The nature of cyber incidents

Based on cyberattack investigations conducted by Kaspersky Global Emergency Response Team
How attackers first gained access

Exploitation of public-facing applications
- 2019: 37.0%
- 2020: 31.5%
- 2021: 53.6%

Compromised accounts
- 2019: 13.0%
- 2020: 31.6%
- 2021: 17.9%

Malicious email
- 2019: 30.0%
- 2020: 23.7%
- 2021: 14.3%

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.

Attack impact

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.

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

Distribution of attacks by duration depending on the initial vector

<table>
<thead>
<tr>
<th>Initial attack vector</th>
<th>Hours</th>
<th>Weeks</th>
<th>Months</th>
<th>Grand Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exploitation of public-facing applications</td>
<td>12.5%</td>
<td>0.0%</td>
<td>25.0%</td>
<td>37.5%</td>
</tr>
<tr>
<td>Malicious email</td>
<td>0.0%</td>
<td>0.0%</td>
<td>25.0%</td>
<td>25.0%</td>
</tr>
<tr>
<td>Compromised accounts</td>
<td>12.5%</td>
<td>12.5%</td>
<td>12.5%</td>
<td>37.5%</td>
</tr>
<tr>
<td>Grand Total</td>
<td>25.0%</td>
<td>12.5%</td>
<td>62.5%</td>
<td>100%</td>
</tr>
</tbody>
</table>

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

And Experts’ Recommendations

Threat intelligence view

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

Initial attack vector

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

53.6% Exploitation of public-facing applications
14.3% Malicious email
17.9% Compromised accounts

Move around and get things done

In 39.7% of all cases, legitimate tools were used

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

Impact

16.0% Data leakage
51.9% Files encrypted
11.1% Active Directory compromised

Industries and regions, %

Security operations metrics view, %

Detection reason

Suspicious activity
Data leakage
Files encrypted
Malicious email
Money theft

Attack duration

- Hours
- Days
- Weeks
- Months
- Years

Detection before or after the impact

Pre-impact
Post-impact

Remediation duration

- Hours
- Days
- Weeks
- Months

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

In 2020, the COVID-19 pandemic forced companies to restructure their information security practices to accommodate remote working.

---

1. The analytics are based on commercial incident response cases performed by Kaspersky
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

- Data leakage: 5.1%
- Malicious email: 1.3%
- Files encrypted: 50.6%
- Money theft: 1.3%
- Suspicious activity: 41.7%

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 and NoRansom project.

False positives

- Security tool alert: 18.2%
- Suspicious email message: 9.1%
- Suspicious file: 9.1%
- Suspicious network activity: 27.3%
- Suspicious endpoint activity: 36.3%

12.9% of all incident response requests were for false alarms. Suspicious activity 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.

Reasons per region

- Africa: Data leakage 2.3%, Malicious email 9.3%, Files encrypted 25.0%, Money theft 100.0%
- APAC: Data leakage 2.5%, Malicious email 7.5%, Files encrypted 75.0%, Money theft 100.0%
- CIS: Data leakage 5.0%, Malicious email 15.0%, Files encrypted 20.0%, Money theft 25.0%
- EU: Data leakage 20.0%, Malicious email 10.0%, Files encrypted 25.0%, Money theft 10.0%
- LatAm: Data leakage 17.5%, Malicious email 25.0%, Files encrypted 25.0%, Money theft 27.5%
- ME: Data leakage 2.3%, Malicious email 9.3%, Files encrypted 25.0%, Money theft 17.5%
- NA: Data leakage 2.5%, Malicious email 12.5%, Files encrypted 75.0%, Money theft 100.0%

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

Reasons per industry

- Education: Data leakage 2.3%, Files encrypted 7.5%, Malicious email 5.0%
- Financial: Data leakage 18.6%, Files encrypted 25.0%, Malicious email 7.5%
- Government: Data leakage 25.6%, Files encrypted 15.0%
- Healthcare: Data leakage 2.3%, Files encrypted 27.9%
- Industrial: Data leakage 9.3%, Files encrypted 17.5%
- IT: Data leakage 2.3%, Files encrypted 2.5%
- Mass Media: Data leakage 2.3%, Files encrypted 2.5%
- Telecom: Data leakage 100.0%
- Transportation: Data leakage 12.5%
- Other: Data leakage 2.3%

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.
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 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.

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

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).

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

<table>
<thead>
<tr>
<th><strong>Frequent</strong></th>
<th>5–8%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cobalt Strike, Mimikatz, PowerShell, PsExec</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Average</strong></th>
<th>3–4%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced IP Scanner, Bitlocker, ProcDump, ProcessHacker</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Rare</strong></th>
<th>1–2%</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyDesk, DiskCryptor, Everything, Fast Reverse Proxy FRP, Meterpreter, reg.exe, RMS, SMBExec, WebBrowserPassView.exe</td>
<td></td>
</tr>
</tbody>
</table>

---

1. https://lolbas-project.github.io
2. Each tool was identified in 5–8% of incident cases
Exploit usage was identified in 14% of all incidents.

Microsoft Exchange CVE-2021-34523
Elevation of Privilege (EoP) vulnerability. The vulnerability allows attackers to raise their permissions. Part of the ProxyShell vulnerabilities chain.

Microsoft Exchange CVE-2021-26857
An insecure deserialization vulnerability in the Unified Messaging service in Microsoft Exchange Server. 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.

Microsoft Exchange CVE-2021-34473
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.

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.

Microsoft Exchange CVE-2021-31207
Security Feature Bypass vulnerability. The vulnerability allows attackers to bypass the authentication process. Part of the ProxyShell vulnerabilities chain.

Apache Solr CVE-2019-17558
Remote code execution vulnerability allows attackers to execute arbitrary code without authentication in Apache Solr through the VelocityResponseWriter.

Microsoft Exchange CVE-2021-34473
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.

Microsoft Exchange CVE-2021-26858
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.

Gigabyte Drivers CVE-2018-19320
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.

Fortinet FortiOS CVE-2018-13379
A path traversal vulnerability in the FortiOS SSL VPN web portal allows unauthenticated attackers to download system files via specially crafted HTTP resource requests.

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

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

- Rush: 52.7% (Hours and days)
- Average: 6.5% (Weeks)
- Long lasting: 17.2% (Months and longer)

Average attack duration

- Rush: 1 day
- Average: 14 days
- Long lasting: 94.5 days

Representative impact

- Ransomware
- Ransomware and money theft
- Data leakage and ransomware

Incident response duration

Time spent investigating

- Attacks that lasted up to a week: 29.4 hours
- Attacks that lasted up to a month: 48.3 hours
- Attacks that lasted more than a month: 60.13 hours

High-velocity ransomware attacks that present the biggest challenge even to mature security operations. Mostly noisy adversary behavior taking advantage of low hanging fruit - publicly available and easily identifiable security issues.

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 owing stages of the attack.

Uneven periods of active and passive phases during the attack.

The duration of active phases is very similar to the previous (Average) group.
Contacts

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

➢ For assistance with emergency cases:
  gert@kaspersky.com