KASPERSKY lab

KASPERSKY SECURITY INTELLIGENCE SERVICES. THREAT INTELLIGENCE SERVICES

www.kaspersky.com

THREAT INTELLIGENCE SERVICES

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

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

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

Kaspersky Lab Threat Intelligence Services include:

- Threat Data Feeds
- Botnet Tracking
- APT Intelligence Reporting

THREAT DATA FEEDS

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

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

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

USE CASES / SERVICE BENEFITS

Kaspersky Lab Threat Data Feeds:

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

Kaspersky Lab offers three types of Threat Data Feed:

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

FEED DESCRIPTION

Malicious URLs – a set of URLs covering malicious links and websites. Masked and non-masked records are available.

Phishing URLs – a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.

Botnet C&C URLs – a set of URLs of botnet command and control (C&C) servers and related malicious objects.

Malware Hashes (ITW) – a set of file hashes and corresponding verdicts covering the most dangerous and prevalent malware delivered through the intelligence of KSN.

Malware Hashes (UDS) – a set of file hashes detected by Kaspersky Lab cloud technologies (UDS stands for Urgent Detection System) based on a file's metadata and statistics (without having the object itself). This enables the identification of new and emerging (zero-day) malicious objects that are not detected by other methods.

Mobile Malware Hashes – a set of file hashes for detecting malicious objects that infect mobile platforms.

P-SMS Trojan Feed — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages.

Mobile Botnet C&C URLs — a set of URLs with context covering mobile botnet C&C servers.

INTELLIGENCE REPORTING

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

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

APT Intelligence reporting

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

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

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

KASPERSKY APT INTELLIGENCE REPORTING PROVIDES:

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

NOTE – SUBSCRIBER LIMITATION

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

INTELLIGENCE REPORTING

Customer-Specific Threat Intelligence Reporting

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

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

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

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

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

QUICK START – EASY TO USE – NO RESOURCES NEEDED

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

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