



# Incident Response Guide

# Contents

About this guide .....	5
Terms and definitions .....	6
Incident Response Basics.....	10
Attack lifecycle (kill chain).....	10
Incident response steps.....	14
Recommended IR process and rules.....	20
Preparation .....	20
Identification .....	23
Incident triggers.....	23
Prioritization guidelines.....	26
Analyzing incidents in SIEM .....	28
Containment .....	33
Eradication.....	35
Recovery .....	35
Lessons learned .....	36
Incident response example .....	37
The attack plan .....	37
The incident response .....	42
Preparation (example).....	42
Identification (example) .....	44
Containment (example) .....	45
Eradication and Recovery (example) .....	51
Lessons learned (example) .....	52
Recommended tools and utilities .....	53
Tools for collecting IOC .....	53
Sysinternals utilities.....	54
AVZ .....	55
GMER.....	56
YARA.....	57
Tools for creating dumps .....	58

GRR Rapid Response .....	58
Forensic Toolkit .....	59
dd utility .....	59
Belkasoft RAM Capturer .....	59
Tools for analysis .....	60
Kaspersky Threat Intelligence Portal .....	61
Tools for analyzing memory dumps .....	64
Tools for analyzing hard disk dumps .....	67
Strings utility .....	68
Tools for eradication .....	69
Kaspersky Virus Removal Tool .....	69
Kaspersky Rescue Disk .....	70
AO Kaspersky Lab .....	71
Trademark notices .....	73

Dear User,

Thank you for choosing Kaspersky Lab as your security software provider. We hope that this document helps you to use our product.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky Lab): all rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky Lab.

This document, and graphic images related to it, may be used for informational, non-commercial, and personal purposes only.

Kaspersky Lab reserves the right to amend this document without additional notification.

Kaspersky Lab assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential harms associated with use of the document.

Document revision date: 24.03.2017

© 2017 AO Kaspersky Lab. All Rights Reserved.

<http://www.kaspersky.com>  
<http://support.kaspersky.com>

---

# About this guide

Every year, Kaspersky Lab discovers about 325 000 new types of malicious software. Not only home users are at risk, but also companies, banks, critical infrastructure, government organizations, and manufacturers that use automatic control systems (ACS).

This guide provides basic explanations and recommendations for responding to information security incidents.

This guide aims to do the following:

- Systematize information about the attack lifecycle and actions involved in the incident response (IR) process.
- Provide a recommended sequence of actions for IR.
- Describe a range of tools and utilities that can be used at every phase of the IR process.
- Provide information about IR best practices.

## **Audience**

This document is intended for technical specialists (system administrators) and managers responsible for IT and information security.

## **Sources for independent research about information security**

This document is not a comprehensive set of instructions for carrying out incident responses. It provides only a basic approach to incident response processes and describes a recommended sequence of actions that can be used to respond to security incidents.

To gain more knowledge about incident response theory and practice, it is recommended that you familiarize yourself with the following subjects:

- Incident response
- Digital forensics
- Advanced analysis and reverse engineering of malicious software

Kaspersky Lab courses offer a broad curriculum in cybersecurity subjects and techniques ranging from basic to advanced. All are available either in-class on customer premises or at a local or regional Kaspersky Lab office, if applicable. For more information about the courses, see <http://www.kaspersky.com/enterprise-security/intelligence-services>.

## In this chapter

Terms and definitions .....	6
-----------------------------	---

# Terms and definitions

This section provides definitions for terms used in this guide. The terms are defined in the scope of this guide.

The following terms are used in this guide:

- APT

An *advanced persistent threat (APT)* is a type of attack in which the attacker gains access to an organization's assets and tries to remain undetected for a long period of time. The goals of an APT attack most often include spying and theft of sensitive data. APT attacks involve the use of customized and highly sophisticated software.

- artifact

An *artifact* is an object created or changed by malicious software in the course of the attack. Examples of artifacts are malicious software files, directories, system log file entries, and registry branches.

- asset

An *asset* is an object or an entity belonging to the organization. Examples of assets are workstations in the organization's network, security controls, and data stored on the workstations.

- attack, cyber attack

An *attack* (*cyber attack*) is an attempt by the attacker to gain control, damage, or destroy a computer network or system.

- attacker

An *attacker* is a person (or a group of persons) who conduct a cyber attack. An attacker usually tries to gain access to the organization's assets.

- C&C server

A *command and control server* (*C&C server*) is a computer that issues commands to the computers compromised by the attacker. Typically, a piece of malicious software makes requests to the C&C server and receives commands in response.

- defensive measures

*Defensive measures* are security controls and processes used by the organization as a defense against cyber attacks. Examples of defensive measures are the organization's proxy server and endpoint protection solutions that protect the workstations.

- endpoint protection solution

An *endpoint protection solution* is a software that protects organization's workstations against cyber attacks. An example of an endpoint protection solution is Kaspersky Endpoint Security solution.

- event

An *event* is any occurrence that involves the organization's assets. An event typically represents a message, pattern, value, or marker that can be recognized within a stream of monitored inputs, such as network traffic, errors or signals, counts, and so on.

- exploit

An *exploit* is a piece of software, a chunk of data, or a sequence of commands that takes advantage of the security vulnerabilities discovered by the attacker and delivers the payload.

- incident

An *incident* is an occurrence where the organization's security or assets can be compromised by a cyber attack.

- incident response (IR)

An *incident response (IR)* is a process of addressing and managing an incident (for example, a cyber attack).

- indicators of compromise (IOC)

*Indicators of compromise (IOC)* are pieces of data that identify potentially malicious activity on a network or system. IOC examples include unusual network traffic, multiple failed login attempts, the presence of files used by malicious software, and suspicious registry or system file changes, strings, URLs, IP addresses, and hashes.

- organization

In this guide, an *organization* is a company that is attacked by an attacker. The organization has a security team that performs incident response.

- payload

A *payload* is software used by an attacker to reach the attack objectives. Depending on the attack objectives, the payload may contain malicious or legitimate software that would allow the attacker to access sensitive data or cause harm to the organization.

- sample (software or malware)

A *software sample (malicious software sample)* is a particular instance or a part of an instance. Samples of malicious software are obtained by the security team from the compromised assets.

- security control

A *security control* is a device or a piece of software used by the organization to protect against cyber attacks.



- security team

A *security team* is a group of organization's employees tasked with providing security and performing incident response.

- SIEM system

A *Security information and event management (SIEM) system* is a type of software that collects events and other security-related information for analysis by gathering the events from workstations, servers, network equipment, and security controls of the organization.

- spear phishing

*Spear phishing* is an approach taken by an attacker in which he or she sends email messages to an organization in order to compromise the organization's assets or gain unauthorized access to confidential data.

- threat feed

A *threat feed* is an ongoing stream of data related to potential or current cyber threats. Threat feeds contain indicators of compromise (IOC), which can be used to identify and mitigate cyber threats. Threat feeds can be integrated into SIEM systems.

- vulnerability

A *vulnerability* is a flaw in the organization's security that is exploited by the attacker to conduct an attack.

---

# Incident Response Basics

This chapter explains the kill chain model for attacks and the basic incident response procedure for countering these attacks.

## In this chapter

Attack lifecycle (kill chain) .....	<a href="#">10</a>
Incident response steps .....	<a href="#">14</a>

## Attack lifecycle (kill chain)

This section describes the lifecycle of a cyber attack and the kill chain model.

### About the kill chain model

When performing a cyber attack, an attacker follows a structured set of actions. One of the models that describe this set of actions is the *kill chain model*.

Originally, the term kill chain was used by the military to describe the structure of an attack. When defenders know the sequence of actions taken by an attacker, the defending side can create a defensive strategy to counter the attack.

The kill chain model was adapted for IT security and can be used to describe cyber attacks. In ways similar to military use of the kill chain model, the cyber security team can create a defensive strategy against cyber threats. To successfully counter a threat, the security team must base the defensive strategy on information about the attacker's sequence of actions.

When applied to cyber attacks, the kill chain model identifies several attack stages. In the kill chain model, an attacker must go through each of these stages to reach the attack's goals. If the attacker is prevented from executing (progressing) at any stage, the attack cannot succeed.

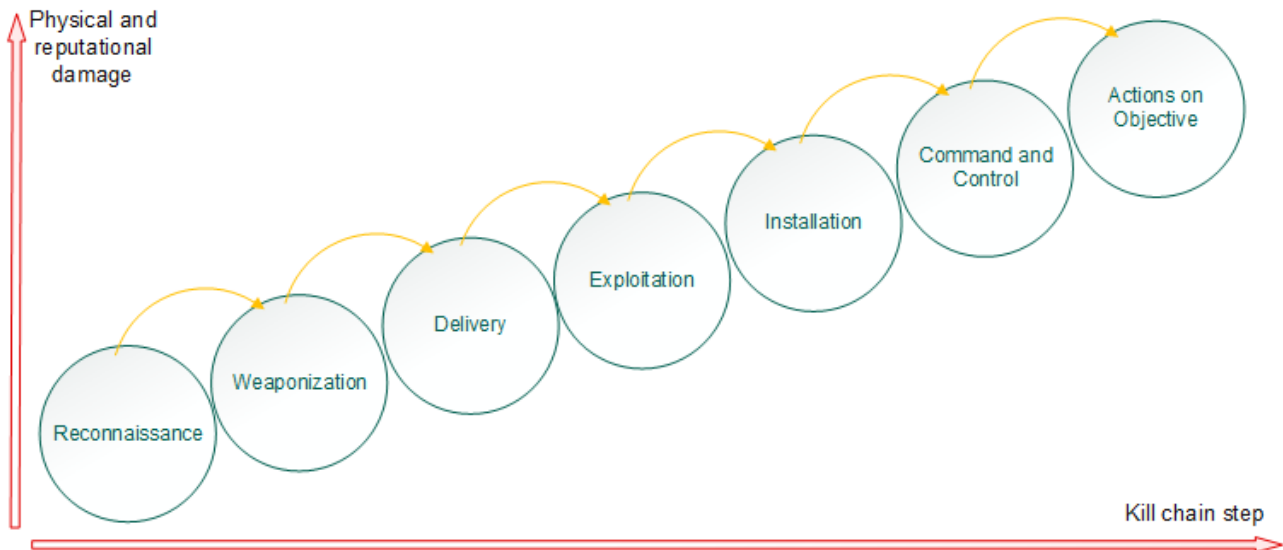


Figure 1: Attack lifecycle (kill chain)

The kill chain model identifies the following sequence of attack stages:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and control
7. Actions on objective

The amount of physical and reputational damage caused by a cyber attack depends on the stage where the attack was detected. The stage also determines the effectiveness of the investigation. If an attack is detected at the *Actions on objective* stage, then the security team is unable to counter the attack and the attacker reaches its goals. A cyber attack causes the least amount of damage if it is detected early, during the *Delivery* or *Installation* stage.

### Stage 1: Reconnaissance

At this stage, the attacker collects information about the targeted organization and its assets. For example, the attacker tries to obtain information about the structure of the targeted organization, its

technology stack, and the organization's security measures. The attacker may also consider using social engineering against the employees. As an example, the attacker can create a list of employee accounts in social networks.

To achieve the goals of this stage, the attacker can use *passive reconnaissance* and *active reconnaissance*. Passive reconnaissance is performed without the direct interaction with the IT infrastructure of the targeted organization. For example, the attacker may obtain DNS and Whois information related to the attacked organization. Active reconnaissance includes active contact with the targeted organization. For example, the attacker may scan open ports on computers in the organization's network, search for security vulnerabilities, or try to obtain information with social engineering.

## **Stage 2: Weaponization**

At this stage, the attacker uses the information obtained during the Reconnaissance stage to determine how the attack must be performed. The attacker chooses the *exploit*, the *payload*, and the method of delivering the exploit and the payload to the targeted organization.

An *exploit* is a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerabilities discovered at the Reconnaissance stage and delivers the *payload* of the attack. The attacker may use existing software or develop new software that is tailored specifically for the vulnerabilities of the targeted organization.

A *payload* is the software that is used by the attacker to reach the attack objectives. Depending on the attack objectives, the payload may contain malicious or legitimate software that would allow the attacker to access sensitive data or cause harm to the targeted organization.

The attacker can choose to deliver the exploit in a variety of ways. For example, the attacker may use infected Microsoft files or PDF documents, malicious software on removable storage devices, or email message attachments. The attacker may also trick company employees into visiting malicious and phishing URLs, or compromise online resources visited by company employees.

## **Stage 3: Delivery**

At this stage, the attacker delivers the exploit to the targeted organization.

Means of delivery usually include spam that contains infected attachments or links to external malicious resources. The attackers may also use other means to trick company's employees into visiting malicious or previously compromised web resources.

Other possible means of delivery include manipulating one of the company's employees into delivering the exploit manually, or compromising other companies that work with the targeted organization, in order to abuse the existing trust.

#### **Stage 4: Exploitation**

At this stage, the exploit takes advantage of the discovered vulnerabilities and delivers the payload.

For example, the exploit can use vulnerability in the network security to install malicious software on a computer in the organization's network. The malicious software then infects other computers in the organization's network and distributes the payload to all the infected computers.

#### **Stage 5: Installation**

At this stage, the payload installs itself, and tries to hide its activity to avoid detection or deletion.

Typically, the payload will try to install itself in such a way as to keep itself operable and undetected even if the vulnerability used by the exploit is found and fixed.

For example, the payload may contain a backdoor. The backdoor installs itself on the infected computer, modifies the system registry to run the backdoor on system startup, and hides its own process, so the user cannot see it in the list of running programs. While the backdoor is running, the attacker can connect to it and perform a number of activities on the infected computer.

#### **Stage 6: Command and control**

At this stage, the payload waits for incoming commands from the attacker.

The most common way of receiving the commands is by establishing a connection to the command and control server (or C&C server) within the targeted organization's network. The C&C server is controlled by the attacker. Once the connection is established, the attacker can send commands to the payload and take actions to achieve objectives. For example, if the payload contains the backdoor software, the attacker can assume control over the infected computers, access the information available on these computers, and spy on user activity.

If the infected computers have no direct access to the Internet and cannot establish a connection to the C&C server, the attacker can give commands to the payload by delivering other malicious software. This can be done, for example, by establishing a proxy on the same network, or even

using physical media to overcome an 'air gap' if the network is physically separated from all other networks.

### **Stage 7: Actions on objective**

At this stage, the attacker uses the payload and other software that was downloaded in the course of the attack to achieve the goals of the attack.

Once the attacker compromises one of the organization's assets, he or she will try to steal, change, or destroy data available on the compromised asset.

For example, if the goal of the attack was theft of sensitive data and the payload was the backdoor software, the attacker may assume control over the infected computers, and search for the required data stored on them.

If the data is not stored on the infected computers, the attacker may advance deeper into the compromised IT network, performing *lateral movement*. The attacker can use the computers under his or her control to infect more computers in the organization's network, steal user credentials to access unavailable computers, or even trick other employees into giving away the required data by impersonating the employees that use the compromised computers.

## **Incident response steps**

This section describes the basics of the incident response process.

### **About incident response**

*Incident response* (IR) is an organized process of addressing and managing the results of an incident (for example, a cyber attack).

The main goals of the incident response are:

- To minimize the damage of the attack.
- To minimize the time of recovery from the attack.
- To create instructions and defensive measures that would prevent such attacks in the future.

The process of incident response starts with the investigation of the security incident. When the security team investigates an incident, it must determine:

- Attack vector

Means by which the attacker has delivered the payload.

- Payload and exploit

Malicious software and other tools used by the attacker.

- Target of the attack

Networks, systems, and data affected by the attack.

- Damage inflicted

The amount of physical and reputational damage caused by the attack.

- Attack state

Current stage of the attack lifecycle, whether the attacker was able to perform actions to achieve objectives, and if the attacker reached the attack goals.

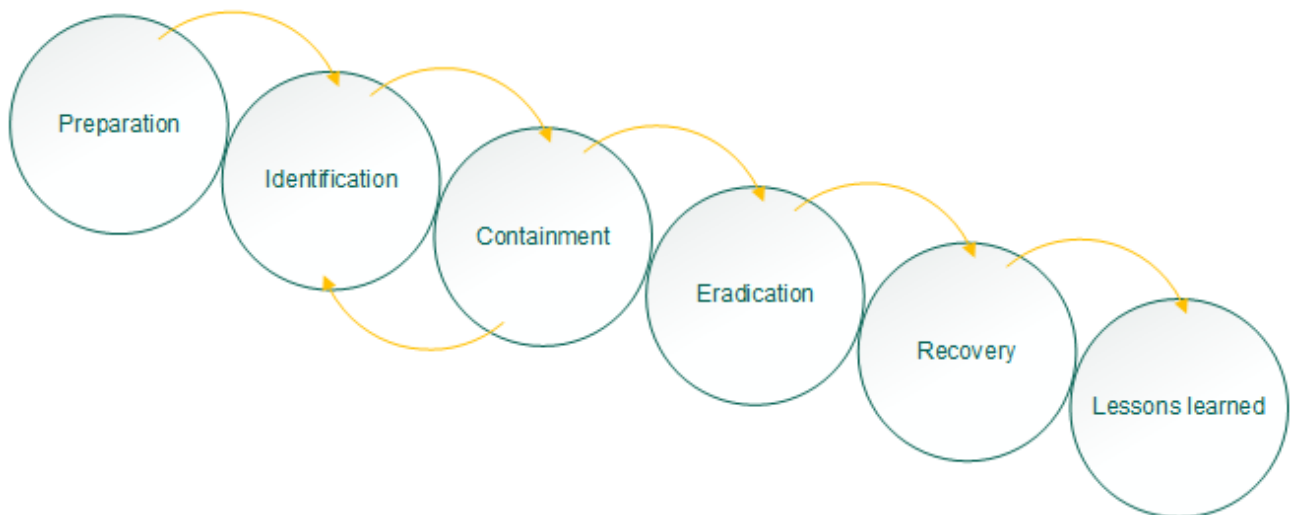
- Attack timeline

When the attack began and ended, when it was detected, and when the security team was able to react to the attack.

When the investigation is complete, the security team must use the obtained information to recover the targeted systems, and update the security policies and the IR plan.

### **About the incident response phases**

Based on the information about the attack lifecycle, the security team can create a defensive strategy and use it for incident response. An example of applying such a strategy is provided in the Incident response example chapter (on page [37](#)).



*Figure 2: Incident response phases*

The process of incident response includes the following phases:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons learned

### **Phase 1: Preparation**

When an attack occurs, the security team must take fast and precise actions. This requires preparation. Members of the security team must prepare processes, tools, and policies that can help prevent, detect, and respond to cyber attacks.

The preparation must also include training for company employees. All company employees must be familiar with the security policies and know what to do when faced with a cyber attack.

The security team that conducts incident response must build expertise by continuously gaining knowledge in the incident response field and through constant practice.



## Phase 2: Identification

In this phase, the security team must determine whether or not an event is an Information security incident. To do so, the security team must compare the available event information to the known *indicators of compromise*.

*Indicators of compromise (IOC)* are pieces of data that identify potentially malicious activity on a system or network. IOC examples include unusual network traffic, multiple failed login attempts, the presence of files used by malicious software, and suspicious registry or system file changes.

To collect IOC, the security team can get information from public reports and threat feeds, and perform static and dynamic analysis of malicious software.

Static analysis is performed without launching the software. It can be used to obtain several types of IOC, including web and email addresses used by the software, and hashes of its files.

Dynamic analysis requires execution of the software in the protected environment (sandbox or standalone computer). Dynamic analysis allows examination of software behavior and IOC gathering related to it.

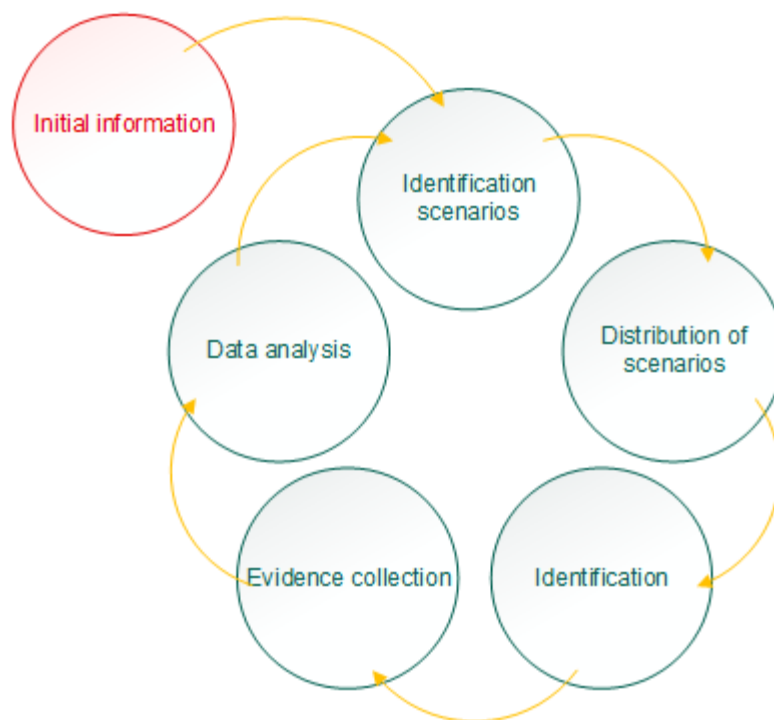


Figure 3: IOC collection cycle

Collecting IOC is a cyclic process. Based on the initial information about the attack, the security team can create the detection scenarios. Applying these scenarios usually enables detection of new IOC. The new IOC help to further identify the attack and obtain more information about it, thus creating a cycle.

Proceed through the remaining phases of the IR process only if an event is considered an incident.

### **Phase 3: Containment**

In this phase, the security team must identify the compromised computers and adjust the security policies to prevent further infection of the company assets. The security team must also reconfigure the organization's network to ensure that the existing business processes would continue running without the compromised assets.

For example, if one of the servers in the organization's network is compromised by the attacker, the security team must isolate this server from the network. The security team must also adjust routing policies to distribute this server's load to other servers.

### **Phase 4: Eradication**

In this phase, the security team must restore the compromised assets to their original state. This usually involves deleting malicious software, restoring the configuration, and deleting any artifacts that were left by the malicious software.

If the company's resources allow this, the compromised machine can be replaced with another machine that is not compromised. The infected machine is then retained in a preserved state in order to protect the evidence for the subsequent investigation.

For example, if a computer was compromised with backdoor software, the security team must delete the backdoor software, restore the compromised files and the system registry to the original state, and delete the backdoor software installation files.

### **Phase 5: Recovery**

In this phase, the previously compromised assets are put back into operation. The security team must monitor the condition of the assets for some time to make sure that the threat was completely eradicated.

For example, if one of the servers in the organization's network is restored, the security team puts it back into the organization's network, adjusts the routing policies to use this server, and monitors the server's behavior for some time to make sure that there is no suspicious activity.

## **Phase 6: Lessons learned**

In this phase, the security team must analyze the incident, develop measures that will help to prevent such incidents in the future, and update the incident response plan for incidents of this kind.

The measures may include adjusting security policies, changing the configuration of the organization's assets, and conducting the information security training for company employees.

The incident response plan is a set of written instructions that allow identification of the incident and responses to it. Even if it is not possible to completely prevent the incident in the future, the incident response plan will help to minimize the time it takes to identify the incident and improve the effectiveness of incident response.

---

# Recommended IR process and rules

This chapter describes rules and recommendations for performing incident response and conducting incident investigations.

## In this chapter

Preparation .....	<a href="#">20</a>
Identification .....	<a href="#">23</a>
Containment.....	<a href="#">33</a>
Eradication .....	<a href="#">35</a>
Recovery.....	<a href="#">35</a>
Lessons learned.....	<a href="#">36</a>

## Preparation

This section provides recommendations for the Preparation phase of the incident response process.

### Defensive measures

To effectively counter cyber attacks, the security team must take defensive measures that protect an organization's assets. It is recommended to create several layers of protection. A security system with several layers of protection can withstand cyber attacks that use multiple attack vectors and evasion techniques.

Adaptive Security Architecture is an information security approach that employs modern tactics and tools to counter cyber attacks. Adaptive Security Architecture goes beyond the traditional

defensive perimeter approach to creating security systems. A *Designing Adaptive Security Architecture for Protection from Advanced Attacks* report by Gartner outlines the four main elements of Adaptive Security Architecture: Predict Prevent, Detect and Respond. To provide a complete protection from advanced threats, all four elements should be implemented using a comprehensive set of solutions and services working together as a multi-layered, adaptive security system.

For example, consider the following Prevention measures:

- An endpoint protection solution is installed on all workstations.
- An intrusion prevention system is installed in the network.
- The gateway to the Internet is protected by a firewall.
- Internet access is available only through the organization's proxy server, a method that requires authorization.

Also, having Detection solutions working on the organization's network is highly recommended:

- The organization uses a SIEM system to track events. The SIEM system has integrated threat feeds.
- A specialized Anti-APT system is deployed in the organization's network. This system analyzes and correlates detection data from multiple security mechanisms, including intrusion detection systems, intrusion prevention systems, Sandboxes in order to discover less obvious attack indicators.
- Endpoint Detection and Response (EDR) capabilities enhance visibility on the Endpoint level and provide means of automated containment and eradication.
- There is a decoy system for the cyber attacks (also called a *honeypot*) that is isolated and closely monitored by the security team.

Kaspersky Lab experts continuously develop new security solutions that provide comprehensive protection against various types of information security threats, and network and phishing attacks:

- To protect workstations against known, unknown, and advanced threats, Kaspersky Lab experts developed Kaspersky Endpoint Security.

- To defend enterprises from targeted attacks and advanced threats, Kaspersky Lab experts created Kaspersky Anti Targeted Attack Platform (KATA).
- For existing solutions, Kaspersky Lab offers Threat Intelligence Data Feeds service, which is part of the Kaspersky Threat Intelligence Portal solution (on page [61](#)).

For more information about Kaspersky Lab solutions for enterprise security, see <http://www.kaspersky.com/enterprise-security>.

## **Security assessments**

In order to predict future cyber attacks, regular security assessments are necessary. Besides general security audits, organization can perform Penetration Testing and Application Security Assessment. Penetration Testing can reveal security weaknesses through life-like attack simulations. Application Security assessment can determine if key applications used by company are vulnerable to exploitation.

Penetration Testing and Application Security Assessment can be conducted by a third-party organization, with the results of the audits reported to the security team. The security team can then use this information to fix the vulnerabilities.

## **Gaining expertise**

Members of the security team must continuously increase their knowledge (through education) of incident response theory and practice.

Kaspersky Lab courses offer a broad curriculum in cybersecurity topics and techniques and assessment ranging from basic to expert. All are available either in classes on customer premises or at a local or regional Kaspersky Lab office, if applicable. For more information about the education, see <http://www.kaspersky.com/enterprise-security/intelligence-services>.

It is essential to have knowledge of events and trends in the information security field, as well as information about emerging cyber-security threats and about defensive measures against these threats. For example, the APT Reports service, which is part of the Kaspersky Threat Intelligence Portal solution (on page [61](#)), provides ongoing access to Kaspersky Lab investigations and discoveries in the field of high profile cyber-espionage campaigns.

## Collecting incident response information

The security team must collect information about incidents and the incident response process, and have a prepared incident response plan. This information can include incident reports and information about the history of incidents that happened within the organization.

# Identification

This section provides recommendations for the Identification phase of the incident response process.

## In this section

Incident triggers .....	<a href="#">23</a>
Prioritization guidelines .....	<a href="#">26</a>
Analyzing incidents in SIEM .....	<a href="#">28</a>

# Incident triggers

This section describes events that can be incident triggers.

The events and incident triggers described in this section do not constitute a full list of suspicious behaviors related to cyber attacks.

## What is an incident trigger?

An *incident trigger* is an event that indicates the presence of a cyber threat. When incident triggers are generated, the security team must be aware that a cyber attack may be in progress. An incident trigger allows a security team to differentiate incidents from events.

## About event sources

Events can come from many sources. Such sources may be Anti-APT systems, honeypot decoys, intrusion prevention systems, and many other security controls.

For the purposes of this guide, events are considered to come from a single category of event sources—SIEM systems and systems designed to manage the endpoint protection solutions in corporate networks.

### Incident triggers generated by SIEM systems

SIEM systems can aggregate information from a very broad scope of software and hardware security controls, including proxy servers and firewalls.

Among the events aggregated by SIEM systems, events generated as a result of matching security control events to threat feeds can be considered incident triggers. The presence of such events signals that indicators of compromise (IOC) from threat feeds were detected in the events generated by security controls.

For the purposes of this guide, it is assumed that Data Feeds from Kaspersky Lab are used to match the events in the SIEM. Data Feeds are part of Kaspersky Threat Intelligence Portal (on page [61](#)).

For example, malicious software on a computer in the organization's network tries to access a malicious URL. As with a regular URL, the organization's proxy server generates an event with the malicious URL and sends it to the organization's SIEM system. The SIEM system then tries to match this URL to Kaspersky Lab threat feeds. The match is successful because this is a malicious URL contained in the Kaspersky Lab threat feeds. The SIEM system receives a new event to signal this match. This new event can be considered an incident trigger.

### Incident triggers generated by endpoint protection management systems

Endpoint protection management systems (EPP management systems) can aggregate events from workstations protected by the endpoint protection solutions.

When an endpoint protection solution on one of the workstations or security controls detects a threat, it generates an event and sends it to the EPP management system.



Not all such events are incident triggers. For example, an event about detecting malicious software can be followed by an event about disinfecting this malicious software. In this case, no investigation is required.

Only the following events received by the EPP management system can be considered an incident trigger:

- Attempts to access a known C&C server
- Failed attempts to disinfect malicious software
- Repeated detection of malicious software on the same computer
- Errors and failures of the endpoint protection solutions that lead to a lowered protection level

The security team must react to these incident triggers in the same way that it reacts to receiving an event in a SIEM system that holds a malicious hash or a malicious URL. All the events from EPP management systems can also be sent to SIEM systems.

### **Suspicious behavior that can be an incident trigger**

There are other events that can be incident triggers. The presence of such events requires attention and investigation by the security team.

Following are examples of suspicious events:

- Presence of unknown software that runs automatically when the operating system starts.
- Presence of unknown services in the list of system services.
- Execution of files from directories that are unlikely to be used for running executable files, for example, from temporary directories and the system cache.
- Loading of dynamic libraries from directories where the presence of these dynamic library files is highly unlikely. For example, when a piece of software loads a system library from a directory where the software's executable file is located.

- Unexpected escalation of user privileges.
- Presence of legitimate software that can be used by the attacker. Examples of such software are Mimikatz, Windows® Credentials Editor, and many remote administration tools.

The following events constitute suspicious behavior related to network activity:

- Unexpected rise in the volume of DNS or ICMP protocol traffic.
- Interaction with domains that frequently change their IP address. This behavior might signal that the attacker uses the fast flux DNS technique to hide the C&C server behind a network of compromised hosts acting as proxies.
- Interaction with URLs that are categorized in the Kaspersky Lab threat feeds. For example, a URL may be categorized as a Malware source or an Exploit pack landing page.
- Interaction with IP addresses that are categorized in the Kaspersky Lab threat feeds. For example, an IP address may be categorized as an IP address used for scanning the network or as an IP address that is used to conduct DDoS attacks.
- Interaction with a domain that has suspicious Whois information.

## Prioritization guidelines

This section describes the basics of incident prioritization.

Time is the resource that is probably in shortest supply in the IR process. The amount of time between the start of an attack and the response of the security team determines whether or not the attacker reaches the attack goals. If the security team faces a large number of security incidents all at once, there may not be enough time to react to all of them. In this case, the incidents must be prioritized.

Incident priority must be determined based on the following factors:

- Network segment where the compromised computer is located.
- Value of the data stored on the compromised computer.

- Type and number of other incidents that affected the same computer.
- Reliability of IOC associated with the incident.

The final incident priority must be determined on the basis of the specifics of each organization. For some organizations the most dangerous incidents are those that involve ransomware (malicious software that encrypts data on infected computers) because the organization works with intellectual property or with sensitive data. Other organizations may prioritize incidents related to potentially dangerous software (such as pornware) because of the reputation risks associated with usage of this software.

As an example, the following prioritization of incidents may be used by the security team:

1. Incidents related to advanced persistent threats (APTs) have first priority.

For more information about detecting APTs, see subsection "Detecting Advanced Persistent Threats" below.

2. Incidents related to malicious software have second priority.
3. Incidents related to potentially dangerous software (adware, pornware, and so forth) have third priority.

## **Detecting advanced persistent threats**

An *advanced persistent threat (APT)* is a type of attack in which the attacker gains access to an organization's assets and tries to remain undetected for a long period of time. The goals of an APT attack most often include spying and theft of sensitive data.

To determine whether a detected attack must be considered an APT, use the following criteria:

- Presence of IOC from Kaspersky Lab APT Reports. APT Reports are a part of Kaspersky Threat Intelligence Portal solution (on page [61](#)).
- Interaction with C&C servers that were previously used by another APT. This interaction can be determined with static and dynamic threat analysis.

To analyze the behavior of the threat and to get a list of URLs that it interacts with, it is recommended to use tools and utilities described in the Tools for analysis section (on page [60](#)).

If IOCs of the threat have a popularity value of 2 or more in the Kaspersky Lab threat feeds, then the threat is regular malicious software. Such threats cannot be considered APTs.

It is also recommended to use the Threat Lookup service which is a part of Kaspersky Threat Intelligence Portal solution (on page [61](#)) to determine the popularity of the threat. If the popularity of the IOC (hash or URL) is low, then the threat may be considered an APT.

## Analyzing incidents in SIEM

This section describes the recommended sequence of actions for analyzing different types of incidents in SIEM systems.

### Actions for all incidents

When the security team receives an incident trigger in a SIEM system, it must follow this recommended sequence of actions:

1. Determine the original event that caused SIEM to generate an incident trigger event. This event has the IOC that was detected by SIEM.
  - If the threat was delivered in the email attachments, check the log files of the organization's mail server.
  - If the threat was delivered from the Internet, check the log files of the organization's proxy server, firewall, UTM gateway, or other device that provides access to the Internet.
2. Determine the current attack stage. This depends on the type of detected IOC. For example, if an interaction with the C&C servers was detected, the attack is at the Command and control stage.
3. Assess the importance of the information stored on the potentially compromised asset and the reliability of IOC associated with the incident. Depending on these two factors, adjust the priority for the incident.
4. Perform the rest of the actions depending on the type of detected threat, as described in the following sections.

If a threat was detected by an endpoint protection solution, then an incident response is required only in the following cases:

- The threat was not blocked by the endpoint protection solution.

For example, if an employee has successfully downloaded the malicious software.

- The threat was blocked, but the event occurred several times.

For example, if a computer in an organization's network continually tries to download the malicious software, it is possible that the computer is infected with malicious software that was not detected by the endpoint protection solution.

### **If the URL related to a threat was detected**

If the URL related to a threat was detected, perform actions based on the category of the URL. The values in parentheses are the categories in the threat feeds from Kaspersky Lab.

#### **► If a phishing URL was detected (*PHISHING* category):**

1. Inspect the source code of the web page that this URL leads to. Determine which information may have been given to the attacker by the employee.
2. In SIEM, analyze the events related to the attacked employee. This should be done for events in the range of 10 minutes before and 10 minutes after the phishing URL was visited by the employee.
  - If any files were sent or downloaded by the employee, perform the actions described in subsection "If a hash of the threat was detected", below, for the hashes of these files.
  - If no files were sent or downloaded by the employee, inform the employee about the incident. It is possible that additional actions are required, depending on the value of the information disclosed by the employee.
3. If there is a probability that the employee's credentials are compromised, change this employee's passwords.

► *If a malicious URL was detected (MALICIOUS category):*

1. Analyze proxy server events to determine if malicious software was downloaded.
  - If malicious software was not downloaded, then there is no risk that the affected asset was compromised. Such an event is not an incident and does not have to be investigated further. Make sure that the malicious URL is blacklisted.
  - If malicious software was downloaded, continue the investigation.
2. Determine whether the malicious software was blocked by defensive measures such as the organization's proxy server or endpoint protection solutions.
  - If the malicious software was blocked, and this was the first occurrence of such an event, then there is no risk that the affected asset was compromised. Such an event is not an incident and need not be investigated further.
  - If the malicious software was blocked, and this was not the first occurrence of such an event, continue the investigation.
  - If the malicious software was not blocked, continue the investigation.
3. Get samples of the malicious software that this URL leads to. If the URL leads to a web page, inspect the source code of the web page to determine which samples may be downloaded from it.
4. Analyze the samples of malicious software.

For more information about analyzing software samples, see section "Tools for analysis (on page [60](#))".

5. Determine if the downloaded malicious software was executed.
6. Scan the compromised computer for IOCs of the detected threat. Scan other computers in the same network segment for IOCs of the detected threat.

Include new IOCs obtained in the course of investigating these scans. For example, new IOCs can be obtained as a result of analyzing the malicious software samples.

7. Continue to the Containment phase (on page [33](#)) of the incident response process.

► *If a Botnet C&C URL was detected (BOTNET C&C category):*

1. Determine the software that tried to interact with the C&C server and analyze it.

For more information about analyzing software samples, see section "Tools for analysis (on page [60](#))".

2. Scan the compromised computer for malicious software. This software may be downloaded by using the commands received from the C&C server.

3. Analyze the URL.

For more information about analyzing URLs, see section "Tools for analysis (on page [60](#))".

4. Scan the compromised computer for IOC of the detected threat. Scan other computers in the same network segment for IOCs of the detected threat.

In these scans, include the new IOCs obtained in the course of the investigation. For example, new IOCs can be obtained from analyzing the URL.

5. Continue to the Containment phase (on page [33](#)) of the incident response process.

If a botnet C&C URL was detected, the attack has reached the Command and control stage. The attack is active at the moment.

► *If a mobile botnet C&C URL was detected (MOBILE BOTNET C&C category):*

1. Scan the compromised mobile phone with a mobile anti-virus solution.
2. Continue to the Containment phase (on page [33](#)) of the incident response process.

**If a hash of the threat was detected**

If a hash of the threat was detected, perform actions based on the category of hash. The values in parentheses are the categories in the threat feeds from Kaspersky Lab.

► *If a malicious or bot hash was detected (MALICIOUS and BOT categories):*

1. Analyze the malicious software that this hash belongs to.

For more information about analyzing software samples, see section "Tools for analysis (on page [60](#))".

2. Scan the compromised computer for IOCs of the detected threat. Scan other computers in the same network segment for IOCs of the detected threat.

In these scans, include new IOCs obtained in the course of the investigation. For example, new IOCs can be obtained from analyzing the malicious software.

► *If a mobile malicious, bot, or trojan hash was detected (MOBILE MALICIOUS, MOBILE BOT, and MOBILE TROJAN categories):*

1. Scan the compromised mobile phone with mobile anti-virus solution.
2. Continue to the Containment phase (on page [33](#)) of the incident response process.

## **If an IP address of the threat was detected**

If an IP address of the threat was detected, perform actions based on the category of the IP address. The following categories are the results of matching SIEM events with threat feeds from Kaspersky Lab.

► *If a Tor® exit node IP address was detected (TOR EXIT NODE category):*

1. Ask the employee if he or she uses Tor.
  - If the employee confirms that he or she uses Tor, then such an event is not an incident and need not be investigated further.
  - If the employee states that he or she does not use Tor, continue the investigation.
2. Scan the compromised computer for software that can use Tor. Such software may be legitimate software, or it may be malicious software that uses Tor to hide its activities. Scan other computers in the same network segment for malicious software.
3. Repeat the full identification process for detected software files.



► *If a spam IP address was detected (SPAM category):*

1. Continue to the Lessons learned phase (on page [36](#)) of the incident response process.

► *If a malicious software IP address was detected (MALWARE category):*

1. Determine the software that tried to interact with the IP address, and analyze it.

For more information about analyzing software samples, see section "Tools for analysis (on page [60](#))".

2. Perform the actions for malicious URLs described in subsection "URL address of the threat was detected" above.

## Containment

This section provides recommendations for the Containment phase of the incident response process.

### Goals of the Containment phase

The Containment phase has two major goals:

- To isolate the compromised assets while keeping the system operable.
- To prevent the deletion of IOC that may be used for investigation.

### Isolating compromised computers

It is recommended to put the compromised computers into a separate isolated network. The security team must change the routing policies to prevent the compromised computers from communicating with other computers in the organization's network and with the Internet.

It is not recommended to shut down the compromised computers. Some types of malicious software keep themselves in memory and do not create files on the hard disk. If a computer with such malicious software is turned off, the IOC for this malicious software will be lost. Other types of malicious software delete their IOC when the system receives a shutdown signal. This will make the investigation more difficult.

It also is not recommended to disable the local network connections of the compromised computers or to physically disconnect them from the network. Some types of malicious software track the status of the local network connection on the compromised computer. If the connection has been disabled for some period of time, the malicious software may begin to delete the signs of its presence, thus destroying the IOC.

## **Creating memory and hard disk dumps**

To continue the investigation, the security team must obtain memory and hard disk dumps from the compromised computers. These dumps contain all the components of the malicious software.

By analyzing memory and hard disk dumps of compromised computers, the security team can obtain the samples of malicious software and IOC associated with the attack, and determine the attack vector.

This information can be used to prevent further attacks of the same type from reaching the Delivery, Exploitation, or Installation stage. By analyzing samples of the malicious software, the security team can find a way to effectively eradicate the malicious software.

If it is very difficult to send memory and hard disk dumps to the security team, it is recommended to send the memory dumps first. After the security team analyzes the memory dumps, the team must decide if they also need the hard disk dumps. For example, such a situation may occur if an organization has several geographically separated offices and a security team is present only in one of them.

For more information about the recommended tools for creating memory and hard disk dumps, see section "Tools for creating dumps (on page [58](#))". For more information about tools for analyzing memory and hard disk dumps, see sections "Tools for analyzing memory dumps (on page [64](#))", and "Tools for analyzing hard disk dumps (on page [67](#))".

The full dump of a hard disk always takes up the full amount of hard disk space available on the hard disk. This happens because the hard disk dump also includes information from free (unused) sectors of the hard disk. For example, if a hard disk has a volume of 400 gigabytes (GB), and 50 GB of the hard disk space is used, the dump of this hard disk will take 400 GB.

## **Preserving operability**

After compromised computers are isolated, the system must retain its operability. For example, if several servers in the organization's network were compromised, the security team must change routing policies so that other servers take the load of the compromised servers.

# Eradication

This section provides recommendations for the Eradication phase of the incident response process.

There are two possible strategies for the Eradication phase:

- Full recovery of the compromised asset.

For example, a workstation can be recovered from a workstation image.

This strategy is well suited for organizations that use the standard set of software for employee workstations. If the compromised asset is a mobile phone or another hardware device, a factory reset can be used, with a subsequent restoration of the configuration parameters.

- Detection of malicious software and removal of its files and all of the artifacts created by it from the compromised asset.

For example, a workstation infected by backdoor software can be recovered by deleting the backdoor and all files created by it from the hard disk, and by restoring the system registry to its original condition.

The artifacts created by the malicious software can be detected by analyzing the malicious software with tools and utilities described in section "Tools for analysis (on page [60](#))".

# Recovery

This section provides recommendations for the Recovery phase of the incident response process.

In this phase, the previously compromised assets are put back into operation. The security team must monitor the condition of the assets for some time to make sure that the threat was completely eradicated.

For example, if one of the servers in the organization's network is restored, the security team puts it back into organization's network, adjusts routing policies to use this server, and monitors the server's behavior for some time to make sure that there is no suspicious activity.

# Lessons learned

This section provides recommendations for the Lessons learned phase of the incident response process.

After the investigation is completed, the security team must create a report. This report must contain answers to the following questions:

- When was the incident detected and by whom?
- What is the scope of the incident? Which assets were affected by the incident?
- How were the Containment, Eradication, and Restoration phases performed?
- In which phases of the incident response process was the security team most effective?
- In which phases of the incident response did the actions of the security team need improvement?

Based on the report and the information obtained during the investigation, the security team must develop measures that will help to prevent such incidents in the future, and update the incident response plan for incidents of this kind.

The measures may include adjusting security policies, changing the configuration of organization's assets, and conducting the information security training for company's employees. The IOC obtained in the course of the incident response can be used by the security team to detect other attacks of this kind in the future.

The incident response plan must include a set of written instructions that allow identifying the incident and responding to it. Even if it is not possible to completely prevent the incident in the future, the incident response plan will help to minimize the time it takes to identify the incident and improve the effectiveness of incident response.

---

# Incident response example

This chapter provides an example of a cyber attack and an example of incident response conducted by the security team.

## In this chapter

The attack plan .....	<a href="#">37</a>
The incident response .....	<a href="#">42</a>

## The attack plan

This section provides an example of a planned cyber attack. In this example, a criminal tries to gain control over the ATM control system of a bank (ATM gateway) in order to withdraw money from ATM terminals.

### Attack goal, payload, exploit, and means of delivery

The goal of the attack is to withdraw money from ATM terminals. The goal is achieved when the attacker gains control over the ATM gateway and compromises the ATM terminals.

The payload of this attack is the loader software. After it is delivered, the loader software will download, install, and run the bot software (described below). Afterwards, the loader software will keep monitoring the bot software. If the bot software is eradicated, the loader software will download and install it again. For example, an endpoint protection solution may eradicate the bot software, but the loader software will install it again and again.

The bot software will allow the attacker to control the compromised computer remotely by sending commands from a C&C server. The bot software has the backdoor software functionality, which allows the attacker to assume control of the compromised computer.

The attacker will use supplementary software to steal the user credentials. He or she chooses the Mimikatz utility, which is legitimate software that can be used for this purpose. After the bot

software establishes connection to the C&C server, the bot software will download Mimikatz from a URL provided by C&C server.

The final piece of software that will be used in this attack is custom software developed by the attacker to compromise the ATM terminals that are located behind the ATM gateway. This software will be downloaded by the bot software once the attacker gains access to the ATM gateway.

The exploit of this attack is contained in the PDF file, which contains the loader software. By taking advantage of a vulnerability in Adobe® Acrobat® Reader software, the exploit will run the loader software when the document is opened.

The attacker delivers the exploit with a spear phishing attack. The exploit will be attached to email messages that are sent to employees of the targeted organization.

### **Stage 1: Reconnaissance**

The attacker gains information about the way to compromise the ATM terminals. To do so, the attacker must gain control over the ATM gateway of a bank, which is a heavily protected asset.

The attacker creates a list of banks that use the same type of ATM gateway. The attacker then collects information about security measures employed by each bank. The attacker analyzes the available information and chooses the target. By using social engineering, the attacker obtains a list of bank employees and their corporate email addresses.

### **Stage 2: Weaponization**

Because an effort to breach the bank's security perimeter is very unlikely to succeed, the attacker chooses to strike from within, by conducting a spear phishing attack on the organization's employees.

The attacker chooses the payload, exploit, and means of delivery described in subsection "Attack goal, payload, exploit, and means of delivery" above.

### **Stage 3: Delivery**

The attacker conducts a spear phishing attack. He or she sends email messages to several employees from the employee list obtained through social engineering. The attacker chooses employees based on their vulnerability to the spear phishing attack. For example, financial department employees may be useful targets for this type of attack.

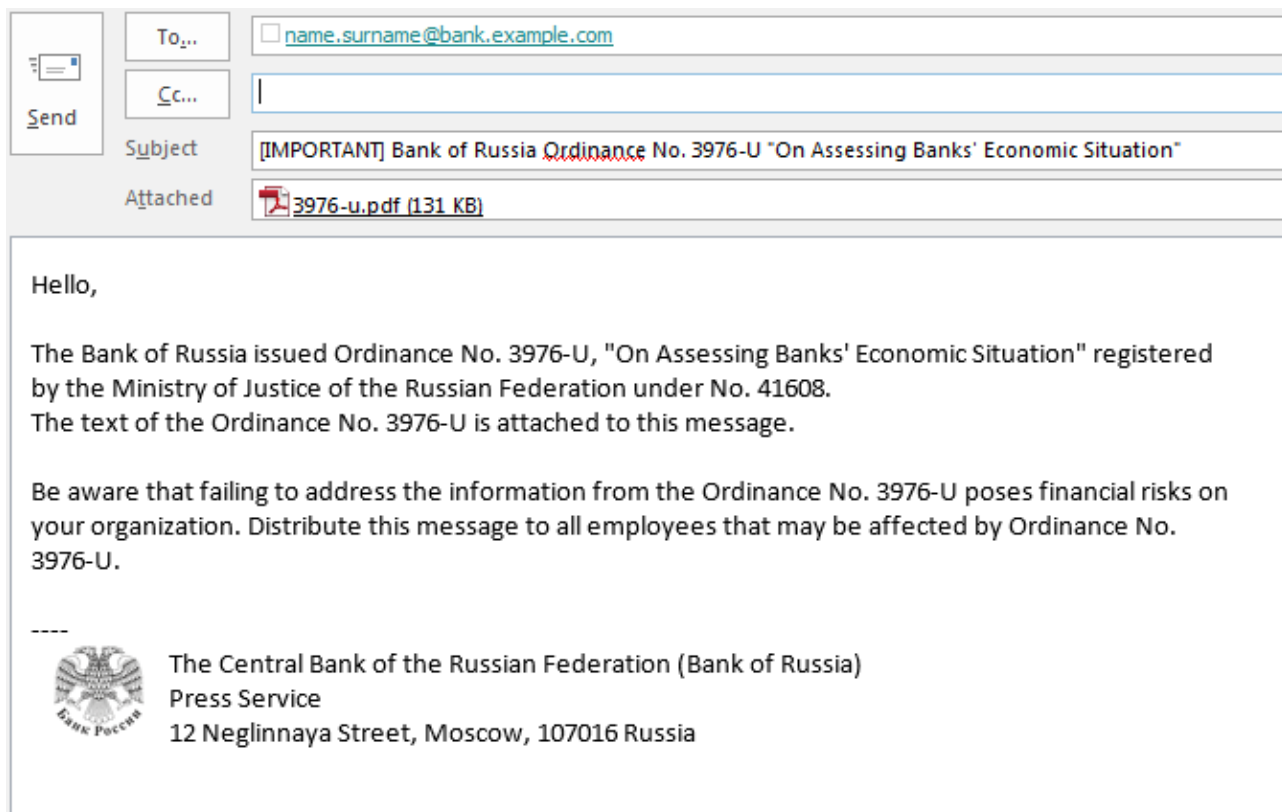


Figure 4: The spear phishing attack is conducted by means of email messages

The email messages seem to be coming from the financial regulatory authority of the country (Bank of Russia). The text of these email messages is worded so as to trick an employee into opening the attached PDF document.

#### Stage 4: Exploitation

After an employee opens the PDF file in Acrobat Reader, the files of the loader software are copied to the employee's computer hard disk and the loader software is added to the list of startup programs on the operating system.

#### Stage 5: Installation

On the next startup of the compromised computer, the operating system will run the loader software. The loader software will download the bot software, install it, and add it to the list of startup programs. After these actions are completed, the loader software will monitor the status of the bot software. If the bot software is not present in the system, the loader software will repeat the installation step.

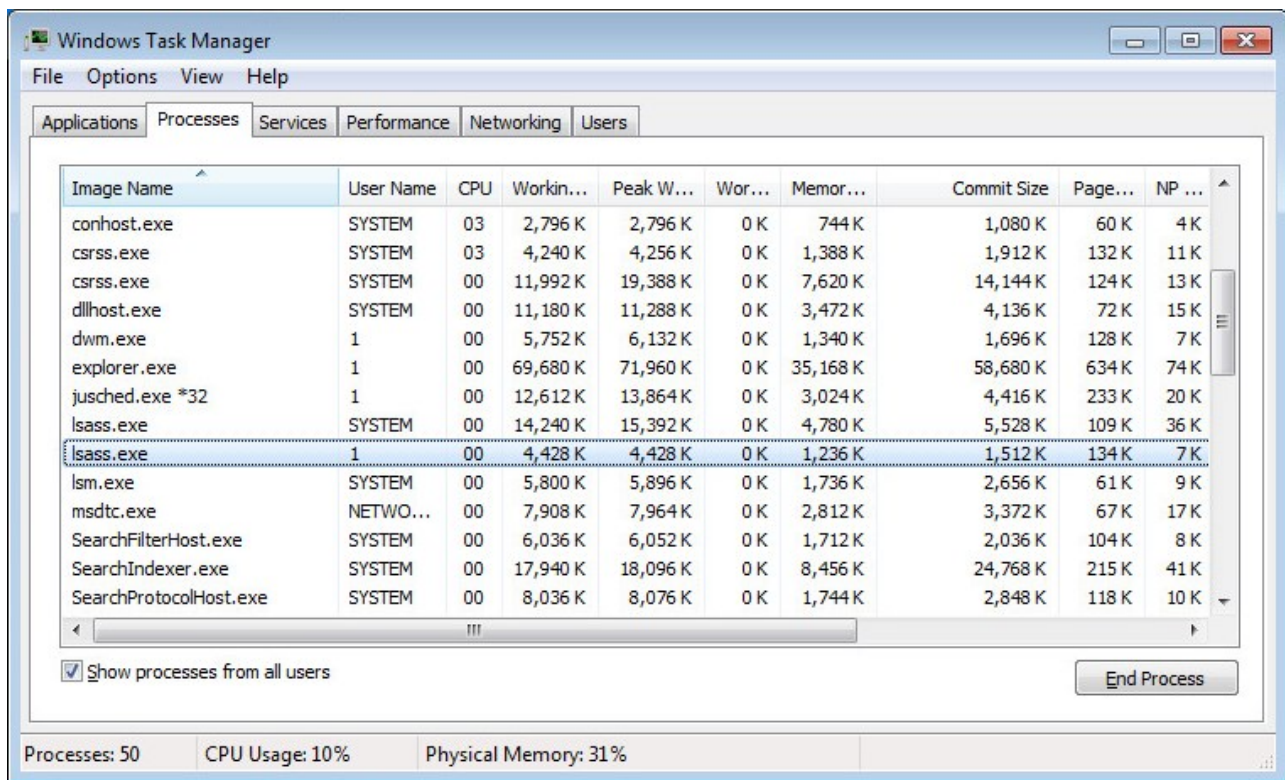


Figure 5: The bot software disguises itself as lsass.exe

The bot software tries to hide its presence from the user by disguising itself as a known legitimate system process lsass.exe (Local Security Authentication Server). This software is always present in the list of processes on Windows operating systems.

## Stage 6: Command and control

The bot software establishes a connection to the C&C server controlled by the attacker.

## Stage 7a: Actions on objective (lateral movement)

The first command that the attacker gives to the bot software is to infect other computers in the organization's network.

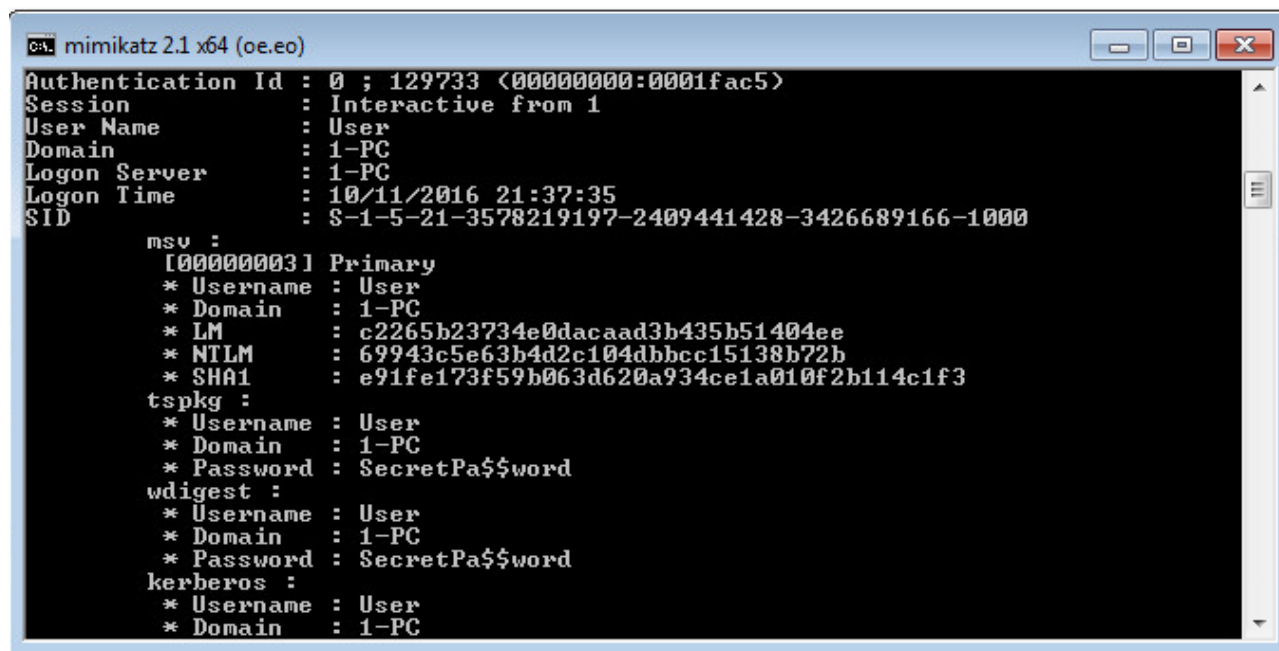
The bot software uses the compromised computer's access rights and user privileges, as well as known vulnerabilities, to deliver the exploit to other computers. The attacker may also choose to compromise other PDF documents that are used within the organization.

The goal of this step is to compromise the computer where an Administrator account has been logged in since the last operating system startup.



## Stage 7b: Actions on objective (theft of credentials)

When a computer (on which an Administrator account is logged in) is found and compromised, the bot software will download Mimikatz and run it.



```
C:\> mimikatz 2.1 x64 (oe.eo)
Authentication Id : 0 ; 129733 (00000000:0001fac5)
Session          : Interactive from 1
User Name        : User
Domain           : 1-PC
Logon Server      : 1-PC
Logon Time       : 10/11/2016 21:37:35
SID              : S-1-5-21-3578219197-2409441428-3426689166-1000

msu :
[00000003] Primary
* Username : User
* Domain   : 1-PC
* LM       : c2265b23734e0dacaad3b435b51404ee
* NTLM     : 69943c5e63b4d2c104dbbcc15138b72b
* SHA1     : e91fe173f59b063d620a934ce1a010f2b114c1f3
tspkg :
* Username : User
* Domain   : 1-PC
* Password : SecretPa$$word
wdigest :
* Username : User
* Domain   : 1-PC
* Password : SecretPa$$word
kerberos :
* Username : User
* Domain   : 1-PC
```

Figure 6: Mimikatz is used by the attacker to steal user names and passwords

The attacker will use Mimikatz to get the user names and passwords (including Microsoft® Active Directory® user credentials) of all users that have logged in on this computer since the last operating system startup. The goal of the attacker at this stage is to obtain the password of the Active Directory Administrator account.

## Stage 7c: Actions on objective (compromising the ATM gateway)

The attacker commands the bot software to gain access to the ATM gateway. The bot software gains control over the ATM gateway using the Administrator credentials obtained at the previous stage. The attack goal is reached.

When the ATM gateway is under control, the bot software downloads and runs the custom software developed by the attacker to compromise the ATM terminals. This action can succeed because the ATM gateway no longer prevents the attacker from accessing the ATM terminals. The attacker then can withdraw money from the compromised ATM terminals by controlling them from the C&C server. For example, the attacker can simulate a cash withdrawal operation for a certain ATM terminal and compel the terminal to dispense the contents of the cash tray.

### Stage 7d: Actions on objective (destroying the evidence)

After the attack goal is reached, the attacker commands the bot software to destroy any evidence of the attack. The goal of this stage is to postpone identification of this attack and to make the investigation more difficult. The bot software will delete itself, the loader software, and Mimikatz from the compromised computers. The bot software also will try to delete artifacts that it created, such as compromised PDF documents.

## The incident response

This section provides an example of an incident response to a cyber attack. In this example, the security team of an attacked bank tries to counter the attacker's attempts to gain control over the bank's ATM control system (ATM gateway).

### In this section

Preparation (example).....	<a href="#">42</a>
Identification (example) .....	<a href="#">44</a>
Containment (example).....	<a href="#">45</a>
Eradication and Recovery (example).....	<a href="#">51</a>
Lessons learned (example) .....	<a href="#">52</a>

## Preparation (example)

This section describes the defensive measures taken by the bank to prevent cyber attacks.

The corporate network of the bank is designed with security considerations in mind.

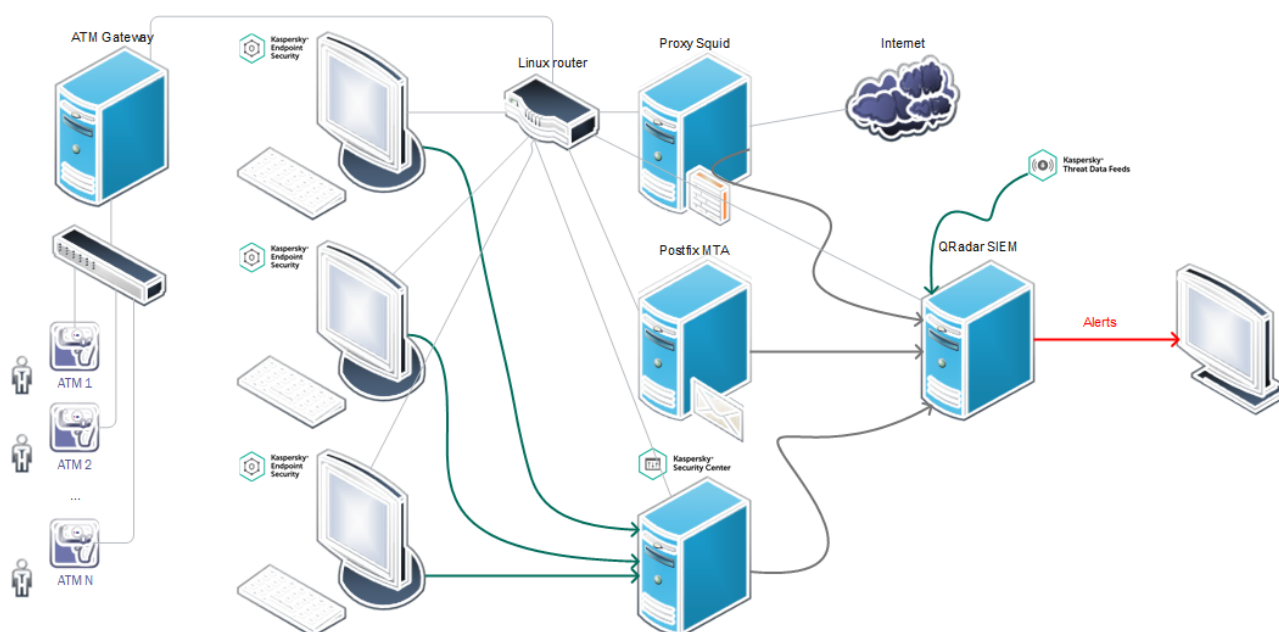


Figure 7: Corporate network of the bank

The bank employs the following defensive measures to counter cyber attack. The bank uses a IBM® QRadar® SIEM system to track events. Kaspersky Lab threat feeds are integrated in the SIEM system.

- Internet access from the organization's network is available only through a Squid proxy server. The proxy server is configured to send events to the SIEM system.
- The bank uses the Postfix mail transfer agent (MTA) for transferring organization's email messages. Postfix MTA also sends events to the SIEM system. These events have information from the email message headers, including the "Received" headers.
- All workstations in the bank's network are protected by Kaspersky Endpoint Security, controlled by Kaspersky Security Center. All alerts from Kaspersky Security Center are sent to the SIEM system.
- The router of the bank operates on Linux® operating systems. The ATM gateway and the ATM terminals are located in an isolated network. Only a small number of users are permitted to access this network.
- The bank has an active subscription to the Kaspersky Threat Intelligence Portal solution (on page [61](#)).

# Identification (example)

This section describes the Identification phase of the incident response example.

## What is likely to happen?

Because the bank uses the SIEM system, all URLs visited from employees' computers and all IP addresses that try to interact with the organization's network are matched to threat feeds. All downloaded files on the workstations are scanned by the endpoint protection solution. The endpoint protection solution also sends hashes of these files to the SIEM system, where they are matched to the threat feeds.

The attack will probably be identified at one of these stages:

- The IP address of the server used by the attacker to send the spear-phishing email messages will match the IP Reputation threat feed. In this case, the attack is identified at the Delivery stage.
- The request for downloading the bot software will match the Malicious URL threat feed. In this case, the attack is identified at the Installation stage.
- The request for connection to a C&C server will match the Botnet C&C URL threat feed. In this case, the attack is identified at the Command and control stage.
- Mimikatz will be detected and deleted by the Kaspersky Endpoint Security solution which protects the workstation. In this case, the attack is identified at the Actions on objective stage.

The attack is unlikely to succeed because preventing the attacker from executing any stage in the attack lifecycle (kill chain) blocks the attack.

## Botnet C&C URLs are detected by SIEM

For the purposes of this example, it is assumed that the attack reached the Command and control stage.

The Identification phase of the IR process begins when a member of the security team receives an incident trigger in the SIEM system.

	Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:22:0...	Botnet Address	10.65.65.65
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2	1	Oct 13, 2016, 7:21:5...	Botnet Address	10.65.65.65

Figure 8: Requests to the Botnet C&C URLs are detected in the SIEM system

In this case, a request to the C&C server was made from the organization's network. The member of the security team classifies this event as an incident trigger, because the Incident Response Guide states that such events are always incident triggers.

## Containment (example)

This section provides an example of conducting the Containment phase of the incident response process.

### Identifying the compromised computers

Requests to the C&C server are a sign of an active attack. The first priority in such a case is to identify the compromised computers and isolate them in a separate network that has no access to the organization's network and the Internet.

To identify the compromised computers, the security team makes a search in the SIEM system for all events associated with requests to the Botnet C&C URL. All network computers in the organization's network that made such requests are compromised.

As was stated in the Incident response steps section (on page [14](#)), collecting IOC is a cyclic process. Later in this example, the security team analyzes the Botnet C&C URL using the Threat Lookup service of Kaspersky Threat Intelligence Portal solution (on page [61](#)). The security team obtains hashes of the malicious software related to this Botnet URL. These hashes are additional IOC that can be used to determine other compromised computers. The next step is to obtain even more IOCs and identify even more compromised computers by getting a list of all URLs accessed by the malicious software that has these hashes. These extra URLs are likely to be other malicious URLs and Botnet C&C URLs.

### Isolating the compromised computers

The security team isolates the compromised computers using the `iptables` program on the organization's router.

For example, a compromised computer's IP address is 192.168.0.3. Executing the following command on the organization's router prevents the compromised computer from sending and receiving any data over the network:

```
iptables -A FORWARD -s 192.168.0.3 -j DROP
```

The security team also adds the Botnet C&C URL that was visited by the compromised computers to the black list. If there are other compromised computers in the organization's network that are as yet unidentified, they will not be able to interact with the C&C server.

### Identifying the attack vector

To identify the attack vector, the security team analyzes all events related to the compromised computers in the QRadar SIEM system.

	Event Name	Log Source
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_BotnetCnC_URL	KL_Threat_Feed_Service_v2
	KL_Malicious_URL	KL_Threat_Feed_Service_v2
	KL_Malicious_URL	KL_Threat_Feed_Service_v2
	KL_IP_Reputation	KL_Threat_Feed_Service_v2

Figure 9: All events that are related to compromised computers and that match threat feeds from Kaspersky Lab

In this example, the earliest event is a match with the IP Reputation threat feed (KL\_IP\_Reputation). The service headers of spear-phishing email messages used by the attacker contained an IP address that was matched to Kaspersky Lab threat feeds. The IP reputation threat feed contains IP addresses associated with spam and phishing attacks. It means that the attack began with delivery of the email messages to bank employees.

Normally, communication with this IP address will be blocked by one of the defensive measures used by the organization, but for the purposes of this example it is assumed that there was no response to this event.

Upon further investigation of the event, the security team finds the email messages from the attacker. Now the security team can analyze the attachments of these email messages to investigate the exploit used by the attacker. Also, by finding all the recipients of the email messages, the security team may be able to determine other computers that are targeted (and possibly compromised by the attack) and prevent the employees from activating the exploit.

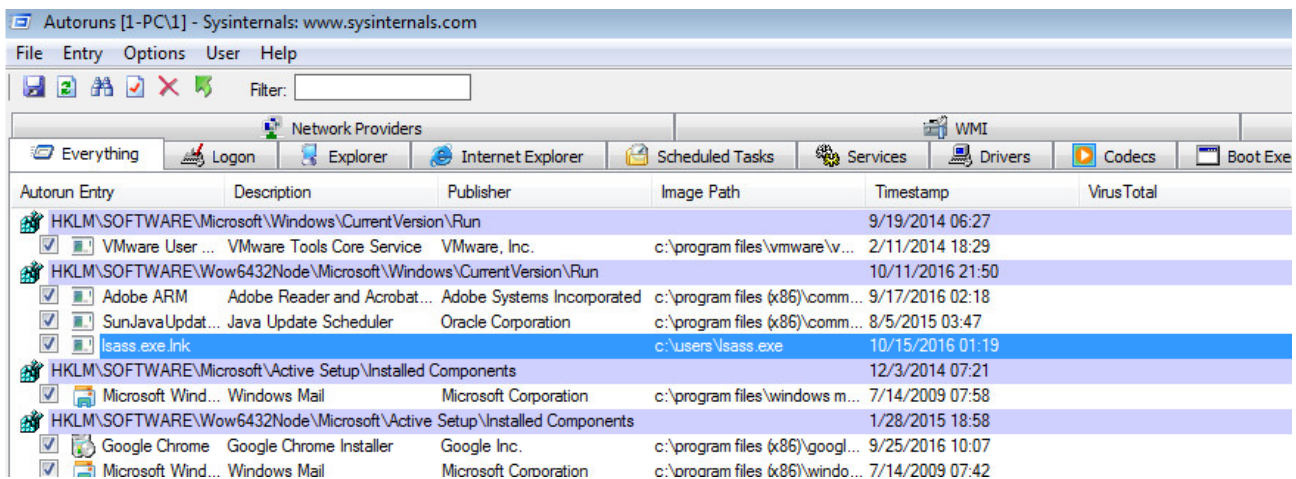
## Analyzing the malicious software

After the compromised computers are isolated, the security team continues its investigation and analyzes the compromised computers.

The security team can use the Threat Lookup service of Kaspersky Threat Intelligence Portal solution to get the information related to the Botnet C&C URL address. Such information includes the hashes of the malicious software files related to this URL and the description of the software related to this URL.

For the purposes of this example, it is assumed that the security team did not use the Threat Lookup service of Kaspersky Threat Intelligence Portal solution. Instead, the security team will try to get information about the malicious software used by the attacker by analyzing the compromised computer with the Autoruns utility (on page 54) from Microsoft Sysinternals and the Volatility tool (on page 64).

If the security team has direct access to the compromised computer, a member of the security team runs the Autoruns utility on it.



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				9/19/2014 06:27	
<input checked="" type="checkbox"/> VMware User ...	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\v...	2/11/2014 18:29	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				10/11/2016 21:50	
<input checked="" type="checkbox"/> Adobe ARM	Adobe Reader and Acrobat...	Adobe Systems Incorporated	c:\program files (x86)\comm...	9/17/2016 02:18	
<input checked="" type="checkbox"/> SunJavaUpdat...	Java Update Scheduler	Oracle Corporation	c:\program files (x86)\comm...	8/5/2015 03:47	
<input checked="" type="checkbox"/> Isass.exe Link			c:\users\Isass.exe	10/15/2016 01:19	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				12/3/2014 07:21	
<input checked="" type="checkbox"/> Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows m...	7/14/2009 07:58	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				1/28/2015 18:58	
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files (x86)\googl...	9/25/2016 10:07	
<input checked="" type="checkbox"/> Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files (x86)\windo...	7/14/2009 07:42	

Figure 10: Analyzing startup programs with Autoruns

The Autoruns tool helps the security member to detect a suspicious Isass.exe file located in the c:\users directory. The presence of such a startup program is highly unlikely on the standard workstations used by the bank employees. If the security team has no direct access to the compromised computer, an employee who has access follows the security team's instructions to create a memory dump of the compromised computer and sends it to the team. AccessData Forensic Toolkit (on page 59) is used to create the memory dump.

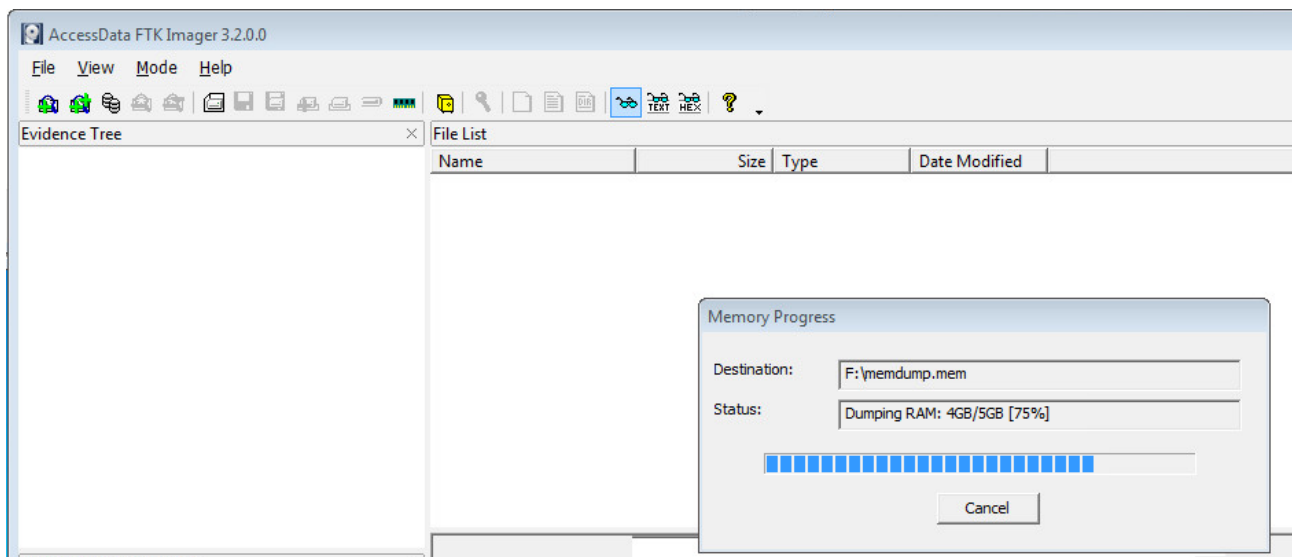


Figure 11: Creating a memory dump of the compromised computer with the FTK Imager utility

After the security team acquires the memory dump, a member of the security team uses the Volatility tool (on page [64](#)) to get a list of processes on the compromised computer.

```
C:\Users\User\volatility_2.5>volatility.exe pslist -f C:\Users\User\Memdump\1-PC.mem
--profile=Win7SP0x64
```

Volatility Foundation Volatility Framework 2.5

Offset (V)	Name	PID	PPID	Thds	Hnds	Sess
0xfffffa8003c6c890	System	4	0	96	2276	-----
0xfffffa8004400950	smss.exe	264	4	2	29	-----
0xfffffa80048e3b30	csrss.exe	352	344	9	620	0
0xfffffa8004b57420	wininit.exe	404	344	3	76	0
0xfffffa8004b45b30	csrss.exe	412	396	10	280	1
0xfffffa8004b7a6a0	winlogon.exe	448	396	3	108	1
0xfffffa8004bcc2e0	services.exe	508	404	7	224	0
0xfffffa8004ca9b30	lsass.exe	516	404	8	847	0
0xfffffa8004cadb30	lsmd.exe	524	404	10	189	0
0xfffffa8005b37660	explorer.exe	1976	1916	33	992	1
0xfffffa8005ce4b30	lsass.exe	2336	1976	10	231	1
0xfffffa8005ceab30	svchost.exe	2348	508	14	334	0



The Volatility tool output shows two lsass.exe processes. The lsass.exe process with PID 516 has PPID 404 (parent PID), which means that it was started by the wininit.exe process (PID 404). The other lsass.exe process with PID 2336 has PPID 1976, which means that it was started by the explorer.exe process (PID 1976). The second lsass.exe process is highly suspicious, because the explorer.exe process is part of Windows Explorer, which is not used to run system processes such as lsass.exe.

Once the malicious software is identified (lsass.exe), the security team must make sure that this software was indeed used to make requests to the C&C server. A member of security team performs a static analysis on the malicious software. He or she uses the Strings utility (on page [68](#)) to search the lsass.exe file for the C&C server URL.

One of the Strings utility parameters defines the length of the symbol. The member of the security team scans the lsass.exe file with different values for this parameter to get ASCII and Unicode strings from the file.

By using the Strings utility with the default parameters, the member of the security team gets the following output (fragment):

```
$ strings -a 'lsass.exe'

f:\dd\vc\tools\crt\crtw32\dllstuff\atoneexit.c

>"g/

BSJB

v4.0.30319

#Strings

#GUID

#Blob

`~, #
```

Then the security team member searches for the Unicode strings, specifying 16-bit strings with `-e 1` parameter. The result is the following output (fragment):

```
$ strings -a -e 1 'lsass.exe'

*.msg

__native_startup_state == __initialized
```

```
_controlfp_s(((void *)0), 0x00010000, 0x00030000)

http://subbotnet-domain_19.botnet-domain.example.com/page/c

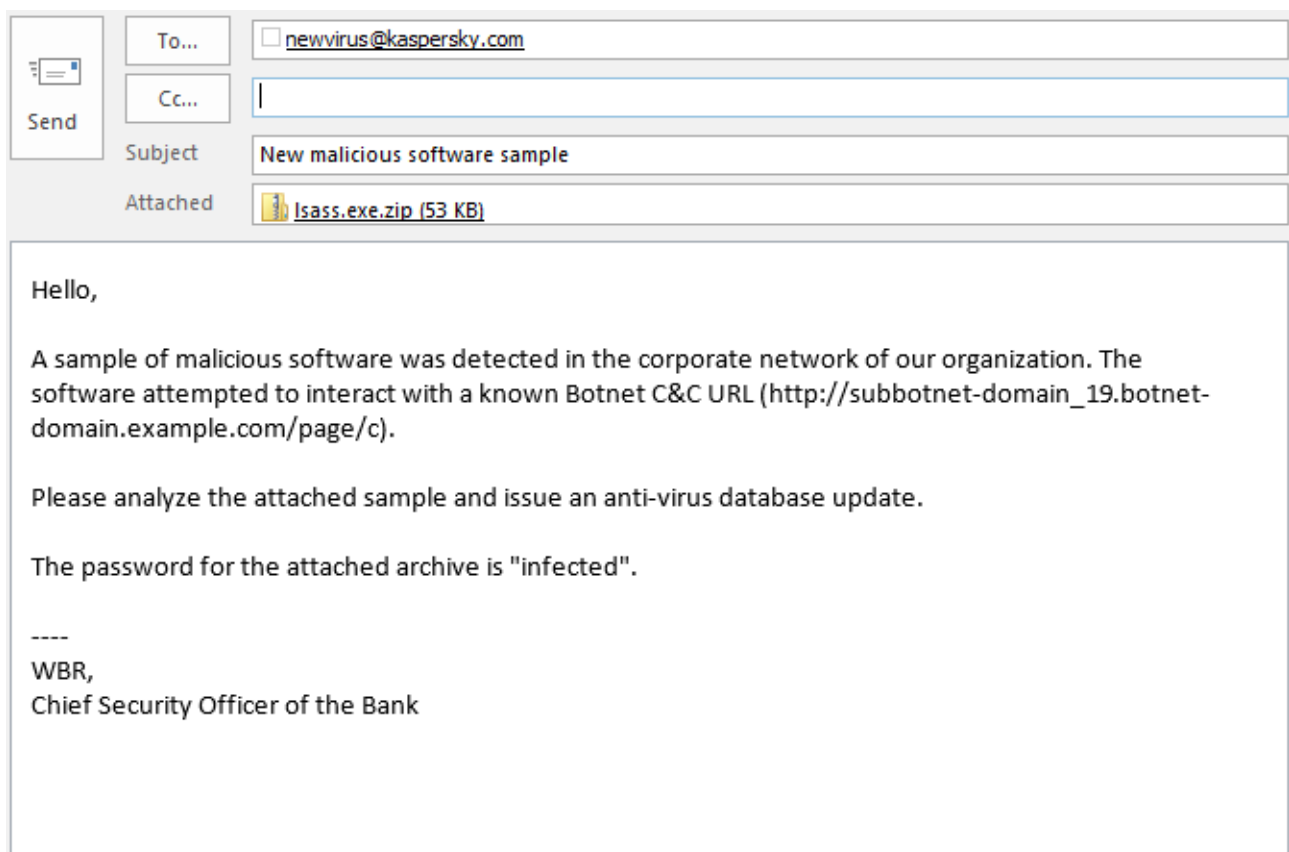
find_proxy

{0}: {1}

--- Start of primary exception ---
```

The `http://subbotnet-domain_19.botnet-domain.example.com/page/c` is the Botnet C&C URL detected by the SIEM system.


The last step in analyzing the malicious software is to send the sample to an anti-virus software company. In this example, the security team sends the malicious software sample to Kaspersky Lab.



**To...**

**Cc...**

**Subject**

**Attached**  [Isass.exe.zip \(53 KB\)](#)

**Send**

Hello,

A sample of malicious software was detected in the corporate network of our organization. The software attempted to interact with a known Botnet C&C URL (`http://subbotnet-domain_19.botnet-domain.example.com/page/c`).

Please analyze the attached sample and issue an anti-virus database update.

The password for the attached archive is "infected".

----

WBR,  
Chief Security Officer of the Bank

Figure 12: Sending the malicious software sample to Kaspersky Lab

Kaspersky Lab experts will analyze the received sample, which will be included in the database update for endpoint protection solutions. This will help to protect other computers from this software in the future.

## Analyzing the exploit and the payload dynamically

The exploit that was detected by the security team while identifying the attack vector must also be analyzed.

The security team analyzes the attachments from the email messages used by the attacker. A member of the security team performs the dynamic analysis of the exploit using the Sandbox service of Kaspersky Threat Intelligence Portal solution (on page [61](#)). As an alternative, he or she can use an isolated virtual machine to perform the dynamic analysis.

The dynamic analysis of the exploit helps to determine the behavior of the exploit. The exploit installs the loader software and tries to download the malicious software.

The security team may also analyze the malicious software downloaded by the exploit. The analysis would confirm that the malicious software tries to access the C&C server.

## The results

By isolating the compromised computers, the security team was able to stop the attack. Further analysis of the compromised computers and malicious software helped the security team to reconstruct the attack plan:

- The attack was conducted via spear-phishing email messages.
- The exploit is the PDF document which compromises the computer by installing the loader software.
- The loader software tries to download the bot software.
- The malicious software tries to make requests to the C&C server. These requests were detected by the security team and the C&C server URL was blacklisted.

As a result, the attack was stopped without causing any damage. The bank management decided that there was no need to notify law enforcement about the attack. The security team proceeds to the Eradication phase (on page [51](#)).

# Eradiation and Recovery (example)

This section provides an example of the Eradication and Recovery phases of the incident response process.

The security team removes the malicious software from the compromised computers. All the computers in the organization's network were scanned for the IOC detected by the security team. This scan revealed no additional compromised computers.

The organization's router is reconfigured to allow the previously compromised computers to send and receive data from the bank's network and from the Internet.

For example, to return the compromised computer with IP address `192.168.0.3` back to the organization's network, a following command can be executed:

```
iptables -D FORWARD -s 192.168.0.3 -j DROP
```

## Lessons learned (example)

The security team creates a report about the incident. All IOC obtained over the course of the incident response process (IP addresses, URLs, hashes) are put on a black list of the security controls used by the organization. The security team conducts training for bank employees about safety practices when working with email messages from untrusted sources.

---

# Recommended tools and utilities

This chapter provides descriptions of tools and utilities that can be used for incident response.

Tools and utilities described in this chapter do not constitute a full list of software that can be used for incident response. Depending on the incident, other software may be used to conduct the investigation.

The tools and utilities described in this chapter are developed by third-party companies. Kaspersky Lab is not responsible for the operability or quality of third-party software. Full descriptions of tools and utilities are available on the third-party companies' websites.

## In this chapter

Tools for collecting IOC .....	<a href="#">53</a>
Tools for creating dumps .....	<a href="#">58</a>
Tools for analysis .....	<a href="#">60</a>
Tools for eradication .....	<a href="#">69</a>

# Tools for collecting IOC

This section provides descriptions of tools and utilities used for collecting indicators of compromise (IOC).

## In this section

Sysinternals utilities .....	<a href="#">54</a>
AVZ .....	<a href="#">55</a>
GMER .....	<a href="#">56</a>
YARA .....	<a href="#">57</a>

# Sysinternals utilities

Sysinternals is a set of tools for administering and monitoring computers running Microsoft Windows. Sysinternals Suite includes more than 60 utilities.

It is recommended to use Sysinternals utilities for collecting IOC and analyzing the compromised computers. The most important Sysinternals utilities that can be used for incident response are described in the following subsections.

Sysinternals utilities can be downloaded from

<https://technet.microsoft.com/en-us/sysinternals/default.aspx>.

## PsTools

PsTools is a set of command-line utilities that can be used to execute processes remotely (PsExec), to list detailed information about processes (PsList), to kill processes by name or process ID (PsKill), and to view and control services (PsService). PsTools also includes utilities for restarting and shutting down the computers, dumping system event log records and many other tasks.

## Process Monitor

Process Monitor is a utility for real-time monitoring of process activity. The utility can monitor registry activity and file system activity, and get information about processes, network activity, and I/O operations.

## Process Explorer

Process Explorer is a tool for controlling processes and getting real-time information about process activity.

Process Explorer allows you to do the following:

- Get detailed information about all currently active processes.
- Kill, suspend, and resume execution of the processes.
- Get information about the handles and dynamic-link libraries (DLLs) that were opened or loaded by the processes.
- Create memory dumps and save them to files.

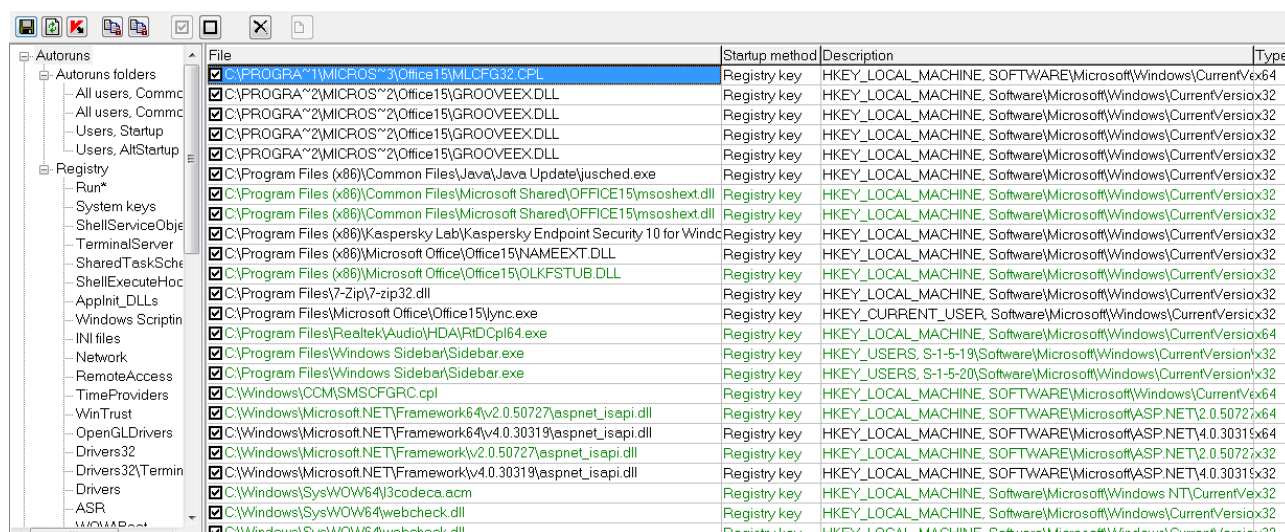
## Autoruns

The Autoruns utility shows which programs are configured to run on system boot or login, and when various built-in Windows applications such as Internet Explorer®, Windows Explorer, and media players are started. The utility also enables or disables the automatic execution of these programs.

The utility supports checking of hashes of the autorun objects with VirusTotal. Unknown files can be sent to anti-virus software companies for analysis.

## AVZ

The AVZ utility can be used for analysis and recovery.



File	Startup method	Description	Type
C:\PROGRA~1\MICROS~3\Office15\MLCFG32.CPL	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion\...
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\PROGRA~2\MICROS~2\Office15\GROOVEEX.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\msoshext.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE15\msoshext.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windc	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Microsoft Office\Office15\NAMEEXT.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Microsoft Office\Office15\OLKFSTUB.DLL	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files (x86)\Microsoft Office\Office15\ync.exe	Registry key	HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\...	HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files\Realtek\Audio\HDA\RtHDVCpl64.exe	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files\Windows Sidebar\SideBar.exe	Registry key	HKEY_USERS, S-1-5-19\Software\Microsoft\Windows\CurrentVersion\...	HKEY_USERS, S-1-5-19\Software\Microsoft\Windows\CurrentVersion\...
C:\Program Files\Windows Sidebar\SideBar.exe	Registry key	HKEY_USERS, S-1-5-20\Software\Microsoft\Windows\CurrentVersion\...	HKEY_USERS, S-1-5-20\Software\Microsoft\Windows\CurrentVersion\...
C:\Windows\CCM\SMSCFGRC.cpl	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\Windows\CurrentVersion\...
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\...
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\...
C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\2.0.50727\...
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll	Registry key	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\...	HKEY_LOCAL_MACHINE, SOFTWARE\Microsoft\ASP.NET\4.0.30319\...
C:\Windows\SysWOW64\3codecs.acm	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows NT\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows NT\CurrentVersion\...
C:\Windows\SysWOW64\webcheck.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...
C:\Windows\SysWOW64\webcheck.dll	Registry key	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...	HKEY_LOCAL_MACHINE, Software\Microsoft\Windows\CurrentVersion\...

Figure 13: Autorun manager of the AVZ utility

It is recommended to use the AVZ utility for obtaining information during incident response. The utility has the following modules:

- Process manager
- Services and drivers manager
- Kernel space modules
- Winsock SPI (LSP, NSP, TSP) manager
- Module for analyzing open TCP and UDP ports

- Autoruns manager
- Internet Explorer extensions manager
- Windows Explorer extensions manager
- Microsoft Windows Control Panel (CPL) applets manager
- Printing system extensions manager
- Task Scheduler jobs manager
- Injected DLLs manager
- Protocols and handlers manager
- Windows Active Setup manager
- Hosts file manager
- Shared resources and network sessions manager

The AVZ utility can be downloaded from <http://www.z-oleg.com/secur/avz/download.php>.

## GMER

GMER is a utility that detects and removes rootkits.

It scans for:

- Hidden processes
- Hidden threads
- Hidden modules
- Hidden services
- Hidden files
- Hidden disk sectors (MBR)



- Hidden registry keys
- Kernel mode driver hooks

The GMER utility can be downloaded from <http://www.gmer.net>.

## YARA

YARA is a tool designed to help malware researchers to identify and classify malicious software samples. YARA is a multi-platform solution, running on Windows, Linux and Apple® Mac® OS X®. It can be used through its command-line interface or from Python scripts with the yara-python extension.

With YARA, malware researchers can create descriptions of malicious software based on textual or binary patterns. Each description (also called a rule) consists of a set of strings and a boolean expression which determine its logic.

Below is an example of a YARA rule that any file containing one of the three strings must be reported as a threat.

```
rule silent_banker : banker
{
    meta:
        description = "This is just an example"
        thread_level = 3
        in_the_wild = true
        strings:
            $a = {6A 40 68 00 30 00 00 6A 14 8D 91}
            $b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9}
            $c = "UVODFRYSIHLNWPEJXQZAKCBGMT"
        condition:
            $a or $b or $c
}
```

The YARA utility can be downloaded from <http://virustotal.github.io/yara>.

# Tools for creating dumps

This section provides descriptions of tools and utilities used for creating memory and hard disk dumps.

## In this section

GRR Rapid Response.....	<a href="#">58</a>
Forensic Toolkit.....	<a href="#">59</a>
dd utility.....	<a href="#">59</a>
Belkasoft RAM Capturer.....	<a href="#">59</a>

# GRR Rapid Response

GRR Rapid Response is an incident response framework focused on remote live forensics.

GRR uses client-server architecture. The client applications (agents) are installed on the workstations and are used to collect data. The server application is used to store and analyze the collected data.

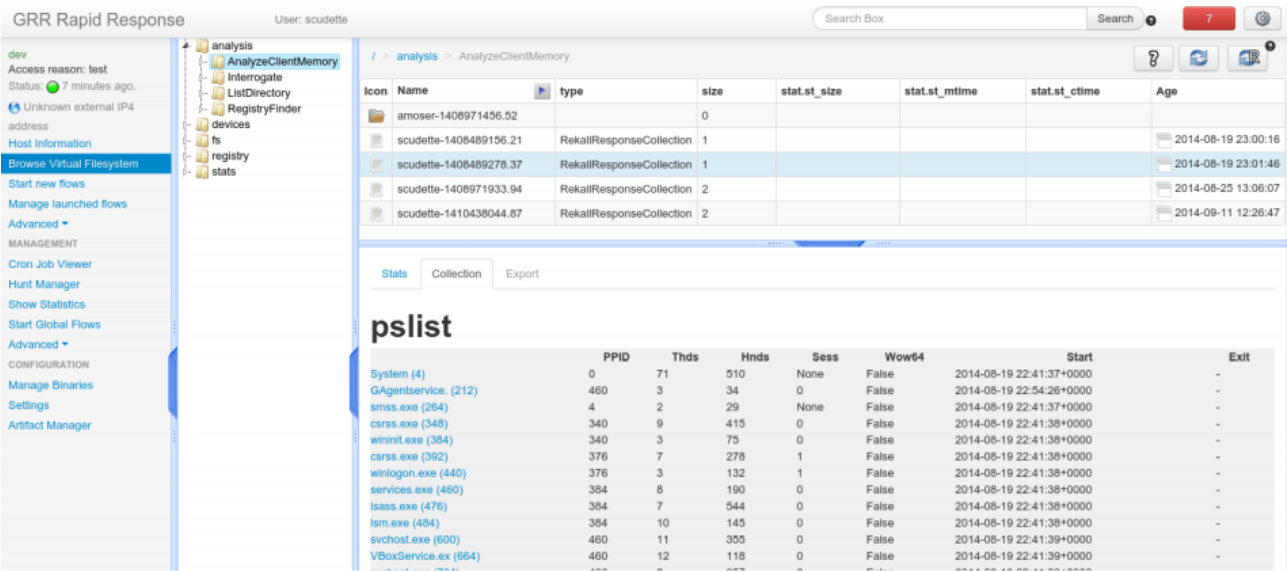


Figure 14: GRR Rapid Response

The main features of the GRR are:

- Remote analysis of memory and system registry on Windows operating systems with the Rekall utility (on page [64](#)).
- Remote analysis of hard disk space with The Sleuth Kit (on page [67](#)).

GRR Rapid Response can be downloaded from <https://github.com/google/grr>.

## Forensic Toolkit

Forensic Toolkit (FTK) is a set of utilities for digital forensics. Forensic Toolkit includes the FTK Imager utility, which can be used to create hard disk and memory dumps.

FTK supports several options for viewing hard disk dumps. For example, there is an option called "Spreadsheets" which shows a list with all spreadsheet files together with a detailed description and location of each spreadsheet. FTK has a list of keywords that can be used to search for IOC.

Forensic Toolkit can be downloaded from

<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk?/solutions/digital-forensics/ftk>.

## dd utility

The dd (dataset definition) tool is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files.

This utility can be used for copying sectors of a hard disk, including the sectors that are not used by the operating system. For example, you can make a backup copy of a hard disk boot sector using the dd utility.

The dd utility is available in all major Linux system distributions. The dd utility is ported to Microsoft Windows as a part of Cygwin. It can be downloaded from <https://cygwin.com>.

## Belkasoft RAM Capturer

Belkasoft RAM Capturer is a free forensic tool for creating memory dumps on computers running Microsoft Windows. The created memory dumps are saved to files.

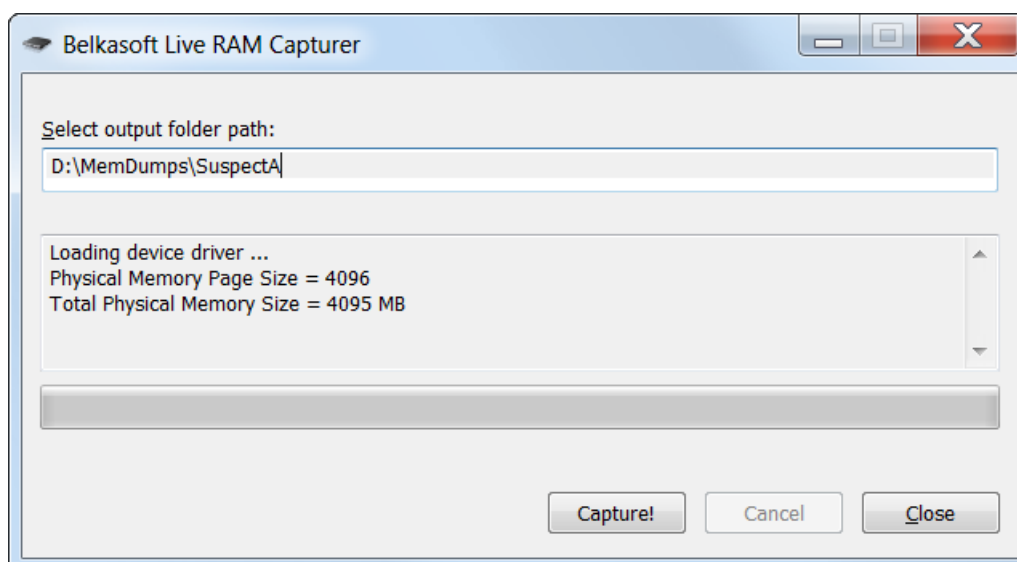


Figure 15: Belkasoft RAM Capturer

Belkasoft RAM Capturer has separate modules for 32-bit and 64-bit versions of Windows. These modules work in kernel mode and allow capturing of memory regions used by the protected processes.

Belkasoft RAM Capturer can be downloaded from <http://belkasoft.com/ram-capturer>.

## Tools for analysis

This section provides descriptions of tools and utilities used for analyzing potential threats and software samples.

Threat analysis requires a great deal of expertise and practice. It is recommended to use the tools described in this section for initial analysis. However, if there is a possibility of an APT attack, it is best to let the experts do the analysis.

### In this section

Kaspersky Threat Intelligence Portal .....	<a href="#">61</a>
Tools for analyzing memory dumps .....	<a href="#">64</a>
Tools for analyzing hard disk dumps .....	<a href="#">67</a>
Strings utility .....	<a href="#">68</a>

# Kaspersky Threat Intelligence Portal

Kaspersky Threat Intelligence Portal is a solution that aggregates several Kaspersky Lab services:

- Threat Lookup

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky Lab about cyber-threats and their relationships, brought together into a single, powerful service. The goal is to provide the security teams with as much data as possible, preventing cyber attacks before they affect the organization. The service retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, hashes, threat names, statistical and behavior data, WHOIS data, and DNS data. The result is global visibility of new and emerging threats, helping to boost the incident response effectiveness and organization's protections against attacks.

- Whois Tracking

This service finds domains and IP addresses by specific WHOIS data search criteria. Such criteria may be domain contact, domain creation date. Specific fields of WHOIS data can be submitted for regular and automatic search of records that meet the specified criteria. Email notifications about new records in the WHOIS database that match search criteria can be automatically sent to a list of specified recipients.

- APT Reports

This service helps to increase the awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky Lab.

- Data Feeds (threat feeds from Kaspersky Lab)

Kaspersky Lab offers continuously updated Threat Intelligence Data Feeds to inform the organizations and clients about risks and implications associated with cyber threats, helping to mitigate threats more effectively and defend against attacks even before they are launched. Data Feeds are available in JSON, CSV, OpenIOC, and STIX™ formats and are provided with connectors for SIEMs, including Splunk, HPE ArcSight, IBM QRadar, EMC® RSA® NetWitness®, LogRhythm, and McAfee® Enterprise Security Manager (ESM).

- Sandbox

This service is an innovative and fully automated file analysis system to detect unknown and advanced threats. It allows submitting files into a safe environment for in-depth dynamic analysis and receive comprehensive file activity logs for further investigation. The technology's benefits are not only the analysis of dormant code and innovative ways to tackle different evasion techniques, but also intuitive reports to be used by SOCs, CERTs, and DFIR teams to boost incident response.

## Threat Lookup

Threat Lookup is a part of the Kaspersky Threat Intelligence Portal solution. It provides threat intelligence about cyber threats, interconnections between cyber threats, legitimate objects, and IOC enriched with context.

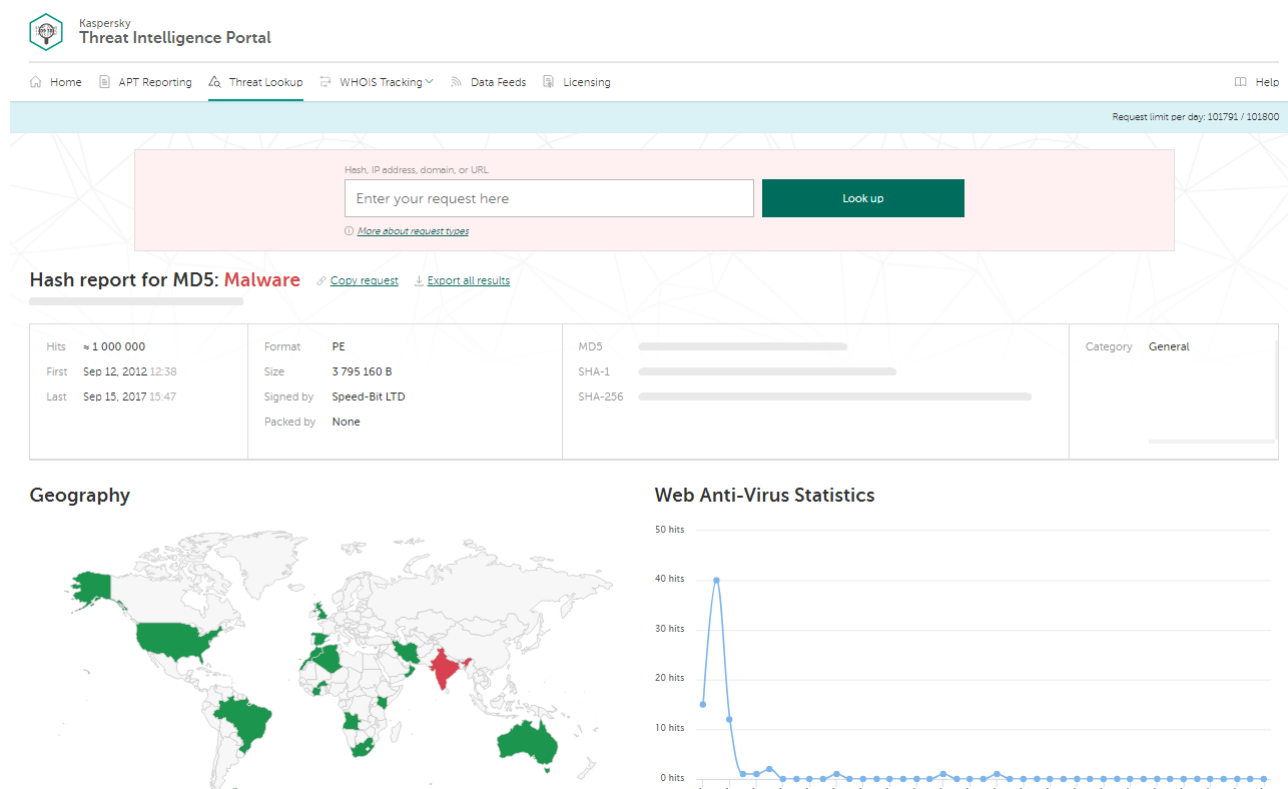


Figure 16: Threat Lookup — Kaspersky Threat Intelligence Portal

The Threat Lookup service allows you to do the following:

- Improve and accelerate incident response and forensic capabilities by providing security teams with meaningful information about threats, as well as global insights into what lies

behind targeted attacks. Security incidents can be diagnosed and analyzed more efficiently and effectively.

- Conduct deep searches into IOC such as IP addresses, malicious URLs, or file hashes with human-validated threat context that allows prioritization of attacks and aids IT staff and resource allocation decisions.
- Enhance the security infrastructure with tactical and strategic threat intelligence by adapting defensive strategies to counter the targeted attacks.

By using Threat Lookup, the security team can get information about the relationships between IOCs. This information can be used to detect threats that are unknown to security controls at the time of the attack. For example, unknown malicious software can be detected because it interacts with a known C&C server URL.

## **Sandbox**

The Kaspersky Threat Intelligence Portal (TIP) solution provides functionality to perform dynamic analysis of threats and software samples in a sandbox environment. As a result, it is possible to detect threats, generate reports about their behavior, and obtain new IOC for incident reports.

A software sample in the TIP sandbox can be analyzed by passing a file, a direct URL, or a hash of the object to the Threat Intelligence Portal (TIP) solution. The analysis yields a behavior report and information about the artifacts related to the analyzed sample. Such information includes PCAP files containing information about the network activity of the analyzed sample and file objects modified or created by the sample.

## **APT Reports**

APT reports from Kaspersky Lab can be used for proactive defense against advanced persistent threats (APTs).

Subscription to APT Reports provides ongoing access to Kaspersky Lab investigations and discoveries, including full technical data on each APT in a range of formats (including YARA and OpenIOC formats).

## **Getting access to Kaspersky Threat Intelligence Portal**

To get access to Kaspersky Threat Intelligence Portal solution, contact [intelligence@kaspersky.com](mailto:intelligence@kaspersky.com) or visit

<http://www.kaspersky.com/enterprise-security/intelligence-services>.

# Tools for analyzing memory dumps

This section describes the Volatility and Rekall utilities, which can be used for analyzing memory dumps.

## Volatility

Volatility Framework is a memory forensics framework for the extraction of digital artifacts from volatile memory (RAM) samples. The utility has profiles for memory dumps taken on Linux, Windows, and Mac OS X operating systems.

Volatility supports the following dump types:

- Raw / padded physical memory
- FireWire® (IEEE 1394)
- Expert Witness (EWF)
- 32-bit and 64-bit Windows Crash Dump
- 32-bit and 64-bit Windows Hibernation
- 32-bit and 64-bit Mach-O files
- Virtualbox Core Dumps
- VMware™ Saved State (.vmss) and Snapshot (.vmsn)
- HPAK format (FastDump)
- LiME (Linux Memory Extractor)
- QEMU VM memory dumps

The distribution kit of the Volatility Framework has about 150 plug-ins. By using these plug-ins, the security team can obtain information about the process call tree and DLLs that were loaded by the processes. For example, the devicetree plug-in can be used to get a list of all devices and drivers associated with these devices. The list can be used to search for drivers used by the rootkits.



The following example demonstrates using Volatility to get a list of loaded DLL modules.

```
$ python vol.py -f stuxnet.vmem --profile=WinXPSP2x86 dlldump -memory -D stuxout/

Volatility Foundation Volatility Framework 2.5

Process(V) Name          Module Base Module Name  Result
-----
0x820df020 smss.exe      0x048580000 smss.exe    OK: module.376.22df020.48580000.dll
0x821a2da0 csrss.exe     0x075b40000 CSRSRV.dll  OK: module.600.23a2da0.75b40000.dll
0x821a2da0 csrss.exe     0x077f10000 GDI32.dll   Error: DllBase is paged
0x821a2da0 csrss.exe     0x075b60000 winsrv.dll  OK: module.600.23a2da0.75b60000.dll
0x81da5650 winlogon.exe 0x001000000 winlogon.exe OK: module.624.1fa5650.1000000.dll
```

Volatility tool can save processes from memory dumps into executable files. These files can be analyzed statically or dynamically. For example, the dynamic analysis can be performed with the Sandbox–Kaspersky Threat Intelligence Portal solution (on page [61](#)); the static analysis can be performed with Strings utility (on page [68](#)).

Volatility Framework can be downloaded from <http://www.volatilityfoundation.org>.

## Rekall

Rekall is a memory analysis framework.

Rekall has three interfaces: command-line, interactive console based on IPython, and web interface. Like Volatility, Rekall has a large number of plugins. For example, the pslist plugin can output a list of all processes that were running on a system; the hooks\_inline plugin can search for all libraries that have hooks (intercepted function calls). Memory dumps on Windows operating systems can be created with the winpmem utility that comes with Rekall.

Rekall allows analysis of both memory dumps and memory on a running operating system. It means that Rekall can be used for analysis without creating memory dumps.

The following example demonstrates analyzing a memory dump with Rekall.

```

user@computer:~/rekall$ rekall -f ~/images/win7.elf

-----

The Rekall

Memory Forensic framework 1.1.0 beta (Buchenegg).

"We can remember it for you wholesale!"

This program is free software; you can redistribute it and/or modify it under
the terms of the GNU General Public License.

See http://www.rekall-forensic.com/docs/Manual/tutorial.html to get started.

-----

win7.elf 12 47 07> pslist

-----> pslist()

  _EPROCESS   Name      PIO PPID Thds Hnds Sess Wow64 Start
-----
0xfa80008959e0 System 4      0   84  511 -   False 2012-10-01 21:39:51+0000

[1] zeus.vmem 00:10:03> hooks_inline proc_regex="services"

-----> hooks_inline(proc_regex="services")

Pid Proc          DLL          Name          Hook          Disassembly
---
676 services.exe ntdll.dll NtCreateThread 0x7e3b47 0x7c90d7d2 e97063ed83 jmp..
                                0x7c90d7d7 ba0003fe7f mov..
                                0x7c90d7dc ff12          call.
                                0x7c90d7de C22000        ret..
                                0x7c90d7e1 90            nop
                                0x7c90d7e6 90            nop
                                0x7c90d7e7 b836000000 mov..

```

Rekall can be downloaded from <http://www.rekall-forensic.com>.

# Tools for analyzing hard disk dumps

This section describes The Sleuth Kit (TSK) and RegRipper tools which can be used for analyzing hard disk dumps.

## The Sleuth Kit (TSK)

The Sleuth Kit (TSK) is a collection of command line tools and a C library that allows analyzing hard disk dumps and recovering files from them.

The command-line tools that come with TSK can be used to do the following:

- List allocated and deleted ASCII and Unicode file names.
- Display the details and contents of all Windows NT File System attributes.
- Display file system and meta-data structure details.
- Create time lines of file activity, which can be imported into a spread sheet to create graphs and reports.
- Look up file hashes in hash databases.
- Organize files based on their type. Pages of thumbnails can be made of graphic images for quick analysis.

Autopsy is a GUI-based program for The Sleuth Kit. It provides a GUI for TSK utilities.

The Sleuth Kit can be downloaded from <http://www.sleuthkit.org/sleuthkit/>. Autopsy can be downloaded from <http://www.sleuthkit.org/autopsy/>.

## RegRipper

RegRipper is a forensic tool for registry analysis.

RegRipper can be used to extract specific registry keys, values, and data from the hard disk dumps. The distributive of RegRipper contains about 300 plug-ins.

The following example demonstrates the usage information for RegRipper.

```

C:\RR>rip.exe

Rip v.2.8_20130801 - CLI RegRipper tool

Rip [-r Reg hive file] [-f plugin file] [-p plugin module] [-l] [-h]

Parse Windows Registry files, using either a single module, or a plugins file.


-r Reg hive file...Registry hive file to parse
-g .....Guess the hive file (experimental)
-f [profile].....use the plugin file (default: plugins\plugins)
-p plugin module...use only this module
-l .....list all plugins
-c .....Output list in CSV format (use with -l)
-s system name.....Server name (TLN support)
-u username.....User name (TLN support)
-h.....Help (print this information)


Ex: C:\>rip -r c:\case\system -f system
C:\>rip -r c:\case\ntuser.dat -p userassist
C:\>rip -l -c


All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

```

RegRipper can be downloaded from <https://github.com/keydet89/RegRipper2.8>.

## Strings utility

Strings is a command-line utility for Unix and Unix-like operating systems which can be used to search for Unicode and ASCII strings in the binary files. Such strings can be used as IOCs or for static analysis of the software sample behavior.

The utility can search for strings in the dump files, to get information about the software used in the development of the analyzed sample, URLs, IP addresses, email addresses, and registry keys accessed by the analyzed sample and other IOCs.

The Strings utility is ported to Microsoft Windows as a part of Cygwin. It can be downloaded from <https://cygwin.com>.

## Tools for eradication

This section provides descriptions of tools and utilities used for the Eradication phase of the incident response process.

### In this section

Kaspersky Virus Removal Tool .....	<a href="#">69</a>
Kaspersky Rescue Disk .....	<a href="#">70</a>

## Kaspersky Virus Removal Tool

Kaspersky Virus Removal Tool is a free solution that can be used to scan for malicious software and to disinfect computers running Microsoft Windows. The tool can work from the command line.

Kaspersky Virus Removal Tool can:

- Detect and eradicate malicious software.
- Detect adware and other legitimate software that can be used by criminals to harm the computer or steal sensitive data.

The utility is not designed for persistent protection. Kaspersky Virus Removal Tool does not update its anti-virus databases. A new version of Kaspersky Virus Removal Tool must be downloaded in order to use the latest databases.

After Kaspersky Virus Removal Tool is used to disinfect a compromised computer, an endpoint protection solution such as Kaspersky Endpoint Security must be installed for persistent protection.

Kaspersky Virus Removal Tool can be downloaded from <https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool>.

Other free utilities for eradicating several types of malicious software are available at [http://support.kaspersky.com/viruses/utility?CID=acq-freekasp-USA&\\_ga=1.198229483.571661967.1434556259](http://support.kaspersky.com/viruses/utility?CID=acq-freekasp-USA&_ga=1.198229483.571661967.1434556259).

## Kaspersky Rescue Disk

Kaspersky Rescue Disk is designed to scan, disinfect, and restore infected operating systems. It can be used when booting the operating system is not possible.

Kaspersky Rescue Disk can efficiently eradicate malicious software because the operating system is not booted and malicious software cannot gain control over the system.

Kaspersky Virus Rescue Disk can be downloaded from <https://support.kaspersky.com/viruses/rescuedisk>.

---

# AO Kaspersky Lab

Kaspersky Lab is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky Lab was rated among the world's top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

**Products.** Kaspersky Lab products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company's portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky Lab virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky Lab applications.

**Technologies.** Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. It is no coincidence that many other developers use the

Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company's innovative technologies are patented.

**Achievements.** Over the years, Kaspersky Lab has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab's main achievement is the loyalty of its users worldwide. The company's products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky Lab website:	<a href="http://www.kaspersky.com">http://www.kaspersky.com</a>
Virus encyclopedia:	<a href="http://www.securelist.com">http://www.securelist.com</a>
Virus Lab:	<a href="http://newvirus.kaspersky.com">http://newvirus.kaspersky.com</a> (for analyzing suspicious files and websites)
Kaspersky Lab's web forum:	<a href="http://forum.kaspersky.com">http://forum.kaspersky.com</a>



---

# Trademark notices

This chapter lists the owners of third-party trademarks that are used in this document.

Registered trademarks and service marks are the property of their respective owners.

Apple, FireWire, Mac, OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

IBM, QRadar are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Internet Explorer, Windows, Active Directory are registered trademarks of Microsoft Corporation in the United States and other countries.

Splunk is a trademark and registered trademark of Splunk Inc. in the United States and other countries.

Python is a trademark or registered trademark of the Python Software Foundation.

Adobe and Acrobat are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions.

UNIX is a registered trade mark in the United States and other countries, licensed exclusively through X/Open Company Limited.

McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries.

EMC, RSA, NetWitness are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries.

Virtualbox is a registered trademark of Oracle and/or its affiliates.

Belkasoft is a registered trademark of Yuri Gubanov in the United States.

QEMU is a trademark of Fabrice Bellard.

AccessData is a registered trademark or trademark of AccessData in the United States and/or other countries.

Tor is a trademark of The Tor Project, U.S. Registration No. 3,465,432.