kaspersky

Incident Response

Analytics Report

2018

www.kaspersky.com

kaspersky

If you would like to request Incident Response, Digital Forensic or Malware Analysis services, please email us at gert@kaspersky.com.

Introduction

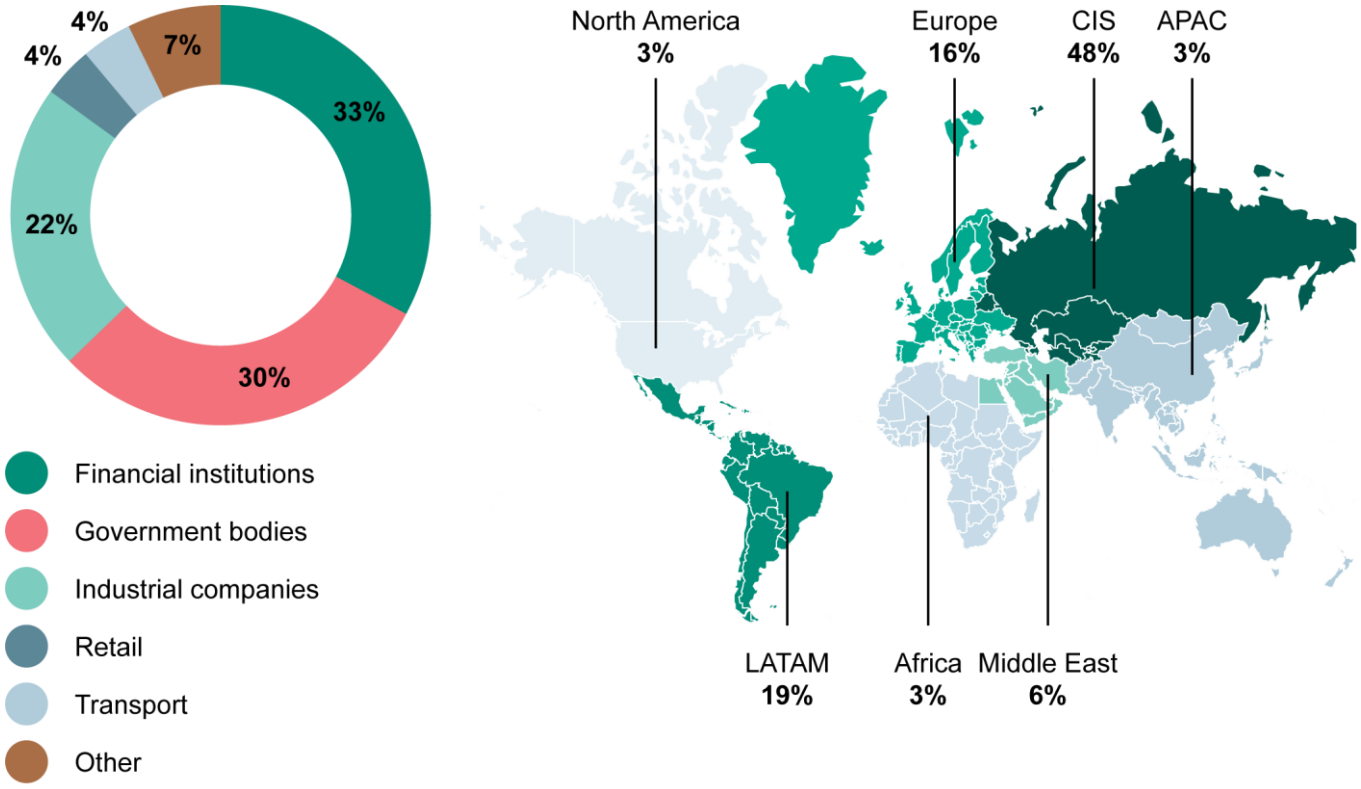
This report covers our team's incident response practices for the year 2018. We have thoroughly analyzed all the service requests, customer conversations and incident response deliverables to provide you an overview in numbers. The report includes statistics on how companies reveal data breaches and compromises, the attack vectors most commonly used by adversaries, how long they remain inside a company's infrastructure and much more. We also provide some high-level recommendations to improve resilience against such attacks.

The data used in this report comes from the wide range of incident investigation services provided by Kaspersky teams. The main digital forensic and incident response operations unit is called the Global Emergency Response Team (GERT)[1] and includes experts in Europe, Latin America, North America, Russia and the Middle East. However, our operational coverage is much greater and that's why our company focused many more resources on incident response and malware analysis activities. An example of this is the advanced targeted attack investigations by the Global Research and Analysis Team (GReAT).[2]

Report navigation

- When do our clients request an investigation?
- How often do companies face incidents and what kind of incidents are they?
- What are the most common attack vectors?
- How long have the adversaries been inside the network?
- What tactics and techniques are the adversaries using?

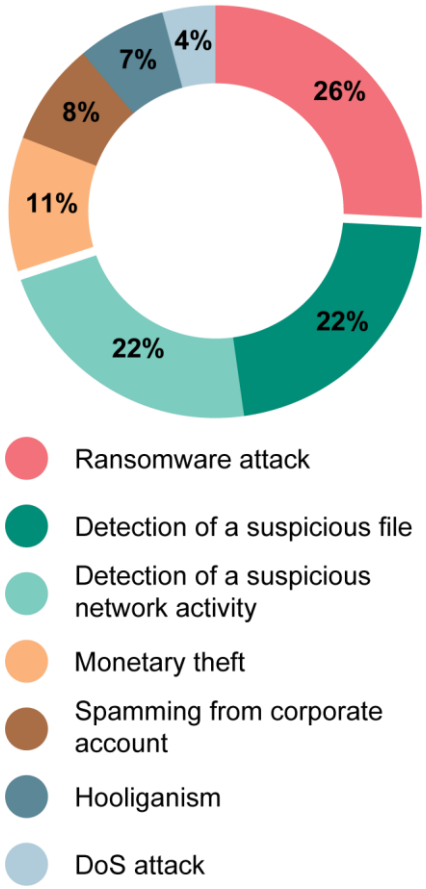
Geography and industry verticals of incident responses in 2018



[1] https://www.kaspersky.com/enterprise-security/incident-response
[2] https://great.kaspersky.com/

kaspersky

Reasons for investigation requests



Reasons for requesting incident response

More than half of the requests for investigation were initiated by customers after detecting an attack that had visible consequences, such as unauthorized money transfers, workstations encrypted by ransomware, service unavailability, etc. This indicates the need to improve attack detection methods and incident response procedures within a company to avoid financial losses and to minimize the impact of attacks on the company's infrastructure.

It should be noted that **in two out of three cases,** investigation of incidents **related to the detection of suspicious** files or network activity revealed **an actual attack** on the customer's infrastructure. In the other cases, suspicious activity was caused by unusual user actions or software behavior related to security misconfigurations.

The most common reason for customer requests was a **ransomware** attack. This category of attack is characterized by rapid development, difficulty of early detection, and contrastingly obvious consequences.

Experts from Kaspersky Anti-Malware Research Department ranked the most common types of ransomware which targeted organizations in 2018[3].

If a ransomware attack is detected, it is recommended to:

- Isolate the host and the network segment where the incident took place to avoid further attack development.
- Take snapshots of RAM and images of the hard drives for further detailed investigation.
- Analyze encrypted files to determine the malware type. This will help to promptly implement a set of initial response measures.
- Conduct an investigation of the incident to determine the initial vector of attack and find possible backdoors to prevent recurrence of the incident.

Top 7 ransomware attacks by share of victims

Name	Share of victims
WannaCry	40.64%
Cryakl	7.37%
GandCrab	5.15%
(generic verdict)	3.63%
Purgen/ GlobeImposter	2.74%
Crysis/Dharma	2.67%
Shade	2.41%

[3] https://securelst.com/kaspersky-security-bulletin-2018-statistics/89145/

kaspersky

There are many more incidents in the wild

Only 22% of companies where evidence of malicious activity was detected requested an Incident Response service.

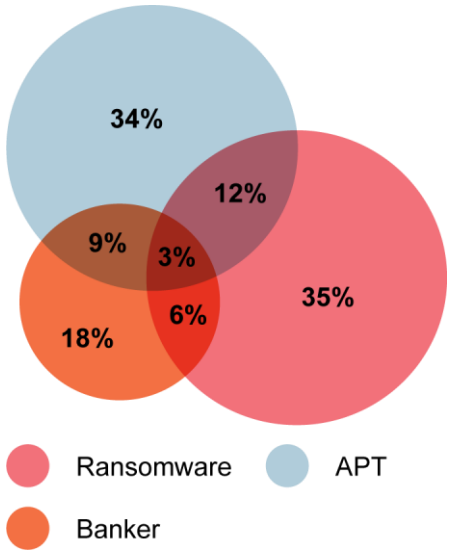
Kaspersky customers often request detailed analysis of the data collected by automated monitoring tools. As a result of analyzing this data, the following conclusions were reached:

81% of organizations that provided data for analysis were found to have indicators of malicious activity in their internal network.

One out of three organizations exhibited signs of an advanced targeted attack.

Attack trends and key security threats were identified for the following major sectors:

Share of customers encountering certain types of malicious activity



Financial Institutions

Signs of **APT attacks** appeared in the infrastructure of financial institutions **one and a half times more often (54%)** than in other organizations.

A small share of financial organizations showed signs of **ransomware (12%)** or **banker (8%)** infections.

Government Bodies

Malicious activity was detected in **95%** of government bodies which is **14% more** than across all organizations in general.

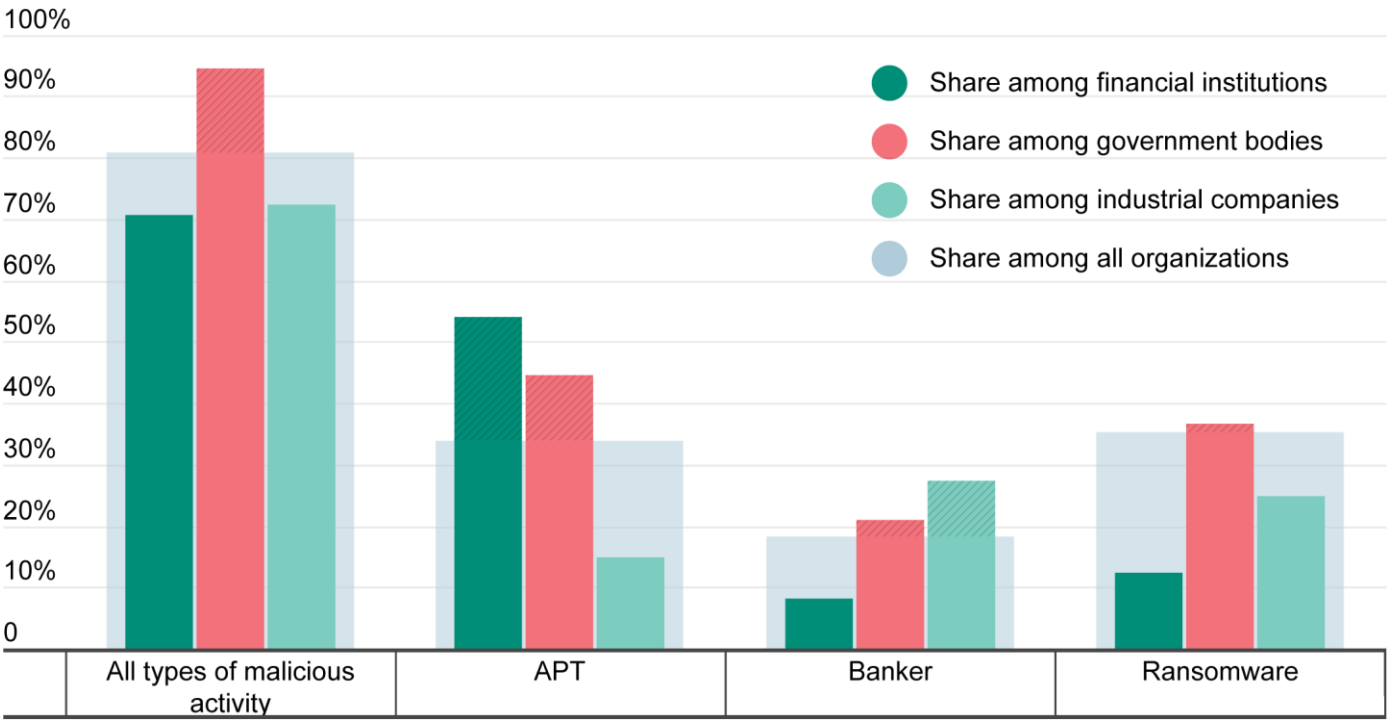
Attempts to access resources associated with **APT attacks** were recorded in **45%** of government bodies.

Industrial Companies

Industrial companies are **more likely to be victims of bankers**. Banker Trojan activity was detected in **27%** of companies.

Manufacturing companies are **less prone to APT attacks (15%)** and **ransomware attacks (25%)**.

Share and type of organizations and incidence of malicious activity by class



Adversary attack vectors

The remote management interface of the RDP service was used in the initial attack vector in **one out of three incidents**. In the majority of cases, an adversary successfully obtained a valid user's credentials as a result of a brute-force attack on the RDP service. Such an attack usually lasted just a few hours because weak or dictionary passwords were used. In addition, in most cases the same credentials were used for authentication in different systems, so an attacker was able to reuse the usernames and passwords to access additional hosts.

In one third of attacks through remote management interfaces, the valid credentials were known to the intruder in advance (no brute-force attempts were detected). They were probably obtained using social engineering methods or were found on unsecured resources with public access (for example, if an employee used the same password to register on third-party resources).

Recommendations:

- Restrict access to any remote management interfaces from external IP addresses. Remote control interfaces should be accessible only from a limited number of workstations. Use third-party solutions to enforce encryption (IPsec, stunnel).
- Enforce a strict password policy for all IT systems.
- Avoid using high-privileged accounts wherever possible: follow the principle of least privilege.
- Consider deployment of two-factor authentication.

33% of attacks occurred due to a lack of security awareness among employees. An employee downloaded a malicious file from untrusted sources and launched it, allowing an adversary to gain control over the workstation. While it is impossible to completely eliminate human error, regular staff training on information security awareness can significantly reduce the success of attacks using social engineering methods.

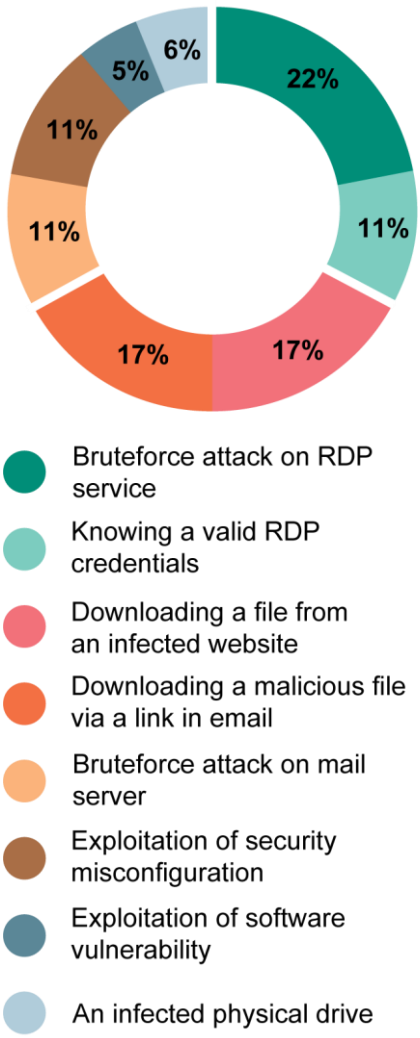
Recommendations:

- Use endpoint protection software on every host in the LAN and ensure it is regularly updated.
- Use a 'sandbox' for analysis of every file downloaded from external resources.
- Increase security awareness among employees, management and IT staff. This can be accomplished by regular security awareness sessions with periodic checks.

From a long-term perspective, the following strategies are recommended:

- Implement patch management procedures that include centralized software updates on all hosts, including those that are not a part of the domain infrastructure.
- Consider deploying a solution for network traffic analysis.
- Automatically back up data to a device that is not writable thereafter.
- Conduct regular security assessments of the IT infrastructure.

Common initial attack vectors[4]



[4] In 20% of cases customers did not provide experts with the necessary data for analysis and investigation.

kaspersky

Attack duration

For a number of incidents, Kaspersky specialists have established the time period between the beginning of the attacker activity and the end of the attack. After analysis, all incidents were divided into three categories of attack duration.

Fast Attacks (a few hours)

This category includes attacks lasting less than 24 hours. These are mainly incidents involving ransomware attacks. Due to the high speed of development, effective countermeasures to such attacks are limited to preventive methods.

In some cases, a delay of up to a week has been observed between the initial compromise and the beginning of the attacker's activity.

Common threat:

Ransomware infection

Common attack vector:

Brute-force attack on RDP service

Attack duration (median):

6 hours

Countermeasures:

- Strict password policy.
- Two-factor authentication.
- Restricted access to management interfaces.
- Endpoint protection on every host in the LAN.

Medium Duration Attacks (a few days)

This group includes attacks that have been developing for several days. In most cases, this activity was aimed at the direct theft of money. Typically, the attackers achieved their goals within a week.

Common threat:

Financial theft

Common attack vector:

- Downloading a malicious file via link in email
- Downloading a malicious file from infected site

Attack duration (median):

8 days

Countermeasures:

- Staff security awareness.
- Endpoint protection on every host in the LAN.

Continuous Attacks (three weeks and longer)

Incidents that lasted more than a few weeks were included in this group. This activity is almost always aimed at stealing sensitive data.

Such attacks are characterized by interchanging active and passive phases. Total duration of the active phases is, on average, similar to the duration of attacks in the previous group.

Common threat:

Cyber-espionage and theft of confidential data

Common attack vector:

Downloading a malicious file via link in email

Attack duration (median):

3 months

Total duration of active phases (median):

7 days

Countermeasures:

- Comprehensive and timely investigation of each information security incident.
- Use of infrastructure protection solutions at the network and workstation levels.
- Use of network activity monitoring tools.
- Correct internal network segmentation.

kaspersky

Attack tactics and techniques

For a number of incidents, a list of MITRE[5] techniques was prepared. The ATT&CK table below shows the frequency with which techniques were observed in the investigated incidents. Unfortunately, not many companies are currently mature enough to gain value from the ATT&CK framework or common descriptions such as STIX. For those capable of ingesting this kind of information, make sure to highlight mentioned techniques in your security tools of choice.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
Spearphishing Attachment	CMSTP	Component Object Model Hijacking	DLL Search Order Hijacking	CMSTP	Brute Force	Account Discovery	Pass the Hash	Data from Local System	Data Compressed	Commonly Used Port
Spearphishing Link	Command-Line Interface	Create Account	Hooking	Component Object Model Hijacking	Credential Dumping	File and Directory Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Data Encrypted	Connection Proxy
Valid Accounts	Execution through API	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Credentials in Files	Network Service Scanning	Remote File Copy	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Encoding
	Graphical User Interface	Hidden Files and Directories	Process Injection	Disabling Security Tools	Exploitation for Credential Access	Network Share Discovery	Remote Services	Input Capture		Remote Access Tools
	LSASS Driver	Hooking	Scheduled Task	DLL Search Order Hijacking	Hooking	Network Sniffing	Windows Admin Shares	Screen Capture		Remote File Copy
	PowerShell	LSASS Driver	Valid Accounts	File Deletion	Input Capture	Peripheral Device Discovery				Standard Application Layer Protocol
	Regsvr32	New Service	Web Shell	Hidden Files and Directories	Network Sniffing	Permission Groups Discovery				
	Rundll32	Registry Run Keys / Startup Folder		Masquerading		Process Discovery				
	Scheduled Task	Scheduled Task		Modify Registry		Query Registry				
	Scripting	Shortcut Modification		Obfuscated Files or Information		Remote System Discovery				
	Service Execution	Valid Accounts		Process Injection		Security Software Discovery				
	Signed Binary Proxy Execution	Web Shell		Regsvr32		System Information Discovery				
	User Execution			Rundll32		System Network Configuration Discovery				
	Windows Management Instrumentation			Scripting		System Network Connections Discovery				
				Signed Binary Proxy Execution		System Owner/User Discovery				
				Software Packing		System Service Discovery				
				Valid Accounts						

> 10% of cases
> 20% of cases
> 50% of cases

[5] https://attack.mitre.org/

kaspersky

Conclusion

From the statistics in this report, we can conclude that cyberattacks target all types of businesses around the globe. It means that having a plan to defend and quickly respond to such attacks is no longer an option; it's a must, regardless of business type.

Maintaining and improving an already existing incident response plan will accelerate handling of security breaches through proper containment, analysis and eradication of infected elements in the network. The risk of re-infection is reduced and defense against complex attacks is improved by utilizing the lessons learned from each incident to enhance the existing security process in the environment.

Along with a powerful auditing policy and a log retention period of at least six months to one year, developing guided procedures for proper handling of digital evidence will definitely help in faster and more complete analysis of incidents by experts. This results in quicker containment and reduces possible loss of assets, data or reputation.

Frequent security assessments have proved effective in discovering weaknesses early enough to fix them and hardening overall infrastructure before adversaries reveal those weaknesses and make use of them in an offensive attack.

Furthermore, we can see that humans are still the weakest link in the security chain. Even with a high-level security policy and security controls in place, a single employee uneducated in information security can trigger a major compromise of the internal environment and assets.