kaspersky BRING ON THE FUTURE

Kaspersky Targeted Attack Discovery

Kaspersky Targeted Attack Discovery will be useful if you are concerned about attacks directed at your industry, if you have noticed suspicious behavior in your own systems, or if your organization simply recognizes the benefits of regular preventative inspections.

The service helps discover:

- **Ongoing attacks**
- **Attacks that occurred in the past**
- **Compromised systems.**

You also get recommendations on how to remediate attacks and prevent similar incidents in future.

The results
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.

How the service works

Our experts detect, identify and analyze ongoing incidents as well as those that occurred in the past, and compile a list of systems affected by those attacks. We help you uncover malicious activities, identify the possible sources of an incident and plan the most effective remedial actions.

We do this by:

- Analyzing the specific threat landscape of your organization
- Conducting in-depth inspections of your IT infrastructure and data (such as log files) to identify possible signs of compromise
- Analyzing your outgoing network connections for suspicious activity
- Uncovering probable sources of an attack and other potentially compromised systems

The service in more detail

The Kaspersky Targeted Attack Discovery includes the following stages:

Gathering and analyzing data on attacks from external sources. The aim at this stage is to obtain a snapshot of the attack surface of a company whose assets are, or were, being targeted by intruders. We tap into a variety of intelligence sources, including underground cybercriminal communities, as well as internal Kaspersky's monitoring systems. Analyzing this intelligence allows us to identify weaknesses in a company's infrastructure that are of interest to cybercriminals, compromised accounts, stolen data and much more.

Onsite or remote data collection and early incident response. This stage sees data collected from workstations, servers, SIEM systems and other equipment in the customer's infrastructure. Data can be collected onsite or remotely using software provided to the customer within the framework of the service. In case of suspicious activity Kaspersky experts collect any type of evidence related to the incident, which may include: log files of operating systems, applications and network equipment, web traffic logs (for example, from proxy servers), network traffic dumps, HDD images, memory dumps and any other types of information, which could be useful for investigation. Interviews with the customer's representatives and of any other entities involved into the incident can also be organized. At this stage Kaspersky provides interim recommendations for initial incident response.

Evidence analysis. Kaspersky performs analysis of all available information (including malware analysis if needed) in order to recreate the picture of the incident. The customer may be asked to provide additional data (via email or various network resources, depending on the type and amount of data requested).

Report preparation. The work carried out within the framework of the service culminates in a final report. It contains the results of data analysis from external sources, as well as descriptions of detected attacks based on analysis of the data collected in the customer's infrastructure. The report also contains remediation recommendations for the detected attacks.

Additional services

If necessary, our experts will analyze the symptoms of an incident, perform deep digital analysis for certain systems, identify a malware binary (if any) and conduct malware analysis. These optional services report separately, with further remediation recommendations. We can also, on request, deploy the **Kaspersky Anti Targeted Attack (KATA)** platform onto your network. This platform combines the latest technologies and global analytics in order to detect and respond promptly to targeted attacks, counteracting them at all stages of their lifecycle in your system.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. This is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Proven.
Transparent.
Independent.