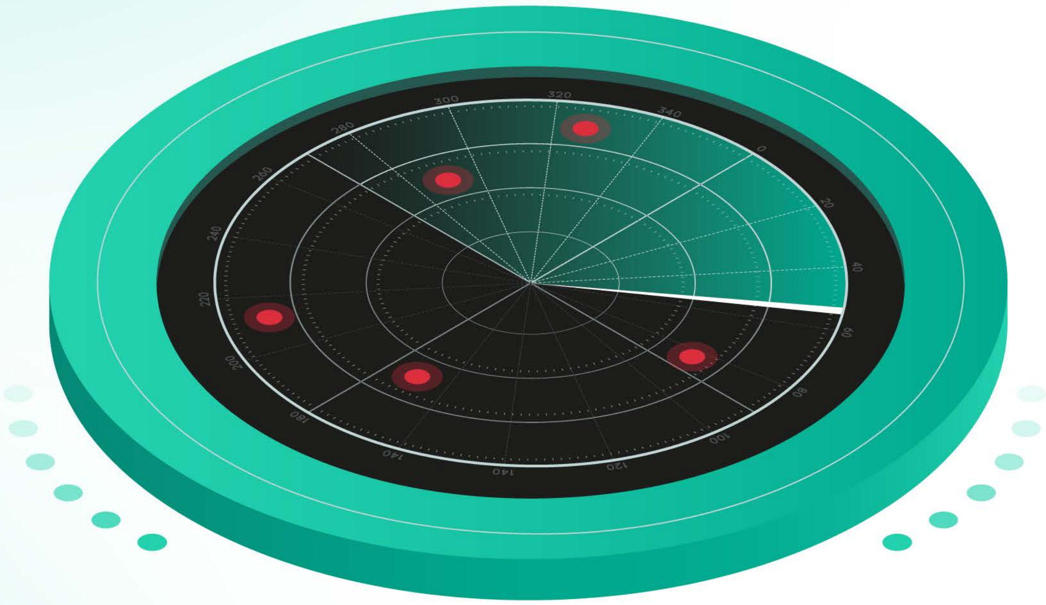
Incident response analyst report

2021



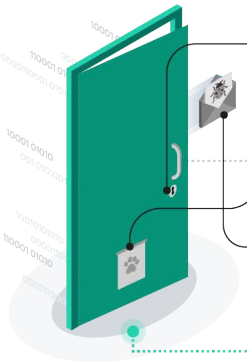
kaspersky

Executive summary

Incident Response statistics are based on IR retainer and emergency cases from 2020.

Threat intelligence view

Initial attack vector



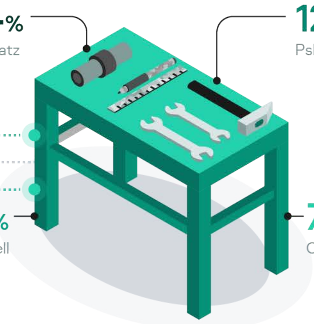
31.6% Brute-force

31.5% Vulnerability exploitation

23.7% Malicious e-mail

- Implement robust password policy and multifactor authentification
- Remove management ports from public access
- Patch management or compensation measures for public-facing applications should have zero tolerance
- Maintain a high level of security awareness among employees

Move around and get things done



13.4% Mimikatz

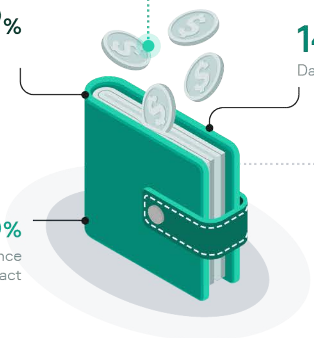
12.3% PsExec

8.2% PowerShell

7.2% Cobalt Strike

- Implement rules for detection of widespread 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)

Impact



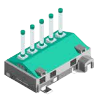
37.9% Ransomware

14.7% Data leakage

10.5% Persistance for future impact

- Backup your data (offline backup)
- Establish an Incident Response Retainer partner to address incidents with prompt SLAs
- Implement strict security programs for applications with PII
- Continuously maintain incident response team readiness through training and offensive exercises

Industry



22%	19%	13%	13%
Industrial	Government	Financial	Telecom

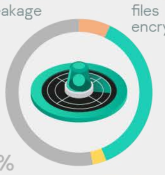
Understand adversary profiles targeting your industry and region to prioritize security operations development

Region

27.8%	26.8%	24.7%	16.5%
CIS	META	Europe	Americas

Security operations metrics view

Detection reason



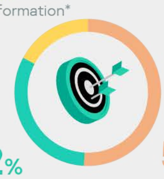
7.2% data leakage

36.7% files encrypted

53% suspicious activity

3.1% money theft

Detection before or after impact



17% no information*

32% before impact

51% after impact

Attack duration

18% months

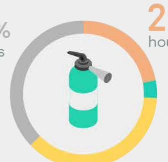
2% years

28% hours

20% weeks

32% days

Remediation duration



37% months

22% hours

4% days

37% weeks

* There is no information about the impact of an event when we act as a complementary supplier for another IR team on the case

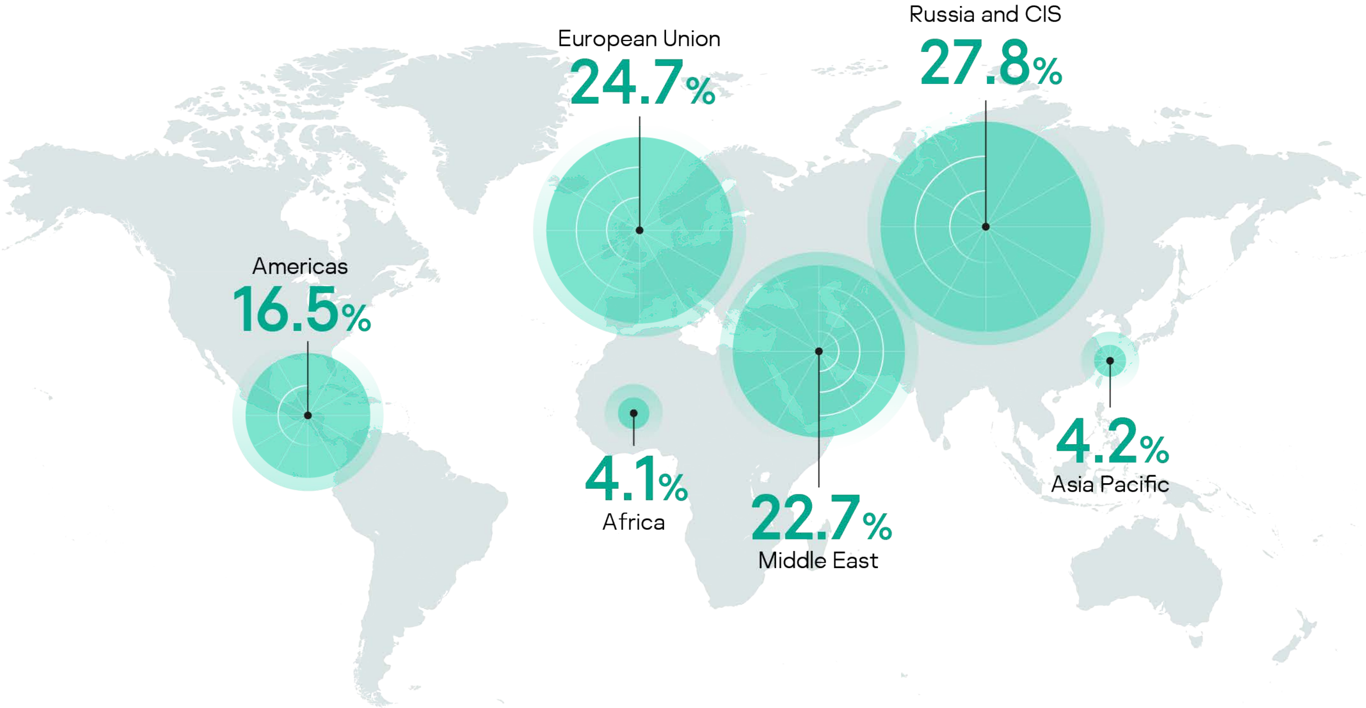
Introduction

The Incident Response Analyst Report provides insights into incident investigation services conducted by Kaspersky in 2020. 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 complementary expert activities for their internal incident response teams.

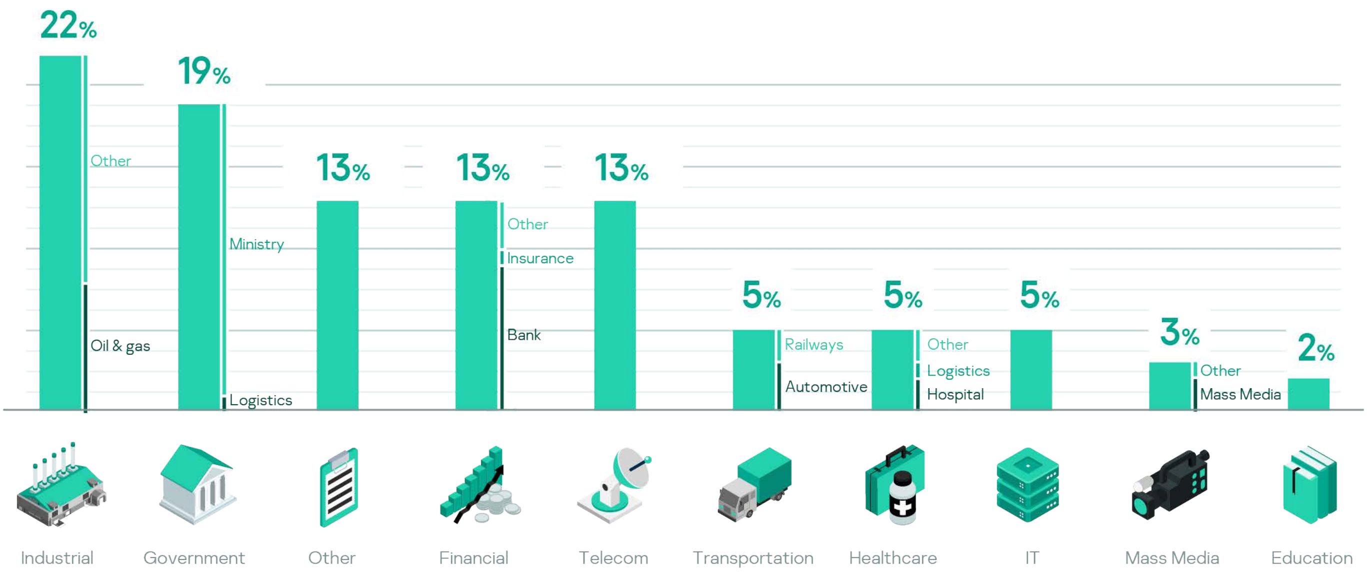
In 2020, pandemic forced companies to restructure their information security practices to accommodate a work from home (WFH) approach. Although the main trends in terms of threats have stayed the same, our service approach moved to a complete — 97% of all cases - remote delivery.

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

Geography of incident responses



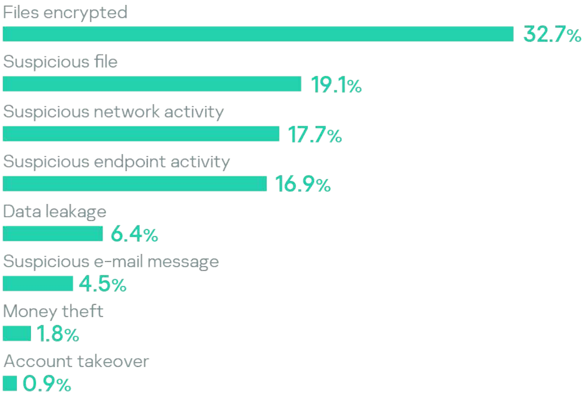
Verticals and Industries



Reasons to go for incident response

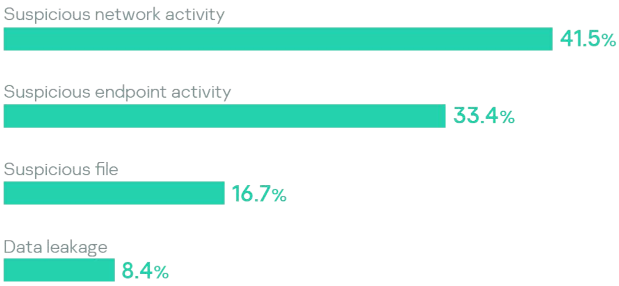
Ransomware is overtaking money theft and other impacts as a more convenient monetization scheme with much broader industry coverage (not just financial). Most of the incidents with causes before the impact (suspicious events, tool alerts, etc.) can be confidently classified as ransomware.

True positives



10% of all incident response requests were for false positives. Suspicious activity* reported by network sensors (NIDS, firewall) and endpoint protection (EPP) generate most of the false positives. Every 4th request based on suspicious activity from a network sensor or endpoint was found to be false positive. Data leakage false positive cases are usually duplicates or leaks from a different organization.

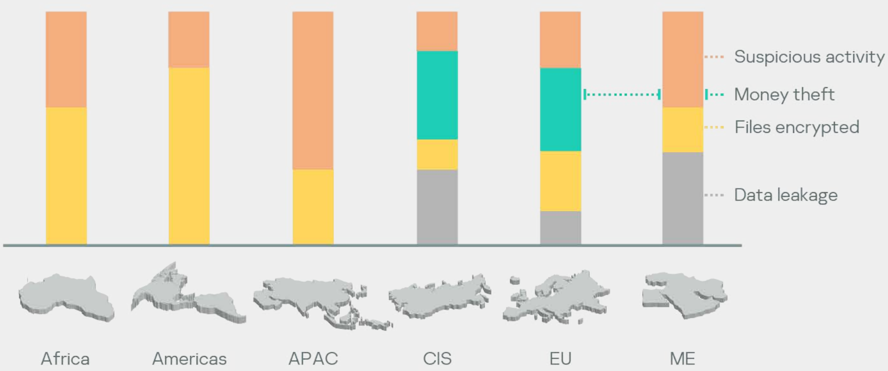
False positives



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

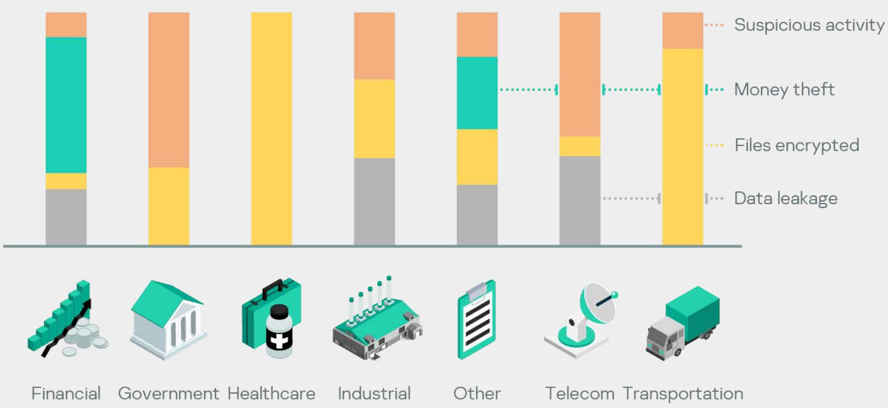
Distribution of reasons for our top regions

The Americas and Africa almost exclusively face ransomware attacks, whereas other regions see a wider variety and obvious PII concerns.



Distribution of reasons for selected industries

Old-school monetization from the financial sector is still in place, while Healthcare, Transportation and Industrial have become extensively affected by ransomware.
The Government sector showing no data leaks is likely due to the fact that governmental PII-heavy systems are usually hosted by Telecom and IT providers.



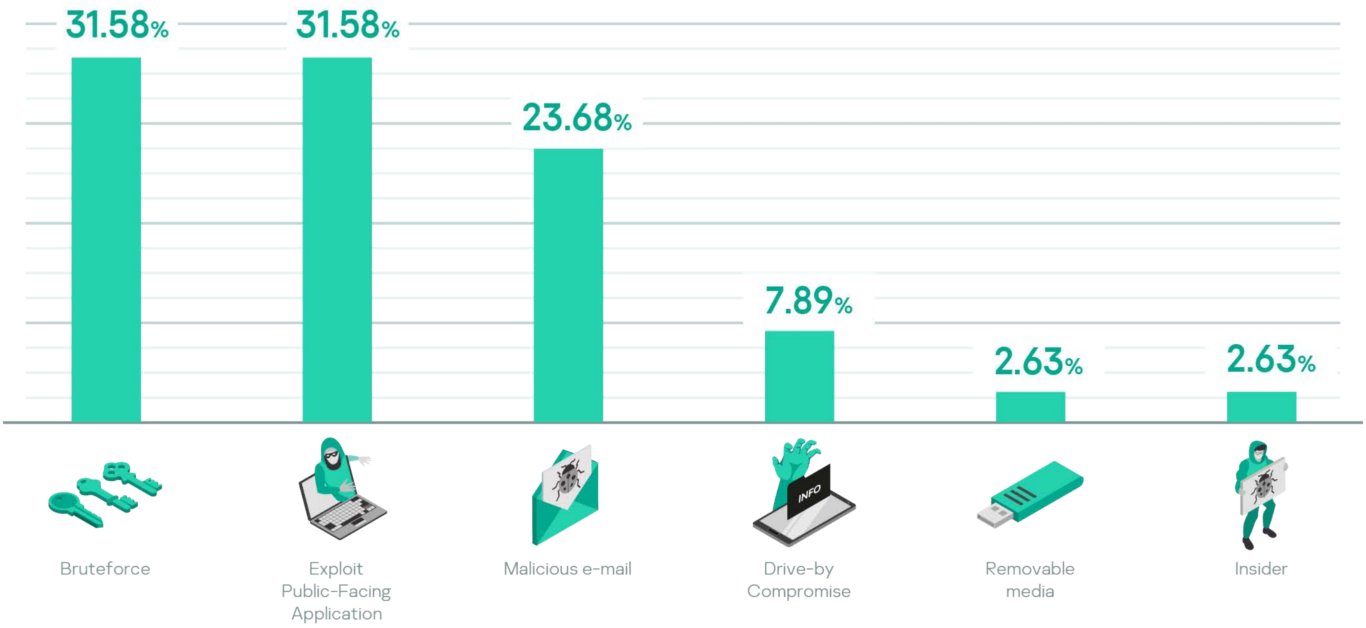
* Suspicious activity is a category for a security tool stack generated alert or a user reported anomaly behavior

Initial vectors

Or how attackers got in

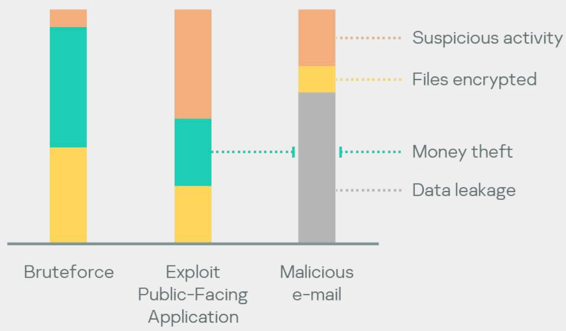
Year after year, security issues with passwords, software vulnerabilities and social engineering combine into the overwhelming majority of initial access vectors* during attacks. Setting up and controlling password policies, security patch management and employee awareness along with anti-phishing measures can 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 reduces the likelihood of becoming a victim by 30%, and implementing a robust password policy reduce the likelihood by 60%**.



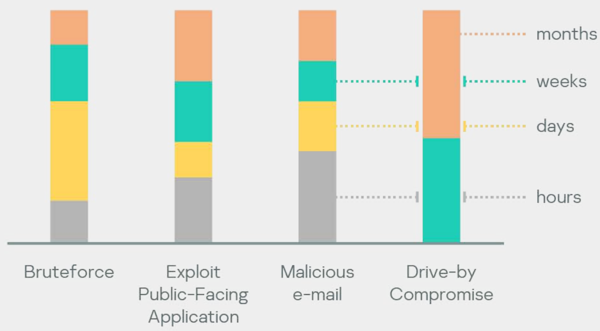
Top initial compromise vectors and how incidents were detected

Ransomware adversaries employ almost all widespread initial access scenarios. Attacks starting with brute force are easy to detect in theory, but in practice only a fraction of them were identified before impact.



How long the attack went unnoticed and top initial vectors

Most cases without initial access identification went unnoticed for more than a year before being detected – no artefacts left for analysis due to log retention policies. More than half of all attacks that started with malicious e-mails, brute force and external application exploitation were detected in hours to days.



* We identified the initial vector of attack in 55% of cases. Very old incidents, unavailable logs, (un)intentional evidence destruction by the victim organization, and supply-chain attacks were among the numerous reasons for failing to identify how adversaries initially gained a foothold in the network

** According to incident cases from our dataset

Tools and exploits

44% of all incidents were tied to tools

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

Inside all incident cases with tools

Frequent

11-13%

contained Mimikatz, PsExec, Advanced IP Scanner

Average

4-8%

contained PowerShell, Cobalt Strike, Process Hacker, ProcDump

Rare

2-3%

contained TeamViewer, Impacket, WMIC, PowerTool, Nmap, fgdump, Masscan, CScript, NetScan, WINrar, AdFind, NBTScan, PuTTY, RDP

Distribution and frequency of tools through ATT&CK tactics demonstrate a clear focus on everything between initial access and impact.

Those tools should be an outstanding instrument to boost incident detection while adversaries explore the network.

Execution	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control
26.2%	7.3%	18.8%	20.5%	18.1%	1.7%	7.4%
Cobalt Strike CScript Impacket PowerShell PsExec	ProcessHacker PowerTool	fgdump Mimikatz PowerTool ProcDump	AdFind Advanced IP Scanner Masscan NBTScan NetScan Nmap WMIC	Cobalt Strike Impacket PsExec	WINrar	PuTTY RDP TeamViewer

Exploit usage was identified in 13% of all incidents

In only a few incidents, vulnerabilities from 2020 were used. In other cases, the vulnerabilities utilized were several years old. This suggests that timely security updates could have prevented a tenth of the investigated attacks.

CVE-2020-0796

SMB service in Microsoft Windows

Remote code execution vulnerability allows attackers to execute arbitrary code without authentication in Microsoft SMBv3 service. Heir of MS17-010.

CVE-2020-0787

Windows Background Intelligent Transfer Service (BITS)

Privilege escalation vulnerability in Windows BITS. Widely used by ransomware.

CVE-2019-11510

Pulse Secure SSL VPN

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

CVE-2019-0604

Microsoft SharePoint

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

CVE-2018-8453

Win32k Microsoft Windows component

An elevation of privilege vulnerability exists in Microsoft Windows when the Win32k component fails to properly handle objects in memory. Used by FruityArmor APT group.

CVE-2017-0144

SMB service in Microsoft Windows

Vulnerability in SMBv1 allows remote attackers to execute arbitrary code via crafted packets. Used in EternalBlue exploit.

CVE-2017-11317

Telerik.Web.UI

Vulnerability uses weak RadAsyncUpload encryption, which allows remote attackers to perform arbitrary file uploads or execute arbitrary code.

CVE-2017-8464

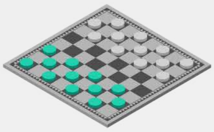
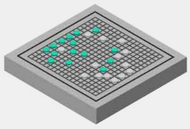
Microsoft Windows Shell

Allows local users or remote attackers to execute arbitrary code via a crafted .LNK file, handled during icon display in Windows Explorer or any other application that parses the icon of the shortcut. Used in LemonDuck attack.

* Each tool was identified in 11-13% incident cases

Attack duration

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

		
Rush hours and days	**Average** weeks	**Long lasting** months and longer
Attack duration average		
1.5 days	18.1 days	90.4 days
Representative impact		
Ransomware	Ransomware and money theft	Data leakage and ransomware
Initial attack vector (rated by frequency in cases)		
▪ Brute force ▪ Exploit public-facing application ▪ Spearphishing link	▪ Exploit public-facing application ▪ Drive-by compromise ▪ Brute force ▪ Replication through removable media ▪ Spearphishing link	▪ Exploit public-facing application ▪ Spearphishing attachment ▪ Brute force ▪ Drive-by compromise ▪ Insider
Incident response duration (effort in hours taken for investigation)		
34.4 hours ▪ 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	48.9 hours ▪ 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 the following stages of attack	105.6 hours ▪ Attacks that lasted more than a month ▪ Uneven periods of active and passive phases during attack. The duration of active phases is very similar to the previous (Average) group

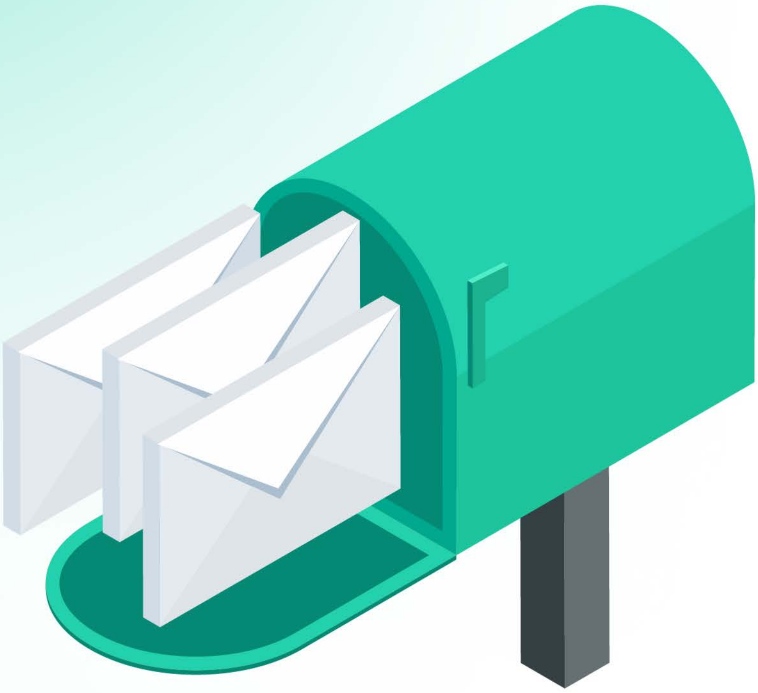
Contacts

Business inquiries

intelligence@kaspersky.com

Report and IR

gert@kasperksy.com



kaspersky