Kaspersky for Business

A comprehensive solution for protecting Token Offering projects from various threats

Kaspersky Token Offering Security

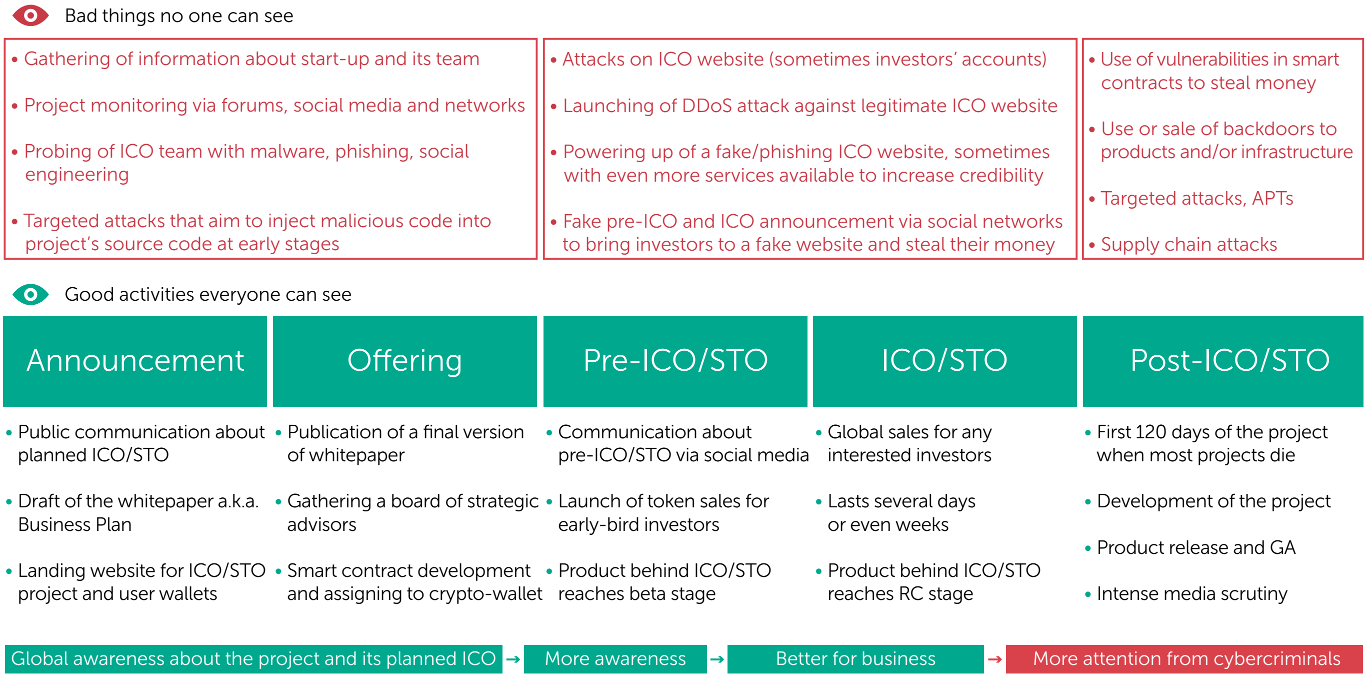
www.kaspersky.com
#truecybersecurity

A modern way of raising funds for developing projects

In the world of cryptocurrency, a Token Offering most of the times means initial coin offering (ICO) or secure token offering (STO) which are similar to initial public offerings (IPO) used by traditional businesses. ICOs and STOs use cryptocurrencies instead of government-issued fiat currencies. Companies start Token Offering to raise capital from investors. They can either use their newly issued cryptocurrency to buy regular national currency, such as US dollars, or another cryptocurrency, such as Bitcoin or Ether.

Relative to ICO utility tokens, which only allow investors to purchase issuer products or speculate on the crypto-exchange, security token offerings (STO) are becoming increasing popular. Security tokens give investors more privileges than traditional securities, such as a share in profits, voting rights, dividends or interest payments.

ICOs and STOs raise billions of US dollars every year. Despite the volatility of cryptocurrencies, investor interest remains strong and the number of offerings is increasing.



Bad things no one can see

- Gathering of information about start-up and its team
- Project monitoring via forums, social media and networks
- Probing of ICO team with malware, phishing, social engineering
- Targeted attacks that aim to inject malicious code into project's source code at early stages

- Attacks on ICO website (sometimes investors' accounts)
- Launching of DDoS attack against legitimate ICO website
- Powering up of a fake/phishing ICO website, sometimes with even more services available to increase credibility
- Fake pre-ICO and ICO announcement via social networks to bring investors to a fake website and steal their money

- Use of vulnerabilities in smart contracts to steal money
- Use or sale of backdoors to products and/or infrastructure
- Targeted attacks, APTs
- Supply chain attacks

Good activities everyone can see

Announcement	Offering	Pre-ICO/STO	ICO/STO	Post-ICO/STO
• Public communication about planned ICO/STO	• Publication of a final version of whitepaper	• Communication about pre-ICO/STO via social media	• Global sales for any interested investors	• First 120 days of the project when most projects die
• Draft of the whitepaper a.k.a. Business Plan	• Gathering a board of strategic advisors	• Launch of token sales for early-bird investors	• Lasts several days or even weeks	• Development of the project • Product release and GA
• Landing website for ICO/STO project and user wallets	• Smart contract development and assigning to crypto-wallet	• Product behind ICO/STO reaches beta stage	• Product behind ICO/STO reaches RC stage	• Intense media scrutiny

Global awareness about the project and its planned ICO → More awareness → Better for business → More attention from cybercriminals

Token Offering vulnerabilities

Crypto-fundraising is associated with a variety of threats at every stage – from product development and the ICO/STO announcement to the end of a token sale.

Announcement

While you communicate with the public about a planned ICO/STO and release a draft whitepaper, hackers can be gathering information about the project and its team. They develop social engineering attacks, probing the team with malware, phishing and social engineering. The hackers may try to penetrate the project and inject malicious code into its source code.

Pre-offering & offering

When you launch a website for your ICO, there may be attempts to disrupt its work with DDoS attacks. Hackers may launch a phishing website or send fake or phishing announcements to your investors.

Post-offering

The largest attacks are often due to flaws in smart contracts. They can either disrupt transactions or be exploited by hackers. In addition to smart contract vulnerabilities, the product itself may be exposed to APTs, targeted attacks or supply-chain attacks.

Under the hood — Ethereum

Most of the times, Token Offering project, including ICO and STO has a smart contract – a program written for a blockchain that contains regulations on how the parties involved interact with each other.

Most users tend to view Bitcoin simply as a fund transfer service where users can quickly and cheaply send money to one another. Strictly speaking, BTC has a sort of contract functionality, but it differs significantly from Ethereum. Ethereum-based smart contracts have become the de-facto standard for ICO/STO.

Smart contracts are mostly written in the Solidity programming language to facilitate the transfer of money between wallets automatically. These programs operate in the same way for every user and, most importantly, function according to known and predictable principles that are transparent and consistent for all users.

Smart contracts provide a high level of reliability. The source code can be viewed by anyone and can be checked to confirm it works as intended.

Make your systems resilient with Kaspersky Security Assessment services

Smart contract vulnerabilities

Typically, the majority of attacks are caused by developers' mistakes at the Solidity code creation stage.

There are more than a dozen serious flaws in smart contracts that, if exploited, could halt all transactions and entail multi-million dollar losses.

Dr. Adrian Manning collects information about known attacks in his Solidity Security Blog on github. A number of experts describe this as the most relevant knowledge on the Web. Others look to DASP Top 10 vulnerabilities. Below is a list of the most common issues:

Sources:
github.com/sigp/solidity-security-blog
https://dasp.co/index.html

Example of a reentrancy attack

Let's take a look at a sample contract

```
contract Victim {
  mapping(address => uint)
  private balances;

  function deposit() public
  payable {
    balances[msg.sender] +=
    msg.value;
}

  function withdraw(uint _
  amount) public {
    require(balances[msg.
    sender] >= _amount);
    require(msg.sender.call.
    value(_amount)());
    balances[msg.sender] -=
    _amount;
    }
}
```

The `withdraw() function` allows users to subtract their balance.

This happens after the function makes an external call `msg.sender.call.value(_amount)`.

Start with **Kaspersky Smart Contract Review** to protect investor funds

A smart contract is code, usually written in the Solidity programming language, for an Ethereum-based blockchain that represents a set of rules for purchasing, storing and transferring crypto-assets. As one of the main components of any ICO or STO – and therefore a prime target for attacks – it needs high-level protection.

Whether you develop smart contracts or applications internally, or order them from third parties, you'll know that a single bug or malicious injection can cause vulnerabilities that could result in considerable financial or reputational damage.

What threats is your smart contract exposed to?

Token Offering projects are often targeted by attackers exploiting vulnerabilities and flaws in smart contracts. Understanding how bugs in the code 'work' helps fraudsters steal large amounts of crypto-assets.

According to the DASP Top 10 vulnerabilities and the Solidity Security Blog, there are a number of smart contract vulnerabilities that pose significant risks to projects:

Reentrancy

A smart contract can not only call wallets but also external contracts. If those contain a malicious fallback function, they can force the initial victim-contract to execute further code. The function re-enters the contract withdrawing ether until the balance is depleted.

Arithmetic overflows and underflows

Some operations require a fixed size variable. For example, a uint8 stores numbers or other data whose size is between 0 and 255. When you add or subtract a number, the result still needs to be between 0 and 255; it can't be negative or exceed 255. It's like going around in a circle.

But what if an attacker decides to initiate a loop during this step? This is possible with another malicious contract which the victim contract calls:

```
Import “Victim.sol”;

contract Malicious {
  Victim public victim;

  constructor(address
  victimAddress) {
    victim =
    Victim(victimAddress);
  }

  function loop() external {
    require(msg.value >=
    1 ether);
    victim.deposit.
    value(1 ether)();
  }

  function() payable {
    if (victim.balance != 0 ) {
      victim.withdraw(1 ether);
    }
  }
}
```

By calling the malicious contract the victim contract triggers any payable fallback function in it. This function calls back `Victim.withdraw()` again and again. The balance of our second contract just hasn't been updated yet, so the attacker is able to drain it.

The DAO reentrancy case

In June 2016, the DAO refund mechanism was exploited. An Ethereum-based smart contract of two steps was able to return Ethereum to the investor. Then it took the tokens from an investor's wallet. The hacker repeated the first step, which wasn't added to blockchain until he gained $79.6 million.

The Ethereum foundation was forced to make a hard fork. That was the history behind the creation of Ethereum Classic.

Source: http://uk.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6

The Parity Multisig WalletLibrary reentrancy case

The user devops199 accidentally locked funds worth $154 million because of this bug. He removed initWallet from blockchain, preventing the contract from sending funds.

Source: https://motherboard.vice.com/en_us/article/ywbqmg/parity-multi-signature-wallet-vulnerability-300-million-hard-fork

Default visibilities

Functions in Solidity have visibility preferences. By default, any function is public if no condition is set. This feature may be a source of problems if a function that has to be private doesn't have a proper attribute.

Other known vulnerabilities include access control, unchecked low level calls and many other issues.

We check and confirm the smart contract:

- ✓ Implements business logic as described in Whitepaper
- ✓ Does not have undeclared features
- ✓ Does not have known vulnerabilities
- ✓ Uses methods safe from reentrance attacks
- ✓ Follows best practices in efficient use of gas
- ✓ Implements and adheres to the existing ERC-20 token standard
- ✓ Documentation and code comments match logic and behavior

Kaspersky Smart Contract Review

In the event of a serious attack, a fork is a possible solution. It is an attempt to make those tokens or assets that are suspected of being stolen unavailable for transactions. But this is always an extreme measure with mixed outcomes that makes preventing an exploitation a more desirable way to mitigate risks.

The **Kaspersky Smart Contract Review** process consists of the following stages:

- Identification of known security vulnerabilities and design flaws that may lead to possible exploitation.
- Identification of undocumented features that are not declared in the corresponding Whitepaper document.
- Provision of a report listing found vulnerabilities, design flaws and undocumented features.
- Provision of recommendations for the mitigation of discovered vulnerabilities, design flaws and undocumented features.

We check and confirm the smart contract:

- Does not have known vulnerabilities.
- Uses methods safe from reentrance attacks.
- Follows best practices in efficient use of gas.
- Implements and adheres to the existing ERC-20 token standard.
- Documentation and code comments match logic and behavior.
- Does not have undeclared features.

Results are provided in a final report including detailed technical information on the assessment processes, results, discovered vulnerabilities and recommendations for remediation, together with an executive summary outlining management implications.

The recommendations can help fix ambiguous functions and add security barriers that will make a potential exploitation much more difficult for attackers.

Why is a fork needed?

When an attack occurs that causes serious damage, a hard fork is a possible solution.

The problem is that once a contract has been deployed, there is no way of editing it. You may then have to create another blockchain protocol that won't be compatible with the previous version of the software.

Investors do not like such measures, so it's important to prevent hacks.

ICOs/STOs are vulnerable to various threats and the damages can be serious

Ernst & Young analyzed 372 ICOs around the world

EY analyzed a variety of material, including public sources, exchanges, data aggregators, ICO reports, ICO trackers, news websites, blockchain networks and platforms, as well as social networks. The analysis shows that in 2017, of the $3.7 billion raised, 10% (or almost $400 million) was stolen or lost.

Source: Ernst&Young

During the investigation into the CoinDash attack, malicious Webshell code was discovered inside the 404.php file.

CoinDash announced on its blog that as part of an initial token offering, an Ethereum smart contract contribution address would be made available to the public following a 30-minute period for "whitelisted" users. Just as the address was about to be revealed, attackers switched the official contribution address to a different address. Because of high demand, the anonymous address managed to collect 43,000 Ether. When the hack was detected, the site was shut down by the administrators. During the seven minutes the address was live, the hackers managed to steal $7 million from CoinDash.

Source: CoinDash

Use **Kaspersky Application Security Assessment** to address flaws and protect your product from attacks

At the heart of any Token Offering project is the product which implements a complicated fundraising procedure. No CEO wants their project to fail and disappoint investors. It's extremely important to ensure the functionality and sustainability of the project. Our experts will do their best to assess the source code and suggest the best security solutions.

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

By 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
- Infiltration and modification of data and systems
- Denial of service attacks
- Fraudulent activities

A wide range of vulnerabilities may be identified by the **Kaspersky Application Security Assessment** service:

- Client-side and server-side vulnerabilities are often exploited by code injection (e.g. SQL Injection, OS Commanding), Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), etc.

- There is a risk of logical vulnerabilities leading to fraud. They might not be identified at the development and testing stages.

- There are a number of web application vulnerabilities leading to the threats listed in WASC Threat Classification v2.0 and the OWASP Top Ten.

What you get:

- Avoid financial, operational and reputational loss, by proactively detecting and fixing the vulnerabilities used in attacks against applications.

- Save on 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.

Results are provided in a final report:

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

Kaspersky Penetration Testing identifies weak points of the system

Kaspersky 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.

Avoid possible risks, financial and reputational losses by preventing attacks.

- **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 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 will visit your site and analyze Wi-Fi security controls.

Protect your project and investors from phishing

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 the phishing URL is targeted at;
  - first seen timestamp;
  - last seen timestamp;
  - popularity of the phishing URL;
  - geolocation of users that are affected by the phishing URL;
  - type of stolen data (credit cards info, credentials for bank, email or social network, personal info, etc.);
  - attack type (a threat to block an account, an offer to download a file, a request to update personal info, etc.);
  - resolved IP addresses of the phishing URL;
  - WHOIS data;
  - and much more.

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

While awareness about your project is increasing, interest from cyberattackers will also be growing.

During the launch of your Token Offering project, you go from putting together a team to the first announcement and then move on to the token sale itself.

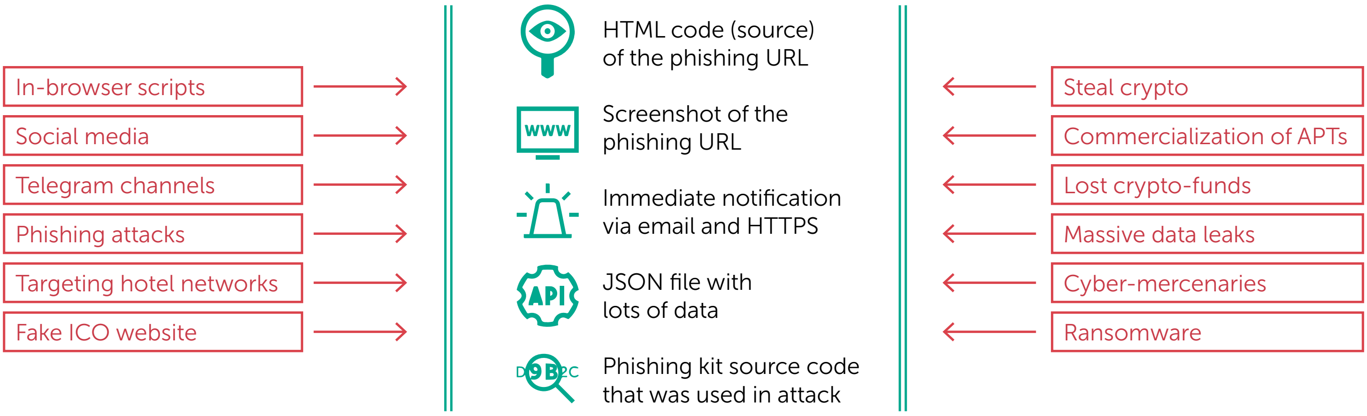
You have to develop various systems and modules, make decisions and communicate constantly with partners and investors. While you may believe you have thought of all the possible features, including security mechanisms, cybercriminals are working out how to break your systems.

You may face a wide range of risks at any stage of the project and it is crucial to be ready to respond.

Every participant in a Token Offering, particularly in ICO or STO, is a potential victim of sophisticated phishing attacks

There are a lot of risks caused by errors, malfunctions or malicious activity from both inside and outside the project.

Kaspersky®
Phishing Detection



In-browser scripts
Social media
Telegram channels
Phishing attacks
Targeting hotel networks
Fake ICO website

HTML code (source) of the phishing URL
Screenshot of the phishing URL
Immediate notification via email and HTTPS
JSON file with lots of data
Phishing kit source code that was used in attack

Steal crypto
Commercialization of APTs
Lost crypto-funds
Massive data leaks
Cyber-mercenaries
Ransomware

Probing a project team with malware, phishing, social engineering

Cybercriminals are able to gather information about a start-up and its team, monitoring it via forums, social media and networks, and then develop social engineering attacks.

At the beginning, the process of fundraising is only about to start and there are no investor assets that can be stolen. But this period can be useful for attackers to gather sensitive information and credentials that can be used later to penetrate the system or take control of it.

Be aware of fraudulent ads! Google has detected billions of display ads which led to malware downloads.

Google in its 2017 annual BadAds report stated that it removed 1.7 billion malicious and misleading ads in 2016, compared to 780 million in 2015. "Trick to click" ads are among the most dangerous and may look like system error notifications that make users download malware. The downloaded virus, such as a Trojan, will scan the computer for passwords and any other valuable data in just a few minutes unless the computer has strong phishing protection.

Source: blog.google

Phishing websites, fake Token Offering announcements

The most common phishing method is to distribute fraudulent offers through social media and email. The victim finds or receives a message encouraging them to become a partner of a particular crypto-project or to make a profit. The link in the message leads to a fake website masquerading as a genuine cryptocurrency website

Using the cutting-edge **Kaspersky Phishing Detection** it is possible to track fake resources and send alerts immediately

- Accurate and detailed ongoing 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 synthesizes data from heterogeneous, highly reliable intelligence sources.

- Kaspersky Security Network (KSN)
- Powerful heuristic engines
- Email honeypots
- Web crawlers
- Spam traps
- Research teams
- Partners
- Historical data for almost two decades

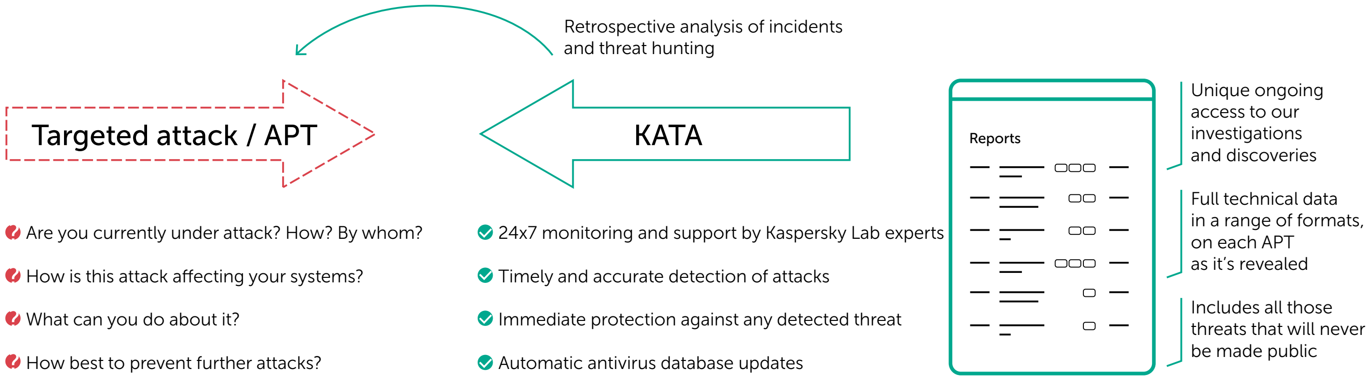
Kaspersky Phishing Detection gives you a critical edge against your attackers.

- Critical **information is provided in real time** and through regular reporting on malicious activities that indicate that 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, all helping your online customers feel better protected and reassured.

- 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.

Tackle Advanced Persistent Threats (APTs) and targeted attacks effectively. Protect your ICO/STO website from DDoS attacks.


Retrospective analysis of incidents and threat hunting
Targeted attack / APT
KATA
Reports
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

- Are you currently under attack? How? By whom?
- How is this attack affecting your systems?
- What can you do about it?
- How best to prevent further attacks?

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

Kaspersky® Targeted Attack Discovery

Kaspersky® Anti Targeted Attack

Kaspersky® APT Intelligence Reporting

Botnet tracking to prevent DDoS attacks

Typically, DDoS attacks are executed by networks infiltrated by malware called botnets.

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, etc.
- 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 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.
- Geographical distribution of detection (top 10 countries) — Statistical data of related malware samples from around the world.

Kaspersky Targeted Attack Discovery

Intruders may be aiming at long-term results. They get closer to a critical system or data step by step, overcoming security barriers following a well-thought-out plan.

For instance, spear-phishing emails can be used to obtain a development team member's credentials or infiltrate their system. This first step will lead to another stage of an attack unless the overall aim is achieved.

Kaspersky Targeted Attack Discovery results will allow you to identify current cybercriminal and cyberespionage activity in your network, understand the reasons behind it, possible sources of incidents, and effectively plan mitigation activities that will help avoid similar attacks in future. **Kaspersky Targeted Attack Discovery** services are designed to tell you:

- Whether you are currently under attack, how, and by whom
- How this attack is affecting your systems, and what you can do about it
- How best to prevent further attacks

Our globally recognized independent experts will reveal, identify and analyze ongoing incidents, APTs, cybercriminal and cyberespionage activities in your network. They will help you uncover malicious activities, understand the possible sources of incidents, and plan the most effective remedial actions.

Our findings are delivered in a detailed report covering:

- General information confirming your network is compromised or signs that it may be;
- Analysis of the intelligence gathered about threats and indicators of compromise (IOC);
- Description of possible attack sources and compromised network components;
- Remediation recommendations to mitigate the impact of an incident and protect your resources from similar attacks in future.

Kaspersky Anti Targeted Attack

Kaspersky Anti Targeted Attack Platform correlates different events and prioritizes incidents to help organizations detect targeted attacks, advanced threats and already compromised systems.

Kaspersky Anti Targeted Attack Platform provides constant monitoring and analysis of cyberthreats by experts, immediate protection against threats through automatic antivirus database updates.

- A continuously high level of protection against targeted attacks and malware, with 24x7 monitoring and support from your own advanced team of Kaspersky Lab experts.

- The timely and accurate detection of non-malware attacks, attacks involving previously unknown tools and attacks exploiting zero-day vulnerabilities.

- Immediate protection against any detected threat through automatic antivirus database updates.

- Retrospective analysis of incidents and threat hunting, including the methods and technologies used by threat actors against your organization.

- An integrated approach – the Kaspersky Lab portfolio includes all the technologies and services you need to implement a complete cycle of protection against targeted attacks: Preparation – Detection-Investigation – Data Analysis – Automated Protection.

Kaspersky DDoS Protection*

*Available in selected countries

Hackers can exploit distributed systems infected with malware (e.g. Trojans). These networks, called botnets, overwhelm Token Offering websites with an excessive amount of queries, so the servers simply run out of resources. It causes them to lose their protective capabilities and makes them vulnerable.

It is important to implement features like cookies or captchas to identify real users. The next step is integration with services protecting websites from DDoS attacks.

Kaspersky DDoS Protection takes care of every stage of defending your business against all forms of DDoS attack.

During an attack, with all your traffic passing through our cleaning centers:

- Your platform is no longer being overwhelmed by the sheer volume of 'junk traffic'.
- Our cleaning process is identifying and discarding all junk traffic.
- Legitimate traffic is being delivered straight back to you as 'clean'.

The entire process is totally transparent to you.

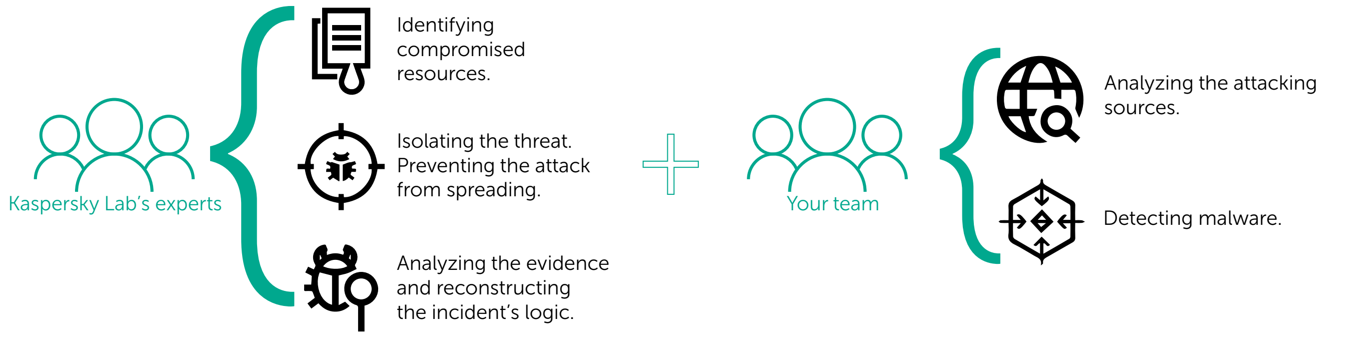
The DDoS attack is effectively neutralized: your business remains fully functional and quite unharmed.

You can ask our experts to engage and execute investigations, identify and isolate compromised modules, prevent threats from spreading and conduct digital forensics.

Improve the incident response process and train your team to act efficiently

Kaspersky®
Incident Response

Kaspersky®
Cybersecurity
Training



Kaspersky Lab's experts

Identifying compromised resources.

Isolating the threat. Preventing the attack from spreading.

Analyzing the evidence and reconstructing the incident's logic.

Your team

Analyzing the attacking sources.

Detecting malware.

The entire incident response cycle

- 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 IT infrastructure to reveal possible signs of compromise.
- Analyzing outgoing connections between your network and external
- resources to detect anything suspicious (such as possible command and control servers).
- Eliminating the threat.
- Recommending further remedial actions you can take.

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.

Kaspersky Incident Response

No one is immune: regardless of how effective your security controls are, you can still become a victim. But it's in our power to limit the resultant damage from attacks, then identify compromised resources, isolate the threat and prevent it from spreading.

The overall aim of **Kaspersky Incident Response** is to reduce the impact of a security breach or an attack on your IT environment.

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.

- **Malware Analysis.** A complete understanding of the behavior and objectives of the specific malware files that are targeting your organization.
- **Digital Forensics.** Kaspersky Lab experts piece together the evidence to understand exactly what's going on, including the use of HDD images, memory dumps and network traces.
- **Delivery options.** Kaspersky Lab's Incident Response Services are available by subscription or in response to a single incident.

Kaspersky Cybersecurity Training

Become highly skilled responders. Our training will help your IT and other personnel to effectively manage cyberthreats, providing practical skills on how to handle attacks.

Online interactive courses help to improve cybersecurity skills even among beginners. The additional security training enables your incident response team to analyze the attacking sources and detect malware.

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.

Prevent damage by using the latest cybersecurity solutions from Kaspersky Lab

Conduct a thorough assessment of your systems

Kaspersky® Smart Contract Review

Kaspersky® Application Security Assessment

Kaspersky® Penetration Testing

Protect your investors from phishing and fraud

Kaspersky® Phishing Detection

mplement comprehensive solutions against attacks

Kaspersky® Anti Targeted Attack

Kaspersky® Targeted Attack Discovery

Kaspersky® APT Intelligence Reporting

Address threats immediately and improve your skills

Kaspersky® Incident Response

Kaspersky® Cybersecurity Training

At no stage of an ICO or STO is your project entirely safe from risks. But it is possible to mitigate those risks by using powerful cybersecurity services.

Conduct a thorough assessment of your systems with Kaspersky Application Security

A Token Offering process consists of many parts, including your product itself, as well as blockchain components and a web application. We provide a security assessment for each component of your project:

- Kaspersky Smart Contract Source Code Review
- Kaspersky Application Security Assessment
- Kaspersky Penetration Testing

Protect yourself and your investors from phishing and fraud with Kaspersky Phishing Detection

Kaspersky Phishing Detection continuously tracks any malicious activity that may be related to your project on the Web and even on the Darknet.

The service continuously tracks and alerts you if phishing sites start targeting your brand. A combination of automated analysis and expert cybersecurity assistance provides immediate alerts, averting any potential financial or reputational losses.

Implement comprehensive solutions against attacks: Kaspersky Targeted Attack Discovery, Kaspersky Anti Targeted Attack and Kaspersky DDoS Protection*

Constant protection by smart services and cybersecurity experts is provided. With Kaspersky Lab's products, you will always be ready to deal with an attack.

Address threats immediately with the help of Kaspersky Incident Response. Improve your cybersecurity skills with Kaspersky Security Training

Should a cyber-incident occur, our pros halt the spread of the threat and help to minimize losses. The Kaspersky Incident Response service provides powerful ongoing support.

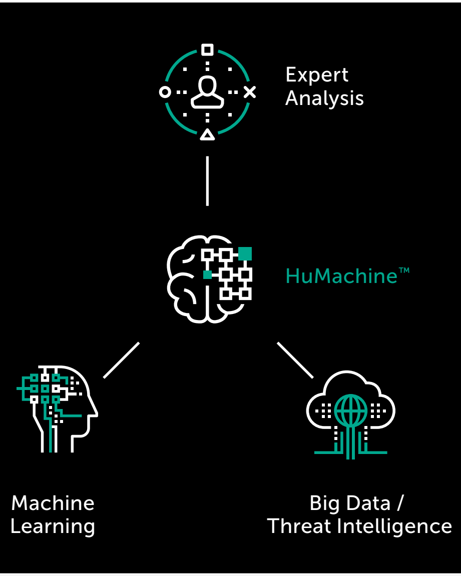
Your IT personnel will be able to resist attacks too. Thanks to the Cyber-Hygiene courses provided as part of Kaspersky Cybersecurity Training, they can learn how to respond in the event of an incident.

* Available in selected countries

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


Expert
Analysis
HuMachine™
Machine
Learning
Big Data /
Threat Intelligence