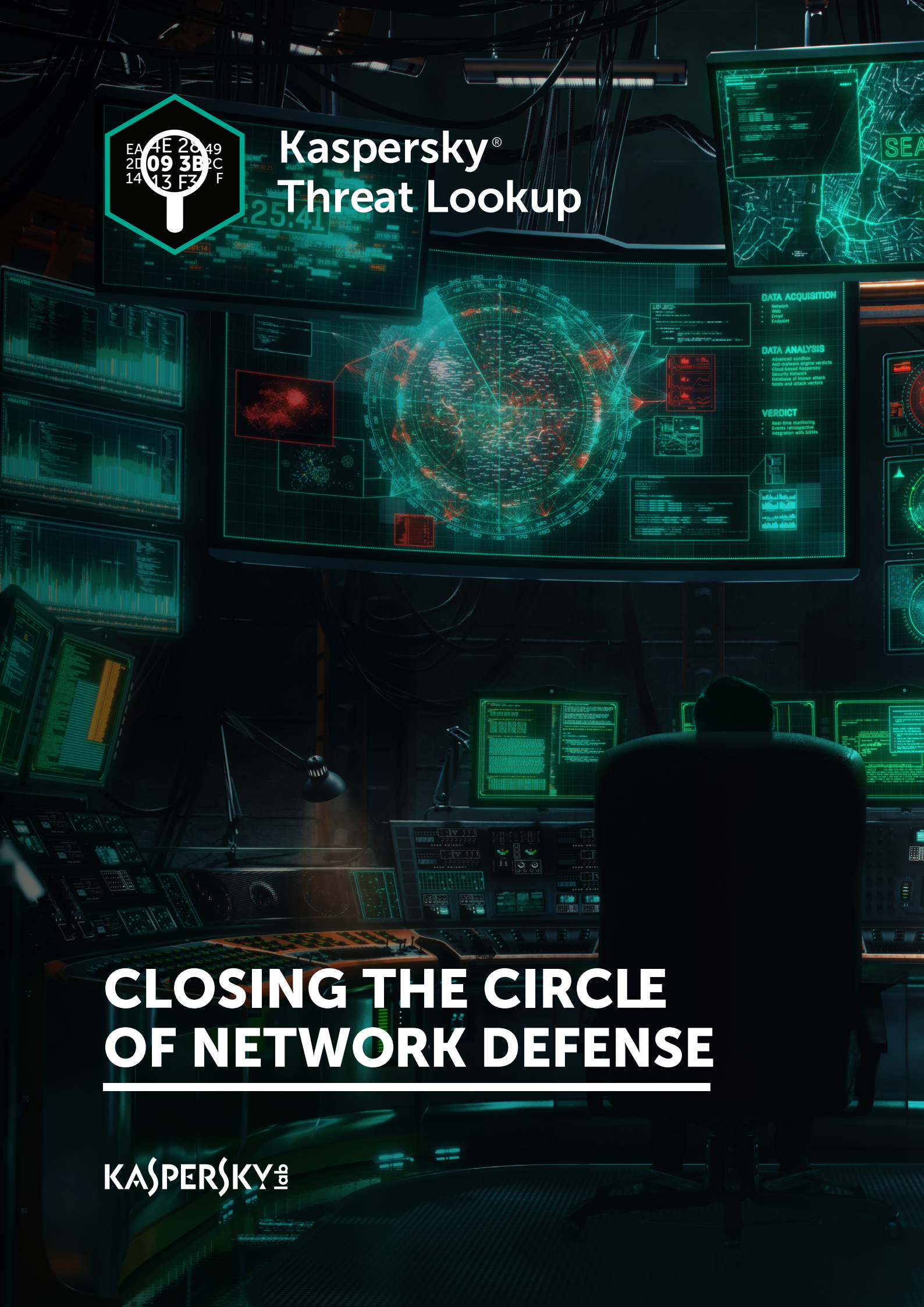
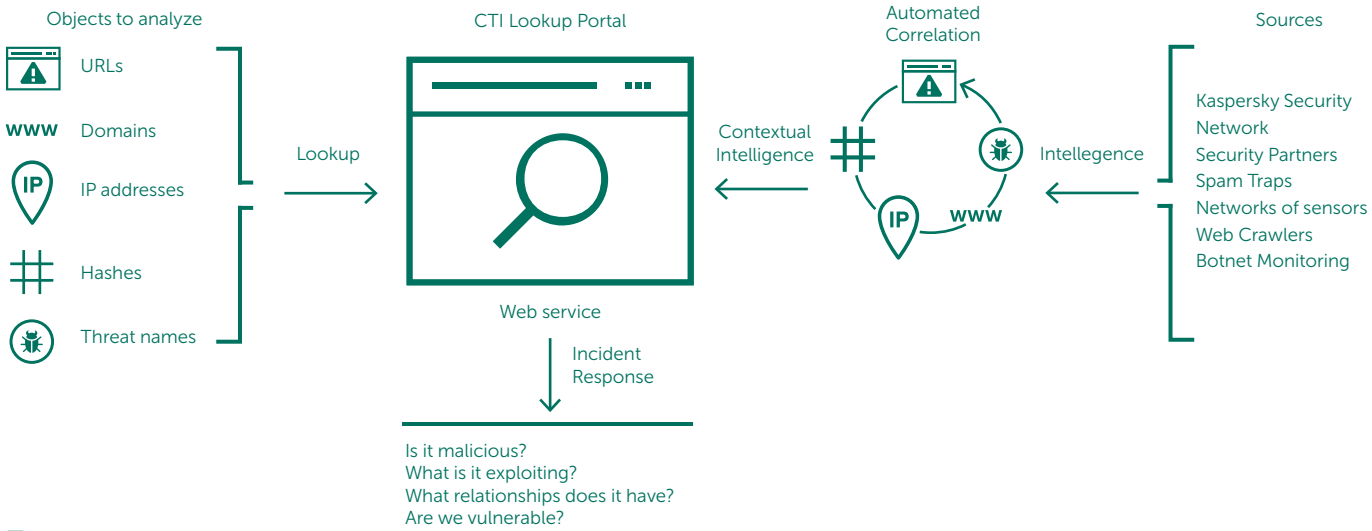



# CLOSING THE CIRCLE OF NETWORK DEFENSE

KASPERSKY lab

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.

Access to Kaspersky Threat Lookup provides reliable, immediate intelligence about cyber-threats, legitimate objects, their inter-connections and indicators, enriched with actionable context to inform your business or clients about the associated risks and implications. Now you can mitigate and respond to threats more effectively, defending against attacks even before they are launched.
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, etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.




## Features:

- **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.
- **High levels of Real Time Coverage:** Threat intelligence is automatically generated in Real Time, based on findings across the globe (thanks to Kaspersky Security Network providing visibility to a significant percentage of all internet traffic and all types of data, covering tens of millions of end-users in more than 213 countries) providing high coverage and accuracy.
- **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.
- **Rich Data:** Threat intelligence delivered by Kaspersky Threat Lookup covers a huge range of different data types including hashes, URLs, IPs, whois, pDNS, GeoIP, file attributes, statistical and behavior data, download chains, timestamps and much more. Empowered with this data, you can survey the diverse landscape of security threats you are facing.
- **Continuous Availability:** Threat intelligence is generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability and consistent performance.
- **Continuous Review by Security Experts:** 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.

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

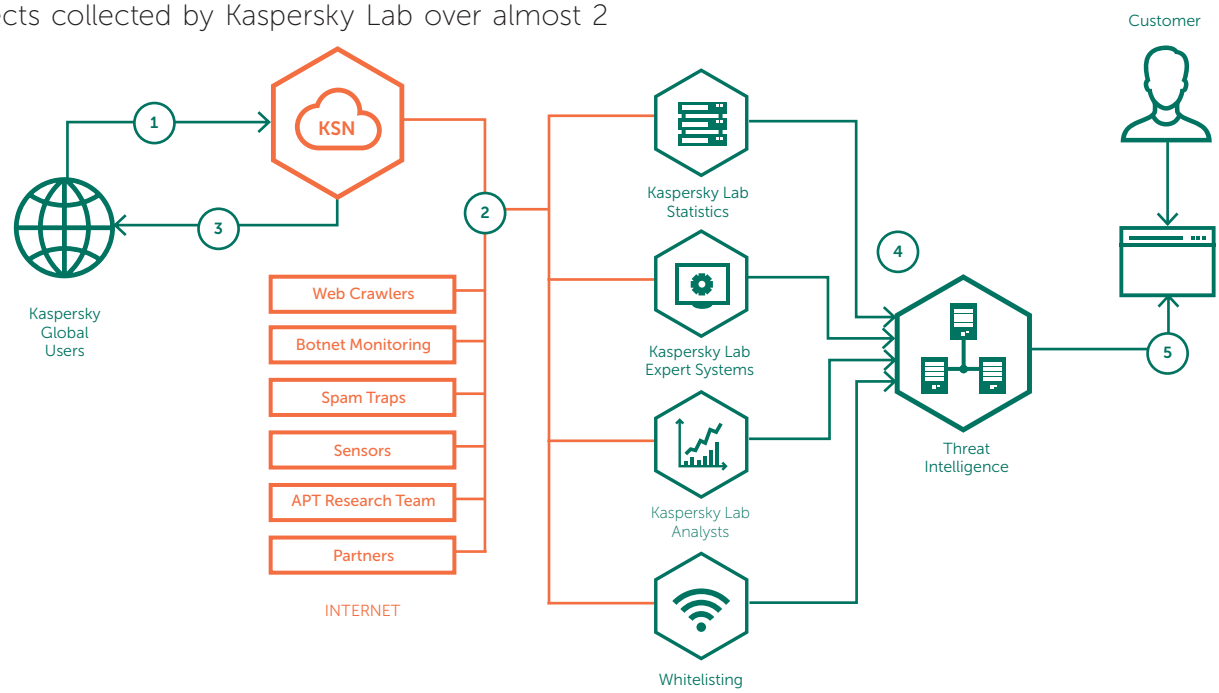
- **Sandbox Analysis:**[2] Detect unknown threats by running suspicious objects in a secure environment, and review the full scope of threat behavior and artifacts through easy-to-read reports.
- **Wide Range of Export Formats:** Export IOCs (Indicators of Compromise) or actionable context into widely used and more organized machine-readable 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.
- **Reverse WHOIS Lookup:** Search required domains and IP addresses by setting specific search criteria within WHOIS data (e.g. domain contact, creation date, etc.).
- **WHOIS Tracking:** Submit specific fields of WHOIS data for regular and automatic search of WHOIS records that meet your criteria. Email notifications about new records in WHOIS database that match search criteria are automatically sent to required recipients.

## 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 the specific threats your organization faces.

## Threat Intelligence Sources:

Threat intelligence is aggregated from a fusion of heterogeneous and highly reliable sources, including the Kaspersky Security Network (KSN) and our own web crawlers, our Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams, partners and other historical data about malicious objects collected by Kaspersky Lab over almost 2 decades. Then, in Real Time, all aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, similarity tools, behavior profiling etc.), analyst validation and whitelisting verification.



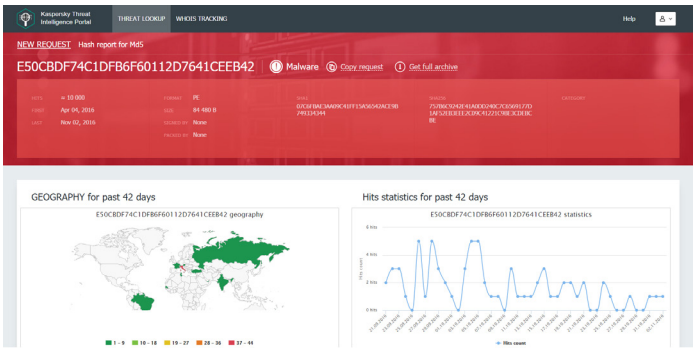

Kaspersky Threat Intelligence comprises thoroughly vetted threat indicator data sourced from the real world in Real Time.

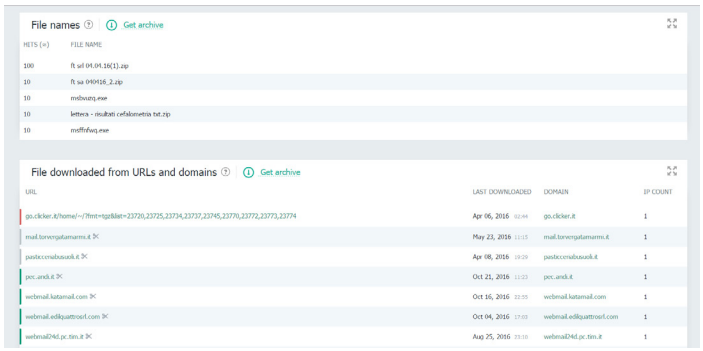
[2]. The feature is planned to be released in H1' 2017.

## Now you can:

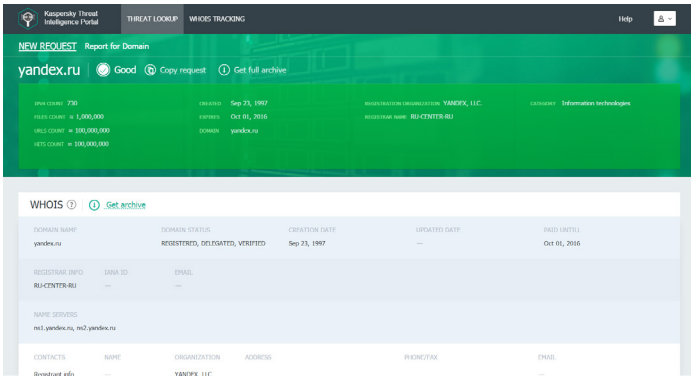
- Look up threat indicators via a web-based interface or via the RESTful API.
- Understand why an object should be treated as malicious.
- Check whether the discovered object is widespread or unique.
- Examine advanced details including certificates, commonly used names, file paths, or related URLs to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

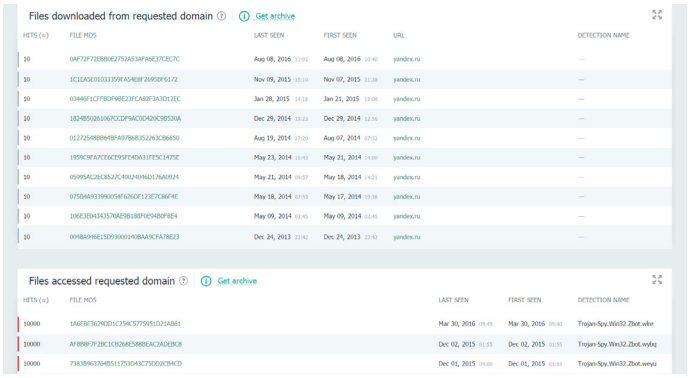
These are just examples. There are so many ways you can leverage this rich, continuous source of relevant, granular intelligence data.




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.

**For more information on Kaspersky Threat Lookup or any of our Security Intelligence Services, please contact intelligence@kaspersky.com**



KASPERSKY lab
THE POWER OF PROTECTION