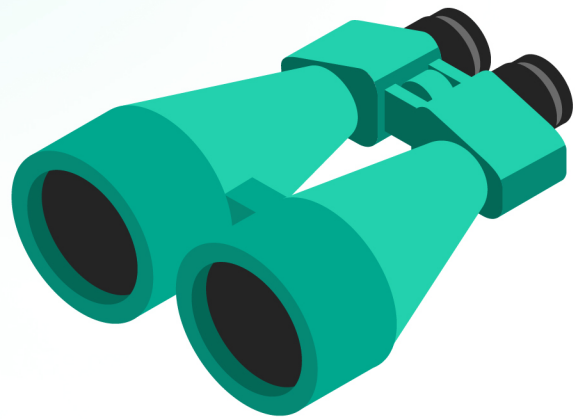


Managed Detection and Response: Analyst Report

Q4 2020



Executive summary



* Critical - high-severity incidents related to human-driven attacks that represent 9% of all identified incidents

Recommendations

- One third of all high severity incidents were human-driven targeted attacks. To fully detect them, automated tools are not enough and manual threat hunting, in combination with classical alert-driven monitoring¹, should be implemented.
- Professional red team exercises² are very similar to advanced attacks and are thus a good approach to assess an organization's operational efficiency.
- Nine percent of the reported high severity incidents were successful social engineering attacks demonstrating the need for employee security awareness³.
- Be ready to detect threats from all tactics (attack kill chain phases). Even complex attacks consist of simple steps, referred to as techniques, and detection of a particular technique can reveal the whole attack.
- Different detection technologies are efficient for different attacker techniques. Maintain a variety of security technologies⁴ to increase the chances of detection.

¹www.kaspersky.com/enterprise-security/managed-detection-and-response

²www.kaspersky.com/enterprise-security/security-assessment

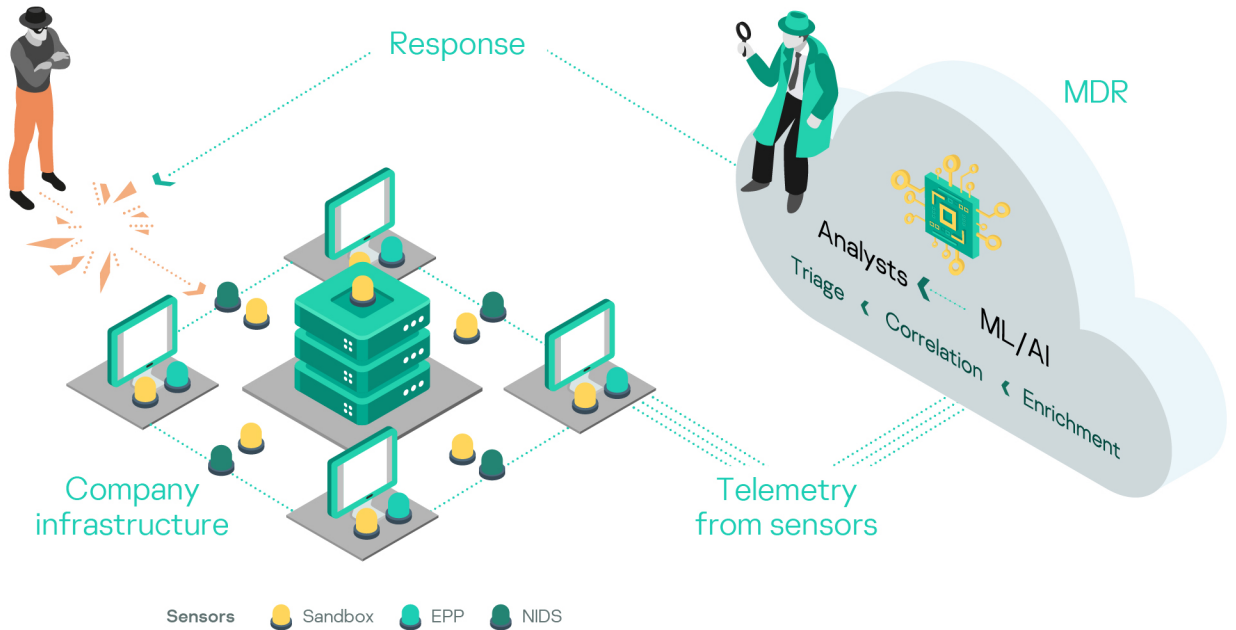
³www.kaspersky.com/enterprise-security/security-awareness

⁴www.kaspersky.com/enterprise-security/wiki-section/products/multi-layered-approach-to-security

Introduction

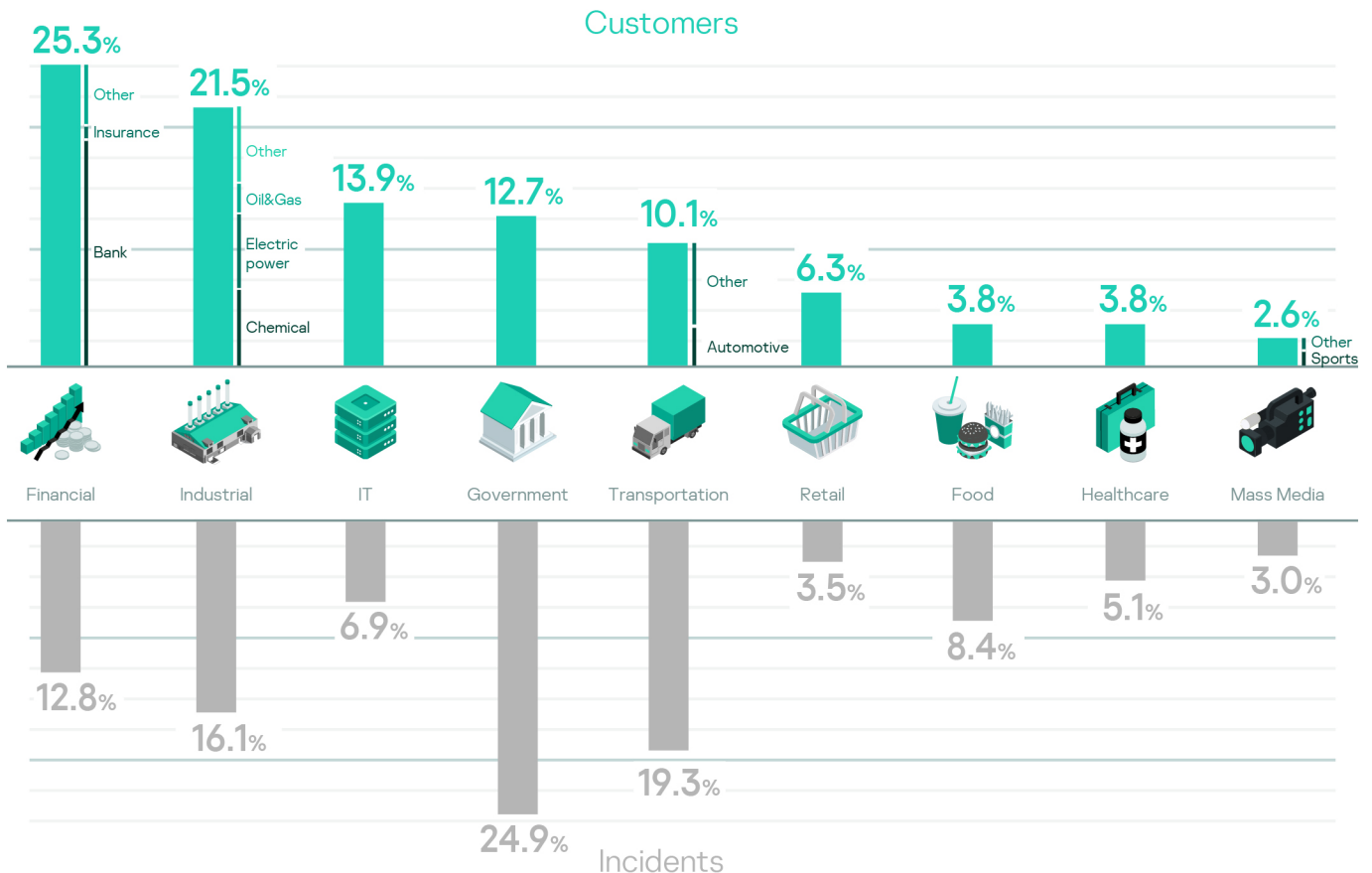
As cyberattacks become more sophisticated, and security solutions require more resources to analyze the huge amount of data gathered every day, many organizations feel the need for advanced security services that can deal with this growing complexity in real time, 24/7.

According to the estimation made in 2020 Gartner MDR Services Market Guide, "by 2025, 50% of organizations will be using Managed Detection and Response services for threat monitoring, detection and response functions that offer threat containment capabilities".



MDR service coverage: industries and verticals

Our MDR service is used across all industry verticals as shown further along with number of detected incidents. All data in the report is presented for 2020 Q4¹.

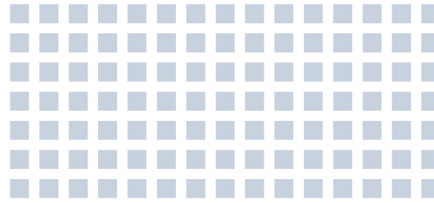


¹The report is based on anonymized metadata voluntarily provided by customers since Q4 2020 when the service was available in selected markets. It was launched globally in Q1 2021

MDR Daily Routine

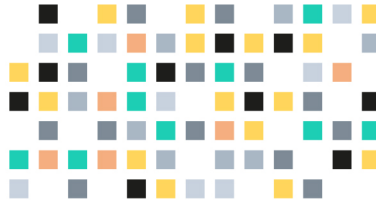
MDR service takes huge amount of raw telemetry from sensors, filters and enriches those events into alerts for threat hunters to produce incidents in a form to facilitate faster response times from human and useful reuse in other security toolstacks.

Daily events from one host
~15K



This value can significantly fluctuate depending on host activity

From which
65K alerts
were processed
for 3 months from all sensors



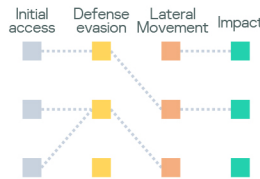
Manually triaged 43K enriched alerts and 22K with the help of [AI/ML](#)

Resulting in
1,506 incidents
reported to customers



- Alerts, related to reported incidents: 2,566
- Conversion from alerts to incidents is 5.9%, thus 94.1% were false positives

92.9%
enriched with ATT&CK



- 1,400 incidents can be mapped to MITRE ATT&CK
- Other incidents may include visibility incidents or low severity incidents without any need to fit the framework

Incident remediation effectiveness

How many alerts were required to remediate an incident?

1 alert
for 80.1% of incidents

Shows the overall effectiveness of incident detection and remediation

80.1%



1 alert

2-4 alerts
for 15.3% of incidents

Shows where adjustments to the incident detection and remediation process may be required. All these cases are subject to new detection logic creation, which then moves them to one-alert-detection statistics

15.3%



2-4 alerts

5 and more alerts
for 4.6% of incidents

Incidents with a large number of alerts are connected to cases where fast remediation is not allowed or not efficient:

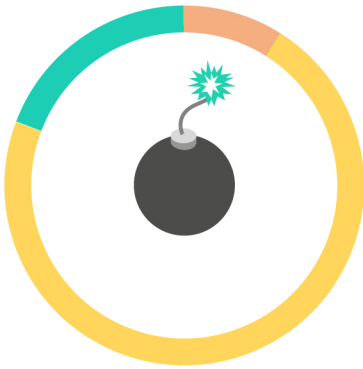
- New targeted attack/APT discovered
- Customer-requested attack monitoring without response
- Non-response security assessments (e.g., penetration testing)

4.6%



5 and more alerts

Severity of incidents



9% high severity incidents

Cause major disruption or unauthorized access to the customer's assets covered by MDR. Identified traces of a targeted attack or unknown threat, requiring further investigation using digital forensics

72% medium severity incidents

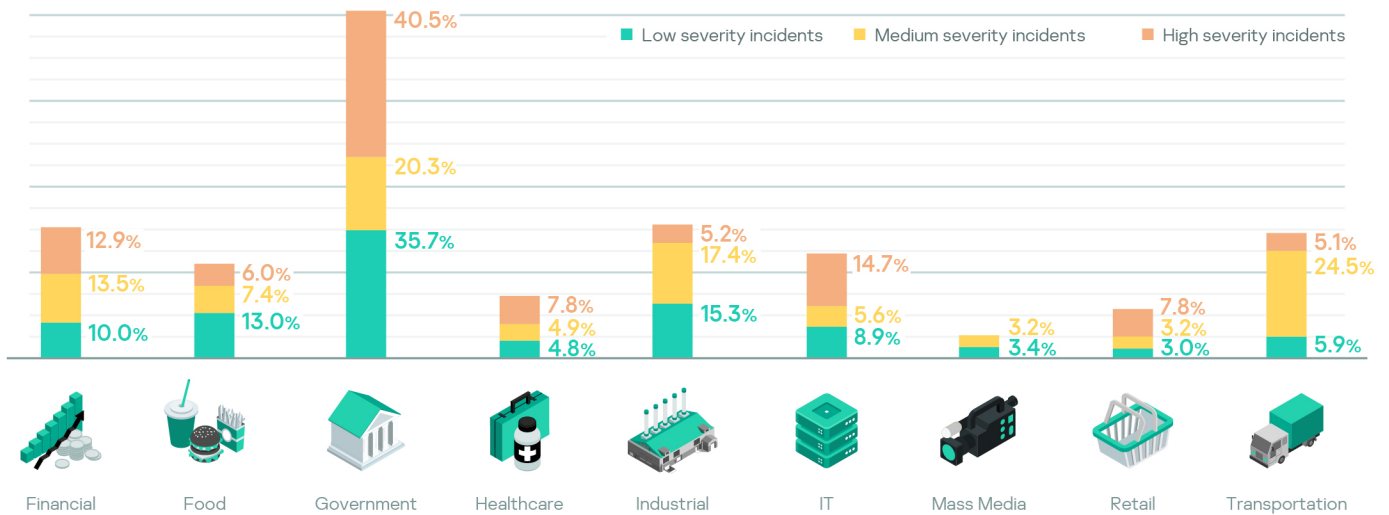
Affect the efficiency or performance of the customer's assets covered by MDR or lead to single cases of data corruption.

19% low severity incidents

Without significant affect the efficiency or performance of the customer's assets covered by MDR and would be unlikely to lead to data corruption.

Identified potential unwanted software – adware, riskware, not-a-virus, etc.

Each day we identified 1-2 high level incidents. Only customers from the Mass Media and Transportation sectors saw no high severity incidents in Q4 2020. Government, Financial and the IT industry constantly faced the biggest challenges in this quarter.



How long does it take to identify an incident?

The life of an alert related to a suspicious event starts in the queue where it waits to be triaged by a human analyst (AI/ML-based alerts - ~33% - are processed in seconds and not presented here). All triaged alerts are converted to incident cases, then

investigated by an analyst and finally an incident card is created and reported to the customer. We share the timeframes for the full processing of alerts (including waiting in the queue) up to the incident report.



52.6 min high severity

The most sensitive incidents requiring additional enrichment and hunting time

21.1 min medium severity






Volume-wise this is the most common incident severity. The fastest time shows the efficiency of templating the most common incident cards

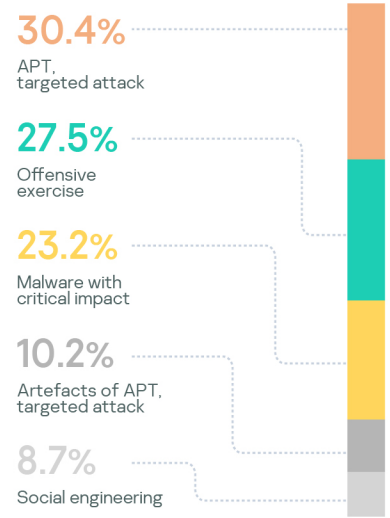
30.2 min low severity

The lowest priority of those incidents means they spend most of the time in the queue for analyst processing

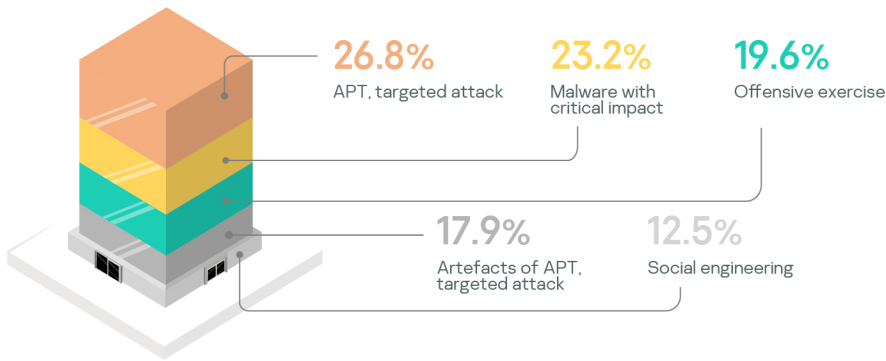
The nature of high severity incidents

What are the causes of high severity incidents?

-  One third (30.4%) of all high severity incidents were targeted attacks or [APTs](#)
-  Every 4th high severity incident was related to a human-driven offensive exercise (penetration testing, red teaming, adversary emulation, etc.)
-  Every 5th incident was a malware outbreak like [ransomware](#) (e.g. [WannaCry](#)) with a significant impact, but not human-driven
-  10% were unclassified incidents with definite signs of a previous attack or offensive exercise (e.g. Lsass dump, kirbi files, signs of persistent OS, etc.). This mostly happened with new clients or the addition of a new host to the monitoring scope
-  9% were successful social engineering initial accesses, but with prevented attacks before they could be properly classified



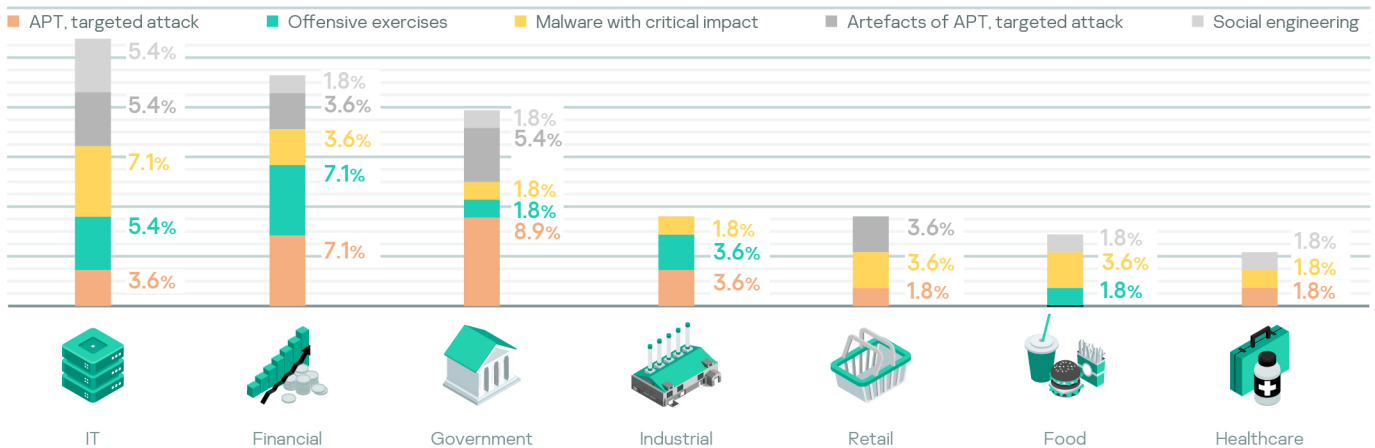
How many organizations experienced high severity incidents?



- 27%** of organizations faced a targeted attack or APT
- 23%** became victims of high impact malware outbreaks (like ransomware)
- 20%** of our clients performed offensive exercises

Number of organizations with high incidents by vertical

Almost all industry sectors faced all types of incidents throughout our three-month analytical period.



APT artefacts (signs of previous human-driven attacks) are almost always found along with active APTs. This proves that if an organization recovered from an APT, it's often attacked again - presumably by the same actor.

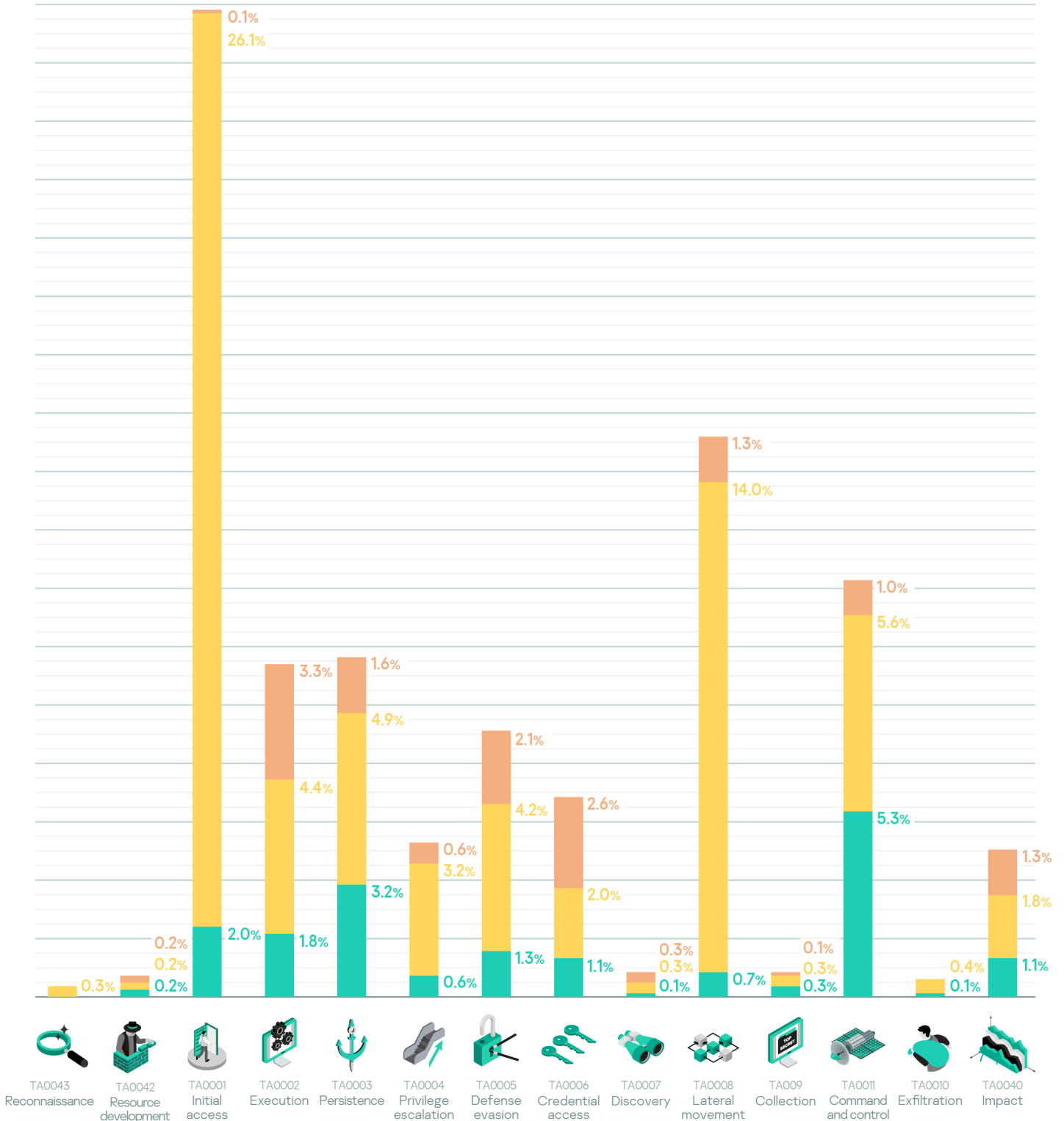
APT targeted sectors usually also conduct red teaming that demonstrates their correct risk assessment.

Detection technology and adversarial TTPs

Adversarial tactics

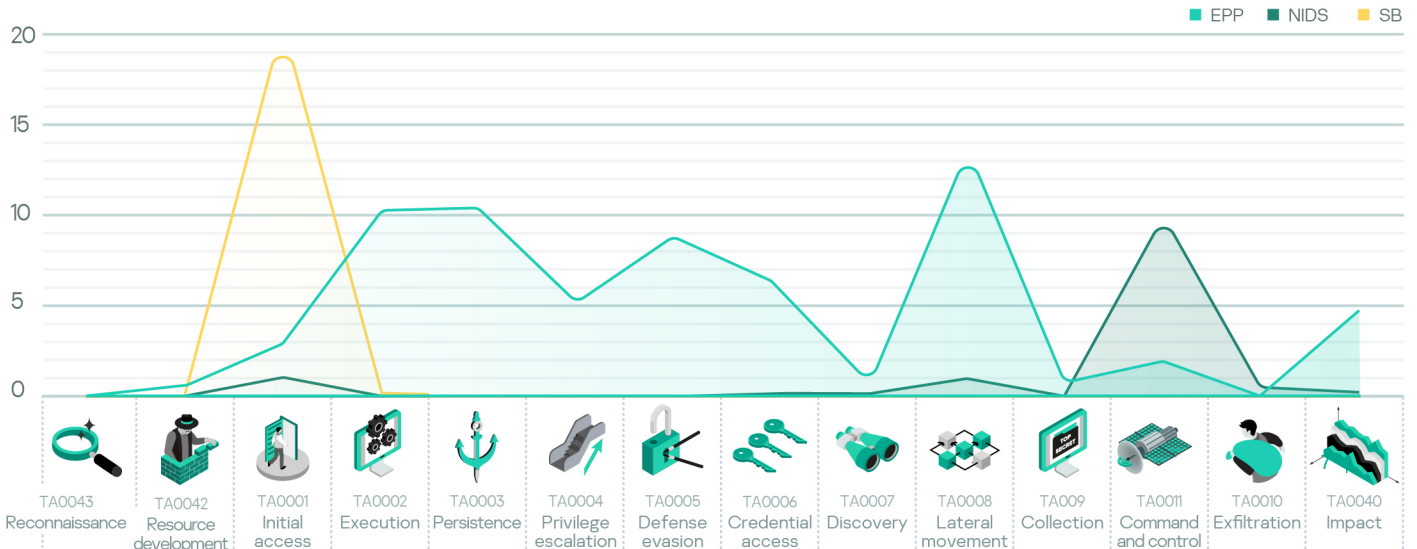
Most of the incidents were detected at the initial access phase. Execution, Persistence, Defense Evasion, Credential Access, Lateral Movement, Command and Control tactics are sources of a substantial number of attack detections. Fewer incidents were detected at the Exfiltration and Collection phases because they were correctly classified and remediated at earlier stages. All cases detected at these late stages are subjected to thorough analysis and detection logic improvement to raise the chances of threat detection as early as possible.

■ Low severity incidents ■ Medium severity incidents ■ High severity incidents



Tactics and detection technology

In MDR we receive telemetry from different types of sensors (detection technologies): Endpoint Protection Platforms (EPP), Sandbox (SB) and Network Intrusion Detection System (NIDS). Network IDS and SB are components of Kaspersky Anti-Targeted Attack Platform¹. Host-based NIDS is part of the comprehensive EPP – Kaspersky Endpoint Security for Business². Next you can see the top performing MITRE ATT&CK techniques in our MDR from each sensor. The graph shows the adversary tactic at the moment of incident detection.



Next you can see top performing (by top most contributing to number of incidents technique) MITRE ATT&CK techniques in our MDR from each sensor

Initial access EPP SB T1566.001 Spearphishing Attachment SB NIDS T1566.002 Spearphishing Link NIDS T1190 Exploit Public-Facing Application NIDS T1133 External Remote Services	Execution EPP SB T1053 Scheduled Task/Job EPP SB T1204 User Execution EPP T1059.001 PowerShell EPP T1059 Command and Scripting Interpreter SB T1204.001 Malicious Link	Persistence EPP SB T1053 Scheduled Task/Job EPP T1547.001 Registry Run Keys / Startup Folder EPP T1546.008 Accessibility Features NIDS T1133 External Remote Services	Privilege escalation EPP SB T1053 Scheduled Task/Job EPP T1547.001 Registry Run Keys / Startup Folder EPP T1546.008 Accessibility Features EPP T1055 Process Injection
Defense evasion EPP T1036 Masquerading EPP T1055 Process Injection	Discovery NIDS T1083 File and Directory Discovery Lateral Movement EPP NIDS T1210 Exploitation of Remote Services EPP T1021 Remote Services	Command and control NIDS T1071 Application Layer Protocol NIDS T1095 Non-Application Layer Protocol NIDS T1102 Web Service	Exfiltration NIDS T1048 Exfiltration Over Alternative Protocol Impact EPP T1496 Resource Hijacking
Credential access EPP T1003 OS Credential Dumping			

EPP <ul style="list-style-type: none"> Obviously, the biggest coverage through all tactics Geared towards the noisiest attack phases: between initial access and established compromise leading to impact 	Sandbox <ul style="list-style-type: none"> Helps to speed up triage and provide additional context for analysts Results focused on the prologue and epilogue of the kill chain 	NIDS <ul style="list-style-type: none"> Distinctive focus on pre-impact tactics A useful addition to cover initial access tactics
--	---	--

¹KATA – www.kaspersky.com/enterprise-security/anti-targeted-attack-platform
²KESB – www.kaspersky.com/enterprise-security/endpoint

Adversarial techniques

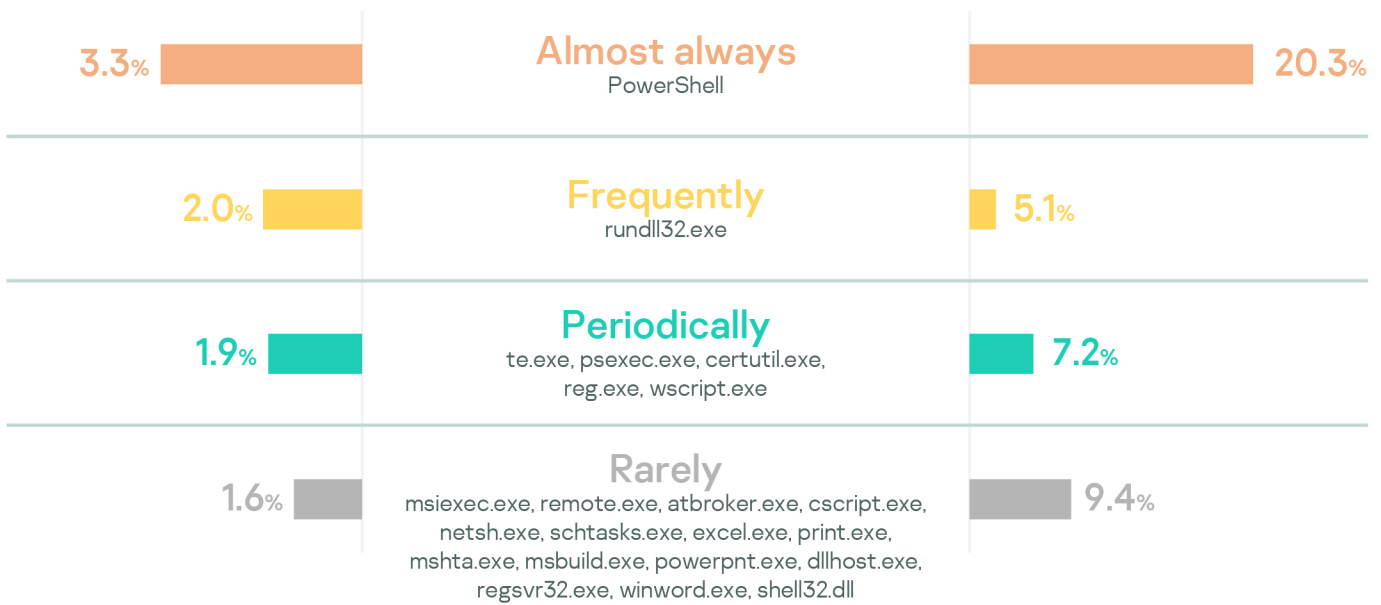
Tools used in incidents

Malefactors tend to use tools integrated into OS to lower their footprint for delivery of instruments, decrease costs of toolset development and, mainly, to blend their work with legitimate activity which makes defender's job much harder. Such tools are called living-off-the-land binaries and can be

reviewed on lolbins project website. Major conclusion is not surprising, although Microsoft has made impressive efforts to improve security and control of PowerShell, it remains the most popular tool used by adversary actors by far.

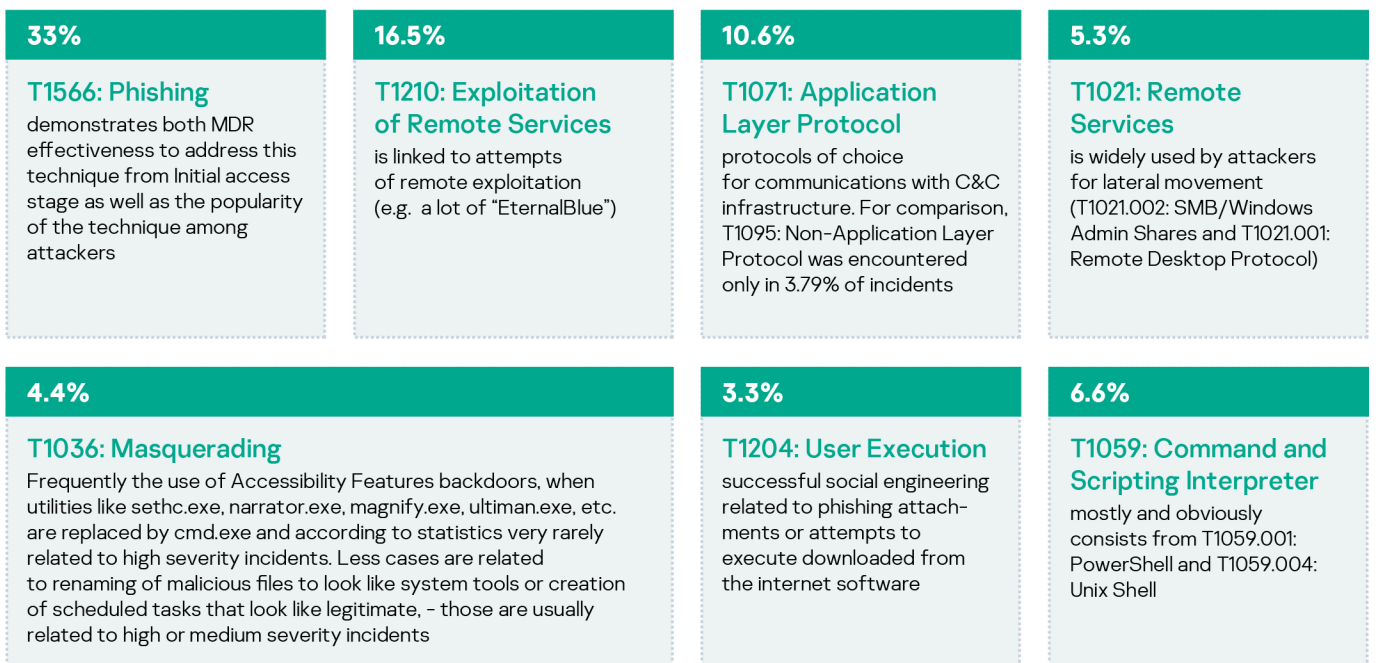
Percentage of incidents with **lolbins** from all incidents

Percentage of high incidents with lolbins (from all high incidents)



Incident mapping to MITRE ATT&CK

A good metric for MITRE techniques-based detection logic is its efficiency. It shows what percent of all reported incidents was detected by threat hunting rules based on particular techniques.



TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1595: Active Scanning	T1587: Develop Capabilities	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1098: Account Manipulation	T1548: Abuse Elevation Control Mechanism	T1140: Deobfuscate/Decode Files or Information
	T1588: Obtain Capabilities	T1133: External Remote Services	T1203: Exploitation for Client Execution	T1547: Boot or Logon Autostart Execution	T1134: Access Token Manipulation	T1564: Hide Artifacts
		T1566: Phishing	T1559: Inter-Process Communication	T1037: Boot or Logon Initialization Scripts	T1546: Event Triggered Execution	T1562: Impair Defenses
		T1091: Replication Through Removable Media	T1053: Scheduled Task/Job	T1554: Compromise Client Software Binary	T1068: Exploitation for Privilege Escalation	T1070: Indicator Removal on Host
		T1078: Valid Accounts	T1569: System Services	T1136: Create Account	T1574: Hijack Execution Flow	T1036: Masquerading
			T1204: User Execution	T1505: Server Software Component	T1055: Process Injection	T1112: Modify Registry
			T1047: Windows Management Instrumentation			T1027: Obfuscated Files or Information
						T1542: Pre-OS Boot
						T1218: Signed Binary Proxy Execution

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1110: Brute Force	T1087: Account Discovery	T1210: Exploitation of Remote Services	T1123: Audio Capture	T1071: Application Layer Protocol	T1048: Exfiltration Over Alternative Protocol	T1485: Data Destruction
T1555: Credentials from Password Stores	T1482: Domain Trust Discovery	T1570: Lateral Tool Transfer	T1005: Data from Local System	T1001: Data Obfuscation		T1486: Data Encrypted for Impact
T1556: Modify Authentication Process	T1083: File and Directory Discovery	T1021: Remote Services	T1056: Input Capture	T1105: Ingress Tool Transfer		T1565: Data Manipulation
T1003: OS Credential Dumping	T1046: Network Service Scanning	T1550: Use Alternate Authentication Material		T1095: Non-Application Layer Protocol		T1561: Disk Wipe
T1552: Unsecured Credentials	T1135: Network Share Discovery			T1090: Proxy		T1496: Resource Hijacking
	T1069: Permission Groups Discovery			T1219: Remote Access Software		
	T1012: Query Registry			T1102: Web Service		
	T1018: Remote System Discovery					
	T1033: System Owner/User Discovery					
	T1497: Virtualization/Sandbox Evasion					