SPECIAL REPORT

BEWARE THE INVISIBLE CYBERCRIMINALS:

Cyberespionage and Your Business

http://usa.kaspersky.com

KASPERSKY lab

"High-profile targeted attacks on enterprises are becoming increasingly widespread. Thousands of businesses have already been hacked and had their sensitive data stolen – resulting in multi-billion dollar losses. Cyberespionage is a tangible and growing global threat today – and fighting it is one of the principal tasks we've set ourselves."

Eugene Kaspersky
CEO, KASPERSKY LAB

CONTENTS

"Many cyberattacks can be mitigated by relatively simple measures. Unfortunately, some people fail to take what appear to be basic precautions – such as using strong passwords, applying patches, and running a security solution. In many cases, breaking into a company's network is easier than it sounds."

Costin Raiu
DIRECTOR,
GLOBAL RESEARCH & ANALYSIS TEAM
KASPERSKY LAB

WHY SHOULD YOUR BUSINESS CARE ABOUT CYBERESPIONAGE?

EXECUTIVE OVERVIEW

Cyberespionage may sound like some strangely exotic activity from the movies. However, the harsh reality is that almost any business can become a target – or can be damaged in the crossfire when cybercriminals launch an attack against another organization.

It's largely immaterial whether your business is being directly targeted or just happens to suffer collateral damage as a result of getting caught up in another organization's 'battle'. Either way, the results can be devastating.

In this report, Kaspersky Lab's cybersecurity experts give you an insight into:

- How businesses can suffer from direct – and indirect cyberespionage attacks
- What you can do to protect your business... and its hard-won reputation
- How specific technologies can help defend your corporate network and data against sophisticated threats

The risks are real – and they're growing in volume and sophistication – but Kaspersky is here with sound advice ... and innovative protection technologies.

ESPIONAGE IS NOTHING NEW

Espionage, in one form or another, has existed for as long as any organization or individual has felt that it could gain an advantage by illicitly accessing someone else's confidential information. Everyone's familiar with various nation states' attempts to steal other countries' secrets. Similarly, industrial espionage has also been a feature of business life for a long time. However, recent years have seen a dramatic change in the level and nature of the espionage threats that can affect businesses of all sizes.

> The ease with which cyberespionage campaigns can be implemented is now enticing more organizations into running their own spying activities – even though many of these organizations would never have considered undertaking old-fashioned industrial espionage.

SO WHAT'S CHANGED?

As the Internet-enabled age gathered pace and greater connectivity and improved mobile communications became possible, businesses were quick to recognize the benefits of giving their employees, customers, and suppliers 'anywhere, anytime access' to business systems and essential data. The efficiency and productivity benefits have been considerable – even 'game changing' for many businesses, as the Internet has helped them to open up new sales channels and generate additional revenues.

However, that same 'always-on connectivity' – to business information and other sensitive data – has also created opportunities for cybercriminals. With businesses storing intellectual property and confidential information within networked systems, spying operations are much easier to implement and can be much more rewarding for the perpetrators.

SIMPLIFIED SPYING... WITH MORE IMMEDIATE REWARDS

Gone are the days of having to break into office premises or patiently wait for 'insider contacts' to gather information and pass on secrets. Rummaging through a company's wastepaper bins or paying office staff to collect data was always inefficient, time-consuming, and risky. Now, it's simply unnecessary. With the right computer hacking skills, individuals and organizations can spy on companies and obtain valuable information – without ever having to leave the comfort of their office.

Businesses can be attacked via insecurities in their own website, through vulnerabilities in popular business software that they're running or as a result of their employees clicking on malware-infected emails.

CYBERATTACKS HAVE A SEVERE IMPACT ON A BUSINESS'S 'BOTTOM LINE'

AVERAGE LOSSES IN THE EVENT OF A TARGETED CYBERATTACK:

$2.4 MILLION

Source: Global Corporate IT Security Risks 2013, B2B International

WHEN BUSINESSES LOSE DATA... ... THEY OFTEN LOSE MUCH MORE

AVERAGE COST OF A DATA LOSS INCIDENT FOR A LARGE ENTERPRISE:

$649,000

Source: Global Corporate IT Security Risks 2013, B2B International

WHAT DO THE PERPETRATORS GAIN FROM CYBERESPIONAGE?

DIFFERENT TYPES OF ATTACKERS HAVE DIFFERENT OBJECTIVES:

- Cybercriminals readily understand the value of corporate information. There are opportunities to gain from extortion and ransom campaigns – as well as selling stolen data on the black market.

- Hacktivists focus on causing reputation damage and disruption to organizations that the hacktivists have issues with. They realize that a leak of confidential information – about customers, suppliers or employees – could lead to severe embarrassment and/or significant legal penalties.

- Cybermercenaries seek payment from anyone who will hire them – including governments, protest groups, or businesses – to steal specific information.

- Nation states (government agencies) – or their contractors – focus on collecting strategic information or disrupting industrial facilities in hostile countries.

"Information is power – so, when a cybercriminal steals information, the theft can neutralize any advantage enjoyed by the original owner of the data. This applies whether the target is a nation state – holding military secrets – or a business with intellectual property and commercial secrets that give them a competitive advantage."

Sergey Lozhkin
Security Researcher
Global Research & Analysis Team
KASPERSKY LAB

IS ANY BUSINESS SAFE FROM CYBERESPIONAGE?

The simple answer is no. Even the smallest businesses can be directly targeted for the sensitive or valuable information they hold – from customer banking details, to supplier information or even data that can be used to help stage an attack on a larger enterprise.

For example, 'supply chain attacks' – such as IceFog (see Appendix I) – collect information from various third-party bodies/suppliers and then use that data to develop and enable targeted attacks against specific businesses or organizations.

"When you're assessing the risks to your business, never underestimate how the 'human element' can weaken your defenses. If employees fall for spearphishing campaigns or click on an 'infected' link in an email, your security could be at risk."

Sergey Lozhkin
Security Researcher
Global Research & Analysis Team
KASPERSKY LAB

"It doesn't matter if you're talking about a Fortune 500 Company, or a two-person start-up operating in someone's parents garage. Everyone has something to lose."

Charles Kolodgy
Research Vice President
Secure Products
IDC

IS YOUR BUSINESS A PRIME TARGET?

It is easy to understand why government organizations and military agencies are subjected to cyberespionage attacks. Apart from state-sponsored initiatives, independent protest groups often attempt to disrupt government operations or steal sensitive information.Cybermercenaries also target government bodies – to fulfill their employers' objectives for stealing money or data.

Similarly, because they hold a wealth of valuable information – and have hard-won business reputations that they need to protect – large enterprises and multinational corporations are also obvious targets for a vast array of different types of cyberattack, including cyberespionage.

GOOGLE, ADOBE AND OTHERS ATTACKED

Described as a watershed moment in cybersecurity, the Operation Aurora attack hit Google, Adobe, and over 30 other high profile companies in 2009.

Despite efforts to address the software vulnerabilities that were exploited by the attackers, in 2012 it was revealed that the exploit continued to target defense contractors and the supply chains of third-party companies.

The attackers seek to gain control over corporate systems and steal sensitive data. Insecure websites and email phishing strategies are at the heart of what is widely believed to be a state-sponsored cyberespionage attack.

ATTACKS AGAINST AMERICAN EXPRESS AND JP MORGAN CHASE

In 2013, both American Express and JP Morgan Chase became the victims of cyberattacks that were claimed to have been launched by a religious group. However, US intelligence and security experts believe that Iran was responsible for the attacks.

The attacks took both companies offline for several hours.

Over a six-week period at the beginning of 2013, 15 of the US's largest banks suffered a total of 249 hours offline as a result of cyberattacks.

EVERY BUSINESS CAN BE A TARGET

Medium-size and small businesses need to be aware that they are also at risk. It's all too easy for medium/small businesses to dismiss the potential threats of cyberespionage and cyberterrorism – and mistakenly believe the risks only apply to nation states and large multinationals. This false sense of security can result in businesses taking an overly relaxed attitude to protecting their systems and data – and that can make it even easier for cyberspies to launch their attacks.

Furthermore, cybercriminals often view medium/small companies as an entry point for attacks against larger businesses. Many smaller businesses enjoy 'trusted partner' status with high profile enterprises – and criminals are increasingly keen to exploit those relationships.

COULD YOUR BUSINESS BE A 'STEPPING STONE' FOR ATTACKS ON OTHER ORGANIZATIONS?

Government agencies, defense departments, critical infrastructure owners – including power generators, gas suppliers, energy distribution grids and water suppliers, plus large companies in virtually every market sector, all recognize that they can be the prime targets for cyberattacks.

So, all of these organizations are likely to have invested in robust cybersecurity measures.

By contrast, many of the companies that work with these organizations – as suppliers or contractors – may not have a sufficiently good understanding of the modern threat landscape, or what's required to ensure they keep ahead of the cyberattackers. This obviously creates opportunities for attackers to gain access to their prime target – via security vulnerabilities within a smaller supplier's or contractor's systems.

Any business, including:

- Service providers
- Hardware suppliers
- Outsourced services companies
- Small or 'one-person' consultancies
- Temporary employees/contractors

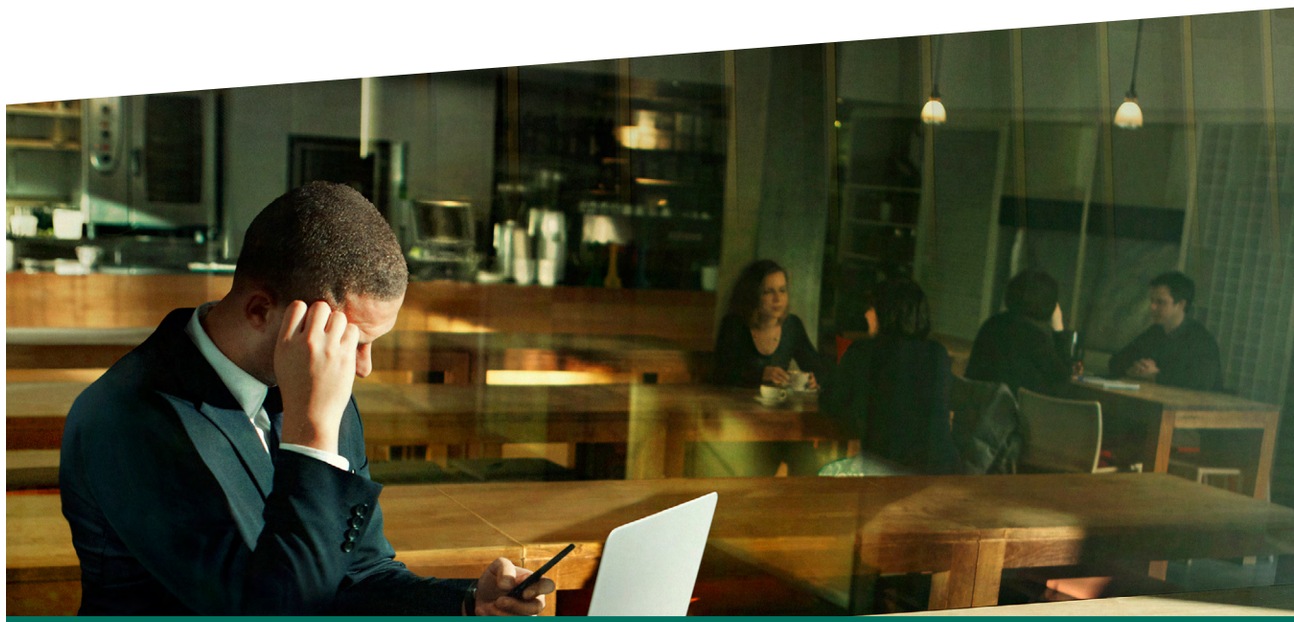
... can be used as the first stage in an attack against a multinational or a public sector organization.

ATTACKS ON SUPPLIERS HELP TO ENABLE TARGETED ATTACK AGAINST LARGE USA MANUFACTURER

In 2011, US defense company – Lockheed Martin – was subject to a significant cyberattack.

The perpetrator had previously attacked two of Lockheed Martin's suppliers, including RSA – a security company. The information gathered from these two attacks is believed to have helped the perpetrator to launch their attack against Lockheed Martin.

Lockheed Martin swiftly detected the attack and protected their systems and data. However, the attack demonstrates how third-party companies can be used as stepping stones in attempts to compromise the security of larger enterprises.



"Recently, the attackers have found it increasingly difficult to break into big companies' networks. Instead, they are focusing on the supply chain. By hacking into smaller companies' networks, the attackers leverage the small companies' knowledge and identities to break into bigger enterprises."

Costin Raiu
Director, Global Research & Analysis Team
KASPERSKY LAB

LOSING YOUR REPUTATION

Of course, if your business is merely used as a vehicle for attacking another organization, you may not suffer any direct damage. However, the potential for indirect damage is considerable. It's worth considering the possible consequences if your business is used as the 'weak link' that enables a cyberespionage attack against one of your customers or partners:

- How would it affect your ongoing relationship with the customer/partner?
- Could there be legal consequences for your business?
- How would any adverse publicity affect your reputation in your market?
- Would you be able to prove that you had taken all possible precautions against the attack?

Clearly, it's best to do everything you can to avoid the embarrassment and loss of reputation that an indirect attack could bring.

"Building a strong business reputation demands tenacity and consistency over an extended period. Losing a hard-earned reputation can take just a few moments."

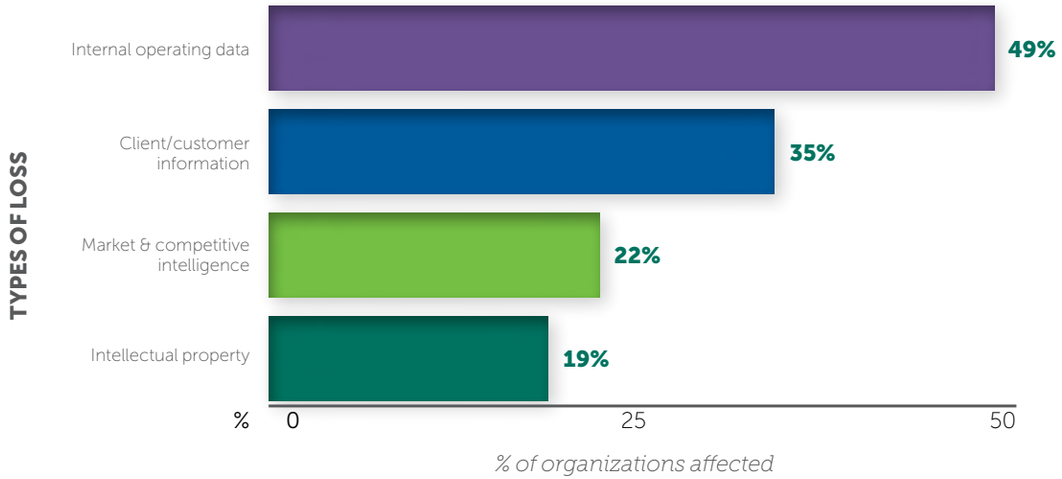
David Emm
Senior Regional Researcher
Global Research & Analysis Team
KASPERSKY LAB

DIRECT LOSS OF VALUABLE INFORMATION

It's also worth assessing what type of information could be at risk if your business does become the main target of a cyberespionage attack. How would it affect your business if any of the following data was stolen:

- Market intelligence – including 'inside information' about your strengths, weaknesses, and competitive position?
- Product designs, details about innovative processes, know-how, and other intellectual property?
- Personal information about your employees?
- Customer databases and confidential information about customers/clients?
- Information about your partners or sensitive partner information?

A RECENT SURVEY REVEALED ORGANIZATIONS AFFECTED BY DATA LEAKS EXPERIENCED THE FOLLOWING LOSSES:



Source: Global Corporate IT Security Risks 2013, B2B International

METHODS OF SPREADING CYBERESPIONAGE MALWARE

In order to distribute cyberespionage programs, cybercriminals use many of the same methods that they employ to spread other forms of malware – including:

- Exploitation of vulnerabilities within operating systems or applications – including some of the most commonly used software products, such as:
  - Java ®
  - Adobe Reader ®
  - Microsoft Office ®
  - Internet Explorer ®
  - Adobe Flash ®... and more
- Social engineering techniques – including spearphishing campaigns
- Drive-by downloads – whereby merely visiting a security compromised website can result in a user's machine becoming infected

THE BOOMERANG EFFECT

After a new cyberespionage program has been detected and identified, you could be forgiven for thinking that the world becomes a safer place. Sadly, you'd be wrong! The risks can increase – and the attack's nasty effects can even boomerang back on the perpetrators that initially launched the threat.

In some cases, attack methods have been copied by other cybercriminals and new attacks have been launched against the original attacker.

"Our understanding of cyberattacks has changed during recent years. What appeared to be isolated incidents – for example Stuxnet and Duqu – were just the tip of the iceberg. In reality, there are hundreds – if not thousands – of attacks ongoing at every single moment... even if only a few are identified."

Costin Raiu
Director, Global Research & Analysis Team
KASPERSKY LAB

BEYOND CYBERESPIONAGE... CYBERWARFARE AND THE RISK OF 'COLLATERAL DAMAGE'

Acts of cyberwarfare – whereby a nation state launches cyberattacks against another country – are on the increase, and they can also have consequences for businesses.

In conventional wars, collateral damage is the euphemistic term used to refer to non-targeted infrastructure and civilians that suffer as a result of military operations. In the world of cyberwarfare, innocent businesses and individuals can become part of the collateral damage that results from an attack against another target.

Once a cyberwarfare attack – against a nation state – has been launched on the Internet, it could have many uncontrolled or undesirable consequences that stretch far beyond the initially intended target. Nation states, military forces, and your business are all using the Internet – so, if a cyberwarfare attack is launched, it's possible that innocent businesses will get caught up in the attack... and suffer malware infections on their corporate IT networks.

So, when it comes to the possibility of collateral damage, if any of your systems are connected to the Internet, they are at risk. It's that simple.

Furthermore, in the case of an attack against a nation's critical infrastructure – even if your business's own corporate systems are not directly affected – you could still suffer as a result of:

- Loss of access to cloud-based services and data storage
- Inability to process online financial transactions – including paying suppliers and employees or enabling customers to place orders
- Supply chain issues – including late shipments and delays in the processing of imports/exports
- Failure of telecoms systems – including communications via VoIP or LAN lines
- Failure of other parts of a country's critical infrastructure – such as power generation/distribution
- Loss of data that's required for compliance activities

HOW CAN YOU PROTECT YOUR BUSINESS AGAINST CYBERESPIONAGE?

Even though some of the attacks may sound like something out of a science fiction novel, unfortunately... they aren't. They are today's reality – and you need to guard against them.

"Cybercriminals are keen to learn new techniques that can make their own attacks more effective. They'll devote significant effort to reverse engineering the most sophisticated attacks – even those developed by nation states.

Once the 'genie is out of the bottle' – and new malware methods are 'in the wild' – your only hope is that your security vendor is at the top of their game."

Sergey Lozhkin
Security Researcher
Global Research & Analysis Team
KASPERSKY LAB

EVALUATE THE RISKS... AND ESTABLISH A SECURITY POLICY

It's important that all businesses assess the risks that could apply to their business – and then establish their own security policy.

Many businesses fall into the trap of basing their security strategy on an out-of-date perception of the risks that existed 10 years ago. So make sure your policy is relevant to today's threats and that it builds on a sound understanding of the current threat landscape. Your policy should:

- Define day-to-day security procedures
- Establish an 'attack response' plan
- Include a mechanism for updating procedures – so they keep up with the evolving nature of the threats
- Set out a routine for regularly performing audits of your IT security provisions

EDUCATE YOUR PERSONNEL ABOUT THE RISKS

This is a key requirement. Many cyberespionage and other cybercrime attacks rely on human error or naiveté to create the conditions that give the cybercriminals access to corporate systems and data. When it comes to defending against attacks – 'forewarned is forearmed'. So make sure you raise awareness of:

- The security risks and how cybercriminals may try to steal information and passwords
- The potential costs to the business if it's attacked
- Simple precautions that employees can take in order to improve security
- Your company's security policy – and what employees need to do to meet its requirements

CONSIDER YOUR OPERATING SYSTEM STRATEGY

Bear in mind that recent operating systems – such as Windows® 7, Windows 8 or Mac OS® X – tend to be more secure than their previous counterparts. So it's worth considering this when devising your IT upgrade strategy.

Similarly, 64-bit versions of most computer operating systems tend to be more resilient against cyberattacks.

DEPLOY A COMPREHENSIVE IT SECURITY SOLUTION

Anti-malware protection is vitally important, but – on its own – it's not enough. Choose a security solution that also includes the following security technologies:

- Vulnerability assessment
- Patch management
- Application controls – that also include whitelisting and default deny functionality
- Device controls – that help you to manage which devices are allowed to be connected to your systems/ network
- Web controls – that make it easy to manage, restrict, and audit access to web resources
- Zero day defences
- Anti-malware that combines signature-based protection plus advanced proactive technologies
- Real-time protection – by using the power of the cloud to deliver a faster response to new malware
- Data encryption
- Mobile security with mobile device management (MDM)

"One of the new trends we have observed is the emergence of destructive malware. One such example is Shamoon – which was used to attack Saudi Aramco and Rasgas, in 2012. Destructive malware focuses on wide damage to the victim's network, disabling their operation temporarily or causing irreparable damage. This is a totally different mind-set from financially motivated attacks, such as banking Trojans – and perhaps it's even more dangerous."

Sergey Lozhkin
Security Researcher- Global Research & Analysis Team
KASPERSKY LAB

THE IMPORTANCE OF MOBILE SECURITY

Today's smartphones are much more than just phones. They are powerful computers that can store a lot of corporate information – and passwords – that could be valuable to cyberspies. So it's important to protect mobile devices – including tablets and smartphones – just as rigorously as you protect your IT systems.

With the increased risk of theft or loss, you could argue that mobile devices actually require even greater levels of protection – in order to secure data on missing devices.

If your business has implemented a Bring Your Own Device (BYOD) strategy, that can add to your mobile security burdens. With an almost limitless range of platforms and models to protect, make sure your security policy takes this into account.

Even if you don't operate a formal BYOD policy, you need to be aware that employees are still likely to bring in their personal smartphones.

SECURE YOUR VIRTUAL ENVIRONMENTS

Some businesses hold onto the mistaken belief that virtualized IT environments are much more secure. This isn't the case. Because virtual machines are running on physical servers, those physical servers are still vulnerable to malware attacks.

Clearly, virtual machines need to be protected. However, in order to improve your return on investment, it's worth considering security solutions that include special provisions for virtual environments. For example, by choosing an agentless security solution – as opposed to a traditional, agent-based security package – you're likely to be able to boost your server consolidation ratios.

COMBINE SECURITY WITH SYSTEMS MANAGEMENT – FOR GREATER VISIBILITY AND LESS COMPLEXITY

Consider a solution that combines security and a wide range of general IT systems management functions. This can help you to gain greater visibility of your network – and, if you can see everything on your network, it will be easier to apply the appropriate security measures.

APPLICATION CONTROL – WITH DEFAULT DENY

Default Deny provides an easy way to manage which applications are permitted to launch on your systems.

Only software that is included on your whitelist of safe applications will be allowed to launch – and all other software will be automatically blocked.

"Virtualization is all about getting more out of your IT infrastructure. If you're running conventional anti-malware software on your virtualized servers, you could be wasting a lot of server processing power and storage capacity.

That could defeat the object of your virtualization program – and significantly reduce your return on investment."

David Emm
SeniorRegional Researcher
Global Research & Analysis Team
KASPERSKY LAB

HOW KASPERSKY LAB SECURITY TECHNOLOGIES CAN HELP PROTECT YOUR BUSINESS

With cybercriminals using increasingly sophisticated methods to launch cyberattacks, it's vital that businesses choose a security solution that is capable of keeping up with the very latest threats.

INNOVATIVE TECHNOLOGIES THAT GIVE YOU MULTI-LAYERED DEFENSES

In addition to the company's award-winning anti-malware capabilities, Kaspersky continues to develop innovative technologies that add further layers of protection for businesses:

Automatic vulnerability scanning and patch management

Many of Kaspersky's security solutions can automatically scan your corporate network to detect the presence of unpatched vulnerabilities within operating systems or applications.

Working with the Microsoft WSUS database, the Secunia Vulnerability Database, and Kaspersky's own unique database of vulnerabilities (delivered via the cloud-enabled Kaspersky Security Network), Kaspersky solutions can regularly synchronize data on Microsoft hotfixes and updates – and then automatically distribute them across your network. In addition, for many non-Microsoft applications, information about patches can be downloaded directly from Kaspersky's servers.

Automatic Exploit Prevention (AEP)

Kaspersky's Automatic Exploit Prevention technology guards against malware infections that can arise from unpatched vulnerabilities within the operating systems – or applications – running on your computers.

Kaspersky Security Network

Millions of members of Kaspersky's global user community have volunteered to provide the cloud-based Kaspersky Security Network (KSN) with data about suspicious activities and attempted malware infections that occur on their computers. Even if you don't opt in to provide data to KSN, your business will still benefit from this real-time inflow of threat data from the field.

KSN helps to deliver a much more rapid response to new threats. In addition, it can also reduce the incidence of 'false positives' – to help your business to boost productivity.

Application Control

Kaspersky's Application Control capabilities help you to manage how applications run on your corporate network. It's easy to set up a Default Allow policy – that blocks the launch of blacklisted applications but lets all other software run – or to apply a Default Deny policy that only allows whitelisted applications to launch.

Whitelisting Lab

Kaspersky is the only security vendor that has invested in establishing its own Whitelisting Lab. The lab is responsible for assessing the security of commonly used applications and it continually issues updates for Kaspersky's whitelist database of applications that are safe to run.

The whitelist updates are delivered from the cloud-enabled Kaspersky Security Network, to ensure Kaspersky customers benefit from the latest whitelisting data.

ZetaShield

Kaspersky's ZetaShield (Zero Day Exploit and Targeted Attack Shield) technology provides protection against unknown malware and exploits – to defend against zero day and zero hour attacks, plus advanced persistent threats (APTs). The combination of Kaspersky's powerful antivirus engine and innovative ZetaShield technology significantly boosts the malware detection rate – for an even higher level of protection.

Mobile security and MDM

Kaspersky's mobile security technologies deliver multi-layered security for mobile devices – including special features to protect data on lost or stolen devices. In addition, Kaspersky provides an array of mobile device management (MDM) functionality that helps businesses to minimize the time they need to spend on managing mobile endpoints.

Security for virtualized environments

Kaspersky offers protection that has been specially developed to meet the unique requirements of virtualized IT environments – including virtualized servers, desktops, and data centers.

By delivering an agentless anti-malware solution, Kaspersky provides a more efficient way to protect virtualized infrastructure – in order to preserve performance, minimize impact on virtualization density and increase overall return on investment.

Far-reaching systems management capabilities

By automating a vast range of regular IT administration tasks, Kaspersky Systems Management gives businesses improved visibility and control of their IT assets – while also freeing up time for IT administrators to work on other tasks.

A WORLD-AUTHORITY ON CYBERSECURITY

As a private company, Kaspersky is totally independent. Although Kaspersky advises many government agencies, it has no political ties to any governments. Kaspersky experts work closely with the global IT security community – including Computer Emergency Response Teams (CERTs) worldwide – and undertake joint investigations of cyberespionage, cybersabotage, and cyberwarfare threats.

Get GReAT on your side

The Global Research & Analysis Team (GReAT) is one of Kaspersky's most important technological assets. With industry-leading security researchers around the globe, GReAT is constantly anlyzing new cyberthreats and developing protection.

"Established in 2008, Kaspersky Lab's Global Research & Analysis Team (GReAT) provides company leadership in anti-malware and cyberespionage research and innovation – both internally and externally. The team's security analysts are based around the world – with each analyst contributing a unique set of skills and expertise to the research and design of solutions to combat increasingly complex malware code.

GReAT conducts incident response during malware-related scenarios. Key responsibilities include thought leadership in threat intelligence, driving and executing initiatives around improving malware detection accuracy rates and efficiency, as well as pre- and post-sales support of key customer accounts with regard to malware intelligence expertise.

Over the last few years, GReAT's combination of expertise, passion, and curiosity led to the discovery of several cyberespionage campaigns, including Flame, Gauss, Red October, NetTraveler, and Icefog."

Costin Raiu
Director, Global Research & Analysis Team
KASPERSKY LAB

"With the rise of advanced persistent threats (APTs), the global cyberthreat landscape has been transformed – putting critical infrastructure, finance, telecommunications, research institutes, military contractors, and government cybernetwork infrastructure at huge risk.

These threats are much more complex and stealthy than the average malware. That's why we continue to invest in GReAT – as a cutting-edge, elite group of cybersecurity experts."

Eugene Kaspersky
CEO
KASPERSKY LAB

COSTIN RAIU
DIRECTOR, GLOBAL RESEARCH & ANALYSIS TEAM
KASPERSKY LAB

Costin Raiu joined Kaspersky in 2000 and has led GReAT since 2010. He specializes in analyzing advanced persistent threats and high-level malware attacks. Costin's work includes analyzing malicious websites, exploits, and online banking malware.

With over 19 years of experience in antivirus technologies and security research, Costin is a member of the Virus Bulletin Technical Advisory Board, a member of the Computer Antivirus Researchers' Organization (CARO), and a reporter for the WildList Organization International. Prior to joining Kaspersky Lab, Costin worked for GeCad as Chief Researcher and as a Data Security Expert with the RAV antivirus developers group.

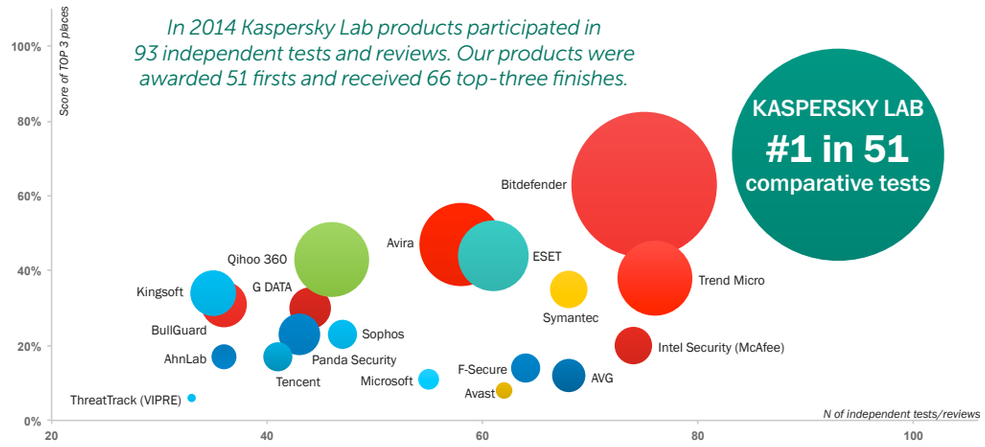
INDEPENDENT AWARDS AND ACHIEVEMENTS

Kaspersky is understandably proud of the number of awards and accolades that have been bestowed upon its technologies:

- 'Information Security Vendor of the Year' award – SC Magazine Awards Europe 2013
- 'Information Security Team of the Year' award – SC Magazine Awards Europe 2013
- Excellence Award winner – SC Magazine Awards 2013
- Kaspersky Endpoint Security for Windows was awarded highest prize in Enterprise Antivirus Protection April – June 2013 test by Dennis Technology Labs
- The greatest number of gold and platinum awards – across all testing categories – from the third-party Anti-Malware Test Lab, since 2004
- More than 50 pass scores on the rigorous VB100 testing regimen, since 2000
- The Checkmark Platinum Product Award from West Coast Labs
- Product of the year – AV Comparatives 2011

KASPERSKY LAB PROVIDES BEST IN THE INDUSTRY PROTECTION*:

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



** 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.

APPENDIX 1

AN OVERVIEW OF SOME SIGNIFICANT CYBERTHREATS

CYBERESPIONAGE THREATS

Icefog

This is an advanced persistent threat (APT) that started in 2011 and has been targeting industrial businesses as well as government institutions, and military contractors. Most of the targets are in Japan or South Korea – but are causing supply chain issues for global companies. The attackers appear to be targeting telecoms operators, satellite operators, mass media, and television services – as well as military, shipbuilding/maritime operations, computer and software development, plus research companies.

Typically, spearphishing emails are used to deliver malware that exploits vulnerabilities within commonly used applications – such as Java and Microsoft Office. Even though the vulnerabilities are well known and patches are readily available, the cybercriminals are relying on the fact that many victims can be slow to distribute patches across their IT infrastructure. It is believed that the attackers are cybermercenaries that are paid to launch attacks.

Kimsuky

A group of North Korean hackers is suspected of launching the Kimsuky cyberespionage campaign in order to steal defense and security data from South Korean targets. Kaspersky Lab researchers discovered the campaign that uses spearphishing techniques to steal users' passwords and other information. The hackers also take control of the infected computers.

Red October

Dating back as far as 2007, Operation Red October continued to be active into 2013. This advanced cyberespionage campaign targets diplomatic and government institutions across the world. It has also targeted research institutions, oil and gas companies, plus other commercial organizations. Red October steals data from computer systems, mobile phones, and enterprise networks. The attacks include exploits that use security vulnerabilities within Microsoft Office and Microsoft Excel ®.

NetTraveler

This is a cyberespionage campaign that has successfully compromised more than 350 high profile victims -in 40 countries. The main tool used by the cybercriminals during these attacks is NetTraveler, a malicious program used for covert computer surveillance. It is designed to steal sensitive data, log keystrokes, and retrieve file system listings and various Office or PDF documents.

NetTraveler has been active since 2004 and has targeted Tibetan/ Uyghur activists, oil industry companies, scientific research centres and institutes, universities, private companies, governments and government institutions, embassies, and military contractors.

Shamoon

When a computer becomes infected with Shamoon, the virus can exploit the presence of shared hard drives in order to spread to other computers on the target organization's network. In addition to sending data to the perpetrator of the attack, Shamoon also deletes files on the victim's computers.

DATA WIPED FROM MAJOR OIL PRODUCER'S COMPUTERS

A Shamoon attack is believed to have destroyed data on 30,000 of Saudi Aramco's computers.

Regardless of whether your company has 10 or 10,000 computers... if they all suffered data loss, could your business recover?

APPENDIX 1

THREATS THAT ARE BELIEVED TO BE SUPPORTED BY NATION STATES – INCLUDING CYBERWARFARE, CYBERSABOTAGE AND CYBERESPIONAGE

Stuxnet (approximate number of victims: over 300,000)

Often regarded as an example of cyberwarfare, Stuxnet was the first malicious program that targeted industrial control systems. The objective behind Stuxnet was to disrupt and sabotage operations at a nuclear facility – by taking control of the operation of uranium enrichment centrifuges. To date, it is the only malware item that is known to have caused physical damage to industrial systems.

However, despite its original objective, Stuxnet propagated in a way that was unstable and led to the infection of hundreds of thousands of PCs at thousands of different organizations.

Duqu (approximate number of victims: 50 – 60)

This sophisticated Trojan has been active since 2007. It was built from the same attack platform as Stuxnet. After Duqu has infected a computer, it downloads additional components in order to steal sensitive information. It also has the ability to destroy all traces of its own activity.

Flame (approximate number of victims: 5,000 – 6,000)

Flame intercepts Microsoft Windows® update requests and substitutes them with its own malware module. The module includes a fake Microsoft certificate that has been generated by cybercriminals.

Active since 2008, Flame can analyze its victim's network traffic, capture screenshots from their computers, record voice communications, and log users' keystrokes.

Gauss (approximate number of victims: 10,000)

Implemented by the same groupthat created the Flame platform, Gauss is a cyberespionage program that has been active since 2011. It includes modules that can perform a variety of malicious acts, including:

- Intercepting cookie files and passwords in the victim's web browser
- Infecting USB storage devices – to steal data
- Intercepting account data for email systems and social networking websites

Gauss has been used to gain access to banking systems in the Middle East.

STUXNET INFECTS OIL GIANT

In October 2012, Chevron – a global giant in the oil industry – was the first US-based business to report that it had been infected by Stuxnet.

A CYBERGLOSSARY

Cyberattack – an attack carried out by a hacker or criminal against a computer, smartphone, tablet or IT network.

Cybercrime – refers to a vast array of illegal activities that are implemented via IT systems, including mobile devices.

Cybercriminal – an individual that undertakes criminal activities via IT systems and/or mobile devices. Cybercriminals can range from individual, opportunistic criminals, through to highly-skilled and professional groups of computer hackers. Cybercriminals may specialize in:

- Developing malware and selling it to others that go on to launch attacks
- Harvesting data – such as credit card numbers – and selling it to other criminals or may undertake every stage of an attack, from developing the malware to stealing money from the victim.

Cyberespionage – the act of spying and illicitly accessing information via IT systems and/or the Internet.

Cyberhooligan – an individual that develops malware and launches attacks for fun. Prevalent during the 1980s and 1990s, cyberhooligans are no longer common. Instead, cybercriminals and cyberterrorists are a much more significant threat.

Cybermercenaries – are effectively 'hackers for hire'. In much the same way that 'professional combat personnel' may offer their services to the highest-bidder nation during a conventional war, cybermercenaries are cybercriminals and hackers that sell their services to others – including nation states or other organizations.

Cybersabotage – activities carried out by cybersaboteurs in order to disrupt legitimate processes or businesses.

Cybersecurity – measures taken to defend IT systems and devices against cyberattacks.

Cyberspace – the intangible area or environment within which computer networks all over the world communicate with each other.

Cyberterrorist – individuals or groups that may be state-backed or operate as part of an independent terrorist organization, in order to launch cyberattacks.

Cyberwar/Cyberwarfare – both terms refer to cyberattacks that are carried out by nation states against other nation states.

Typically, cyberwarfare will seek to damage state-owned infrastructure or cause damage by stealing sensitive data – rather than trying to steal money. Common targets will include military facilities and critical infrastructure, such as transport networks, air traffic control services, power distribution grids, telecommunications, the food chain... and more.

Cyberweapons – are items of malware (malicious software) that have been developed to harm others. Cyberweapons are used to perform cyberespionage and cybersabotage attacks. Unlike conventional weapons, cyberweapons are easy to clone and reprogram.

Hacktivists – despite the absence of 'cyber' in their title, these hacker-activists deserve a mention in our glossary. Hacktivists are computer hackers that have aligned themselves with a specific protest organization or group of activists. Their activities can be similar to those of cyberterrorists or cybersaboteurs.

TRY THE POWER OF PROTECTION

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

GET YOUR FREE TRIAL TODAY!

JOIN THE CONVERSATION

Watch us on YouTube

Like us on Facebook

Review our blog

Follow us on Twitter

Join us on LinkedIn

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 security solutions for endpoint users (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.

Learn more at www.kaspersky.com/business.

Call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com, to learn more about Kaspersky Endpoint Security for Business.

KASPERSKY lab

THE POWER OF PROTECTION