adopted by NIST in 2006, having been available and used on a wide scale at least since 2004.

Interestingly, one of the widely discussed incidents has direct implications for the antivirus industry. In September, Belgacom, a Belgian telecommunications operator announced it was hacked. During a routine investigation, Belgacom staff identified an unknown virus in a number of servers and employee computers. Later, speculations appeared about the origin of the virus and the attack, which pointed towards GCHQ and NSA. Although samples of the malware have not been made available to the security industry, further details appeared which indicate the attack took place through "poisoned" LinkedIn pages that had been booby-trapped through man-in-the-middle techniques, with links pointing to CNE (computer network exploitation) servers.

All these stories about surveillance have also raised questions about the level of cooperation between security companies and governments. The EFF, together with other groups, published a letter on 25th October, asking security vendors a number of questions regarding the detection and blocking of state-sponsored malware.

At Kaspersky Lab, we have a very simple and straightforward policy concerning the detection of malware: We detect and remediate any malware attack, regardless of its origin or purpose. There is no such thing as "right" or "wrong" malware for us. Our research team has been actively involved in the discovery and disclosure of several malware attacks with links to governments and nation-states. In 2012, we published thorough research into Flame and Gauss, two of the biggest nation-

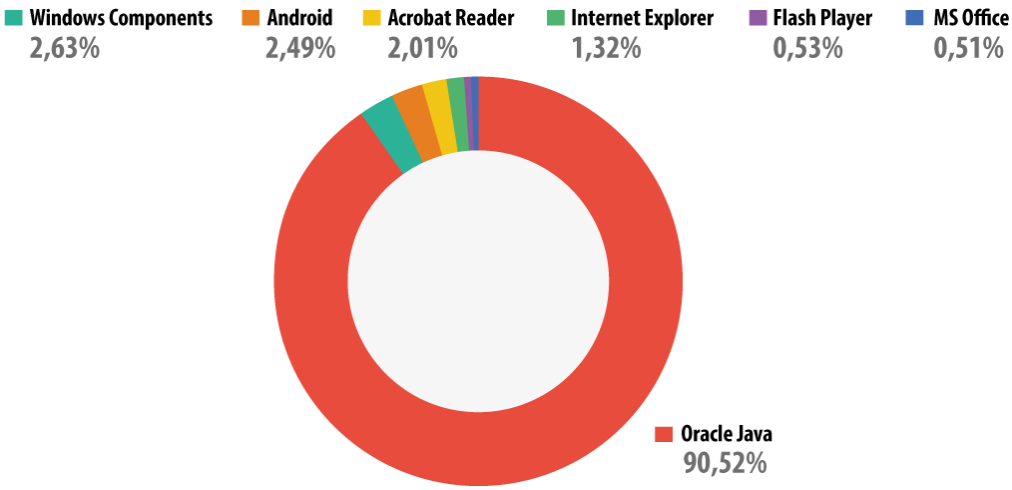
state mass-surveillance operations known to date. We have also issued public warnings about the risks of so-called "legal" surveillance tools such as HackingTeam's DaVinci and Gamma's FinFisher. It's imperative that these surveillance tools do not fall into the wrong hands, and that's why the IT security industry can make no exceptions when it comes to detecting malware. In reality, it is very unlikely that any competent and knowledgeable government organization will request an antivirus developer (or developers) to turn a blind eye to specific state-sponsored malware. It is quite easy for the "undetected" malware to fall into the wrong hands and be used against the very same people who created it.

9. VULNERABILITIES AND ZERO-DAYS

Cybercriminals have continued to make widespread use of vulnerabilities in legitimate software to launch malware attacks. They do this using exploits – fragments of code designed to use a vulnerability in a program to install malware on a victim's computer without the need for any user interaction. This exploit code may be embedded in a specially-crafted e-mail attachment, or it may target a vulnerability in the browser. The exploit acts as a loader for the malware the cybercriminal wishes to install.

Of course, if an attacker exploits a vulnerability is known only to the attacker – a so-called 'zero-day' vulnerability – everyone using the vulnerable application will remain unprotected until the vendor has developed a patch that closes up the loophole. But in many cases cybercriminals make successful use of well-known vulnerabilities for which a patch has already been released. This is true for many of the major targeted attacks of 2013 – including Red October, MiniDuke, TeamSpy and NetTraveler. And it's also true for many of the random, speculative attacks that make up the bulk of cybercrime.

Cybercriminals focus their attention on applications that are widely-used and are likely to remain unpatched for the longest time – giving them a large window of opportunity through which to achieve their goals. In 2013, Java vulnerabilities accounted for around 90.52% of attacks, while Adobe Acrobat Reader accounted for 2.01%. This follows an established trend and isn't surprising. Java is not only installed on a huge number of computers (3 billion, according to Oracle), but its updates are not installed automatically. Adobe Reader continues to be an application exploited by cybercriminals, though the volume of exploits for this application has reduced greatly over the last 12 months, as a result of Adobe's more frequent (and, in the latest version, automatic) patch routine.

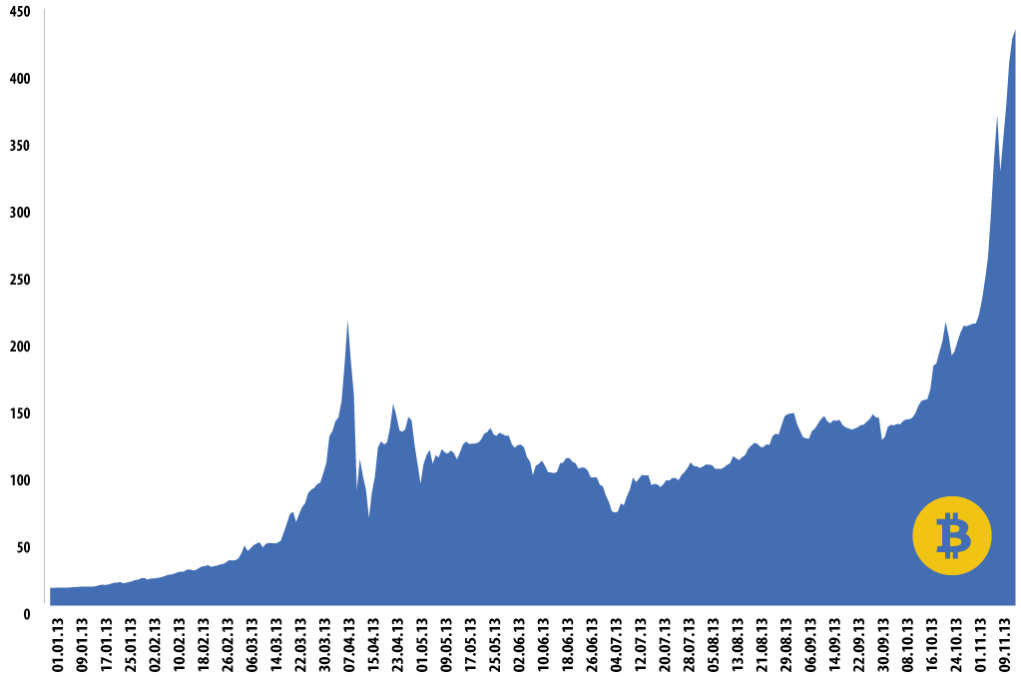


To reduce their 'attack surface', businesses must ensure that they run the latest versions of all software used in the company, apply security updates as they become available and remove software that is no longer needed in the organization. They can further reduce risks by using a vulnerability scanner to identify unpatched applications and by deploying an anti-malware solution that prevents the use of exploits in un-patched applications.

10. THE UPS AND DOWNS OF CRYPTOCURRENCIES – HOW THE BITCOINS RULE THE WORLD

In 2009, a guy named Satoshi Nakamoto published a paper that would revolutionize the world of e-currencies. Named "Bitcoin: A Peer-to-Peer Electronic Cash System", the paper defined the foundations for a distributed, de-centralized financial payment system, with no transaction fees. The Bitcoin system was implemented and people started using it. What kind of people? In the beginning, they were mostly hobbyists and mathematicians. Soon, they were joined by others – mostly ordinary people, but also cybercriminals and terrorists.

Back in January 2013, the Bitcoin was priced at 13$. As more and more services started adopting the Bitcoin as a means for payment, the price rose. On April 9, 2013, it reached $260 dollars (the average price was $214) before crashing the next day as Bitcoin-rich entities started swapping them for real life money.



Bitcoin daily average price (MT. Gox)

In November 2013, the Bitcoin started gaining strength again, surpassing the 400$ mark, heading towards 450$ and perhaps above.

So why are Bitcoins so popular? First of all, they provide an almost anonymous and secure means of paying for goods. In the wake of the surveillance stories of 2013, there is perhaps little surprise that people are looking for alternative forms of payment. Secondly, there is perhaps little doubt that they are also popular with cybercriminals, who are looking at ways to evade the law.

In May, we wrote about Brazilian cybercriminals trying to impersonate Bitcoin exchange houses. Bitcoin mining botnets have also appeared, as well as malware designed to steal Bitcoin wallets.

On Friday, October 25, during a joint operation between the FBI and the DEA, the infamous Silk Road was shut down. Silk Road was “a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful goods and services anonymously and beyond the reach of law

enforcement", according to the Press Release from the US Attorney's Office. It was operating on Bitcoins, which allowed both sellers and customers to remain unknown. The FBI and DEA seized about 140k Bitcoins (worth approximately $56 mil, at today's rates) from "Dread Pirate Roberts", Silk Road's operator. Founded in 2011, Silk Road was operating through the TOR Onion network, having amassed over 9.5 million BTC in sales revenue.

Although it's clear that cybercriminals have found safe havens in Bitcoins, there are also many other users who have no malicious intentions. As Bitcoin becomes more and more popular, it will be interesting to see if there is any government crackdown on the exchanges in a bid to put a stop to their illicit usage.

If you happen to own Bitcoins, perhaps the most important problem is how to keep them safe. You can find some tips in this post published by our colleagues Stefan Tanase and Sergey Lozhkin.

CONCLUSIONS AND LOOKING FORWARD: "2014, THE YEAR OF TRUST"

Back in 2011, we said the year was explosive. We also predicted 2012 to be revealing and 2013 to be eye opening.

Indeed, some of the revelations of 2013 were eye opening and raised questions about the way we use the Internet nowadays and the category of risks we face. In 2013, advanced threat actors have continued large-scale operations, such as RedOctober or NetTraveler. New techniques have been adopted, such as watering-hole attacks, while zero-days are still popular with advanced actors. We've also noticed the emergence of cyber-mercenaries, specialized "for hire" APT groups focusing on hit-and-run operations. Hacktivists were constantly in the news, together with the term "leak", which is sure to put fear into the heart of any serious sys-admin out there. In the meantime, cybercriminals were busy devising new methods to steal your money or Bitcoins; and ransomware has become almost ubiquitous. Last but not least, mobile malware remains a serious problem, for which no easy solution exists.

Of course, everyone is curious about how all these stories are going to influence 2014. In our opinion, 2014 will be all about rebuilding trust.

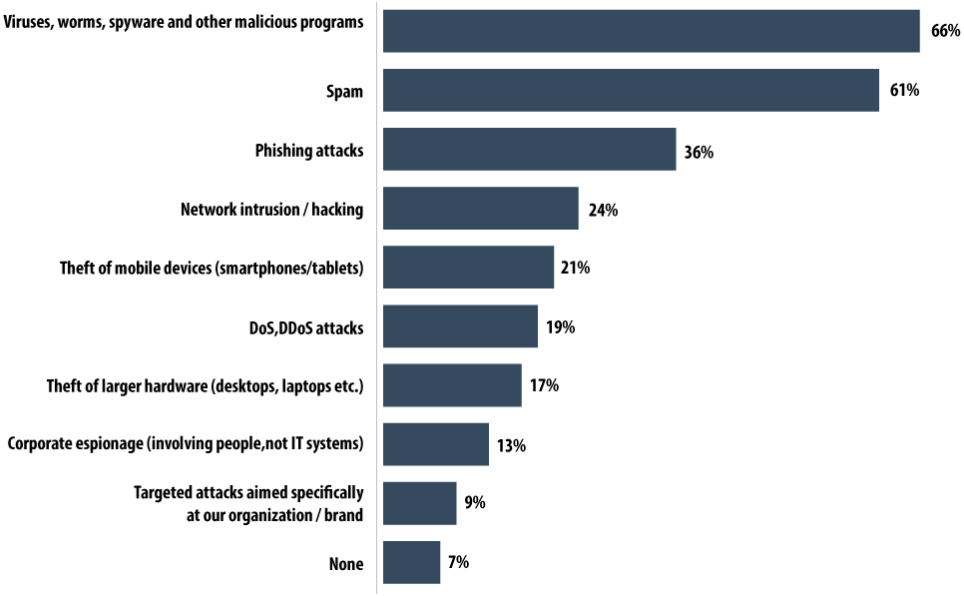
Privacy will be a hot subject, with its ups and downs. Encryption will be back in fashion and we believe countless new services will appear, claiming to keep you safe from prying eyes. The Cloud, the wonder child of previous years, is now forgotten as people have lost trust and countries begin thinking more seriously about privacy implications. In 2014, financial markets will probably feel the ripples of the Bitcoin, as massive amounts of money are being pumped in from China and worldwide. Perhaps the Bitcoin will reach the mark of $10,000, or perhaps it will crash and people will start looking for more trustworthy alternatives.

CORPORATE THREATS

Vitaly Kamluk, Sergey Lozhkin

The number of serious cyber-attacks detected over the last two years has increased so much that new attacks rarely cause much surprise. It's now commonplace for antivirus companies to issue a report about the discovery of another botnet or highly sophisticated malware campaign that is gathering data.

Companies are increasingly falling victim to cyber-attacks. According to a survey conducted by Kaspersky Lab and B2B International, 91% of the organizations polled suffered a cyber-attack at least once over a 12-month period, while 9% were the victims of targeted attacks.



The extensive use of computers and other digital devices in all areas of business has created ideal conditions for cyber espionage programs and malware capable of stealing corporate data. The potential is so great that malicious programs may soon completely replace company insiders as a way of gathering information. However, the risks to the corporate sector do not end there. This

dependence on the reliable operation of computers and the channels that connect them means cybercriminals are presented with a variety of other ways to target companies using destructive programs, from so-called encryptors and shredders that spread like the plague in a corporate environment, to an army of zombies that devours every available resource on web servers and data transfer networks.

THE MOTIVES

- **Stealing information.** The theft of valuable corporate data, commercial secrets, personal data of staff and customers, and monitoring of company activities are common goals of businesses that turn to cybercriminals to penetrate their competitors' networks or government intelligence agencies.

- **Wiping data or blocking infrastructure operations.** Some malicious programs are used to carry out a form of sabotage – destroying critical data or disrupting a company's operational infrastructure. For example, the Wiper and Shamoon Trojans irrevocably wipe system data from workstations and servers.

- **Stealing money.** Companies can incur financial losses as a result of activity by specialized Trojan programs capable of stealing money via online banking systems or which perform targeted attacks on the internal resources of processing centers.

- **Damaging a company's reputation.** Malicious users are attracted by successful companies and official websites with high visitor numbers, especially those in the Internet service sphere. A compromised corporate site that redirects visitors to malicious resources, malicious advertising banners or banners that display a political message can cause significant damage to a company's reputation in the eyes of its clients.

  Another serious reputational risk is linked to the theft of digital certificates. For public certification authorities, for example, the loss of certificates or the penetration of the digital certificate infrastructure can, in some cases, lead to a complete breakdown in trust and the subsequent closure of the business.

- **Financial losses.** One popular method of causing direct damage to a company or organization is by subjecting it to a DDoS attack. Cybercriminals are continuously coming up with new ways of carrying out such attacks. As a result of a DDoS attack a company's public-facing web resources can be put out of action for several days. In situations like this clients not only have no access to a company's services – resulting in direct

financial losses for the latter – but they also start looking for a more reliable company, which in turn reduces the customer base and results in long-term financial losses.

2013 saw an increase in the popularity of DNS Amplification attacks where malicious users, with the help of botnets, send recursive queries to DNS servers, reflecting the amplified response to the targeted system. This was the tactic used in one of the most powerful DDoS attacks this year – the attack on the Spamhaus site.

TARGET ORGANIZATIONS

When it comes to the mass distribution of malicious programs any company can be affected. Notorious banking Trojans such as ZeuS and SpyEye can penetrate the computers of even small commercial organizations resulting in the loss of money and intellectual property.

However, there are also numerous cases of carefully planned activity aimed at infecting the network infrastructure of a specific organization or individual. The results of our research showed that in 2013 the victims of these targeted attacks included companies from the oil and telecommunications industries, scientific research centers, as well as companies working in sectors such as aerospace, shipbuilding and other hi-tech industries.

PREPARING AN ATTACK

Cybercriminals have a large array of sophisticated tools to help them penetrate corporate networks. Planning a targeted attack on a company can take several months, after which all available tactics are deployed, starting with social engineering and progressing to exploits for unknown software vulnerabilities.

The attackers meticulously examine the target company's commercial profile, public resources, websites, employee profiles on social networks, announcements and the results of various presentations, exhibitions etc. for any piece of useful information. When planning a strategy for an intrusion and subsequent data theft, the criminals may study the company's network infrastructure, network resources and communication centers.

When planning their attack, the cybercriminals may create a fake malicious website that is an exact copy of the target's own site and register it with a similar domain name. It will then be used to trick users and infect their computers.

INTRUSION TECHNIQUES

One of the most popular techniques for inserting malware in corporate networks in 2013 was to send emails containing malicious attachments to company employees. More often than not, the documents in these emails were in familiar Word, Excel or PDF formats. When the attached file is opened a software vulnerability – if present – is exploited and the system is infected by a malicious program.

WEAK LINK

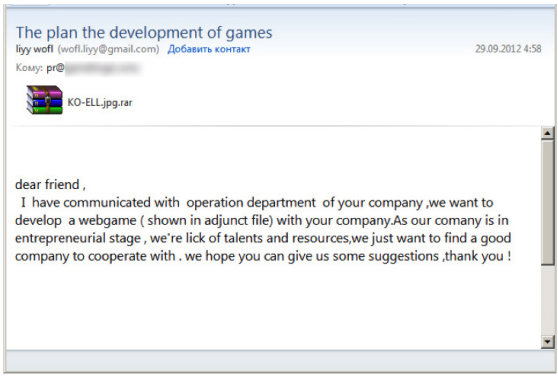
Employees who regularly have to communicate with people outside their corporate structure are often the recipients of malicious emails. More often than not the recipients work in the public relations department.

Departments involved in hiring new staff also receive lots of emails from external users. A cybercriminal may pretend to be a potential candidate for a job, and send a resume in an infected PDF file. Of course, the file will be opened by an HR employee, and if there is a vulnerability on the workstation, it will then be infected.

Finance departments may also receive malicious messages under the guise of requests or demands from the tax authorities, while legal departments might receive messages that appear to be from judicial bodies, the police or other government agencies.

SOCIAL ENGINEERING

The content of the message is intended to pique the interest of the employee it addresses, whether in relation to his/her job responsibilities or the company's general sphere of business. For instance, the hacking group Winnti sent messages to private video game manufacturers suggesting possible cooperation as part of a targeted attack:


The plan the development of games

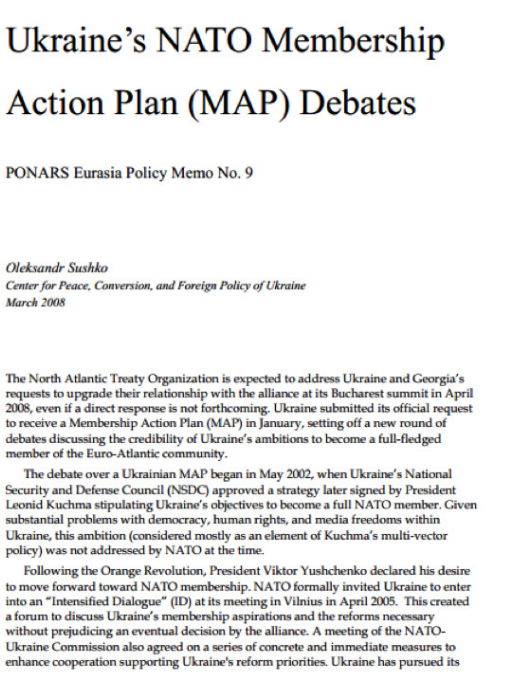
liyy wofl (wofl.liyy@gmail.com) Добавить контакт 29.09.2012 4:58

Кому: pr@

KO-ELL.jpg.rar

dear friend ,
I have communicated with operation department of your company ,we want to develop a webgame (shown in adjunct file) with your company.As our comany is in entrepreneurial stage , we're lick of talents and resources,we just want to find a good company to cooperate with . we hope you can give us some suggestions ,thank you !

The spyware Miniduke was distributed in a letter about Ukraine's foreign policy plans and Ukraine–NATO relations:


Ukraine's NATO Membership Action Plan (MAP) Debates

PONARS Eurasia Policy Memo No. 9

Oleksandr Sushko
Center for Peace, Conversion, and Foreign Policy of Ukraine
March 2008

The North Atlantic Treaty Organization is expected to address Ukraine and Georgia's requests to upgrade their relationship with the alliance at its Bucharest summit in April 2008, even if a direct response is not forthcoming. Ukraine submitted its official request to receive a Membership Action Plan (MAP) in January, setting off a new round of debates discussing the credibility of Ukraine's ambitions to become a full-fledged member of the Euro-Atlantic community.

The debate over a Ukrainian MAP began in May 2002, when Ukraine's National Security and Defense Council (NSDC) approved a strategy later signed by President Leonid Kuchma stipulating Ukraine's objectives to become a full NATO member. Given substantial problems with democracy, human rights, and media freedoms within Ukraine, this ambition (considered mostly as an element of Kuchma's multi-vector policy) was not addressed by NATO at the time.

Following the Orange Revolution, President Viktor Yushchenko declared his desire to move forward toward NATO membership. NATO formally invited Ukraine to enter into an "Intensified Dialogue" (ID) at its meeting in Vilnius in April 2005. This created a forum to discuss Ukraine's membership aspirations and the reforms necessary without prejudicing an eventual decision by the alliance. A meeting of the NATO-Ukraine Commission also agreed on a series of concrete and immediate measures to enhance cooperation supporting Ukraine's reform priorities. Ukraine has pursued its

VULNERABILITIES AND EXPLOITS

Cybercriminals actively use exploits to known software vulnerabilities.

The renowned Red October, for instance, used at least three different exploits to known vulnerabilities in Microsoft Office: CVE-2009-3129 (MS Excel), CVE-2010-3333 (MS Word) and CVE-2012-0158 (MS Word). Nettraveler used an exploit of CVE-2013-2465, which is a vulnerability of Java versions 5, 6 and 7; it was only patched by Oracle in June 2013.

However, so-called zero-day vulnerabilities – currently unknown to the software manufacturer – are the most dangerous. Cybercriminals actively search popular programs for unknown loopholes and create exploits to them. If such a vulnerability exists in a piece of software, it is very likely to get exploited. Miniduke used such a vulnerability (CVE-2013-0640) in Adobe Reader versions 9, 10, 11 – it was unknown at the time of the attack.

TECHNOLOGIES

Cybercriminals continuously improve malware, using unconventional approaches and solutions to steal information.

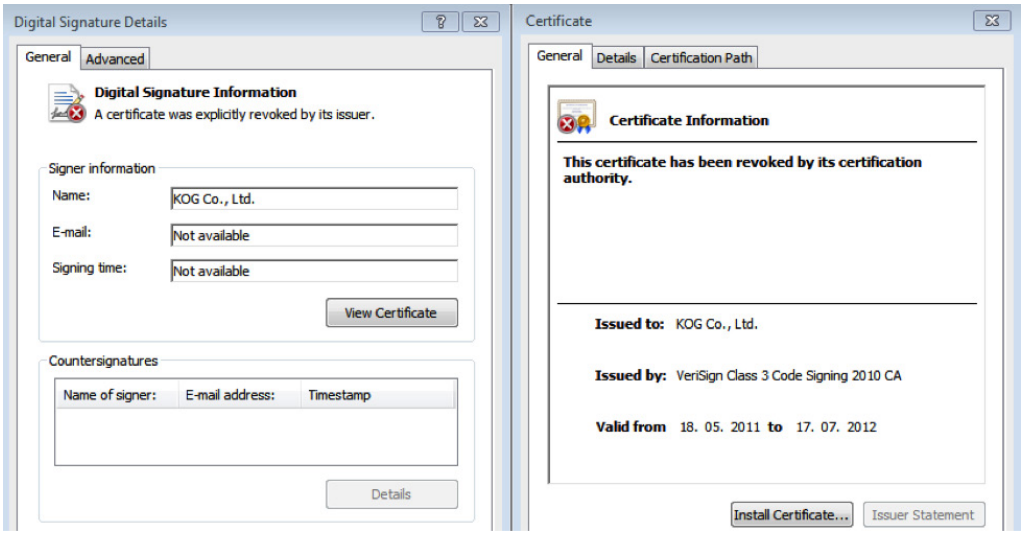
Red October, once it got a foothold within a system, worked as a multifunctional module-based platform. It added various modules to the infected system depending on the set target. Each of these modules performed a certain range of actions: from collecting information about the infected computer and its network infrastructure, stealing various passwords, keylogging, self-propagation, sending stolen information etc.

It should be also noted that cybercriminals have also responded to the development of mobile technologies and the spread of mobile devices in corporate environments. A modern smartphone or tablet PC is effectively a full-bodied workstation storing a huge amount of data, and thus is a potential target for cybercriminals. The creators of Red October developed dedicated modules which determined when smartphones running under Apple iOS, Windows Mobile as well as cellphones manufactured by Nokia connected to the infected workstation, copied data from them and sent it to the C&C server.

The creators of Kimsuky have integrated an entire module into their piece of malware which can remotely manage infected systems. Interestingly, they have done so with the help of TeamViewer, a quite legitimate remote management tool, by introducing slight modifications into its program code. After that, operators could manual connect to infected computers to collect and copy information that was of interest.

The Winnti hacker group stole digital certificates from the corporate networks of online game manufacturers, and used them to sign their malicious driver, subsequently infecting other companies. For example, a digital certificate was stolen from the South Korean company KOG. When we informed the company about the theft, the compromised certificate was revoked.

This is the revoked certificate:



In addition, the 64-bit Trojan included a fully functional backdoor module. This is the first case, as far as we know, when a 64-bit malicious program has been used with a valid digital signature belonging to a legitimate company.

The Miniduke spyware used Twitter to receive information from C&C servers. Miniduke's operators used dedicated accounts to publish specially crafted tweets which included an encoded C&C URL address.

The Trojan read Twitter on an infected computer and used the address to connect to the C&C.

WHAT GETS STOLEN

Cybercriminals are interested in stealing information of all kinds. It could be cutting-edge technology developed by companies and research institutes, source codes of software products, financial and legal documents, personal information about employees and clients, and any other information that may constitute a commercial secret. This information is often stored in plain text in corporate networks in the form of electronic documents, draft documents, reports, drawings, presentations, images etc.

As stated above, cybercriminals take different approaches to data gathering. Some malicious programs collect practically all types of electronic documents. For example, Red October was interested in documents in **txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, etc.** formats; the malicious program sent all of these to the C&C servers.

Another approach, which we identified with Kimsuky and Icefog is essentially a manual analysis of the data stored in corporate networks using remote-access technologies integrated into malware on infected workstations, and the subsequent copying of those documents that were specifically required or of value to the cybercriminals. When launching such attacks, cybercriminals take into account all the details of the targeted company and have a clear understanding of what data formats are used in that company and what types of information are stored. Thus, during Kimsuky and Icefog attacks, the targeted companies lost documents which were very specific to their activities and were stored in the HWP format which is widely used in South Korea.

THE RISE OF THE CYBERMERCENARIES

While analyzing the latest targeted attacks, we came to the conclusion that a new category of attackers has emerged. We call them cybermercenaries. These are organized groups of highly qualified hackers who can be hired by governments or private companies to organize and conduct complex, effective targeted attacks aimed at stealing information and destroying data or infrastructure.

Cybermercenaries are given a contract which stipulates the goals and a description of the task, after which they start to thoroughly prepare for and then launch the attack. While earlier attacks tended to steal information indiscriminately, cybermercenaries now aim to lay their hands on very specific documents or the contacts of people who might own the target information.

In 2013, we investigated the activity of the cybermercenary group Icefog, which launched target attacks under the same name. During the investigation, we managed to locate an Icefog operator activity log, which detailed all the attack activities. It became obvious from that log that the criminals not only have a good knowledge of Chinese, Korean and Japanese, but also know exactly where to look for the information they are interested in.

CONSEQUENCES OF HIGH-PROFILE DISCLOSURES

2013 saw some major disclosures about attacks launched by spyware that were related, directly or indirectly, to the activities of various governments. These disclosures could potentially lead to a loss of confidence in global services and corporations and greater interest in creating national equivalents of global services. This might lead to a peculiar type of de-globalization, causing a growing demand for IT in general, but a fragmentation of the users of the global network and a certain segmentation of online services. Already in many countries, there are local versions of global services, including national search engines, mail services, national IM services and even local social networks.

This growing number of new national software products and services is delivered by national manufacturers. These companies are typically smaller in size and budget than global market leaders.

As a result it's possible that their products may not be of the same quality as those of the larger international companies. Our experience of investigating cyber-attacks suggests that the smaller and less experienced the software developer is, the more vulnerabilities will be found in its code. As a result targeted attacks become easier and more effective.

Moreover, as states seize the initiative in controlling information and hardware resources, some states may legally oblige local companies to use national software products or online services, which may ultimately affect the security of the corporate sector as well.

OVERALL STATISTICS FOR 2013

Maria Garnaeva, Christian Funk

This section of the report forms part of the Kaspersky Security Bulletin 2013 and is based on data obtained and processed using Kaspersky Security Network (KSN). KSN integrates cloud-based technologies into personal and corporate products, and is one of Kaspersky Lab's most important innovations.

The statistics in this report are based on data obtained from Kaspersky Lab products installed on users' computers worldwide and were obtained with the full consent of the users involved.

2013 IN FIGURES

- According to KSN data, in 2013 Kaspersky Lab products neutralized **5 188 740 554** cyber-attacks on user computers and mobile devices
- **104 427** new modifications of malicious programs for mobile devices were detected.
- Kaspersky Lab products neutralized **1 700 870 654** attacks launched from online resources located all over the world.
- Kaspersky Lab products detected almost **3 billion** malware attacks on user computers. A total of **1.8 million** malicious and potentially unwanted programs were detected in these attacks.
- 45% of web attacks neutralized by Kaspersky Lab products were launched from malicious web resources located in the USA and Russia.

MOBILE THREATS

The mobile world is one the fastest-developing IT security areas. In 2013 security issues around mobiles have reached new heights and attained a new level of maturity in terms of both quality and quantity. If 2011 was the year when mobile malware gained traction, especially in Android-land, and 2012 was the year of mobile malware diversification, then 2013 saw mobile malware come of age. It's no great surprise that mobile malware is approaching the PC threat landscape in terms of cybercriminal business models and technical methods; however the speed of this development is remarkable.

Obad, probably the most remarkable discovery in the mobile field, is being distributed by multiple methods, including an pre-established botnet. Android-based smartphones infected with Trojan-SMS.AndroidOS.Opfake.a are used as multipliers, sending text messages containing malicious links to every contact on the victim's device. This has been common practice in the PC threat landscape and is a popular service provided by bot-herders in underground cybercriminal economy.

Mobile botnets actually offer a significant advantage over traditional botnets: smartphones are rarely shut down, making the botnet far more reliable since almost all its assets are always available and ready for new instructions. Common tasks performed by botnets include mass spam mail-outs, DDoS attacks and mass spying on personal information, all of them non-demanding actions in terms of performance and easily achieved on smartphones. The MTK botnet, appearing in early 2013, and Opfake, among many others, are proof that mobile botnets are no longer just a playground for cybercriminals, but have become common practice to serve the main purpose: financial profit.

SIGNIFICANT EVENTS

- **Mobile Banking Trojans.** These include mobile phishing, theft of credit card information, transferring money from a bank card to the mobile account and finally to a QIWI wallet. In 2013 we also saw mobile Trojans which could check on the victim's balance to ensure the maximum profit.
- **Mobile Botnets.** As stated above, botnet functionalities offer greater flexibility in illegal money-making schemes. This trend has now reached the mobile world and is here to stay. According to our estimates, about 60% of mobile malware includes elements of large or small botnets.

- **Backdoor.AndroidOS.Obad.** This malware is probably the most versatile piece of mobile malware found to date, including a staggering total of three exploits, a backdoor, SMS Trojan and bot capabilities and further functionalities. It's a kind of Swiss Army knife, comprising a whole range of different tools.

- **Using GCM to control botnets.** Cybercriminals have discovered a way to use Google Cloud Messaging (GCM) to control zombie devices in a botnet. This method is used by a relatively small number of malicious programs, but some of them are widespread. The execution of commands received from GCM is performed by the GCM system and it is impossible to block them directly on an infected device.

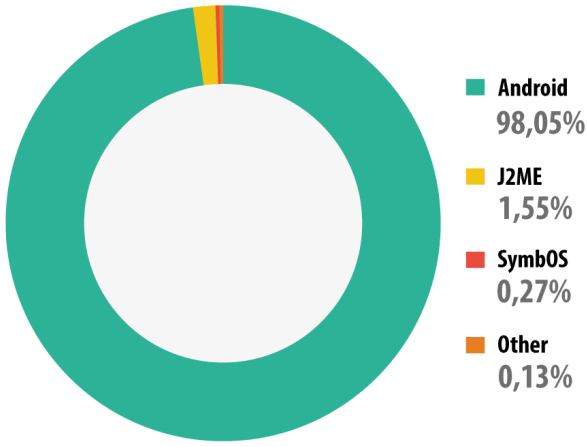
- **APT attacks against Uyghur activists.** We've seen both Windows and Mac OS X malware deployed against Uyghur activists in targeted attacks. PDF, XLS, DOC and ZIP files were sent in e-mails to perform the attacks in the past. APK files have now been added to the arsenal, spying on the personal information stored on the victim's device and also transmiting its location.

- **Vulnerabilities in Android.** In a nutshell, we have seen exploits targeting Android for three purposes: to circumvent Android's app integrity check on installation (also known as master key vulnerability, to gain enhanced rights, and to hinder the analysis of an app. The latter two types were also used in Obad.

- **Attacks on PCs through an Android device.** While we have seen PC malware that can infect smartphones, we have also come across Android malware that does it the other way round. When an infected Android device is connected to a PC in the USB drive emulation mode, its malicious payload is launched.

STATISTICS

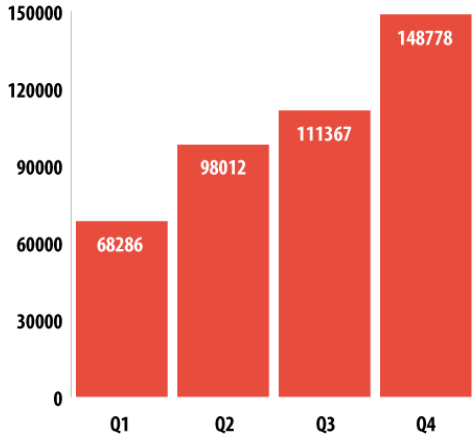
In terms of the mobile operating systems that are being targeted by malware, nothing has significantly changed in 2013. Android is still target number one, attracting a whopping 98.05% of known malware. No other OS gets anywhere close, as seen below. The reasons for this are Android's leading market position, the prevalence of third party app stores and the fact that Android has a rather open architecture, making it easy to use for both app developers and malware authors alike. We do not expect this trend to change in near future.



Mobile malware distribution by platform

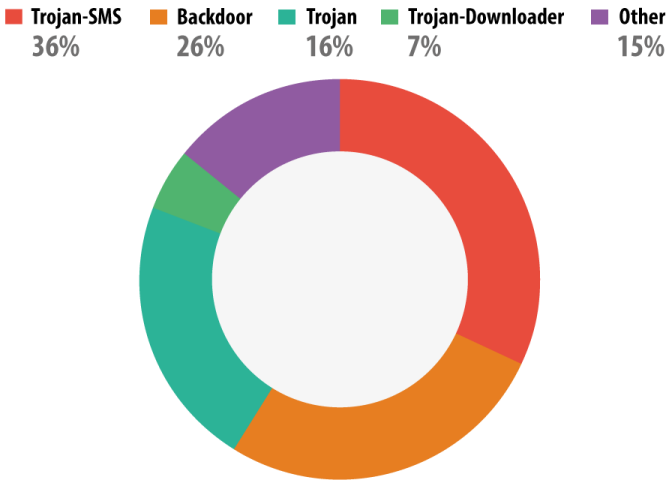
To date we have collected 8,260,509 unique malware installation packs. Note that different installation packs may launch applications with the same features. The difference is in the malware interface and, for instance, the content of the text messages they send out.

The total number of mobile malware samples in our collection is 148,778 at the time of writing – 104,421 of them were found in 2013. October alone has seen 19,966 modifications, half the total that Kaspersky Lab found in the whole of 2012. Fortunately, this is this far from the situation we're experiencing in the PC world, where we process a stream of more than 315,000 malware samples per day in our lab. Still, the trend is highly visible and continuing.



Number of mobile malware samples in our collection

Among mobile malware, SMS Trojans are still leading the field:



Malware distribution by behavior type

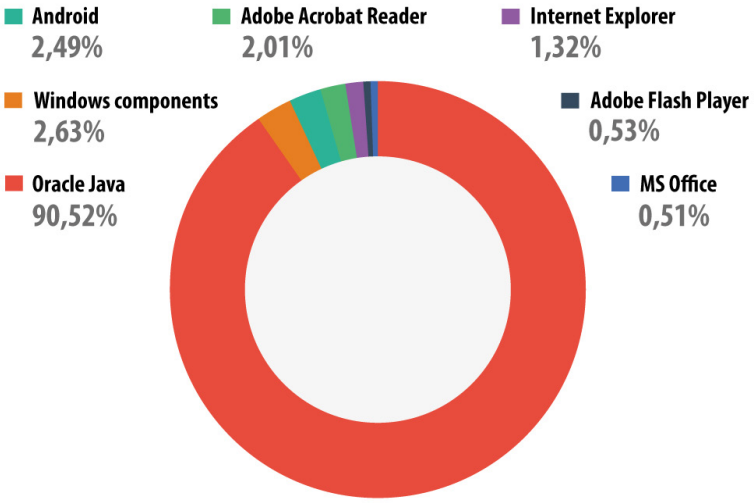
However, SMS Trojans, with a few exceptions, have evolved into bots, so we can easily unite the leaders of both into a single category – Backdoor Malware. So, 62% of malicious applications are elements of mobile botnets.

MAIN FINDINGS:

- All the techniques and mechanisms of infection and malware are moving very quickly from PC to Android thanks to the openness and popularity of the mobile platform.
- The majority of malicious mobile applications are targeted primarily at stealing money and, secondly, at stealing personal data.
- The majority of mobile malware is made up of bots with rich features sets. In the near future, the buying and selling of mobile botnets is likely to begin.
- Online banking is a clear target for mobile malware. Cybercriminals are watching the development of mobile banking. If a smartphone is successfully infected, they check whether that phone is tethered to a bank card.

VULNERABLE APPLICATIONS EXPLOITED BY CYBERCRIMINALS

The following rating of vulnerable applications is based on data about exploits blocked by our products and used by cybercriminals both in Internet attacks and in compromising local applications, including users' mobile devices.



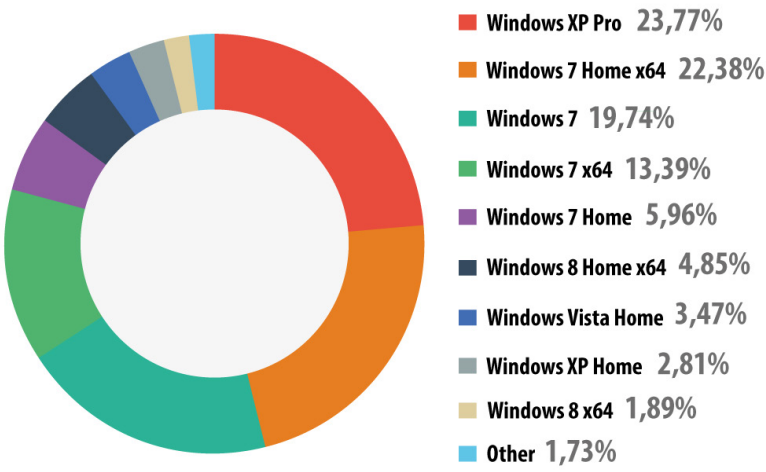
Malware distribution by behavior type

90.52% of all detected attempts to exploit vulnerabilities targeted Oracle Java. These vulnerabilities are exploited by drive-by attacks conducted via the Internet, and new Java exploits are now present in lots of exploit packs. More details can be found in our article about Java exploits.

Second place is taken by the 'Windows components' category, including vulnerable Windows OS files that do not apply to Internet Explorer and Microsoft Office – we assigned them to a separate category. Most of the attacks in this category target a vulnerability discovered in win32k.sys – CVE-2011-3402 – which was first used in Duqu.

In third place with 2.5% are exploits for Android. Cybercriminals (and sometimes users themselves) use Android vulnerabilities in order to gain root privileges, which grants unlimited abilities to manipulate a system. These breaches are not used in drive-by attacks, and exploits for them are detected either by an antivirus, if there was an attempt to download an application containing an

exploit, or by a file antivirus when an exploit is found on a device. It was recently reported that the Chrome browser for Nexus 4 and Samsung Galaxy S4 contained a vulnerability which could be used in future exploitation of Android vulnerabilities in drive-by attacks.



Distribution of OS Windows versions installed on user computers, 2013

Among the users of Kaspersky Lab products who consented to participate in KSN, 61.5% use a version of Windows 7 (5% more than last year); 6.3% use Windows XP (7.75% less than in 2012).

ONLINE THREATS (ATTACKS VIA THE WEB)

The statistics in this section were derived from web antivirus components which protect users when malicious code attempts to download from infected websites. Infected websites might be created by malicious users, or they could also be made up of user-contributed content (such as forums) and legitimate resources that have been hacked.

The number of attacks launched from web resources located all over the world increased from 1 595 587 670 in 2012 to **1 700 870 654**. That means that Kaspersky Lab products protected users an average of 4 659 920 times every day when they were online.

Compared to last year, there has been a fall in the growth rate of browser-based attacks. The number of neutralized web-based attacks in 2013 is 1.07 times more than in 2012, while in 2012 the corresponding figure was 1.7. The main tool behind browser-based attacks is still the exploit pack, which gives cybercriminals a surefire way of infecting victim computers that do not have a security product installed, or have at least one popular application that is vulnerable (requiring security updates).

TOP 20 MALICIOUS PROGRAMS ON THE INTERNET

We have identified the top 20 most active malicious programs involved in web attacks on users' computers. This list accounts for 99.9% of all web attacks.

	NAME*	% OF ALL ATTACKS**
1	**Malicious URL**	93.01%
2	**Trojan.Script.Generic**	3.37%
3	**AdWare.Win32.MegaSearch.am**	0.91%
4	**Trojan.Script.Iframer**	0.88%
5	**Exploit.Script.Blocker**	0.49%
6	**Trojan.Win32.Generic**	0.28%
7	**Trojan-Downloader.Script.Generic**	0.22%
8	**Trojan-Downloader.Win32.Generic**	0.10%
9	**Hoax.SWF.FakeAntivirus.i**	0.09%
10	**Exploit.Java.Generic**	0.08%
11	**Exploit.Script.Blocker.u**	0.08%
12	**Exploit.Script.Generic**	0.07%
13	**Trojan.JS.Iframe.aeq**	0.06%
14	**Packed.Multi.MultiPacked.gen**	0.05%
15	**AdWare.Win32.Agent.aece**	0.04%
16	**WebToolbar.Win32.MyWebSearch.rh**	0.04%
17	**AdWare.Win32.Agent.aeph**	0.03%
18	**Hoax.HTML.FraudLoad.i**	0.02%
19	**AdWare.Win32.IBryte.heur**	0.02%
20	**Trojan-Downloader.HTML.Iframe.ahs**	0.02%

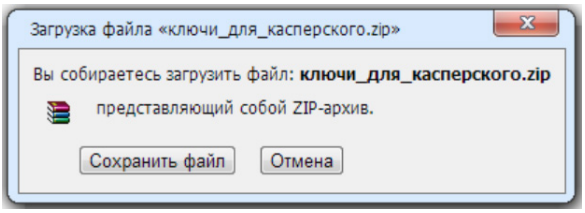
*These statistics represent detection verdicts of the web-based antivirus module and were submitted by users of Kaspersky Lab products who consented to share their local data.
**The percentage of unique incidents recorded by web-based antivirus on user computers.

Compared to 2012, there was an increase in the proportion of blacklisted malicious links blocked (Malicious URL in 1st place). New, enhanced detection technologies that rely on KSN's capabilities have resulted in the share of threats detected via heuristic methods rising from 87% to 93% over the past year. Most malicious URL detections were for websites containing exploits and for sites redirecting to exploits.

Seven entries in this Top 20 rating were verdicts identifying threats that are blocked during attempted drive-by attacks, which are currently the most common attack method for web-borne malware. They are the heuristic verdicts Trojan.Script.Generic, Trojan.Script.Iframer, Exploit.Script.Blocker, Trojan-Downloader.Script.Generic, Exploit.Java.Generic, Exploit.Script.Generic and the non-heuristic. These verdicts are assigned to scripts that redirect to exploits as well as to the exploits themselves.

In 9th place is a flash file detected as Hoax.SWF.FakeAntivirus.i that contains animation imitating the activity of an antivirus program. A "scan" of the victim's computer reveals a huge number of "infections" that require a specialist security solution. The victim is prompted to send a text message to a short number and receives a link so the so-called solution can be downloaded. Flash files like this can appear on sites with advertising banners that from time to time include redirects to unwanted content.

In 18th place is Hoax.HTML.FraudLoad.i, detected as an HTML page that imitates the familiar file download window:



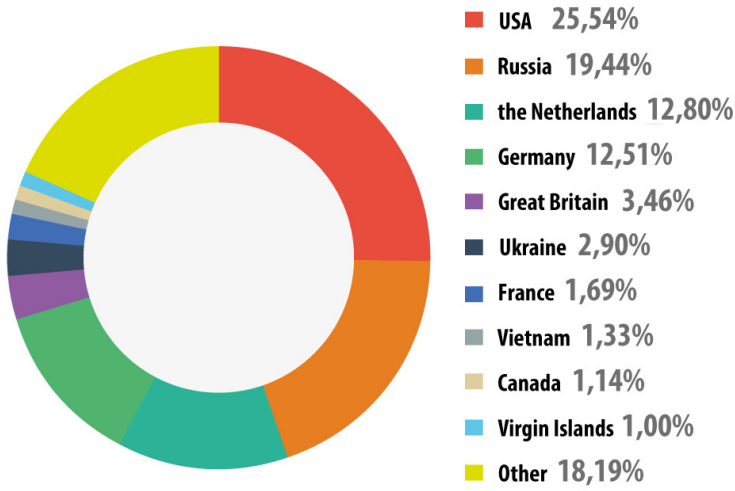
Users can end up on these sorts of pages from a variety of Russian-language download sites offering games, software and films. They tend to be hosted on free hosting resources. If users click 'Save', they are redirected to a file hosting site where they are prompted to download a file after paying for subscription via a text message. However, after fulfilling all the requirements, instead of receiving the desired content users get a text file with instructions on using search engines or, even worse, malicious programs.

There are more adware verdicts in this year's rating than in 2012, with the overall share rising from 0.3% to 1.04%.

COUNTRIES WHERE ONLINE RESOURCES ARE SEEDED WITH MALWARE: TOP 10

The following stats are based on the physical location of the online resources, which were used in attacks, blocked by the antivirus (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.



Distribution of online resources seeded with malicious programs, by country

In order to conduct **1 700 870 654** attacks over the Internet, cybercriminals used 10 604 273 unique hosts, which is 4 million more than in 2012. 82% of notifications on blocked web attacks were generated by blocking web resources located in ten countries, which is 14.1 percentage points less than in 2012.

In 2013 there was little change to the Top 10 rating of leading malware sources compared to 2012. China, which was the traditional leader prior to 2010, dropped out of the top 10 and Vietnam appeared in 8th place. In 2010 the Chinese authorities succeeded in shutting down lots of malicious hosting resources in their part of cyberspace, at the same time hardening their legislation on domain names in the .cn domain zone, which resulted in the reduction of malicious sources in China. In 2010 China was in 3rd place, 6th in 2011, 8th in 2012 and in 2013 it fell to 21st place in the rating.

COUNTRIES WHERE USERS FACE THE HIGHEST 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 to which computers are exposed in different countries across the globe, providing an indicator of the aggressiveness of the environment in which computers work in different countries.

Top 20 countries with the highest risk of computer infection via Internet:

NUMBER	COUNTRY*	% OF UNIQUE USERS**
1	**Azerbaijan**	56.29%
2	**Kazakhstan**	55.62%
3	**Armenia**	54.92%
4	**Russia**	54.50%
5	**Tajikistan**	53.54%
6	**Vietnam**	50.34%
7	**Moldova**	47.20%
8	**Belarus**	47.08%
9	**Ukraine**	45.66%
10	**Kyrgyzstan**	44.04%
11	**Sri Lanka**	43.66%
12	**Austria**	42.05%
13	**Germany**	41.95%
14	**India**	41.90%
15	**Uzbekistan**	41.49%
16	**Georgia**	40.96%
17	**Malaysia**	40.22%
18	**Algiers**	39.98%
19	**Greece**	39.92%
20	**Italy**	39.61%

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 2013 saw a new leader emerge, with Azerbaijan finishing in first place with 56.3% of attacked users. Russia, which came top in the previous two years, fell to 4th place with 54.4% (4.1 percentage points less than the previous year).

The USA, Spain, Oman, Sudan, Bangladesh, the Maldives and Turkmenistan dropped out of the TOP 20 list of countries. Among the newcomers are Austria, Germany, Greece, Georgia, Kyrgyzstan, Vietnam and Algeria.

The USA dropped from 19th to 25th. Its share fell by 7 percentage points to 38.1%. To recap, just two years ago the USA was in 3rd place. The declining level of risk associated with web-based attacks in the USA may be linked with the growing popularity of web surfing via mobile devices. Spain, which rounded off the TOP 20 rating last year, appeared at 31st place in 2013 (36.7% - 8 points less than the previous year).

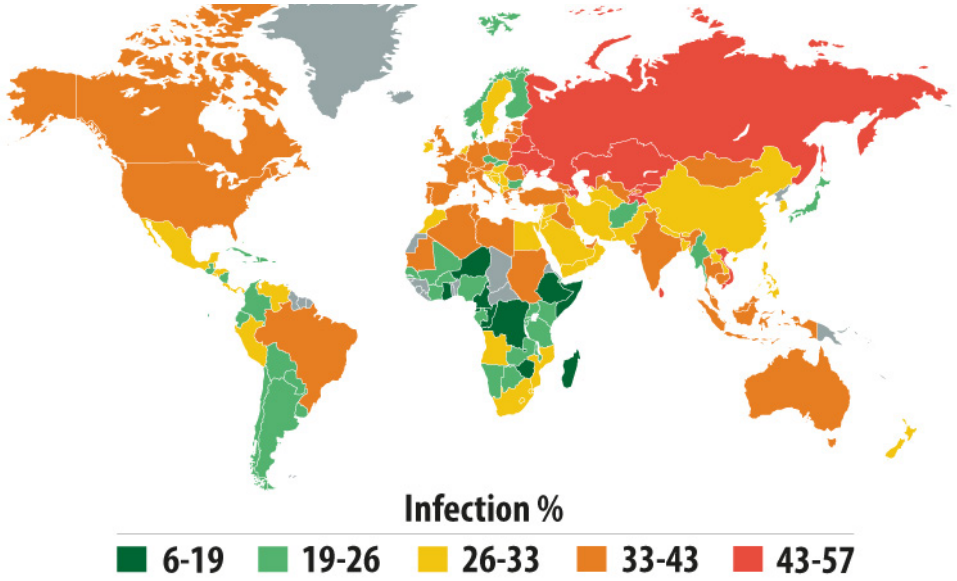
Austria (+8 points) ended the year in 12th place, Germany is in 13th (+9.3 points), and Greece (-1.6 points) is in 19th. Another Western European country – Italy (-6 points) – completes the rating.

All countries can be assigned to one of the following categories based on their risk level while surfing the Internet:

- **High risk.** This group includes 15 countries from the TOP 20 in the range of 41-60%. They are Russia, Austria, Germany, several former Soviet republics and Asian countries. This group has more than halved since last year when it consisted of 31 countries.
- **Moderate Risk.** A total of 118 countries in the range of 21-40.99%: Australia (38.9%), the USA (38.1%), Canada (36.5%), Italy (39.6%), France (38.1%), Spain (36.7%), the UK (36.7%), the Netherlands (27.3%), Finland (23.6%), Denmark (21.8%); Poland (37.6%), Romania (33.2%), Bulgaria (24.1%), Brazil (34.6%), Mexico (29.5%), Argentina (25%), China (32.2%), Japan (25.3%).
- **Low risk (0-20.99%).** A total of 25 countries: the Czech Republic (20.3%), Slovakia (19.7%), Singapore (18.5%) and a number of African countries.

The African countries with a low risk level turned out to have high and moderate risk of infection by local threats (see below). The Internet in these countries is still not highly developed. Therefore, to share data users still make use of a variety of removable media. That is why web attacks are

threatening so few users, while malware, distributed over removable data carriers, is frequently detected on computers.



The average global Internet threat level grew by 6.9 percentage points – in 2013, 41.6% of user computers encountered attacks at least once. The Internet is still the main source of malware for users in the majority of countries worldwide.

LOCAL THREATS

Local infection statistics for user computers are a critically 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 of the report contains an analysis of statistics based on data obtained from the on-access scanner and scanning statistics for different disks, including removable media (the on-demand scanner).

Kaspersky Lab antivirus solutions detected nearly 3 billion malware incidents on computers participating in the Kaspersky Security Network.

In total, 1.8 million malicious or potentially unwanted programs were detected in these incidents.

THE TOP 20 MALICIOUS OBJECTS DETECTED ON USER COMPUTERS:

	NAME	% OF INDIVIDUAL USERS*
1	**DangerousObject.Multi.Generic**	39.1%
2	**Trojan.Win32.Generic**	38.0%
3	**Trojan.Win32.AutoRun.gen**	20.1%
4	**Virus.Win32.Sality.gen**	13.4%
5	**Exploit.Win32.CVE-2010-2568.gen**	10.6%
6	**AdWare.Win32.DelBar.a**	8.0%
7	**Trojan.Win32.Starter.lgb**	6.6%
8	**Virus.Win32.Nimnul.a**	5.5%
9	**Worm.Win32.Debris.a**	5.4%
10	**Virus.Win32.Generic**	5.4%
11	**Trojan.Script.Generic**	5.4%
12	**Net-Worm.Win32.Kido.ih**	5.1%
13	**AdWare.Win32.Bromngr.i**	4.6%
14	**Net-Worm.Win32.Kido.ir**	4.4%
15	**Trojan.Win32.Starter.yy**	3.9%
16	**DangerousPattern.Multi.Generic**	3.8%
17	**HiddenObject.Multi.Generic**	3.8%

18	**Trojan.Win32.Hosts2.gen**	3.7%
19	**AdWare.Win32.Agent.aeph**	3.6%
20	**Trojan.WinLNK.Runner.ea**	3.6%

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.

In 2013, malicious programs classified as DangerousObject.Multi.Generic and detected using cloud technologies ranked first in the list of the Top 20 malicious objects detected on user computers. Cloud technologies work when there are still no signatures in antivirus databases, and no heuristics for detecting malicious programs, but Kaspersky Lab's cloud already has data about the threat. This is essentially how the newest malicious programs are detected. With the Urgent Detection System (UDS) implemented in Kaspersky Security Network over 11 million computers received real-time protection.

Last year's leader Trojan.Win32.Generic came second based on verdicts issued by the heuristic analyzer.

Exploit.Win32.CVE-2010-2568.gen (5th place) and Trojan.WinLNK.Runner.ea (20th place) are the verdicts assigned to malicious lnk files (shortcuts) are detected. The lnk files of these families launch other malicious executable files. They are actively used by worms for distribution via USB storage media.

Eight out of the Top 20 programs either integrate the self-proliferating mechanism or are used as one of the components in the scheme of worm distribution: Virus.Win32.Sality.gen (4th place), Trojan.Win32.Starter.lgb (7th place), Virus.Win32.Nimnul.a (8th place), Worm.Win32.Debris.a (9th place), Virus.Win32.Generic (10th place), Net-Worm.Win32.Kido.ih (12th place), Net-Worm.Win32.Kido.ir (14th place), Trojan.Win32.Starter.yy (15th place).

The percentage of Net-Worm.Win32.Kido worms (12th and 14th place), which first appeared in 2008, is declining with every year as users update their systems.

The Virus.Win32.Virut family of verdicts failed to make it into the Top 20 in 2013, while the share of other viruses – Sality (4th place) and Nimnul (8th place) – grew by 8.5 and 1.4 percentage points respectively.

This year's newcomer Worm.Win32.Debris.a ended up in 9th place. This worm is distributed via removable media with the help of lnk files. The payload of this worm is the Andromeda malicious program which is used to download third-party files. This program first appeared on the virus writer black market in 2011. However, new methods of installation and distribution means we have assigned it to a separate family.

Trojan.Win32.Hosts2.gen is in 18th place. This verdict is assigned to malicious programs that try to change the special hosts file redirecting user requests to certain domains to hosts under their control.

COUNTRIES WHERE USERS FACE THE HIGHEST RISK OF LOCAL INFECTION

In order to assess the risk level for local infection faced by users in different countries, we calculated just how often users with Kaspersky Lab products encountered antivirus detections over the course of the year. Of interest was data concerning the detection of malware on user machines or on removable media connected to computers – USB flash drives, camera and phone memory cards, external hard drives. Essentially, these statistics reflect the level of personal computer infections in different countries of the world.

Computer infection levels by country – Top 20:

COUNTRY*	%**
Vietnam	68.14%
Bangladesh	64.93%
Nepal	62.39%
Mongolia	60.18%
India	59.26%
Sudan	58.35%
Afghanistan	57.46%
Algeria	56.65%
Laos	56.29%
Cambodia	55.57%

Iraq	54.91%
Djibouti	54.36%
Maldives	54.34%
Pakistan	54.12%
Sri Lanka	53.36%
Mauritania	53.02%
Indonesia	52.03%
Rwanda	51.68%
Angola	50.91%
Egypt	50.67%

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

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

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

For more than a year, the Top 20 positions in this category were held by countries in Africa, the Middle East, and South East Asia. Since last year's ranking, the situation in the top-ranked countries has improved: in 2012, the figure for the first-placed country was over 99%; in 2013, the highest figure did not reach 70%.

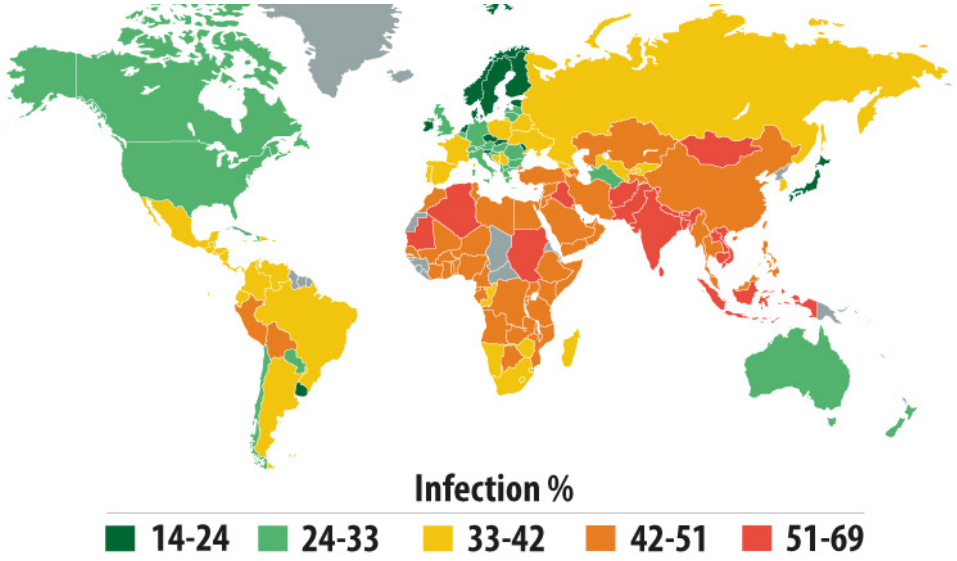
In 2013, an average of 60.1% of computers connected to KSN were subjected to at least one attack while surfing the web compared to 73.8% in 2012.

Countries can be divided into categories in terms of local threats. Considering the overall reduction in the level of local infections most probably caused by the decline in the use of flash drives for exchanging information, we have lowered the threshold for the group levels (compared with the statistics for 2012).

- **Maximum risk (over 60%):** four countries including Vietnam (68.1%), Bangladesh (64.9%), Nepal (62.4%) and Mongolia (60.2%).
- **High risk (41-60%):** 67 countries across the globe, including India (59.2%), China (46.7%), Kazakhstan (46%), Azerbaijan (44.1%), Russia (41.5%), most African countries.
- **Moderate local infection rate (21-40.99%).** 78 countries across the globe, including Spain (36%), France (33.9%), Portugal (33.1%), Italy (32.9%), Germany (30.2%), the USA (29%), the

UK (28.5%), Switzerland (24.6%), Sweden (21.4%), Ukraine (37.3%), Brazil (40.2%), Argentina (35.2%), Chile (28.9%), South Korea (35.2%), Singapore (22.8%).

> **Low local infection rate (0- 20.99%).** Nine countries from across the globe.



The Top 10 countries with the lowest risk of local infection were:

RANK	COUNTRY	%
1	**Denmark**	14.74%
2	**Czech Republic**	15.584%
3	**Finland**	15.93%
4	**Cuba**	17.18%
5	**Japan**	18.93%
6	**Slovakia**	19.24%
7	**Slovenia**	19.32%
8	**Norway**	19.36%
9	**Seychelles**	19.90%
10	**Malta**	21.28%

In 2013, one new country – the Seychelles – appeared in this Top 10, pushing out the Netherlands.

On average, 18.4% of user machines were attacked in the low risk group of countries. This is 6.6 percentage points less than last year.

FORECASTS

Alexander Gostev

MOBILE THREATS

Having begun many years ago with the Gpcode Trojan, malicious ransomware has developed into two main types—Trojans that block the computer's operation and demand money to unblock it, and Trojans that encrypt the data on the computer and require even bigger sums to decrypt it.

In 2014, we can expect cybercriminals to take another logical step in the development of these types of Trojan programs and turn their attention to mobile devices. Android-based devices will no doubt be the first to be targeted. Encryption of user data on smartphones – photos, contacts, correspondence – is easy if the Trojan has administrator rights, and distributing such programs (including via official stores like Google Play) is not difficult either.

It seems that the trend of making malicious programs even more complicated in 2013 will continue next year. As before, the fraudsters will try to get at users' money with the help of mobile Trojans. Tools developed to access bank accounts of mobile device owners (mobile phishing, banking Trojans) will be further improved. Mobile botnets will be sold and bought and will also be used to distribute malicious attachments on behalf of third parties. Vulnerabilities in the Android OS will be exploited to infect mobile devices; it's unlikely they will be involved in drive-by attacks on smartphones.

ATTACKS ON BITCOIN

Attacks on Bitcoin pools, exchanges and Bitcoin users will become one of the most high-profile topics of the year.

Attacks on stock exchanges will be especially popular with the fraudsters as their cost-to-income ratio is very favorable.

As for Bitcoin users, in 2014 we expect considerable growth in the number of attacks targeting their wallets. Previously, criminals infected victim computers and went on to use them for mining. However, this method is now far less effective than before while the theft of Bitcoins promises cybercriminals huge profits and complete anonymity.

THE PROBLEMS OF PROTECTING PRIVACY

People want to hide their private life from intelligence agencies around the world. It is impossible to ensure user data is protected without popular Internet services – social networking sites, mail and cloud services – taking appropriate measures. However, the current protection methods are not enough. A number of these services have already announced the implementation of additional measures to protect user data, for example, encryption of all data transmitted between their own servers. Implementing more sophisticated protection measures will continue, and is likely to become a key factor when users choose between rival web services.

End users also face problems as they try to protect the information stored on their computers and devices, while also ensuring their online behavior remains confidential. This will lead to greater popularity for VPN services and Tor-anonymizers as well as increased demand for local encryption tools.

ATTACKS ON CLOUD STORAGE FACILITIES

'Clouds' are facing tough times. First, trust in cloud storage has been hit hard by Snowden's leaks and the newly discovered facts of data collection by various state-sponsored intelligence services. At the same time, the types of data being stored in these facilities are becoming ever more attractive to cybercriminals. Three years ago we assumed that in due course it would be easier for a fraudster to hack a cloud storage provider and steal company data from there, rather than hacking the company itself. It looks like that time is almost upon us. Hackers are targeting cloud service employees, seeing them as the weakest link in the security chain. A successful attack here could hand cybercriminals the keys to huge volumes of data. In addition to data theft attackers may be interested in deleting or

modifying information, which in some cases may be even more valuable for those who commission the attacks.

ATTACKS ON SOFTWARE DEVELOPERS

Something related to the problem mentioned above is the likely rise in attacks on software developers. In 2013, we uncovered a series of attacks staged by the Winnti cybercriminal gang. The victims of these attacks were gaming companies that had had their online games server sources stolen. Adobe was yet another victim – its Adobe Acrobat and Cold Fusion sources fell prey to the attackers. There are also earlier examples of successful attacks by the fraudsters: in 2011, they targeted RSA and managed to get hold of Secure ID source code which they used in a subsequent attack on Lockheed Martin.

The theft of popular product sources gives attackers an excellent opportunity to find vulnerabilities in the products and then to use them for their own fraudulent purposes. Additionally, if cybercriminals have access to the victim's repositories, they can modify the program source code and embed backdoors to them.

This again puts at risk the developers of mobile applications, which are created in their thousands and distributed to hundreds of millions of devices.

CYBER-MERCENARIES

Snowden's leaks have demonstrated that one of the goals of cyber espionage between states is to provide economic aid to "friendly" companies. This factor has broken down ethical barriers which initially restrained business from using radical methods to compete with their rivals. In the new realities of cyberspace, businesses are facing the possibility of conducting this kind of activity for themselves.

The companies will have to resort to business cyber-espionage as a means of remaining competitive because their rivals are already spying in order to get a competitive advantage. Some companies may even spy on government structures as well as on their employees, partners and suppliers.

This will only be possible if companies employ cyber-mercenaries, organized groups of qualified hackers who can offer bespoke cyber-espionage services. Most probably, these hackers will describe themselves as cyber-detectives.

In summer 2013 Kaspersky Lab detected commercial activity by the Icefog cyber-mercenary gang.

FRAGMENTATION OF THE INTERNET

Amazing things have happened to the Internet. Many experts, including Eugene Kaspersky, are talking about the need to create some kind of parallel "safe Internet" which won't allow anonymous users to roam, with potentially criminal intent. Meanwhile, cybercriminals have created their own Darknet based on Tor and I2P technologies allowing anonymous cybercriminal activity, commercial activity and communication.

At the same time, the Internet has begun to break up into national segments. Until recently this only really applied to the Great Firewall of China. But the People's Republic is no longer alone in its efforts to separate and manage their own Internet resources. Several countries, including Russia, have adopted or are planning to adopt legislation prohibiting the use of foreign services. Snowden's revelations have intensified the demand for these rules. In November, Germany announced that all communications between the German authorities would be fully locked within the country. Brazil has announced its plans to build an alternative Internet channel so as not to use the one that goes through Florida (USA).

The World Wide Web has begun to break up into pieces. Individual countries are no longer willing to let a single byte of information out of their networks. These aspirations will grow ever stronger and legislative restrictions will inevitably transform into technical prohibitions. The next step will most likely be attempts to limit foreign access to data inside a country.

As this trend develops further it will soon lead to the collapse of the current Internet, which will break into dozens of national networks. It is possible that some of them will prove unable to communicate with each other at all. The shadowy Darknet will be the only truly world-wide web.

THE PYRAMID OF CYBER-THREATS

The easiest way to describe the anticipated events and trends of 2014 is to do it graphically in the form of the pyramid of cyber-threats which we presented a year ago.

This pyramid consists of three levels. The threats used in attacks on ordinary users by regular cybercriminals driven solely by the prospect of financial gain are at the bottom of the pyramid. The middle level hosts the threats used in targeted corporate cyber-espionage attacks as well as so-called police spyware exploited by states to spy on their citizens and companies. The top of the pyramid is for the threats created by states to conduct cyber-attacks on other nations.

Most of these cyber-threat developments belong to the middle layer of threats. Therefore, in 2014 we expect significant growth in the number of threats related to economic and domestic cyber-espionage.

There will be an increase in such attacks as the cybercriminals currently attacking ordinary users transform into cyber-mercenaries and cyber-detectives. Furthermore, it is highly likely that cyber-mercenary services will be provided by IT specialists who have never before been engaged in criminal activity. The halo of legitimacy that comes with working for reputable companies will contribute to the development of this trend.