Executive summary

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

Threat intelligence view

- Initial attack vector
  - 31.6% - Phishing
  - 31.5% - Vulnerability exploitation
  - 23.7% - Malicious email

- Impact
  - 37.9% - Ransomware
  - 14.7% - Data leakage
  - 10.5% - Persistence for future impact

- Move around and get things done
  - 13.4% - Mirkatz
  - 12.3% - Ploxx
  - 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)

- 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

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

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

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

* 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 of 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 Incident Investigation Unit (CIU), and Global Research and Analysis Team (GReAT) with experts in Europe, Asia, South and North America, Middle East and Africa.

Geography of incident responses

- European Union: 24.7%
- Russia and CIS: 27.8%
- Americas: 16.5%
- Africa: 4.1%
- Middle East: 22.7%
- Asia Pacific: 4.2%

Verticals and Industries

- Other: 19%
- Oil & Gas: 13%
- Logistics: 13%
- Bank: 13%
- Transport: 5%
- Automotive: 5%
- Other: 5%
- Hospital: 3%
- Mass Media: 2%
- Industrial: Other
- Financial
- Telecom
- Transportation
- Healthcare
- IT

kaspersky
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

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files encrypted</td>
<td>32.7%</td>
</tr>
<tr>
<td>Suspicious file</td>
<td>19.1%</td>
</tr>
<tr>
<td>Suspicious network activity</td>
<td>17.7%</td>
</tr>
<tr>
<td>Suspicious endpoint activity</td>
<td>16.9%</td>
</tr>
<tr>
<td>Data leakage</td>
<td>6.4%</td>
</tr>
<tr>
<td>Suspicious e-mail message</td>
<td>4.5%</td>
</tr>
<tr>
<td>Money theft</td>
<td>1.8%</td>
</tr>
<tr>
<td>Account takeover</td>
<td>0.9%</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suspicious network activity</td>
<td>41.5%</td>
</tr>
<tr>
<td>Suspicious endpoint activity</td>
<td>33.4%</td>
</tr>
<tr>
<td>Suspicious file</td>
<td>33.4%</td>
</tr>
<tr>
<td>Data leakage</td>
<td>8.4%</td>
</tr>
</tbody>
</table>

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.

---

* 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 LOLBing), well-known offensive tools from GitHub (e.g., Mimikatz, AdFind, Masscan) and specialized commercial frameworks (Cobalt Strike).

Inside all incident cases with tools

<table>
<thead>
<tr>
<th>Frequent</th>
<th>Average</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-13%</td>
<td>4-8%</td>
<td>2-3%</td>
</tr>
<tr>
<td>Mimikatz, PowerExec, Advanced IP Scanner</td>
<td>Cobalt Strike, Process Hacker, ProcDump</td>
<td>TeamViewer, Impacket, WMIC, PowerTool, Nmap, fgdump, Masscan, CScript, NetScan, Winrar, AdFind, NBTScan, PuTTY, RDP</td>
</tr>
</tbody>
</table>

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

- **Execution**: Cobalt Strike, CScript, Impacket, PowerShell, PsExec
- **Defense evasion**: Process Hacker, PowerTool
- **Credential access**: fgdump, Mimikatz, PowerShell, ProcDump
- **Discovery**: AdFind, Advanced IP Scanner, Masscan, NBTScan, NetScan, Nmap, WMIC
- **Lateral movement**: Cobalt Strike, Impacket, PsExec
- **Collection**: Winrar
- **Command and control**: PuTTY, RDP, TeamViewer

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

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 NSZ7-010.

**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.WebUI
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. Handling 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.

<table>
<thead>
<tr>
<th>Rush</th>
<th>Average</th>
<th>Long lasting</th>
</tr>
</thead>
<tbody>
<tr>
<td>hours and days</td>
<td>weeks</td>
<td>months and longer</td>
</tr>
</tbody>
</table>

### Attack duration average

- 15 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)

- **Rush**
  - Brute force
  - Exploit public-facing application
  - Spearphishing link

- **Average**
  - Exploit public-facing application
  - Drive-by compromise
  - Brute force
  - Replication through removable media
  - Spearphishing link

- **Long lasting**
  - 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