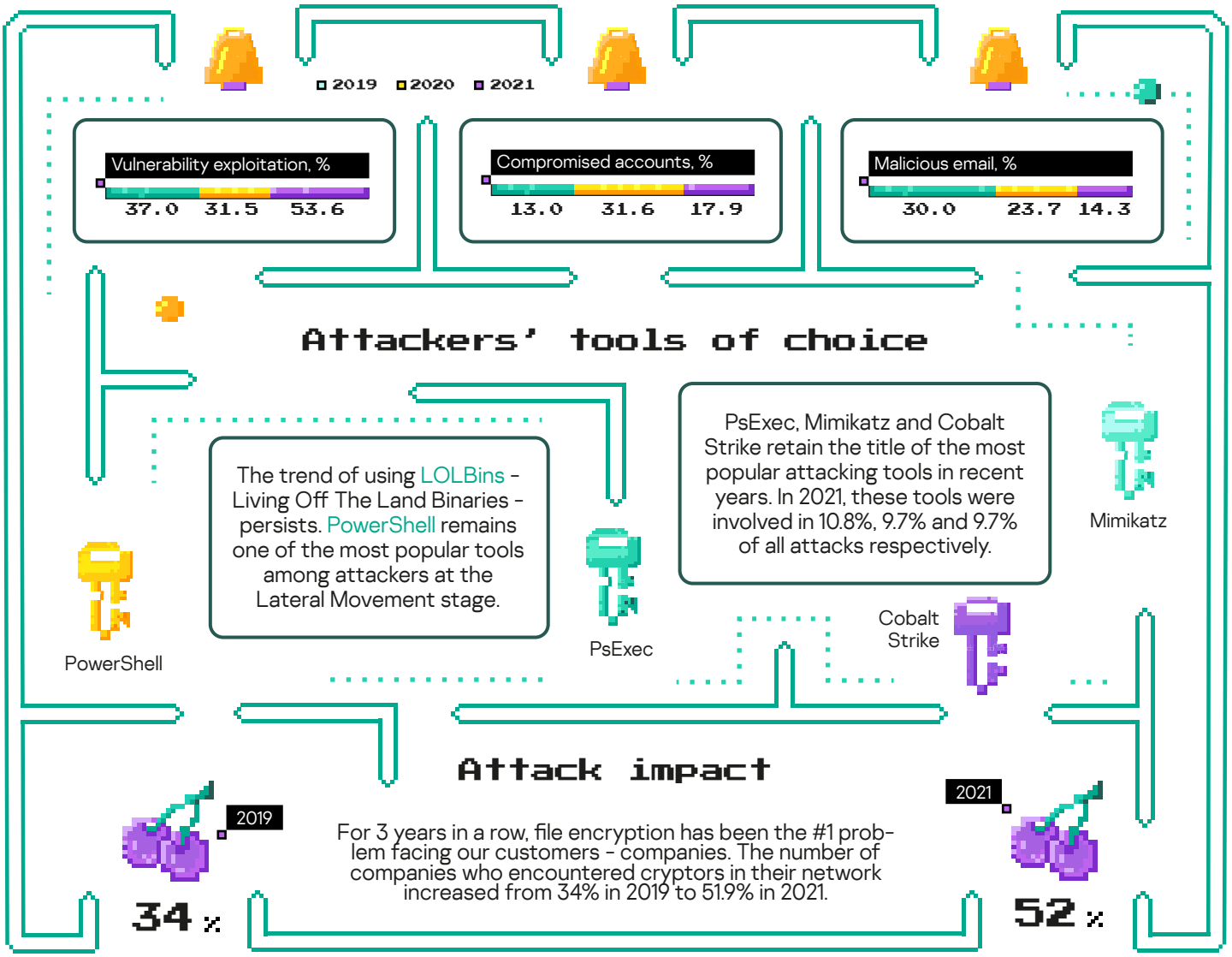
The nature of cyber incidents

Based on cyberattack investigations by Kaspersky Global Emergency Response Team

kaspersky

How attackers first gained access



Attackers' tools of choice

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 retain the title of the most popular attacking tools in recent years. In 2021, these tools were involved in 10.8%, 9.7% and 9.7% of all attacks respectively.

PowerShell

PsExec

Mimikatz

Cobalt Strike

Attack impact

2019

34%

For 3 years in a row, file encryption has been the #1 problem facing our customers - companies. The number of companies who encountered cryptors in their network increased from 34% in 2019 to 51.9% in 2021.

2021

52%

Top targeted industries

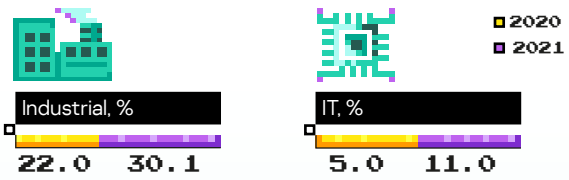
Industrial, Government and Financial remain the top 3 targeted industries.

Industrial

Government

Financial

In 2021 we noticed a significant growth in incident response requests from Industrial and IT companies.



Top 3 attacked regions

Companies requesting Kaspersky Incident Response services were mostly from 3 regions.

Europe
Came out on top in 2021 with 30.1%

CIS
First place in 2020

Middle East
The #1 region in 2019

Trends in 2021

Ransomware cases

Distribution of attacks by duration depending on the initial vector

Initial attack vector	Hours	Weeks	Months	Grand Total
Exploitation of public-facing applications	12.5%	0.0%	25.0%	37.5%
Malicious email	0.0%	0.0%	25.0%	25.0%
Compromised accounts	12.5%	12.5%	12.5%	37.5%
Grand Total	25.0%	12.5%	62.5%	100.0%

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 vulnerabilities and previously compromised user accounts were used in 37.5% of cases, while malicious mail was used in every fourth case with cryptors.

However, in a number of attacks, the adversary's 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 10% of cases with cryptors.

In addition, the purpose of using cryptors is sometimes to hide the initial traces of an attack and complicate incident investigations.
Analyzing the duration of attacks with cryptors, it can be concluded that a significant period of time passes between the initial compromise of the network and the final stage of the attack. In 62.5% of attacks, attackers spend more than a month inside the network before encrypting data. A properly organized process of attack detection and response reduces the time it takes to detect attackers in the network and prevent final damage.
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 CVE-2021-26855 Microsoft Exchange SSRF vulnerability in Microsoft Exchange Server which allows attackers to send arbitrary HTTP requests and authenticate as the Exchange server (used by Hafnium group). It was exploited in 22.7% of cases when vulnerabilities were used.
Despite the fact that the protection measures against this attack vector are straightforward - security update, 1-day vulnerabilities are far ahead of other methods of initial penetration.

2021 Incident Response Overview & Experts' Recommendations

Response statistics are based on IR retainer and emergency cases from 2021.

Threat intelligence view

Initial attack vector

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

53.6% Exploitation of public-facing applications

14.3% Malicious email

17.9% Compromised accounts

- 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
- Ensure employees maintain a high level of security awareness

Move around and get things done

In 39.7 % of all cases, legitimate tools were used

Cobalt Strike	Mimikatz	PowerShell	PsExec
9.7%	9.7%	8.6%	10.8%

Impact

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

16.0% Data leakage

51.9% Files encrypted

11.1% Active Directory compromised

Understand the adversary profiles targeting your industry and region to prioritize security operations development

Industry, %

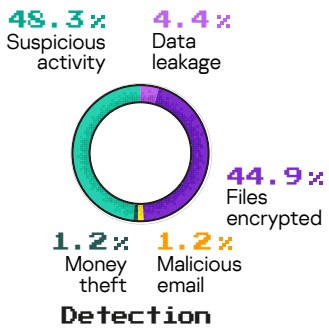
12.9	19.4	30.1	11.8
Financial	Government	Industrial	IT

Regions, %

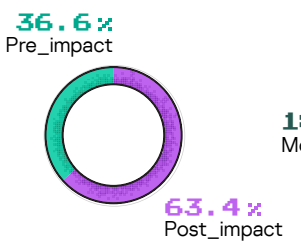
6.5	3.2	24.7	30.1	8.6	23.7	3.2
Africa	APAC	CIS	EU	LatAm	ME	NA

Security operations metrics view

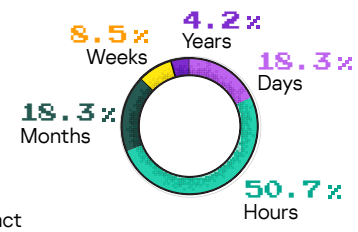
Detection reason



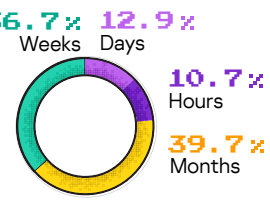
Detection before or after the impact



Attack duration



Remediation duration



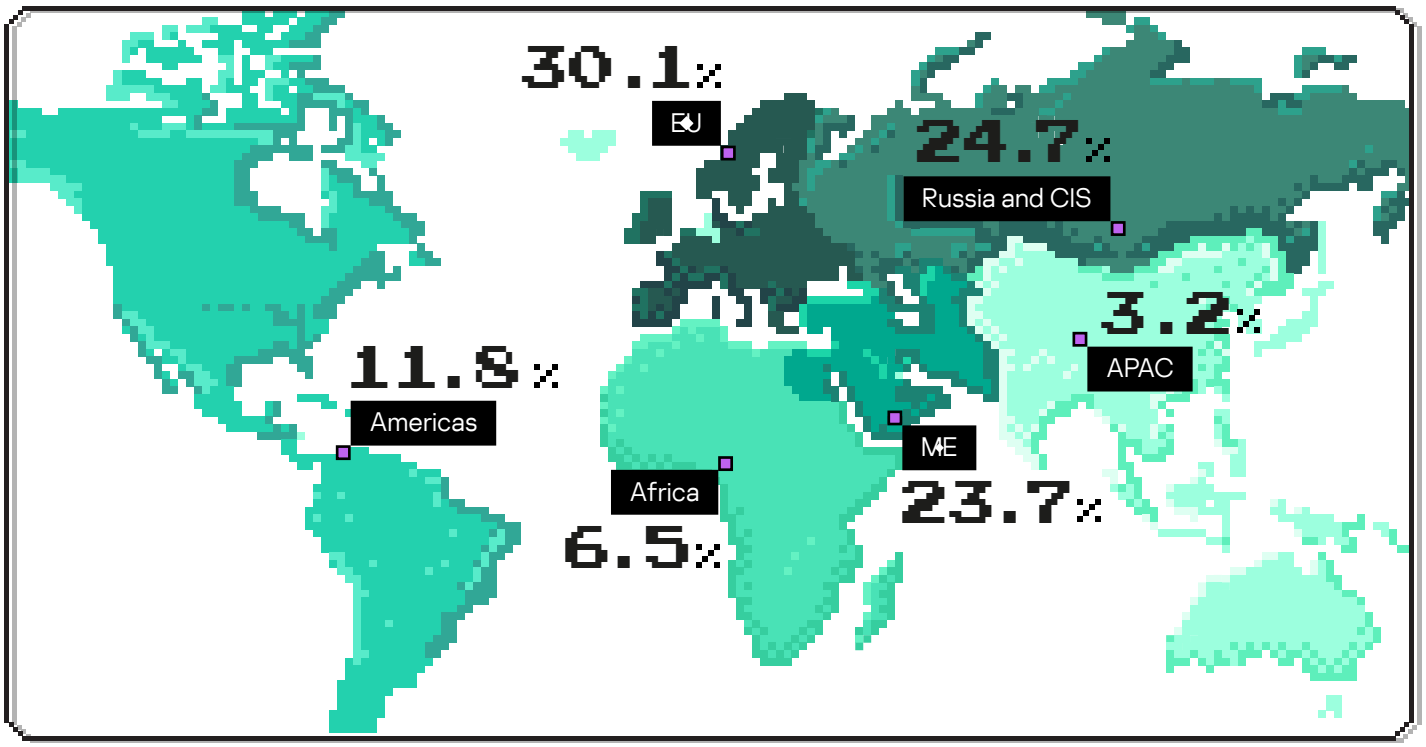
Introduction

The Incident Response Analyst Report provides insights into incident investigation services conducted by Kaspersky in 2021. 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[1].

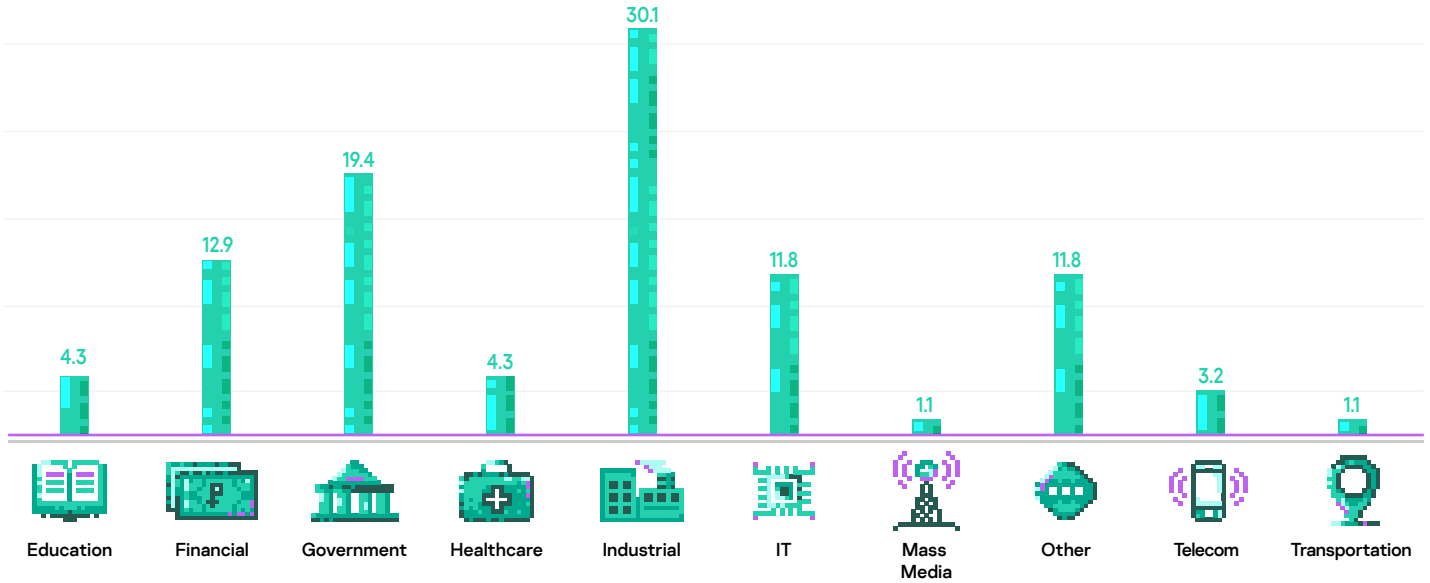
In 2020, the COVID-19 pandemic forced companies to restructure their information security practices to accommodate remote working. In 2021, although the main threat trends remained, our service approach moved to near-complete - 98% of all cases - remote delivery.

Kaspersky Digital Forensics and Incident Response operations are handled by our Global Emergency Response Team (GERT)[2] with experts in Europe, Asia, South and North America, the Middle East and Africa.

Geography of incident responses



Verticals and industries, %



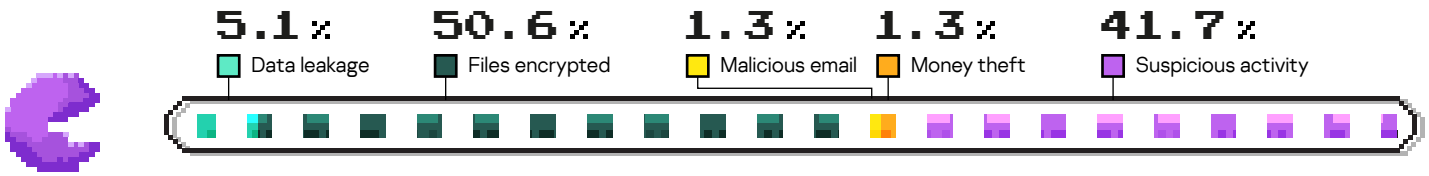
[1] The analytics are based on commercial incident response cases performed by Kaspersky
[2] https://www.kaspersky.com/enterprise-security/incident-response

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 financial).

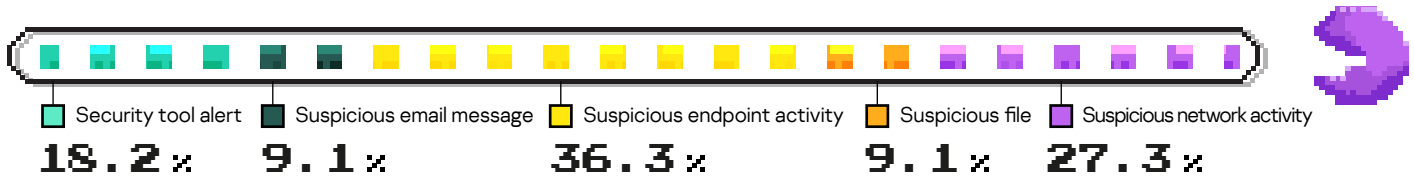
We can confidently classify most incidents with causes before impact (suspicious events, tool alerts, etc.) as ransomware.

True positives



12.9% of all incident response requests were for false alarms. Suspicious activity[3] reported by network sensors (NIDS, firewall) and endpoint protection (EPP) generate the most false positives. Every second request based on suspicious activity from a network sensor or endpoint was a false positive. Data leakage false positive cases are usually duplicates or leaks from a different organization.

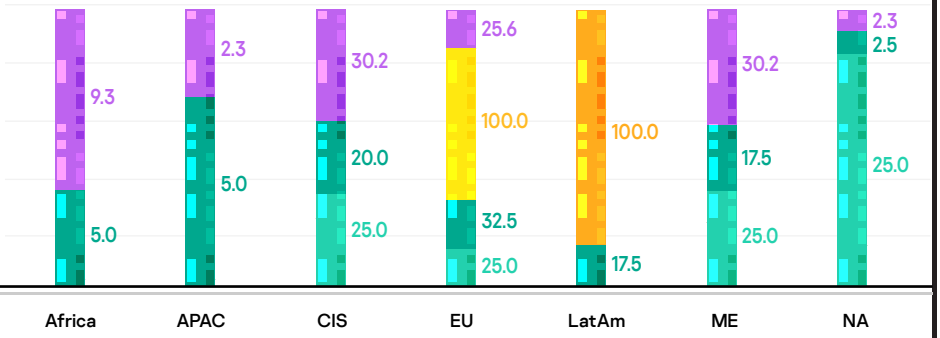
False positives

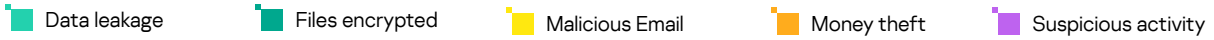


For many years, ransomware attacks have retained a dominant role in the cybersecurity threat landscape. We urge you to get up-to-date and actionable information about ransomware attacks from our publications[4] and NoRansom[5] project.

Reasons per region

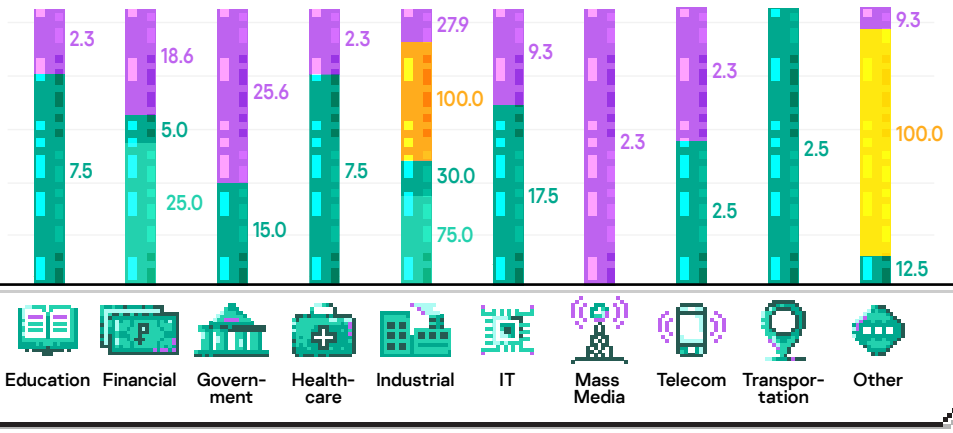
Ransomware attacks and suspicious activity were the primary reasons to trigger an investigation throughout most regions.





Reasons per industry

Even when targeting the financial sector, money is no longer the goal for attackers. Data is the target - and data leakage is the reason for half of our investigations in the sector.



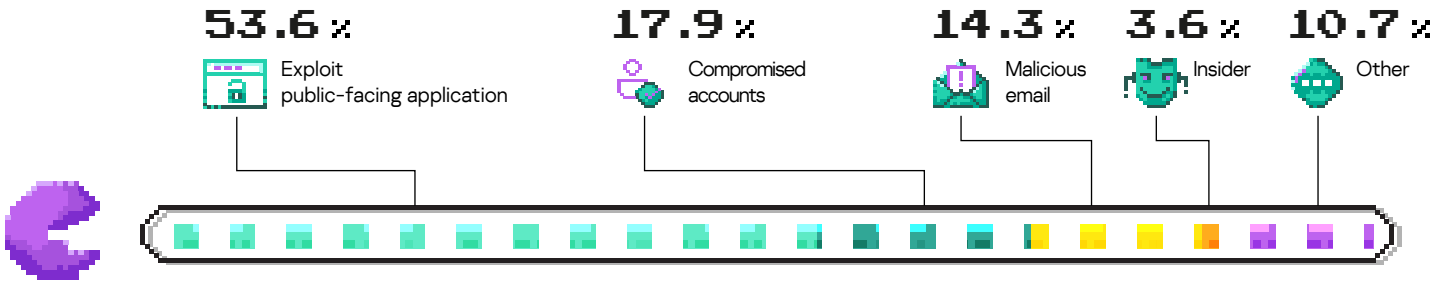
[3] Suspicious activity is a category for a security tool stack generated alert or user reported anomalous behavior
[4] https://www.kaspersky.com/enterprise-security/apt-intelligence-reporting
[5] https://noransom.kaspersky.com

Initial vectors

Or how attackers get in

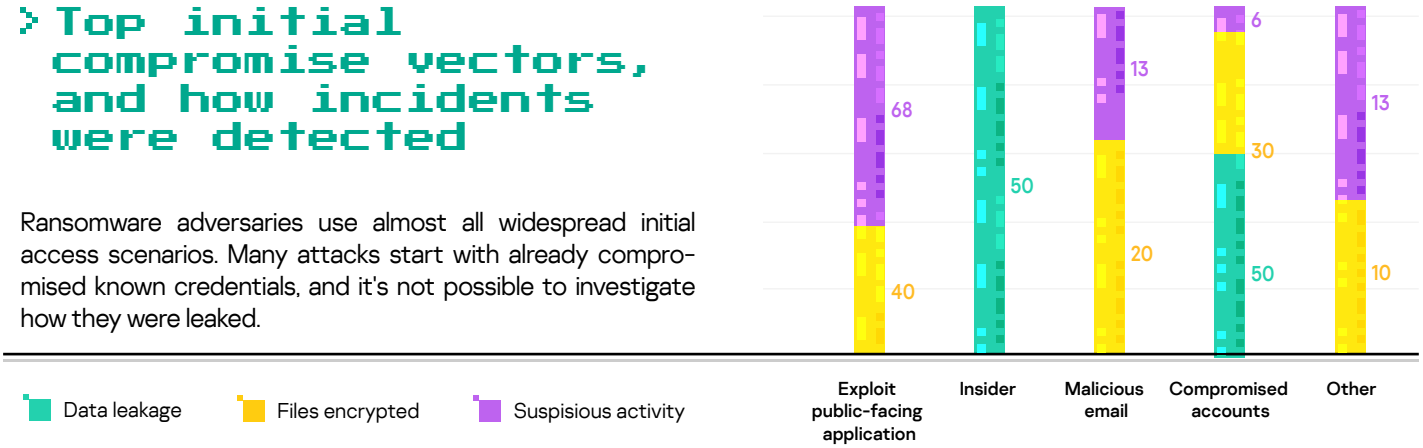
Year after year, security issues with passwords, software vulnerabilities and social engineering combine into an overwhelming majority of initial access vectors[6] during attacks. Setting up and controlling a password policy, patch management and employee awareness along with anti-phishing measures significantly 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 50%.

In 2021, vulnerabilities were discovered in MS Exchange. Because of Exchange's ubiquitous nature and publicly available exploits for these vulnerabilities, the result is a huge number of related incidents.



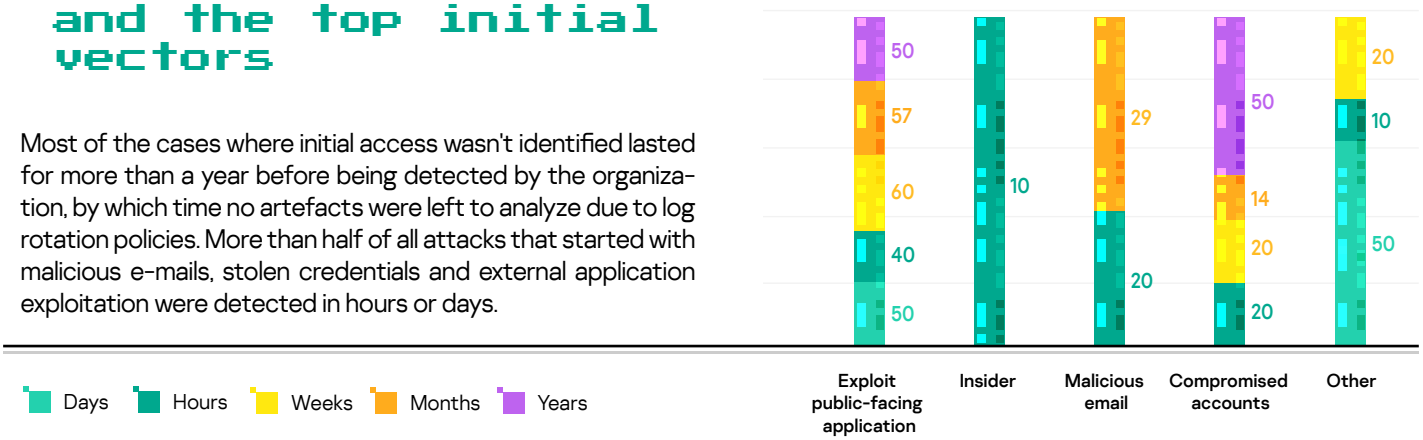
Top initial compromise vectors, and how incidents were detected

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.



How long the attack went unnoticed, and the top initial vectors

Most of the cases where initial access wasn't identified 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 and external application exploitation were detected in hours or days.



[6] We identified the initial vector of attack for 30% of cases. Very old incidents, unavailable logs, (un)intentional evidence destruction by victim organization, and supply-chain attacks are among the numerous reasons not to reveal how adversaries initially gained a foothold into the network

Tools and exploits

40%

of all incidents were tied to tools

Almost half of all incident cases included the usage of existing OS tools (like Lolbins)[7], well known offensive tools from github (e.g. Mimikatz, AdFind, Masscan) and specialized commercial frameworks (Cobalt Strike). Because it's very hard to detect these with traditional security controls, another approach is required. Kaspersky Managed Detection and Response detects the usage of such software.

Distribution and frequency of tools inside incident cases

Frequent

5–8%[8]

Cobalt Strike, Mimikatz, PowerShell, PsExec

Average

3–4%

Advanced IP Scanner, Bitlocker, ProcDump, ProcessHacker

Rare

1–2%

AnyDesk, DiskCryptor, Everything, Fast Reverse Proxy FRP, Meterpreter, reg.exe, RMS, SMBExec, WebBrowser-PassView.exe

Distribution and frequency of tools through 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	Defense evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Impact
20.9%	11.9%	26.1%	13.4%	12.7%	2.2%	8.3%	4.5%
PowerShell PsExec SmbExec	ProcessHacker PCHunter PowerTool	Mimikatz PowerTool ProcDump	Advanced IP Scanner nbtscan wmic	Cobalt Strike Impacket PowerSploit Empire_Powershell	Everything 7zip	RDP AnyDesk RMS	DiskCryptor BitLocker

[7] https://lolbas-project.github.io
[8] Each tool was identified in 5-8% of incident cases

Exploit usage was identified in 14% of all incidents

In 2021, vulnerabilities for widely used software were published and affected many companies. Patch management policies continue to be a very important security point.

CVE-2021-34523

Microsoft Exchange

Elevation of Privilege (EoP) vulnerability.
The vulnerability allows attackers to raise their permissions.
Part of the ProxyShell vulnerabilities chain.

CVE-2021-26857

Microsoft Exchange

An insecure deserialization vulnerability in the Unified Messaging service in Microsoft Exchange. Attackers need to authenticate using other exploits or stolen credentials. The vulnerability allows attackers to execute arbitrary code and write arbitrary files.
Used by the Hafnium group.

CVE-2021-34473

Microsoft Exchange

Remote Code Execution (RCE) vulnerability. Flaw in the Autodiscover service of Exchange Server, unauthenticated attackers can access its restricted resources and leverage this in conjunction with other vulnerabilities to execute arbitrary code.
Part of the ProxyShell vulnerabilities chain.

CVE-2021-26855

Microsoft Exchange

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.

CVE-2021-31207

Microsoft Exchange

Security Feature Bypass vulnerability.
The vulnerability allows attackers to bypass the authentication process. Part of the ProxyShell vulnerabilities chain.

CVE-2019-17558

Apache Solr

Remote code execution vulnerability allows attackers to execute arbitrary code without authentication in Apache Solr through the VelocityResponseWriter.

CVE-2021-27065

Microsoft Exchange

Post-authentication arbitrary file write vulnerability. Attackers need to authenticate using other exploits or stolen credentials. The vulnerability allows attackers to execute arbitrary code and write arbitrary files. Used by the Hafnium group.

CVE-2018-19320

Gigabyte Drivers

GDrv low-level driver vulnerability. The attackers use the exposed functions in gdrv.sys that allow a low-level user to allocate and write data to memory for escalating the privileges to SYSTEM.

CVE-2021-26858

Microsoft Exchange

Post-authentication arbitrary file write vulnerability. Attackers need to authenticate using other exploits or using stolen credentials. The vulnerability allows attackers to execute arbitrary code and write arbitrary files. Used by the Hafnium group.

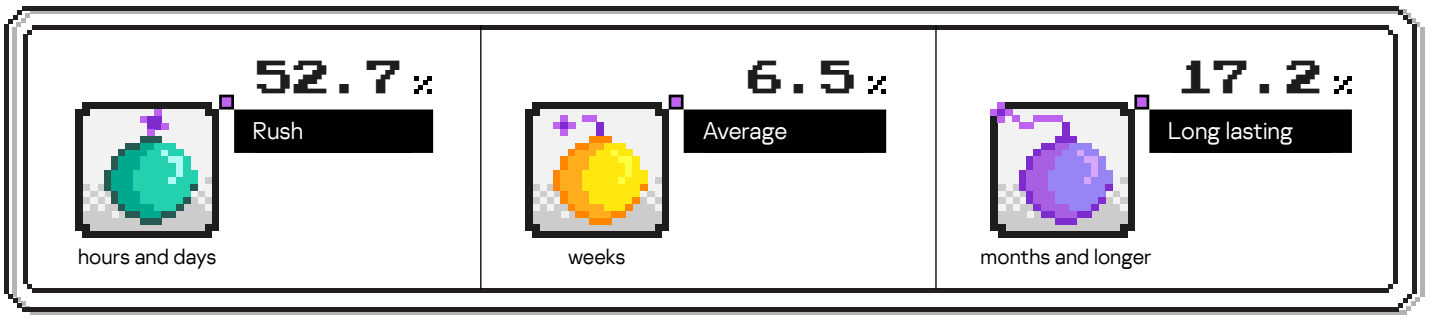
CVE-2018-13379

Fortinet FortiOS

A path traversal vulnerability in the FortiOS SSL VPN web portal allows unauthenticated attackers to download system files via specially crafted HTTP resource requests.

Attack duration

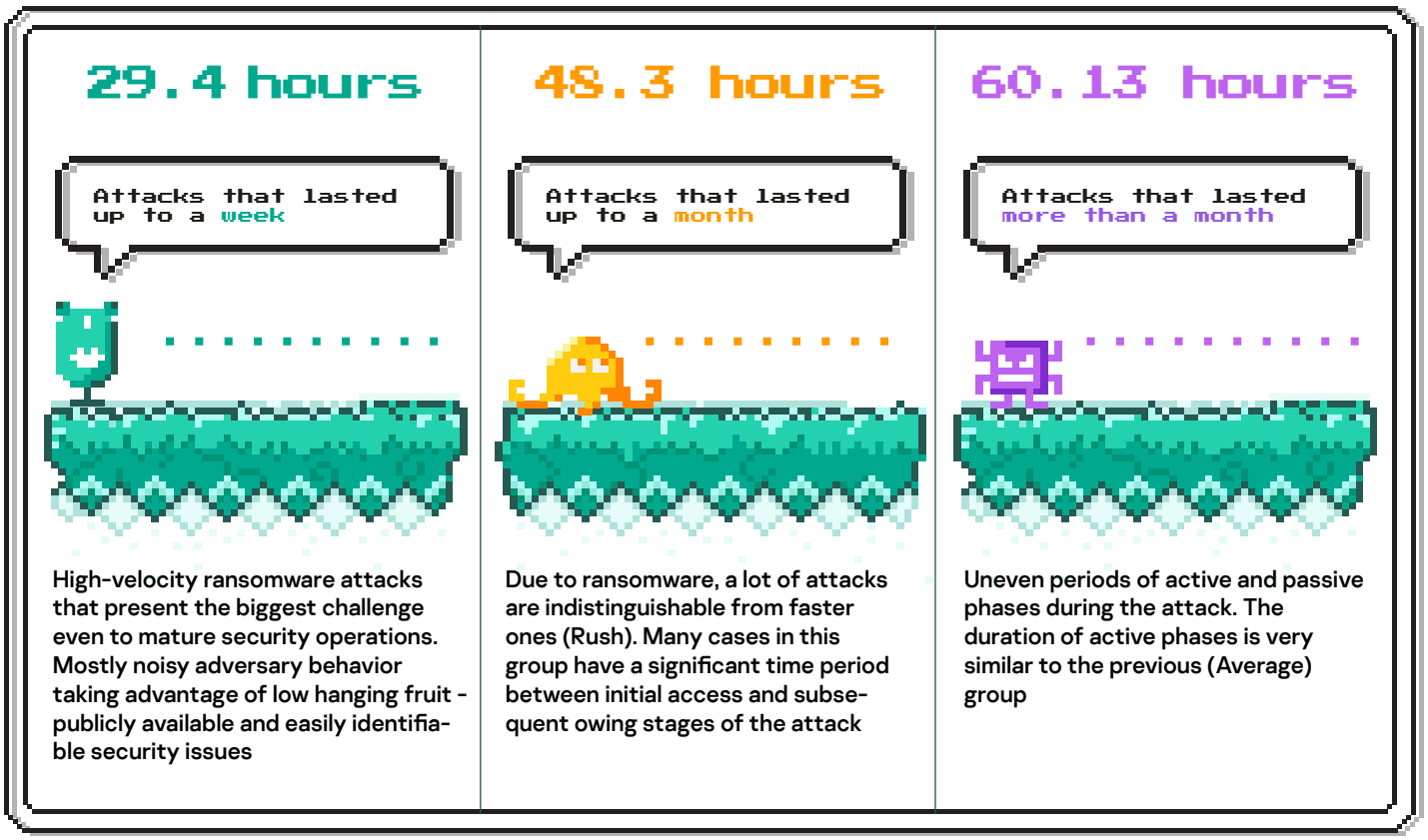
All incident cases can be grouped into three categories with different attack dwell times, incident response duration and attack impact.



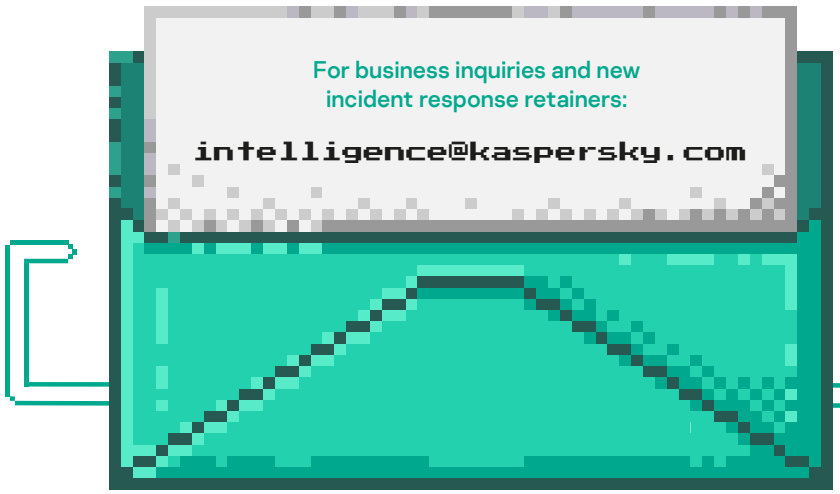
Average attack duration

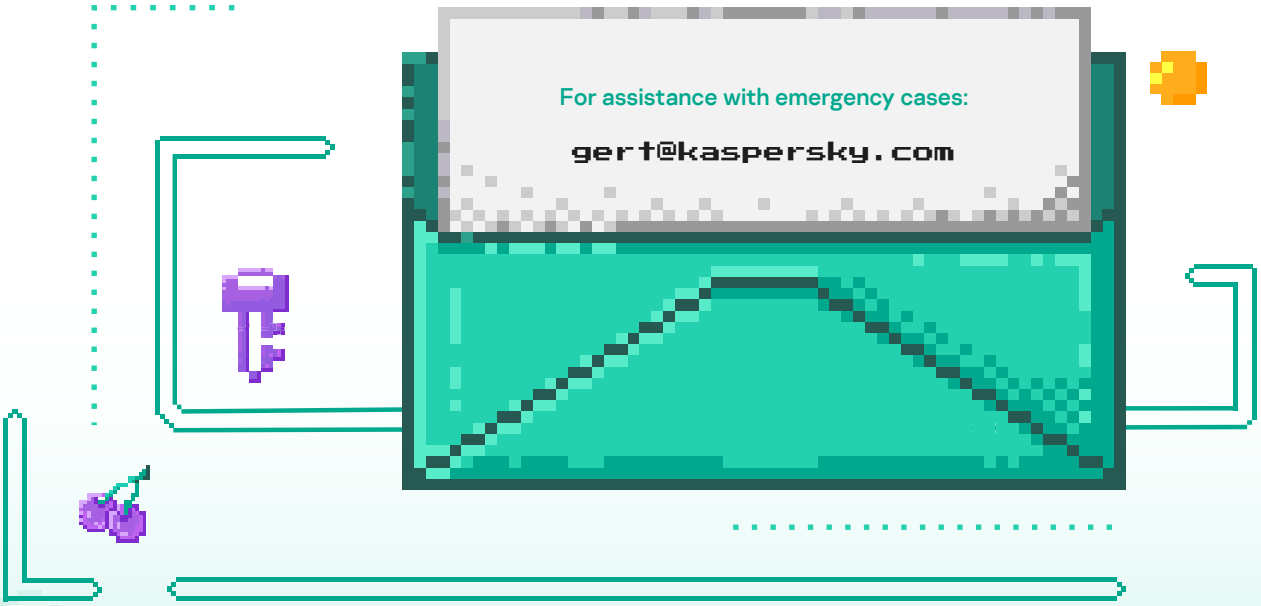
Representative impact

Incident response duration (time spent investigating)



Contacts


For business inquiries and new incident response retainers:
intelligence@kaspersky.com


For assistance with emergency cases:
gert@kaspersky.com