KASPERSKY lab

Kaspersky Security Bulletin 2015

EVOLUTION OF CYBER THREATS IN THE CORPORATE SECTOR

GREAT

#KLReport

CONTENT

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

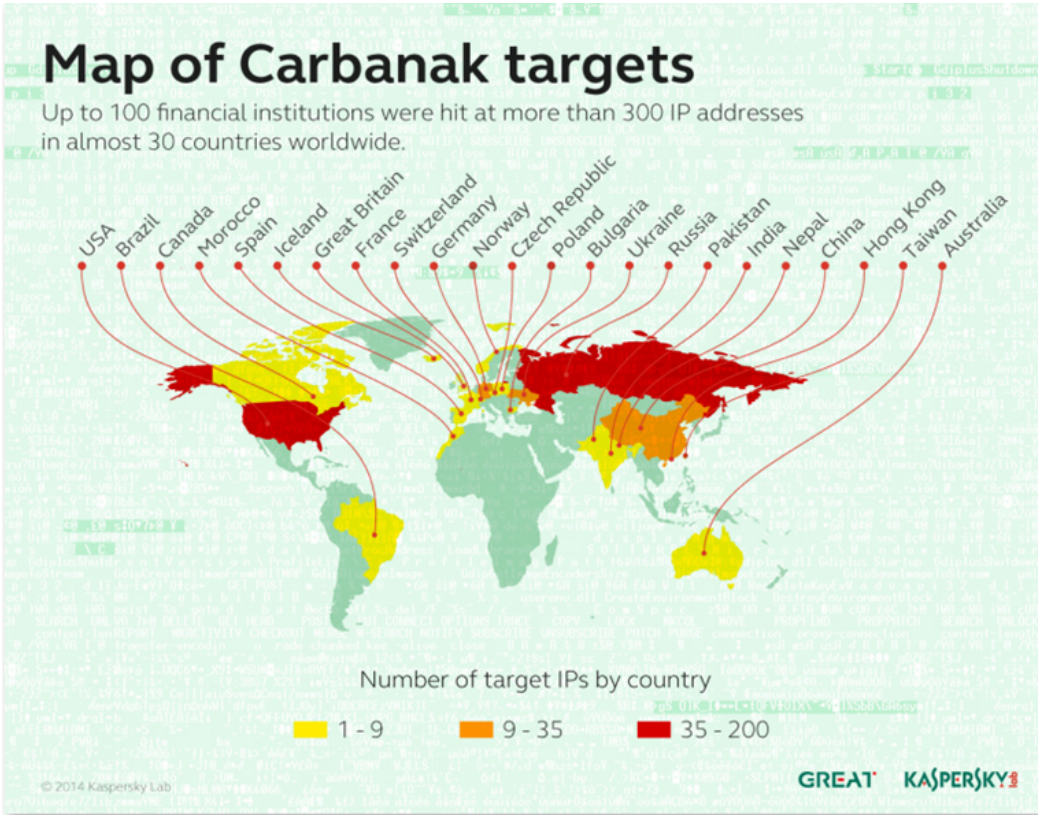
- In 2015 one or more malware attacks were blocked on 58% of corporate computers. This is a 3 p.p. rise on the previous year.
- 29% of computers – i.e. almost every third business-owned computer – were subjected to one or more web-based attacks.
- Malware exploiting vulnerabilities in office applications 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.

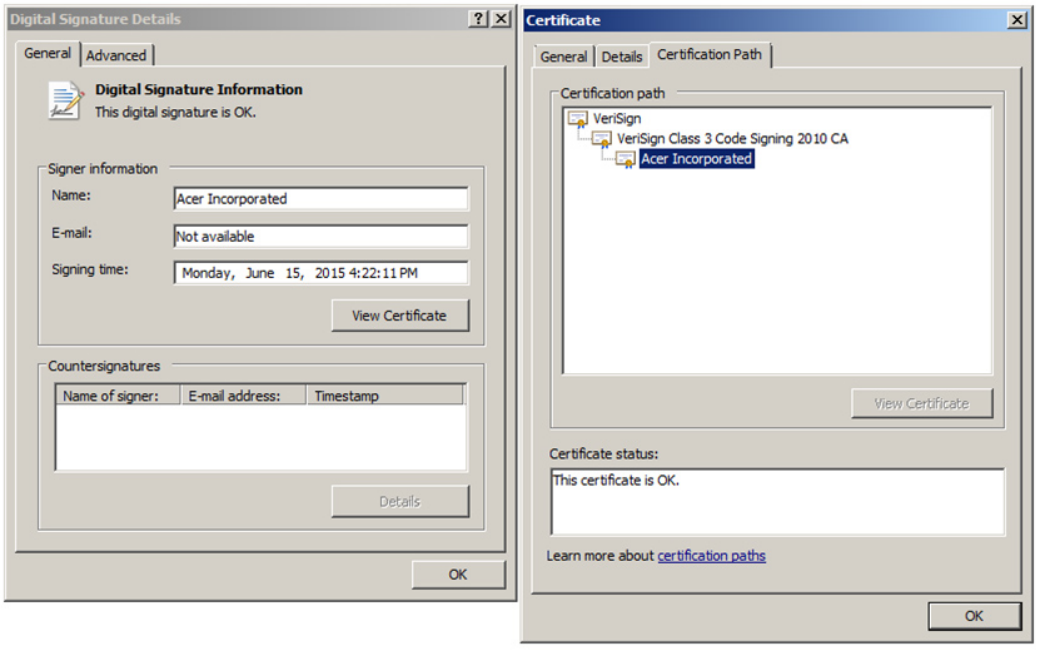
Most of the organizations targeted were located in Eastern Europe. However, the Carbanak campaign has also targeted victims in the US, Germany and China. Up to 100 financial institutions have been affected across the globe, and the total losses could be as a high as $1 billion.



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.



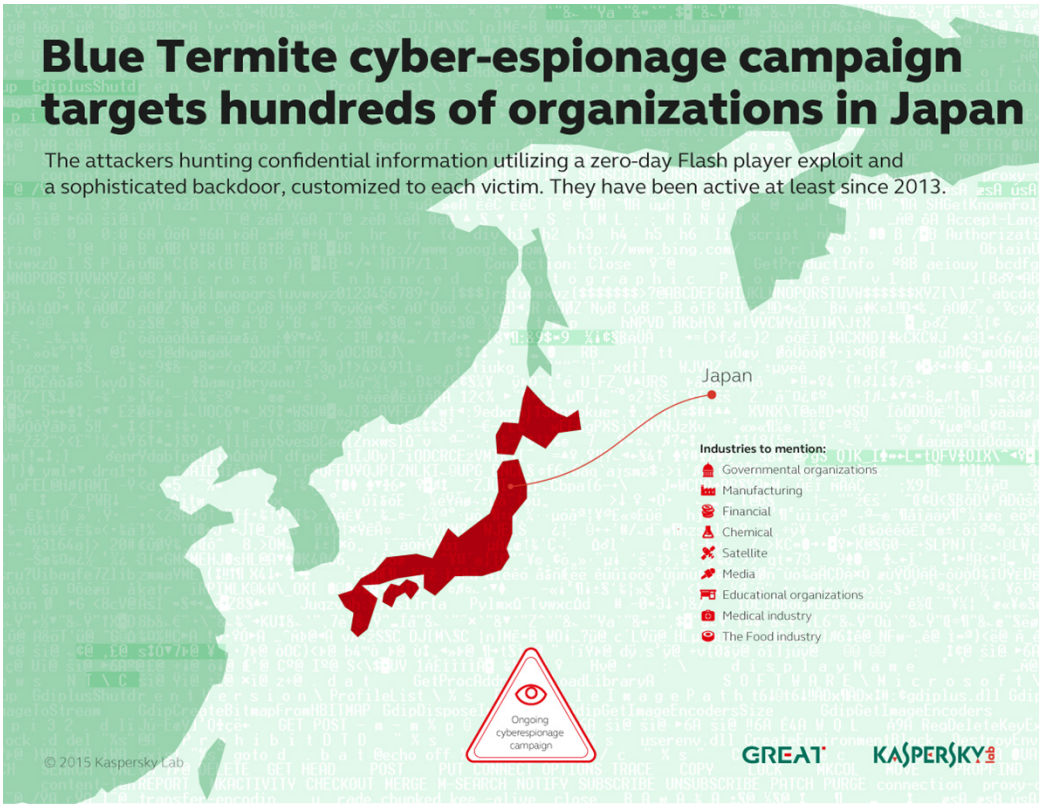
Stolen Acer certificate in the Wild Neutron installer

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.

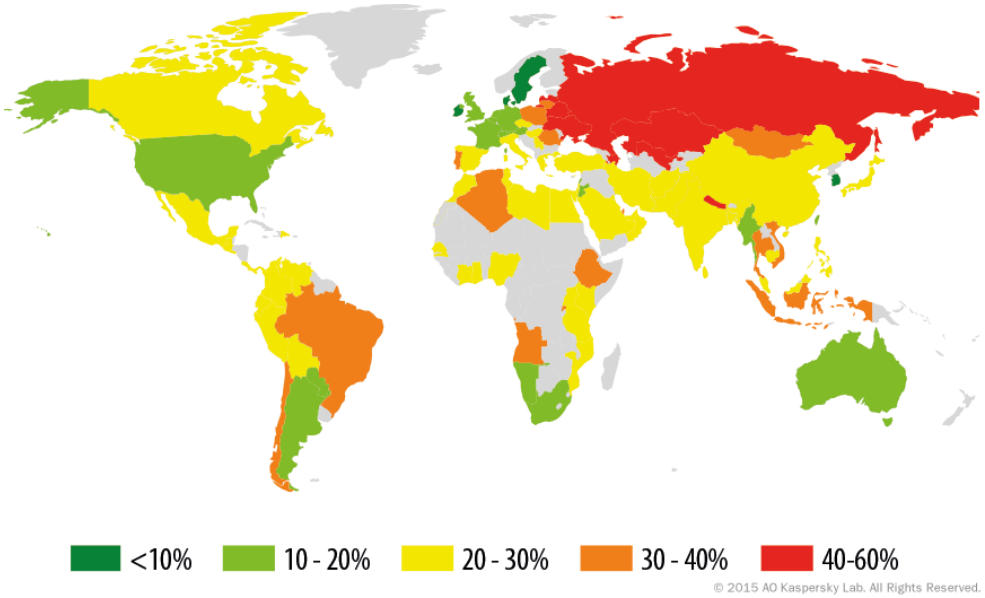
	Name*	% of unique users attacked**
1	Malicious URL	57%
2	Trojan.Script.Generic	24.7%
3	Trojan.Script.Iframer	16.0%
4	Exploit.Script.Blocker	4.1%
5	Trojan-Downloader.Win32.Generic	2.5%
6	Trojan.Win32.Generic	2.3%
7	Trojan-Downloader.JS.Iframe.diq	2.0%
8	Exploit.Script.Generic	1.2%
9	Packed.Multi.MultiPacked.gen	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%
8	Trojan.Script.Generic	2.9%
9	DangerousPattern.Multi.Generic	2.7%
10	Worm.Win32.Debris.a	2.6%

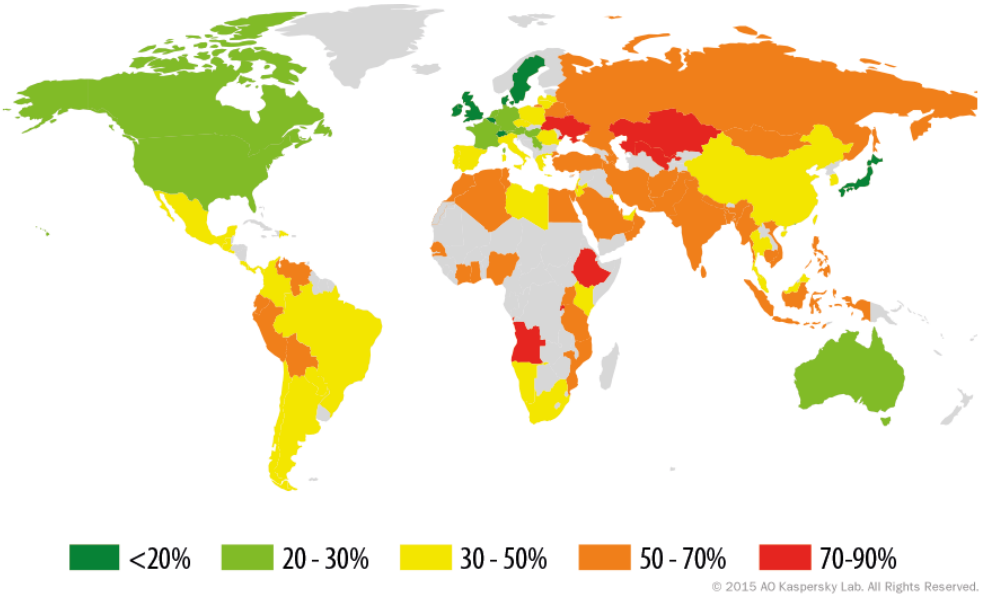
** These statistics are compiled from malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who have consented to submit their statistical data.*

*** 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:

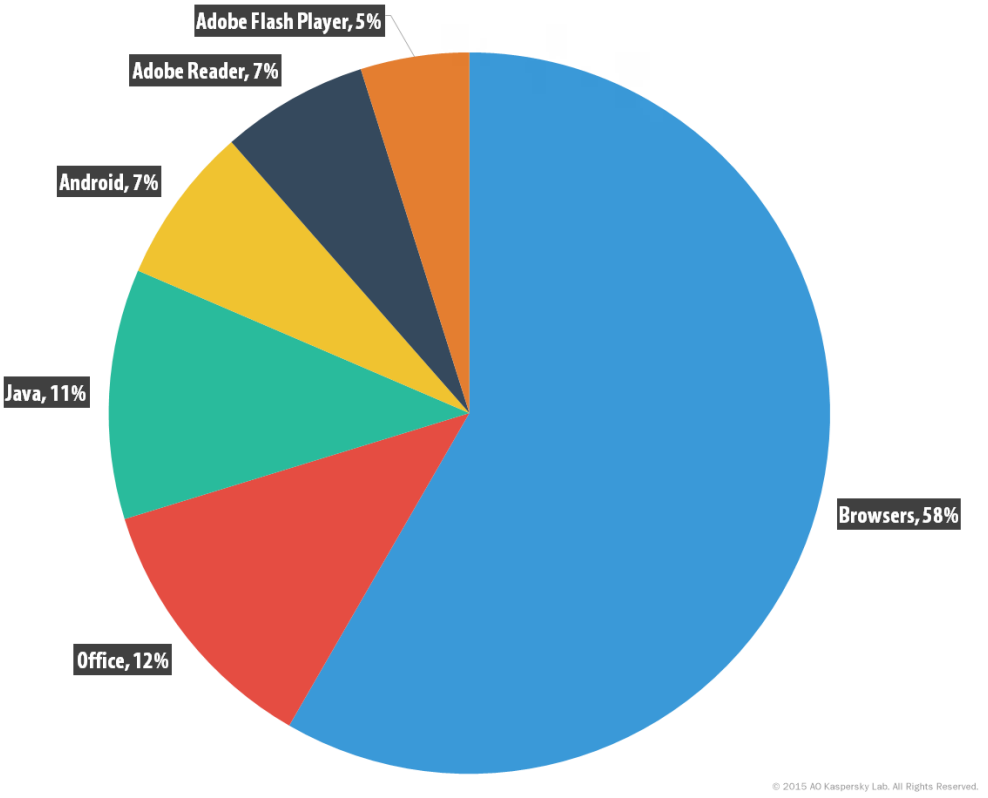
- exploits for vulnerabilities found in office applications are used three times more often than in attacks on home users;
- use of malicious files signed with valid digital certificates;
- use of legitimate programs in attacks, allowing the attackers to go undetected for longer.

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

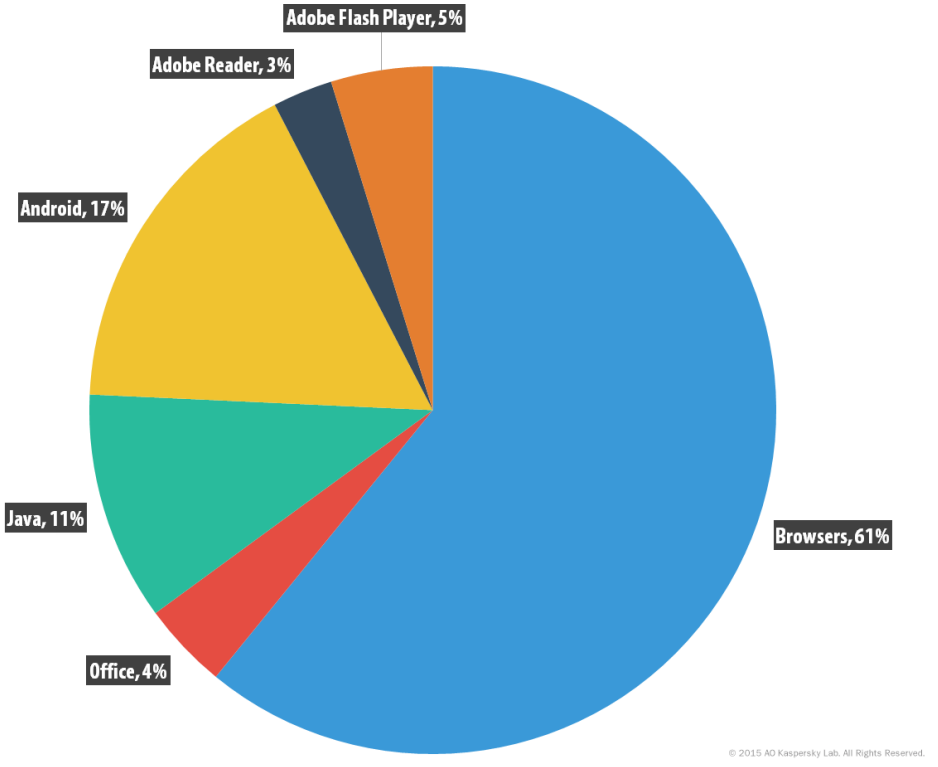
In this particular context, the majority of cases are not APT attacks: "standard" cybercriminals are simply focusing on corporate users, and sometimes on a particular company that is of interest to them.

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.



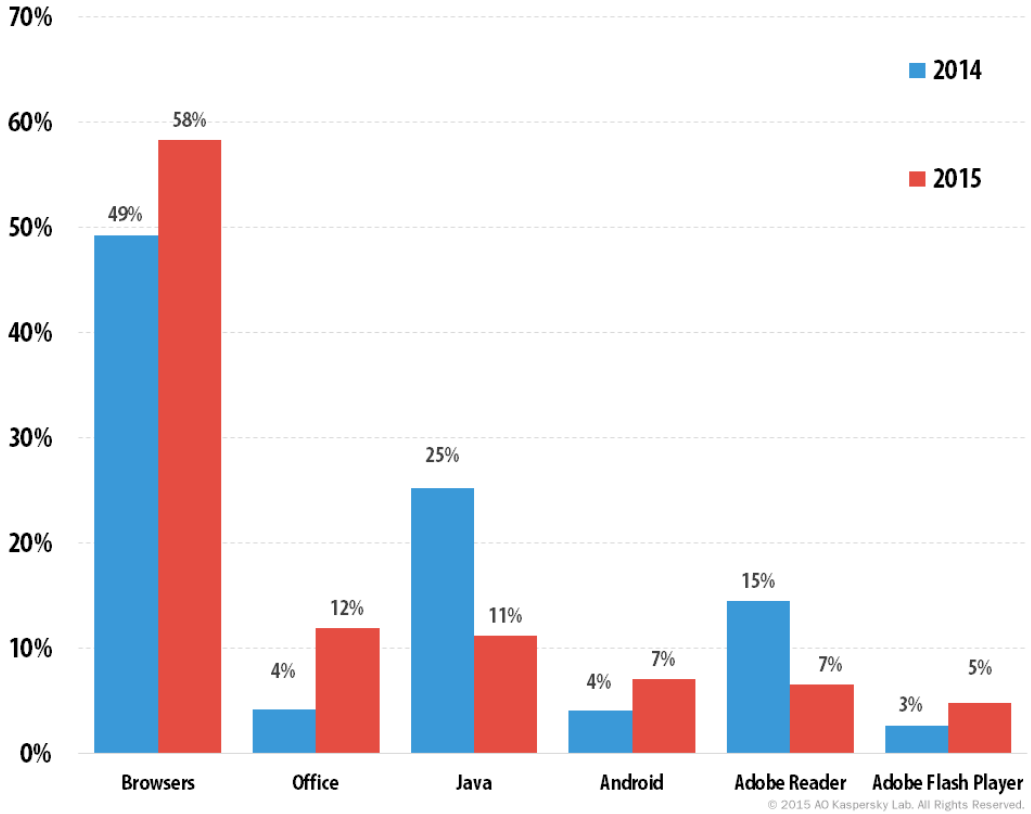
Distribution of exploits used in cybercriminal attacks by type of attacked application (corporate users, 2015)



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.

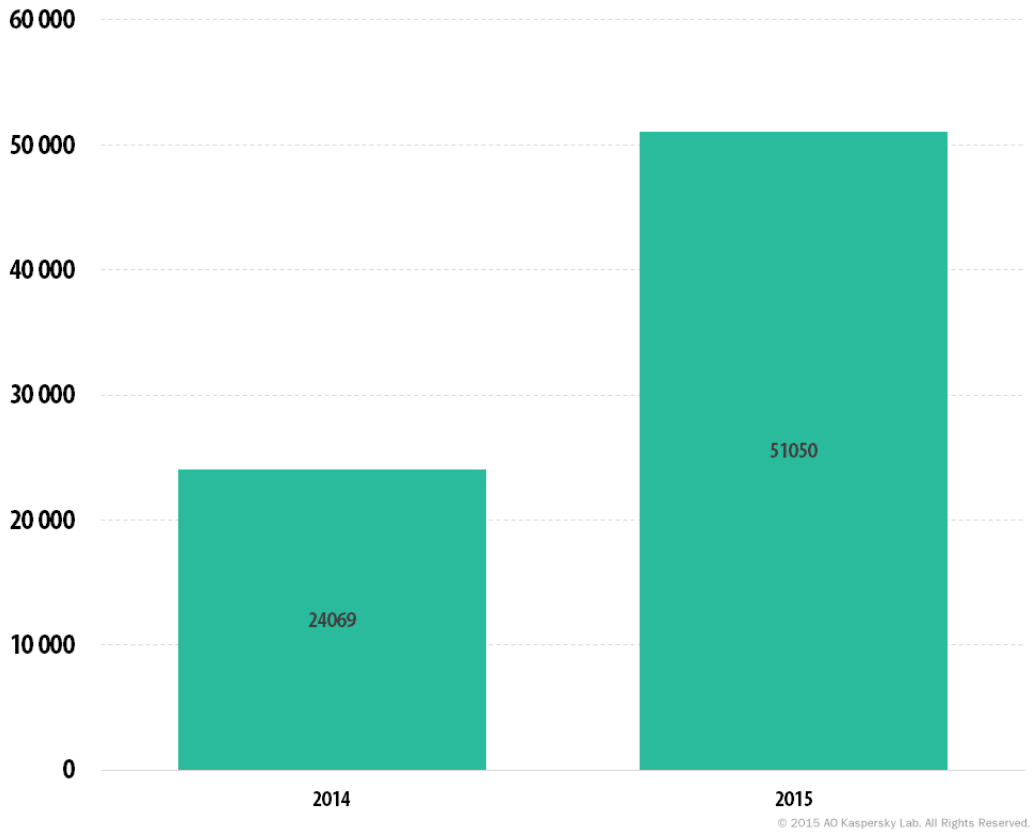
Investigations of security incidents have shown that even in targeted attacks on corporations, cybercriminals often use exploits for known vulnerabilities. This is because corporate environments are slow to install appropriate

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.

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