KASPERSKY lab

Improved protection for cryptocurrency exchange applications, web layers and networks

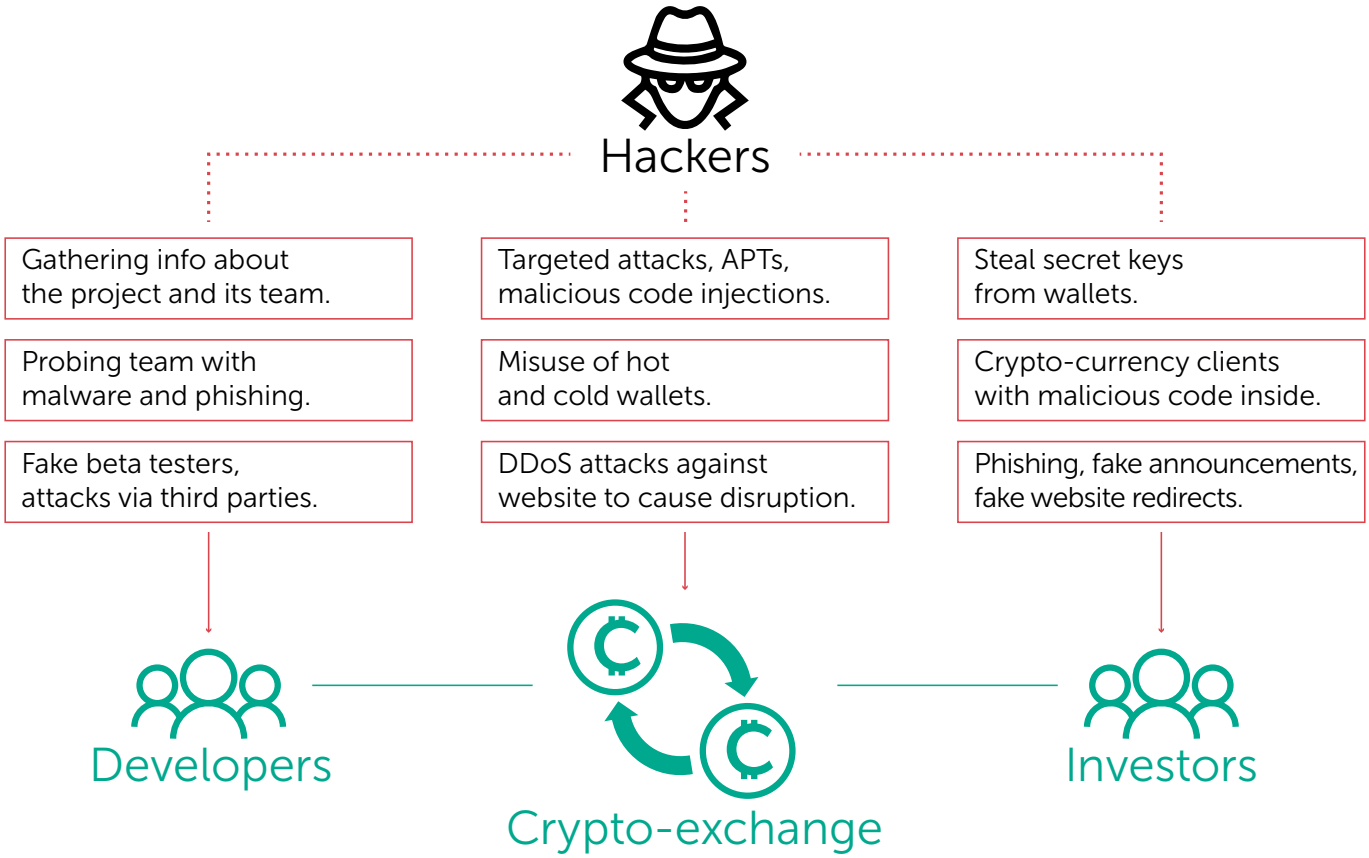
Kaspersky Crypto-Exchange Security

www.kaspersky.com
#truecybersecurity

How not to become the next target of cybercriminals and not to lose billions of dollars.

A crypto-exchange is a type of online stock exchange where customers buy and sell a variety of crypto-assets. These online platforms usually charge small fees to traders to generate income. With monthly trading volumes amounting to millions and even billions of dollars, the hacking of crypto-exchanges by cybercriminals is a real threat that cannot be ignored. Every year there are numerous online violations that see assets worth hundreds of millions of dollars irrevocably lost due to stolen cryptocurrency.

Every year, the record for the number of cryptocurrency exchange infringements is shattered, with a huge amount of assets stolen every day. Cryptocurrency exchanges need to be aware of and able to withstand the threats that they face.



Protect investor assets by improving application and IT infrastructure resilience

Common vulnerabilities and protection techniques for crypto-exchanges

According to icorating.com, there are four main types of cybersecurity factors with their own unique parameters that crypto-exchanges have to consider. They are user security, domain and registrar security, web security, and denial-of-service (DoS) attack protection. Source: icorating.com

User security includes methods for user activity verification.

Among the threats to which users can be exposed, malfunctions in applications are the most severe. For example, attackers can inject JavaScript code in a web page and capture user data. Another important issue is that of crypto-exchanges allowing users to create weak passwords, while even strong passwords can be stored with weak cryptography.

Some ways of resolving these problems are noteworthy, such as email confirmation of registration and activities, as well as two-factor authentication. It ensures that the real user is active now, not the hacker. But this may also not be enough.

In fact, one of the most popular types of attack involves hacking an email account first, then restoring access to the account using the account password recovery procedure.

A complex solution might consider two-factor authentication (2FA) as a valid option, which includes both 2FA apps (Google Authenticator) and more traditional options, such as confirmation via mobile phone number.

Protection of domain names and role accounts is crucial for providing safe transactions

You must take care of your domain security. By setting the registry lock you can prevent domain hijacking. Another issue you need to consider is a domain expiration period of at least six months.

Multilevel access and role-based access control (RBAC) help to protect a system from targeted attacks.

The domain name system (DNS) is a fundamental part of web security. To avoid or minimize the risk of DNS cache poisoning you can use DNSSEC. It is also important that from February 2019 a number of major DNS software and service providers have launched the process of removing accommodations for non-compliant DNS implementations from their software or services. For instance, it will discover new functionality for operators, such as new DDoS-protection mechanisms. source: https://dnsflagday.net/

Attempts by hackers to exploit cryptocurrency vulnerabilities are not a regular occurrence due to the complexity of such hacks. In most cases, the hackers are interested in the crypto-exchanges themselves because they are mostly centralized applications. Typical threats facing these applications include backdoors embedded at the development stage, web vulnerabilities such as cross-site scripting (XSS) and social engineering attacks such as phishing.

As the number of crypto-exchanges grows, so does the number of threats.

Online crypto-exchange platforms are usually centralized, unlike blockchain technology. Developed primarily as web applications, crypto-exchange platforms can be susceptible to the same security problems as other websites. Both frontend and backend components of such applications have to be equally protected.

Kaspersky Security Assessment delivers thorough analysis and investigation of application component vulnerabilities

Use services that are tailored to your needs and application specifics. In order to conduct an in-depth assessment of each security layer of a product, we work closely with our clients as expert advisors. The main objective is to harden your security and mitigate possible threats in the future.

Assessment and test activity results are provided in a final report that includes a comprehensive description of detected vulnerabilities. The report is structured as follows:

- Detailed technical information on assessment processes.
- Detected vulnerabilities.
- Recommendations.
- Executive summary outlining management implications.
- Videos and presentations for your technical team or top management can also be provided if required.

Kaspersky Application Security Assessment

Complex systems such as cryptocurrency exchanges consist of many components with specific structures and functions. This necessitates multiple assessment and testing techniques, because even the slightest flaw can be exploited by attackers.

Kaspersky Application Security Assessment service is capable of identifying a wide range of vulnerabilities.

- Multi-factor authentication is preferable when it comes to protection measures for sensitive information and assets belonging to investors. But the risk of flaws in authentication and authorization modules cannot be excluded.

- Common client-side and server-side vulnerabilities are code injection (e.g. SQL Injection, OS Commanding), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), etc. Malicious code can be used to intercept user credentials, cookies, assets or other data transferred between client and server. The application may contain configuration flaws as well, including those that lead to session attacks.

- Many web platforms still allow users to set weak passwords, while even strong passphrases can be stored with weak encryption/hashing scheme, such as MD5.

Crypto-exchanges can suffer from attacks at any moment

There are a number of security techniques that help crypto-exchanges protect their web layer.

A number of issues are considered critical, such as:

- **Clickjacking** - tricking users into clicking on links hidden in invisible layers above the page.
- **Drive-by Download attack** - the unintentional download of malicious code that leaves the user's computer or mobile device open to a cyberattack.
- **POODLE attacks** - exploits SSL 3.0 to reduce system security.
- **Robot vulnerabilities.**

Crypto-exchanges must implement an HSTS header to only allow HTTPS access, as well as the Content-Security-Policy frame-ancestors directive, and keep server software up to date.

Crypto-exchanges are exposed to DoS (Denial-of-Service) attacks

DoS attacks place excessive loads on servers, resulting in host unavailability. Implementing the most relevant web technologies and cybersecurity techniques helps minimize this risk.

What does the final Kaspersky Application Security Assessment report include?

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.

Vulnerabilities that can be identified by Kaspersky Application Security Assessment services

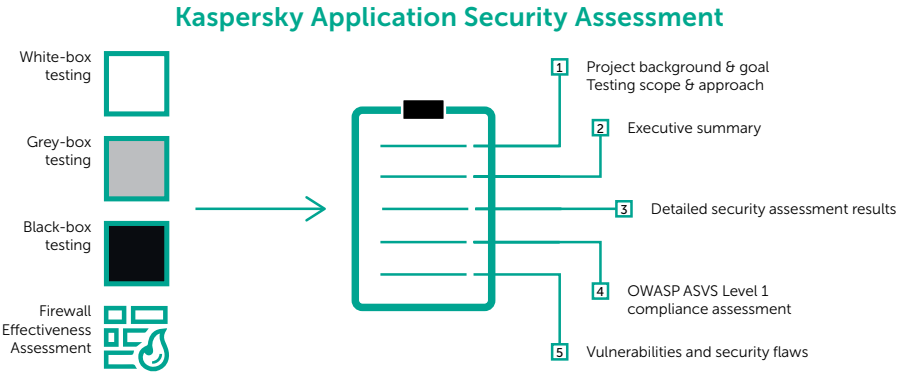
- Flaws in authentication and authorization, including multi-factor authentication
- Code injection (SQL Injection, OS Commanding, etc.)
- Logical vulnerabilities leading to fraud
- Client-side vulnerabilities (Cross-Site Scripting, Cross-Site Request Forgery, etc.)
- Use of weak cryptography
- Vulnerabilities in client-server communications
- Insecure data storage or transfer, for instance lack of PAN masking in payment systems
- Configuration flaws, including those leading to session attacks
- Disclosure of sensitive information
- Other web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.
- There is a risk of logical vulnerabilities leading to fraud. This may go unnoticed at the development and testing stages.
- Insecure data storage or transfer, for instance, storing payment card data in payment systems, can lead to the theft of investors' assets. Disclosure of sensitive information is unacceptable for a crypto-exchange, meaning every weak point must be identified.
- There are a number of web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

Kaspersky Application Security Assessment covers all product components, helping to prevent as many threats as possible. The service may include:

- **Black-box testing** — emulating an external attacker.
- **Grey-box testing** — emulating legitimate users with a range of privileged profiles.
- **White-box testing** — analysis with full access to the application, including source code; 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.

By analyzing the entire application architecture, we at Kaspersky Lab are capable of preventing a large amount of unwanted damage.

- **Avoid financial, operational and reputational losses** by proactively detecting and fixing vulnerabilities in your crypto-exchange application and front-end.
- **Save on remediation costs** by tracking down vulnerabilities in applications still in development and testing, before they reach the user environment.
- **Support a secure software development lifecycle (S-SDLC)** committed to creating and maintaining secure applications.



Penetration testing results

Kaspersky Penetration Testing 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 outdated hardware and software versions without the latest security updates
- Information disclosure

Attack on a crypto-exchange using code injection:

On November 3, 2018, an attack took place on the cryptocurrency exchange Gate.io. The web analytics platform StatCounter was used as an entry point by the intruders. The malicious code inserted into the platform's script modified the JavaScript on each page of Gate.io. It replaced the destination address of a transfer with one belonging to the hackers. The amount of stolen coins remains unclear. Source: TheBlockCrypto

Kaspersky Penetration Testing

Kaspersky Penetration Testing helps you understand which components in your IT infrastructure are vulnerable to cyberattacks. We simulate malicious activities by a cybercriminal trying to attack your application or website. The process identifies ways to take over your systems and data, potentially leading to financial or reputational losses.

Identifying the weakest points of a platform can help avoid possible risks, and financial and reputational losses caused by attacks.

It's not only the application that needs to be secure; you need to ensure the sustainability and resilience of the environment that your crypto-exchange platform is based on.

The process involves testing the network architecture, application code, hardware and software.

A variety of methodologies are used to test your IT infrastructure for vulnerabilities:

- **External penetration testing:** Security assessment conducted via the internet by an 'attacker' with no prior knowledge of your systems.
- **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 system 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 network security assessment:** Our experts visit your site and analyze Wi-Fi security controls.

Ensure safe transactions by preventing phishing attacks

How phishing helped cybercriminals get inside the Bitstamp infrastructure:

Hackers sent a series of spear-phishing emails to six Bitstamp employees over the course of several weeks. The attackers completed background checks on the employees, solicited them over Skype, and eventually managed to convince a Bitstamp system administrator to download a Word document.

The Word document contained an obscured Visual Basic for Applications (VBA) script that downloaded a malicious file and compromised the sys-admin's machine. Once compromised, the attacker had access to the main Bitstamp hot wallet servers, including passphrases.

Social engineering and phishing are still effective:

North Korean group Lazarus started their network penetration with emails sent to employees of several crypto-exchanges. They contained a message offering to install a trading app called Celas Trade Pro. The official website had a valid SSL certificate and everything seemed legitimate. Once installed the app tried to download and install an update which in fact was a backdoor Trojan. Source: Kaspersky Lab blog

Every Kaspersky Phishing Detection notification is delivered via HTTPS and includes:

- Screenshot of the phishing URL;
- HTML code of the phishing URL;
- JSON file that includes the following fields:
  - the phishing URL;
  - brand name targeted by the phishing URL;
  - first seen timestamp;
  - last seen timestamp;
  - popularity of the phishing URL;
  - geolocation of users affected by the phishing URL;
  - type of stolen data (credit card info, credentials for bank, email or social network, personal info, etc.);
  - attack type (threat to block an account, an offer to download a file, a request to update personal info, etc.);
  - IP addresses resolved by the phishing URL;
  - WHOIS data;
  - and much more.

A variety of phishing methods are employed by attackers. They may send fake emails with "special offers" or "partnership proposals" containing links to fake websites. It can be hard to recognize a spoof, and users can even end up giving their credentials to cybercriminals while trying to log in to a malicious clone of a website they know well. The starting point for this kind of incident is the appearance of website clones on the internet.

In-browser scripts that carry out malicious activity in the background pose huge risks as well. They can replace URLs and data transmitted in requests in such a way that assets, crypto-funds or sensitive information can be obtained by the attackers.

Less subtle methods such as ransomware operate more openly, as they find system vulnerabilities and extort users' funds.

Kaspersky Phishing Detection actively tracks and alerts you in real time about the appearance of phishing sites targeting your brand

Using this cutting-edge technology from Kaspersky Lab it is possible to track phishing attempts and send immediate alerts.

- Accurate and detailed real-time reporting about phishing or fraudulent activity directly relevant to your business, including injected malware and phishing URLs that steal credentials, sensitive information, financial information and personal data from your users.

- Email notifications confirm phishing threats against your brands, company name or trademarks. Every notification provides deep coverage, high accuracy and reliable information about phishing attacks.

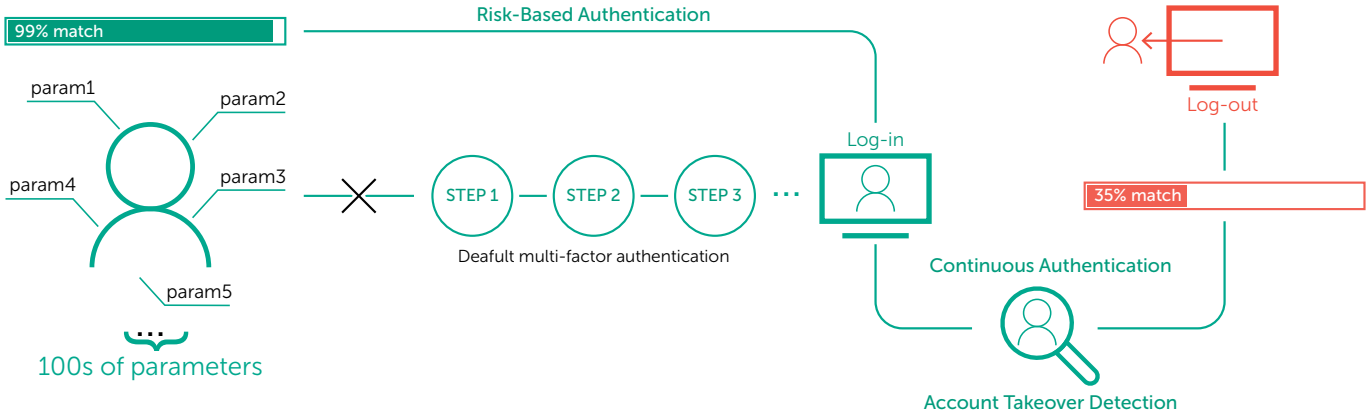
Kaspersky Phishing Detection gives you a critical edge against your attackers.

- Critical **information is provided in real time** and through regular reporting on malicious activities that indicate advanced attacks are being planned, as well as those that are in progress.

- Once you know and understand your spear-phishing adversaries, **you can plan appropriate protection**, from banning outdated software to introducing SMS-based authorization, helping reassure your online customers and making them feel better protected.

- Knowing the URLs of phishing websites means ISPs hosting the sites can be notified, **preventing the further leakage of any personal data** acquired by the site and stopping the attack in its tracks.

Prevent fraudulent activities and account takeover



Advanced Authentication knows who is using your services on web and mobile channels: a legitimate user or a fraudster, a human or a bot.

Analysis of behavioral data, passive biometrics as well as the device and its environment result in an objective risk assessment. The weighted analysis of hundreds of unique parameters from the beginning of the session provides a balanced estimation with certain outcomes:

- Legitimate users get rid of annoying and unnecessary authentication steps
- Suspicious users undergo additional verification
- The most suspicious activities are subject to strong verification and may be denied access

Kaspersky Fraud Prevention provides you with valuable data and knowledge to spot anomalies and suspicious behavior before any fraud is even committed.

Account takeover and fraud prevention

Digital technology is now ubiquitous. Millions of users globally are choosing tablets and mobile phones to access services and personal accounts. One of the most business-critical tasks nowadays is to create the right conditions for users:

- Fast and seamless access to personal accounts
- User-friendly authentication methods
- Confidence that the services being used are safe

Kaspersky Advanced Authentication is designed to improve the user experience, cut the costs of second-factor authentication and continuously detect suspicious activity, enabling business growth and a higher level of security.

Functional components of Advanced Authentication:

- **Risk-Based Authentication** eliminates additional authentication steps for legitimate users, giving them access to a session with minimal friction. Continuous analysis of hundreds of parameters in real time enables a dynamic risk assessment. Actions that differ from the behavior of a legitimate user based on a number of indicators are considered to be potentially fraudulent and are subject to additional verification.

- **Continuous Authentication** provides a higher level of security during the whole session. It analyzes behavioral data, device reputation and other valuable non-personalized information that is processed by **Kaspersky Fraud Prevention**. If there are signs of abnormal or suspicious behavior, the Advanced Authentication component automatically sends the appropriate verdicts to the authentication services with a request for the second factor to stop potentially illegal use of the personal account.

- **Account Takeover Detection** enabled by Advanced Authentication informs you who is behind a device: a legitimate user or a fraudster. The solution is able to identify new devices with a unique device fingerprinting functionality. Additionally, the real-time analysis of behavioral data determines deviations from the typical user behavior. In the event of fraudulent activity, the system initiates a log-out.

Transparency & Fraud Analytics for Anti Money Laundering*
***Additional Advanced Service**

With entity-linking functionality and device fingerprinting, **Kaspersky Fraud Prevention** reveals groups of accounts accessed from a single PC or mobile device. Behavioral analysis enhances the detection rate, meaning good users can be separated from fraudsters. Thanks to global device reputation, **Kaspersky Fraud Prevention** also detects links between money mules across companies stopping cross-organizational fraud schemes.

This tool, which helps perform a thorough analysis of blockchain transactions, is available to users of the Transparency & Fraud Analytics package.

Blockchain Analytics provides graphic data about all blockchain transactions to monitor activities and trace those that are unreliable. Data is directly extracted from the public blockchain node and processed in order to be applicable for data mining, information retrieval, graph analysis and machine learning.

Benefits from automated fraud analytics:

- Real-time detection of suspicious activity even before fraud has actually damaged the business
- More fraud scenarios detected with a higher level of accuracy
- Detection of fraudulent groups with global device reputation and extended fingerprinting
- Detection of cross-organizational money laundering scenarios
- Generation of ready-to-use incidents feeding your internal monitoring solutions
- Advanced incident investigation capability with comprehensive GUI

We provide incident response best practices and train your team to manage cybersecurity risks

- Identifying compromised resources.
- Isolating the threat.
- Preventing the attack from spreading.
- Finding and gathering evidence.
- Analyzing the evidence and reconstructing the incident's chronology and logic.
- Analyzing the malware used in the attack (if any malware is found).
- Uncovering the sources of the attack and other potentially compromised systems (if possible).
- Conducting tool-aided scans of your crypto-exchange application and web layer to reveal possible signs of compromise.
- Analyzing outgoing connections between your platform and external resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial actions you can take.

While there is a possibility that an attack may be missed, the cybersecurity team needs to be ready to respond. The awareness and ability to defend against threats is achieved by continuous work by experts and the involvement of your IT personnel in the response process.

Kaspersky Incident Response

Sometimes it's almost impossible to prevent an attack, but it's in our power to limit the resulting damage. The overall aim of incident response is to reduce the impact of a security breach or an attack on your IT environment and to eliminate any malware.

The service covers the entire incident investigation cycle, from the onsite acquisition of evidence to the identification of additional indicators of compromise, preparing a remediation plan and completely eliminating the threat to your organization.

You can ask our experts to execute the complete investigation cycle, to simply identify and isolate compromised machines and prevent dissemination of the threat, or to conduct Malware Analysis or Digital Forensics.

Incident response SLA. Our team of experts will offer you immediate assistance in reducing the impact of an attack on your IT environment. Includes 40 hours of remote assistance by Kaspersky Lab experts.

- **Incident response.** Instant response until complete elimination of any threat.
- **Digital forensics.** Reconstruction of the attack timeline and logic, revealing the cause of the incident.
- **Threat analysis and recommendations.** Development of recommendations on how to protect your IT environment, based on the specific threat's behavior and ability to gain functionality.

An incident takes place in a simulated real-life environment, with the course covering the following topics that arise from that scenario:

- Incident response process and its workflow
- The differences between normal threats and APTs
- APT Cyber Kill Chain
- The incident response process for different incident scenarios
- Cyber Kill Chain for the simulated environment
- Live analysis on victim machines for first responders
- Forensically sound evidence-acquisition techniques
- Post-mortem analysis and digital forensics
- Memory forensics
- Log file analysis with regular expressions and ELK
- Cyberthreat intelligence
- IoCs (indicators of compromise), with YARA and SNORT
- Malware analysis and sandboxing
- Network traffic forensics
- Incident analysis reporting and recommendations on building CSIRT
- Test of the newly gained skills using another simulated scenario

Kaspersky Security Training

IT security staff need to be skilled in the advanced techniques that form a key component of effective enterprise threat management and mitigation strategies.

- Online interactive training for personnel not directly involved with security issues. They also need to have knowledge of the latest security techniques to be able to respond and make decisions in case of intrusions or data leakage.

- Tech guys and security pros can be subscribed to the online education platform for advanced training. Teach your staff with a technical background to think and act as incident responders.

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.

Improve the expertise of your in-house digital forensics and incident response team.

Courses are designed to fill experience gaps:

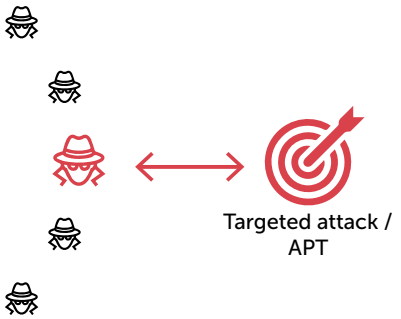
- Developing and enhancing practical skills in searching for digital cybercrime tracks;
- Analyzing different types of data for restoring attack timelines and sources.

Having completed the course, students will be able to successfully investigate computer incidents and improve the security level of the business.

These two types of education reduce the potential costs of a cyber-incident and decrease recovery time.

- **Up to 90%** reduction in the total number of incidents
- **At least a 50%** reduction in the financial impact of incidents
- **More than 30-fold** increase in ROI from security awareness
- **An amazing 86%** of participants willing to recommend the experience

Protect your system from targeted attacks and APTs



KATA

- 24x7 monitoring and support by Kaspersky Lab experts
- Timely and accurate detection of attacks
- Immediate protection against any detected threat
- Automatic antivirus database updates

Unique ongoing access to our investigations and discoveries

Full technical data in a range of formats, on each APT as it's revealed

Includes all those threats that will never be made public

Kaspersky Threat Attribution Engine
instantly links a new attack to a known APT malware, previous targeted attacks and hacker groups.

Kaspersky® Anti Targeted Attack

Kaspersky® APT Intelligence Reporting

Organized crime takes crypto-threats to a new level

According to a Chainalysis report, two professional hacking groups have emerged on the market. As of early 2019 these groups were responsible for a series of attacks causing damage of around $1 billion and accounting for at least 60% of all publicly reported hacks.

The average amount of stolen funds is equivalent to $90 million. Over a period of several months the cryptocurrency is redeployed between a large number of wallets to cover the criminals' tracks and then cashed out.

The organization of malicious activity is constantly improving, with cybercriminals gaining larger and more efficient resources. It means future attacks are expected to be much more sophisticated and powerful.

Kaspersky Anti Targeted Attack Platform features

Automated aggregation of essential telemetry and data across the entire network

The platform leverages network and endpoint data to deliver complete visibility across distributed enterprise networks for early threat detection and comprehensive response. Objects can be collected through SPAN, ICAP, POP3S or SMTP. Suspicious objects can also be extracted from third-party systems' custom connectors.

Multi-dimensional advanced detection

Based on leading security intelligence and advanced machine learning technologies, the Kaspersky Anti Targeted Attack Platform combines network and endpoint data, sandbox and intelligent analysis to correlate incidents, search for indicators of compromise and help uncover the most complex targeted attacks. Connecting up the various pieces of an incident provides a comprehensive view of the entire attack chain, increasing confidence in assigned threat scores and reducing false positives to zero.

Kaspersky Anti Targeted Attack Platform delivers a new strategic approach to detecting targeted attacks

Complemented by our multi-layered prevention technologies and solutions, as well as an extensive portfolio of **Security Intelligence Services** for response and prediction, **Kaspersky Lab** delivers a truly integrated, strategic approach to targeted attacks and to threat detection and response.

Based on leading security intelligence and advanced machine learning technologies, **Kaspersky Anti Targeted Attack Platform** combines network data, sandbox and intelligent analysis to correlate incidents, search for indicators of compromise and help uncover the most complex targeted attacks. Connecting up the various pieces of an incident provides a comprehensive view of the entire attack chain, increasing confidence in assigned threat scores and reducing false positives to zero.

The **Kaspersky Anti Targeted Attack Platform** includes:

- **Multi-layered sensor architecture** – to give 'all round' visibility. Through a combination of network, web and email, and endpoint sensors, **Kaspersky Anti Targeted Attack Platform** provides advanced detection at every level of your corporate IT infrastructure.
- **Advanced Sandbox** – to assess new threats. The result of over a decade of continuous development, our Advanced Sandbox offers an isolated, virtualized environment where suspicious objects can be safely executed so their behavior can be observed.
- **Powerful analytical engines** – for rapid verdicts and fewer false positives. The Targeted Attack Analyzer assesses data from network and endpoint sensors and rapidly generates threat detection verdicts for the security team.

Discover who's behind an attack with **Kaspersky Threat Attribution Engine**

This is a high-performance genotyping code classifier that can instantly link a new attack to known APT malware, previous targeted attacks and hacker groups.

For instance, in 2015, Kaspersky Lab experts managed to discover a connection between a malicious program for Windows called Octopus and the group of attackers we named DustSquad. That was made possible with our Kaspersky Threat Attribution Engine.

Automated prevention of advanced threats and comprehensive response

Kaspersky Anti Targeted Attack Platform can automatically share verdicts with traditional security Kaspersky Lab solutions via an on-premise intelligence sharing layer – Kaspersky Private Security Network. This tight integration from global network to endpoint level, between Kaspersky Anti Targeted Attack Platform, Kaspersky Security for Mail Gateway, Kaspersky Endpoint Security, Kaspersky security for Virtualization and Kaspersky Endpoint Detection and Response, means immediate, informed action can be taken when an incident emerges.

Kaspersky APT Intelligence Reporting delivers exclusive, proactive access to descriptions of high-profile cyber-espionage campaigns, including indicators of compromise (IOCs) and YARA rules.

Kaspersky Lab has discovered some of the most relevant advanced persistent threat (APT) attacks ever. However, not all APT discoveries are reported immediately, and many are never publicly announced.

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

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 they are all reported to our customers.
- Detailed supporting technical data including an extended list of indicators of compromise (IOCs), available in standard formats including OpenIOC or STIX, and access to our YARA rules.

Ongoing threat monitoring and cybersecurity incident mitigation by the crypto Security Operations Center (SOC)

Kaspersky Threat Data Feeds service highlights:

- Data feeds littered with false positives are valueless, so extensive tests and filters are applied before releasing feeds, to ensure 100% vetted data is delivered;
- Data feeds are automatically generated in real time, based on findings across the globe (Kaspersky Security Network provides visibility to a significant percentage of all internet traffic, covering tens of millions of end users in more than 213 countries) providing high detection rates and accuracy;
- All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability;
- The data feeds allow immediate detection of URLs used to host phishing, malware, exploits, botnet C&C URLs and other malicious content;
- Malware in all types of traffic (web, email, P2P, IM, etc.) and targeted at mobile platforms can also be instantly detected and identified;
- Simple lightweight dissemination formats (JSON, CSV, OpenIoC, STIX) via HTTPS or ad-hoc delivery mechanisms support easy integration of feeds into security solutions;
- Hundreds of experts, including security analysts from across the globe, world-renowned security experts from the GReAT team and leading-edge R&D teams, contribute to the feeds. Security officers receive critical information and alerts generated from the highest quality data, with no risk of being deluged by superfluous indicators and warnings;
- Ease of implementation. Supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky Lab all combine to enable straightforward integration.

Threats are constantly evolving and challenging developers. Your cybersecurity team needs up-to-the-minute data to manage new risks and inform investors about possible dangers.

Kaspersky Threat Data Feeds give you access to the most relevant data on cyberthreats

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.

Continuously updated **Kaspersky Threat Data Feeds** inform you about risks and implications associated with cyberthreats.

Feeds comprise:

- **IP Reputation Feed** — a set of IP addresses covering suspicious and malicious hosts with the corresponding threat context;
- **Malicious and Phishing URL Feed** — covering malicious and phishing links and websites;
- **Ransomware URL Feed** — covering links that host ransomware objects or that are accessed by them;
- **APT IoC Feeds** — covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks;
- **Passive DNS (pDNS) Feed** — a set of records that contain the results of DNS resolutions for domains and the corresponding IP addresses;
- **Malicious Hash Feed** — covering the most dangerous, prevalent and emerging malware;
- **Whitelisting Data Feed** — providing third-party solutions and services with a systematic knowledge of legitimate software.

What you get:

- **Reinforce your network defense solutions**, including SIEMs, Firewalls, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated indicators of compromise (IOCs) and actionable context, delivering insights into cyberattacks and a greater understanding of the intent, capabilities and targets of your adversaries;
- **Help to mitigate targeted attacks.** Enhance your security posture with tactical and strategic threat intelligence by adapting defensive strategies to counter the specific threats your organization faces;
- Use threat intelligence **to detect malicious content hosted on your networks**;
- **Prevent the exfiltration of sensitive information and assets;**

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 they are all reported to our customers.
- Detailed supporting technical data, 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 an investigation (information on APT distribution, IOCs, C&C infrastructure).
- Contents for different audiences. Each report contains an executive summary describing the related APT. This summary is followed by a detailed technical description of the APT with the related IOCs and YARA rules giving security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable advice for superior protection from the related threat.
- Retrospective analysis. Access to all previously issued private reports is provided throughout the period of your subscription.
- Threat Intelligence Portal. All the reports, including the most recent IoCs, are available via our Threat Intelligence Portal or via its RESTful API, creating a seamless user experience for our customers.

Note – Subscriber Limitation

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

- **Conduct deep searches into threat indicators** such as command-and-control protocols, IP addresses, malicious URLs or file hashes, with a human-validated threat context that allows the prioritization of attacks;

- Use our expertise and actionable contextual intelligence to **enhance the protection delivered by your products and services** such as web content filtering, spam/phishing blocking, etc.

Note that attackers can disclose information about your project in public sources and on the DarkNet.

With **Digital Risks Snapshot**, a detailed quarterly report on everything we gather about your project in public sources and on the DarkNet, you will be informed immediately about reputational and cybersecurity risks.

Kaspersky Threat Lookup web portal provides access to all knowledge acquired by **Kaspersky Lab** about threat indicators and their relationships.

Based on validated security intelligence data, Kaspersky Threat Lookup provides an effective tool for enterprises to improve their incident response and forensics.

Several petabytes of global security intelligence data is updated almost in real time.

This always-on web service helps businesses to properly analyze digital evidence in light of a security incident and obtain the insights needed to speed up detection and remediation.

Once suspicious indicators such as an IP, URL or file hash have been identified by a corporate IT security officer, they can be entered into the service web interface. In return, users are provided with meaningful and structured information about a potential threat, as well as global insights that help identify a targeted attack in progress.

Kaspersky Threat Lookup offers enterprises the same level of intelligence that Kaspersky Lab specialists use to analyze the most sophisticated threats, and includes indicators of compromise for these new attacks.

- Kaspersky Lab's security intelligence is collected from various sources including Kaspersky Lab's cloud security network, spam traps, botnet monitoring initiatives and web crawlers.

- The data is constantly cross-checked by Kaspersky Lab's own research team and automatically correlated.

- Quickly investigate the source of the problem, distinguish between potentially malicious and benign actions, and obtain data for fast and efficient incident investigation.

- Prioritize and act efficiently even when the number of alerts reaches hundreds or thousands per day.

- Obtain access to large databases of malicious objects as well as clean objects (part of the Kaspersky Whitelist service).

Incident Response

The course will guide your in-house team through all of the stages of the incident response process and equip them with the comprehensive knowledge needed for successful incident remediation.

An incident will take place in a simulated real-life environment, with the course covering the following topics that arise from the scenario:

- The incident response process and its workflow
- Differences between normal threats and APTs
- APT Cyber Kill Chain
- Incident response processes for various incident scenarios
- Cyber Kill Chain in the simulated environment
- Live analysis on victim machines for first responders
- Forensically sound evidence-acquisition techniques
- Post-mortem analysis and digital forensics
- Memory forensics
- Log file analysis with regular expressions and ELK
- Cyberthreat intelligence
- IoCs (indicators of compromise), with YARA and SNORT
- Malware analysis and sandboxing
- Network traffic forensics
- Incident analysis reporting and recommendations on building CSIRT
- Test of newly gained skills using another simulated scenario

Skills you gain with our courses:

- Understanding of incident response phases
- What to consider when responding to a cyber-incident
- Understanding of various attack techniques and targeted attack anatomy through the Cyber Kill Chain
- How to respond to different incidents with appropriate actions
- The ability to differentiate APTs from other threats
- Confirming cyber-incidents using live analysis tools
- Understanding the difference between live analysis and post-mortem – and when to apply them
- Identifying digital evidence; HDD, memory and network traffic with an introduction to their forensic analysis
- Writing YARA and SNORT IOCs for a detected attack
- Log file analysis
- Understanding of the process involved in building an IR team

Use comprehensive measures for better crypto-exchange security

Meet all the safety and reliability requirements for crypto-investor asset management. With the newest Kaspersky Lab solutions you can build a sustainable and resilient system that provides secure transactions and asset storage.

Protect your applications

Kaspersky®
Security Assessment

Identify weak points in your system

Kaspersky®
Penetration Testing

Track malicious activity on the Web

Kaspersky®
Phishing Detection

Keep access to your system secure

Kaspersky®
Fraud Prevention

Respond to attacks effectively

Kaspersky®
Incident Response

Kaspersky®
Cybersecurity
Training

Address targeted attacks and APTs

Kaspersky®
Anti Targeted
Attack

Kaspersky®
APT Intelligence
Reporting

Continuously monitor and be ready to address threats

Kaspersky®
Threat Data Feeds

Kaspersky®
Threat Lookup

Protect your applications with Kaspersky Security Assessment

A comprehensive audit to identify flaws and vulnerabilities in application, web-layer and network security. It helps prevent a wide range of attacks and errors related to both client-side and server-side vulnerabilities.

Identify weak points in your system using Kaspersky Penetration Testing

Multiple stages of testing can discover entry points for attackers. Mitigate the risk and fix flaws before they are exploited.

Track malicious activity on the Web with Kaspersky Phishing Detection

During a crowdsale Kaspersky Phishing Detection protects you and your investors from probing by malware, fake ICO websites, in-browser scripts, massive data leaks, crypto theft and commercialization of APTs.

Keep access to your system secure with Kaspersky Fraud Prevention

Ensure a seamless user experience for legitimate clients and protect interaction with your exchange. Account takeover (ATO) detection powered by real-time discovery of early signs of an ATO and other malicious activities.

Respond to attacks with Kaspersky Incident Response, Cyber-Hygiene Education and Security Training

Kaspersky Incident Response includes ongoing security mechanisms and algorithms that help to stop a threat spreading within the system or network and minimize damage.

To enhance efficiency and professionalism, your security specialists can take our cybersecurity course. It delivers hands-on experience that is indispensable when it comes to real threats.

Address targeted attacks and APTs effectively

Kaspersky Anti Targeted Attack Platform delivers a new, strategic approach to detecting targeted attacks.

Increase your awareness and knowledge of high-profile cyber-espionage campaigns with comprehensive and practical **APT Intelligence Reporting** from **Kaspersky Lab**.

Continuously monitor and be ready to immediately address threats with Kaspersky Crypto Security Operations Center (SOC)

Kaspersky Threat Data Feeds provide continuously updated data feeds informing you about the risks and implications associated with cyber threats.

The Kaspersky Threat Lookup web portal gives you access to petabytes of global security intelligence data.

Improve your malware analysis skills with the Kaspersky Incident Response course.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com