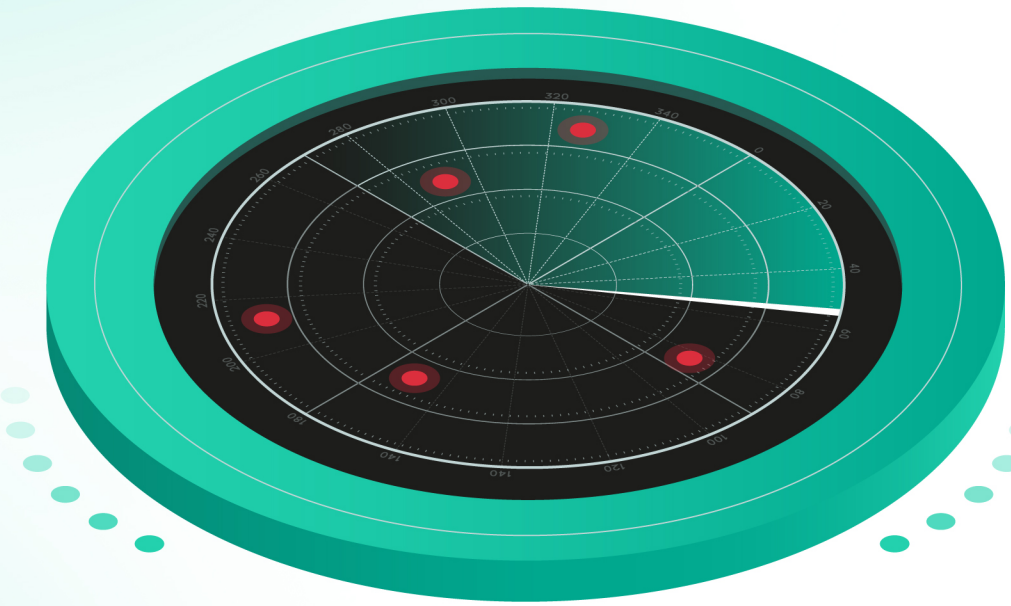
Incident response analyst report

2020



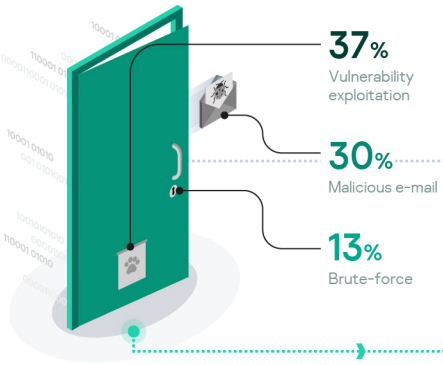
kaspersky

Executive summary

Incident Response statistics are based on IR retainer services and IR fireman services for organizations contacting us during an incident.

Threat intelligence view

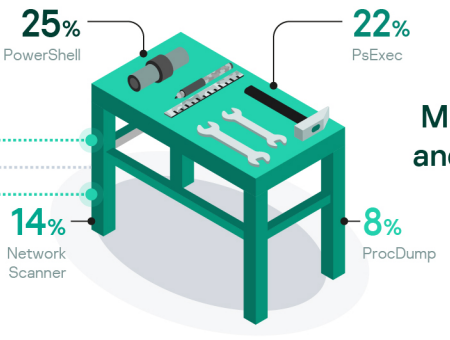
Initial attack vector



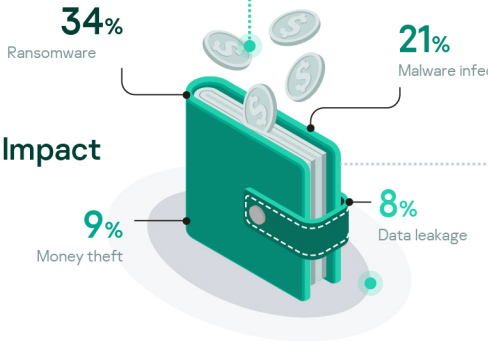
- Patch your publicly available services now
- Enhance your e-mail protection and employee awareness
- Remove management interfaces from public access

- Threat hunting with rich telemetry and specifically deep tracing of PowerShell is a must to be able to detect attacks
- PsExec is not a suspicious event, but an incident to manage

Move around and get things done



Impact



- Exercise pace of security operations as it matters for Ransomware
- Backup your data frequently and on separated infrastructure

Industry

29%	16%	15%	10%
Industrial	Financial	Government	Telecom

Learn adversaries and attacks targeting your industry and region to prioritize security investments

Region

32%	24%	21%	15%
Middle East	Europe	CIS	LATAM

Security operations metrics view

Attack duration

31%	24%	22%	13%
days	months	weeks	hours

Most of fast detection times are related to visible infrastructure or process disruptions from Ransomware

Detection reason

32%	27%	13%	11%
suspicious file	files encrypted	suspicious endpoint activity	other security tool alert

Security operations and toolstacks play a big role in incident identification

Remediation duration

43%	27%	15%	13%
weeks	days	months	hours

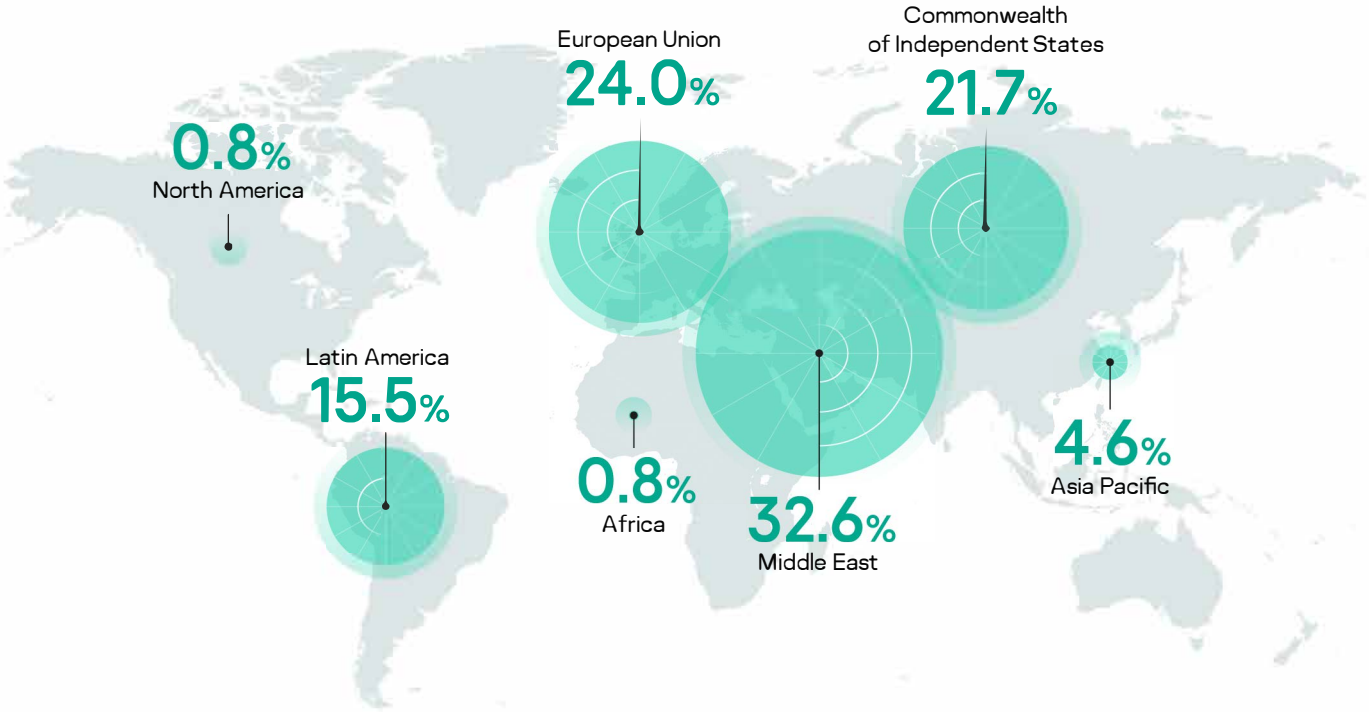
There is always room for improvement. Stick with IR retainer or prepare a list of IR providers and exercise with them

Introduction

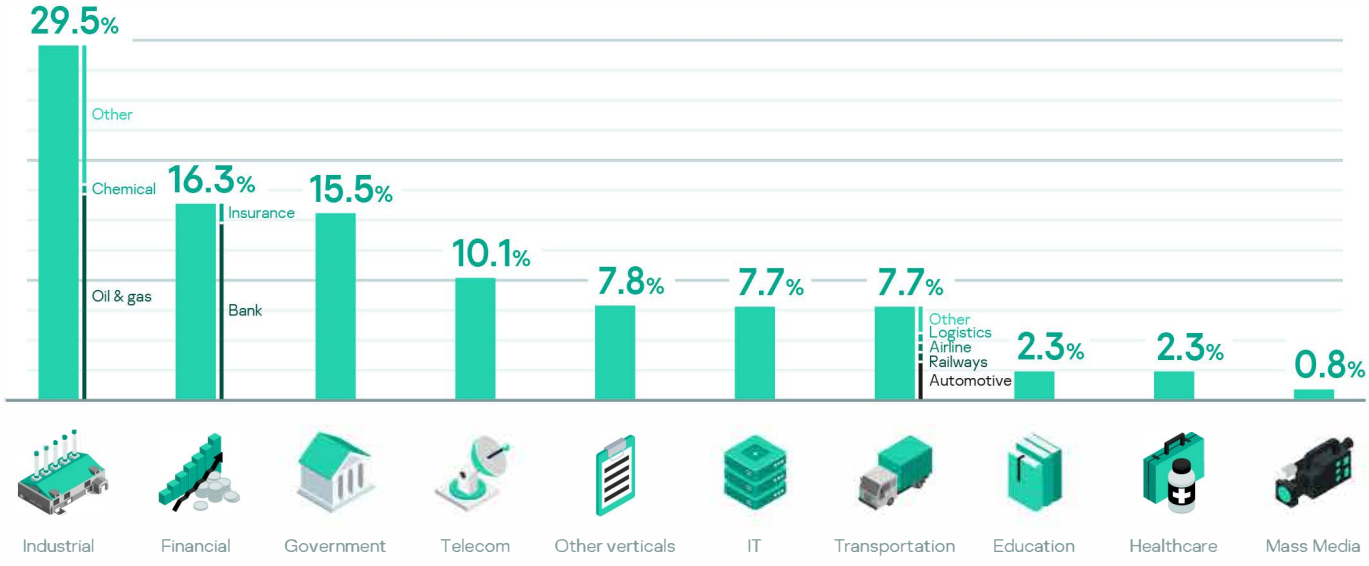
The Incident Response Analyst Report provides insights into incident investigation services conducted by Kaspersky in 2019. We deliver a range of services to help organizations when they are in need: incident response, digital forensics and malware analysis. Data in the report comes from our daily practices with organizations seeking assistance with full-blown incident response or complimentary expert activities for their internal incident response teams.

Kaspersky Digital Forensics and Incident Response operations are presented by Global Emergency Response Team (GERT), Computer Incidents Investigation Unit (CIIU), Global Research and Analysis Team (GReAT) with experts in Europe, Asia, South and North America, Middle East and Africa.

Geography of incident responses



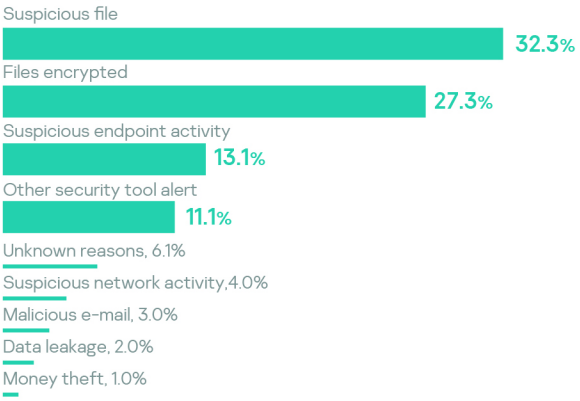
Verticals and Industries



Reasons to go for incident response

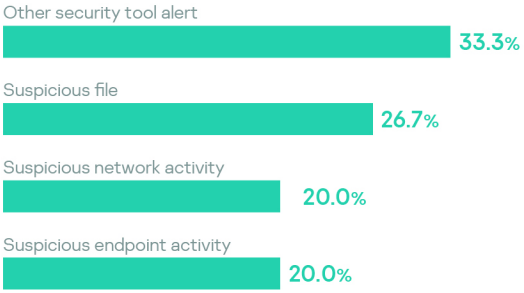
Noticeable impact on infrastructure such as encrypted asset, money loss, data leakage, suspicious e-mail led to 30% of requests for investigation. More than 50% of requests came from alerts in security toolstacks: endpoint (EPP, EDR), network (NTA) and other (FW, IDS/IPS, etc.).

True positives



Often organizations became aware of incident only after noticeable impact, even when basic security toolstacks had produced alerts uncovering some part of the attack. Lack of security operations staff is the most common reason to miss these indications. Suspicious files identified by security operations and suspicious endpoint activity led to uncovered incident in 75% of cases, while suspicious network activity in 60% of cases were false positives.

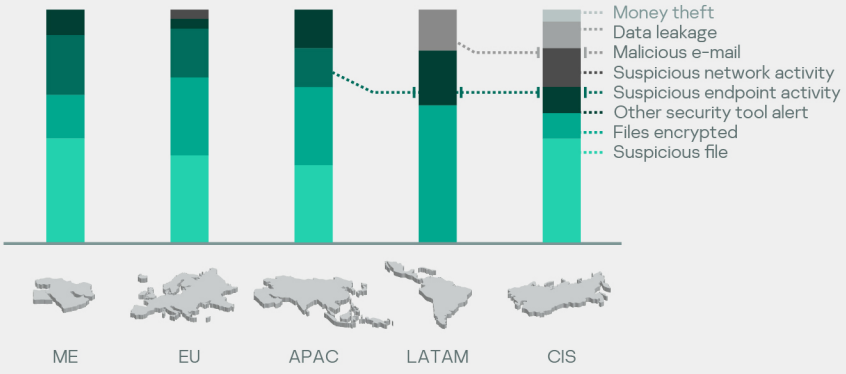
False positives



One of the most common reasons for an incident response service request is a ransomware attack: a challenge for detection even for mature security operations. For more details on types of ransomware and how to fight against this attack, visit our story "Cities under ransomware siege".

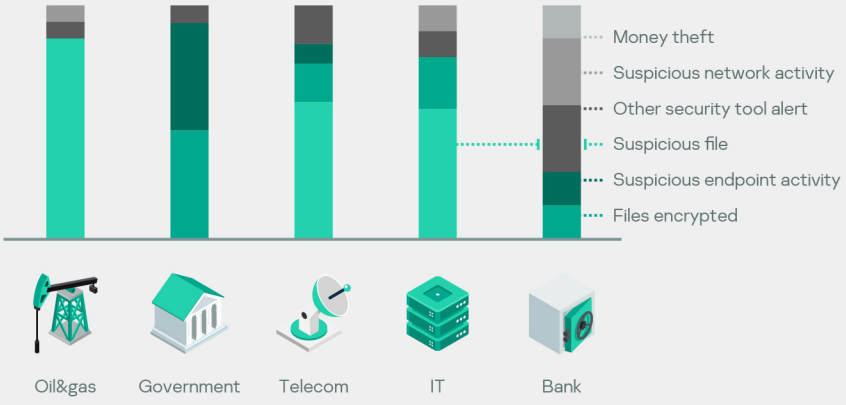
Distribution of reasons for our top regions

- Nature of biggest proportion – Suspicious file – shows file-oriented detection is still prevalent in a lot of organizations
- 100% of cases involving financial cybercrime and data leakages that we investigated appeared in CIS countries



Distribution of reasons for selected industries

- Surprisingly, 100% of money theft is inside the Financial industry (banks)
- Ransomware is detected after impact primarily within government, telecom and IT sectors

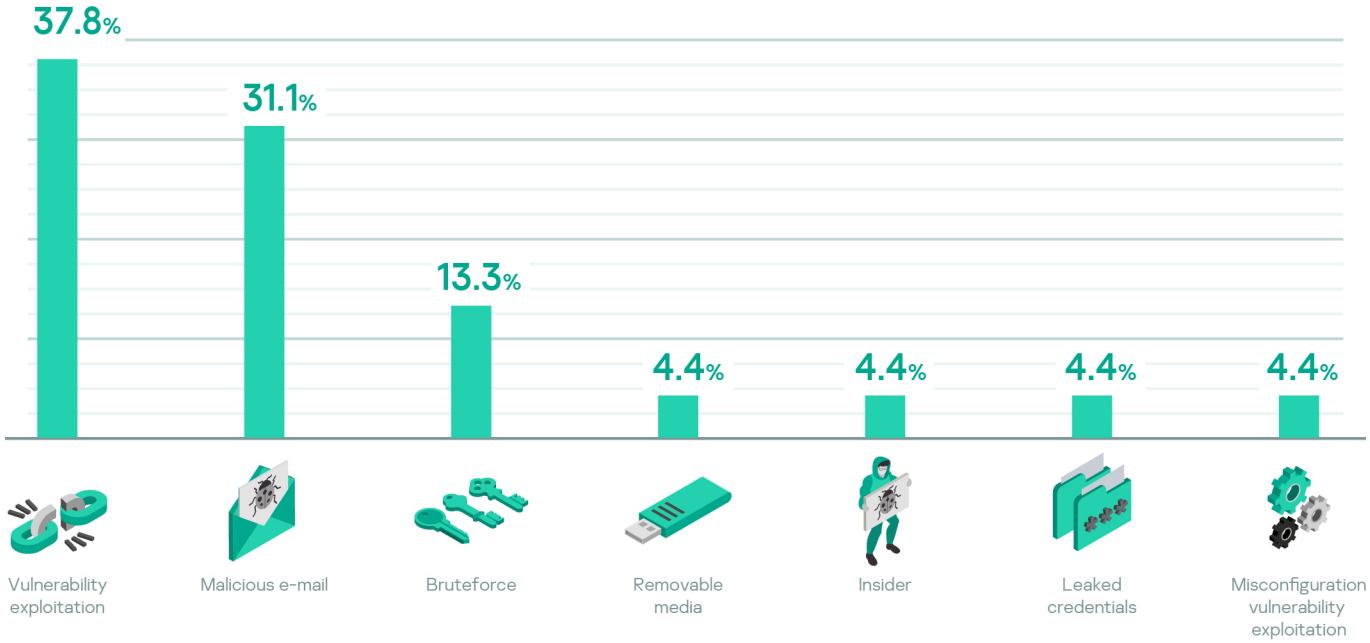


Initial vectors

Or how attackers got in

Dominant initial vectors are exploitation of vulnerabilities (0- and 1-day), malicious e-mails, and Bruteforce attacks. Patch management for 1-day vulnerabilities, applying password policies, and avoiding management interfaces on the Internet are well-suited to address most cases.

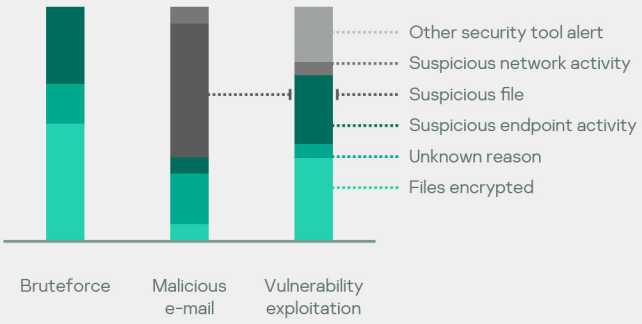
0-day vulnerabilities and social engineering attacks via e-mail are much harder to address and require a decent level of maturity from internal security operations.



Links between top initial compromise vectors and how the incident was detected

Sometimes we act as complimentary experts for primary incident response team from victim organization and we had no visibility into their findings – that's why we have Unknown reasons on the charts

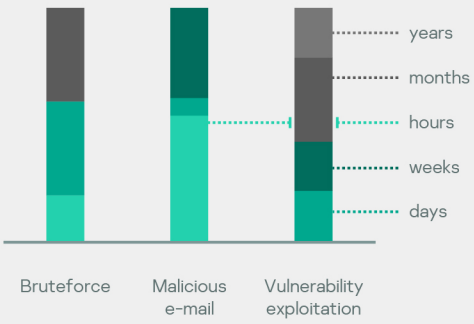
Malicious e-mails are most likely to be detected by a variety of security toolstacks, but that's not showing distribution of 0- to 1-day vulnerabilities



Distribution of how long the attack went unnoticed and how the organization was compromised

Our cases beginning with vulnerability exploitation on an organization's network perimeter were the longest lasting

Social engineering attacks through e-mail were the most short-lived

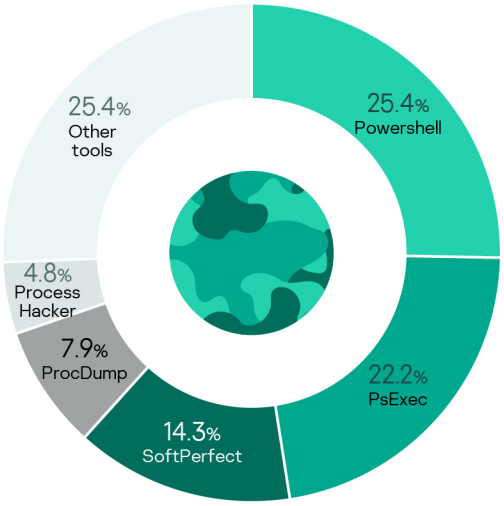


Tools and exploits

30% of all incidents were tied to legitimate tools

In cyber-attacks, adversaries use legitimate tools which can't be detected as malicious utilities as they are often used in ordinary daily activities.

Suspicious events that blend with normal activity can be identified after deep analysis of malicious attack and connection of the use of these tools to the incident. The top used tools are PowerShell, PsExec, SoftPerfect Network Scanner, and ProcDump.



Most legitimate tools are used for harvesting credentials from memory, evading security mechanisms by unloading security solutions, and for discovery of services in the network. PowerShell can be used for virtually any task.

Let's weight those tools based on occurrence of such tool in the incident — we will also see tactics* where they are usually applied.

Execution	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control	Impact
38.6%	9.6%	10.8%	16.9%	19.3%	1.2%	1.2%	2.4%
Powershell PsExec PsTools Rexec	PC Hunter Powertool Process Hacker Sdelete	Mouse Lock NirSoft Password Recovery Powertool ProcDump PsTools	Advanced Port Scanner KPortScan Nmap PsTools SoftPerfect	PsExec PsTools Rexec	Mouse Lock	TightVNC	DiskCryptor

Exploits

Most of the identified exploits in incident cases appeared in 2019 along with well-known remote code execution vulnerability in Windows SMB service (MS17-010) being actively exploited by a large number of attackers.

MS17-010

SMB service in Microsoft Windows

Remote code execution vulnerability that was used in several large attacks such as WannaCry, NotPetya, WannaMine etc.

CVE-2019-0604

Microsoft Sharepoint

Remote code execution vulnerability allows attackers to execute arbitrary code without authentication in Microsoft Sharepoint.

CVE-2019-19781

Citrix Application Delivery Controller & Citrix Gateway

This vulnerability allows unauthenticated remote code execution on all hosts connected to Citrix infrastructure.

CVE-2019-0708

RDP service in Microsoft Windows

Remote code execution vulnerability (codename: BlueKeep) for a very widespread and unfortunately frequently publicly available RDP service.

CVE-2018-7600

Drupal

Remote code execution vulnerability also known as Drupalgeddon2. Widely used in installation of backdoors, web-miners and other malware on compromised web-servers.

CVE-2019-11510

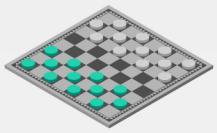
Pulse Secure SSL VPN

Unauthenticated retrieval of VPN server user credentials. Instant access to victim organization through legitimate channel.

* MITRE ATT&CK

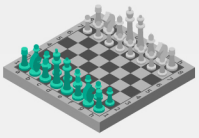
Attack duration

Kaspersky specialists have established the time period between the beginning of the attackers' activity and the end of the attack. As a result of the subsequent analysis, all incidents were divided into three categories of attack duration.



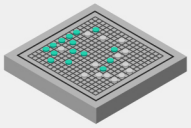
Rush

hours and days



Average

weeks



Long lasting

months and longer

Common threat

Rush	Average	Long lasting
Ransomware infection	Financial theft	Cyber espionage and theft of confidential data

Common attack vector

Rush	Average	Long lasting
▪ Downloading a malicious file by link in email ▪ Downloading a malicious file from infected site ▪ Exploitation of vulnerabilities on network perimeter ▪ Credentials guessing attack (bruteforce)	▪ Downloading a malicious file by link in email ▪ Exploitation of vulnerabilities on network perimeter	▪ Exploitation of vulnerabilities on network perimeter

Attack Duration (median)

Rush	Average	Long lasting
1 day	10 days	122 days

Incident response duration

Hours to days

This category includes attacks lasting up to a week. These are mainly incidents involving ransomware attacks. Due to the high speed of development, effective counteraction to these attacks is possible only by preventive methods. In some cases, up to a week delay has been observed between the initial compromising and the beginning of the attacker's activity.

Weeks

This group includes attacks that have been developing for a week or several weeks. In most cases, this activity was aimed at the direct theft of money.

Typically, the attackers achieved their goals within a week.

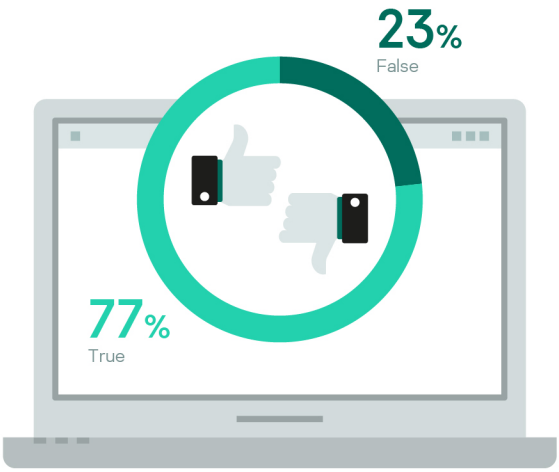
Months

Incidents that lasted more than a month 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. The total duration of active phases is on average close to the duration of attacks from the previous group.

Operational metrics

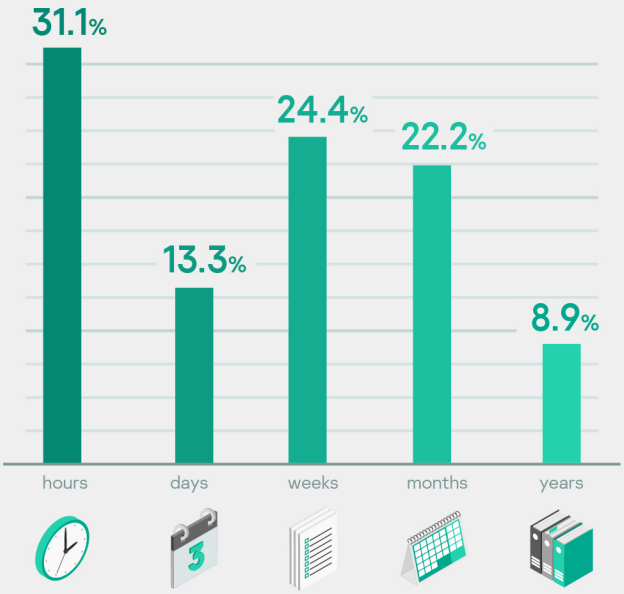
False positives rate

False positive for incident response is a very expensive activity. It means that triage of security event led to involvement of incident response experts who later identified that there is no incident. Usually this means the organization doesn't have a specialist in threat hunting or they are managed by external SOC which doesn't have context for the event.



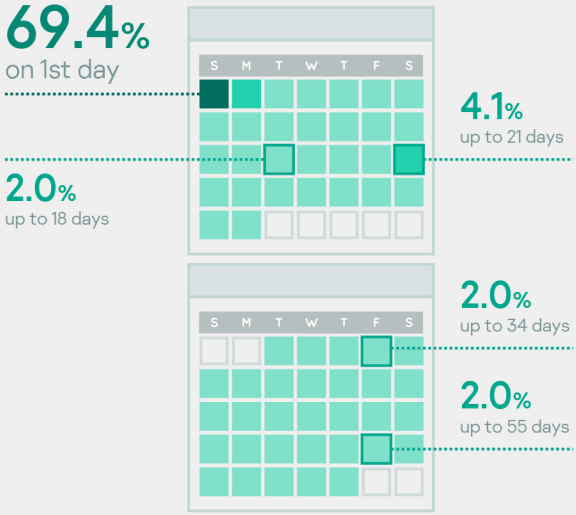
Age of attack

This defines the time for incident detection by organization after the attack started. Usually detecting the attack in the early hours and even days is good. In case of more low-profile attacks it can take weeks which is ok, but taking months and years is definitely bad.



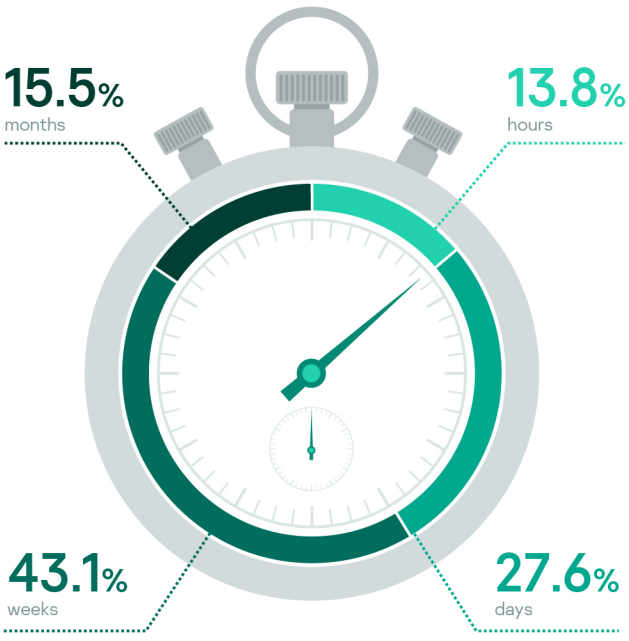
How fast we started

How long it took to start response after organization contacted us. In 70% of time we are working from day 1, but a variety of factors can influence the duration in some occasions.



How long response took

Distribution of time required for incident response activities.



MITRE ATT&CK tactics and techniques

Mapping to ATT&CK frameworks was done for about 50% of all incident response cases.

>0% >5% >10% >25% >50%

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Valid Accounts	Windows Remote Management	Accessibility Features	Accessibility Features	Obfuscated Files or Information	Credential Dumping
Replication Through Removable Media	Service Execution	DLL Search Order Hijacking	DLL Search Order Hijacking	Masquerading	Network Sniffing
External Remote Services	Windows Management Instrumentation	New Service	New Service	DLL Search Order Hijacking	Input Capture
Drive-by Compromise	Scheduled Task	Scheduled Task	Scheduled Task	Software Packing	Credentials in Files
Exploit Public-Facing Application	Command-Line Interface	Registry Run Keys / Startup Folder	Process Injection	Process Injection	Account Manipulation
Spearphishing Link	Graphical User Interface	Valid Accounts	Valid Accounts	Scripting	Brute Force
Spearphishing Attachment	Scripting	Windows Management Instrumentation Event Subscription	Web Shell	Indicator Removal on Host	LLMNR/NBT-NS Poisoning and Relay
	Third-party Software	Account Manipulation	Access Token Manipulation	Valid Accounts	Password Filter DLL
	Rundll32	Web Shell	Hooking	Rundll32	Hooking
	PowerShell	External Remote Services		Disabling Security Tools	Kerberoasting
	Execution through API	Create Account		Connection Proxy	
	Trusted Developer Utilities	Office Application Startup		Web Service	
	Execution through Module Load	Hidden Files and Directories		File Deletion	
	Mshta	Hooking		Modify Registry	
	Component Object Model and Distributed COM			Code Signing	
	User Execution			Trusted Developer Utilities	
	Signed Binary Proxy Execution			Access Token Manipulation	
				Deobfuscate / Decode Files or Information	
				Hidden Files and Directories	
				Mshta	
				Process Doppelgänging	
				DCShadow	
				Signed Binary Proxy Execution	
				Group Policy Modification	

>0% >5% >10% >25% >50%

Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Application Window Discovery	Windows Remote Management	Data from Network Shared Drive	Data Compressed	Data Obfuscation	Data Encrypted for Impact
Query Registry	Third-party Software	Input Capture	Automated Exfiltration	Fallback Channels	Inhibit System Recovery
System Network Configuration Discovery	Pass the Hash	Screen Capture	Data Encrypted	Custom Cryptographic Protocol	Stored Data Manipulation
Remote System Discovery	Remote Desktop Protocol	Email Collection	Exfiltration Over Command and Control Channel	Standard Cryptographic Protocol	Runtime Data Manipulation
Network Sniffing	Windows Admin Shares	Clipboard Data	Exfiltration Over Alternative Protocol	Commonly Used Port	Resource Hijacking
Network Service Scanning	Replication Through Removable Media	Data from Information Repositories	Exfiltration Over Physical Medium	Standard Application Layer Protocol	
System Network Connections Discovery	Pass the Ticket			Multilayer Encryption	
Process Discovery	Remote File Copy			Connection Proxy	
Permission Groups Discovery	Component Object Model and Distributed COM			Custom Command and Control Protocol	
System Information Discovery	Exploitation of Remote Services			Standard Non-Application Layer Protocol	
File and Directory Discovery	Exploitation of Remote Services			Web Service	
Account Discovery				Remote File Copy	
Peripheral Device Discovery				Data Encoding	
Network Share Discovery				Domain Fronting	
				Remote Access Tools	
				Domain Generation Algorithms	