KASPERSKY lab

KASPERSKY SECURITY INTELLIGENCE SERVICES

2015

Cybercrime today knows no borders, and its technical capabilities are improving fast: we're seeing how attacks are becoming increasingly sophisticated. Our mission is to save the world from all types of cyberthreat. To achieve this, and to make using the Internet safe and secure, it's vital to share threat intelligence in real time. Timely access to information is central to maintaining effective protection of data and networks.

Eugene Kaspersky
Chairman and CEO, Kaspersky Lab

INTRODUCTION

More cyberthreats are appearing every day, in all their different guises and through many different attack vectors.

There is no single solution that offers comprehensive protection. However, even in our big-data world, knowing where to look for danger is a large part of being able to combat the latest threats.

As a business manager, it`s your responsibility to protect your organization against today's threats, and to anticipate the dangers that lie ahead in the coming years. This needs more than just smart operational protection against known threats; it demands a level of strategic security intelligence that very few companies have the resources to develop in-house.

At Kaspersky Lab, we understand that it takes long-lasting relationships to bring long-term prosperity to a business.

Kaspersky Lab is a valuable business partner, always available to share its up-to-the-minute intelligence with your team via different channels. Our broad range of delivery methods helps your security operation center (SOC)/IT security team remain fully equipped to protect the organization from any online threat.

Even if your organization does not use Kaspersky Lab products, you can still benefit from Kaspersky Lab Security Intelligence Services.

SECURITY WITH A DIFFERENCE

World-leading Security Intelligence is built into our DNA – helping us deliver the most powerful anti-malware protection on the market and influencing everything we do.

We're a technology-driven company – from top to bottom – starting with our CEO, Eugene Kaspersky.

Our Global Research & Analysis Team (GReAT), an elite group of IT security experts, has led the way in uncovering many of the world's most dangerous malware threats and targeted attacks.

Many of the world's most respected security organizations and law enforcement agencies – including INTERPOL, Europol, CERT, City of London Police – have actively sought our assistance.

Kaspersky Lab develops and perfects all of its own core technologies in-house, so our products and intelligence are naturally more reliable and efficient.

The most widely respected industry analysts – including Gartner, Forrester Research and International Data Corporation (IDC) – rate us as a Leader within many key IT security categories.

Over 130 OEMs – including Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent and more – use our technologies within their own products and services.

CYBERSECURITY TRAINING

Leverage Kaspersky Lab's cybersecurity knowledge, experience and intelligence through these innovative training programs.

Cybersecurity awareness and education are now critical requirements for enterprises faced with an increasing volume of constantly evolving threats. Security employees need to be skilled in the advanced security techniques that form a key component of effective enterprise threat management and mitigation strategies, while all employees should have a basic awareness of the dangers and how to work securely.

Kaspersky Lab's Cybersecurity Training courses have been developed specifically for any organization looking to better protect its infrastructure and intellectual property. All training courses are offered in English.

THE COURSES

NON-IT AWARENESS	IT SECURITY EDUCATION	
Employees	Level 1 - Beginner	
ONLINE TRAINING PLATFORM	CORE SECURITY FUNDAMENTALS Basic IT knowledge	PRACTICAL SECURITY FUNDAMENTALS WITH LABS Basic IT knowledge
Line Managers	Level 2 - Intermediate	
CYBERSAFETY GAMES	DIGITAL FORENSICS System Administrator skills required	MALWARE ANALYSIS & REVERSE ENGINEERING Programming skills required
Business Managers	Level 3 - Advanced	
CYBERSAFETY CULTURE ASSESSMENT	ADVANCED DIGITAL FORENSICS System Administrator advanced skills required	ADVANCED MALWARE ANALYSIS & REVERSE ENGINEERING Assembler skills required

CYBERSECURITY AWARENESS

Online interactive training modules and on-site cybersafety game training for all employees who use computers or mobile devices at work, and those who manage them.

Around 80% of all cyber incidents are caused by human error. Companies are spending Millions on the cybersecurity awareness programs, but few CISOs are really satisfied with the results. What's wrong?

Most cybersecurity awareness training is too long, technical and essentially negative. This does not play to people's core strengths - their decision-making principles and learning abilities - and as a result can render training ineffectual.

So organizations are seeking more sophisticated behavioral support approaches (such as corporate culture development) that deliver a quantifiable and worthwhile return on their investment in security awareness.

Kaspersky Lab Cybersecurity Awareness courses work by:

- Changing behavior – stimulating the individual's commitment to working securely, building a corporate environment where "Everybody else cares about cybersafety, so I do, too".
- Combining a motivational approach, gamification learning techniques, simulated attacks and in-depth interactive cybersecurity skills training.

HOW IT WORKS

Comprehensive but straightforward	Training covers a wide range of security issues – from how data leaks occur to internet based malware attacks and safe social networking, through a series of simple exercises. We use learning techniques – group dynamics, interactive modules, cartoons and gamification to make the learning process engaging.
Continuous motivation	We create teachable moments - by gamification and competition, and then re-inforce these training moments throughout the year via online simulated attack exercises, assessment and training campaigns.
Changing beliefs	We teach people that it is human beings, not machines, who are the primary targets of cybercriminals. We show how, through working in a more safety-conscious manner, individuals can avoid becoming victims and exposing themselves and their workplace to attack.
Building a corporate cybersafety culture	We train management to become security advocates; a culture where cybersecurity becomes second nature is best achieved through management commitment and example, and cannot simply be imposed by IT.
Positive and collaborative	We demonstrate how security practices make a positive contribution to business efficiency, and promote more effective cooperation with other internal departments, including the IT Security team.
Measurable	We provide tools to measure employee skills, along with corporate-level assessments analyzing staff attitudes to cybersecurity in their daily work.

IT STAFF SECURITY EDUCATION

These courses offer a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert. All are available either in-class on customer premises or at a local or regional Kaspersky Lab office, if applicable.

Courses are designed to include both theoretical classes and hands-on 'labs'. On completion of each course, attendees will be invited to complete an evaluation to validate their knowledge.

BEGINNER, INTERMEDIATE OR EXPERT?

The program covers everything from security fundamentals to advanced digital forensics and malware analysis, allowing organizations to improve their cybersecurity knowledge pool in three main domains:

- Fundamental knowledge of the topic
- Digital Forensics and Incident Response
- Malware Analysis & Reverse Engineering

SERVICE BENEFITS

LEVEL 1 – Core Security Fundamentals
Equip IT and Security Administrators and Managers with a basic understanding of the latest thinking on practical IT security measures from an industry leader.

LEVEL 1 – Practical Security Fundamentals
Benefit from a in-depth understanding of security though practical exercises using modern security-related tools.

LEVELS 2-3 – Digital Forensics
Improve the expertise of your in-house digital forensics and incident response team.

LEVELS 2-3 – Malware Analysis & Reverse Engineering
Improve the expertise of your in-house malware analysis and reverse engineering team.

HANDS-ON EXPERIENCE

From a leading security vendor, working and learning alongside our global experts who inspire participants through their own experience at the 'sharp end' of cybercrime detection and prevention.

PROGRAM DESCRIPTION

TOPICS	Duration	Skills gained
LEVEL 1 – CORE SECURITY FUNDAMENTALS		
• Cyberthreats & underground market overview • Spam & phishing, email security • Fraud protection technologies • Exploits, mobile and advanced persistent threats • Investigation basics using public web tools • Securing your workplace	2 days	• Recognize security incidents and take decisions to resolve them • Reduce the load on Information Security departments • Increase the security level of each employer's workplace with additional tools • Perform simple investigations • Analyze phishing mails • Recognize infected or fake websites

TOPICS	Duration	Skills gained
LEVEL 1 – PRACTICAL SECURITY FUNDAMENTALS		
• Security basics • Open-source intelligence • Enterprise network security • Application security & exploit prevention • DDoS attacks & banking threats • Wireless LAN security & global mobile network • Banking & mobile threats • Cloud and virtual environment security incident response	5 days	• Provide basic investigations, using public resources, specialist search engines and social networks • Create a secure network perimeter • Basic penetration testing skills • Inspect traffic for different types of attack • Ensure secure software development • Identify malicious code injection • Undertake basic malware analysis and Digital forensics
LEVEL 2 – GENERAL DIGITAL FORENSICS		
• Introduction to Digital Forensics • Live response and evidence acquisition • Windows registry internals • Windows artifacts analysis • Browsers forensics • Email analysis	5 days	• Build a Digital Forensics lab • Collect digital evidence and deal with it properly • Reconstruct an incident and use time stamps • Find traces of intrusion based on artifacts in Windows OS • Find and analyze browser and email history • Be able be apply with the tools and instruments of digital forensics
LEVEL 2 – GENERAL MALWARE ANALYSIS & REVERSE ENGINEERING		
• Malware Analysis & Reverse Engineering goals and techniques • Windows internals, executable files, x86 assembler • Basic static analysis techniques (strings extracting, import analysis, PE entry points at a glance, automatic unpacking, etc.) • Basic dynamic analysis techniques (debugging, monitoring tools, traffic interception, etc.) • .NET, Visual Basic, Win64 files analysis • Script and non-PE analysis techniques (Batch files; Autoit; Python; Jscript; JavaScript; VBS)	5 days	• Build a secure environment for malware analysis: deploy sandbox and all necessary tools • Understand principles of Windows program execution • Unpack, debug and analyze malicious object, identify its functions • Detect malicious sites through script malware analysis • Conduct express malware analysis
LEVEL 3 – ADVANCED DIGITAL FORENSICS		
• Deep Windows Forensics • Data recovery • Network and cloud forensics • Memory forensics • Timeline analysis • Real world targeted attack forensics practice	5 days	• Be able to perform deep file system analysis • Be able to recover deleted files • Be able to analyze network traffic • Reveal malicious activities from dumps • Reconstruct the incident timeline
LEVEL 3 – ADVANCED MALWARE ANALYISIS & REVERSE ENGINEERING		
• Malware Analysis & Reverse Engineering goals and techniques • Advanced static & dynamic analysis techniques • (manual unpacking) • Deobfuscation techniques • Rootkit & bootkit analysis • Exploits analysis (.pdf, .doc, .swf, etc.) • Non-Windows malware analysis (Android, Linux, Mac OS)	5 days	• Use the world best practices in reverse engineering • Recognize anti-reverse engineering techniques (obfuscation, anti-debugging) • Apply advanced malware analysis for Rootkits/Bootkits • Analyze exploit shellcode, embedded in different file types • Analyze non-Windows malware

THREAT INTELLIGENCE SERVICES

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Enterprises across all sectors are facing a shortage of the up-to-the-minute, relevant data they need to help them manage the risks associated with IT security threats.

Security Threat Intelligence Services from Kaspersky Lab gives you access to the intelligence you need to mitigate these threats, provided by our world-leading team of researchers and analysts.

Kaspersky Lab's knowledge, experience and deep intelligence on every aspect of cybersecurity has made it the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. You can leverage this intelligence in your organization today.

Kaspersky Lab Threat Intelligence Services include:

- Threat Data Feeds
- Botnet Tracking
- APT Intelligence Reporting

THREAT DATA FEEDS

Reinforce your network defense solutions, including SIEMs, Firewalls, IPS/IDS, Anti-APT and sandbox/simulation technologies, with continuously updating, comprehensive data, providing insights into cyberthreats and targeted attacks.

Malware families and variations have grown exponentially in the last few years; Kaspersky Lab is currently detecting about 325,000 unique new malware samples every day. To defend their endpoints against these threats, most organizations deploy classical protection measures like anti-malware solutions, intrusion prevention or threat detection systems. In a fast-changing environment where cybersecurity is always trying to stay one step ahead of cybercrime, these classical solutions need to be reinforced with access to up-to-the-minute threat intelligence.

Kaspersky Lab's Threat Data Feeds are designed to integrate into existing Security Information and Event Management (SIEM) systems, providing an additional layer of protection. Threat Data Feed integration makes it possible, for example, to correlate the logs coming to the SIEM from different network devices with the URL feeds from Kaspersky Lab. A connection with HP ArcSight SIEM is included. Connectors for Splunk and QRadar are also available.

USE CASES / SERVICE BENEFITS

Kaspersky Lab Threat Data Feeds:

- Empower your SIEM solution by leveraging data about harmful URLs. The SIEM is notified about malware, phishing and Botnet C&C URLs from logs coming to the SIEM from different network devices (user PCs, network proxies, firewalls, other servers)
- Empower primary network defense solutions such as firewalls, IPS/IDS, SIEM solutions, Anti-APT, sandbox/simulation technology, UTM appliances etc with continuously updated threat intelligence
- Improve your forensic capabilities by providing security teams with meaningful information about threats and insights into the thinking behind targeted attacks
- Support your research. Information about harmful URLs and MD5 hashes of malicious files makes a valuable contribution to threat research projects

Kaspersky Lab offers three types of Threat Data Feed:

1. Malicious URLs and masks
2. MD5 hashes of malicious objects database
3. Mobile Thread Feeds

FEED DESCRIPTION

Malicious URLs – a set of URLs covering malicious links and websites. Masked and non-masked records are available.
Phishing URLs – a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.
Botnet C&C URLs – a set of URLs of botnet command and control (C&C) servers and related malicious objects.
Malware Hashes (ITW) – a set of file hashes and corresponding verdicts covering the most dangerous and prevalent malware delivered through the intelligence of KSN.
Malware Hashes (UDS) – a set of file hashes detected by Kaspersky Lab cloud technologies (UDS stands for Urgent Detection System) based on a file's metadata and statistics (without having the object itself). This enables the identification of new and emerging (zero-day) malicious objects that are not detected by other methods.
Mobile Malware Hashes – a set of file hashes for detecting malicious objects that infect mobile platforms.
P-SMS Trojan Feed — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages.
Mobile Botnet C&C URLs — a set of URLs with context covering mobile botnet C&C servers.

BOTNET TRACKING

Expert monitoring and notification services to identify botnets threatening your customers and your reputation.

Many network attacks are organized using botnets. These attacks can target casual internet users, but often these threats are aimed at the online customers of specific organizations and their online customers.

Kaspersky Lab's expert solution tracks the activity of botnets and provides rapid (within 20 minutes) notification of threats associated with the users of individual online payment and banking systems. You can use this information to advise and inform your customers, security services providers and local law enforcement agencies about current threats. Protect your organization's reputation and customers today with Kaspersky Lab's Botnet Tracking Service.

USE CASES / SERVICE BENEFITS

- Proactive alerts about threats coming from botnets that target your online users allow you to always remain one step ahead of the attack
- Identifying a list of Botnet Command & Control server URLs that are targeting your online users allows you to block them by sending requests to CERTs or law enforcement agencies
- Improve your online banking / payment cabinets by understanding the nature of attack
- Train your online users to recognize and avoid falling foul of the social engineering used in attacks

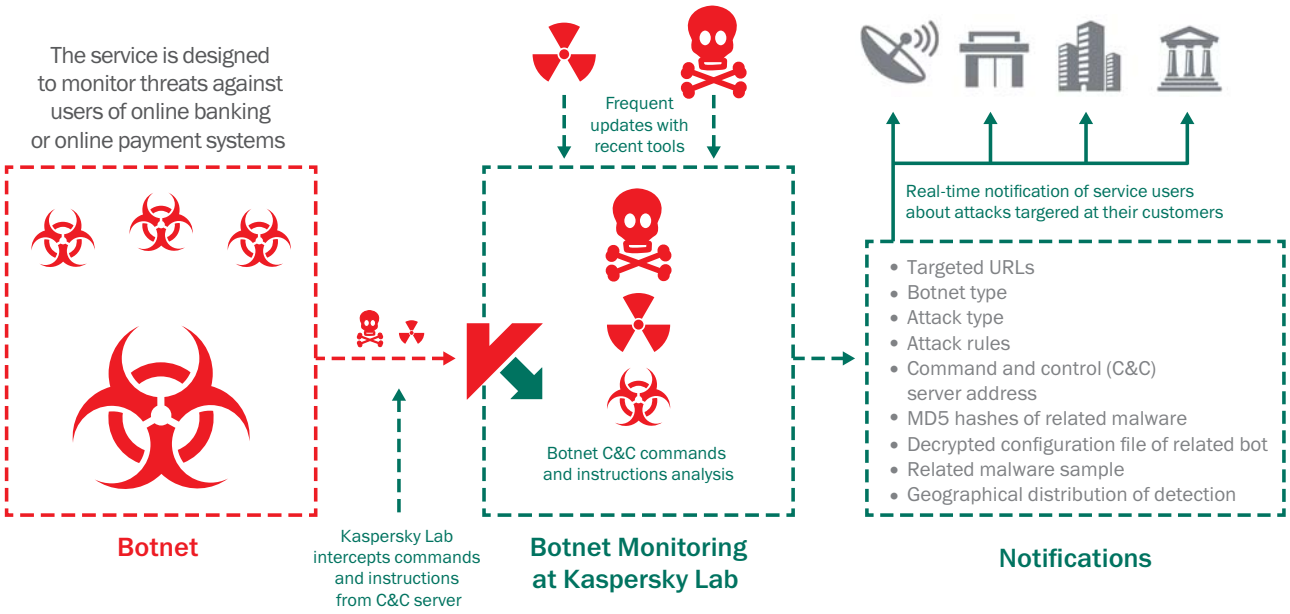
TAKE ACTION WITH REAL-TIME DELIVERABLES:

The service provides a subscription to personalized notifications containing intelligence about matching brand names by tracking keywords in the botnets monitored by Kaspersky Lab. Notifications can be delivered via email or RSS in either HTML or JSON format. Notifications include:

- **Targeted URL(s)** — Bot malware is designed to wait until the user accesses the URL(s) of the targeted organization and then starts the attack.
- **Botnet type** — Understand exactly what malware threat is being employed by the cybercriminal to jeopardize your customers' transactions. Examples include Zeus, SpyEye, and Citadel.
- **Attack type** — Identify what the cybercriminals are using the malware to do; for example, web data injection, screen wipes, video capture or forwarding to phishing URL.
- **Attack rules** — Know what different rules of web code injection are being used such as HTML requests (GET / POST), data of web page before injection, data of web page after injection.
- **Command and Control (C&C) server address** — Enables you to notify the Internet service provider of the offending server to dismantle of the threat faster.
- **MD5 hashes of related malware** — Kaspersky Lab provides the hash sum that is used for malware verification.
- **Decrypted configuration file of related bot** — identifying the full list of targeted URLs.
- **Related malware sample** — for further reversing and digital forensic analysis of the botnet attack.
- **Geographical distribution of detection (top 10 countries)** — Statistical data of related malware samples from around the world.

BOTNET TRACKING: ARCHITECTURE

FROM C&C SERVER



Kaspersky Lab's solution is available in either Standard or Premium, offering a variety of service terms and monitored URLs. Consult with Kaspersky Lab or your reseller partner to determine which package is right for your enterprise.

SUBSCRIPTION LEVELS AND DELIVERABLES

Premium

Notification in email or JSON format — 10 URLs monitored

- Decrypted configuration file of related bot
- Related malware sample (on demand)
- Geographical distribution of detections for related malware samples

Standard

Notification in email format — 5 URLs monitored

- Target URL (identifying the URL(s) were the bot program is targeting users)
- Botnet type (e.g., Zeus, SpyEye, Citadel, Kins, etc.)
- Attack type
- Attack rules, including: Web data injection; URL, screen, Video capture, etc.
- C&C address
- MD5 hashes of related malware

INTELLIGENCE REPORTING

Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky Lab.

Leveraging the information and tools provided in these reports, you can respond quickly to new threats and vulnerabilities - blocking attacks via known vectors, reducing the damage caused by advanced attacks and enhancing your security strategy, or that of your customers.

APT Intelligence reporting

Not all Advanced Persistent Threat discoveries are reported immediately, and many are never publicly announced. Be the first to know, and exclusively In the Know, with our in-depth, actionable intelligence reporting on APTs.

As a subscriber to Kaspersky APT Intelligence Reporting, we provide you with unique ongoing access to our investigations and discoveries, including full technical data provided in a range of formats, on each APT revealed as it's revealed, including all those threats that will never be made public.

Our experts, the most skilled and successful APT hunters in the industry, will also alert you immediately to any changes they detect in the tactics of cyber-criminal and cyber-terrorist groups. And you will have access to Kaspersky Lab's complete APT reports database – a further powerful research and analysis component of your corporate security armory.

KASPERSKY APT INTELLIGENCE REPORTING PROVIDES:

- **Exclusive access** to technical descriptions of cutting edge threats during the ongoing investigation, before public release.
- **Insight into non-public APTs**. Not all high profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability fixing process or associated law enforcement activity, are never made public. But all are reported to our customers.
- **Detailed supporting** technical data, samples and tools, including an extended list of Indicators of Compromise (IOCs), available in standard formats including openIOC or STIX, and access to our Yara Rules.
- **Continuous APT campaign monitoring**. Access to actionable intelligence during the investigation (information on APT distribution, IOCs, C&C infrastructure).
- **Retrospective analysis**. Access to all previously issued private reports is provided throughout the period of your subscription.

NOTE – SUBSCRIBER LIMITATION

Due to the sensitive and specific nature of some of the information contained in the reports provided by this service, we are obliged to limit subscriptions to trusted government, public and private organizations only.

INTELLIGENCE REPORTING

Customer-Specific Threat Intelligence Reporting

What's the best way to mount an attack against your organization? Which routes and what information is available to an attacker specifically targeting you? Has an attack already been mounted, or are you about to come under threat?

Kaspersky customer-specific Threat Intelligence Reporting answers these questions and more, as our experts piece together a comprehensive picture of your current attack status, identifying weak-spots ripe for exploitation and revealing evidence of past, present and planned attacks.

Empowered by this unique insight, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting quickly and with precision to repel intruders and minimize the risk of a successful attack.

Developed using open source intelligence (OSINT), deep analysis of Kaspersky Lab expert systems and databases and our knowledge of underground cybercriminal networks, these reports cover areas including:

- **Identification of threat vectors**: Identification and status analysis of externally available critical components of your network –including ATMs, video surveillance and other systems using mobile technologies, employee social network profiles and personal email accounts – that are potential targets for attack.
- **Malware and cyber-attack tracking analysis**: Identification, monitoring and analysis of any active or inactive malware samples targeting your organization, any past or present botnet activity and any suspicious network based activity.
- **Third-party attacks**: Evidence of threats and botnet activity specifically targeting your customers, partners and subscribers, whose infected systems could then be used to attack you.
- **Information leakage**: through discreet monitoring of underground online forums and communities, we discover whether hackers are discussing attack plans with you in mind or, for example, if an unscrupulous employee is trading information.
- **Current attack status**: APT attacks can continue undetected for many years. If we detect a current attack affecting your infrastructure, we provide advice on effective remediation.

QUICK START – EASY TO USE – NO RESOURCES NEEDED

Once parameters (for customer-specific reports) and preferred data formats are established, no additional infrastructure is needed to startusing this Kaspersky Lab service.

Kaspersky Threat Intelligence Reporting has no impact on the integrity and availability of resources, including network resources.

EXPERT SERVICES

Expert Services from Kaspersky Lab are exactly that – the services of our in-house experts, many of them global authorities in their own right, whose knowledge and experience is fundamental to our reputation as world leaders in security intelligence.

Because no two IT infrastructures are exactly the same, and because the most powerful cyberthreats are tailor-made to exploit the specific vulnerabilities of the individual organization, our expert services are also tailor-made. The services described on the following pages form a part of our professional toolkit – some or all of these services, in part or in full, may be applied as we work with you.

Our objective, above all, is to work with you, one on one, as your expert advisors, helping to evaluate your risk, harden your security and mitigate against future threats.

Expert services include:

- Incident Investigation
- Penetration Testing
- Application Security Assessment

INCIDENT INVESTIGATION

Digital forensics | malware analysis

Personalized incident investigation support to help your organization identify and resolve IT security incidents.

Cyberattacks are an increasing danger for enterprise networks. Tailor-made to exploit the unique vulnerabilities of the criminal's chosen target, these attacks are often designed to steal or destroy sensitive information or intellectual property, undermine operations, damage industrial facilities or steal money.

Protecting an enterprise against these sophisticated, well-planned attacks has become increasingly complicated. It can even be difficult to establish for certain whether your organization is in fact under attack.

Kaspersky Lab's Incident Investigation Services can help organizations formulate their defense strategies through providing in-depth threat analysis and advising on appropriate steps toward resolution of the incident.

SERVICE BENEFITS

Kaspersky Lab Incident Investigation Services help you to resolve live security issues and understand malware behavior and its consequences, providing guidance on remediation. This approach indirectly helps to:

- Reduce the costs of resolving issues arising from a cyber-infection
- Stop the leakage of confidential information that can potentially flow from infected PCs
- Reduce reputational risk caused by the infection harming operational processes
- Restore the normal work of PCs that were damaged by infection

Kaspersky Lab's investigations are carried out by highly experienced analysts with practical expertise in digital forensics and malware analysis. On completion of the investigation, you are provided with a detailed report, giving the full results of the cyber investigation and proposing remediation steps.

DIGITAL FORENSICS

Digital Forensics is an investigation service aimed at producing a detailed picture of an incident. Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab experts piece together the evidence to understand exactly what is going on, including the use of HDD images, memory dumps and network traces. The result is a detailed explanation of the incident.

You as the customer initiate the process by gathering evidence and an outline of the incident. Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of specific malware files that are targeting your organization.

Kaspersky Lab's experts carry out a thorough analysis of the malware sample provided by your organization, creating a detailed report that includes:

- **Sample properties**: A short description of the sample and a verdict on its malware classification
- **Detailed malware description**: An in-depth analysis of your malware sample's functions, threat behavior and objectives - including IOCs - arming you with the information required to neutralize its activities
- **Remediation scenario**: The report will suggest steps to fully secure your organization against this type of threat

DELIVERY OPTIONS

Kaspersky Lab Investigation Services are available:

- by subscription, based on an agreed number of incidents
- in response to a single incident

PENETRATION TESTING SERVICES

Ensuring that your IT infrastructure is fully secured against potential cyber-attack is an ongoing challenge for any organization, but even more so for large enterprises with perhaps thousands of employees, hundreds of information systems, and multiple locations worldwide.

While your IT and security specialists work hard to ensure that every network component is both secure against intruders and fully available to legitimate users, a single vulnerability can offer an open door to any cybercriminal intent on gaining control over your information systems.

Penetration testing is a practical demonstration of possible attack scenarios where a malicious actor may attempt to bypass security controls in your corporate network to obtain high privileges in important systems.

Kaspersky Lab's Penetration Testing Service gives you a greater understanding of security flaws in your infrastructure, revealing vulnerabilities, analyzing the possible consequences of different forms of attack, evaluating the effectiveness of your current security measures and suggesting remedial actions and improvements.

Penetration Testing from Kaspersky Lab helps you and your organization to:

- **Identify the weakest points in your network,** so you can make fully informed decisions about where best to focus your attention and budget in order to mitigate future risk.
- **Avoid financial, operational and reputational losses caused by cyber-attacks** by preventing these attacks from ever happening through proactively detecting and fixing vulnerabilities.
- **Comply with government, industry or internal corporate standards** that require this form of security assessment (for example Payment Card Industry Data Security Standard (PCI DSS)).

SERVICE SCOPE AND OPTIONS

Depending on your needs and your IT infrastructure, you may choose to employ any or all of these Penetration Testing Services:

- **External penetration testing** – Security assessment conducted through the Internet by an 'attacker' with no preliminary knowledge of your system.
- **Internal penetration testing** – Scenarios based on an internal attacker, such as a visitor with only physical access to your offices or a contractor with limited systems access.
- **Social engineering testing** – An assessment of security awareness among your personnel by emulating social engineering attacks, such as phishing, pseudo-malicious links in emails, suspicious attachments, etc.
- **Wireless networks security assessment** – Our experts will visit your site and analyze WiFi security controls

You can include any part of your IT infrastructure into the scope of penetration testing, but we strongly recommend you consider the whole network or its largest segments, as test results are always more worthwhile when our experts are working under the same conditions as a potential intruder.

PENETRATION TESTING RESULTS

The Penetration Testing Service is designed to reveal security shortcomings which could be exploited to gain unauthorized access to critical network components. These could include:

- Vulnerable network architecture, insufficient network protection
- Vulnerabilities leading to network traffic interception and redirection
- Insufficient authentication and authorization in different services
- Weak user credentials
- Configuration flaws, including excessive user privileges
- Vulnerabilities caused by errors in application code (code injections, path traversal, client-side vulnerabilities, etc.)
- Vulnerabilities caused by usage of outdated hardware and software versions without latest security updates
- Information disclosure

Results are given in a final report including detailed technical information on the testing process, results, vulnerabilities revealed and recommendations for remediation, as well as an executive summary outlining test results and illustrating attack vectors. Videos and presentations for your technical team or top management can also be provided if required.

ABOUT KASPERSKY LAB'S APPROACH TO PENETRATION TESTING

While penetration testing emulates genuine hacker attacks, these tests are tightly controlled; performed by Kaspersky Lab security experts with full regard to your systems' confidentiality, integrity and availability, and in strict adherence to international standards and best practices including:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- Common Vulnerability Scoring System (CVSS)

Project team members are experienced professionals with a deep, current practical knowledge of this field, acknowledged as security advisors by industry leaders including Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens and SAP.

DELIVERY OPTIONS:

Depending on the type of security assessment service, your systems specifics and working practices, security assessment services can be provided remotely or onsite. Most services can be performed rremotely, and internal penetration testing can even be performed through VPN access, while some services (like wireless networks security assessment) require an onsite presence.

APPLICATION SECURITY ASSESSMENT SERVICES

Whether you develop corporate applications internally, or purchase them from third parties, you'll know that a single coding error can create a vulnerability exposing you to attacks resulting in considerable financial or reputational damage. New vulnerabilities can also be generated during an application's lifecycle, through software updates or insecure component configuration, or can arise through new attack methods.

Kaspersky Lab's Application Security Assessment Services uncover vulnerabilities in applications of any kind, from large cloud-based solutions, ERP systems, online banking and other specific business applications, to embedded and mobile applications on different platforms (iOS, Android and others).

Combining practical knowledge and experience with international best practices, our experts detect security flaws which could expose your organization to threats including:

- Syphoning off confidential data
- Infiltrating and modifying data and systems
- Initiating denial of service attacks
- Undertaking fraudulent activities

Following our recommendations, vulnerabilities revealed in applications can be fixed, and such attacks prevented.

SERVICE BENEFITS

Kaspersky Lab Application Security Assessment Services help application owners and developers to:

- **Avoid financial, operational and reputational loss**, by proactively detecting and fixing the vulnerabilities used in attacks against applications
- **Save remediation costs** by tracking down vulnerabilities in applications still in development and test, before they reach the user environment where fixing them may involve considerable disruption and expense.
- **Support a secure software development lifecycle** (S-SDLC) committed to creating and maintaining secure applications.
- **Comply with government, industry or internal corporate standards** covering application security, such as PCI DSS or HIPAA

SERVICE SCOPE AND OPTIONS

Applications assessed can include official web sites and business applications, standard or cloud based, including embedded and mobile applications.

The services are tailored to your needs and application specifics, and may involve:

- **Black-box testing** – emulating an external attacker
- **Grey-box testing** – emulating legitimate users with a range of profiles
- **White-box testing** - analysis with full access to the application, including source codes; this approach is the most effective in terms of revealing numbers of vulnerabilities
- **Application firewall effectiveness assessment** – applications are tested with and without firewall protection enabled, to find vulnerabilities and verify whether potential exploits are blocked

RESULTS

Vulnerabilities which may be identified by Kaspersky Lab Application Security Assessment Services include:

- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transferring, for instance lack of PAN masking in payment systems
- Configuration flaws, including ones leading to session attacks
- Sensitive information disclosure
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

Results are given in a final report including detailed technical information on the assessment processes, results, vulnerabilities revealed and recommendations for remediation, together with an executive summary outlining management implications. Videos and presentations for your technical team or top management can also be provided if required.

ABOUT KASPERSKY LAB'S APPROACH TO APPLICATION SECURITY ASSESSMENT

Security assessments of applications are performed by Kaspersky Lab security experts both manually and through applying automated tools, with full regard of your systems' confidentiality, integrity and availability and in strict adherence to international standards and best practices, such as:

- Web Application Security Consortium (WASC) Threat Classification
- Open Web Application Security Project (OWASP) Testing Guide
- OWASP Mobile Security Testing Guide
- Other standards, depending on your organization's business and location

Project team members are experienced professionals with a deep, current practical knowledge of the field, including different platforms, programming languages, frameworks, vulnerabilities and attack methods. They speak at leading international conferences, and provide security advisory services to major vendors of applications and cloud services, including Oracle, Google, Apple, Facebook and PayPal.

DELIVERY OPTIONS:

Depending on a type of security assessment service, specifics of systems in the scope, and your requirements to work conditions, security assessment services can be provided remotely or onsite. Most of these services can be performed remotely.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

To find out more about the products and services outlined here, or communicate with us regarding how these services may be applicable to the security of your organization, please contact us via e-mail intelligence@kaspersky.com

Please note that terms and conditions which apply may vary from region to region including, but not limited to: scope of work, timelines, local services availability, language of delivery, costs.

Security Intelligence Services Catalogue August 2015 GL

KASPERSKY lab