KASPERSKY lab

NAVIGATING THE THREAT LANDSCAPE

A practical guide

David Emm, Principal Security Researcher
Global Research & Analysis Team, Kaspersky Lab

www.kaspersky.com/business
#SecureBiz

Contents

About the author

David Emm, Principal Security Researcher Global Research & Analysis Team (GReAT)

David Emm is Principal Security Researcher at Kaspersky Lab, a provider of security and threat management solutions. He has been with Kaspersky Lab since 2004 and is currently part of the company's Global Research & Analysis Team. He has worked in the anti-malware industry since 1990 in a variety of roles, including Senior Technology Consultant at Dr Solomon's Software, and Systems Engineer and Product Manager at McAfee. In his current role, David regularly delivers presentations on malware and other IT threats at exhibitions and events, highlighting what organizations and consumers can do to stay safe online. He also provides comment to broadcast and media on the ever-changing cybersecurity and threat landscape. David has a strong interest in malware, ID theft and the security industry in general. He is a knowledgeable advisor on all aspects of online security.

Chapter 1: The evolution of malware

It's over 25 years since the first PC viruses appeared. Since then the nature of the threat has changed significantly and today the threats are more complex than ever before.

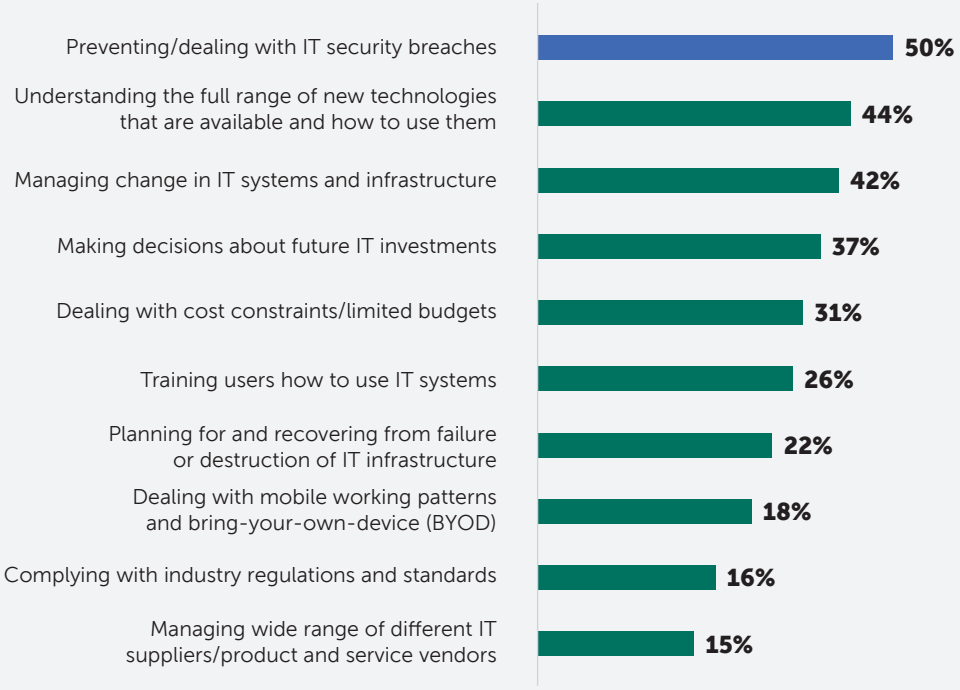
In recent years, the **Kaspersky Lab Global IT Risks Survey** has highlighted changes in working practices, all of which have had a significant impact on corporate security. These include growing mobility and the trend towards BYOD; the storage of business data in the cloud; the increased use of virtualized systems; and the widespread use of social media at work.

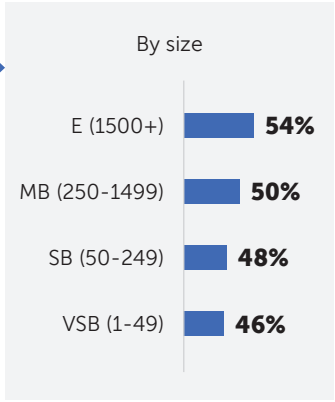
Security concerns around these developments continue to figure highly in the survey and, unsurprisingly, the 2015 results highlight that 'preventing and dealing with security breaches is a primary concern for 50% of companies[1] and guarding against cyberthreats is the top security priority for 27% of companies'.[2]

Dealing with security breaches is a primary concern for **50%** of companies.[1]

TOP CONCERNS OF THE IT FUNCTION[1]

Dealing with security breaches, understanding new technologies and managing changes to IT systems are the primary concerns. Security breaches are a concern to companies of all sizes.





1: Kaspersky Lab Global IT Risks Security Survey 2015
2: Kaspersky Lab Global IT Risks Security Survey 2015

COMPANY IT SECURITY PRIORITIES FOR THE NEXT 12 MONTHS[2]

Guarding against cyberthreats is now the top priority (previously third), supplanting preventing data leaks.

Increasing in scale, increasing in severity

The interconnected world means that attacks can be launched on victim's devices very quickly, and as widely or selectively as the malware authors and criminal underground sponsors require.

Malicious code can be embedded in an email, injected into fake software packs, placed on 'grey-zone' webpages, or download by a Trojan installed on an infected computer.

The scale of the problem has also continued to increase. The number of new malware samples discovered daily by Kaspersky Lab runs into hundreds of thousands.

2: Kaspersky Lab Global IT Risks Security Survey 2015

A problem of perception

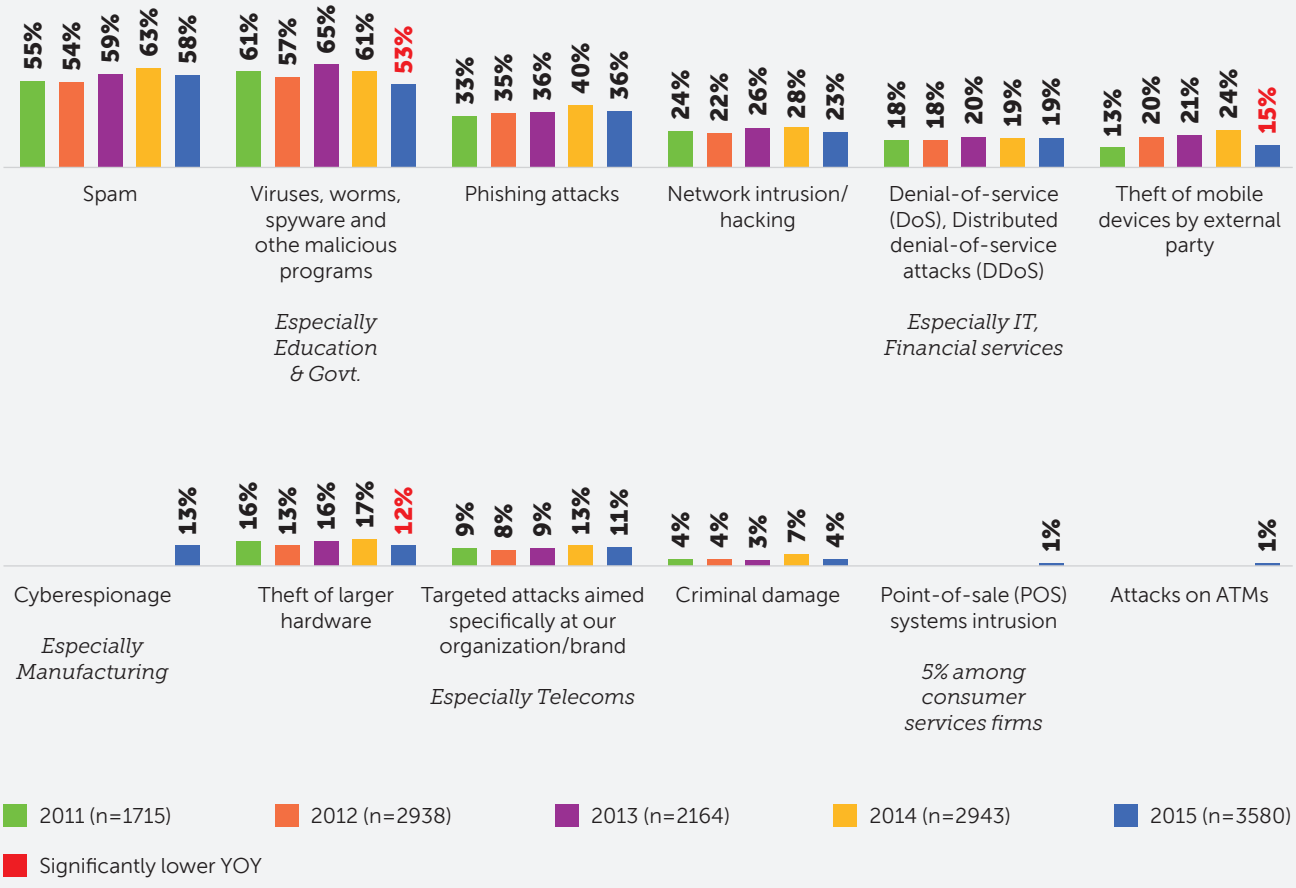
In the past 12 months 90% of companies experienced some form of external attack and 46% of companies reported an increase in the number of attacks[3], although there is a perception that there were fewer instances of data theft and obvious malware events in 2015.

But there's a misconception that malware belongs on its own, in a discrete category. In fact, malware forms an essential component of many cyberattacks and remains the most numerous and dangerous threat to IT security. Targeted attacks, cyberespionage, phishing attacks and more, all incorporate malware. So it's not that malware attacks are declining, but that they may not be perceived as malware attacks.

90% of companies had experienced some form of external incident.[3]

EXTERNAL THREATS EXPERIENCED[3]

90% of companies had experienced some form of external incident.
Fewer instances of theft and 'obvious' malware events in 2015 compared to previous waves.



3: Kaspersky Lab Global IT Risks Security Survey 2015

From cyber-vandalism to cybercrime

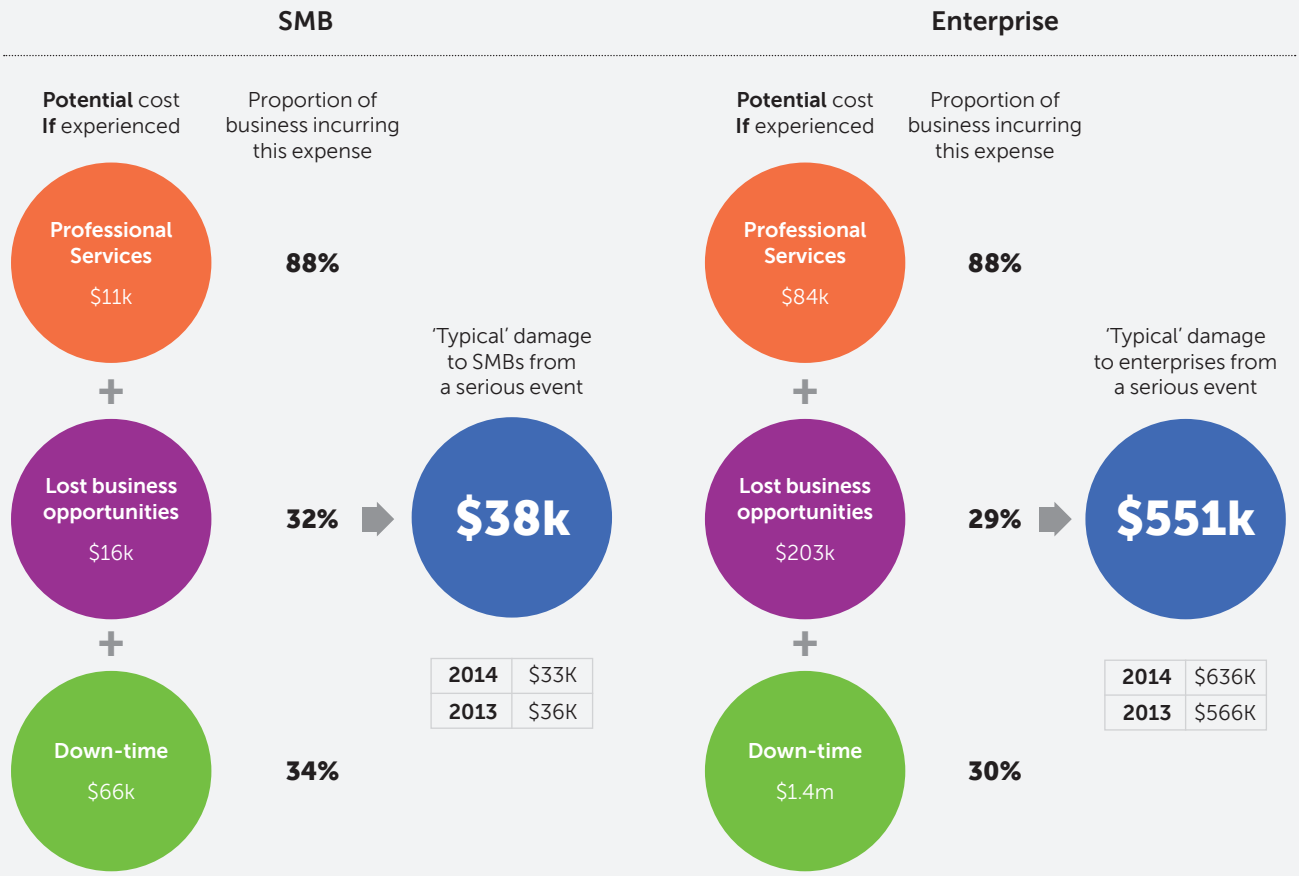
Until around 2003, viruses and other types of malware were largely isolated acts of computer vandalism – 'anti-social self-expression' using hi-tech means. Most viruses confined themselves to infecting other disks or programs.

After 2003, the threat landscape changed. Much of today's malware is purpose-built to hijack computers and make money illegally. As a result, the threats businesses now face have become significantly more complex. IT administrators have a lot more to contend with – there are more types of threats to protect against and the damage they cause is likely to be financial, not just 'IT down-time'.

1 in 3 companies who've experienced a data breach event suffered temporary loss of ability to trade and typical direct costs incurred from a serious event are **$38k** for **SMBs** and **$551k** for **enterprises.**[4]

ESTIMATED DIRECT COSTS INCURRED RESULTING FROM ANY SERIOUS DATA LOSS INCIDENT[4]

Although not every expense is incurred by every business, we can nonetheless estimate a typical loss taking into account the likelihood of an organization incurring each expense.



Each potential cost is multiplied by the likelihood to experience that cost then summed to find the expected overall 'typical' costs.

4: Kaspersky Lab Global IT Risks Security Survey 2015

New motives, new tactics

The change in motive also brought about a change in tactics. There was a decline in the number of global epidemics – designed to spread malware as far and as quickly as possible. Attacks have become more focused.

The main reason for the change is that attacks now have criminal intent and look to steal confidential data, which can then be processed and used. Where millions of victim machines are involved, detection is more likely and it creates a huge logistical operation. Therefore, malicious code authors now prefer to focus their attacks.

Malicious code authors now prefer to focus their attacks.

The rise of the Trojan

Trojans are the most common type of malware today. They are categorized according to their function: the most common include backdoors, password stealers, downloaders, and banking Trojans.

They are used to steal confidential information (username, password, PIN, etc.) for bank fraud.

They can be used to spy on victims. They can be used to install additional malware to suit the needs of the attackers. They can be used in DDoS (Distributed Denial of Service) attacks on organizations: such attacks seek to extort money from organizations, using a 'demonstration' DDoS attack to give the victim a taste of what will happen if they don't pay up.

Holding you to ransom

In recent years, there has also been a steady growth in 'ransomware'. This is the name given to malicious programs designed to extort money from their victims by either blocking access to the computer or encrypting the data stored on it. The malware displays a message offering to restore the system in return for a payment.

Sometimes the cybercriminals behind the scam try to lend credibility to their operation by masquerading as law enforcement officials: their ransom message states that access to the system has been blocked, or the data encrypted, because the victim is running unlicensed software or has accessed illegal content, for which the victim must pay a fine.

While anti-malware can detect ransomware, it may not be possible to decrypt the data. So it's vital to take regular backups – not only to avoid data loss resulting from ransomware, but to safeguard data from loss because of other computer problems.

Typically, compromised computers are combined into networks. The activities of these bot networks, or botnets, are controlled using websites or Twitter accounts. If the botnet has a single Command-and-Control (C2) server, it's possible to take it down once its location has been identified. But in recent years cybercriminals have developed more complex botnets that employ a peer-to-peer model, to avoid having a single point of failure. This has now become a standard feature of botnets.

A GReAT tip: Regularly back up your data

Even if you outsource the handling and storage of your data, you can't outsource the responsibility for it in the event of a security breach. Assess the potential risks in the same way you would if you were storing data internally. Data backup can help ensure an inconvenience doesn't turn into a disaster.

Phishing – masquerading as someone else

The use of malicious code is not the only method used by cybercriminals to gather personal data that can be used to make money illegally. Phishing involves tricking people into disclosing their personal details (username, password, PIN or any other access information) and then using these details to obtain money under false pretences.

Phishers create an almost 100% perfect replica of a chosen financial institution's website. They then spam out an email that imitates a genuine piece of correspondence from the real financial institution. Phishers typically use legitimate logos, good business style and even make reference to real names from the financial institution's senior management. They also spoof the header of the email to make it look like it has come from the legitimate bank.

The fake emails distributed by phishers have one thing in common: they are the bait used to try and lure the customer into clicking on a link provided in the message. If the bait is taken, the link takes the user directly to an imitation site, which contains a form for the victim to complete. Here they unwittingly hand over all the information the cybercriminal needs to access their account and steal their money.

Rootkits and code obfuscation

Rootkits are used to mask the presence of malicious code. They hide the changes they have made to a victim's machine.

Typically, the malware writer obtains access to the system by cracking a password or exploiting an application vulnerability, and then uses this to gain other system information until he achieves administrator access to the machine. Rootkits are often used to hide the presence of a Trojan, by concealing registry edits, the Trojan's process(es) and other system activity.

There has been a further development of the rootkit, known as a 'bootkit'. The first of these found in the field, in 2008, was Sinowal (also known as Mebroot). The aim is the same as any rootkit – mask the presence of malware in the system. But a bootkit installs itself on the Master Boot Record (MBR), in order to load early (the MBR is the first physical sector on the hard disk and code written to this sector is loaded immediately after the instructions in the BIOS are loaded). Since that time, there has been a steady stream of bootkits, including 64-bit versions.

A GReAT tip: Develop a security strategy

Your security strategy should be tailored to your business – not based on generic 'best practices' and 'guesstimates'. A thorough risk assessment can determine the risks your business faces. You'll need a mechanism to measure the effectiveness of your security tools and a process for updating the strategy to meet new threats.

Chapter 2: How malware spreads

Cybercriminals use different techniques to infect their victims. They are outlined individually below:

Drive-by downloads

This is one of the main methods used to spread malware. Cybercriminals look for insecure websites and hide their code in one of the webpages: when someone views that page, malware may be transferred automatically, and invisibly, to their computer along with the rest of the content that was requested. It's known as a 'drive-by download' because it doesn't require interaction from the victim – beyond simply visiting the compromised webpage.

The cybercriminals inject a malicious script into the webpage, which installs malware on the victim's computer or, more typically, takes the form of an iframe redirect to a site controlled by the cybercriminals. The victim becomes infected if the operating system or applications on their computer are unpatched.

Cybercriminals inject a malicious script into the webpage, which installs malware on the victim's computer or, more typically, takes the form of an iframe redirect to a site controlled by the cybercriminals.

Social networks

Cybercriminals, like pickpockets in the real world, 'work' the crowds. Some social networks have a user-base the size of a large country, thus providing a ready-made pool of potential victims. They use social networks in different ways.

- First, they use hacked accounts to distribute messages that contain links to malicious code
- Second, they develop fake 'apps' that harvest the victim's personal data (this can then be sold to other cybercriminals) or install malware (for example fake anti-virus programs)
- Third, they create fake accounts that gather 'friends', collect personal information and sell it on to advertisers.

Email and instant messaging

Around 3% of emails contain malware, in the form of attachments or links to malicious websites. In addition to the bulk phishing campaigns, designed to steal confidential data from anyone who falls for the scam, email is also used in targeted attacks, as a way of getting an initial foothold in the target organization(s). In this case, the email is sent to a specific person in an organization, in the hope that they will run the attachment or click the link and begin the process by which the attackers gain access to the system. This approach is known as spear-phishing.

To maximize their chances of success, cybercriminals typically send their email to public-facing (often non-technical) staff, such as sales and marketing managers. The email addresses the person by name, the 'From' address is spoofed to look like it has come from a trusted insider in the organization and the content of the email is tailored to the interests of the organization, so that it looks legitimate.

Typically targeted attack campaigns vary the content, depending on the specific nature of the company they are going after. Cybercriminals also make use of instant messaging to spread links to malware.

To maximize their chances of success, cybercriminals typically send their email to public-facing (often non-technical) staff, such as sales and marketing managers.

Removable media

Physical storage devices provide an ideal way for malware to spread. USB keys, for example, have been used to extend the penetration of malware within an organization, following the initial infection.

They have also been used to help malware to hop across the 'air-gap' between a computer connected to the Internet and a trusted network that is isolated from the Internet.

Often malware uses vulnerabilities in the way that USB keys are handled to launch code automatically when the device is inserted into a computer.

Vulnerabilities and exploits

One of the key methods used by cybercriminals to install malware on victims' computers is to exploit un-patched vulnerabilities in applications. This relies on the existence of vulnerabilities and the failure of individuals or businesses to patch their applications.

Such vulnerabilities – or loopholes – can be found within an operating system or the applications running on the computer. Cybercriminals typically focus their attention on applications that are widely used and are likely to be un-patched for the longest time – giving them a sufficient window of opportunity to achieve their goals.

Zero day exploits

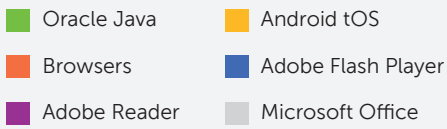
Cybercriminals don't just rely on the fact that people don't always patch their applications.

Sometimes they are even able to identify vulnerabilities before an application vendor does and write exploit code to take advantage of the flaw.

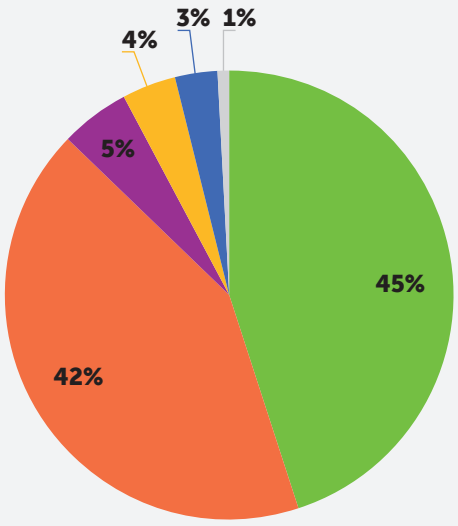
These are known as zero-day exploits and provide cybercriminals with the chance to spread their malware on any computer where the vulnerable application is found – there simply is no patch available to block the loophole.

VULNERABLE APPLICATIONS USED BY FRAUDSTERS

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



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



Source: Kaspersky Lab

Digital certificates

We are all predisposed to trust websites with a security certificate issued by a bona fide Certificate Authority (CA), or an application with a valid digital certificate.

Unfortunately, not only have cybercriminals been able to issue fake certificates for their malware – using so-called self-signed certificates, they have also been able to successfully breach the systems of various CAs and use stolen certificates to sign their code.

This effectively gives a cybercriminal the status of a trusted insider and maximizes their chances of success – clearly organizations and individuals are more likely to trust signed code.

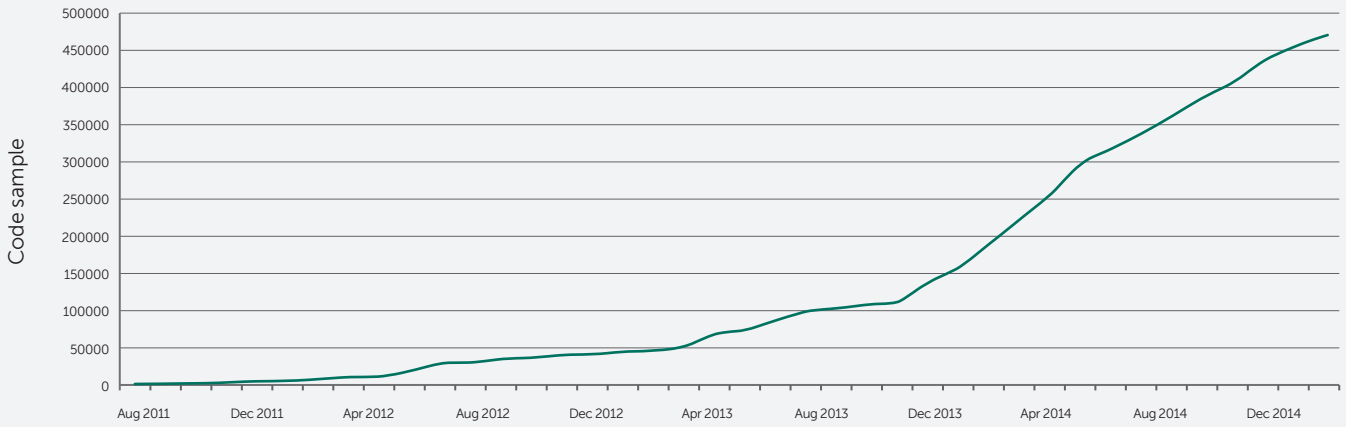
A GReAT tip: Deploy comprehensive and integrated anti-malware

Make sure you're always running the latest security software, applying updates when they are available and removing software when it becomes superfluous.

Chapter 3: The growth of mobile malware

Cybercriminals are now turning their attention to mobile devices. The first mobile threats appeared in 2004, but mobile malware didn't become a significant threat until some years after this. The tipping point came in 2011: the same number of threats was found in 2011 as had been seen in the entire period from 2004 to 2010. This explosive growth has continued since then. By the end of 2014 there were over 470,000 unique mobile malware code samples.

MOBILE MALWARE
14,643,582 installation packs



Source: Kaspersky Lab

In 2014 alone more than 295,000 samples appeared. These code samples are often reused and repackaged many times, so the number of malicious installation packs far exceeds the number of code samples: by the end of 2014, the total number of mobile malware installation packs was almost 15 million. During 2014, Kaspersky Lab blocked more than 1.3 million attacks and 19% of people using Android devices encountered at least one mobile malware threat. Notwithstanding the dramatic growth in mobile malware, many businesses remain unaware of the potential danger and, as a result, many mobile devices go unprotected.

The largest share of mobile malware is targeted at Android devices. The main reason is that Android provides an open environment for developers of apps and this has led to the creation of a large and diverse selection of apps. There is little restriction on where people can download them from, which increases people's exposure to malicious apps. By contrast, iOS is a closed, restricted file system, allowing the download and use of apps from just a single source – the App Store. This means a lower security risk: in order to distribute code, would-be malware writers have to find some way of 'sneaking' code into the App Store, or confine their attacks to 'jailbroken' iOS devices. So it's likely that, for the time being at least, Android will remain the chief focus of cybercriminals.

By the end of 2014, the total number of mobile malware installation packages was almost 15 million.

Mobile banking – the next cybercrime hotspot?

The use of smartphones for online banking is growing and it's clear that cybercriminals are turning their attention to it.

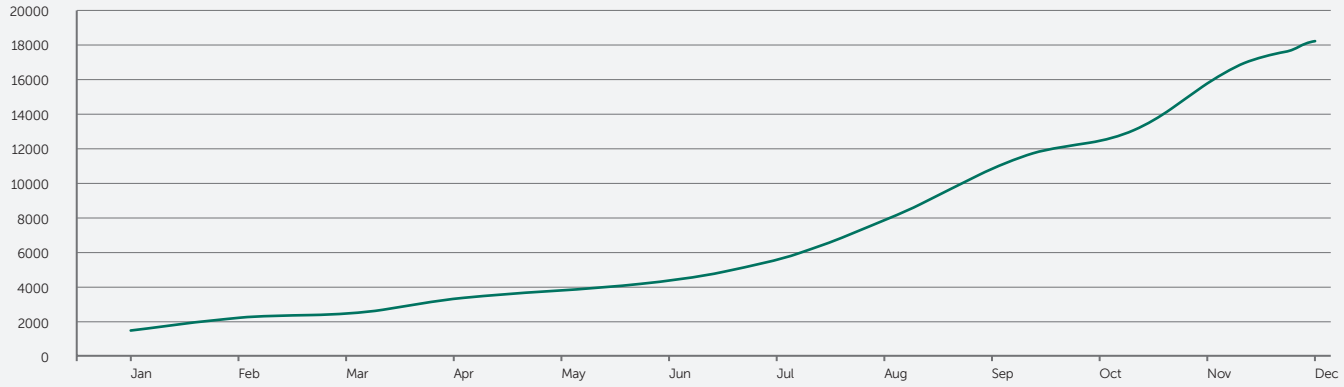
The use of mobile devices as part of two-factor authentication of banking transactions conducted on a desktop or laptop is already well established. This is where a one-time password for a transaction is sent by the bank to a customer's smartphone via SMS.

So it's no surprise that we have seen specific threats designed to capture mTANs (mobile Transaction Authentication Numbers). These are known as 'Man-in-the-Mobile' attacks and a number of specific threats have been developed for this purpose – including ZeuS-in-the-Mobile (or 'ZitMo'), 'SpyEye-in-the-Mobile' (or SpitMo) and Carberp-in-the-Mobile (or CitMo).

The number of banking Trojans increased dramatically during 2014, from less than 2,000 at the start of the year to more than 18,000 by the end of the year. Such Trojans, once aimed almost exclusively at Russian victims, are now found in many countries around the world.

MOBILE BANKING TROJANS

Dramatic growth in 2014



Source: Kaspersky Lab

A GReAT tip: Implement a 'follow-me' security policy

Make sure your security solutions are flexible and reflect changes in working practices.
This way, every employee is protected inside and outside the workplace, on whichever device they use.

Chapter 4: Are you in the firing line? A new era of targeted attacks

Attacks and targeted attacks

The threat landscape continues to be dominated by random, speculative attacks designed to steal personal information from anyone unlucky enough to fall victim to the attack. Such attacks affect not only individual consumers but also businesses. Often the aim is to use stolen credentials to gain access to financial accounts and to steal money. But it's clear that the number of targeted attacks on organizations is growing and they have become an established feature of the threat landscape.

The aim is get a foothold in a target company, steal corporate data or damage a company's reputation.

Also, we are now in an era where malicious code can be used as a cyberweapon: and while a particular organization may not be in the direct firing line it could become 'collateral damage' if it isn't adequately protected.

It's easy to read the headlines in the media and draw the conclusion that targeted attacks are a problem only for large organizations, particularly those who maintain 'critical infrastructure' systems within a country. However, any organization can become a victim. All organizations hold data that could be of value to cybercriminals; and they can also be used as a 'stepping-stone' to reach other companies.

Cyberweapons

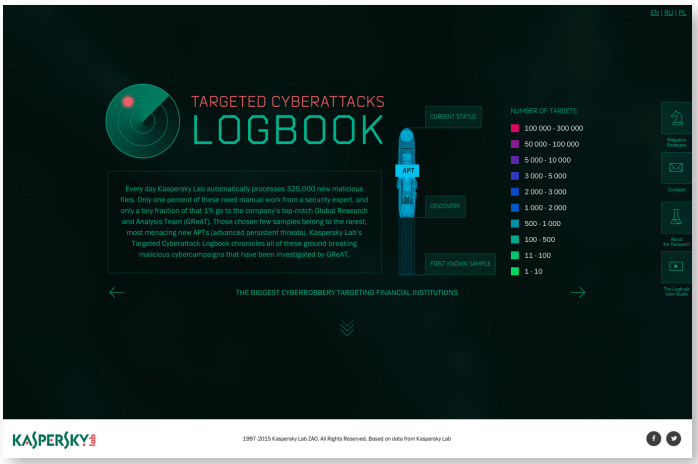
Stuxnet pioneered the use of highly sophisticated malware for targeted attacks on key production facilities. Furthermore, the appearance of other nation-state sponsored attacks – Duqu, Flame, Gauss, Careto, Regin, Equation and Duqu 2.0 – has made it clear that this type of attack is far from being an isolated incident.

We have entered an era of cold 'cyberwar', where nations have the ability to fight each other unconstrained by the limitations of real-world warfare. Looking forward we can expect more countries to develop cyberweapons – designed to steal information or sabotage systems – not least because the entry-level for developing such weapons is much lower than is the case with real-world weapons.

It's also possible that we may see 'copy-cat' attacks by non-nation states, with an increased risk of 'collateral damage' beyond the intended victim of the attack. The targets for such cyberattacks could include energy supply and transportation control facilities, financial and telecommunications systems and other 'critical infrastructure' facilities.

Targeted Cyberattacks Logbook

Kaspersky Lab's Targeted Cyberattack Logbook chronicles all of the ground-breaking malicious cybercampaigns that have been investigated by GReAT.



Visit https://apt.securelist.com/ for more information

Chapter 5: The human factor in security

The human factor

Humans are typically the weakest link in any security chain. There are several reasons for this:

- Many people are unaware of the tricks used by cybercriminals
- Successive scams never look quite the same, which makes it difficult for individuals to know what what to look out for

The problem can be worse in the case of smartphones and tablets. Their size and portability can be a great advantage, but they're also easily lost or stolen. If they fall into the wrong hands, a weak (or non-existent) PIN or passcode becomes a single point of failure – the only thing between an unauthorized person and the data stored on the device.

Equally, while it's a benefit to have staff 'always-on', it's dangerous if staff conduct confidential transactions on untrusted wi-fi networks or if they inadvertently connect to a fake hot-spot (the wi-fi network called 'coffee-shop' might be legitimate, but the one named 'coffee-shop-fast' might belong to a criminal looking to collect data from the unwary).

Sometimes people cut corners in order to make their lives easier and simply don't understand the security implications. This is true of passwords, for example. Many people use the same password for everything – often something that's as easy to remember as 'password', '123456', 'qwerty' or 'football'!

This increases the likelihood of a cybercriminal guessing the password. And if one account is compromised, it offers easy access to other accounts. Even when they are made aware of the potential danger, most individuals don't see a feasible alternative, since they think they can't possibly remember lots of unique, complex passwords.

A GReAT tip: Keep your password safe

For more information on keeping your password secure read David Emm's blog on The Huffington Post.

Social engineering

Social engineering is the manipulation of human psychology – getting someone to do what you want them to do. In the context of IT security, it means tricking someone into doing something that undermines their security, or the security of the organization they work in. Phishing emails provide a good example of social engineering. They generally take the form of spam emails sent to large numbers of people, although spear-phishing is a targeted version designed to trick victims in specific organizations. They masquerade as legitimate emails from a bona fide organization. They mimic the logo, typeface and style of the legitimate organization, in the hope that enough people who receive the email will be fooled into thinking that it's a legitimate communication. When the victim clicks on the link, they are redirected to a fake website where they are asked to disclose their personal information – such as usernames, passwords, PINs and any other information that cybercriminals can use.

The widespread use of social networks has also made it easier for cybercriminals. They are able to gather data that people post online and use it to add credibility to a phishing email.

A GReAT tip: Raise awareness

Cybercriminals are increasingly using public data to launch targeted attacks against businesses.
Tell your colleagues about the risks associated with sharing personal and business information online.

For more tips on how to spread the message with your colleagues check out the 10 top tips at the end of this guide.

Chapter 6: Anti-malware technologies

Anti-malware technologies used today
Hundreds of thousands of unique malware samples appear every day. This explosive growth in recent years has made it ever more important to block threats proactively – signatures alone are no longer enough. Some of the main anti-malware technologies used today are outlined below.

Heuristic analysis
This is used to detect new, unknown threats. It includes the use of a signature that identifies known malicious instructions, rather than a specific piece of malware. It also refers to the use of a sandbox (a secure virtual environment created in memory) to examine how the code will behave when it is executed on the real computer.

Vulnerability scanning and patch management
Since cybercriminals make extensive use of vulnerabilities in applications, it makes sense to be able to identify those applications on a system that are vulnerable to attack, allowing businesses or individuals to take remedial action with patch management. Some solutions also include a real time scan of a computer, to block the use of zero-day vulnerabilities.

Signatures
Traditionally, a characteristic sequence of bytes used to identify a particular piece of malware. But anti-malware solutions today make extensive use of generic signatures to detect large numbers of malware belonging to the same malware family.

Behavioral analysis
This involves monitoring the system in real time to see how a piece of code interacts with the computer. The more sophisticated monitors don't just look at code in isolation, but track its activities across different sessions, as well as looking at how it interacts with other processes on the computer. To protect against cryptors Kaspersky Lab uses two technologies: **System Watcher**, which is a part of proactive protection and **Application Privilege Control**, which can restrict an application's rights. For example it can prohibit applications from making changes to systems files.

Whitelisting
Historically, anti-malware solutions have been based on identifying code that is known to be malicious, i.e. 'blacklisting' programs. Whitelisting and Default Deny takes the opposite approach, blocking it if it is not in the list of acceptable programs.

Reputation services
These days, many solutions make extensive use of a cloud-based infrastructure, allowing near real-time protection from a newly-discovered threat.

In simple terms, metadata about any program run on a protected computer is uploaded to the vendor's cloud-based computers, where its overall reputation is assessed – i.e. is it known-good, known-bad, an unknown quantity, how often has it been seen, where has it been seen, etc. The system operates like a global neighborhood watch, monitoring what is being run on computers around the world and providing protection to every protected computer if something malicious is detected.

Kaspersky Security Network
Kaspersky Security Network (KSN), is Kaspersky Lab's cloud-assisted service. It provides additional value to customers, even protecting them even from, as yet, unknown threats by constantly monitoring the reputation of executed applications and accessed URLs. If the file reputation suddenly changes from 'good' to 'bad', KSN customers are informed within minutes and their corporate assets are immediately protected against them.

Evolved malware requires an evolved solution – the rise of integrated platforms

Malware continues to grow in volume and in sophistication. So for businesses today, there are more and more attack vectors to contend with.

In particular, keeping up with and controlling web usage, increasingly mobile employees (and data) and updating an increasingly complex array of applications, mean that the average under-resourced IT team often has to make compromises in its IT security.

As the environment gets more complex, the solution can be to add new technologies to manage and protect the various risk areas – but that increases the IT team's workload, cost and even risk.

This new threat landscape has led to the first ever truly integrated single security platform, developed by Kaspersky Lab. This platform is the best way to bring every technology area together – all viewed, managed and protected in one single management console.

A GReAT tip: Use proactive technology

Deploy anti-malware solutions that bring together different technologies to block known, unknown and advanced threats in real-time, rather than relying on signature-based protection alone.

The GReAT Team

The expert insight in this report is provided by Kaspersky Lab's Global Research and Analysis Team (GReAT). Since 2008 GReAT has been leading the way in anti-threat intelligence, research and innovation – within Kaspersky Lab and externally.

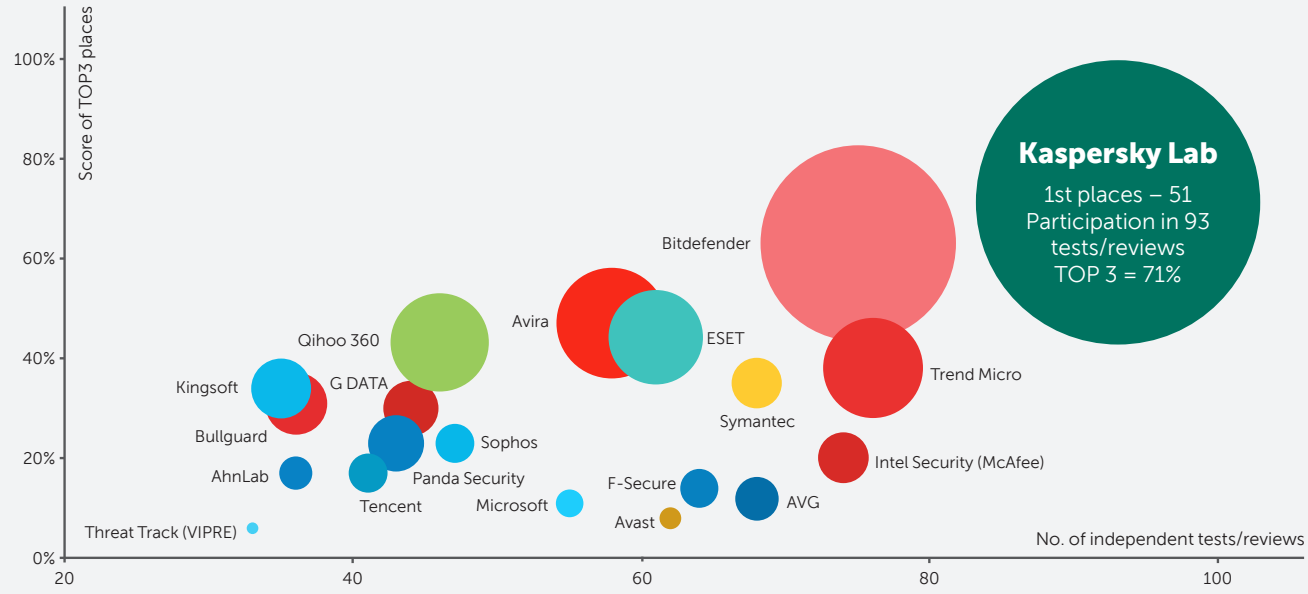
GReAT has been at the forefront of analysing some of the world's most sophisticated threats, including Stuxnet, Duqu, Flame, Red October, NetTraveler, Careto, Equation, Carbanak and Duqu 2.0. In 2013, GReAT won '**Information Security Team of the Year**' at the SC Awards.

Why Kaspersky?

Kaspersky Lab is one of the fastest-growing IT security vendors worldwide and is firmly positioned as a top-four global security company. Operating in almost 200 countries and territories worldwide, we provide protection for over 400 million users and over 270,000 corporate clients – from small and medium-sized businesses to large governmental and commercial organizations.

Our advanced, integrated security solutions give businesses an unparalleled ability to control application, web and device usage: you set the rules and our solutions help manage them. Kaspersky Endpoint Security for Business is specifically designed to combat and block today's most advanced persistent threats. Deployed in conjunction with Kaspersky Security Center, it gives security teams the administrative visibility and control they need – whatever threats they face.

In 2014 Kaspersky Lab products participated in 93 independent tests and reviews. Our products were awarded 51 firsts and received 66 top-three finishes.[5]



** Notes: According to summary results of independent tests in 2014 for corporate, consumer and mobile products.*

Summary includes tests conducted by the following independent test labs and magazines: Test labs: AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin. The size of the bubble reflects the number of 1st places achieved.

5: http://www.kaspersky.com/TOP3/

10 Top tips for creating security awareness in your organization

Creating awareness in your business about the importance of IT security can be difficult, so we've put together ten tips to help make communicating the issues of security to your business a little easier.

1
Address your audience correctly
Avoid calling anyone 'users' – it's impersonal and can leave your audience feeling a little disassociated from what you're saying. Use 'employee', 'colleague' or 'person' instead.

2
Use the right tone of voice
An approachable and friendly tone will help you communicate to your audience more effectively, ensuring you can educate your colleagues on what they can each do to protect the business.

3
Get support from the HR and legal teams
Where necessary, they can put real policies in place and provide support if it breaches are made.

4
Keep colleagues informed
Consider the timing and frequency of your IT security inductions and briefings. Ensure they are regular and memorable.

5
Use your imagination
There are lots of ways to make information more engaging. The more creative and interesting, the greater the chances it will be read. Try comic strips, posters and quizzes.

6
Review your efforts
Has your information sunk in? Test your colleagues and see what they have remembered and what they have forgotten. A quiz on the top five IT security issues is a good place to start.

7
Make it personal
Tapping into your colleagues' self-interests will help them gain a better understanding of the importance and context of IT security. For example, discuss how security breaches might affect their mobile devices.

8
Avoid jargon
Most people will not have the same depth of knowledge as you, so make sure you explain everything in a way that is easy to understand.

9
Encourage an open dialogue
Ensure people understand the consequences of a security breach; and the importance of keeping you informed. Some may fear they will be disciplined if they have clicked on a phishing email and as a result avoid notifying the correct people.

10
Consult the marketing team
When it comes to internal communications within your organization, they are the experts – so ask for their help on how to best engage your colleagues.

GET STARTED NOW
FREE 30 DAY TRIAL

Discover how our premium security can protect your business from malware and cybercrime with a no-obligation trial.

Visit **kaspersky.com/trials** today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL NOW

JOIN THE CONVERSATION

#SecureBiz

Watch us on YouTube

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

View us on SlideShare

Review our blog

Join us on Threatpost

View us on Securelist

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of IT security solutions (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

kaspersky.com/business
#SecureBiz