THE THREAT LANDSCAPE

A practical guide from the Kaspersky Lab experts

Written by David Emm
Senior Regional Researcher, Global Research & Analysis Team

ABOUT THE AUTHOR

David Emm
Senior Regional Researcher
Global Research & Analysis Team, also known as the GReAT team

David has been with Kaspersky Lab since 2004. In his role as Senior Technology Consultant David presented information on malware and other IT threats at exhibitions and events, and provided comment to both broadcast and print media. He also provided information on Kaspersky Lab products and technologies. He was promoted to his current position in 2008. David has a particular interest in the malware ecosystem, ID theft, and Kaspersky Lab technologies, and he conceived and developed the company's Malware Defence Workshop.

David has worked in the anti-virus industry since 1990 in a variety of roles. Prior to joining Kaspersky Lab David worked as Systems Engineer, Product Manager and Product Marketing Manager at McAfee; and before that as Technical Support Manager and Senior Technology Consultant at Dr Solomon's Software.

CONTENTS

CHAPTER 1

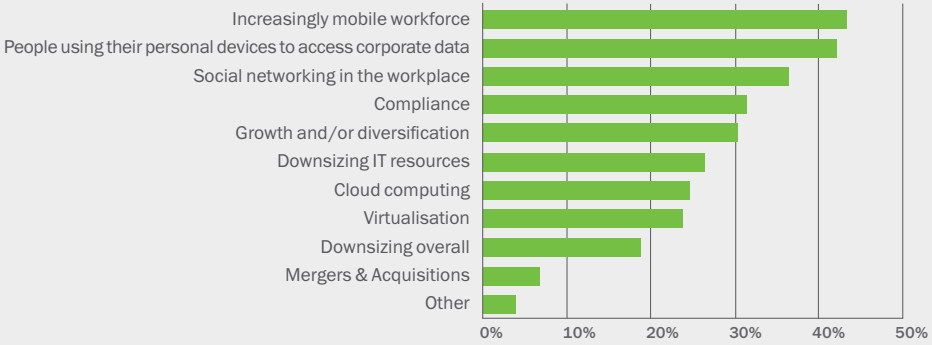
THE EVOLUTION OF MALWARE

CONTEXT

It is more than 25 years since the first PC viruses appeared. Over time, the nature of the threat has changed significantly. Today's threats faced by businesses are more complex than ever before.

In Kaspersky's 2013 Global IT Risks Survey, we found that new technology – leading to new ways of working – were of most concern to IT managers. Mobility, use of personal devices at work (BYOD) and social media in the work place were the top three concerns.

What challenges are creating the biggest security headaches for your organisation?



This paints a picture of a technology environment under significant change. The big trends we've seen that impact organisations from a security perspective are:

- **Mobility/BYOD:** ubiquitous mobility and increasing consumerisation in the business environment means a typical end-user community is now mobile.
- **Cloud:** accessing company data via the cloud from an increasing variety of devices puts strain on IT security.
- **Virtualisation:** increasing use of virtualised environments to reduce cost and increase flexibility creates specific areas of IT security complexity.
- **Social media:** employee use of social media in itself is rarely an issue, but cybercriminals are increasingly using the 'openness' of people's behaviour on these sites to gain access to valuable data.

INCREASING IN SCALE, INCREASING IN SEVERITY

The connectivity provided by the Internet means that attacks can be launched on victim's computers very quickly, as widely or selectively as malware authors, and the criminal underground that sponsor them, require.

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

The scale of the problem, in terms of numbers alone, has also continued to increase. The number of unique malware samples analysed daily now runs into hundreds of thousands.

19% of people ranked cyberthreats the number 1 current business risk

FROM CYBER-VANDALISM TO CYBERCRIME

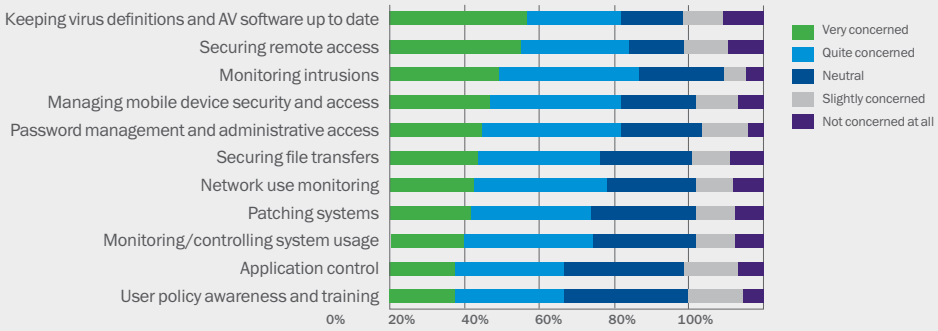
Until around 2003, viruses and other types of malware were largely isolated acts of computer vandalism – anti-social self-expression using hi-tech means. Most viruses confined themselves to infecting other disks or programmes.

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 now 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 downtime'.

This explains why in our 2013 Global IT Risks Survey the range and complexity of IT security concerns is significant and rather than facing 'one big issue' IT administrators are concerned about a range of issues.

How concerned are you about the following IT security challenges within your organisation on a day-to-day basis?



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 targeted.

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

THE RISE OF THE TROJAN

Trojans are used to harvest confidential information (username, password, PIN, etc.) for computer fraud. They can be used in DDoS (Distributed Denial of Service) attacks on organisations. Such attacks can be used to extort money from organisations: a 'demonstration' DDoS attack offers the victim a 'taster' of what will happen if they don't pay up.

There has also been a steady growth in the number of 'ransomware' Trojans, used to try to extort money from individual users. These programs encrypt the victim's data and display a message (in the form of a 'readme' file or popup) asking the victim to transfer money to the author of the programme using one of the many e-payment services.

Typically, compromised computers are combined into networks. The activities of these bot networks, or botnets, are controlled using web sites or Twitter accounts. If the botnet has a single control-and-command (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. The so-called 'Storm Worm', early in 2007, pioneered this method and it has been implemented in many botnets since then (including Conficker, Kelihos and Red October).

Until a few years ago, most epidemics involved worms that hijacked the mail system to distribute themselves proactively, harvesting additional contacts from infected machines as they spread.

Now, increasing numbers of malicious programmes are being deliberately spammed to victim machines. This allows the author(s) to control the distribution of their code to a targeted PC population, rather than letting it spread at will.

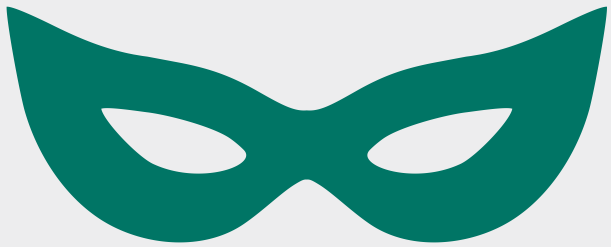
PHISHING – MASQUERADING AS SOMEONE ELSE

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 number or any other access information) and then using these details to obtain money under false pretences.

For example phishers create an almost 100% perfect replica of a chosen financial institution's web site. 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. The term rootkit is borrowed from the Unix world, where it was used to describe tools used to maintain 'root' access, while remaining invisible to the system administrator. But within the context of Windows malware, it's a stealth technique used by malware writers to 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 to be 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 BIOS). Since that time, there has been a steady stream of bootkits, including 64-bit versions.

THE TERM ROOTKIT IS BORROWED FROM THE UNIX WORLD, WHERE IT WAS USED TO DESCRIBE TOOLS USED TO MAINTAIN 'ROOT' ACCESS, WHILE REMAINING INVISIBLE TO THE SYSTEM ADMINISTRATOR.

A GReAT tip: Develop a security strategy

Your security strategy should be tailored to your business – not based on generic 'best practices' and guess estimates. 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

ARE YOU IN THE FIRING LINE?

A NEW ERA OF TARGETED ATTACKS

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. But it's clear that the number of targeted attacks 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 cyber-weapon: and while an organisation 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 organisations, particularly those who maintain 'critical infrastructure' systems within a country. However, any organisation can become a victim. All organisations hold data that could be of value to cybercriminals; and they can also be used as a 'stepping-stones' to reach other companies.

A GReAT tip: Regularly backup 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.

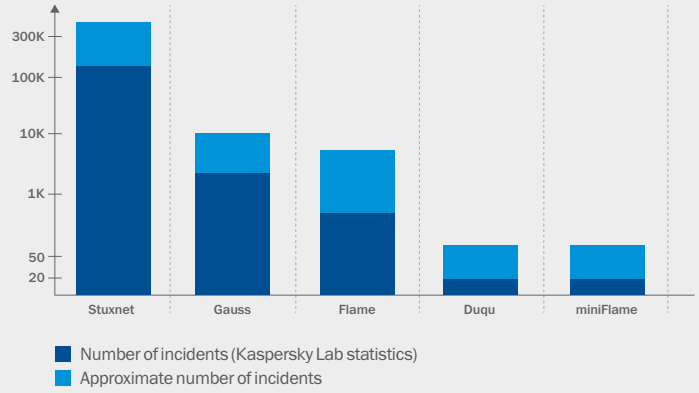
CYBER-WEAPONS

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 and Gauss – has made it clear that this type of attack was not an isolated incident.

We have entered an era of cold 'cyber-war', 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 cyber-weapons – 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 cyber-attacks could include energy supply and transportation control facilities, financial and telecommunications systems and other 'critical infrastructure' facilities.

Number of victims



CHAPTER 3

MALWARE: NOW ON THE MOVE AS MUCH AS YOU ARE

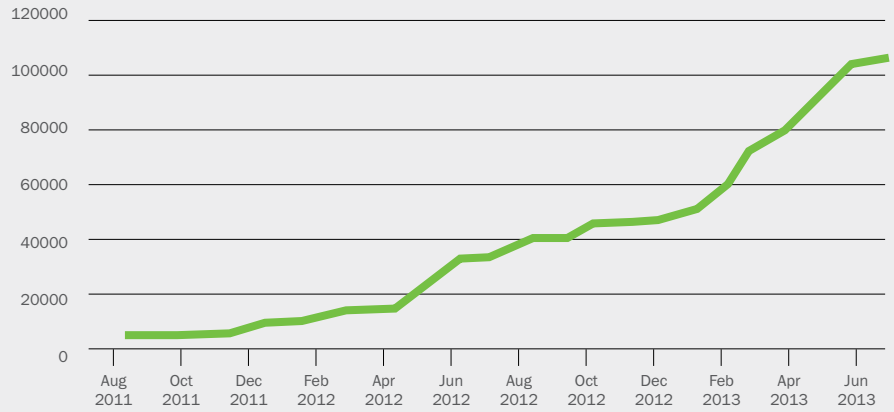
THE GROWTH OF MOBILE MALWARE

Cybercriminals are now turning their attention more and more to mobile devices.

The first threats appeared in 2004, but mobile malware didn't become a significant threat for some years. 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.

The explosive growth is still continuing to rise.

Number of unique samples



THE DEVELOPMENT OF MOBILE MALWARE

Early mobile threats targeted Symbian and, to a lesser extent, WinCE. However, malware authors soon began to develop threats using Java Mobile Edition (J2ME) – driven by the need to create cross-platform malware at a time when the smartphone market was fragmented.

By the end of 2009, around 35 per cent of threats were Java-based. By the following year, Java-based threats reached around 57 per cent, eclipsing Symbian as the main target of malware authors.

In 2012 almost 94% of threats targeted Android

In 2011 there was a massive increase in the number of threats targeting Android (64%). In 2012, almost 94 per cent of threats targeted Android.

The main reason is that Android provides an open environment for developers of 'apps' and this has led to a large and diverse selection of 'apps'. There is little restriction on where people can download 'apps' 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.

So it's likely that, for the time-being at least, Android will remain the chief focus of cybercriminals.

MOBILE BANKING – THE NEXT CYBERCRIME HOTSPOT?

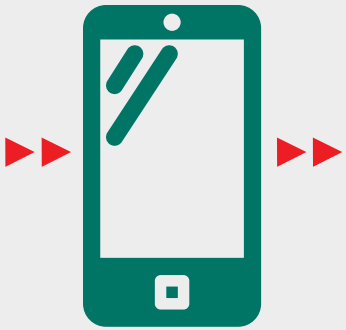
The use of smartphones for online banking is not yet well-established, so it will take time for cybercriminals to turn their full attention to this. However, the use of mobile devices as part of two-factor authentication of banking transactions conducted on a desktop or laptop is well-established.

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 three specific threats have been developed for this purpose – ZeuS-in-the-Mobile (or 'ZitMo'), 'SpyEye-in-the-Mobile' (or SpitMo) and Carberb-in-the-Mobile (or CitMo).

Cybercriminals are continually exploring different ways of making money; and this includes smartphones. The SpamSold botnet, for example, which appeared late in 2012, sends out spam SMS messages from infected devices.

To-date, most malware has been designed to get root access to the device. In the future, we are likely to see the use of vulnerabilities that target the operating system and, based on this, the development of 'drive-by downloads'.



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

HOW MALWARE SPREADS

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

DRIVE-BY DOWNLOADS

This is currently the main method used to spread malware. Cybercriminals look for insecure web sites and hide their code in one of the web pages: 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 web page.

The cybercriminals inject a malicious script into the web page, which installs malware on the victim's computer or, more typically, takes the form of an IFRAME re-direct to a site controlled by the cybercriminals. The victim becomes infected if there is an insecure, unpatched application on their computer.

CYBERCRIMINALS INJECT A MALICIOUS SCRIPT INTO THE WEB PAGE, WHICH INSTALLS MALWARE ON THE VICTIM'S COMPUTER OR, MORE TYPICALLY, TAKES THE FORM OF AN IFRAME RE-DIRECT 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 programmes)
- Third, they create fake accounts that gather 'friends', collect personal information and sell it on to advertisers

Cybercriminals cash in on the fact that people in social networks are pre-disposed to over-share information and to trust people they know.

EMAIL AND INSTANT MESSAGING

Around three per cent of emails contain malware, in the form of attachments or links. Email is also used in targeted attacks, as a way of getting an initial foothold in the target organisation(s). In this case, the email is sent to a specific person in an organisation, 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 maximise 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 organisation and the content of the email is tailored to the interests of the organisation, so that it looks legitimate.

Some 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.

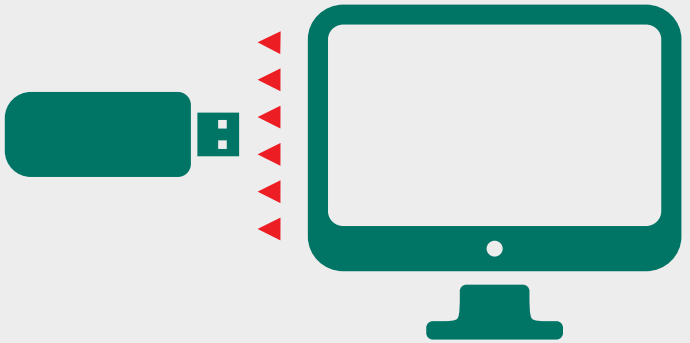
TO MAXIMISE THEIR CHANCES OF SUCCESS, CYBERCRIMINALS TYPICALLY SEND THEIR EMAIL TO PUBLIC-FACING (OFTEN NON-TECHNICAL) STAFF, SUCH AS SALES AND MARKETING MANAGERS.

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 organisation, following the initial infection.

They have also been used to help malware to 'hop' between an untrusted computer connected to the Internet and a trusted network (this method was used by Stuxnet, for example).

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.

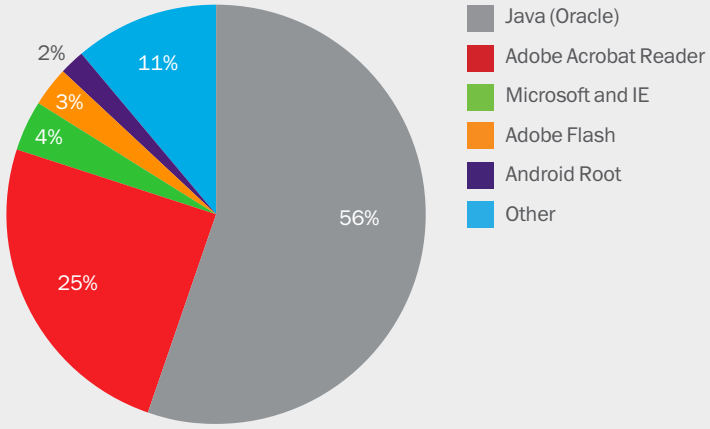
Such vulnerabilities – or bugs – can be found within an operating system. Cybercriminals typically focus their attention on applications that are widely-used and are likely to be un-patched for the longest time – giving them a sufficient window of opportunity to achieve their goals.

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.

These are known as zero-day vulnerabilities and provide cybercriminals with the chance to spread their malware on any computer where the vulnerable application is found – irrespective of whether or not the latest patch has been installed.

Most Targeted Applications



DIGITAL CERTIFICATES

We are all predisposed to trust web sites 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 maximises their chances of success – clearly organisations 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 5

THE HUMAN FACTOR IN SECURITY

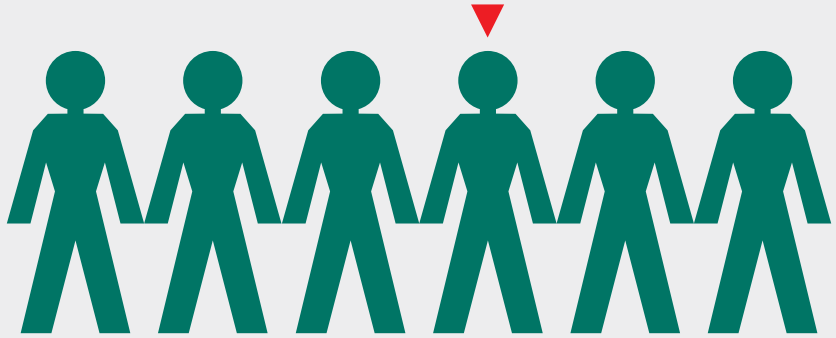
THE HUMAN FACTOR

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
- They don't know the signs to look out for
- Furthermore, successive scams never look quite the same, which makes it difficult for individuals to know what is safe and what is unsafe

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 easy to remember. Or they just used 'password'!

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 cannot possibly remember lots of unique passwords.



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 organisation 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. They masquerade as legitimate emails from a bona fide organisation. They mimic the logo, type-face and style of the legitimate organisation, 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 to a fake web site 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. The main anti-malware technologies used today are outlined below.

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.

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.

Behavioural analysis

This involves monitoring the system in real time to see how a piece of code interacts with the computer. The more sophisticated system watchers 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.

Whitelisting

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

For more information on whitelist, go to: http://whitelist.kaspersky.com/
For detailed information download: http://media.kaspersky.com/en/business-security/application-security-control-tools%20best-practices.pdf

Vulnerability scanning

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. Some solutions also include a real time scan of a computer, to block the use of zero-day vulnerabilities.

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 programme 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 neighbourhood watch, monitoring what is being run on computers around the world and providing protection to every protected computer if something malicious is detected.

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.

To find out more about integrated platforms, download:
http://media.kaspersky.com/en/business-security/10-Kaspersky-Integrated-Security-Solution-Benefits.pdf

A GReAT tip: Use proactive technology

Deploy anti-malware solutions that bring together different technologies to block new, unknown 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 and externally. GReAT has been at the forefront of detecting and eliminating some of the world's largest malware threats for over ten years, including Stuxnet, Duqu, Flame and NetTraveler. In 2013, it won 'Information Security Team of the Year' at the SC Awards.

There have been a number of GReAT tips throughout this report, designed to help you get the most from your security software.

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 300 million users and over 200,000 corporate clients – from small and medium-sized businesses to large governmental and commercial organisations.

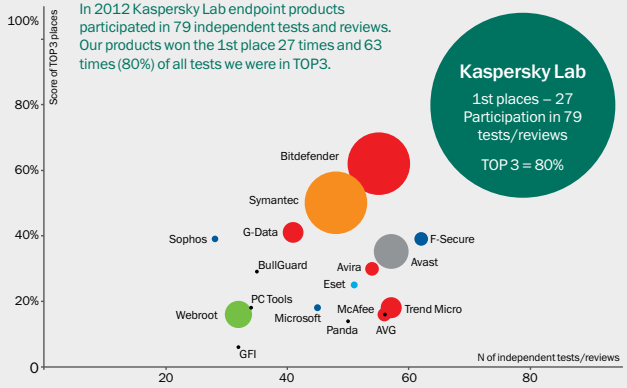
In 2012 Kaspersky Lab products participated in 79 independent tests and reviews. Our products were awarded 27 firsts and received 63 top-three finishes.

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.

For more info, go to:
www.kaspersky.com/business

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*:



*
Notes:
- According to summary result of independent test in 2012 for corporate, consumer and mobile products
- Summary includes tests conducted by the following independent test labs and magazines:
  - Test labs: AV-Test, AV-Comparatives, VB100, PC Security Labs, Matousec, Anti-Malware.ru, Dennis Technology Labs
  - Magazines: CHIP Online, PC Advisor, PC Magazine, TopTenREVIEWS, CNET, PCWorld, ComputerBild, PC-Welt
- The size of the bubble is number of 1st places

10 TOP TIPS FOR CREATING SECURITY AWARENESS IN YOUR ORGANISATION

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 with 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 5 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 organisation, they are the experts – so ask for their help on how to best engage your colleagues.

KASPERSKY lab