Kaspersky Threat Intelligence Services

www.kaspersky.com
#truecybersecurity

Kaspersky 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.

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.

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 Threat Intelligence Services include:

- Threat Data Feeds
- APT Intelligence Reporting
- Tailored Threat Reporting
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

Threat Data Feeds

First-tier security vendors and enterprises use time-honored and authoritative Kaspersky Threat Data Feeds to **produce premium security solutions or to protect their business**.

Cyber attacks happen every day. Cyber threats are constantly growing in frequency, complexity and obfuscation, as they try to **compromise your defenses**. Adversaries currently use complicated intrusion **kill chains**, campaigns and customized **Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your clients**.

Kaspersky Lab offers **continuously updated** Threat Data Feeds to **inform your business or clients about risks** and implications associated with cyber threats, helping you to **mitigate threats more effectively** and **defend against attacks** even before they are launched.

Intelligence Cycle

The Data Feeds

Feeds comprise sets of:

- IP Reputation Feed – a set of IP addresses with context covering suspicious and malicious hosts;
- Malicious and Phishing URL Feed – covering malicious and phishing links and websites;
- Botnet C&C URL Feed – covering desktop botnet C&C servers and related malicious objects;
- Mobile Botnet C&C URL Feed – covering mobile botnet C&C servers. Identify infected machines that communicates with C&Cs;
- Malicious Hash Feed – covering the most dangerous, prevalent and emerging malware;
- Mobile Malicious Hash Feed – supporting the detection of malicious objects that infect mobile Android and iPhone platforms;
- P-SMS Trojan Feed – supporting the detection of SMS Trojans enabling attackers to steal, delete and respond to SMS messages, as well as ringing up premium charges for mobile users;
- Whitelisting Data Feed – providing third-party solutions and services with a systematic knowledge of legitimate software.
- **NEW!!! Kaspersky Transforms for Maltego** – providing Maltego users with a set of transforms that give access to Kaspersky Lab Threat Data Feeds. Kaspersky Transforms for Maltego allows you to check URLs, hashes, and IP addresses against the feeds from Kaspersky Lab. The transforms can determine the category of an object as well as provide actionable context about it.

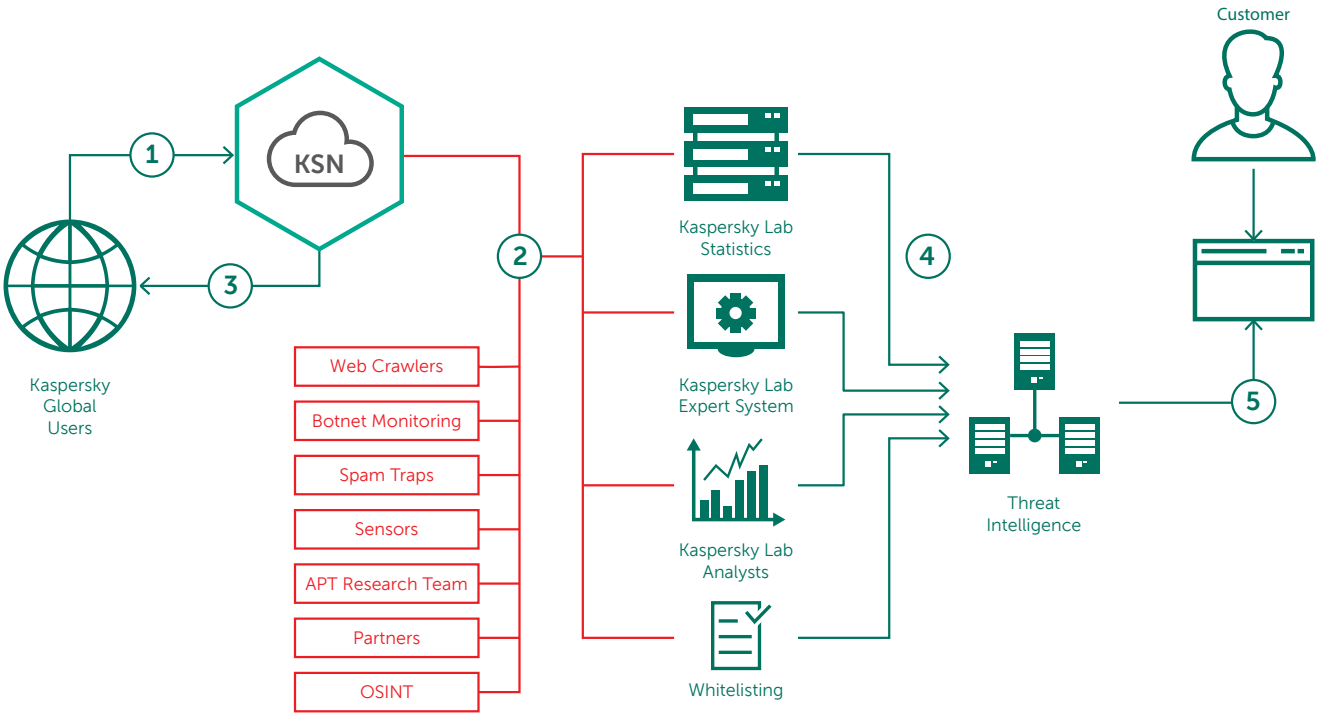
Contextual Data

Every record in each Data Feed is enriched with **actionable context** (threat names, timestamps, geolocation, resolved IPs addresses of infected web resources, hashes, popularity etc). Contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can more readily be used to answer the **who, what, where, when questions** which lead to identifying your adversaries, helping you make timely decisions and actions **specific to your organization.**

Collection and processing

Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network and our own web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams and partners.

Then, in real-time, all the aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling etc.), analysts validation and whitelisting verification:



Kaspersky Threat Data Feeds contain thoroughly vetted threat indicator data sourced from the real world in real time.

Service Highlights

- Data Feeds littered with **False Positives** are valueless, so very extensive tests and filters are applied before releasing feeds, to ensure that 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,...) 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-famous **security experts from GReAT team and leading-edge R&D teams**, contribute to generating these 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.

Benefits

- **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 insight into cyber-attacks and a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including HP ArcSight, IBM QRadar, Splunk etc.) are fully supported;
- Develop or enhance **anti-malware protection for perimeter and edge network devices** (such as routers, gateways, UTM appliances).
- **Improve and accelerate your incident response and forensic capabilities** by providing security/SOC teams with meaningful information about threats and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats to minimize incident response time and disrupt the kill chain before critical systems and data are compromised;
- **Provide threat intelligence to enterprise subscribers**. Leverage the first-hand information about emerging malware and other malicious threats to **preemptively strengthen your defensive posture and prevent compromises**;
- **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 and data centers**;
- **Prevent the exfiltration of sensitive assets and intellectual property** from infected machines to outside the organization, detecting infected assets fast, preventing competitive advantage and business opportunities loss and protecting the reputation of your brand;
- Conduct deep searches into threat indicators such as command-and-control protocols, IP addresses, malicious URLs or file hashes, with human-validated threat context that allows the prioritization of attacks, improves IT expenditure and resource allocation decisions and **supports you in focusing on mitigating those threats that pose the most risk to your business**;
- 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 and etc;
- **As an MSSP**, grow your business through providing industry-leading threat intelligence as a premium service to your customers. **As a CERT**, enhance and extend your cyber threat detection and identification capabilities.

APT Intelligence Reporting

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

Leveraging the information 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.

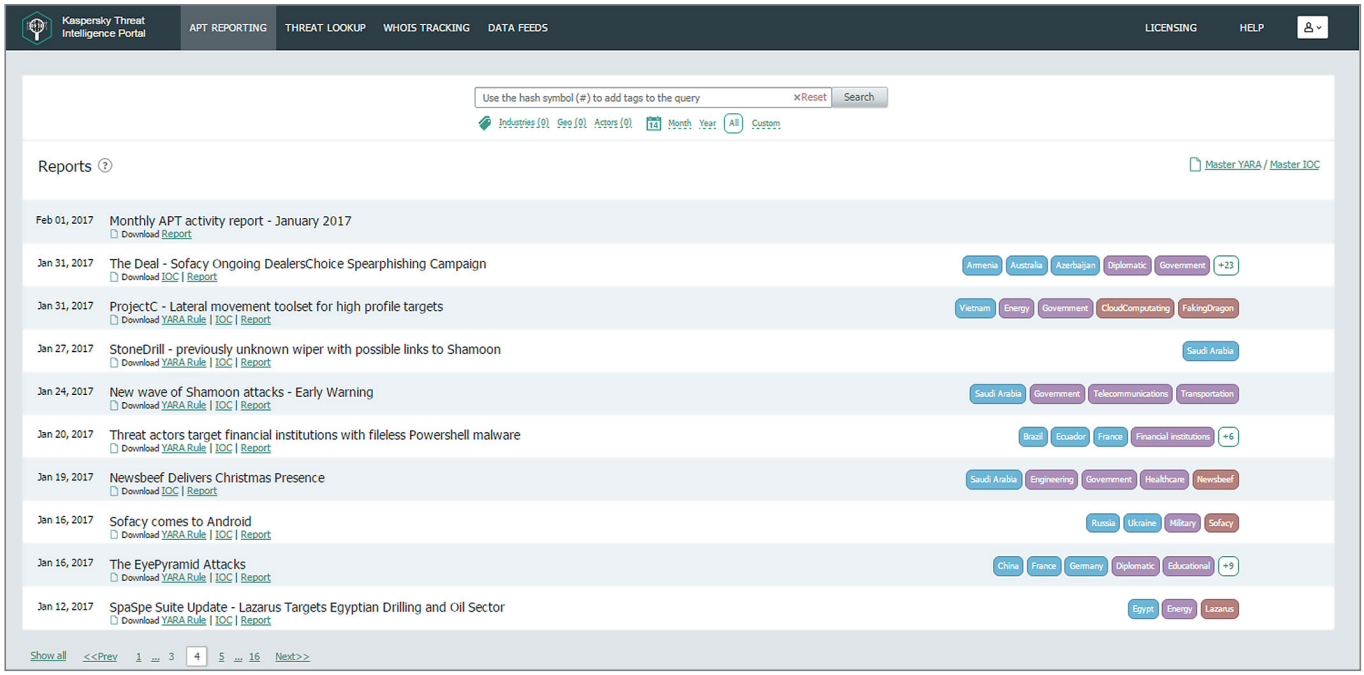
Kaspersky Lab has discovered some of the most relevant APT attacks ever. However, not all Advanced Persistent Threat discoveries are reported immediately, and many are never publicly announced.

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 as it's revealed, including all those threats that will never be made public. During 2016 we have created more than 100 reports!

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 cybercriminal 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 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).

- **Contents for different audience.** Each of the report contains executive summary offering C-level oriented and easy to understand information describing the related APT. Executive 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 an actionable advise for superior protection from the related threat.

- **Retrospective analysis.** Access to all previously issued private reports is provided throughout the period of your subscription.

- **APT Intelligence Portal.** All of the reports including most recent IoC's are available via our APT Intelligence Portal creating seamless user experience for our customers. API is also available.

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.

Tailored Threat Reporting

Customer-specific Threat 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 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 and preferred data formats are established, no additional infrastructure is needed to start usingthis Kaspersky Lab service.

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

The service can be provided as a one-time project or periodically under a subscription (for example, quarterly).

Country-specific Threat Reporting

Cybersecurity of a country comprises protection of all its major institutions and organizations. Advanced persistent threats (APT) against government authorities can affect national security; possible cyberattacks against manufacturing, transportation, telecommunication, banking and other pivotal industries potentially can lead to significant damage on the state level, like financial losses, production accidents, blockage of network communications, and popular discontent.

Having an overview of the current attack surface and the current trends in malware and hacker attacks targeting your country, you can focus your defense strategy on areas pinpointed as cybercriminals' prime targets, acting fast and with precision to repel intruders and minimize the risk of successful attacks.

Created using approaches ranging from Open Source Intelligence (OSINT) to deep analysis of Kaspersky Lab expert systems and databases, and our knowledge of the underground cybercriminal networks, Country-specific Threat reports cover areas including:

- **Identification of threat vectors**: identification and status analysis of externally available critical IT resources of the country – including vulnerable government applications, telecommunication equipment, industrial control systems' components (such as SCADA, PLCs, etc.), ATMs, etc.

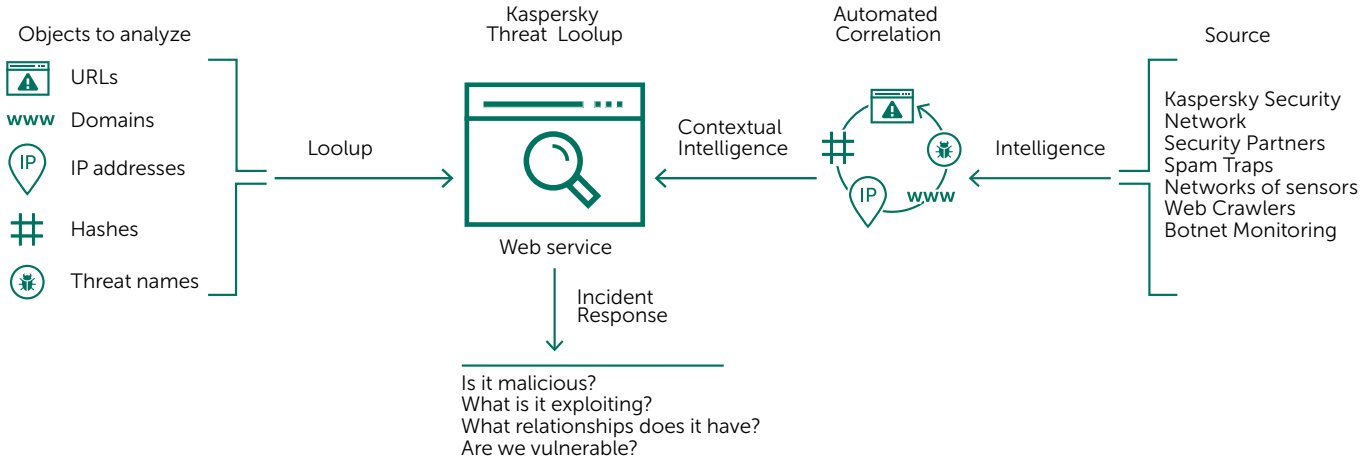
- **Malware and cyber-attack tracking analysis**: identification and analysis of APT campaigns, active or inactive malware samples, past or present botnet activity, and other notable threats targeting your country, based on data available in our unique internal monitoring resources.

- **Information leakages**: through clandestine monitoring of underground forums and online communities, we discover whether hackers are discussing attack plans with certain organizations in mind. We also reveal notable compromised accounts, which could pose risks to suffered organizations and institutions (for instance, accounts belonging to government agencies' employees available in the Ashley Madison breach, which could be used for blackmailing).

Kaspersky Threat Intelligence Reporting has no impact on the integrity and availability of the network resources being inspected. The service is based on non-intrusive network reconnaissance methods, and analysis of information available in open sources and resources of limited access.

As the conclusion of the service you will be provided with a report containing description of notable threats for different state industries and institutions, as well as additional information on detailed technical analysis results. Reports are delivered via encrypted email messages.

Threat Lookup



Service highlights

- **Trusted Intelligence**: A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky Lab products lead the field in anti-malware tests[1], demonstrating the unequalled quality of our security intelligence by delivering the highest detection rates, with near-zero false positives.
- **Threat Hunting**: Be proactive in preventing, detecting and responding to attacks, to minimize their impact and frequency. Track and aggressively eliminate attacks as early as possible. The earlier you can discover a threat – the less damage is caused, the faster repairs take place and the sooner network operations can get back to normal.
- **Sandbox Analysis**:[2] Detect unknown threats by running suspicious objects in a secure environment, and review the full scope of threat behavior and artifacts through easy-to-read reports.
- **Wide Range of Export Formats**: Export IOCs (Indicators of Compromise) or actionable context into widely used and more organized machinereadable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV, to enjoy the full benefits of threat intelligence, automate operations workflow, or integrate into security controls such as SIEMs.
- **Easy-to-use Web Interface or RESTful API**: Use the service in manual mode through a web interface (via a web browser) or access via a simple RESTful API as you prefer.

Cybercrime today knows no borders, and technical capabilities are improving fast: we're seeing attacks becoming increasingly sophisticated as cybercriminals use dark web resources to threaten their targets. Cyber-threats are constantly growing in frequency, complexity and obfuscation, as new attempts are made to compromise your defenses. Attackers are using complicated kill chains, and customized Tactics, Techniques and Procedures (TTPs) in their campaigns to disrupt your business, steal your assets or damage your clients.

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky Lab about cyber-threats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyber-attacks before they impact your organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

Threat intelligence delivered by Kaspersky Threat Lookup is generated and monitored in real time by a highly fault-tolerant infrastructure ensuring continuous availability and consistent performance. Hundreds of experts, including security analysts from across the globe, world-famous security experts from our GReAT team and leading-edge R&D teams, all contribute to generating valuable real-world threat intelligence.

Key Benefits

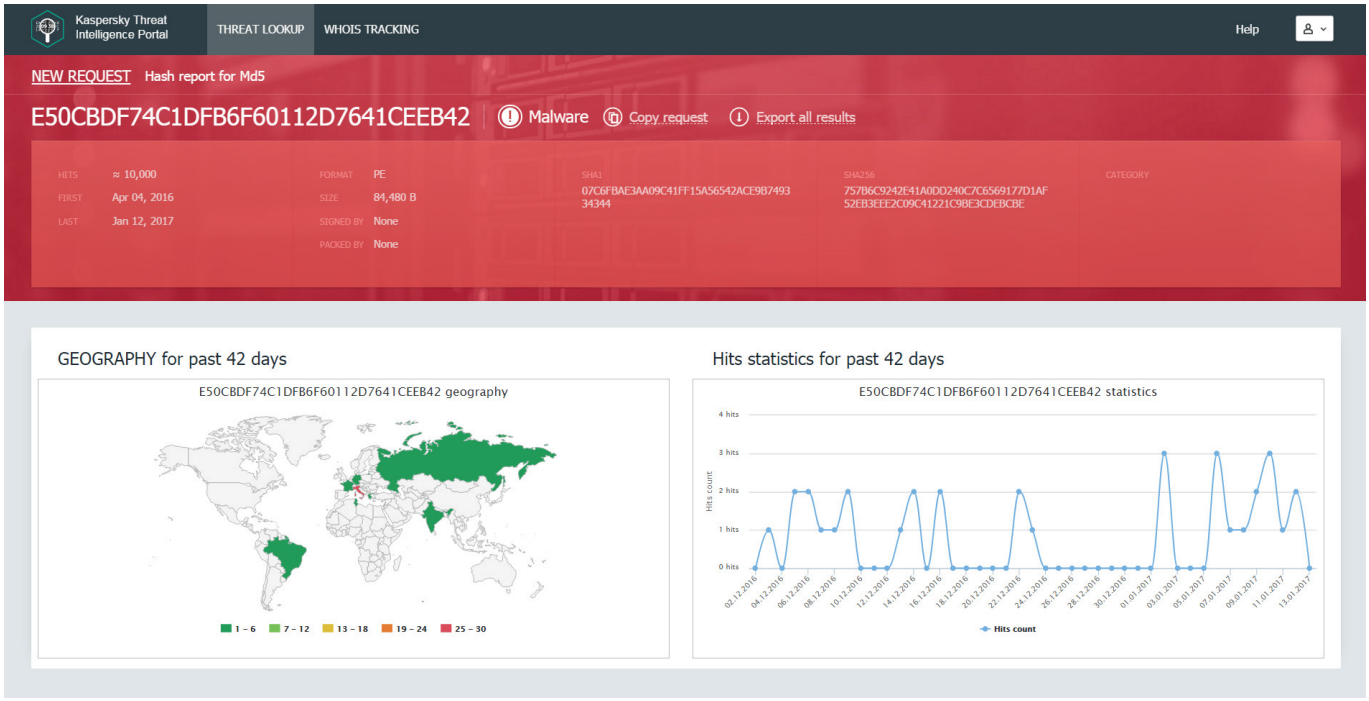
- **Improve and accelerate your incident response and forensic capabilities** by giving security/SOC teams meaningful information about threats, and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats, minimizing incident response time and disrupting the kill chain before critical systems and data are compromised.

- **Conduct deep searches into threat indicators** such as IP addresses, URLs, domains or file hashes, with highly-validated threat context that allows you to prioritize attacks, improve staffing and resource allocation decisions, and focus on mitigating the threats that pose the most risk to your business.

- **Mitigate targeted attacks**. Enhance your security infrastructure with tactical and strategic threat intelligence by adapting defensive strategies to counter.

1 http://www.kaspersky.com/top3

2 The feature is planned to be released in H1' 2017.



Now You Can

- Look up threat indicators via a web-based interface or via the RESTful API.
- Understand why an object should be treated as malicious.
- Check whether the discovered object is widespread or unique.
- Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects.

These are just examples. There are so many ways you can leverage this rich, continuous source of relevant, granular intelligence data.

Know your enemies and your friends. Recognize proven non-malicious files, URLs and IP addresses, increasing investigation speed. When every second could be critical, don't waste precious time analyzing trusted objects.

Our mission is to save the world from all types of cyber-threat. To achieve this, and to make the Internet safe and secure, it's vital to share and access threat intelligence in Real Time. Timely access to information is central to maintaining the effective protection of your data and networks. Now, Kaspersky Threat Lookup makes accessing this intelligence more efficient and straightforward than ever.

Every Kaspersky Phishing Tracking 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, and etc.);
  - attack type (a menace to block an account, an offer to download a file, a request to update personal info, and etc.);
  - resolved IP addresses of this phishing URL;
  - WHOIS data;
  - and much more.

Phishing Tracking

Phishing, and particularly targeted spear-phishing, is one of today's most dangerous and effective online fraud methodologies. Fake websites capture logins and passwords to hijack users' online identities, then steal money or spread spam and malware through compromised email accounts and social networking platforms. It's a powerful weapon in the cybercrime armory, and the frequency and diversity of attacks continues to accelerate.

And it's not just financial institutions being hit. Everyone, from online retailers to ISPs and government institutions, now risks coming under active attack from spear-phishing. Picture perfect copies of your website complete with full corporate branding, or messages appearing to come directly from your own named executives, can easily convince users to hand over confidential data – damaging themselves, and causing massive potential damage to your enterprise.

A single successful phishing attack can have a huge impact on its corporate victim. Aside from direct losses, there are all the indirect costs, like cleaning up compromised websites and accounts. And then, of course, there's the reputational damage, which can be worst of all – an erosion of user trust in your online services that can see you hemorrhaging customers and facing credibility challenges for years to come.Cybercrime today knows no borders, and technical capabilities are improving fast: we're seeing attacks becoming increasingly sophisticated as cybercriminals use dark web resources to threaten their targets. Cyber-threats are constantly growing in frequency, complexity and obfuscation, as new attempts are made to compromise your defenses. Attackers are using complicated kill chains, and customized Tactics, Techniques and Procedures (TTPs) in their campaigns to disrupt your business, steal your assets or damage your clients.

Our Solution – Kaspersky Phishing Tracking Service

This service actively tracks and alerts you in real time to the appearance of phishing sites targeting your brand, and provides you with relevant, 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. The service also monitors specific Top Level Domains (TLDs) or even whole regions for the appearance of phishing sites

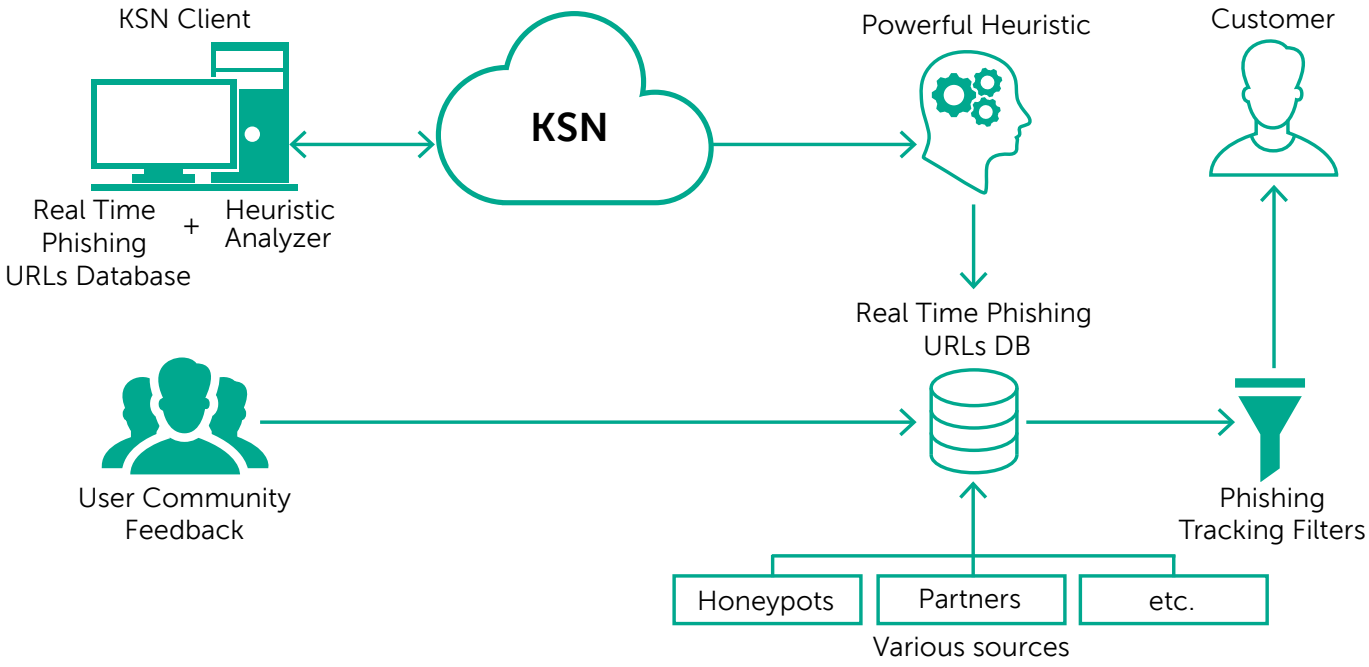
Email notifications confirmed phishing threats against your brands, company name or trademarks are continuously. Every notification provides deep coverage, high accuracy and reliable information about increasingly sophisticated phishing attacks, enabling you to react fast to dynamically generated phishing domains and URLs as well as to phishing outbreaks. Together with a list of phishing sites, you will receive additional intelligence so you can immediately take specific measures against any phishing attack.

Empowered with this timely, professionally validated intelligence, you can act swiftly and with precision to mitigate the impact of phishing activity on your organization and your users, taking a proactive stance against fraud.

Sources of intelligence

Kaspersky Phishing Tracking synthesizes data from heterogeneous, highly reliable intelligence sources, including the Kaspersky Security Network (KSN), powerful heuristic engines, email honeypots, web crawlers, spam traps, research teams, partners and historical data about malicious objects we've been collecting for almost 2 decades. Aggregated data is then fully inspected in real time, and refined using multiple preprocessing techniques including statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), content analyst validation and whitelisting verification tools.

The worldwide coverage of Kaspersky Security Network, combined with Kaspersky Lab detection technologies and a barrage of tests and filters ensures the maximum detection of any kind of phishing attack and threat with no false positives, as is continuously confirmed through independent tests*.



Your Early Warning of Phishing Attacks

Subscribing to the Kaspersky Phishing Tracking Service gives you a critical edge against your attackers. Armed with early warning of phishing attacks, in progress or still in planning, that are targeting your brands, online services and customers, enables you to protect resources and mitigate risk more pragmatically, more accurately and more cost-effectively.

Getting Ahead

Critical information is provided in real time, as well as through regular reporting on malicious activities that indicate that advanced attacks are being planned, as well as those in progress. Now it's you, not the cybercriminals who have you in their sights, that's one step ahead.

Improving Your Users' Experience

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.

Minimizing Impact

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.

Staying Better Informed

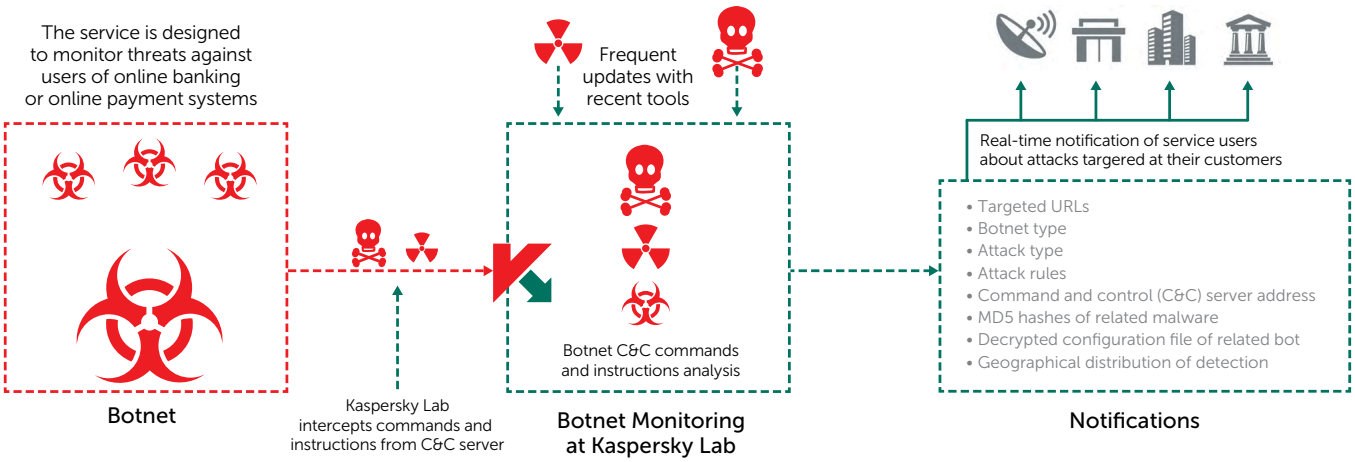
This flow of relevant, accurate and detailed information, with no 'false positives' or time-wasting, provides new insights to help inform and enhance your current and future security strategy. Now, you and your business can take a proactive, informed stance against online fraud.

AV comparatives Approved 2016 Anti-Phishing

* AV-comparatives test reports are available upon request.

Botnet Tracking

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



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

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