Kaspersky Compromise Assessment

kaspersky BRING ON THE FUTURE

Cybercriminals attack users with 400,000 new malicious files every single day

What is Kaspersky Compromise Assessment?

Kaspersky Compromise Assessment (CA) uncovers active cyberattacks as well as previous unknown attacks that flew under the radar of your IT security tools and processes. The goal is to get the highest possible level of assurance as to whether or not your network is compromised, with independent expert analysis. The service establishes the most likely reasons for an incident, its source and impact, and recommends remediation actions.

How CA can help

- Understand your specific threat landscape by analyzing threat intelligence sources (including darknet)
- Reveal possible signs of compromise
- Perform tool-aided endpoint scanning of your IT infrastructure
- Analyze security event logs and network activity including outgoing connections to Command and Control servers of malware
- Conduct an initial incident investigation to identify malware used for the attack(s)

How Kaspersky Compromise Assessment works

Compromise Assessment consists of the following stages:

Data Collection

At the Data Collection stage, we'll scan all your hosts, and collect relevant forensic metadata and historical logs to look for footprints of cybercrime. Our team will analyze multiple threat intelligence sources to understand your organization's specific threat landscape, including APT groups attacking your industry and region.

Remediation & Reporting

We'll prepare a final report with detailed answers to key questions:

- Are you compromised? We'll provide you with an executive summary on the presence, or absence, of signs of compromise in your network.
- If you have been compromised — what happened? You'll be able to see a detailed picture of cyberespionage activity in your network, including discovered incidents, affected network components, a description of the vulnerabilities used, likely attack sources, and the results of malware analysis.
- What needs to be done? You will receive recommendations on how to protect your resources from similar attacks in the future, and how to enhance protection against the detected security flaws and misconfigurations that have been dealt with.

Threat Hunting

We'll then process all the data we've collected and identify incidents in your network. Some incidents will be 100% confirmed (e.g. a malware infection). In these cases, we will immediately provide response recommendations. Some incidents may require additional confirmation and validation (e.g. suspicious user behavior).

Incident Validation and Early Response

To confirm the more severe incidents, we may need additional data for in-depth analysis, e.g. the compromised system's disk image, or executable binary or script, to see whether or not it's malicious. For all confirmed incidents we develop actionable threat intelligence to scope the incident and contain the threat.

Kaspersky Compromise Assessment deliverables

The service's findings cover:

1. Conclusions as to whether or not your network is, or has been, compromised
2. Collected threat intelligence and indicators of compromise (IOC)
3. Details of possible attack sources and compromised network components
4. Remediation recommendations to mitigate the impact of detected incidents

Recommendations on how to protect your resources from similar attacks in the future.

Why Kaspersky

Certified Threat Hunters

Our team consists of certified experts in digital forensics, reverse engineering, malware analysis, and network security

Adaptive Tools and Telemetry

Threats are detected using IoC, TTP, YARA, and Threat Intelligence. We can easily modify our detection rules, tools, and telemetry to find new types of threats

Actionable Threat Intelligence

As a global threat intelligence provider, we have an extensive blacklist database as well as a huge whitelist database, which helps to identify threats faster

Kaspersky Compromise Assessment

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture