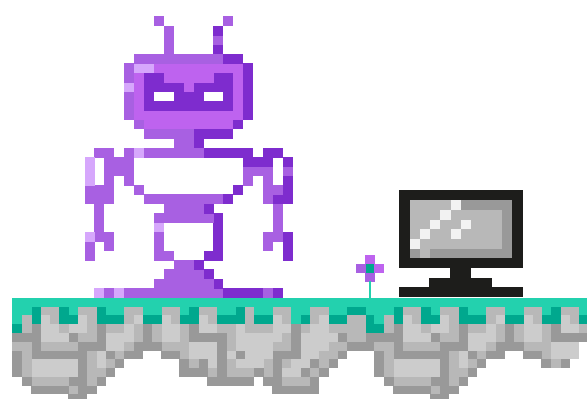
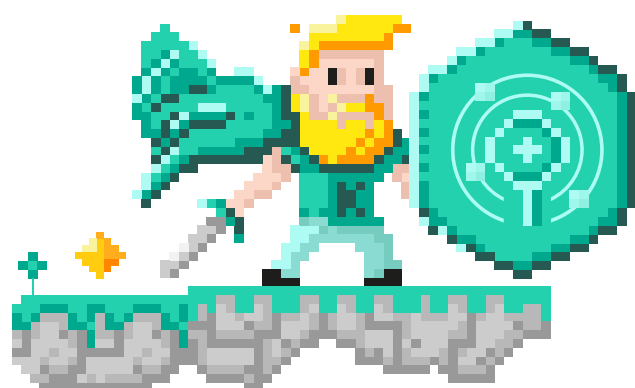


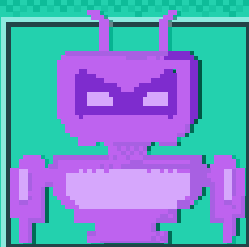
# Managed Detection and Response: Analyst Report

2021



## Executive

## summary



Managed Detection and Response

up to **2**

critical incident every day

**41** min

average detection time

**77**%

defeat rate from 1st try

Top target regions  
(% of clients)

47%

Europe

23%

CIS

16%

APAC

Top target Europe locations  
(% of clients)

30%

Italy

25%

Germany

11%

Austria

Top target facilities  
(% of clients)

17%

Factory

16%

Bank

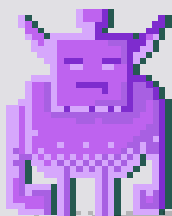
12%

Server center

## Favorite skins ▾

41%

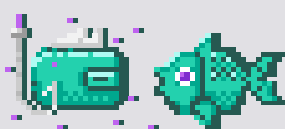
APT



## Favorite spells ▾

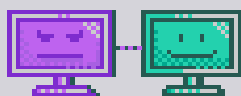
T1566:

Phishing



TA0001: Initial Access

T1210:

Exploitation  
of Remote  
Services

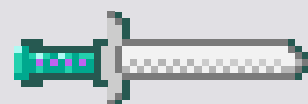
TA0008: Lateral Movement

T1204:

User  
Execution

TA0002: Execution

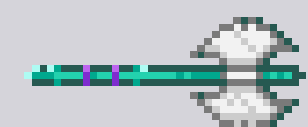
## Favorite tools ▾



powershell.exe



rundll32.exe



certutil.exe

## Incidents severity

14.3% High

65.4% Medium

20.3% Low



## Recommendations

- Year by year, the share of human-driven targeted attacks is increasing. To efficiently detect them, manual threat hunting in combination with classical alert-driven monitoring<sup>1</sup> should be implemented
- Red team exercises are similar to advanced attacks and are thus a good approach to assess an organization's security<sup>2</sup>
- More than 14% of high-severity incidents are related to malware that proves the need of comprehensive anti-malware protection<sup>3</sup>
- Focus on threat detection through all MITRE ATT&CK tactics<sup>4</sup>. Even complex attacks consist of simple steps, referred to as techniques, and detection of a single technique can reveal the whole attack

<sup>1</sup> <https://www.kaspersky.com/enterprise-security/managed-detection-and-response>

<sup>2</sup> <https://www.kaspersky.com/enterprise-security/security-assessment>

<sup>3</sup> <https://www.kaspersky.com/enterprise-security/wiki-section/products/multi-layered-approach-to-security>

<sup>4</sup> <https://attack.mitre.org/tactics/enterprise/>

# Introduction

## > About MDR

Kaspersky Managed Detection and Response (MDR) helps organizations to complement existing detection function or to expand limited in-house resources to protect their infrastructure from the growing number and complexity of threats in real time, 24/7. We collect telemetry from clients' networks and analyze it using machine learning and artificial intelligence technologies, and human threat hunting analysts.

Kaspersky SOC investigates the alerts and notify the client if there is something bad going on, providing response actions or recommendations.

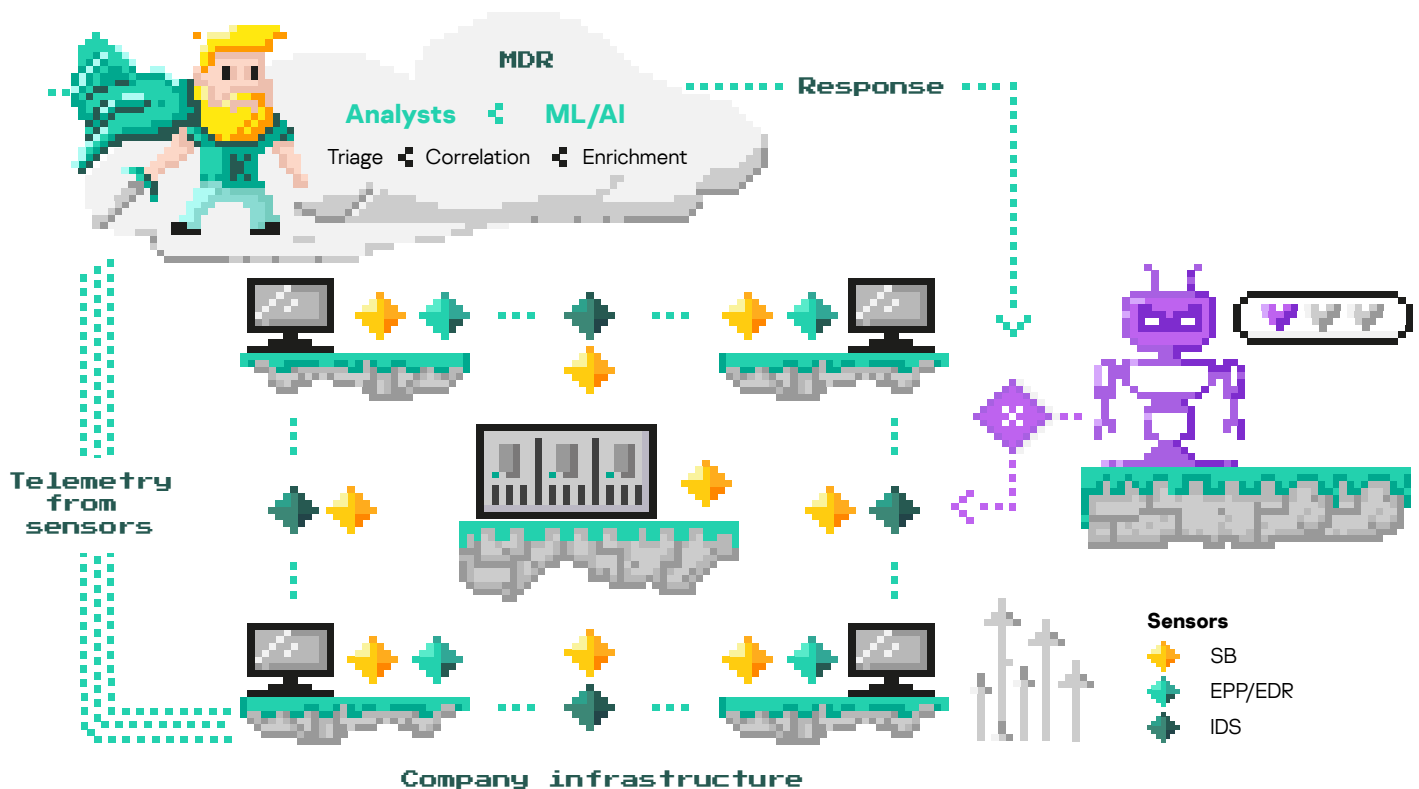
i

5/5

Overall Rating  
of Kaspersky

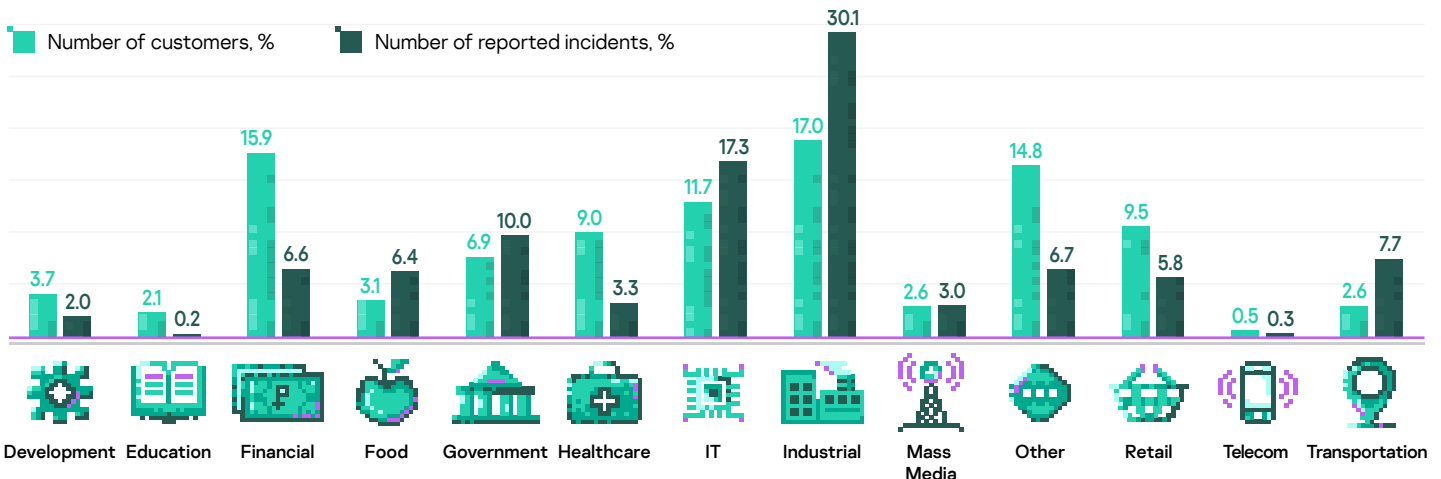
in the Managed Detection and Response Services

based on review ratings from real users/customers  
on Gartner Peer Insights<sup>1</sup> (as of 9th February 2022)



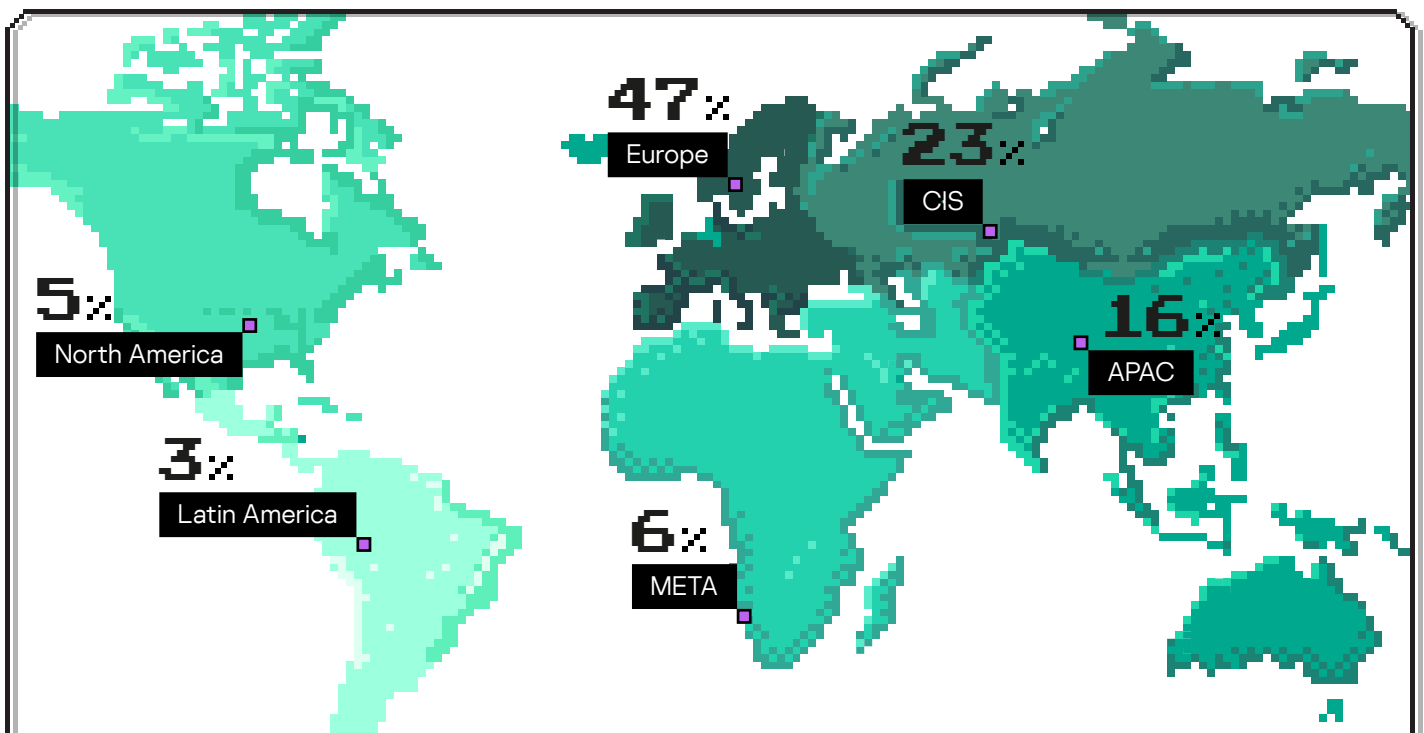
## > MDR service coverage: industries

Kaspersky MDR service in 2021 was used across different industries. Most of our customers are from industrial, financial or IT organizations.

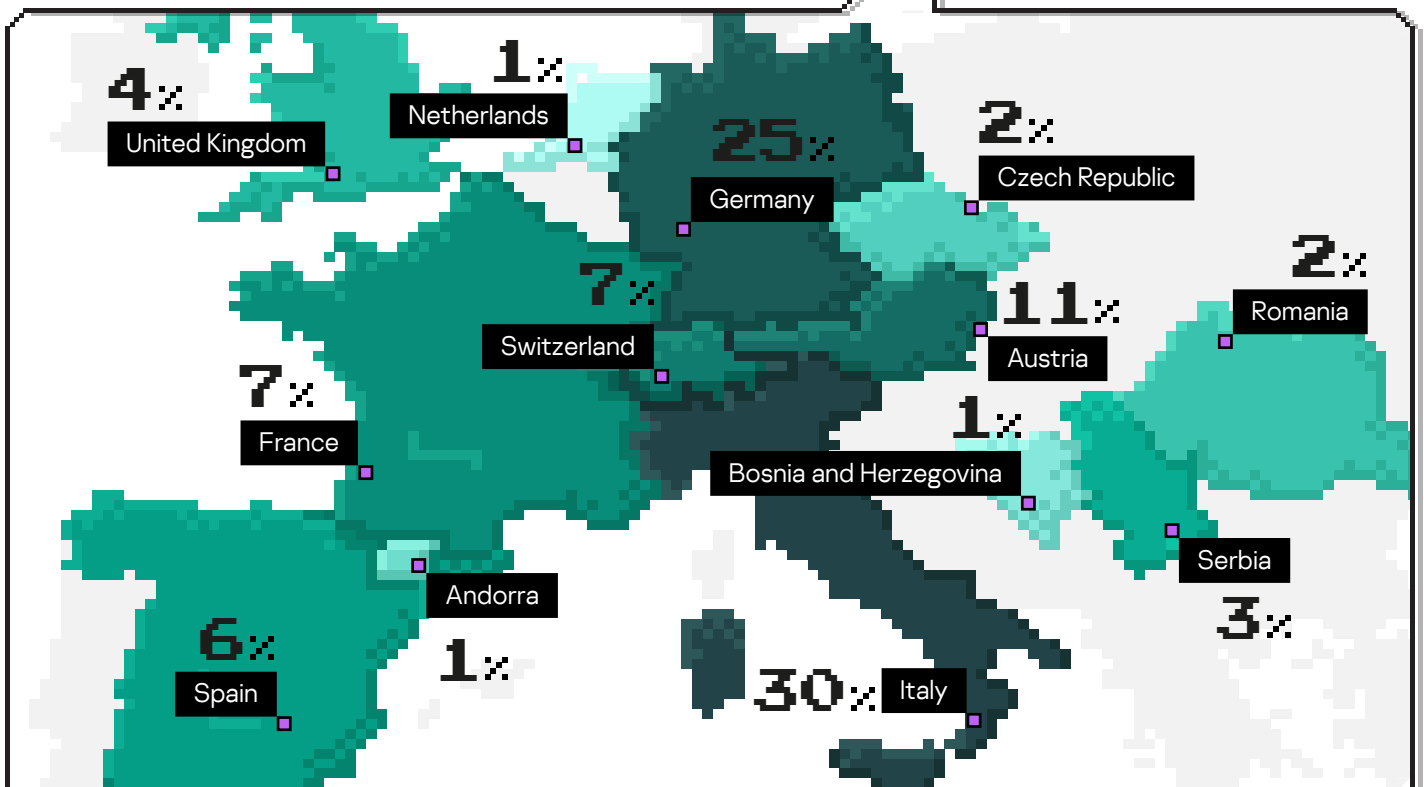


<sup>1</sup> [https://www.kaspersky.com/about/press-releases/2022\\_kaspersky-managed-detection-and-response-gets-highest-rating-in-gartner-peer-insightstm](https://www.kaspersky.com/about/press-releases/2022_kaspersky-managed-detection-and-response-gets-highest-rating-in-gartner-peer-insightstm)

## MDR coverage of regions



Accurate perception of the report in terms of threat intelligence requires us to disclose coverage of regions where we deliver the service: incident volumes, tactics and techniques do have geographical specifics.



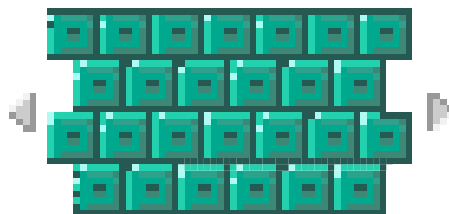
In Europe, the top countries where Kaspersky MDR is popular are Italy, Germany and Austria.

# MDR Daily Routine

In 2021, each day MDR received a huge amount of telemetry that was processed into alerts. 73.74% of received alerts were processed by SOC analysts and 6.67% were related to real incidents that were reported to customers via the MDR portal.

Daily events  
from one host

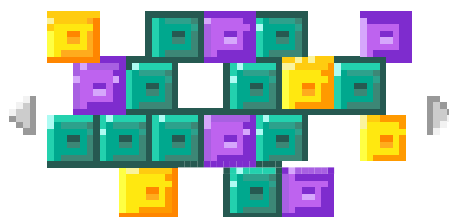
~15k



This number can vary significantly  
depending on the host activity

From which

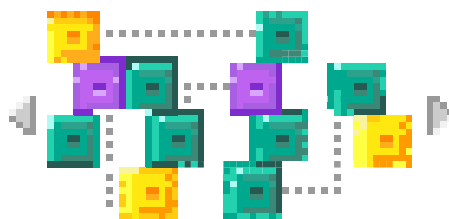
414k alerts  
were processed



150k+ alerts were processed  
automatically using AI technology  
264k+ were analyzed by SOC analysts

Resulting in

8,479  
incidents  
reported to customers



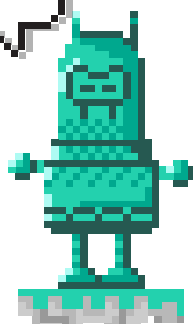
~18k alerts were related to security  
incidents, which was ~7% of the total

## > Incidents remediation effectiveness

### 1 alert

77.39% of all incidents are related to only one alert. That demonstrates a pretty high incident remediation efficiency. Also, typical incidents with well-defined playbooks<sup>1</sup> fall into this category. The share of High severity incidents here is the lowest – only 11.38%.

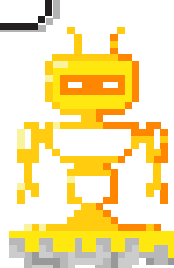
77.4%



### 2-4 alerts

17.13% of incidents are linked with 2-4 alerts. To prevent detect evasion we use completely different technologies for the same threat. Different technologies generate different alerts and this category demonstrates to us there is room for more comprehensive alerts processing.

17.1%



### 5+ alerts

Less than 5.48% of incidents are linked to 4 alerts or more. They are cases where remediation is not allowed or not efficient: new targeted attacks that require careful investigation before remediation, or the customer requested attack monitoring without response. The share of High severity incidents here is the biggest – more than 27% and for Low – only ~12%.

5.5%



<sup>1</sup> For example, incidents related to Accessibility Features(T1546.008), LSASS memory dump (T1003.001), Registry dump (T1003.004), Rootkit detection (T1014) Brute force (T1110) and many others

# Severity of incidents

In MDR, all incidents are actionable. That means we don't report incidents without a recommendation to prevent or decrease the probability of a possible impact.



## 14%

High severity incidents

human-driven attack  
or malware outbreak with huge impact

## 66%

Medium severity incidents

have no signs of human-driven activities,  
related to medium level of impact

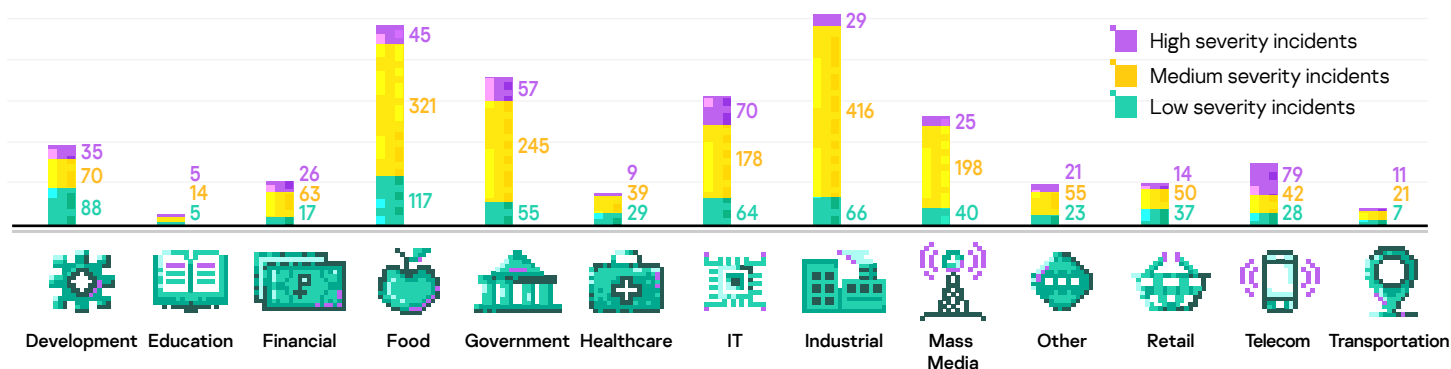
## 20%

Low severity incidents

without significant effect on corporate  
business processes, but still have actions  
that might be implemented to improve  
overall security posture

In 2021, we detected more than one High severity incident each day.

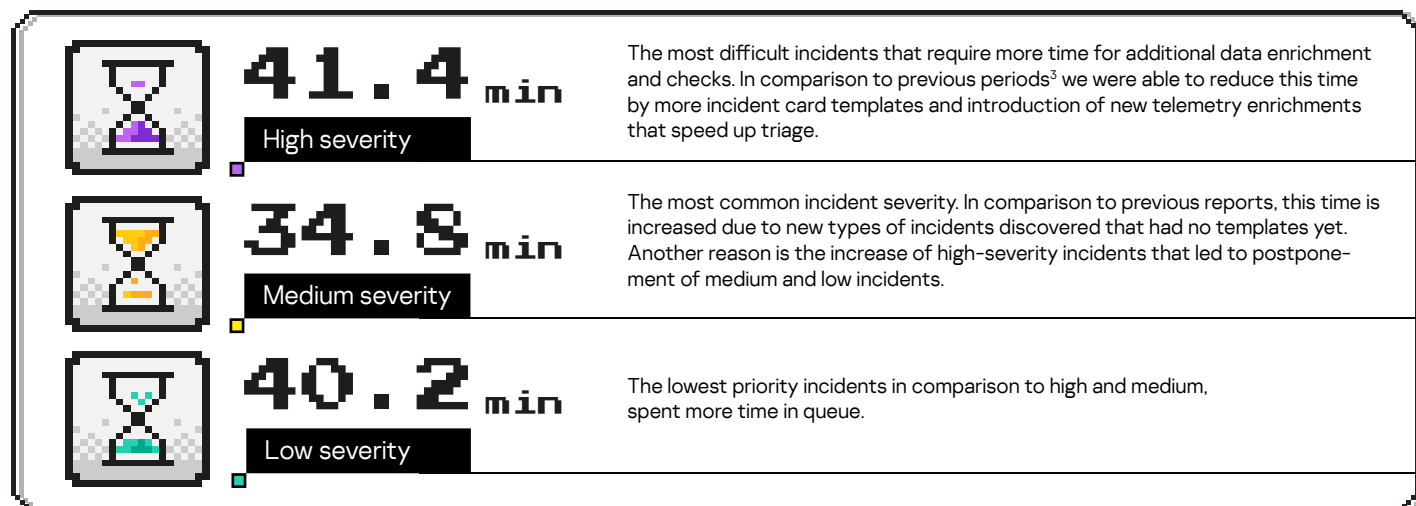
The diagram below reflects the number of incidents per 10k computers being monitored.



## > How long does it take to identify an incident?

The life of an alert related to suspicious activity starts in a queue assigned to SOC analyst who opens it in accordance with severity and time to SLA breach. If Alert data analysis shows that it's a FP<sup>1</sup>, it's ignored and custom and/or global filters<sup>2</sup> are created. Then, the alert is imported to a case.

After an investigation, the case can be either closed as a FP or reported as an incident via MDR portal along with recommended response actions. If the customer approves, endpoint agents will automatically fulfill them.



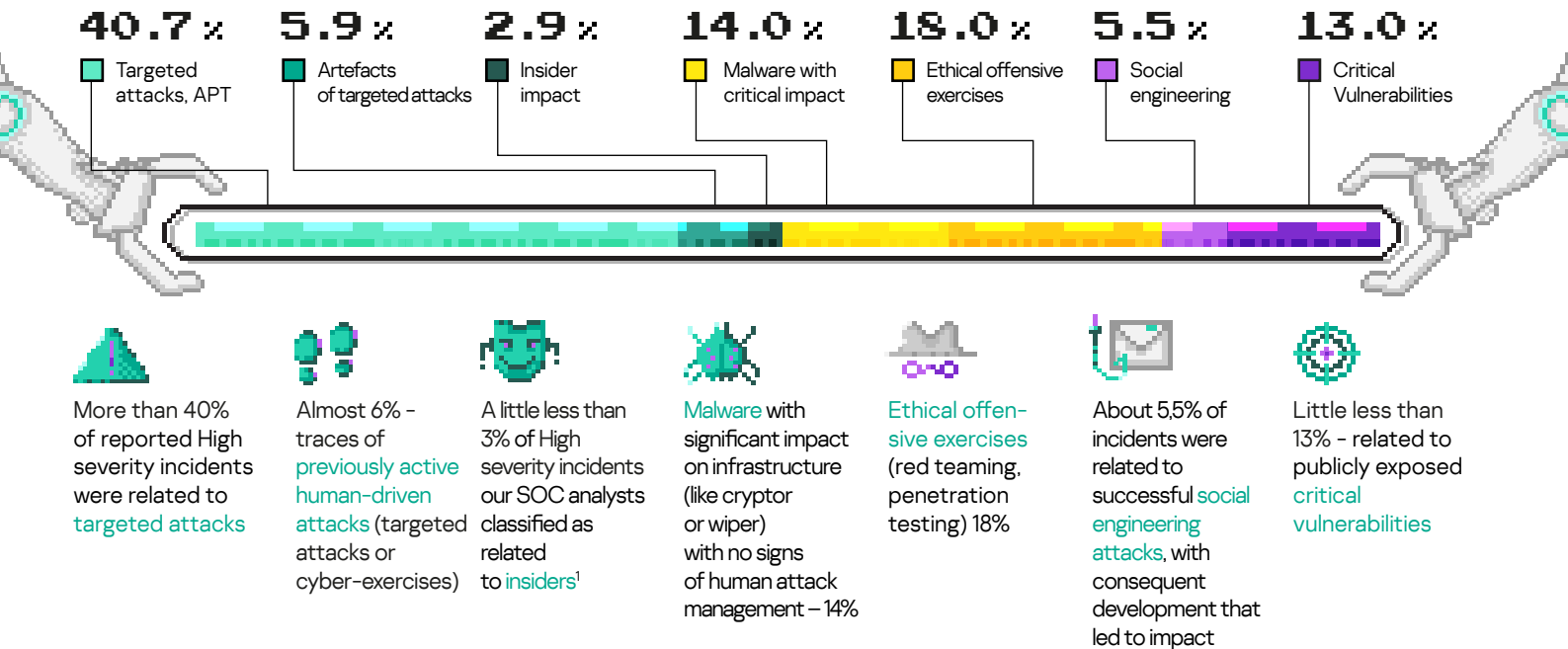
<sup>1</sup>There are two main types of FP: Infrastructural – the alert logic is OK, but due to customer's infrastructure peculiarities this is not actionable incident; Technological – the alert logic works wrong and should be fixed.

<sup>2</sup>Custom filter is adjustment of detection logic for particular customer infrastructure, – this sort of filters is created to fix Infrastructural FP. Global filter is detection logic adjustments in case of Technological FP.

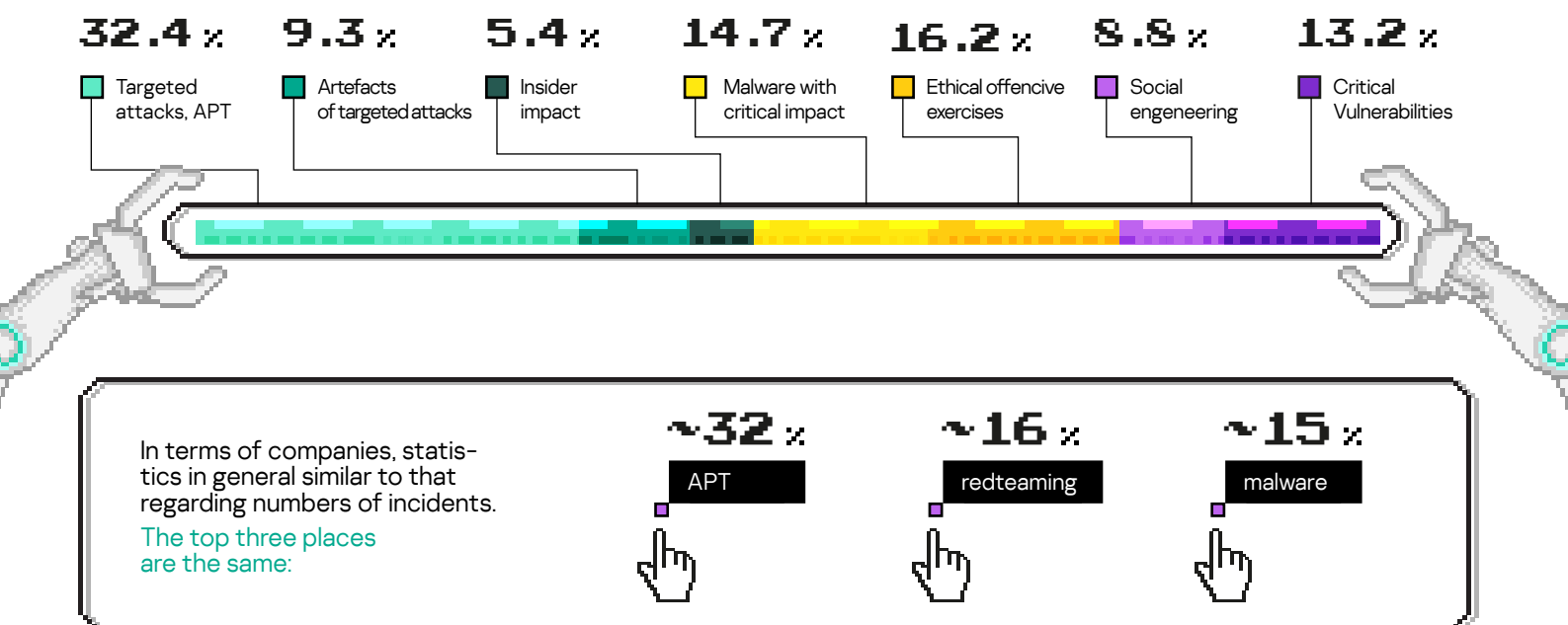
<sup>3</sup><https://securelist.com/managed-detection-and-response-in-q4-2020/103387/>

# The nature of High severity incidents

## > What are the causes of High severity incidents?



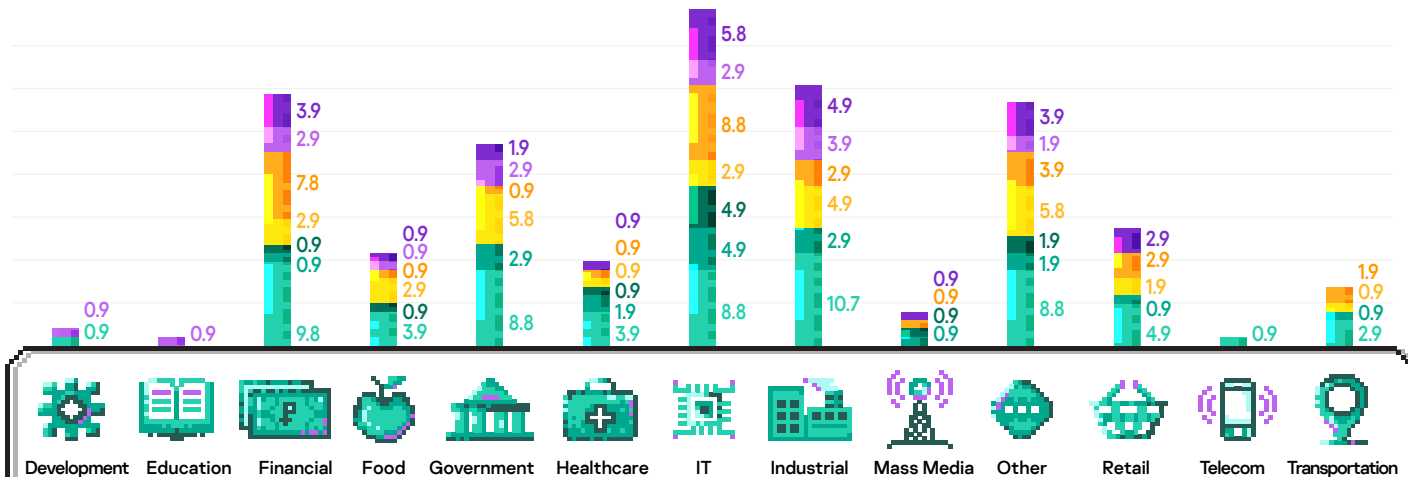
## > How many organizations experienced High severity incidents?



<sup>1</sup>In this type of incidents, we were not able to observe any signs of external attackers, but suspicious actions were done by legitimate privileged accounts. We asked customers if observed activities were legit or not, but did not receive any answer – that's why we have no reason to classify such cases as false positive (In reality it might be attempts to test MDR operational readiness, or really illegal activities from IT staff that customers preferred not to share with us)

# The nature of High severity incidents

## > Number of organizations with High severity incidents by industry, %

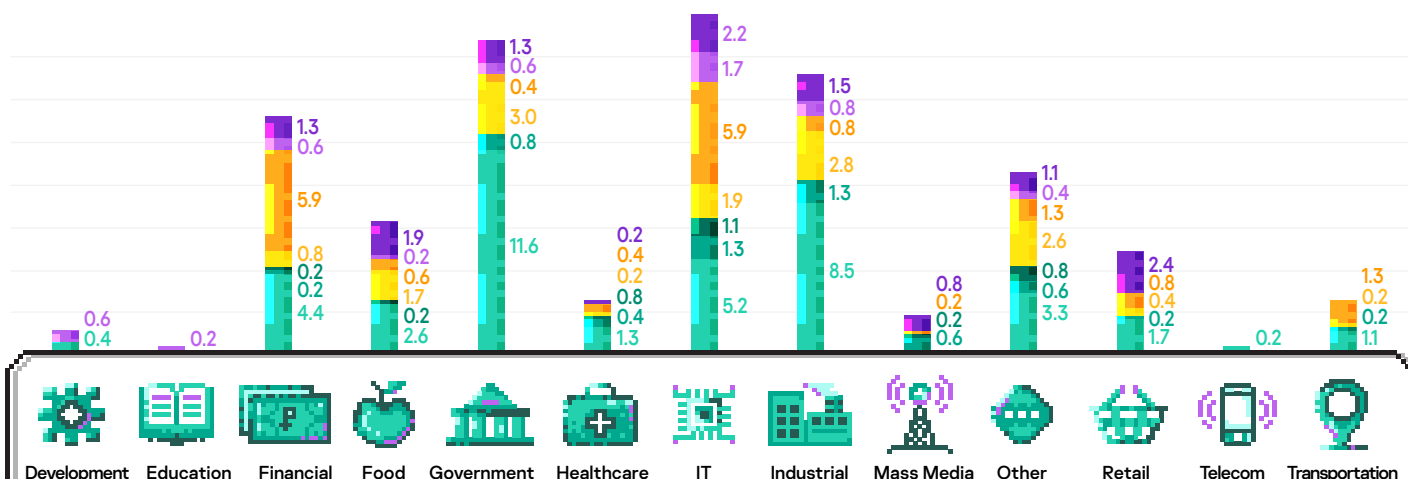


### The main findings from this statistic are:

- APTs were detected in each vertical except Education and Mass Media
- Mass Media was also compromised previously because there were reported incidents related to APT traces
- Most verticals experienced all types of High severity incidents
- In 2021 almost all verticals except Development, Education and Telecom practiced red team exercises
- Social engineering is still very efficient



## > Number of High severity incidents by industry, %



### This statistic shows that:

- The biggest numbers of APT-related incidents were detected in Government, Industrial, IT and Financial
- Financial and IT are in top by number of red teaming cases
- Development and Telecom experienced APTs but didn't conduct red teaming
- Successful social engineering and publicly faced vulnerabilities correlate to distribution of APT cases
- APT cases in general go hand in hand with cases related to traces of previous APT



# Detection technology and adversarial TTP

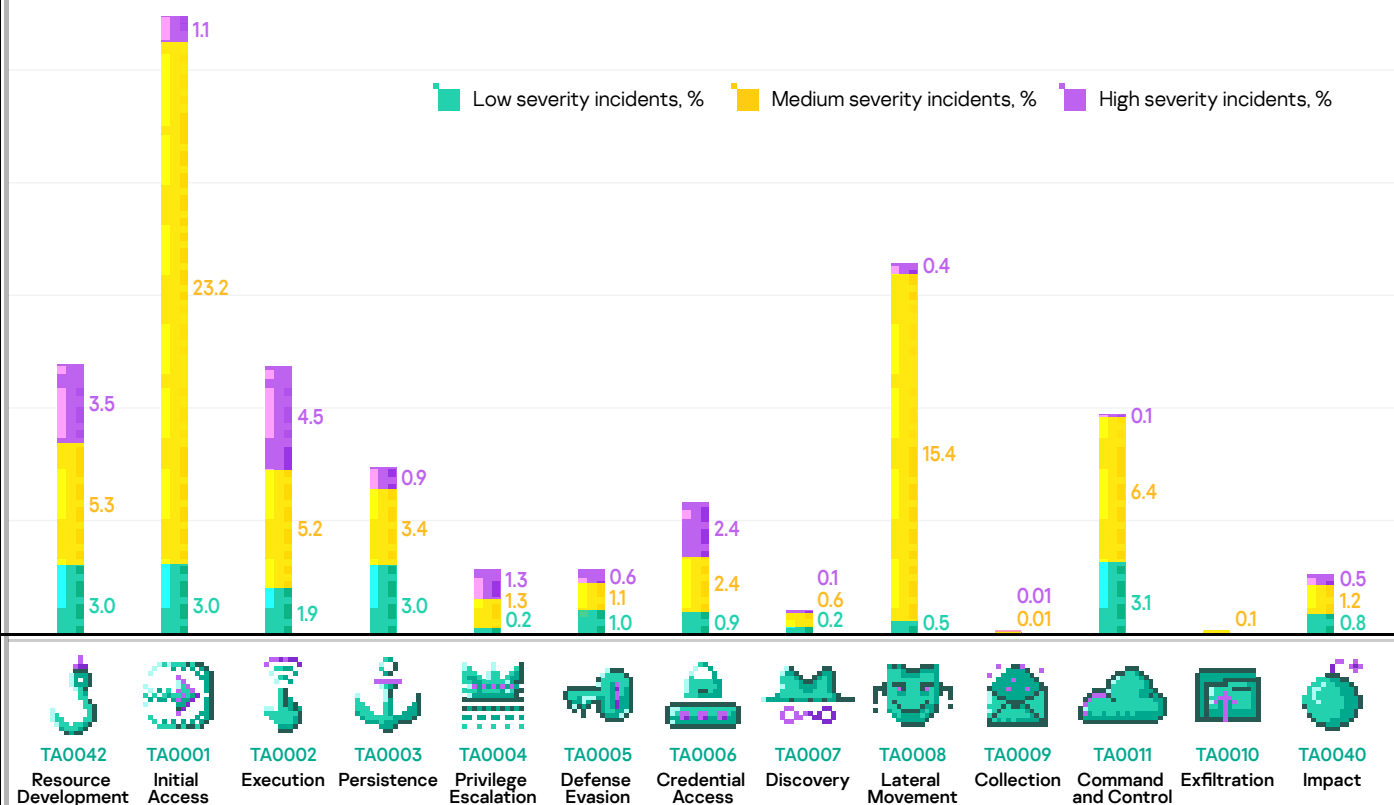
## > Adversarial tactics

MDR is capable of detecting Incidents at different stages of the attack kill chain. Usually, an incident is observed in different stages (MITRE ATT&CK tactics), but in the diagram below we count the earliest tactic for an incident. ...I

[More](#)

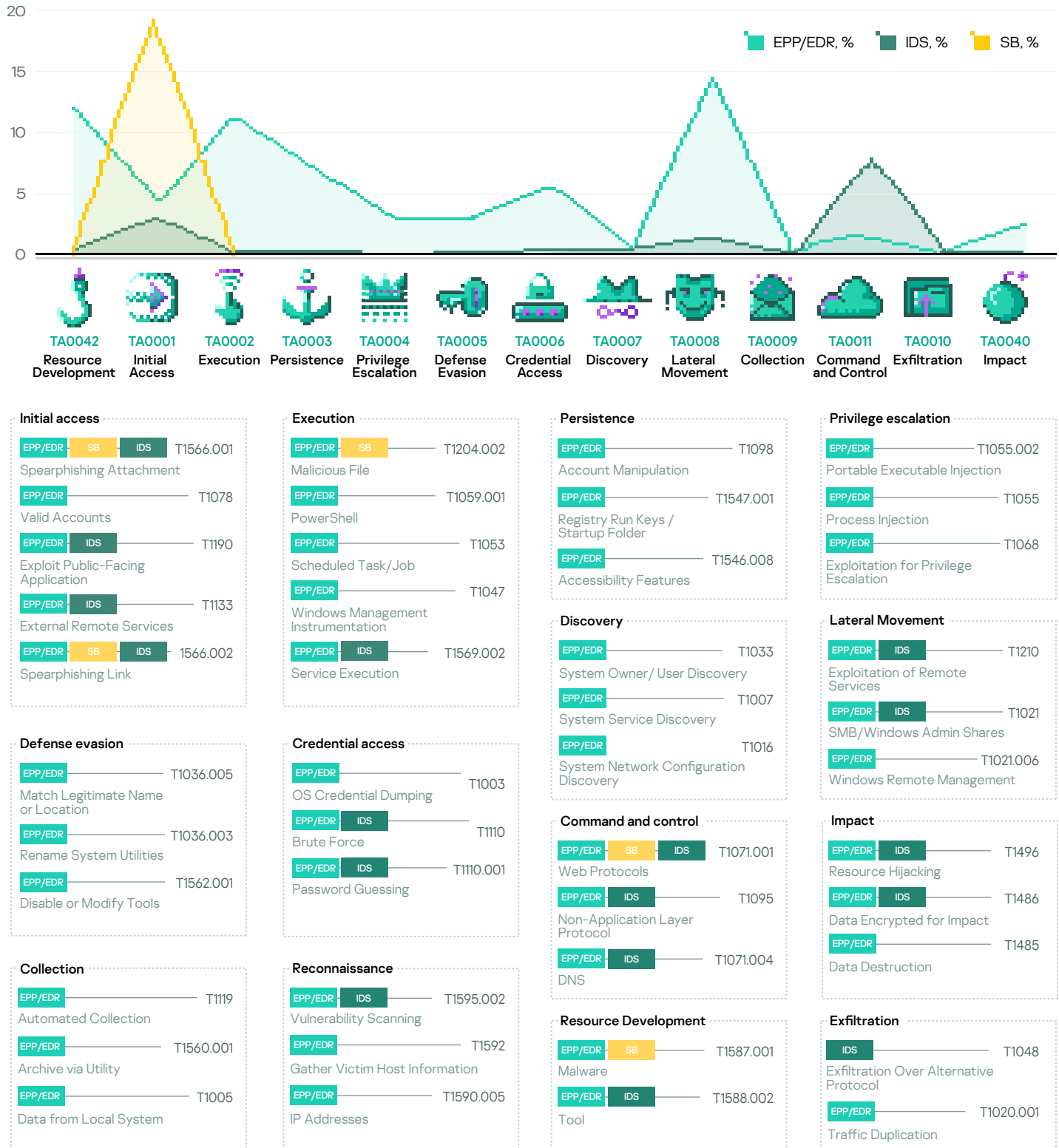
### Top tactics where we detect incidents are:

- **Initial Access** mainly covered by Kaspersky Anti-Targeted Attack platform on the perimeter detecting phishing and social engineering that are still very popular
- **Resource Development** might sound strange, but it's related to many incidents like 'suspicious file' where a potentially offensive tool was observed without any signs of execution. Often it's related to red teaming, but sometimes it's linked to real attacker's foothold
- Detection at the **Execution** stage is very similar to previous, but we observed tool execution. Execution is always noisy if comprehensive EPP is a part of the detection pipeline and thus the most High severity incidents were detected here. This fact shows that tool-based detection is still pretty efficient because most actors use off-the-shelf attack frameworks
- **Lateral Movement** is usually pretty noisy as well, but is related to fewer high-severity incidents detected here
- **Command and Control** is also common, but for Low and Medium severity incidents
- Not many incidents were detected at the **Impact** stage because usually it might be too late
- Very few incidents are detected at the **Discovery** tactic. This is due to difficulty of creating detections with a reasonable number of FP
- More efficient detections are on **Credential access**, **Persistence** and **Privilege Escalation** that in practice have a lower false positive rate. Also, attempts to **evade defense** often lead to successful detection



# Tactics and Detection technology

In MDR we analyze telemetry from different types of sensors: Endpoint (EPP/EDR), Network Intrusion Detection System (IDS) and Sandbox (SB). Network IDS and sandbox are parts of Kaspersky Anti-Targeted attack platform (KATA). The percentage of incidents detected by different types of sensors is provided in the diagram below.

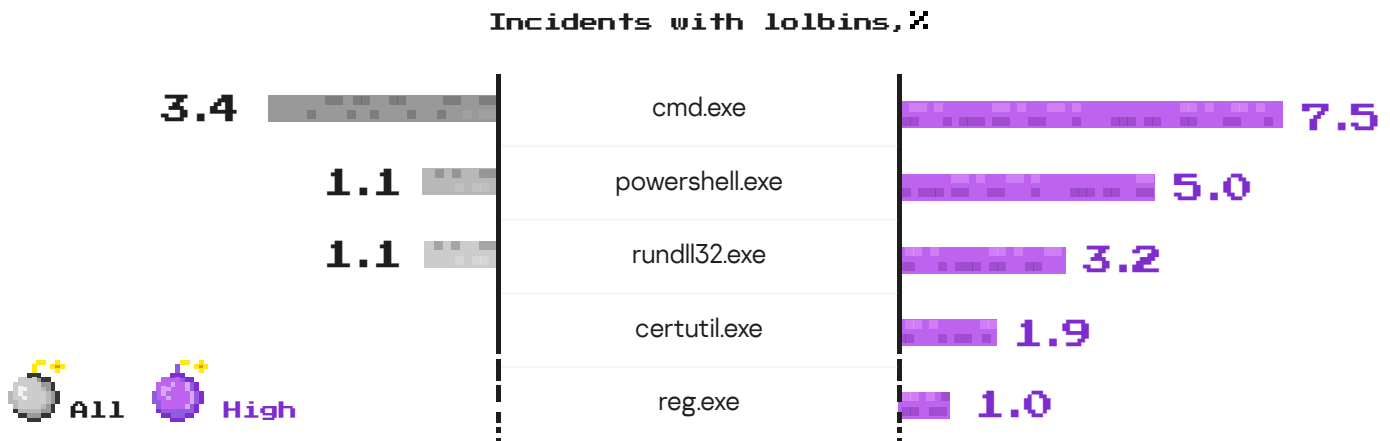


The high efficiency of sandbox and network IDS on **Initial Access** tactic is due to common use of KATA that detects phishing attacks. Also there are many Network IDS detects on **Lateral Movement** stage, and on **Command and Control** it's practically irreplaceable. For **Execution**, **Persistence**, **Privilege Escalation**, **Defense Evasion**, **Credential Access** and **Impact** tactics, the endpoint sensor is the main contributor. It is interesting to note that the **Lateral Movement** tactic is also well covered by endpoint.

# Adversarial techniques

## > Tools used in incidents

👉 Adversaries use built-in OS tools to minimize their chances of being detected during instruments delivery.

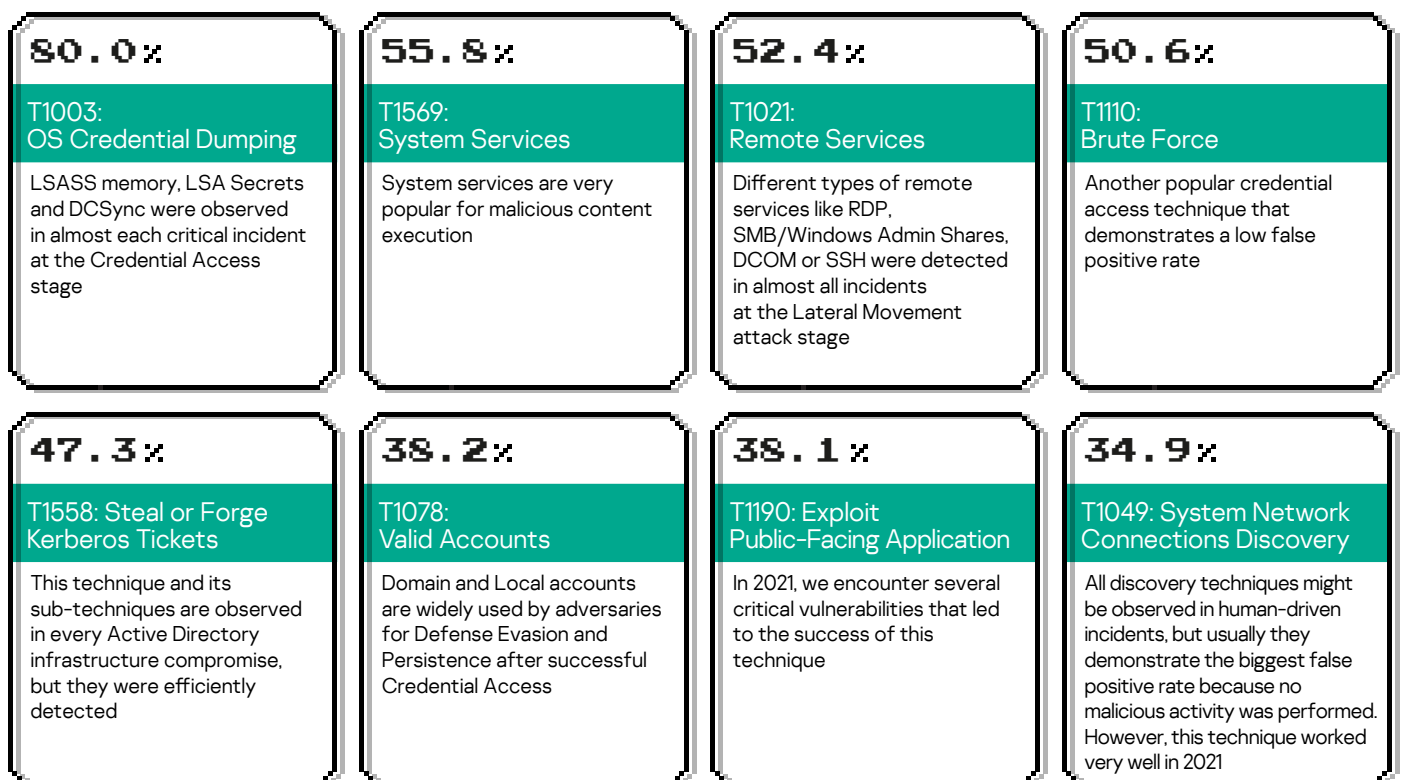


The most popular LOL-binaries<sup>1</sup> that are observed almost in any incident are cmd.exe and powershell.exe. rundll32.exe is also pretty popular among incidents of all severities.

High-severity incidents are distinguished by a wide variety of LOL tools used. In addition to aforementioned tools, in high-severity incidents reg.exe, te.exe and certutil.exe are also pretty popular.

## > Incident mapping to MITRE ATT&CK

👉 Our detection logic is mapped to MITRE ATT&CK techniques. For each detect, we calculate conversion and contribution and that's why we can share them for techniques. Below, eight techniques that showed the highest conversion are listed and the following heatmap demonstrates techniques contribution<sup>2</sup>.



<sup>1</sup><https://lolbas-project.github.io/>

<sup>2</sup> Conversion – the ratio of alerts classified as incidents to the total number of alerts based on particular technique.

Contribution – the ratio of incidents based on particular technique to the total number of incidents.

<0,5%
  <5%
  <10%
  <20%

| TA0043:<br>Reconnaissance                   | TA0042:<br>Resource<br>Development      | TA0001:<br>Initial<br>Access                     | TA0002:<br>Execution                            | TA0003:<br>Persistence  | TA0004:<br>Privilege<br>Escalation                 | TA0005:<br>Defense<br>Evasion   |
|---|---|--|---|---|--|---|
| T1590.005:<br>IP Addresses                  | T1583.005:<br>Botnet                    | T1078:<br>Valid Accounts                         | T1047: Windows<br>Management<br>Instrumentation | T1037: Boot<br>or Logon<br>Initialization Scripts                         | T1055: Process<br>Injection                        | T1014: Rootkit  |
| T1592: Gather<br>Victim Host<br>Information | T1583.006:<br>Web Services              | T1091: Replication<br>Through Removable<br>Media | T1053.005:<br>Scheduled Task                    | T1098: Account<br>Manipulation  | T1068: Exploitation<br>for Privilege<br>Escalation | T1027: Obfuscated<br>Files or Information                               |
| T1595:<br>Active Scanning                   | T1587.001:<br>Malware                   | T1133: External<br>Remote Services               | T1053:<br>Scheduled<br>Task/Job                 | T1136: Create<br>Account  | T1134: Access<br>Token Manipulation                | T1036: Masquerading   |
| T1598.003:<br>Spearphishing Link            | T1588.001:<br>Malware                   | T1189: Drive-by<br>Compromise                    | T1059: Command<br>and Scripting<br>Interpreter  | T1137: Office<br>Application Startup                                      | T1548.002:<br>Bypass User<br>Account Control       | T1070: Indicator<br>Removal on Host                                     |
|   | T1588.002:<br>Tool                      | T1190: Exploit<br>Public-Facing<br>Application   | T1064: Scripting                                | T1176: Browser<br>Extensions  |  | T1112: Modify<br>Registry   |
|   | T1588.003: Code<br>Signing Certificates | T1195: Supply<br>Chain Compromise                | T1106: Native API                               | T1197: BITS Jobs  |  | T1127.001: MSBuild  |
|   | T1588.005:<br>Exploits                  | T1566.001:<br>Spearphishing<br>Attachment        | T1129: Shared<br>Modules                        | T1205.001: Port<br>Knocking   |  | T1140: Deobfuscate/<br>Decode Files<br>or Information                   |
|   | T1588.006:<br>Vulnerabilities           | T1566.002:<br>Spearphishing Link                 | T1203: Exploitation<br>for Client Execution     | T1505.003:<br>Web Shell   |  | T1202: Indirect<br>Command Execution                                    |
|   | T1608.002:<br>Upload Tool               |  | T1204: User<br>Execution                        | T1542:<br>Pre-OS Boot   |  | T1207: Rogue<br>Domain Controller                                       |
|   |   |  | T1569: System<br>Services                       | T1543: Create<br>or Modify System<br>Process                              |  | T1211: Exploitation<br>for Defense Evasion                              |
|   |   |  |   | T1546.002:<br>Screensaver   |  | T1218: Signed Binary<br>Proxy Execution                                 |
|   |   |  |   | T1546.003: Windows<br>Management<br>Instrumentation<br>Event Subscription |  | T1220: XSL<br>Script Processing   |
|   |   |  |   | T1546.007:<br>Netsh Helper DLL  |  | T1222.001: Windows<br>File and Directory<br>Permissions<br>Modification |
|   |   |  |   | T1546.008:<br>Accessibility<br>Features                                   |  | T1497: Virtualization/<br>Sandbox Evasion                               |
|   |   |  |   | T1546.010:<br>Applnit DLLs  |  | T1550.002:<br>Pass the Hash   |
|   |   |  |   | T1546.012: Image<br>File Execution<br>Options Injection                   |  | T1550.003:<br>Pass the Ticket   |
|   |   |  |   | T1546.015:<br>Component Object<br>Model Hijacking                         |  | T1553.002:<br>Code Signing  |
|   |   |  |   | T1547: Boot<br>or Logon Autostart<br>Execution                            |  | T1553.004:<br>Install Root<br>Certificate                               |
|   |   |  |   | T1554: Compromise<br>Client Software<br>Binary                            |  | T1562.001:<br>Disable or Modify<br>Tools                                |
|   |   |  |   | T1556.002:<br>Password Filter DLL   |  | T1564.001:<br>Hidden Files<br>and Directories                           |
|   |   |  |   | T1574.002:<br>DLL Side-Loading  |  | T1564.002:<br>Hidden Users  |
|   |   |  |   |   |  | T1564.004:<br>NTFS File<br>Attributes                                   |

<0,5%
  <5%
  <10%
  <20%

| TA0006:<br>Credential<br>Access           | TA0007:<br>Discovery                          | TA0008:<br>Lateral<br>Movement         | TA0009:<br>Collection          | TA0011:<br>Command<br>and Control       | TA0010:<br>Exfiltration                       | TA0040:<br>Impact                |
|---|---|--|--------------------------------|---|---|----------------------------------|
| T1003: OS Credential Dumping              | T1007: System Service Discovery               | T1021: Remote Services                 | T1005: Data from Local System  | T1001: Data Obfuscation                 | T1020.001: Traffic Duplication                | T1485: Data Destruction          |
| T1040: Network Sniffing                   | T1012: Query Registry                         | T1210: Exploitation of Remote Services | T1113: Screen Capture          | T1071: Application Layer Protocol       | T1048: Exfiltration Over Alternative Protocol | T1486: Data Encrypted for Impact |
| T1056: Input Capture                      | T1016: System Network Configuration Discovery | T1570: Lateral Tool Transfer           | T1119: Automated Collection    | T1090: Proxy                            | T1052: Exfiltration Over Physical Medium      | T1496: Resource Hijacking        |
| T1110: Brute Force                        | T1018: Remote System Discovery                |  | T1560.001: Archive via Utility | T1095: Non-Application Layer Protocol   |   | T1561.001: Disk Content Wipe     |
| T1212: Exploitation for Credential Access | T1033: System Owner/User Discovery            |  |                                | T1102: Web Service                      |   | T1561.002: Disk Structure Wipe   |
| T1555: Credentials from Password Stores   | T1046: Network Service Scanning               |  |                                | T1104: Multi-Stage Channels             |   | T1565: Data Manipulation         |
| T1558: Steal or Forge Kerberos Tickets    | T1049: System Network Connections Discovery   |  |                                | T1105: Ingress Tool Transfer            |   |                                  |
|   | T1069: Permission Groups Discovery            |  |                                | T1219: Remote Access Software           |   |                                  |
|   | T1082: System Information Discovery           |  |                                | T1568.002: Domain Generation Algorithms |   |                                  |
|   | T1083: File and Directory Discovery           |  |                                | T1571: Non-Standard Port                |   |                                  |
|   | T1087: Account Discovery                      |  |                                | T1572: Protocol Tunneling               |   |                                  |
|   | T1124: System Time Discovery                  |  |                                |   |   |                                  |
|   | T1135: Network Share Discovery                |  |                                |   |   |                                  |
|   | T1482: Domain Trust Discovery                 |  |                                |   |   |                                  |
|   | T1518.001: Security Software Discovery        |  |                                |   |   |                                  |