INTELLIGENCE SERVICE: INCIDENT INVESTIGATION

MALWARE ANALYSIS | DIGITAL FORENSICS | INCIDENT RESPONSE

Personalized incident investigation support to help your organization identify and resolve IT security incidents.

Cyberattacks are an increasing danger for enterprise networks. Tailor-made to exploit the unique vulnerabilities of the criminal's chosen target, these attacks are often designed to steal or destroy sensitive information or intellectual property, undermine operations, damage industrial facilities or steal money.

Protecting an enterprise against these sophisticated, well-planned attacks has become increasingly complicated. It can even be difficult to establish for certain whether your organization is in fact under attack.

Kaspersky Lab's Investigation Services can help organizations formulate their defense strategies through providing in-depth threat analysis and advising on appropriate steps toward resolution of the incident.

SERVICE BENEFITS

Kaspersky Lab Investigation Services help our customers to **resolve live security issues and understand malware behavior and its consequences, providing guidance on remediation**. This approach indirectly helps organizations to:

- **Reduce the costs** of resolving the issues arising from a cyber-infection
- **Stop the leakage of confidential information** that can potentially flow from infected PCs
- **Reduce reputational risks** caused by the infection harming operational processes
- **Restore the normal work of PCs** that were damaged by infection

Kaspersky Lab's investigations are carried out by highly experienced analysts with practical expertise in digital forensics and malware analysis. On completion of the investigation, you as the customer are provided with a detailed report, giving the full results of the cyber investigation and proposing remediation steps.

DIGITAL FORENSICS

Digital Forensics is an investigation service aimed at producing a detailed picture of an incident. Forensics can include malware analysis as above, if any malware was discovered during the investigation. Kaspersky Lab's expert use various pieces of evidence to understand exactly what is going on, including HDD images, memory dumps and network traces. All of this helps to produce a detailed explanation of the incident.

The customer carries out its own incident assessment and collects evidence, presenting Kaspersky Lab with an outline of the incident and the evidence gathered in-house. Then Kaspersky Lab experts analyze the incident symptoms, identify the malware binary (if any) and conduct the malware analysis in order to provide a detailed report including remediation steps.

MALWARE ANALYSIS

Malware Analysis offers a complete understanding of the behavior and objectives of specific malware files that are targeting your organization.

The customer begins the investigation for itself, assessing the incident, collecting evidence and performing a digital forensic analysis. Then it provides Kaspersky Lab with the malware binary. Kaspersky Lab's experts carry out a thorough analysis of the malware sample provided by your organization, creating a detailed report that includes:

- Sample properties: a short description of the sample and a verdict on its malware classification
- Detailed malware description: an in-depth analysis of your malware sample's functions, threat behavior and objectives - including IOCs - arming you with the information required to neutralize its activities
- Remediation scenario: the report will suggest steps to fully secure your organization against this type of threat

INCIDENT RESPONSE

Incident response is our top-level service, covering the full incident investigation cycle. All the expertise in Digital Forensics and Malware Analysis can be brought to the customer's site to assist in the resolution of a security incident.

Kaspersky Lab's experts visit the scene of the incident and carry out all aspects of the investigation in order to deliver targeted incident resolution instructions, including remediation steps. The incident is described in a detailed investigation report.

DELIVERY OPTIONS

Kaspersky Lab Investigation Services are available:

- on subscription, based on an agreed number of incidents
- in response to a single incident

INCIDENT INVESTIGATION WORKFLOW

Kaspersky Lab offers three levels of investigation:

- Malware Analysis – helping you to understand the behavior and objectives of specific malware files that are targeting your organization.
- Digital Forensics – providing a complete picture of the incident and how your organization could be affected.
- Incident Response – a full cycle incident investigation that includes an on-site visit from Kaspersky Lab's experts.

No	Investigation phases	Malware Analysis	Digital Forensics	Incident Response
1	**Incident assessment** • Rapid response to the incident • Minimization of the consequences • Initial analysis of the incident, that can be done onsite if required, to establish a full understanding of the issue and determine how to collect the necessary evidence			X
2	**Collecting evidence** Depending on the situation, gather HDD images, memory dumps, network traces etc related to the incident under investigation			X
3	**Performing forensic analysis** • Establishing a clear, detailed picture of the incident: – What happened – Who was targeted – When it happened – Where it happened – Why it happened – How it happened • Analyzing the evidence to find the malware that caused the incident		X	X
4	**Performing malware analysis** Analyzing the malware to understand how it works, including its: • Classification • Functions • Related vulnerability and exploits • Means of propagation • Destructive activity • Means of installation	X	X	X
5	**Creating a remediation plan** • Understanding the objective of the malware binary • Developing ways to stop its propagation • Developing uninstallation plans	X	X	X
6	**Creating an investigation report** Upon the completion of their analysis Kaspersky Lab experts provide a detailed report, including investigation details and a remediation scenario	X	X	X

WHY KASPERSKY LAB?

- Founded and led by the world's foremost security expert, Eugene Kaspersky
- Partnerships with global law enforcement agencies such as Interpol and CERTS
- Cloud-based tools monitoring millions of cyberthreats across the globe in real time
- Global teams analyzing and understanding Internet threats of all kinds
- World's largest independent security software company — focused on threat intelligence and technology leadership
- Undisputed leader in more independent malware detection tests than any other vendor
- Identified as a Leader by Gartner, Forrester and IDC

For more information on Kaspersky Intelligence Services, please contact us via intelligence@kaspersky.com.
TO LEARN MORE VISIT www.kaspersky.com.

KASPERSKY lab