KASPERSKY lab

KASPERSKY SECURITY BULLETIN 2015

GREAT

#KLReport

CONTENT

TOP SECURITY STORIES

The end of the year is traditionally a time for reflection – for taking stock of our lives before considering what lies ahead. We'd like to offer our customary retrospective of the key events that have shaped the threat landscape in 2015.

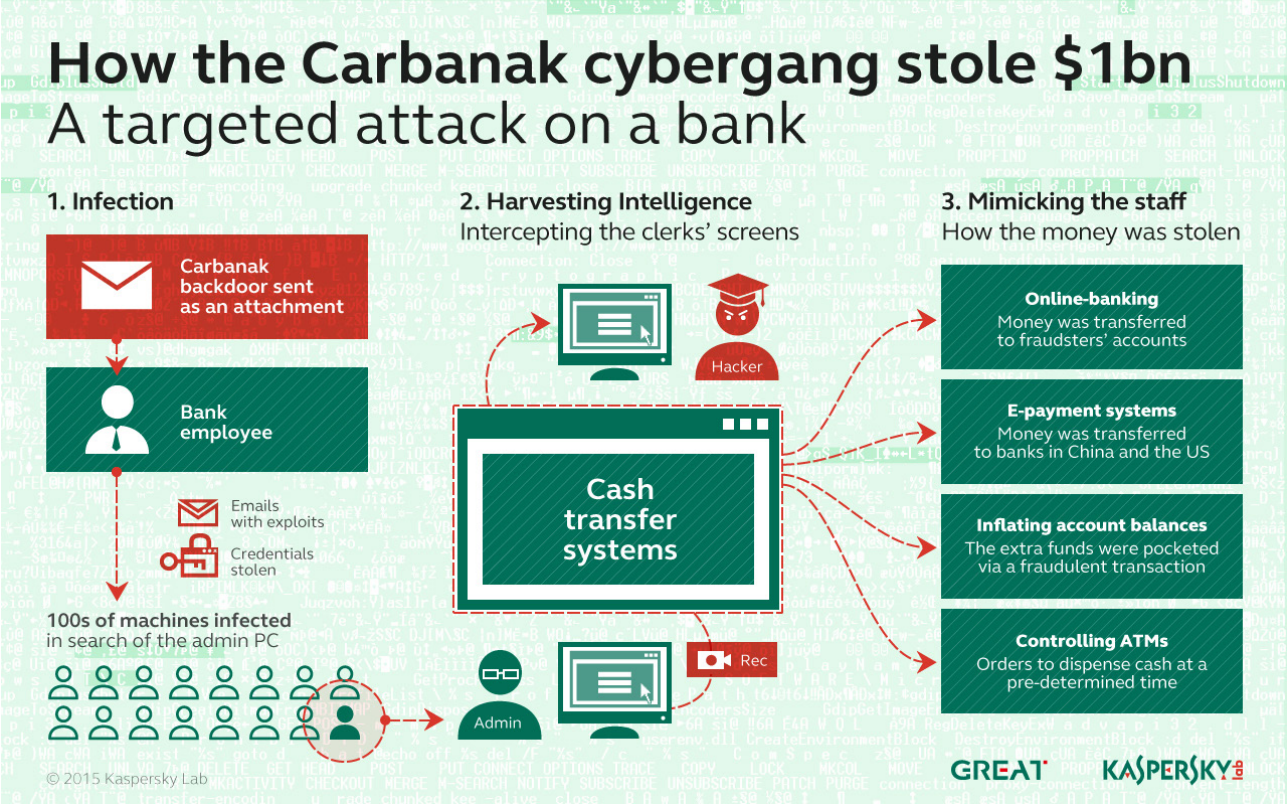
TARGETED ATTACKS AND MALWARE CAMPAIGNS

Targeted attacks are now an established part of the threat landscape, so it's no surprise to see such attacks feature in our yearly review. Last year, in our security forecast, we outlined what we saw as the likely future APT developments.

- The merger of cybercrime and APT
- Fragmentation of bigger APT groups
- Evolving malware techniques
- New methods of data exfiltration
- APT arms race

Here are the major APT campaigns that we reported this year.

Carbanak combined cybercrime – in this case, stealing money from financial institutions – with the infiltration techniques typical of a targeted attack. The campaign was uncovered in spring 2015: Kaspersky Lab was invited to conduct a forensic investigation of a bank's systems after some of its ATMs started to dispense cash 'randomly'. It turned out that the bank was infected. Carbanak is a backdoor designed to carry out espionage, data exfiltration and remote control of infected computers. The attackers used APT-style methods to compromise their victims – sending spear-phishing e-mails to bank employees. Once installed on a bank's computer, the attackers carried out reconnaissance to identify systems related to processing, accounting and ATMs and simply mimicked the activities of legitimate employees. Carbanak used three methods to steal money: (1) dispensing cash from ATMs, (2) transferring money to cybercriminals using the SWIFT network and (3) creating fake accounts and using mule services to collect the money. The attackers targeted around 100 financial institutions, with total losses amounting to almost $1 billion.



One of most talked-about news stories of Q1 2015 surrounded the Equation cyber-espionage group. The attackers behind Equation successfully infected the computers of thousands of victims in Iran, Russia, Syria, Afghanistan, the United States and elsewhere – victims included government and diplomatic institutions, telecommunications companies and energy firms. This is one of the most sophisticated APT campaigns we've seen: one of the many modules developed by the group modifies the firmware of hard drives – providing a level of stealth and persistence beyond other targeted attacks. It's clear that development of the code stretches back to 2001 or earlier. It's also related to other notorious attacks, Stuxnet and Flame – for example, its arsenal included two zero-day vulnerabilities that were later to be used in Stuxnet.

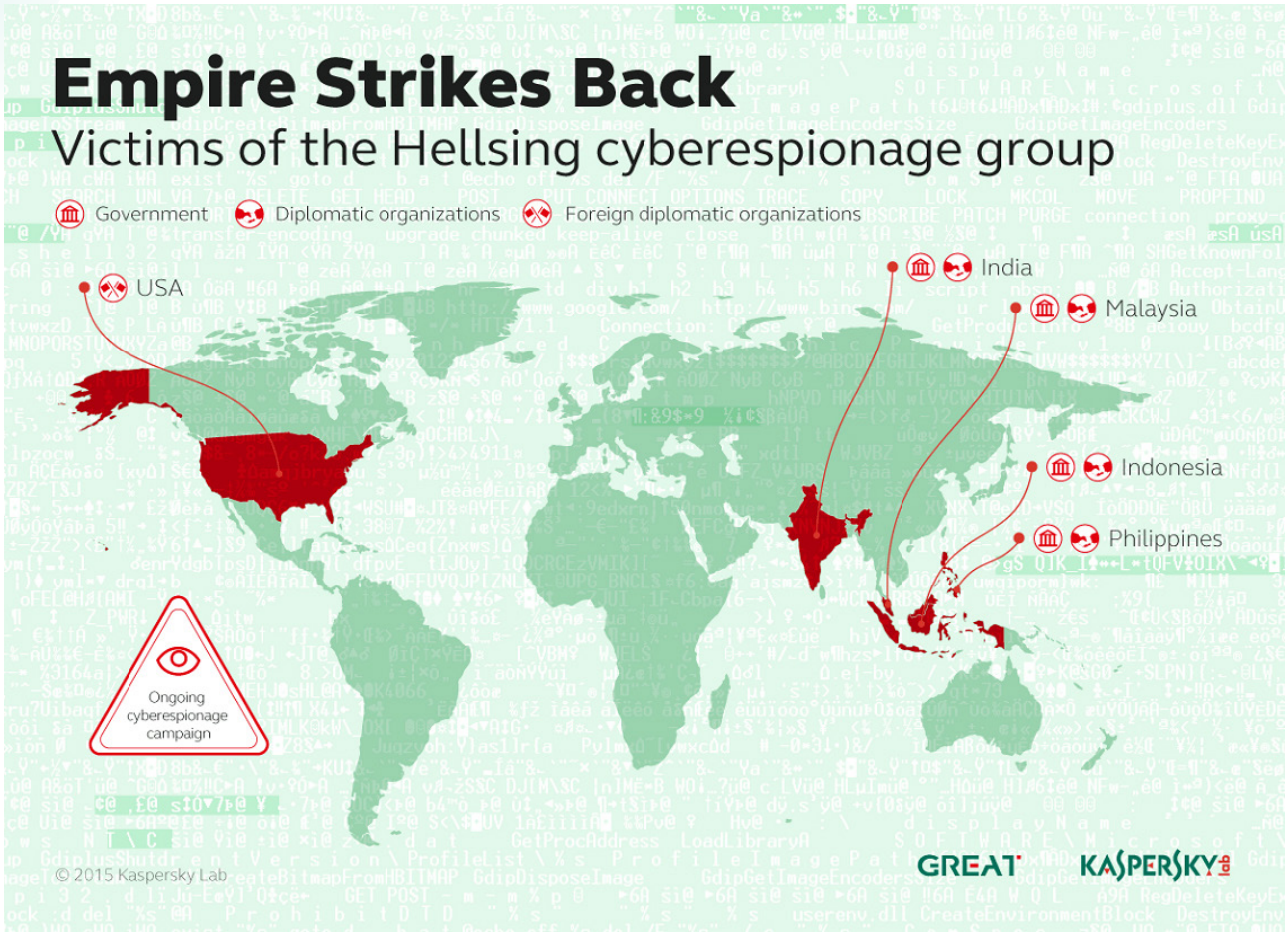
While investigating an incident in the Middle East, we uncovered the activity of a previously unknown group conducting targeted attacks. Desert Falcons is the first Arabic-speaking group that has been seen conducting full-scale cyber-espionage operations – apparently connected with the political situation in the region. The first signs of this campaign date back to 2011. The first infections took place in 2013, although the peak of activity was in late 2014 and early 2015. The group has stolen over 1 million files from more than 3,000 victims. The victims include political activists and leaders, government and military organizations, mass media and financial institutions – located primarily in Palestine, Egypt, Israel and Jordan. It's clear that members of the Desert Falcons group aren't beginners: they developed Windows and Android malware from scratch, and skillfully organized attacks that relied on phishing e-mails, fake web sites and fake social network accounts.

In March 2015, we published our report on the Animal Farm APT, although information on the tools used in this campaign started appearing in the previous year. In March 2014, the French newspaper, Le Monde, published an article on a cyber-espionage toolset that had been identified by Communications Security Establishment Canada (CSEC): this toolset had been used in the 'Snowglobe' operation that targeted French-speaking media in Canada, as well as Greece, France, Norway and some African countries. CSEC believed that the operation might have been initiated by French intelligence agencies. A year later, security researchers published analyses (here, here and here) of malicious programs that had much in common with 'Snowglobe': in particular, the research included samples with the internal name 'Babar' – the name of the program mentioned by CSEC. Following analysis of the malicious programs, and the connections between them, Kaspersky Lab named the group behind the attacks as Animal Farm. The group's arsenal included two of the three zero-day vulnerabilities that we had found in 2014 and that had been used by cybercriminals: for example, an attack from the compromised web site of the Syrian Ministry of Justice using CVE-2014-0515 exploits led to the download of an Animal Farm tool called 'Casper'. One curious feature of this campaign is that one of its programs, 'NBOT', is designed to conduct DDoS (Distributed Denial of Service) attacks. This is rare for APT groups. One of the malicious 'animals' in the farm has the strange name 'Tafacalou' – possibly an Occitan word (a language spoken in France and some other places).

In April 2015, we reported the appearance of a new member of a growing 'Duke' family that already includes MiniDuke, CosmicDuke and OnionDuke. The CozyDuke APT (also known as 'CozyBear', 'CozyCat' and 'Office Monkeys') targets government organisations and businesses in the United States, Germany, South Korea and Uzbekistan. The attack implements a number of sophisticated techniques, including the use of encryption, anti-detection capabilities and a well-developed set of components that are structurally similar to earlier threats within the 'Duke' family. However, one of its most notable features is its use of social engineering. Some of the attackers' spear-phishing e-mails contain a link to hacked web sites – including high-profile, legitimate sites – that host a ZIP archive. This archive contains a RAR SFX that installs the malware while showing an empty PDF as a decoy. Another approach is to send out fake flash videos as e-mail attachments. A notable example (one that gives the malware one of its names) is 'OfficeMonkeys LOL Video.zip'. When run, this drops a CozyDuke executable on to the computer, while playing a 'fun' decoy video showing monkeys working in an office. This encourages victims to pass the video around the office, increasing the number of compromised computers. The successful use of social engineering to trick staff into doing something that jeopardises corporate security – by CozyDuke and so many other targeted attackers – underlines the need to make staff education a core component of any business security strategy.

The Naikon APT focused on sensitive targets in south-eastern Asia and around the South China Sea. The attackers, who seem to be Chinese-speaking and have been active for at least five years, target top-level government agencies and civil and military organisations in the Philippines, Malaysia, Cambodia, Indonesia, Vietnam, Myanmar, Singapore, Nepal, Thailand, Laos and China. Like so many targeted attack campaigns, Naikon makes extensive use of social engineering to trick employees of target organizations into installing the malware. The main module is a remote administration tool that supports 48 commands designed to exercise control over infected computers: these include commands to take a complete inventory, download and upload data, install add-on modules and the use of keyloggers to obtain employees' credentials. The attackers assigned an operator to each target country, able to take advantage of local cultural features – for example, the tendency to use personal e-mail accounts for work. They also made use of a specific proxy server within a country's borders, to manage connections to infected computers and transfer of data to the attackers' Command-and-Control (C2) servers. You can find our main report and follow-up report on our web site.

While researching Naikon, we also uncovered the activities of the Hellsing APT group. This group focused mainly on government and diplomatic organisations in Asia: most victims are located in Malaysia and the Philippines, although we have also seen victims in India, Indonesia and the US. In itself, Hellsing is a small and technically unremarkable cyber-espionage group (around 20 organisations have been targeted by Hellsing). What makes it interesting is that the group found itself on the receiving end of a spear-phishing attack by the Naikon APT group – and decided to strike back! The target of the e-mail questioned the authenticity of the e-mail with the sender. They subsequently received a response from the attacker, but didn't open the attachment. Instead, shortly afterwards they sent an e-mail back to the attackers that contained their own malware. It's clear that, having detected that they were being targeted, the Hellsing group was intent on identifying the attackers and gathering intelligence on their activities. In the past, we've seen APT groups accidentally treading on each other's toes – for example, stealing address books from victims and then mass-mailing everyone on each of the lists. But an ATP-on-APT attack is unusual.

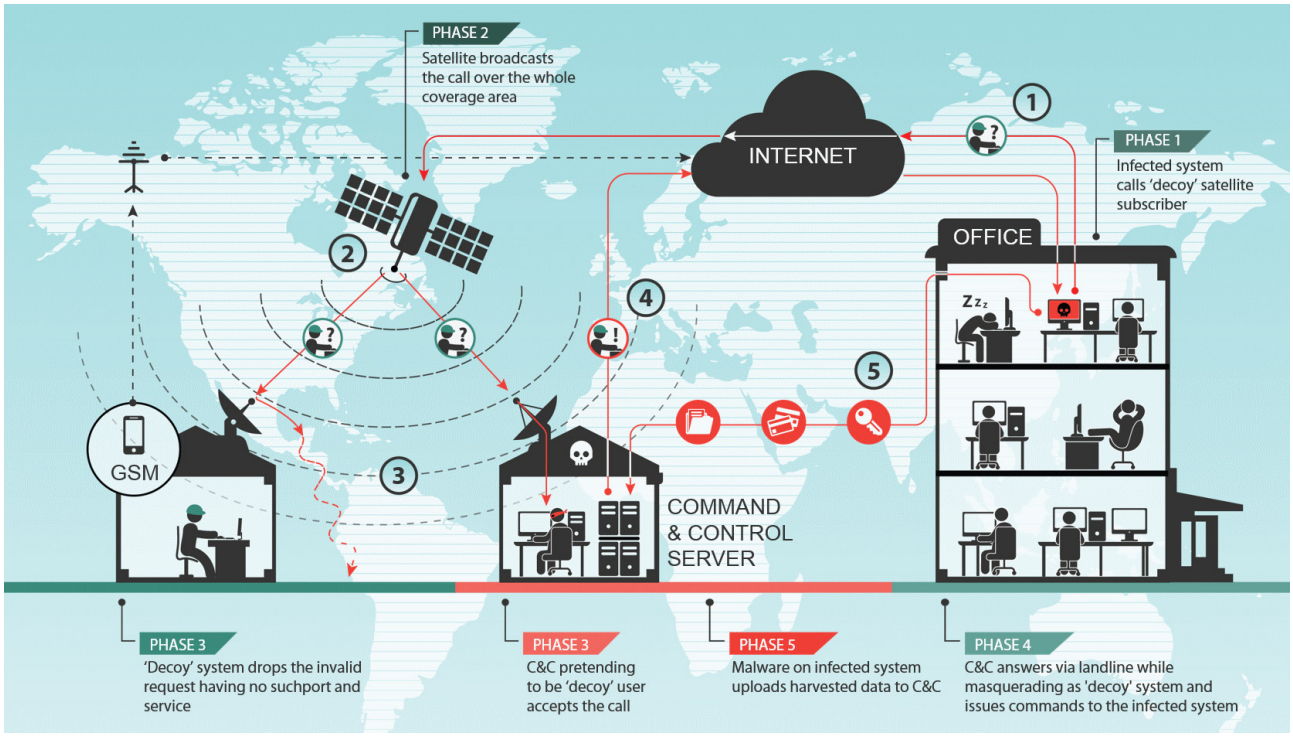


Many targeted attack campaigns focus on large enterprises, government agencies and other high-profile organisations. So it's easy to read the headlines and imagine that such organisations are the only ones on the radar of those behind targeted attacks. However, one of the campaigns we reported last quarter showed clearly that it's not only 'big fish' that attackers are interested in. The Grabit cyber-espionage campaign is designed to steal data from small- and medium-sized organisations – mainly based in Thailand, Vietnam and India, although we have also seen victims in the US, UAE, Turkey, Russia, China, Germany and elsewhere. The targeted sectors include chemicals, nanotechnology, education, agriculture, media and construction. We estimate that the group behind the attacks has been able to steal around 10,000 files. There's no question that every business is a potential target – for its own assets, or as a way of infiltrating another organisation.

In spring 2015, during a security sweep, Kaspersky Lab detected a cyber-intrusion affecting several internal systems. The full-scale investigation that followed uncovered the development of a new malware platform from one of the most skilled, mysterious and powerful groups in the APT world – Duqu, sometimes referred to as the step-brother of Stuxnet. We named this new platform 'Duqu 2.0'. In the case of Kaspersky Lab, the attack took advantage of a zero-day vulnerability in the Windows kernel (patched by Microsoft on 9 June 2015) and possibly up to two others (now patched) that were also zero-day vulnerabilities at the time. The main goal of the attackers was to spy on Kaspersky Lab technologies, ongoing research and internal processes. However, Kaspersky Lab was not the only target. Some Duqu 2.0 infections were linked to the P5+1 events related to negotiations with Iran about a nuclear deal: the attackers appear to have launched attacks at the venues for some of these high-level talks. In addition, the group launched a similar attack related to the 70th anniversary event of the liberation of Auschwitz-Birkenau. One of the most notable features of Duqu 2.0 was its lack of persistence, leaving almost no traces in the system. The malware made no changes to the disk or system settings: the malware platform was designed in such a way that it survives almost exclusively in the memory of infected systems. This suggests that the attackers were confident that they could maintain their presence in the system even if an individual victim's computer was re-booted and the malware was cleared from memory. The Duqu 2.0 technical paper and analysis of the persistence module can be found on our web site.

In August, we reported on the Blue Termite APT, a targeted attack campaign focused on stealing information from organisations in Japan. These include government agencies, local government bodies, public interest groups, universities, banks, financial services, energy, communication, heavy industry, chemical, automotive, electrical, news media, information services sector, health care, real estate, food, semiconductor, robotics, construction, insurance, transportation and more. One of the most high profile targets was the Japan Pension Service. The malware is customized according to the specific victim. The Blue Termite backdoor stores data about itself – including C2, API name, strings for anti-analysis, values of mutexes, as well as the MD5 checksum of backdoor commands and the internal proxy information. The data is stored in encrypted form, making analysis of the malware more difficult – a unique decryption key is required for each sample. The main method of infection, as with so many targeted attack campaigns, is via spear-phishing e-mails. However, we have other methods of infection. These include drive-by downloads using a Flash exploit (CVE-2015-5119) – one of the exploits leaked following the Hacking Team security breach – several Japanese web sites were compromised this way. We also found some watering-hole attacks, including one on a web site belonging to a prominent member of the Japanese government.

The group behind the Turla cyber-espionage campaign has been active for more than eight years now (our initial report, follow-up analysis and campaign overview can be found on securelist.com), infecting hundreds of computers in more than 45 countries. The attackers profile their victims using watering-hole attacks in the initial stages. However, as outlined in our latest report, for subsequent operations the group makes use of satellite communications to manage its C2 traffic. The method used by Turla to hijack downstream satellite links does not require a valid satellite Internet subscription. The key benefit is that it's anonymous – it's very hard to identify the attackers. The satellite receivers can be located anywhere within the area covered by the satellite (typically a wide area) and the true location and hardware of the C2 server can't be identified easily or physically seized. It's also cheaper than purchasing a satellite-based link and easier than hijacking traffic between the victim and the satellite operator and injecting packets along the way. The Turla group tends to focus on satellite Internet providers located in the Middle East and Africa, including Congo, Lebanon, Libya, Niger, Nigeria, Somalia and the UAE. Satellite broadcasts from these countries don't normally cover European and North American countries, making it very hard for security researchers to investigate such attacks. The use of satellite-based Internet links is an interesting development. The hijacking of downstream bandwidth is cheap (around $1,000 for the initial investment and around $1,000 per year in maintenance), easy to do and offers a high degree of anonymity. On the other hand, it is not always as reliable as more traditional methods (bullet-proof hosting, multiple proxy levels and hacked web sites) – all of which Turla also uses. This makes it less likely that it will be used to maintain extensive botnets. Nevertheless, if this method becomes widespread among APT groups or cybercriminals, it will pose a serious problem for the IT security industry and law enforcement agencies.



In August 2015, we published an update on the Darkhotel APT. These attacks were originally characterised by the misuse of stolen certificates, the deployment of HTA files using multiple methods and the infiltration of hotel Wi-Fi to place backdoors on targets' computers.

While the attackers behind this APT continue to use these methods, they have supplemented their armoury, shifting their attention more towards spear-phishing of their chosen victims. As well as using HTA files, they are also deploying infected RAR files, using the RTLO (right to left override) mechanism to mask the real extension of the file. The attackers also use Flash exploits, including a zero-day exploit leaked as a result of the Hacking Team security breach. The group has also extended its geographic reach to include victims in North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, India, Mozambique and Germany.

DATA BREACHES

There has been a steady stream of security breaches this year. That such incidents have become routine is hardly surprising: personal information is a valuable commodity – not just for legitimate companies, but for cybercriminals too. Among the biggest incidents this year were attacks on Anthem, LastPass, Hacking Team, the United States Office of Personnel Management, Ashley Madison, Carphone Warehouse, Experian and TalkTalk. Some of these attacks resulted in the theft of huge amounts of data, highlighting the fact that many companies are failing to take adequate steps to defend themselves. It's not simply a matter of defending the corporate perimeter. There's no such thing as 100 per cent security, so it's not possible to guarantee that systems can't be breached, especially where someone on the inside is tricked into doing something that jeopardises corporate security. But any organisation that holds personal data has a duty of care to secure it effectively. This includes hashing and salting customer passwords and encrypting other sensitive data.

On the other hand, consumers can limit the damage of a security breach at an online provider by ensuring that they choose passwords that are unique and complex: an ideal password is at least 15 characters long and consists of a mixture of letters, numbers and symbols from the entire keyboard. As an alternative, people can use a password manager application to handle all this for them automatically.

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

The theft of personal data can have serious consequences for those affected. However, sometimes there can be serious knock-on effects. The Hacking Team breach resulted in the publication of 400GB of data: this included exploits used by the Italian company in its surveillance software. Some of the exploits were used in APT attacks – Darkhotel and Blue Termite. Unsurprisingly, the breach was followed by a scramble to patch the vulnerabilities exposed by the attackers.

SMART (BUT NOT NECESSARILY SECURE) DEVICES

The Internet is woven into the fabric of our lives – literally in the case of the growing number of everyday objects used in the modern home – smart TVs, smart meters, baby monitors, kettles and more. You may remember that last year one of our security researchers investigated his own home, to determine whether it was really cyber-secure. You can find a follow-up to this research here. However, the 'Internet of Things' encompasses more than household devices.

Researchers have been investigating the potential security risks associated with connected cars for some years. In July 2014 Kaspersky Lab and IAB published a study looking at the potential problem areas of connected cars. Until this year, the focus was on accessing the car's systems by means of a physical connection to the vehicle. This changed when researchers Charlie Miller and Chris Valasek found a way to gain wireless access to the critical systems of a Jeep Cherokee – successfully taking control and driving it off the road! (You can read the story here).

This story underlines some of the problems with connected devices that extend beyond the car industry – to any connected device. Unfortunately, security features are hard to sell; and in a competitive marketplace, things that make customers' lives easier tend to take precedence. In addition, connectivity is often added to a pre-existing communication network that wasn't created with security in mind. Finally, history shows that security tends to be retro-fitted only after something bad happens to demonstrate the impact of a security weakness. You can read more on these issues in a blog post written by Eugene Kaspersky published in the aftermath of the above research.

Such problems apply also to 'smart cities'. For example, the use of CCTV systems by governments and law enforcement agencies to monitor public places has grown enormously in recent years. Many CCTV cameras are connected wirelessly to the Internet, enabling police to monitor them remotely. However, they are not necessarily secure: there's the potential for cybercriminals to passively monitor security camera feeds, to inject code into the network – thereby replacing a camera feed with fake footage – or to take systems offline. Two security researchers (Vasilios Hioureas from Kaspersky Lab and Thomas Kinsey from Exigent Systems) recently conducted research into the potential security weaknesses in CCTV systems in one city. You can read Vasilios's report on our web site).

Unfortunately, there had been no attempt to mask the cameras, so it was easy to determine the makes and models of the cameras being used, examine at the relevant specifications and create their own scaled model in the lab. The equipment being used provided effective security controls, but these controls were not being implemented. Data packets passing across the mesh network were not being encrypted, so an attacker would be able to create their own version of the software and manipulate data travelling across it. One way this could potentially be used by attackers would be to spoof footage sent to a police station, making it appear as if there is an incident in one location, thereby distracting police from a real attack occurring somewhere else in the city.

The researchers reported the issues to those in charge of the real world city surveillance system and they are in the process of fixing the security problems. In general, it's important that WPA encryption, protected by a strong password, is implemented in such networks; that labelling is removed from hardware, to make it harder for would-be attackers to find out how the equipment operates; and to encrypt footage as it travels through the network.

The wider issue here is that more and more aspects of everyday life are being made digital: if security isn't considered at the design stage, the potential dangers could be far-reaching – and retro-fitting security might not be straightforward. The Securing Smart Cities initiative, supported by Kaspersky Lab, is designed to help those responsible for developing smart cities to do so with cyber-security in mind.

INTERNATIONAL CO-OPERATION AGAINST CYBERCRIMINALS

Cybercrime is now an established part of life, on the back of the ever-increasing online activities we engage in. This is now being reflected in official statistics. In the UK, for example, the Office for National Statistics now includes cybercrime among its estimates of the scale of crime, reflecting the fact that nature of crime in society is changing. While there's no question that cybercrime can be lucrative, cybercriminals aren't always able to act with impunity; and the actions of law enforcement agencies around the world can have a significant impact. International co-operation is particularly important, given the global nature of cybercrime. This year there have been some notable police operations.

In April, Kaspersky Lab was involved in the take-down of the Simda botnet, co-ordinated by the Interpol Global Complex for Innovation. The investigation was started by Microsoft and expanded to other participants, including Trend Micro, the Cyber Defense Institute, officers from the Dutch National High Tech Crime Unit (NHTCU), the FBI, the Police Grand-Ducale Section Nouvelles Technologies in Luxembourg, and the Russian Ministry of the Interior's Cybercrime Department 'K' supported by the INTERPOL National Central Bureau in Moscow. As a result of the operation, 14 servers in the Netherlands, the US, Luxembourg, Poland and Russia were taken down. Preliminary analysis of some of the sink-holed server logs revealed that 190 countries had been affected by the botnet.

In September, the Dutch police arrested two men for suspected involvement in CoinVault ransomware attacks, following a joint effort by Kaspersky Lab, Panda Security and the Dutch National High Tech Crime Unit (NHTCU). This malware campaign started in May 2014 and continued into this year, targeting victims in more than 20 countries, with the majority of victims in the Netherlands, Germany, the United States, France and Great Britain. They successfully encrypted files on more than 1,500 Windows-based computers, demanding payment in bitcoin to decrypt data. The cybercriminals responsible for this ransomware campaign modified their creations several times to keep on targeting new victims. In November 2014, Kaspersky Lab and the Dutch NHTCU launched a web site to act as a repository of decryption keys; and we also made available online a decryption tool to help victims recover their data without having to pay the ransom. You can find our analysis of the twists and turns employed by the CoinVault authors here. Ransomware has become a notable fixture of the threat landscape. While this case shows that collaboration between researchers and law enforcement agencies

can lead to positive results, it's essential for consumers and businesses alike to take steps to mitigate the risks of this type of malware. Ransomware operations rely on their victims paying up. In September, an FBI agent caused controversy by suggesting that victims should pay the ransom in order to recover their data. While this might seem to be a pragmatic solution (not least because there are situations where recovery of data is not possible), it's a dangerous strategy. First, there's no guarantee that the cybercriminals will provide the necessary mechanism to decrypt the data. Second, it reinforces their business model and makes the further development of ransomware more likely. We would recommend that businesses and individuals alike make regular backups of data, to avoid being put in this invidious position.

ATTACKS ON INDUSTRIAL OBJECTS

Incidents caused by cybersecurity problems are a fairly regular occurrence at industrial objects. For example, according to US ICS CERT data, 245 such incidents were recorded in the US during the 2014 fiscal year, and 22 incidents in July and August 2015. However, we believe these numbers do not reflect the actual situation: there are many more cyber incidents than this. And while enterprise operators and owners prefer to keep quiet about some of these incidents, they are simply unaware of others.

Let's have a look at two cases that caught our attention in 2015.

One is an incident that took place at a steel mill in Germany. Towards the end of 2014, the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) published a report which mentioned a cyber incident at a German steel mill. Theincident resulted in physical damage to a blast furnace.

This is the second cyberattack that we know of, after Stuxnet, to cause physical damage to industrial facilities. According to BSI, the attackers first used phishing emails to infect the enterprise's office network, after which the hackers managed to infect a SCADA computer and attack the physical equipment. Unfortunately, BSI did not provide any additional information, so we do not know which malware was used and how it operated.

This secrecy is bad for everybody: operators of other similar enterprises (with the possible exception of German facilities) will not be able to analyze the attack and implement countermeasures; cybersecurity experts are also in the dark and are unable to suggest security measures to their customers.

Another curious incident was an attack against the Frederic Chopin Airport in Warsaw in June 2015., The computer system responsible for preparing flight plans for LOT, Poland's national airline, was taken down for about five hours one Sunday. According to Reuters, this caused delays to a dozen flights.

The airport management provided no details and experts had to form their opinions based on their experience. Ruben Santamarta, Principal Security Consultant at IOActive, has previously called attention to IT security issues in aviation. Based on what the LOT representatives said, he suggested that the company had fallen victim to a targeted attack: the system couldn't generate flight plans because key nodes in the back office were compromised, or perhaps the attack targeted ground communication devices, resulting in the inability to perform or validate data loading on aircraft (including flight plans).

Our experts also responded to the incident, suggesting there could be two possible scenarios. The incident may have been the result of human error or equipment malfunction. Alternatively, the incident at the relatively small Warsaw airport could be a precursor of larger-scale attacks in other, much larger, airports.

It was later announced that a DDoS attack had taken place and that no penetration had actually taken place. Once again, no detailed information about the incident was disclosed and we can either believe the official information or guess at the real reasons and goals of the attack.

Whoever was behind the attacks described above and whatever goals they pursued, these incidents clearly demonstrate how significant a part of our lives computers have become and how vulnerable infrastructure objects have become in recent years.

Unfortunately, today many governments and regulators resort to a policy of secrecy. We believe that transparency and the exchange of information about cyberattacks is an important part of providing adequate protection for industrial objects. Without this knowledge, it is very hard to protect these objects against future threats.

In conclusion, we would like to mention one more trend that is already relevant and will continue to affect us all in the coming years: the hardware used by industrial enterprises is being actively connected to the Web. The Internet may have appeared quite a long time ago, but it is only now that it is being introduced to industrial processes. It is no exaggeration to say that this represents a new industrial revolution: we are witnessing the birth of the 'Industrial Internet of Things' or Enterprise 4.0. As a result, enterprises receive a whole host of additional benefits and can improve their manufacturing efficiency.

In order to keep up with this trend, equipment manufacturers simply add sensors and controllers to proven, safe and reliable equipment originally developed for the 'offline' world, provide Internet connectivity for their devices and then offer this 'new equipment' to customers. They forget, however, that when online features are added to any device, this gives rise to new cybersecurity-related risks and threats. This is no longer a 'physical' device, but a 'cyber-physical' one.

In the world of physical devices, all industrial devices, instruments, communication protocols, etc. were designed with safety in mind – in other words, they were built to be foolproof. This meant that if a device was designed to meet functional safety requirements, operating it without violating the safety rules would not result in any failures or damage to people or the environment.

Enterprise 4.0 brings with it a new security dimension: IT security or protection against intentional external manipulation. You cannot simply connect an object or device from the pre-Internet era to the Internet: the consequences of this can be – and often are – disastrous.

Engineers who embrace old 'pre-revolutionary' design principles often fail to realize that their devices can now be 'operated' not only by engineers, who know which actions are admissible and which are not, but also by hackers for whom there is no such thing as inadmissible remote object operations. This is one of the main reasons why today some well-established companies with many years of experience offer hardware that may be reliable from the point of view of functional safety, but which does not provide an adequate level of cybersecurity.

In the world of cyber-physical devices, physical and cyber components are tightly integrated. A cyberattack can disrupt an industrial process, damage equipment or cause a technogenic disaster. Hackers are a real threat and anything that is connected to the Internet can be attacked. This is why equipment manufacturers, when designing new connected industrial equipment, should be as careful about implementing protection against cyberthreats as they are about designing functional safety features.

CONCLUSION

In 2015, perhaps for the first time in the entire history of the Internet, issues related to protecting networks and being protected online were discussed in connection with every sector of the economy and with people's everyday life. Choose any sector of modern civilization – finances, industrial production, cars, planes, wearable devices, healthcare and many others – and you will be sure to find publications this year on incidents or cybersecurity problems related to that sector.

Regrettably, cybersecurity has now become inseparably linked with terrorism. Defensive, as well as offensive, methods used online are attracting lots of interest from various illegal organizations and groups.

Cybersecurity issues have risen to the level of top diplomats and government officials. In 2015, cybersecurity agreements were signed between Russia and China, China and the US, China and the UK. In these documents, governments not only agree to cooperate, but also accept the responsibility to refrain from any attacks on each other. At the same time, there was extensive discussion of recent changes to the Wassenaar Arrangement restricting spyware exports. A recurring theme of the year was the use of insecure email services by various political figures across the globe, including the then US Secretary of State Hillary Clinton.

All this has led to a huge surge in interest in cybersecurity issues, not only from the mass media but also from the entertainment industry. There were feature films and TV series produced, some of them starring cybersecurity experts, sometimes as themselves.

The word cybersecurity became fashionable in 2015, but this does not mean the problem has been solved. We are seeing what amounts to exponential growth in everything related to cybercrime, including increases in the number of attacks and attackers, the number of victims, defense and protection related costs, laws and agreements that regulate cybersecurity or establish new standards. For us, this is primarily about the sophistication of the attacks we detect. The confrontation is now in the active stage, with the final stage not even on the horizon.

To find out what to expect in the nearest future, read our predictions for 2016.

EVOLUTION OF CYBER THREATS IN THE CORPORATE SECTOR

In late 2014, we published predictions for how the world of cyber threats may evolve in 2015. Four of the nine predictions we made were directly connected with threats to businesses. Our predictions proved accurate – three of the four business-related threats have already been fulfilled:

- Cybercriminals embrace APT tactics for targeted attacks – yes.
- APT groups fragment, diversify attacks – yes.
- Escalation of ATM and PoS attacks – yes.
- Attacks against virtual payment systems – no.

Let's have a look back at the major incidents of 2015 and at the new trends we have observed in information security within the business environment.

THE YEAR IN FIGURES

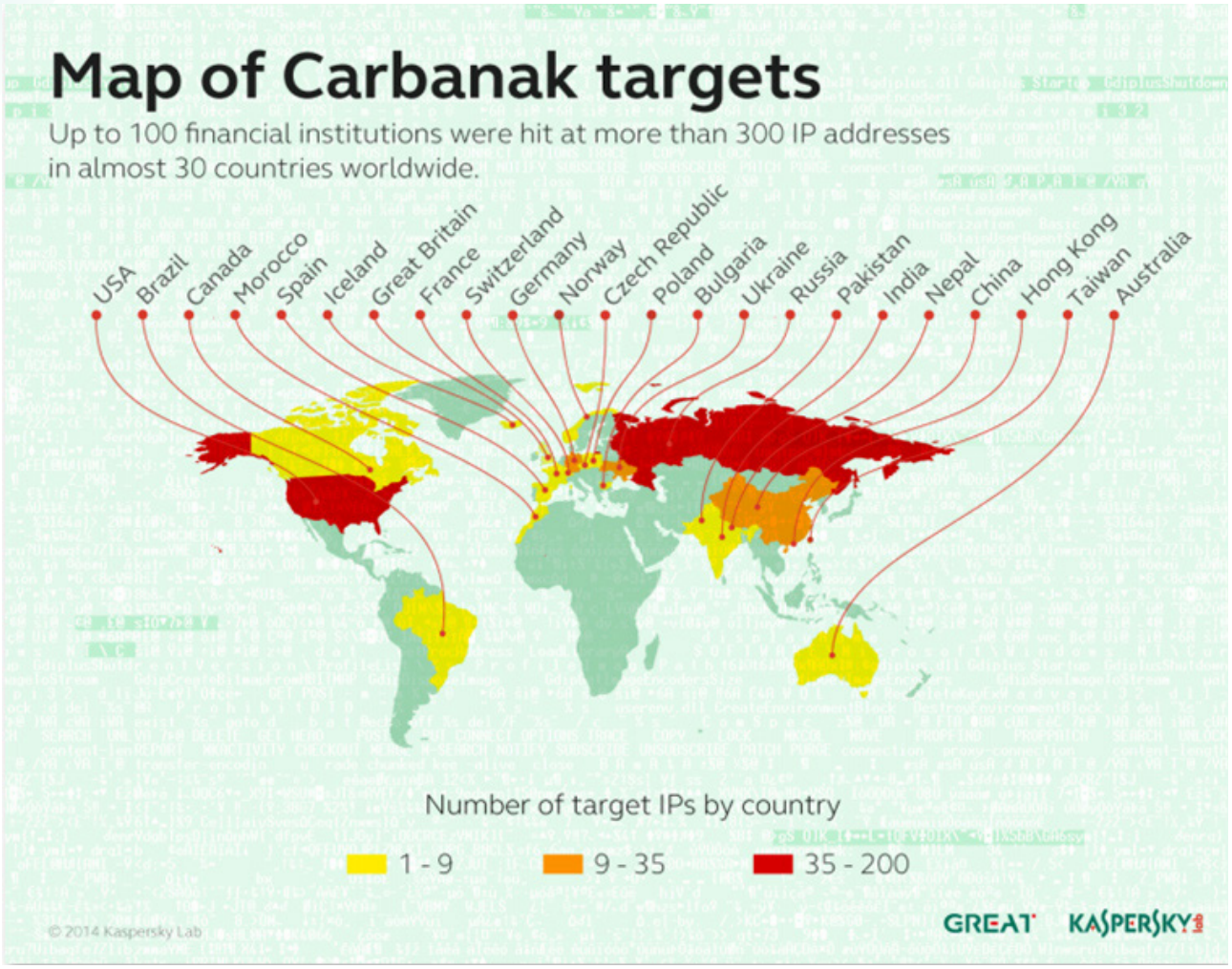
- In 2015 one or more malware attacks were blocked on 58% of corporate computers. This is a 3 p.p. rise on the previous year.
- 29% of computers – i.e. almost every third business-owned computer – were subjected to one or more web-based attacks.
- Malware exploiting vulnerabilities in office applications were used 3 times more often than in attacks against home users.
- File antivirus detection was triggered on 41% of corporate computers (objects were detected on computers or on removable media connected to computers: flash drives, memory cards, telephones, external hard drives, or network disks).

TARGETED ATTACKS ON BUSINESSES: APT AND CYBERCRIMINALS

2015 saw a number of APT attacks launched against businesses. The toolkits and methods used were very similar to those we observed when analyzing earlier APT attacks, but it was cybercriminals rather than state-sponsored groups who were behind the attacks. The methods used may not be characteristic of cybercriminals, but the main aim of their attacks remained the same: financial gain.

The Carbanak campaign became a vivid example of how APT-class targeted attacks have shifted focus to financial organizations. The campaign was one of bona fide bank robberies in the digital age: the cybercriminals penetrated a bank's network looking for a critical system, which they then used to siphon off money. After stealing a hefty sum (anywhere between $2.5 million and $10 million) from a bank, they moved on to the next victim.

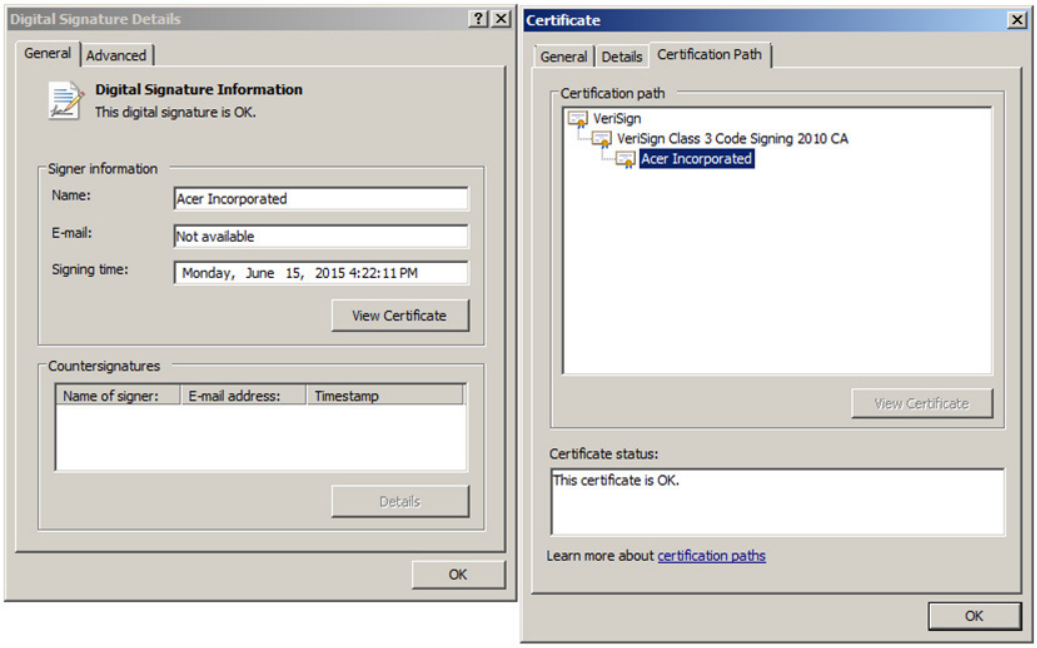
Most of the organizations targeted were located in Eastern Europe. However, the Carbanak campaign has also targeted victims in the US, Germany and China. Up to 100 financial institutions have been affected across the globe, and the total losses could be as a high as $1 billion.



It shouldn't be forgotten that information can also be of great value, especially if it can be used when making deals or trading on the stock exchange, be it in commodities, securities or currency markets, including cryptocurrency markets. One example of a targeted attack that may have been hunting for such information is Wild Neutron (aka Jripbot and Morpho). This cyber-espionage campaign first hit the headlines in 2013 when it affected several reputable companies, including Apple, Facebook, Twitter and Microsoft. After these incidents received widespread publicity the actors behind the cyberespionage campaign suspended their activities. However, about a year later Kaspersky Lab observed that Wild Neutron had resumed operations.

Our research has shown that the cyberespionage campaign caused infections on user computers in 11 countries and territories, namely Russia, France, Switzerland, Germany, Austria, Slovenia, Palestine, the United Arab Emirates, Kazakhstan, Algeria and the US. The victims included law firms, investment companies, bitcoin-related companies, enterprises and business groups involved in M&A deals, IT companies, healthcare companies, real estate companies, as well as individual users.

It should be noted that Wild Neutron used a code signing certificate stolen from Acer.

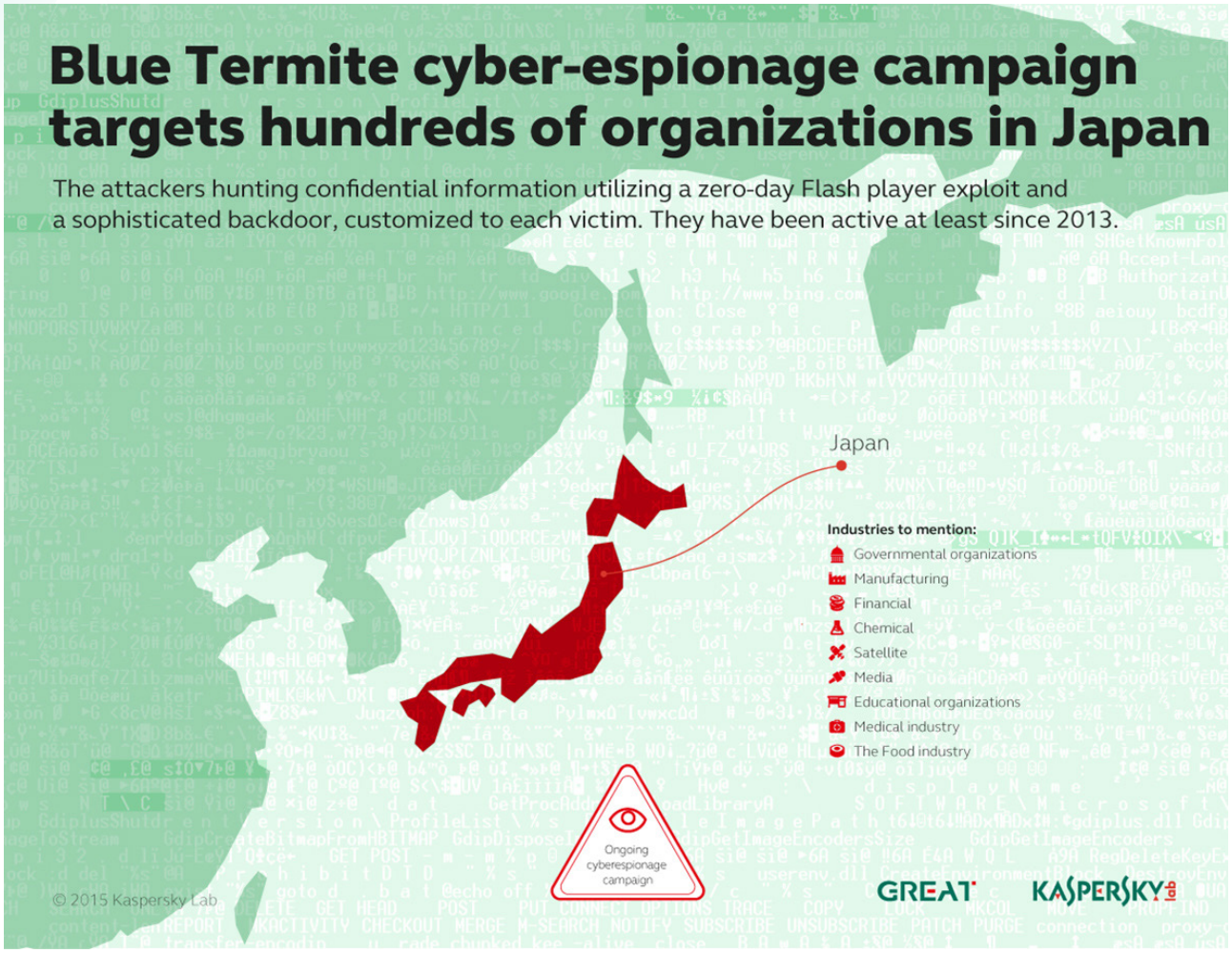


Stolen Acer certificate in the Wild Neutron installer

The trend towards the diversification of APT attacks is well illustrated by the change in targets attacked by the Chinese cybercriminal group Winnti. It was a long-held belief that Winnti only attacked computer gaming companies. However, in autumn 2015 evidence began to emerge that showed the group had performed a test run of their tools and methods and were trying to make money by attacking new targets. Their attention is no longer limited to the entertainment industry, with recent targets including pharmaceutical and telecom companies. Analysis of the new wave of Winnti attacks has revealed that (as with Wild Neutron) the Winnti rootkit was signed with a stolen certificate that belonged to a division at a major Japanese conglomerate.

Another development in 2015 was the expanding geographies of both the attacks and the attackers. For example, when Kaspersky Lab experts were investigating a Middle East incident, they came across activity by a previously unknown group conducting targeted attacks. The group, dubbed the Desert Falcons, is the first Arab actor to conduct full-blown cyberespionage attacks. At the time the group was detected, its victims numbered around 300, including financial organizations.

Another group named Blue Termite attacked organizations and companies in Japan:



Information about targeted attacks on businesses is available in the following Kaspersky Lab reports: Carbanak, Wild Neutron, Winnti, DarkHotel 2015, Desert Falcons, Blue Termit, Grabit. More detailed research results are provided to subscribers of the Kaspersky Intelligence Service.

Analysis of these attacks has identified several trends in the evolution of targeted attacks on businesses:

- Financial organizations such as banks, funds and exchange-related companies, including cryptocurrency exchanges, have been subjected to attacks by cybercriminals.
- The attacks are meticulously planned. The cybercriminals scrutinize the interests of potential victims (employees at the targeted company), and identify the websites they are most likely to visit; they examine the targeted company's contacts, equipment and service providers.

- The information collected at the preparation stage is then put to use. The attackers hack legitimate websites that have been identified and the business contact accounts of the targeted company's employees. The sites and accounts are used for several hours to distribute malicious code, after which the infection is deactivated. This means the cybercriminals can re-use the compromised resources again later.
- Signed files and legitimate software is used to collect information from the attacked network.
- Attacks are diversifying to include small and medium-sized businesses.
- The geography of attacks on businesses is expanding: a massive attack occurred in Japan, the emergence of new APT groups in Arab countries.

Although there are relatively few APT attacks launched by cybercriminals, the way they are developing will undoubtedly influence the methods and approaches employed by other cybercriminals in their operations against businesses.

STATISTICS

The statistics for corporate users (including the geography of attacks and ratings for detected objects) tend to coincide with those for home users. This is unsurprising because business users do not exist in an isolated environment and their computers are targeted by cybercriminals who spread malware irrespective of the nature of the target. These types of attacks and malware constitute the majority, while attacks specifically targeting business users have little impact on the overall statistics.

In 2015, one or more malware attack was blocked on 58% of corporate user computers, which is a 3 p.p. rise on last year.

Online threats (Web-based attacks)

In 2015, almost every third (29%) computer in a business environment was subjected to one or more web-based attacks.

TOP 10 web-based malicious programs

Please note that this ranking includes malicious programs only, and no adware. Although intrusive and annoying for users, adware does not cause any damage to a computer.

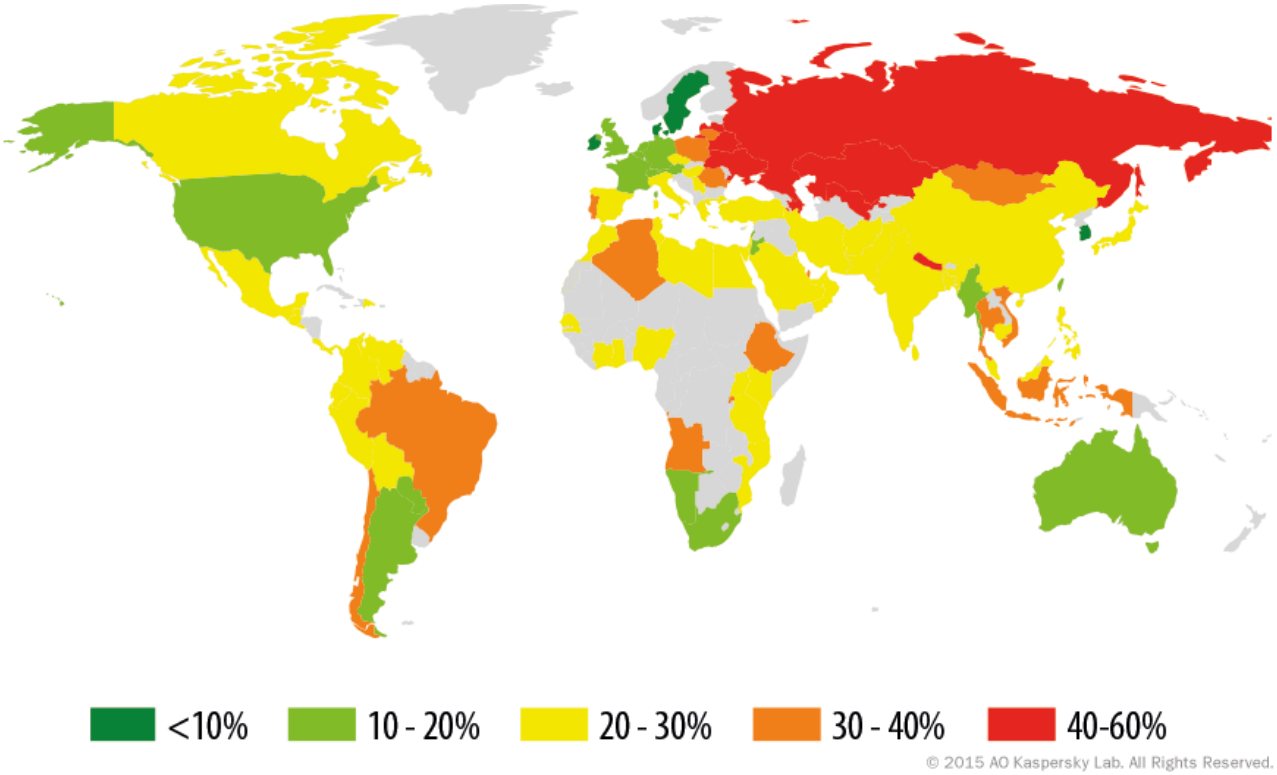
	Name*	% of unique users attacked**
1	Malicious URL	57%
2	Trojan.Script.Generic	24.7%
3	Trojan.Script.Iframer	16.0%
4	Exploit.Script.Blocker	4.1%
5	Trojan-Downloader.Win32.Generic	2.5%
6	Trojan.Win32.Generic	2.3%
7	Trojan-Downloader.JS.Iframe.diq	2.0%
8	Exploit.Script.Generic	1.2%
9	Packed.Multi.MultiPacked.gen	1.0%
10	Trojan-Downloader.Script.Generic	0.9%

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

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

This Top 10 consists almost exclusively of verdicts assigned to malicious objects that are used in drive-by attacks – Trojan downloaders and exploits.

Geography of web-based attacks



Geography of web-based attacks in 2015
(percentage of attacked corporate users in each country)

Local threats

The file antivirus detection was triggered on 41% of corporate user computers. The detected objects were located on computers or on removable media connected to the computers, such as flash drives, memory cards, telephones, external hard drives and network drives.

TOP 10 malicious programs detected on user computers

This ranking includes malicious programs only, and no adware. Although intrusive and annoying for users, adware does not cause any damage to a computer.

	Name*	% unique users attacked**
1	DangerousObject.Multi.Generic	23.1%
2	Trojan.Win32.Generic	18.8%
3	Trojan.WinLNK.StartPage.gena	7.2%
4	Trojan.Win32.AutoRun.gen	4.8%
5	Worm.VBS.Dinihou.r	4.6%
6	Net-Worm.Win32.Kido.ih	4.0%
7	Virus.Win32.Sality.gen	4.0%

	Name*	% unique users attacked**
8	Trojan.Script.Generic	2.9%
9	DangerousPattern.Multi.Generic	2.7%
10	Worm.Win32.Debris.a	2.6%

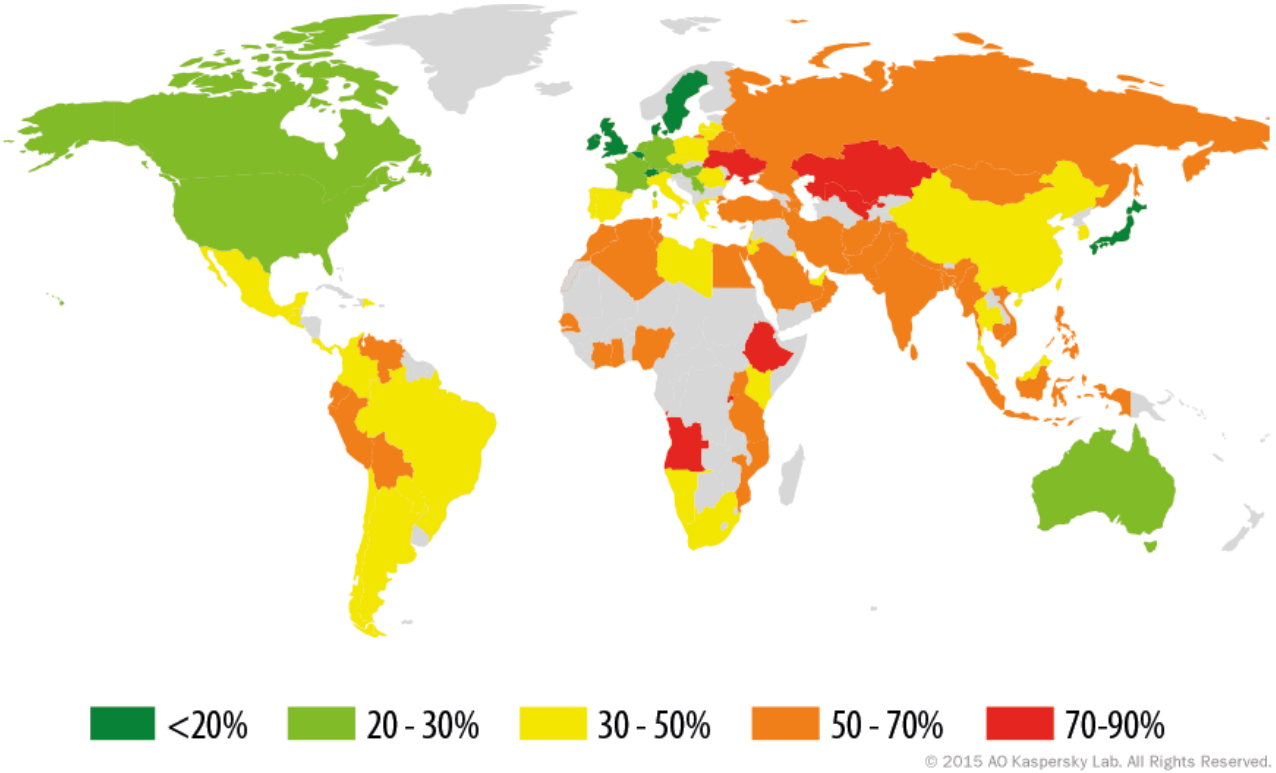
** These statistics are compiled from malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who have consented to submit their statistical data.*

*** The proportion of individual users on whose computers the antivirus module detected these objects as a percentage of all attacked individual users.*

First place is occupied by various malicious programs that were detected with the help of cloud technologies, and assigned the umbrella verdict of 'DangerousObject.Multi.Generic'. Cloud technologies work when antivirus databases do not yet contain signatures or heuristics to detect a malicious program but the company's cloud antivirus database already includes information about the object. When a client company cannot send statistics to the cloud, Kaspersky Private Security Network is used instead, meaning that network computers receive protection from the cloud.

Most of the remaining positions in the ranking are occupied by self-propagating malware programs and their components.

Geography of local threats



Geography of local threat detections in 2015
(percentage of attacked corporate users in each country)

CHARACTERISTICS OF ATTACKS ON BUSINESSES

The overall statistics for corporate users do not reflect the specific attributes of attacks launched against businesses; the stats are influenced more by the probability of a computer infection in a country, or by how popular a specific malware program is with cybercriminals.

However, a more detailed analysis reveals the peculiarities of attacks on corporate users:

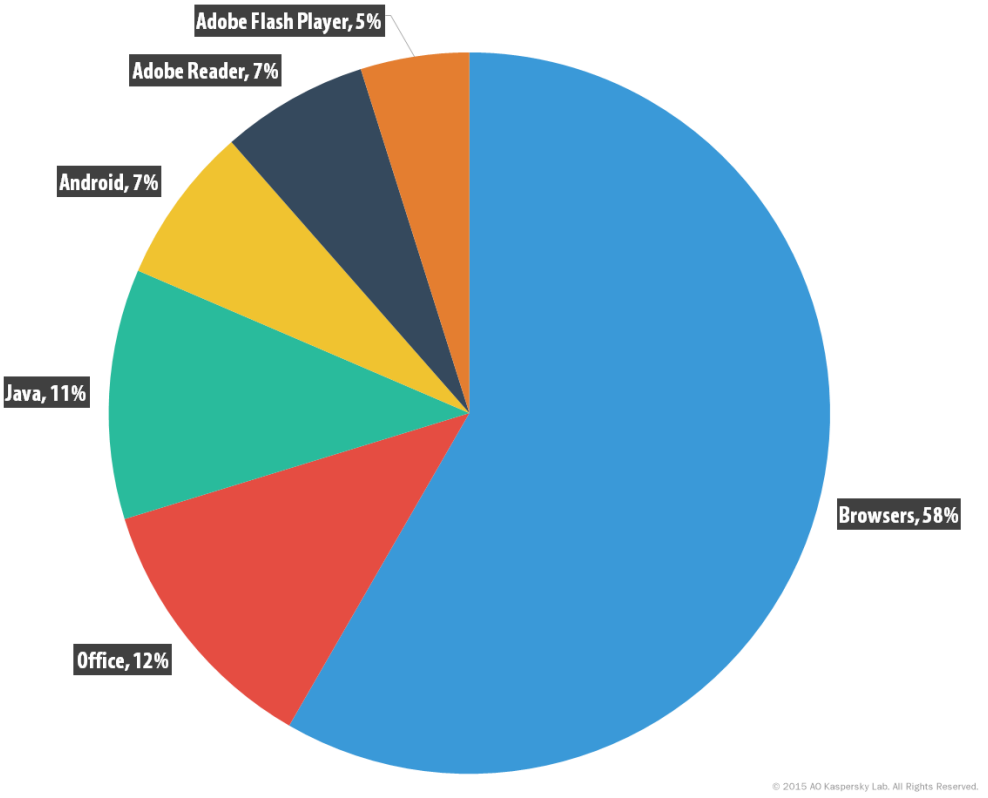
- exploits for vulnerabilities found in office applications are used three times more often than in attacks on home users;
- use of malicious files signed with valid digital certificates;
- use of legitimate programs in attacks, allowing the attackers to go undetected for longer.

We have also observed a rapid growth in the number of corporate user computers attacked by encryptor programs.

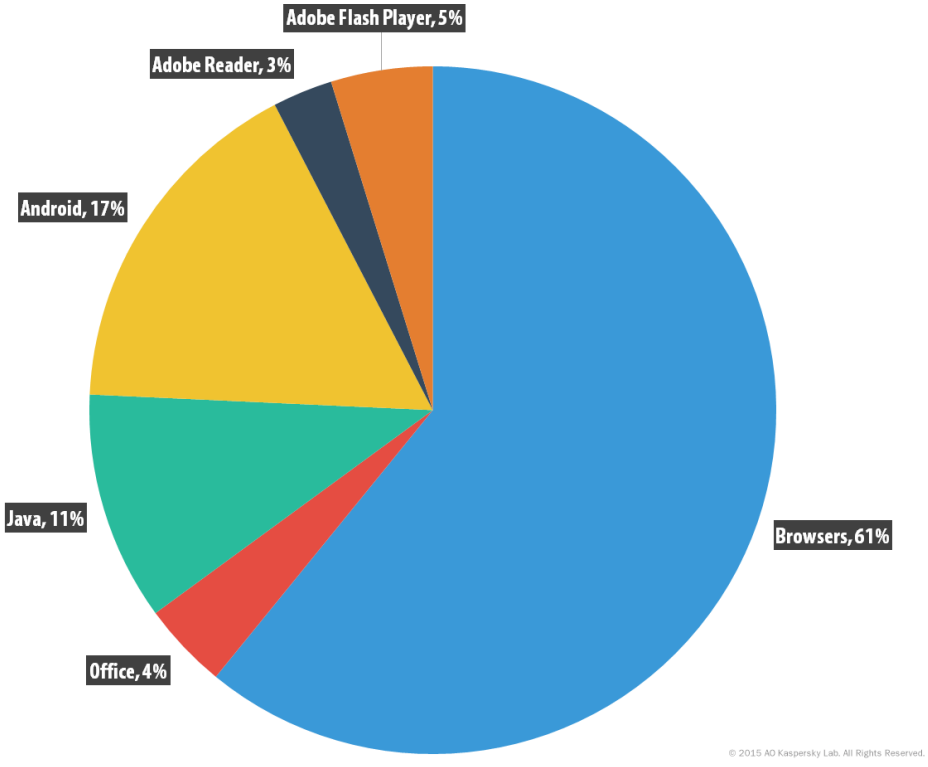
In this particular context, the majority of cases are not APT attacks: "standard" cybercriminals are simply focusing on corporate users, and sometimes on a particular company that is of interest to them.

Use of exploits in attacks on businesses

The ranking of vulnerable applications is compiled based on information about exploits blocked by Kaspersky Lab products and used by cybercriminals, both in web- and email-based attacks, as well as attempts to compromise local applications, including those on mobile devices.



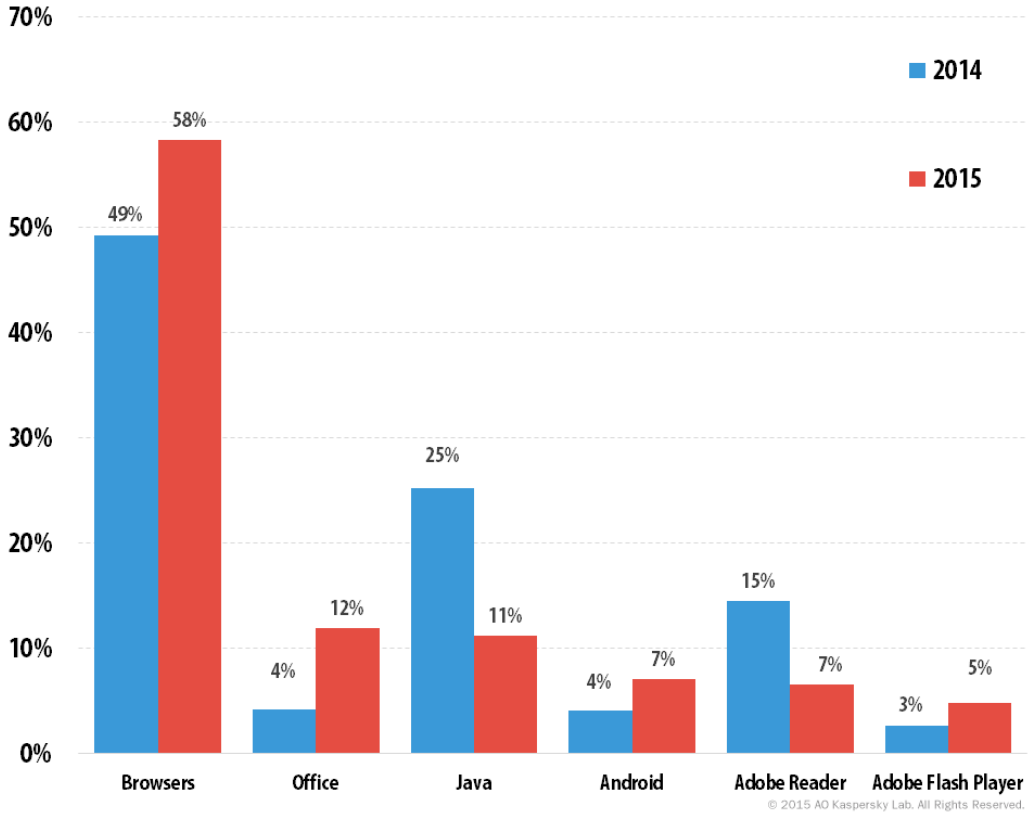
Distribution of exploits used in cybercriminal attacks by type of attacked application (corporate users, 2015)



Distribution of exploits used in cybercriminal attacks by type of attacked application (home users, 2015)

If we compare the use of exploits by cybercriminals to attack home and corporate users, the first obvious difference is that exploits for office software vulnerabilities are used much more often in attacks launched against businesses. They are only used in 4% of attacks on home users, but when it comes to attacks on corporate users, they make up 12% of all exploits detected throughout the year.

Web browsers are the applications targeted most often by exploits in attacks on both home and corporate users. When viewing these statistics, it should be noted that Kaspersky Lab technologies detect exploits at various stages. Detection of landing pages from which exploits are distributed are also counted in the 'Browsers' category. We have observed that most often these are exploits for vulnerabilities in Adobe Flash Player.



Distribution of exploits used in cybercriminal attacks by type of attacked application in 2014 and 2015

The proportions of Java and PDF exploits have declined significantly compared to 2014, by 14 p.p. and 8 p.p., respectively. Java exploits have lost some of their popularity in spite of the fact that several zero-day vulnerabilities that been found during the year. The proportion of attacks launched using vulnerabilities in office software (+8 p.p.), browsers (+9 p.p.), Adobe Flash Player (+9 p.p), and Android software (+3 p.p.) have risen.

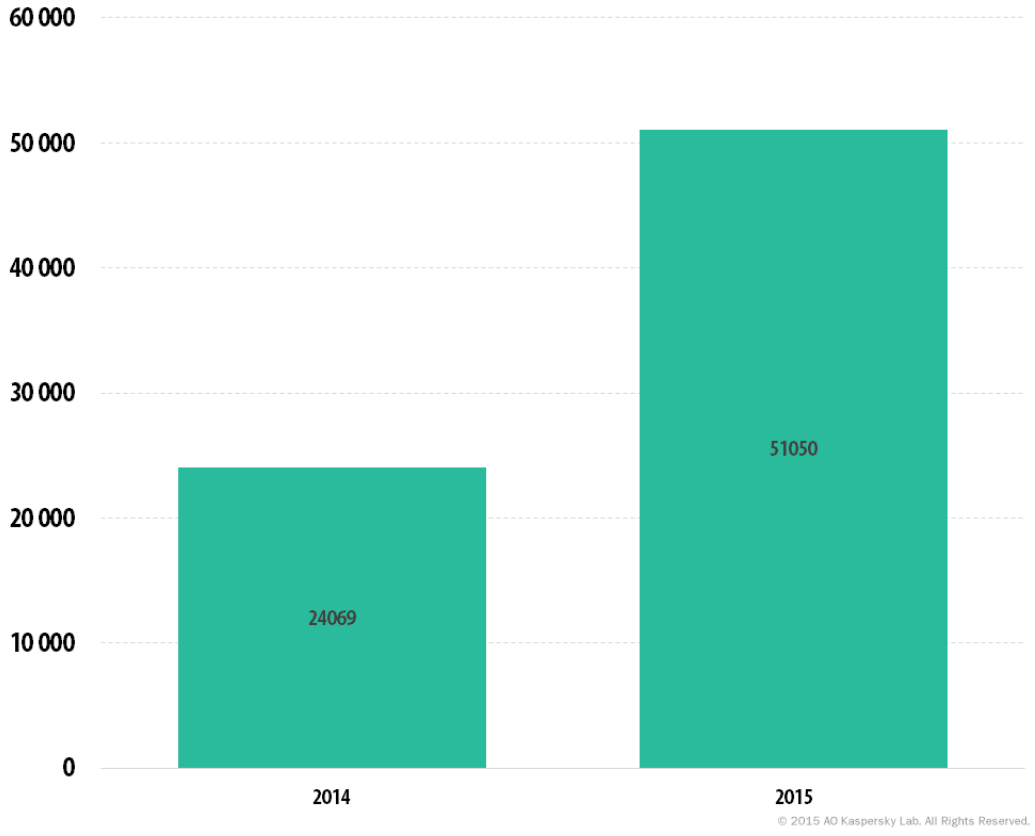
Investigations of security incidents have shown that even in targeted attacks on corporations, cybercriminals often use exploits for known vulnerabilities. This is because corporate environments are slow to install appropriate

security patches. The proportion of exploits that target vulnerabilities in Android applications has risen to 7%, which suggests cybercriminals have a growing interest in corporate data stored on employees' mobile devices.

Ransomware

Encryption Trojans were long considered to be a threat to home users only. Nowadays, however, we see ransomware actors paying more attention to organizations as targets.

In 2015, Kaspersky Lab solutions detected ransomware on more than **50,000 computers** in corporate networks, which is **double the figure for 2014**. It is important to keep in mind that the real number of incidents is several times higher: the statistics reflect only the results of signature-based and heuristic detections, while in most cases Kaspersky Lab products detect encryption Trojans based on behavior recognition models.



The number of unique corporate users attacked by encryption Trojans in 2014 and 2015

There are two reasons for the surge in interest in businesses by ransomware actors. Firstly, they can receive much bigger ransoms from organizations than from individual users. Secondly, there is a better chance the ransom will be paid: some companies simply cannot continue their operations if information has been encrypted and is unavailable on critical computers and/or servers.

One of the most interesting developments of 2015 in this realm has been the emergence of the first Linux encryption malware (Kaspersky Lab products detect it as the verdict 'Trojan-Ransom.Linux.Cryptor'), which targets websites, including online stores. The cybercriminals exploited vulnerabilities in web applications to gain access to websites, and then uploaded a malicious program to the sites that encrypted the server data. In the majority of cases, this brought the site down. The cybercriminals demanded a ransom of one bitcoin to restore the site. Around 2,000 websites are estimated to have been infected. Given the popularity of *nix servers in the business environment, it is reasonable to assume that next year there may be more ransomware attacks against non-Windows platforms.

TOP 10 encryptor Trojan families

	Family	% attacked users*
1	Scatter	21
2	Onion	16
3	Cryakl	15
4	Snocry	11
5	Cryptodef	8
6	Rakhni	7
7	Crypmod	6
8	Shade	5
9	Mor	3
10	Crypren	2

**The proportion of users attacked by malicious programs from this family, as a percentage of all attacked users.*

Virtually all the ransomware families in the Top 10 demand ransoms in bitcoins.

The Scatter family of Trojans occupies first place. They encrypt files on the hard drive and leave encrypted files with the extension .vault. Scatter Trojans are multi-module, multi-purpose script-based malicious programs. This malware family has quickly evolved over a short period, developing new Email-Worm and Trojan-PSW capabilities on top of file encryption.

In second place is the Onion family of encryptors, known for the fact that their C&C servers are located within the Tor network. In third place is the Cryakl family of encryptors, which are written in Delphi and emerged back in April 2014.

In some cases, it may be possible to restore the data encrypted by these ransomware programs, usually when there are mistakes of some kind in their algorithms. However, it is currently impossible to decrypt data that has been encrypted by the latest versions of the malicious programs in the Top 10.

It is important for companies to understand that an infection by malware of this kind can interfere with business operations if critical business data is lost or a critical server operation is blocked due to encryption. Attacks like this can lead to huge losses, comparable to those caused by the Wiper malware attacks that destroyed data in corporate networks.

To address this threat, a number of measures should be taken:

- deploy protection against exploits;
- ensure behavioral detection methods are enabled in your security product (in Kaspersky Lab products, this is done in the System Watcher component);
- configure a data backup procedure.

ATTACKS ON POS TERMINALS

The security of point-of-sale (PoS) terminals has turned into another pressing issue for businesses, especially those involved in trading activities. Any computer with a special card reader device connected to it and the right software installed can be used as a PoS terminal. Cybercriminals hunt for these computers and infect them with malicious programs that allow them to steal the details of bank cards used to pay at the terminals.

Kaspersky Lab's security products have blocked over 11,500 such attacks across the world. To date, there are 10 malware families in our collection that are designed to steal data from PoS terminals. Seven of these emerged this year. Despite the small number of attacks that are attempted, this risk should not be underestimated, because just one successful attack could compromise the details of tens of thousands of credit cards. Such a large number of potential victims is possible because business owners and system administrators do not see PoS terminals as devices that require protection. As a result, an infected terminal could go unnoticed for a long time, during which the malicious program sends the details of all the credit cards passing through the terminal to cybercriminals.

This problem is especially relevant in those countries where cards with EMV chips are not used. The adoption of EMV chip cards should make it far more difficult to obtain the data required to clone banking cards, although the adoption process could take a long time. In the meantime, there are some minimum measures that should be taken to protect PoS devices. Fortunately, for these devices it is fairly easy to configure the 'default deny' security policy, which blocks unknown programs from launching by default.

We expect that in the future cybercriminals will start targeting mobile PoS devices running under Android.

CONCLUSION

The data collected from Kaspersky Lab products shows that the tools used to attack businesses differ from those used against home users. In attacks on corporate users, exploits for office application vulnerabilities are used much more often, malicious files are often signed with valid digital certificates, and cybercriminals try to use legitimate software for their purposes, so they can go unnoticed for longer. We have also observed strong growth in the numbers of corporate user computers targeted by ransomware. This also applies to incidents not classified as APT attacks, where cybercriminals merely focus on corporate users, and sometimes on employees of specific companies.

The fact that cybercriminal groups use APT methods and programs to attack businesses takes them to a different level and makes them much more dangerous. Cybercriminals have begun to use these methods primarily to steal large sums of money from banks. They can use the same methods to steal a company's money from bank accounts by gaining access to its corporate network.

Cybercriminals rely on exploiting known vulnerabilities to conduct their attacks – this is due to the fact that many organizations are slow to implement software updates on their corporate computers. In addition, cybercriminals make use of signed malicious files and legitimate tools to create channels for extracting information: these tools include popular remote administration software, SSH clients, password restoration software, etc.

More and more frequently, corporate servers are being targeted by cybercriminals. Besides stealing data, there have been cases when the attacked servers were used to launch DDoS attacks, or the data on the servers was encrypted for ransom. Recent developments have shown that this is true for both Windows and Linux servers.

Many of the organizations that suffered attacks have received ransom demands asking for payments in return for halting an ongoing DDoS attack, unblocking encrypted data, or for not disclosing stolen information. When an organization faces such demands, the first thing they should do is contact law enforcement agencies and computer security specialists. Even if a ransom is paid, the cybercriminals may still not fulfil their promise, as was the case with the ProtonMail DDoS attack that continued after a ransom was paid.

PREDICTIONS

Growing numbers of attacks against financial organizations, financial fraud on exchange markets

In the coming year, we expect to see growing numbers of attacks launched against financial organizations, as well as a difference in the quality of these attacks. Besides transferring money to their own accounts and converting it to cash, we may also see cybercriminals employing some new techniques. These could include data manipulation on trading platforms where both traditional and new financial instruments, such as cryptocurrencies, are traded.

Attacks on infrastructure

Even if an organization is difficult to penetrate, it is now typical for organizations to store their valuable data on servers located in data centers rather than on the infrastructure located on their own premises. Attempts to gain unauthorized access to these outsourced components of a company's infrastructure will become an important attack vector in 2016.

Exploiting IoT vulnerabilities to penetrate corporate networks

IoT (Internet of Things) devices can be found in almost every corporate network. Research conducted in 2015 has shown that there are a number of security problems with these devices and cybercriminals are likely to exploit them because they offer a convenient foothold at the initial stage of penetrating a corporate network.

More rigid security standards, cooperation with law enforcement agencies

In response to the growing number of computer incidents in business environments and the changes to the overall cyber-threat landscape, regulatory authorities will develop new security standards and update those already in effect. Organizations that are interested in the integrity and security of their digital values will cooperate more actively with law enforcement agencies, or find themselves obliged to do so by the standards mentioned above. This may lead to more concerted efforts to catch cybercriminals, so expect to hear about new arrests in 2016.

WHAT TO DO?

In 2015, we have seen cybercriminals begin to actively use APT attack methods to penetrate company networks. We are talking here about reconnaissance that aims to identify weak spots in a corporate infrastructure and gathering information about employees. There is also the use of spear phishing and waterhole attacks, the active use of exploits to execute code and gain administrator rights, the use of legitimate software along with Trojans for remote administration, research of the targeted network and abuse of password restoration software. All this requires the development of methods and techniques to protect corporate networks.

As for specific recommendations, the TOP 35 cyber-intrusion mitigation strategies developed by the Australian Signals Directorate (ASD) should be consulted first of all. Through comprehensive, detailed analysis of local attacks and threats, ASD has found that at least 85% of targeted cyber intrusions could be mitigated by four basic strategies. Three of them are related to specialized security solutions. Kaspersky Lab products include technological solutions to cover the first three major strategies.

Below is a list of the four basic strategies that reduce the possibility of a successful targeted attack:

- Use application whitelisting to help prevent malicious software and unapproved programs from running
- Patch applications such as Java, PDF viewers, Flash, web browsers and Microsoft Office
- Patch operating system vulnerabilities
- Restrict administrative privileges to operating systems and applications, based on user duties.

For detailed information about the ASD mitigation strategies, consult the threat mitigation article in the Securelist encyclopedia.

Another important factor is the use of the latest threat data, i.e. threat intelligence services (Kaspersky Lab, for example, provides its own Kaspersky Intelligence Service). A timely configuration and checkup of the corporate network using this data will help protect against attacks or detect an attack at an early stage.

The basic principles of ensuring security in corporate networks remain unchanged:

- Train staff. Maintaining information security is not only the job of the corporate security service but also the responsibility of every employee.
- Organize security procedures. The corporate security system must provide an adequate response to evolving threats.
- Use new technologies and methods. Each added layer of protection helps reduce the risk of intrusion.

OVERALL STATISTICS FOR 2015

THE YEAR IN FIGURES

- In 2015, there were **1,966,324** registered notifications about attempted malware infections that aimed to steal money via online access to bank accounts.
- Ransomware programs were detected on **753,684** computers of unique users; **179,209** computers were targeted by encryption ransomware.
- Kaspersky Lab's web antivirus detected **121,262,075** unique malicious objects: scripts, exploits, executable files, etc.
- Kaspersky Lab solutions repelled **798,113,087** attacks launched from online resources located all over the world.
- **34.2%** of user computers were subjected to at least one web attack over the year.
- To carry out their attacks, cybercriminals used **6,563,145** unique hosts.
- **24%** of web attacks neutralized by Kaspersky Lab products were carried out using malicious web resources located in the US.
- Kaspersky Lab's antivirus solutions detected a total of **4,000,000** unique malicious and potentially unwanted objects.

VULNERABLE APPLICATIONS USED IN CYBERATTACKS

In 2015, we saw the use of new techniques for masking exploits, shellcodes and payloads to make detecting infections and analyzing malicious code more difficult. Specifically, cybercriminals:

- Used the Diffie-Hellman encryption protocol
- Concealed exploit packs in Flash objects

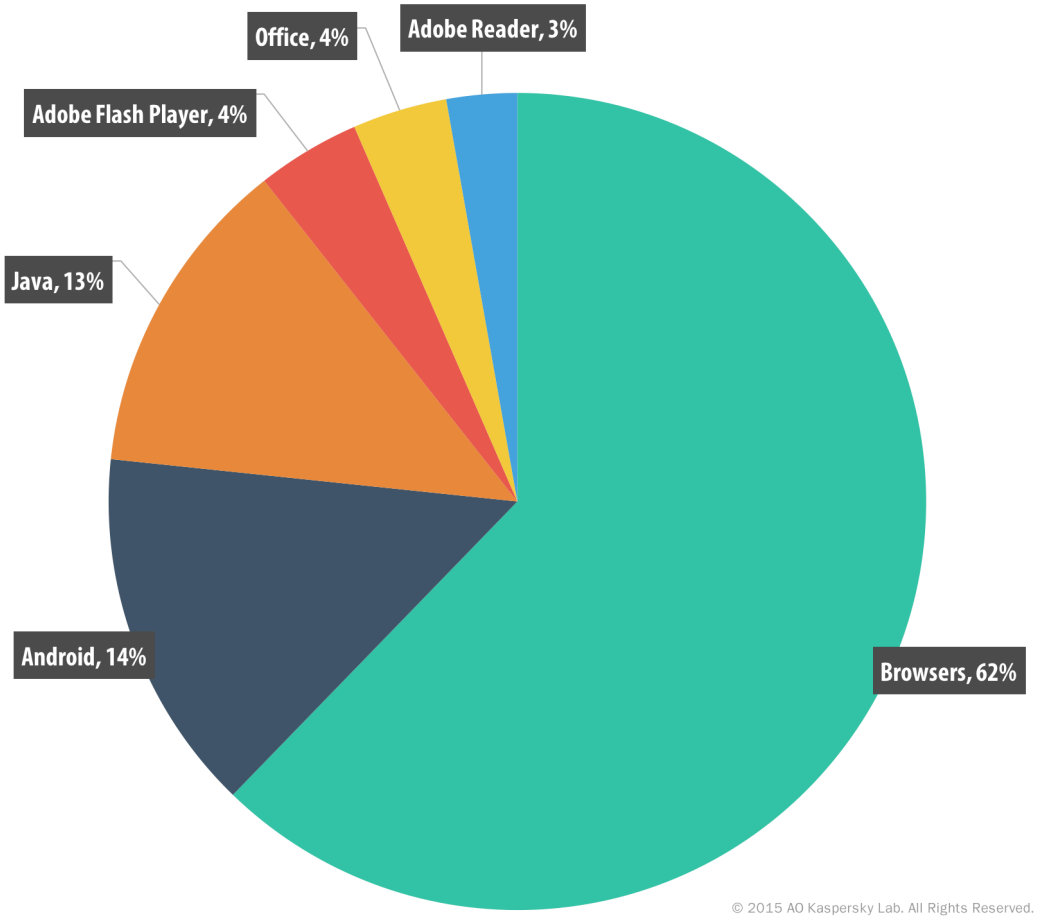
The detection of two families of critical vulnerabilities for Android was one of the more remarkable events of the year. Exploiting Stagefright vulnerabilities enabled an attacker to remotely execute arbitrary code on a device by sending a specially crafted MMS to the victim's number. Exploiting Stagefright 2 pursued the same purpose, but this time using a specially crafted media file.

Exploits for Adobe Flash Player were popular among malware writers in 2015. This can be explained by the fact that a large number of vulnerabilities were identified in the product throughout the year. In addition, cybercriminals used the information about unknown Flash Player vulnerabilities that became public as a result of the Hacking Team data breach.

When new Adobe Flash Player vulnerabilities were discovered, developers of various exploit packs were quick to respond by adding new exploits to their products. Here is the 'devil's dozen' of Adobe Flash Player vulnerabilities that gained popularity among cybercriminals and were added to common exploit packs:

1. CVE-2015-0310
2. CVE-2015-0311
3. CVE-2015-0313
4. CVE-2015-0336
5. CVE-2015-0359
6. CVE-2015-3090
7. CVE-2015-3104
8. CVE-2015-3105
9. CVE-2015-3113
10. CVE-2015-5119
11. CVE-2015-5122
12. CVE-2015-5560
13. CVE-2015-7645

Some well-known exploit packs have traditionally included an exploit for an Internet Explorer vulnerability (CVE-2015-2419). We also saw a Microsoft Silverlight vulnerability (CVE-2015-1671) used in 2015 to infect users. It is worth noting, however, that this exploit is not popular with the main 'players' in the exploit market.



Distribution of exploits used in cyberattacks, by type of application attacked, 2015

Vulnerable applications were ranked based on data on exploits blocked by Kaspersky Lab products, used both for online attacks and to compromise local applications, including those on mobile devices.

Although the share of exploits for Adobe Flash Player in our ranking was only 4%, they are quite common in the wild. When looking at these statistics, it should be kept in mind that Kaspersky Lab technologies detect exploits at different stages. As a result, the Browsers category (62%) also includes the detection of landing pages that serve exploits. According to our observations, exploits for Adobe Flash Player are most commonly served by such pages.

We saw the number of cases which involved the use of Java exploits decrease over the year. In late 2014 their proportion of all the exploits blocked was 45%, but this proportion gradually diminished by 32 p.p. during the year, falling to 13%. Moreover, Java exploits have now been removed from all known exploit packs.

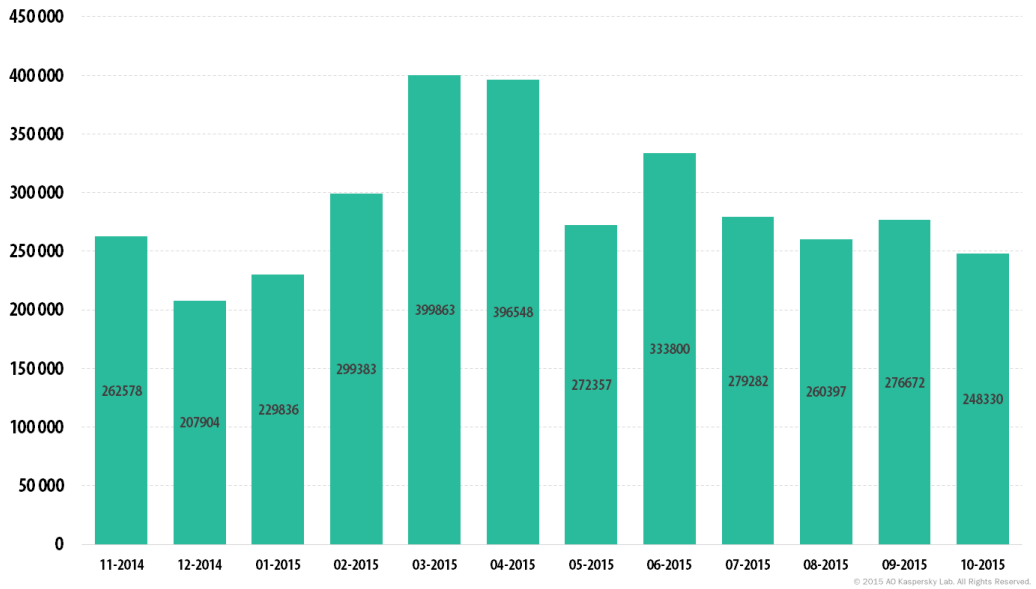
At the same time, the use of Microsoft Office exploits increased from 1% to 4%. Based on our observations, in 2015 these exploits were distributed via mass emailing.

ONLINE THREATS IN THE BANKING SECTOR

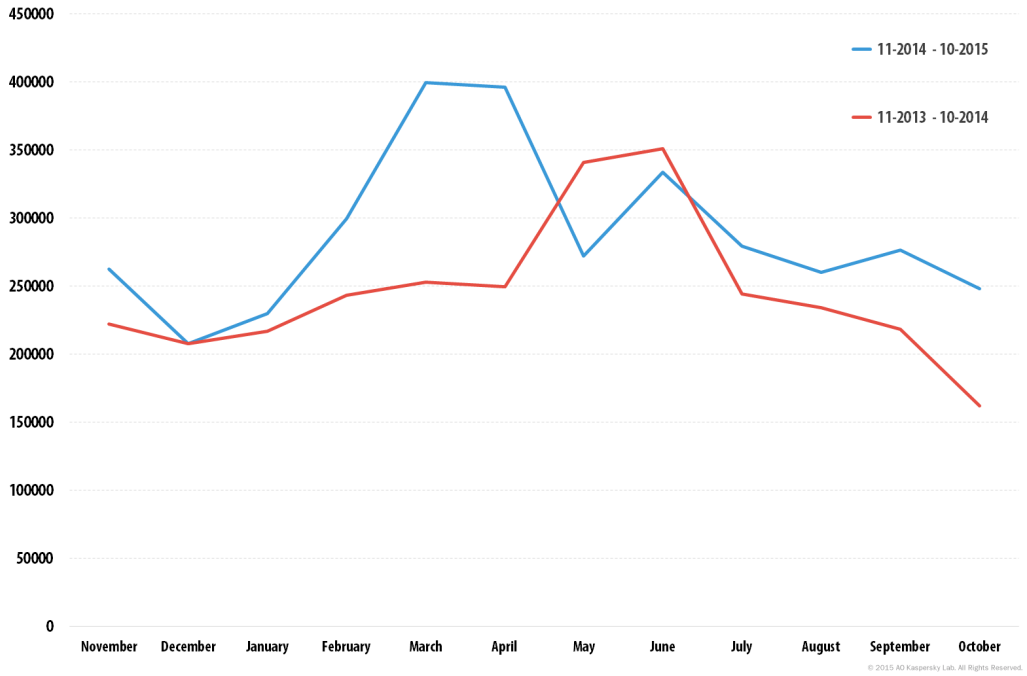
These statistics are based on the detection verdicts returned by the antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

The annual statistics for 2015 are based on data received between November 2014 and October 2015.

In 2015, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **1,966,324** computers. This number is 2.8% higher than in 2014 (1,910,520).



The number of users attacked by financial malware, November 2014-October 2015

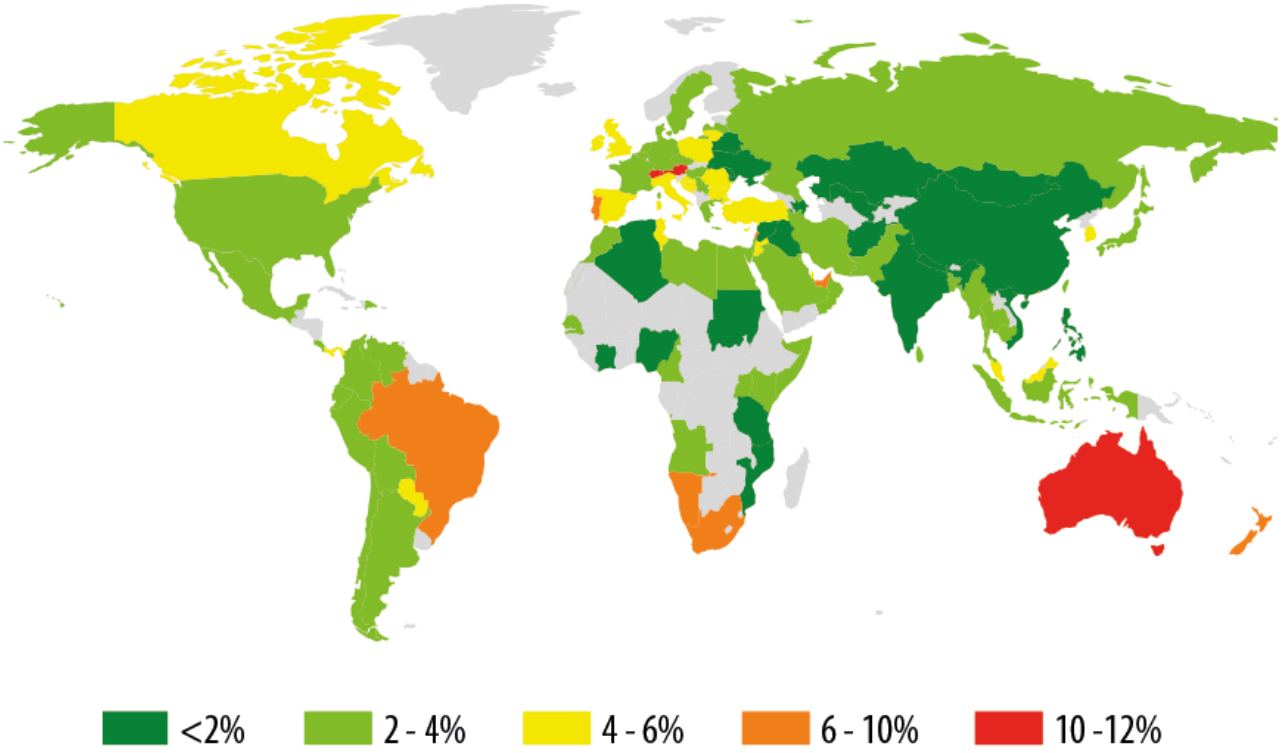


Number of users attacked by financial malware in 2014 and 2015

In 2015, the number of attacks grew steadily from February till April, with the peak in March-April. Another burst was recorded in June. In 2014, most users were targeted by financial malware in May and June. During the period between June and October in both 2014 and 2015 the number of users attacked fell gradually.

Geography of attacks

In order to evaluate the popularity of financial malware among cybercriminals and the risk of user computers around the world being infected by banking Trojans, we calculate the percentage of Kaspersky Lab users who encountered this type of threat during the reporting period in the country, relative to all users of our products in the county.



Geography of banking malware attacks in 2015 (users attacked by banking Trojans as a percentage of all users attacked by all types of malware)

TOP 10 countries by percentage of attacked users

	Country*	% attacked users**
1	Singapore	11.6
2	Austria	10.6
3	Switzerland	10.6
4	Australia	10.1
5	New Zealand	10.0
6	Brazil	9.8
7	Namibia	9.3
8	Hong Kong	9.0
9	Republic of South Africa	8.2
10	Lebanon	6.6

** 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.*

Singapore leads this rating. Of all the Kaspersky Lab users attacked by malware in the country, 11.6% were targeted at least once by banking Trojans throughout the year. This reflects the popularity of financial threats in relation to all threats in the country.

5.4% of users attacked in Spain encountered a banking Trojan at least once in 2015. The figure for Italy was 5%; 5.1% in Britain; 3.8% in Germany; 2.9% in France; 3.2% in the US; and 2.5% in Japan.

2% of users attacked in Russia were targeted by banking Trojans.

The TOP 10 banking malware families

The table below shows the Top 10 malware families most commonly used in 2015 to attack online banking users (as a percentage of users attacked):

	Name*	% users attacked**
1	Trojan-Downloader.Win32.Upatre	42.36
2	Trojan-Spy.Win32.Zbot	26.38
3	Trojan-Banker.Win32.ChePro	9.22
4	Trojan-Banker.Win32.Shiotob	5.10
5	Trojan-Banker.Win32.Banbra	3.51
6	Trojan-Banker.Win32.Caphaw	3,14
7	Trojan-Banker.AndroidOS.Faketoken	2.76
8	Trojan-Banker.AndroidOS.Marcher	2.41
9	Trojan-Banker.Win32.Tinba	2.05
10	Trojan-Banker.JS.Agent	1.88

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

*** Unique users whose computers have been targeted by the malicious program, as a percentage of all unique users targeted by financial malware attacks.*

The majority of the Top 10 malicious programs work by injecting random HTML code in the web page displayed by the browser and intercepting any payment data entered by the user in the original or inserted web forms.

The Trojan-Downloader.Win32.Upatre family of malicious programs remained at the top of the ranking throughout the year. The malware is no larger than 3.5 KB in size, and is limited to downloading the payload to the victim computer, most typically a banker Trojan from the Dyre/Dyzap/Dyreza family whose main aim is to steal the user's payment details. Dyre does this by intercepting the data from a banking session between the victim's browser and the online banking web app, in other words, by using a Man-in-the-Browser (MITB) technique. This malicious program is spread via specially created emails with an attachment containing a document with the downloader. In the summer of 2015, however, Trojan-Downloader.Win32.Upatre was spotted on compromised home routers, which is a testimony to how cybercriminals make use of this multi-purpose malware.

Yet another permanent resident of this ranking is Trojan-Spy.Win32.Zbot (in second place) which consistently occupies one of the leading positions. The Trojans of the Zbot family were among the first to use web injections to compromise the payment details of online banking users and to modify the contents of banking web pages. They encrypt their configuration files at several levels; the decrypted configuration file is never stored in the memory in its entirety, but is instead loaded in parts.

Representatives of the Trojan-Banker.Win32.ChePro family were first detected in October 2012. At that time, these banking Trojans were mostly aimed at users in Brazil, Portugal and Russia. Now they are being used to attack the users worldwide. Most programs of this type are downloaders which need other files to successfully infect the system. Generally, they are malicious banking programs, allowing the fraudsters to take screenshots, to intercept keystrokes, and to read the content of the copy buffer, i.e. they possess functionality that allows a malicious program to be used for attacks on almost any online banking system.

Of particular interest is the fact that two families of mobile banking Trojans are present in this ranking: Faketoken and Marcher. The malicious programs belonging to the latter family steal payment details from Android devices.

The representatives of the Trojan-Banker.AndroidOS.Faketoken family work in partnership with computer Trojans. To distribute this malware, cybercriminals use social engineering techniques. When a user visits his online banking account, the Trojan modifies the page, asking him to download an Android application which is allegedly required to securely confirm the transaction. In fact the link leads to the Faketoken application. Once Faketoken is on the user's smartphone, the cybercriminals gain access to the user's banking account via the computer infected with the banking Trojan and the compromised mobile device allows them to intercept the one-time confirmation code (mTAN).

The second family of mobile banking Trojans is Trojan-Banker.AndroidOS.Marcher. After infecting a device, the malware tracks the launch of just two apps – the mobile banking customer of a European bank and Google Play. If the user starts Google Play, Marcher displays a false window requesting credit card details which then go to the fraudsters. The same method is used by the Trojan if the user starts the banking application.

Tenth place in the 2015 ranking was occupied by the Trojan-Banker.JS.Agent family. This is the malicious JavaScript code that results from an injection into an online banking page. The aim of this code is to intercept payment details that the user enters into online banking forms.

2015 – AN INTERESTING YEAR FOR RANSOMWARE

The Trojan-Ransom class represents malware intended for the unauthorized modification of user data that renders a computer inoperable (for example, encryptors), or for blocking the normal operation of a computer. In order to decrypt files and unblock a computer the malware owners usually demand a ransom from the victims.

Since its emergence with CryptoLocker in 2013, ransomware has come a long way. For example, in 2014 we spotted the first version of ransomware for Android. Just a year later, 17% of the infections we saw were on Android devices.

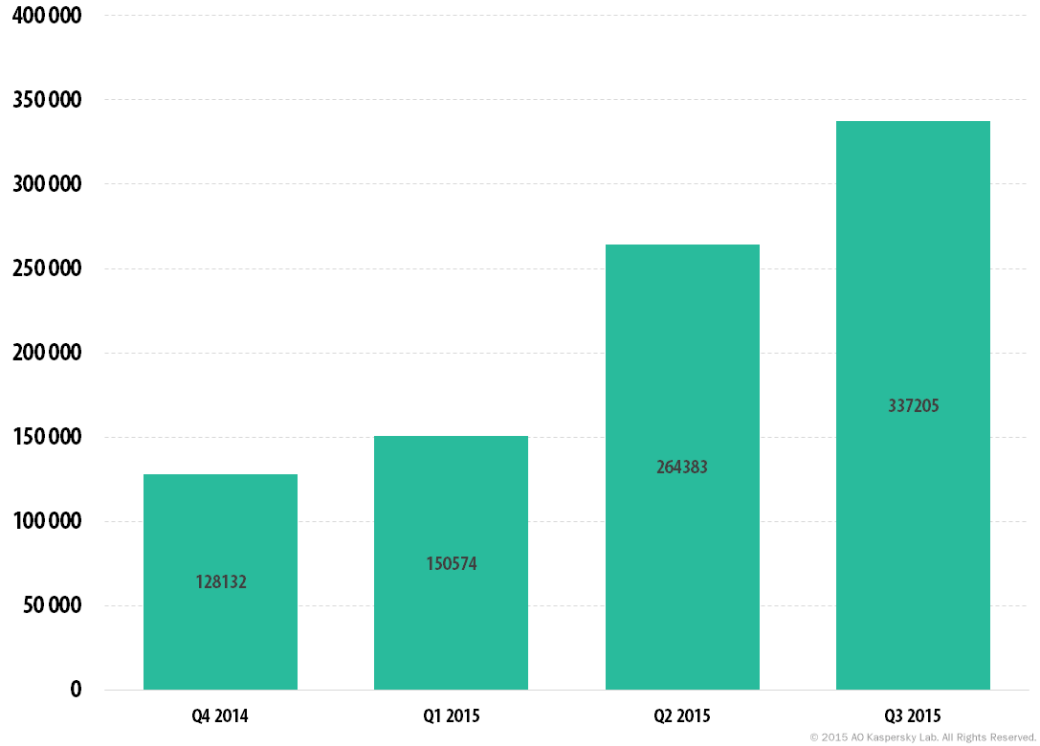
2015 also saw the first ransomware for Linux, which can be found in the Trojan-Ransom.Linux class. On the positive side, the malware authors made a small implementation error, which makes it possible to decrypt the files without paying a ransom.

Unfortunately, these implementation errors are occurring less and less. This prompted the FBI to state: "The ransomware is that good... To be honest, we often advise people just to pay the ransom". That this is not always a good idea was also shown this year, when the Dutch police were able to apprehend two suspects behind the CoinVault malware. A little later we received all 14,000 encryption keys, which we added to a new decryption tool. All the CoinVault victims were then able to decrypt their files for free.

2015 was also the year that marked the birth of TeslaCrypt. TeslaCrypt has a history of using graphical interfaces from other ransomware families. Initially it was CryptoLocker, but this later changed to CryptoWall. This time they copied the HTML page in full from CryptoWall 3.0, only changing the URLs.

Number of users attacked

The following graph shows the rise in users with detected Trojan-Ransom within the last year:



Number of users attacked by Trojan-Ransom malware (Q4 2014 – Q3 2015)

Overall in 2015, Trojan-Ransom was detected on **753,684** computers. Ransomware is thus becoming more and more of a problem.

TOP 10 Trojan-Ransom families

The Top 10 most prevalent ransomware families are represented here. The list consists of browser-based extortion or blocker families and some notorious encryptors. So-called Windows blockers that restrict access to a system (for example, the Trojan-Ransom.Win32.Blocker family) and demand a ransom were very popular a few years ago – starting off in Russia then moving west – but are not as widespread anymore and are not represented in the Top 10.

	Name*	Users percentage**
1	Trojan-Ransom.HTML.Agent	38.0
2	Trojan-Ransom.JS.Blocker	20.7
3	Trojan-Ransom.JS.InstallExtension	8.0
4	Trojan-Ransom.NSIS.Onion	5.8
5	Trojan-Ransom.Win32.Cryakl	4.3
6	Trojan-Ransom.Win32.Cryptodef	3.1
7	Trojan-Ransom.Win32.Snocry	3.0

	Name*	Users percentage**
8	Trojan-Ransom.BAT.Scatter	3.0
9	Trojan-Ransom.Win32.Crypmod	1.8
10	Trojan-Ransom.Win32.Shade	1.8

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

*** Percentage of users attacked by a Trojan-Ransom family relative to all users attacked with Trojan-Ransom malware.*

First place is occupied by Trojan-Ransom.HTML.Agent (38%) with the Trojan-Ransom.JS.Blocker family (20.7%) in second. They represent browser-blocking web pages with various unwanted content usually containing the extortion message (for example, a "warning" from a law enforcement agency) or containing JavaScript code that blocks the browser along with a message.

In third place is Trojan-Ransom.JS.InstallExtension (8%), a browser-blocking web page that imposes a Chrome extension installation on the user. When attempting to close the page a voice mp3 file is often played: "In order to close the page, press the 'Add' button". The extensions involved are not harmful, but the offer is very obtrusive and difficult for the user to reject. This kind of extension propagation is used by a partnership program. These three families are particularly prevalent in Russia and almost as prevalent in some post-Soviet countries.

When we look at where ransomware is most prevalent (not just the three families mentioned above), we see that the top three consists of Kazakhstan, Russia and Ukraine.

Cryakl became relatively active in Q3 2015, when we saw peaks of up to 2300 attempted infections a day. An interesting aspect of Cryakl is its encryption scheme. Rather than encrypting the whole file, Cryakl encrypts the first 29 bytes plus three other blocks located randomly in the file. This is done to evade behavioral detection, while encrypting the first 29 bytes destroys the header.

Cryptodef is the infamous Cryptowall ransomware. Cryptowall is found most often, in contrast to the other families discussed here, in the US. In fact, there are three times as many infections in the US than there are in Russia. Cryptowall is spread through spam emails, where the user receives a zipped JavaScript. Once executed, the JavaScript downloads Cryptowall and it starts encrypting files. A change in the ransom message is also observed: victims are now congratulated by the malware authors on "becoming part of the large Cryptowall community".

Encryptors can be implemented not only as executables but also using simple scripting languages, as in the case of the Trojan-Ransom.BAT.Scatter family. The Scatter family appeared in 2014 and quickly evolved, providing itself with the functionality of Email-Worm and Trojan-PSW. Encryption makes use of two pairs of assymetric keys, making it possible to encrypt the user's files without revealing their private key. It employs renamed legitimate utilities to encrypt files.

The Trojan-Ransom.Win32.Shade encryptor, which is also very prevalent in Russia, is able to request a list from the C&C server containing the URLs of additional malware. It then downloads that malware and installs it in the system. All its C&C servers are located in the Tor network. Shade is also suspected of propagating via a partnership program.

TOP 10 countries attacked by Trojan-Ransom malware

	Country*	% of users attacked by Trojan-Ransom**
1	Kazakhstan	5,47
2	Ukraine	3,75
3	Russian Federation	3,72
4	Netherlands	1,26
5	Belgium	1,08
6	Belarus	0,94
7	Kyrgyzstan	0,76
8	Uzbekistan	0,69
9	Tajikistan	0,69
10	Italy	0,57

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

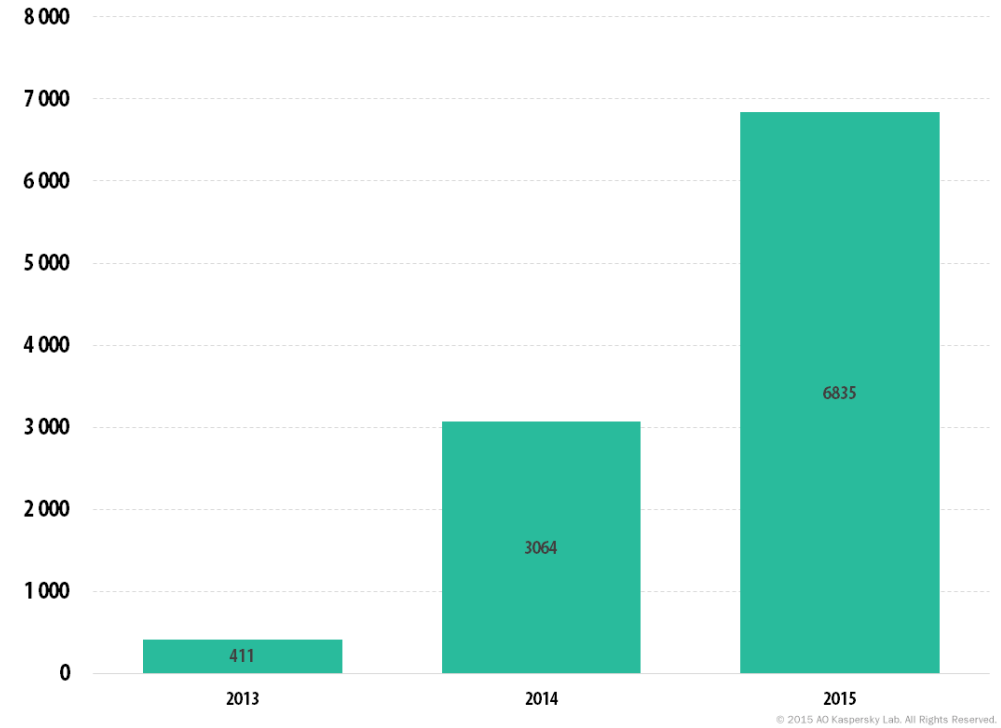
***Unique users whose computers have been targeted by Trojan-Ransom as a percentage of all unique users of Kaspersky Lab products in the country.*

Encryptors

Even if today's encryptors are not as popular among cybercriminals as blockers were, they inflict more damage on users. So it's worth investigating them separately.

The number of new Trojan-Ransom encryptors

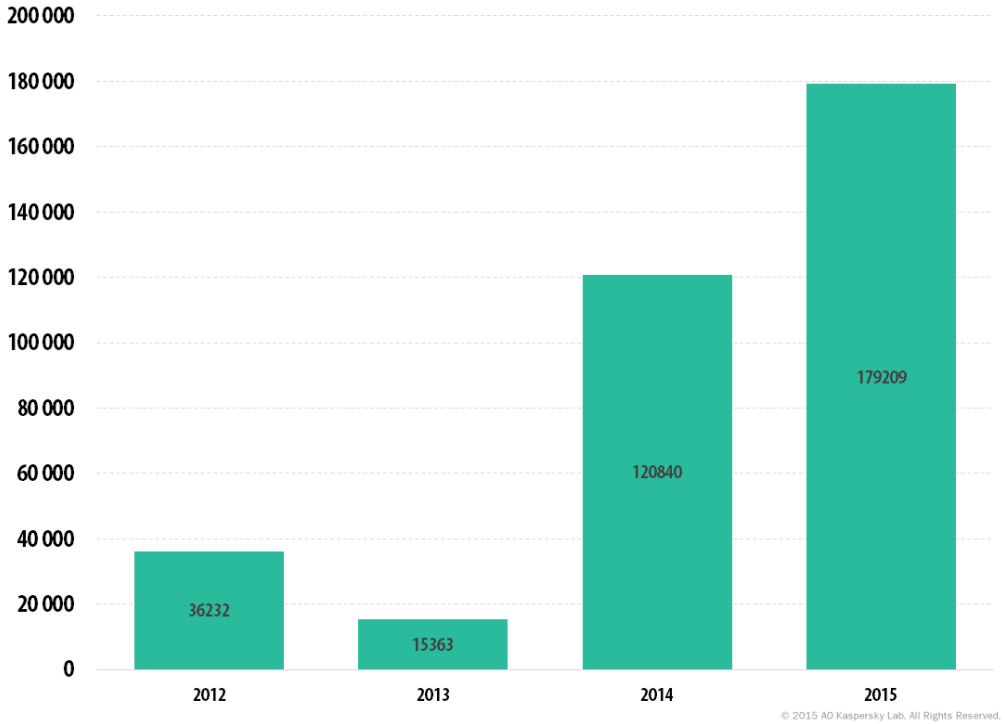
The following graph represents the rise of newly created encryptor modifications per year.



Number of Trojan-Ransom encryptor modifications in Kaspersky Lab's Virus Collection (2013 – 2015)

The overall number of encryptor modifications in our Virus Collection to date is at least **11,000**. Ten new encryptor families were created in 2015.

The number of users attacked by encryptors



Number of users attacked by Trojan-Ransom encryptor malware (2012 – 2015)

In 2015, **179,209** unique users were attacked by encryptors. About 20% of those attacked were in the corporate sector.

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

Top 10 countries attacked by encryptors

	Country*	% of users attacked by encryptors
1	Netherlands	1.06
2	Belgium	1.00
3	Russian Federation	0.65
4	Brazil	0.44
5	Kazakhstan	0.42
6	Italy	0.36
7	Latvia	0.34
8	Turkey	0.31
9	Ukraine	0.31
10	Austria	0.30

** 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 Trojan-Ransom encryptor malware as a percentage of all unique users of Kaspersky Lab products in the country.*

First place is occupied by the Netherlands. The most widespread encryptor family is CTB-Locker (Trojan-Ransom.Win32/NSIS.Onion). In 2015 an affiliate program utilizing CTB-Locker was launched and new languages were added including Dutch. Users are mainly infected by emails with malicious attachments. It appears there may be a native Dutch speaker involved in the infection campaign, as the emails are written in relatively good Dutch.

A similar situation exists in Belgium: CTB-Locker is the most widespread encryptor there, too.

In Russia, Trojan-Ransom.Win32.Cryakl tops the list of encryptors targeting users.

ONLINE THREATS (WEB-BASED ATTACKS)

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

The TOP 20 malicious objects detected online

Throughout 2015, Kaspersky Lab's web antivirus detected **121,262,075** unique malicious objects: scripts, exploits, executable files, etc.

We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2015. As in the previous year, advertising programs and their components occupy 12 positions in that Top 20. During the year, advertising programs and their components were registered on 26.1% of all user computers where our web antivirus is installed. The increase in the number of advertising programs, their aggressive distribution methods and their efforts to counteract anti-virus detection, continue the trend of 2014.

Although aggressive advertising does annoy users, it does not harm computers. That is why we have compiled another rating of exclusively malicious objects detected online that does not include the Adware or Riskware classes of program. These 20 programs accounted for 96.6% of all online attacks.

	Name*	% of all attacks**
1	Malicious URL	75.76
2	Trojan.Script.Generic	8.19
3	Trojan.Script.Iframer	8.08
4	Trojan.Win32.Generic	1.01
5	Expoit.Script.Blocker	0.79
6	Trojan-Downloader.Win32.Generic	0.69
7	Trojan-Downloader.Script.Generic	0.36
8	Trojan.JS.Redirector.ads	0.31
9	Trojan-Ransom.JS.Blocker.a	0.19
10	Trojan-Clicker.JS.Agent.pq	0.14
11	Trojan-Downloader.JS.Iframe.diq	0..13
12	Trojan.JS.Iframe.ajh	0.12
13	Exploit.Script.Generic	0.10
14	Packed.Multi.MultiPacked.gen	0.09

	Name*	% of all attacks**
15	Exploit.Script.Blocker.u	0.09
16	Trojan.Script.Iframer.a	0.09
17	Trojan-Clicker.HTML.Iframe.ev	0.09
18	Hoax.HTML.ExtInstall.a	0.06
19	Trojan-Downloader.JS.Agent.hbs	0.06
20	Trojan-Downloader.Win32.Genome.qhcr	0.05

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

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

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

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

The Trojan.JS.Redirector.ads verdict (8th place) is assigned to script that cybercriminals place on infected web resources. It redirects users to other websites, such as those of online casinos. The fact that this verdict is included in the rating should serve as a reminder to web administrators of how easily their sites can be automatically infected by programs – even those that are not very complex.

The Trojan-Ransom.JS.Blocker.a verdict (9th place) is a script that tries to block the browser by means of a cyclic update of the page, and displays a message stating that a "fine" needs to be paid for viewing inappropriate materials. The user is told to transfer the money to a specified digital wallet. This script is mostly found on pornographic sites and is detected in Russia and CIS countries.

The script with the Trojan-Downloader.JS.Iframe.djq verdict (11th place) is found on infected sites running under WordPress, Joomla and Drupal. The campaign launched to infect sites with this script began on a massive scale in August 2015. First, it sends information about the header of the infected page, the current domain, and the address from which the user landed on the page with the script to the fraudsters' server. Then, by using iframe, another script is downloaded in the user's browser. It collects information about the system on the user's computer, the time zone and the availability of Adobe Flash Player. After this and a series of redirects, the user ends up on sites that prompt him to install an update for Adobe Flash Player that is actually adware, or to install browser plugins.

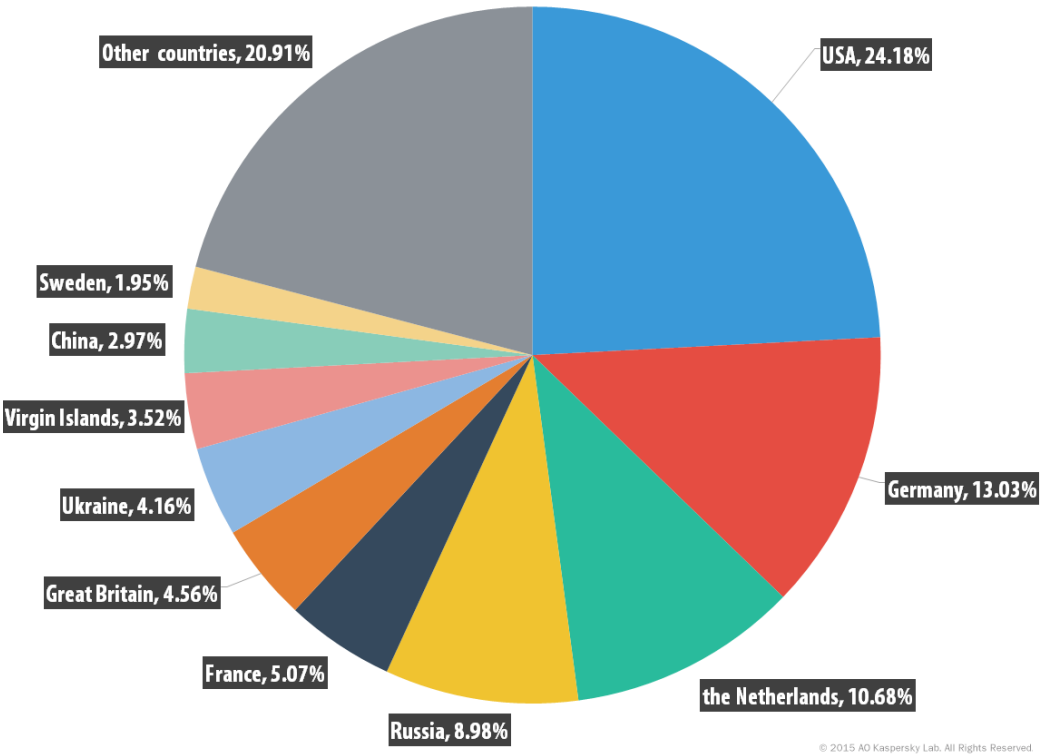
The TOP 10 countries where online resources are seeded with malware

The following statistics are based on the physical location of the online resources that were used in attacks and blocked by our antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host could be the source of one or more web attacks. The statistics do not include sources used for distributing advertising programs or hosts linked to advertising program activity.

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

In 2015, Kaspersky Lab solutions blocked **798,113,087** attacks launched from web resources located in various countries around the world. To carry out their attacks, the fraudsters used **6,563,145** unique hosts.

80% of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries.



The distribution of online resources seeded with malicious programs in 2015

The top four countries where online resources are seeded with malware remained unchanged from the previous year. France moved up from 7th to 5th place (5.07%) while Ukraine dropped from 5th to 7th position (4.16%). Canada and Vietnam left the Top 20. This year's newcomers, China and Sweden, were in 9th and 10th places respectively.

This rating demonstrates that cybercriminals prefer to operate and use hosting services in different countries where the hosting market is well-developed.

Countries where users face the greatest risk of online infection

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

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

	Country*	% of unique users**
1	Russia	48.90
2	Kazakhstan	46.27
3	Azerbaijan	43.23
4	Ukraine	40.40
5	Vietnam	39.55
6	Mongolia	38.27
7	Belarus	37.91
8	Armenia	36.63
9	Algeria	35.64
10	Qatar	35.55
11	Latvia	34.20
12	Nepal	33.94
13	Brazil	33.66
14	Kyrgyzstan	33.37
15	Moldova	33.28
16	China	33.12
17	Thailand	32.92
18	Lithuania	32.80
19	UAE	32.58
20	Portugal	32.31

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 2015, the top three saw no change from the previous year. Russia remained in first place although the percentage of unique users in the country decreased by 4.9 p.p.

Germany, Tajikistan, Georgia, Saudi Arabia, Austria, Sri Lanka and Turkey left the Top 20. Among the newcomers are Latvia, Nepal, Brazil, China, Thailand, the United Arab Emirates and Portugal.

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

1. **The high risk group (over 41%)**

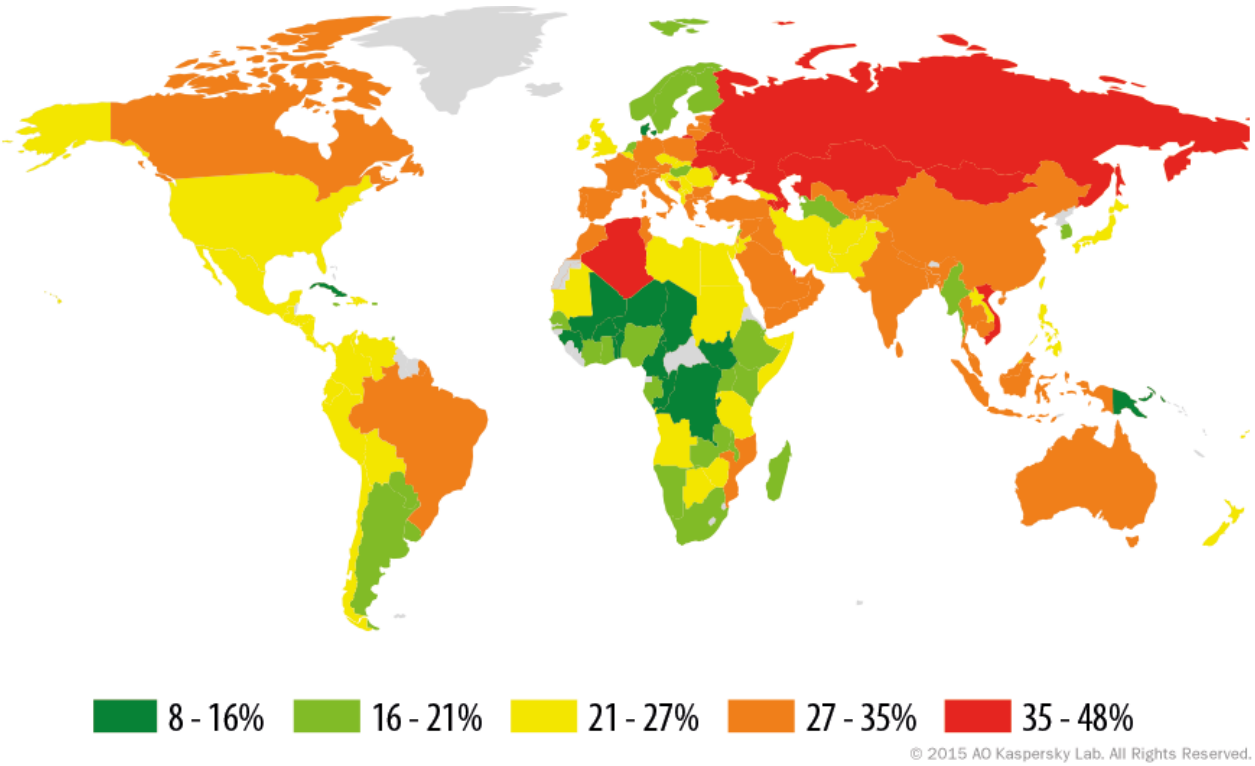
   In 2015, this group includes the first three countries from the Top 20 - Russia, Kazakhstan and Azerbaijan.

2. **The medium risk group (21-40.9%)**

   This group includes 109 countries; among them are France (32.1%), Germany (32.0%), India (31.6%), Spain (31.4%), Turkey (31.0%), Greece (30.3%), Canada (30.2%), Italy (29.4%), Switzerland (28.6%), Australia (28.0%), Bulgaria (27.0%), USA (26.4%), Georgia (26, 2%), Israel (25.8%), Mexico (24.3%), Egypt (23.9%), Romania (23.4%), UK (22.4%), Czech Republic (22.0%), Ireland (21.6%), and Japan (21.1%).

3. **The low risk group (0-20.9%)**

   The 52 countries with the safest online surfing environments include Kenya (20.8%), Hungary (20.7%), Malta (19.4%), the Netherlands (18.7%), Norway (18.3%), Argentina (18.3%), Singapore (18,2%), Sweden (18%), South Korea (17.2%), Finland (16.5%), and Denmark (15, 2%).



In 2015, **34.2%** of computers were attacked at least once while their owners were online.

On average, the risk of being infected while surfing the Internet decreased by 4.1 p.p. over the year. This could be due to several factors:

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

LOCAL THREATS

Local infection statistics for user computers are a very important indicator: they reflect threats that have penetrated computer systems by infecting files or removable media, or initially got on the computer in an encrypted format (for example, programs integrated in complex installers, encrypted files, etc.). In addition, these statistics include objects detected on user computers after the first scan of the system by Kaspersky Lab's file antivirus.

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

In 2015, Kaspersky Lab's antivirus solutions detected **4 million** unique malicious and potentially unwanted objects, a twofold increase from the previous year.

The TOP 20 malicious objects detected on user computers

For this rating we identified the 20 most frequently detected threats on user computers in 2015. This rating does not include the Adware and Riskware classes of program.

	Name*	% of unique attacked users**
1	DangerousObject.Multi.Generic	39.70
2	Trojan.Win32.Generic	27.30
3	Trojan.WinLNK.StartPage.gena	17.19
4	Trojan.Win32.AutoRun.gen	6.29
5	Virus.Win32.Sality.gen	5.53
6	Worm.VBS.Dinihou.r	5.40
7	Trojan.Script.Generic	5.01
8	DangerousPattern.Multi.Generic	4.93
9	Trojan-Downloader.Win32.Generic	4.36
10	Trojan.WinLNK.Agent.ew	3.42
11	Worm.Win32.Debris.a	3.24
12	Trojan.VBS.Agent.ue	2.79
13	Trojan.Win32.Autoit.cfo	2.61
14	Virus.Win32.Nimnul.a	2.37
15	Worm.Script.Generic	2.23

	Name*	% of unique attacked users**
16	Trojan.Win32.Starter.lgb	2.04
17	Worm.Win32.Autoit.aiy	1.97
18	Worm.Win32.Generic	1.94
19	HiddenObject.Multi.Generic	1.66
20	Trojan-Dropper.VBS.Agent.bp	1.55

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

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

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

The DangerousObject.Multi.Generic verdict, which is used for malware detected with the help of cloud technologies, is in 1st place (39.7%). Cloud technologies work when the antivirus databases do not yet contain either signatures or heuristics to detect a malicious program but the company's cloud antivirus database already has information about the object. In fact, this is how the very latest malware is detected.

The proportion of viruses continues to decrease: for example, last year Virus.Win32.Sality.gen affected 6.69% of users while in 2015 – only 5.53%. For Virus.Win32.Nimnul these figures are 2.8% in 2014 and 2.37% in 2015. The Trojan-Dropper.VBS.Agent.bp verdict, which is 20th in the rating, is a VBS script that extracts Virus.Win32.Nimnul from itself and saves in to the disk.

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

Countries where users face the highest risk of local infection

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

The TOP 20 countries by the level of infection

	Country*	% of unique users**
1	Vietnam	70.83
2	Bangladesh	69.55
3	Russia	68.81
4	Mongolia	66.30
5	Armenia	65.61
6	Somali	65.22
7	Georgia	65.20
8	Nepal	65.10
9	Yemen	64.65
10	Kazakhstan	63.71
11	Iraq	63.37
12	Iran	63.14
13	Laos	62.75
14	Algeria	62.68
15	Cambodia	61.66
16	Rwanda	61.37
17	Pakistan	61.36
18	Syria	61.00
19	Palestine	60.95
20	Ukraine	60.78

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.

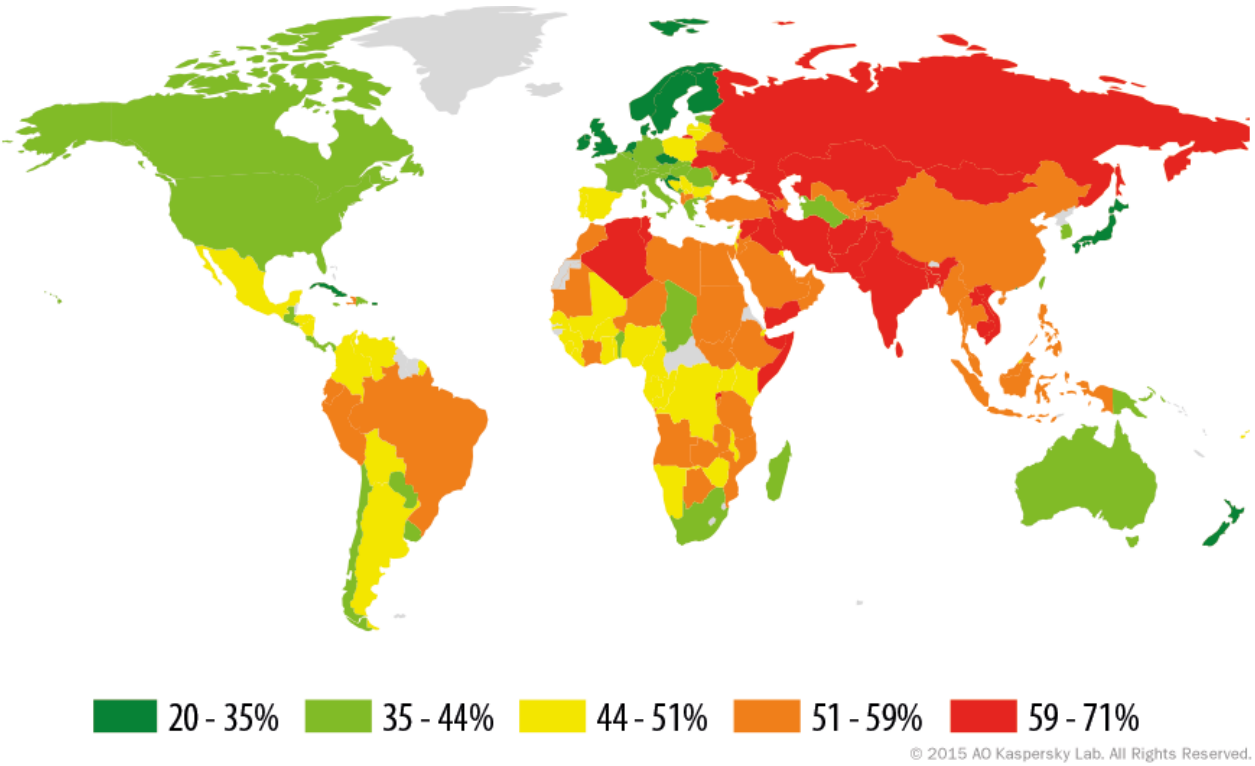
** When calculating, we excluded countries where there are fewer than 10,000 Kaspersky Lab users*

*** 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 the third year in a row Vietnam topped the rating. Mongolia and Bangladesh swapped places – Bangladesh climbed from 4th to 2nd, while Mongolia moved from 2nd to 4th. Russia, which was not in last year's Top 20, came third in 2015.

India, Afghanistan, Egypt, Saudi Arabia, Sudan, Sri Lanka, Myanmar, and Turkey all left the Top 20. The newcomers were Russia, Armenia, Somalia, Georgia, Iran, Rwanda, the Palestinian territories, and Ukraine.

In the Top 20 countries at least one malicious object was found on an average of 67.7% of computers, hard drives or removable media belonging to KSN users. The 2014 the figure was 58.7%.



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

1. **Maximum risk (over 60%):** 22 countries, including Kyrgyzstan (60.77%), Afghanistan (60.54%)
2. **High risk (41-60%):** 98 countries including India (59.7%), Egypt (57.3%), Belarus (56.7%), Turkey (56.2%), Brazil (53.9%), China (53.4%), UAE (52.7%), Serbia (50.1%), Bulgaria (47.7%), Argentina (47.4%), Israel (47.3%), Latvia (45.9%), Spain (44.6%), Poland (44.3%), Germany (44%), Greece (42.8%), France (42.6%), Korea (41.7%), Austria (41.7%).
3. **Moderate local infection rate (21-40.99%):** 45 countries including Romania (40%), Italy (39.3%), Canada (39.2%), Australia (38.5%), Hungary (38.2%), Switzerland (37.2%), USA (36.7%), UK (34.7%), Ireland (32.7%), Netherlands (32.1%), Czech Republic (31.5%), Singapore (31.4%), Norway (30.5%), Finland (27.4%), Sweden (27.4%), Denmark (25.8%), Japan (25.6%).

The 10 safest countries were:

	Country	%*
1	Cuba	20.8
2	Seychelles	25.3
3	Japan	25.6
4	Denmark	25.8
5	Sweden	27.4
6	Finland	27.4
7	Andorra	28.7
8	Norway	30.5
9	Singapore	31.4
10	Czech Republic	31.5

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

The appearance of Andorra, replacing Martinique, was the only change to this rating in 2015 compared to the previous year.

On average, 26.9% of user computers were attacked at least once during the year in the 10 safest countries. This is an increase of 3.9 p.p. compared to 2014.

CONCLUSION

Based on analysis of the statistics, we can highlight the main trends in cybercriminal activity:

- Some of those involved in cybercrime are looking to minimize the risk of criminal prosecution and switching from malware attacks to the aggressive distribution of adware.
- The proportion of relatively simple programs used in mass attacks is growing. This approach allows the attackers to quickly update malware which enhances the effectiveness of attacks.
- Attackers have mastered non-Windows platforms – Android and Linux: almost all types of malicious programs are created and used for these platforms.
- Cybercriminals are making active use of Tor anonymization technology to hide command servers, and Bitcoins for making transactions.

An increasing proportion of antivirus detections fall into a 'gray zone'. This applies primarily to a variety of advertising programs and their modules. In our 2015 ranking of web-based threats, the representatives of this class of program occupy 12 places in the Top 20. During the year, advertising programs and their components were registered on 26.1% of all user computers where our web antivirus is installed. The growth in the volume of advertising programs, along with their aggressive distribution methods and attempts to counteract anti-virus detection, continues the trend of 2014. Spreading adware earns good money, and in the pursuit of profit the authors sometimes use the tricks and technologies typical of malicious programs.

In 2015, virus writers demonstrated a particular interest in exploits for Adobe Flash Player. According to our observations, landing pages with exploits are often downloaded by exploits for Adobe Flash Player. There are two factors at play here: firstly, a large number of vulnerabilities were detected in the product over the year; secondly, as a result of a data leak by Hacking Team, information about previously unknown vulnerabilities in Flash Player were made public, and attackers wasted no time in taking advantage.

The banking Trojan sphere witnessed an interesting development in 2015. The numerous modifications of ZeuS, which had continuously topped the ranking of the most commonly used malware families for several years, were dethroned by Trojan-Banker.Win32.Dyreza. Throughout the year, the rating for malicious programs designed to steal money via Internet banking systems was headed by Upatre, which downloads

banking Trojans from the family known as Dyre/Dyzap/Dyreza to victims' computers. In the banking Trojan sector as a whole, the share of users attacked by Dyreza exceeded 40%. The banker uses an effective of web injection method in order to steal data to access the online banking system.

Also of note is the fact that two families of mobile banking Trojans – Faketoken and Marcher – were included in the Top 10 banking Trojans most commonly used in 2015. Based on current trends, we can assume that next year mobile bankers will account for a much greater percentage in the rating.

In 2015, there were a number of changes in the ransomware camp:

1. While the popularity of blockers is gradually falling, the number of users attacked by encryption ransomware increased by 48.3% in 2015. Encrypting files instead of simply blocking the computer is a method that in most cases makes it very difficult for the victims to regain access to their information. The attackers are especially active in utilizing encryption ransomware for attacks on business users, who are more likely to pay a ransom than ordinary home users. This is confirmed by the appearance in 2015 of the first ransomware for Linux, targeting web servers.
2. At the same time, encryptors are becoming multi-module and, in addition to encryption, include functionality designed to steal data from user computers.
3. While Linux may only now have attracted the attention of fraudsters, the first ransomware Trojan for Android was detected back in 2014. In 2015, the number of attacks aimed at the Android OS grew rapidly, and by the end of the year 17% of attacks involving ransomware were blocked on Android devices.
4. The threat is actively spreading all over the planet: Kaspersky Lab products detected ransomware Trojans in 200 countries and territories, which is practically everywhere.

We expect that in 2016 cybercriminals will continue to develop encryption ransomware that targets non-Windows platforms: the proportion of encryptors targeting Android will increase, while others will emerge for Mac. Given that Android is widely used in consumer electronics, the first ransomware attack on 'smart' devices may occur.

2016 PREDICTIONS: IT'S THE END OF THE WORLD FOR APTS AS WE KNOW THEM

INTRODUCTION

As the year comes to an end, we have an opportunity to take stock of how the industry has evolved and to cast our predictions for the coming years. Taking advantage of a rare global meeting of our GReAT and Anti-Malware Research experts, we tossed ideas into the ring and I have the privilege of selecting some of the more noteworthy and plausible for both the coming year and the long-term future as we foresee it. The outlook for our rapidly evolving field of study is quite thought-provoking and will continue to present us with interesting challenges. By sticking to sober metrics, perhaps we can skip the usual science fiction fear mongering and come to some accurate predictions for both the short- and long-term.

NO MORE APTs

Before you start celebrating, we should point out that we're referring to the 'Advanced' and 'Persistent' elements – both of which the threat actors would gladly drop for overall stealth. We expect to see a decrease in the emphasis on persistence, placing a greater focus on memory-resident or fileless malware. The idea will be to reduce the traces left on an infected system and thus avoid detection altogether. Another approach will be to reduce the emphasis on advanced malware. Rather than investing in bootkits, rootkits, and custom malware that gets burned by research teams, we expect an increase in the repurposing of off-the-shelf malware. Not only does this mean that the malware platform isn't burned upon discovery but it also has the added benefit of hiding the actor and his intentions in a larger crowd of mundane uses for a commercially available RAT. As the shine of cyber-capabilities wears off, return on investment will rule much of the decision-making of state-sponsored attackers – and nothing beats low initial investment for maximizing ROI.

THE NIGHTMARE OF RANSOMWARE CONTINUES

We expect to see the success of Ransomware spread to new frontiers. Ransomware has two advantages over traditional banking threats: direct monetization and relatively low cost per victim. This amounts to decreased interest from well-resourced third-parties such as banks, as well as low levels of reporting to law-enforcement agencies. Not only do we expect ransomware to gain ground on banking trojans but we also expect it to transition into other platforms. Weak attempts at bringing ransomware to mobile (Simplelocker) and Linux (Ransom.Linux.Cryptor, Trojan-Ransom.FreeBSD.Cryptor) have already been witnessed, but perhaps the more desirable target platform is OS X. We expect ransomware to cross the Rubicon to not only target Macs but also charge 'Mac prices'. Then, in the longer term, there is the likelihood of IoT ransomware, begging the question, how much would you be willing to pay to regain access to your TV programming? Your fridge? Your car?

BETTING AGAINST THE HOUSE: FINANCIAL CRIMES AT THE HIGHEST LEVEL

The merging of cybercrime and APT has emboldened financially motivated criminals who have gracefully transitioned from attacking end users to going after the financial institutions themselves. The past year has seen plenty of examples of attacks on point-of-sale systems and ATMs, not to mention the daring Carbanak heist that pilfered hundreds of millions of dollars. In the same vein, we expect cybercriminals to set their sights on novelties like alternate payment systems (ApplePay and AndroidPay) whose increasing rate of adoption should offer a new means of immediate monetization. Another inevitable point of interest is stock exchanges, the true mother lode. While frontal attacks may yield quick payoffs, we mustn't overlook the possibility of more subtle means of interference, such as going after the black-box algorithms employed in high-frequency trading to ensure prolonged gains with a lower likelihood of getting caught.

ATTACKS ON SECURITY VENDORS

As attacks on security vendors rise, we foresee an interesting vector in compromising industry-standard reverse-engineering tools like IDA and Hiew, debugging tools like OllyDbg and WinDbg, or virtualization tools like the VMware suite and VirtualBox. CVE-2014-8485, a vulnerability in the Linux implementation of 'strings', presents an example of the vulnerable landscape of nontrivial security research tools that determined attackers may choose to exploit when targeting researchers themselves. In a similar vein, the sharing of freeware research tools through code repositories like Github is an area ripe for abuse, as users will more often than not pull code and execute it on their systems without so much as a glance. Perhaps we should also be casting a suspicious glance towards popular implementations of PGP so eagerly embraced by the infosec community.

SABOTAGE, EXTORTION AND SHAME

From dumps of celebrity nudes to the Sony and Ashley Madison hacks and the HackingTeam dump, there has been an undeniable increase in DOXing, public shaming, and extortion. Hacktivists, criminals, and state-sponsored attackers alike have embraced the strategic dumping of private pictures, information, customer lists, and code to shame their targets. While some of these attacks are strategically targeted, some are also the product of opportunism, taking advantage of poor cybersecurity to feign hacker prowess. Sadly, we can only expect this practice to continue to rise exponentially.

WHOM DO YOU TRUST?

Perhaps the scarcest commodity in the current internet age is trust. Abuse of trusted resources will further drive this scarcity. Attackers will continue to enlist open-source libraries and whitelisted resources for malicious purposes. We expect another form of trust to be abused, that of a company's internal resources: as crafty attackers seek to expand their foothold on an infected network, they may target resources limited to the company intranet such as waterholing Sharepoint, file server, or ADP portals. Perhaps we'll even witness the furthest extension of the already rampant abuse of trusted certificates as attackers establish an entirely fabricated certificate authority to issue certificates for their malware.

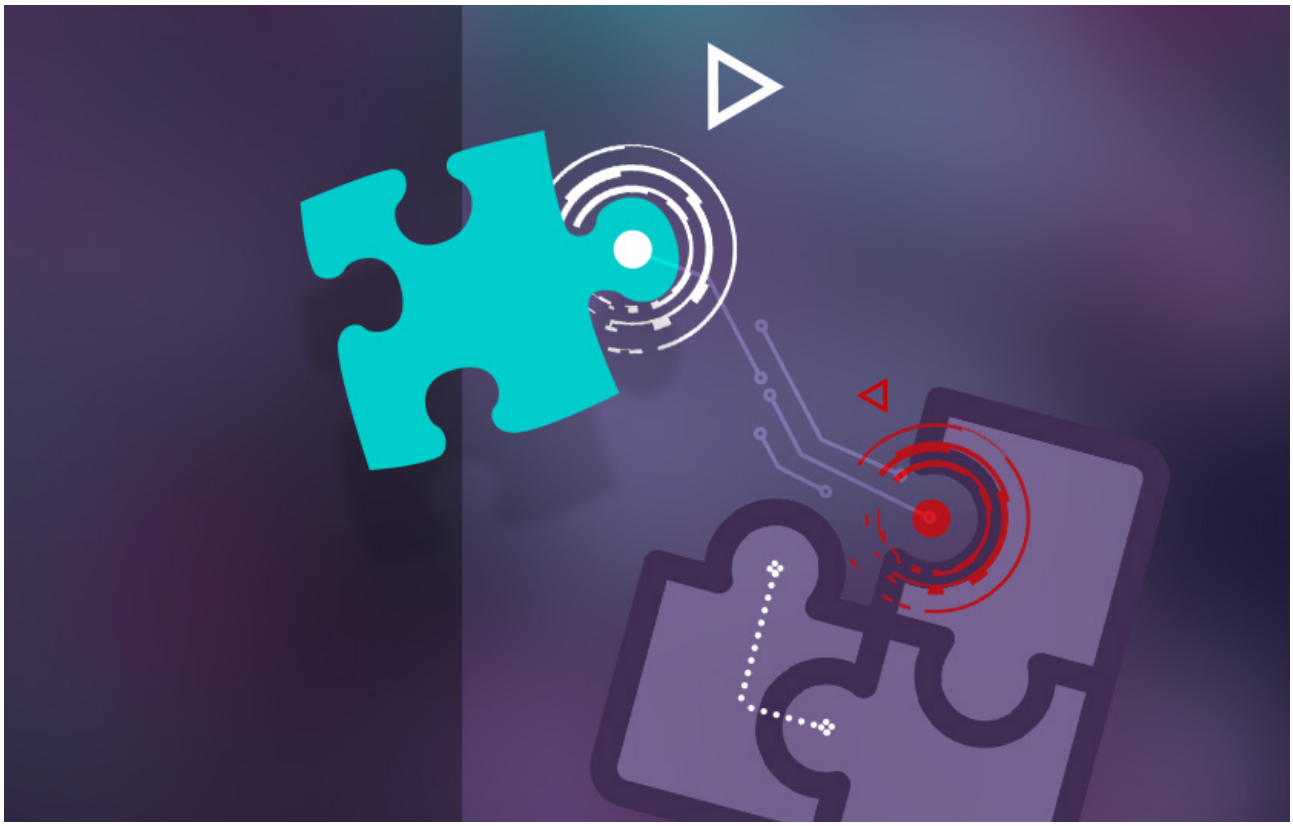
APT ACTORS DOWN THE ROAD

The profitability of cyberespionage has not escaped the attention of our foes and, as we expected, mercenaries have begun populating the scene. This trend will only increase to match the demand for cyber-capabilities by both companies as well as known APT actors looking to outsource less critical tasking without risking their tools and infrastructure. We could float the term 'APT-as-a-Service', but perhaps more interestingly we can expect the evolution of targeted attacks to yield 'Access-as-a-Service'. The latter entails the sale of access to high-profile targets that have already fallen victim to mercenaries.

Looking further into the future of cyberespionage, we see members of well-established APT teams ('APT 1%ers', if you will) potentially coming out of the shadows. This would happen in one of two forms: as part of the private sector with the proliferation of 'hacking back', or by sharing their insights with the larger infosec community, perhaps by joining us at conferences to share the other side of the story. In the meantime, we can expect the APT Tower of Babel to incorporate a few more languages.

THE FUTURE OF THE INTERNET

The infrastructure of the internet itself has shown signs of tension and cracks in recent years. Concerns over massive router botnets, BGP hijacking and dampening, DNS attacks en masse, or server-powered DDoSes betray a lack of accountability and enforcement on a global scale. Looking further down the line to long-term predictions, we can consider what the internet might look like if that narrative of a globally connected village continues to wither. We may end up with a balkanized internet divided by national borders. At that point, concerns over availability may come down to attacks on the service junctures that provide access between different sections, or perhaps geopolitical tensions that target the cables that connect large swathes of the internet. Perhaps we'll even see the rise of a black market for connectivity. Similarly, we can expect that as technologies that power the internet's underbelly continue to gain mainstream attention and widespread adoption, developers with a stake in shadow markets, exchanges, and forums are likely to develop better technologies to keep the underground truly underground.

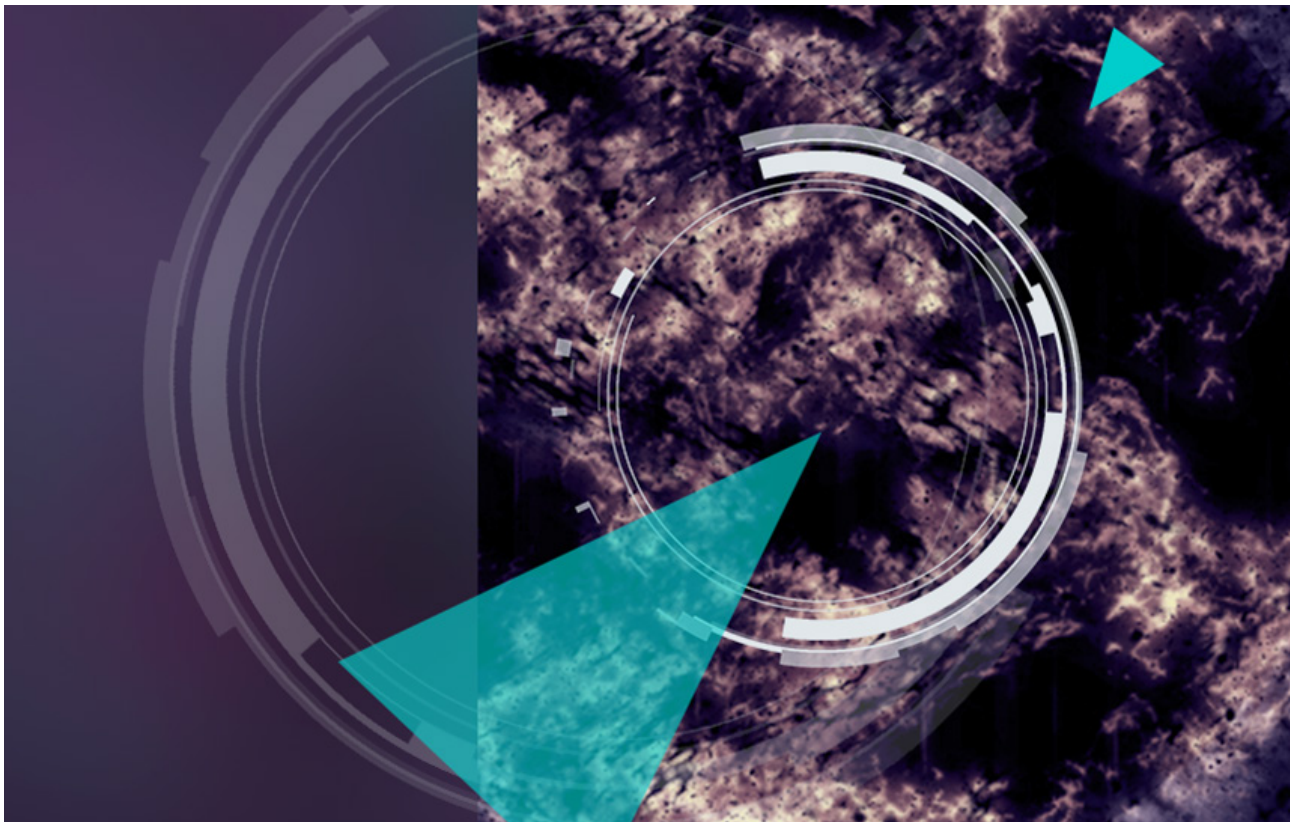


THE FUTURE OF TRANSPORTATION

As investment and high-end research capabilities are dedicated to developing autonomous vehicles for both personal and commercial distribution, we will witness the rise of distributed systems to manage the routes and traffic of large volumes of these vehicles. The attacks may not focus on the distribution systems themselves, but perhaps on the interception and spoofing of the protocols they rely on (a proof of concept of the vulnerabilities of the widely adopted Global Star satcom system was presented by a Synack researcher at this year's BlackHat conference). Foreseeable intentions behind these attacks include theft of high-value goods or kinetic damage resulting in loss of life.

THE CRYPTOPOCALYPSE IS NIGH

Finally, we cannot overemphasize the importance of cryptographic standards in maintaining the functional value of the internet as an information-sharing and transactional tool of unparalleled promise. These cryptographic standards rely on the expectation that the computational power required to break their encrypted output is simply above and beyond our combined means as a species. But what happens when we take a paradigmatic leap in computational capabilities as promised by future breakthroughs in quantum computing? Though quantum capabilities will not be initially available to the common cybercriminal, it signals a breakdown in the reliability of current crypto-standards and a need to design and implement 'post-quantum cryptography'. Given the poor rate of adoption or proper implementation of high-quality cryptography as it is, we do not foresee a smooth transition to counterbalance cryptographic failures at scale.



Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy