ADEO CYBER SECURITY

ADEO MANAGED DETECTION AND RESPONSE SERVICE REPORT 2022

www.adeo.com.tr

TABLE OF CONTENTS

1. About ADEO MDR Report

MDR remotely monitors, detects and responds to threats detected within your organization. For this, the service provider uses an endpoint detection and response (EDR*) tool, which provides the necessary visibility into security events at the endpoint. After providing the required visibility, telemetry data from endpoints is collected in the center console. Here, with the help of threat intelligence data and advanced analytics, suspicious incidents are detected and responded quickly.

This tools;

- allow attacks detected by the MDR team to be highly accurate.
- provide a detailed view of what happened before and after the relevant cyber incident.
- allow planning actions to quickly prevent a similar attack immediately after a Cyber attack.

In this way, institutions gain resistance against both known and unknown cyber attacks.

MDR Analysts can detect real-time cyber incidents and take very fast action regarding these detected cyber attacks.

Fast verification and action capabilities are of critical importance in the response of advanced cyber attacks.

"MDR is a cybersecurity service that combines technology and human expertise to perform threat hunting, monitoring and response."

**EDR (Endpoint Detection and Response)*
It is a tool that records all the processes running at the endpoints and their activities, provides detection and threat hunting according to behavioral indicators as well as atomic indicators, and where evidence of suspicious activities can be collected or intervened when necessary.

**XDR (Extended Detection and Response)*
In addition to EDR tools, they are tools that can analyze records from various sources such as network, cloud, identity management, e-mail security.

ADEO CYBER SECURITY

ADEO MDR SERVICE

WHAT WE DID IN 2022?

2. 2022 STATISTICS

BUSIEST DAY:

7 APRIL

NUMBER OF ALARMS* REVİEWED TODAY

652

PERCENTAGE OF ALARMS RESOLVED WITHOUT INCIDENT RESPONSE:

%99

MOST TARGETED INDUSTRIES AND THEIR TOTAL NUMBER OF INCIDENT:

MANUFACTURING

23 INCIDENT

TRANSPORT

7 INCIDENT

BUSIEST MONTH:

FEBRUARY

NUMBER OF INCIDENT SEEN:

5

***ALARM:**

Warning messages falling on security tools used to detect cyber attacks are called. These alarms are grouped according to their criticality level.

***INCIDENT:**

Attacker activities that require in-depth analysis and incident response processes as a result of analyzing a true detected alarm. They are mostly activities that spread and persist in more than one machine in a short time.

2022 STATISTICS

"New vulnerabilities are followed 7x24x365 days and the relevant rules are written by ADEO MDR Threat Hunters."

"ADEO Intelligence Service is constantly fed by real events and current attacks."

***Initial Access Technique:** By taking advantage of various vulnerabilities, the attacker gains the initial access to the system and starts to use other tactics and techniques by reaching the targets.*

The number of Detection Rules was increased from **2000** in January 2022 to **4,000** at the end of the year.

The number of IOCs, which was **20.000** in January 2022, increased to **51.000** at the end of the year.

Total Number of Rules Developed:

4000+

Number of IOCs scanned with threat intelligence provided internally and externally

51K

Most Used Initial Access* Technique

Phishing

%9,24

3. DAILY ROUTINE OF MDR SERVICE

97% of inspected alarms are analyzed by **ADEO MDR** teams without notifying customers. **Necessary procedures** are applied according to the maturity of the product used. In this way, our customers can safely focus on their daily workflows. The analyzes made and the actions taken are reported and communicated to the customers at certain periods.

TRUE POSITIVE ALARM:
These are alarms that indicate a real attack or unwanted/illegal behavior.

An average of **30** new detection rules are written daily by **ADEO MDR** team.
Tightening/improvement works are also carried out in accordance with the rules determined as false positive*.

FALSE POSITIVE ALARM:
These are the alarms that are determined as a result of the analyzes that do not indicate a real attack or that occur in accordance with the wrongly written rules.

3% of alarms are confirmed and necessary actions are taken after confirmation.

The detected **IP** and **Domain** are checked by the **intelligence services** and the **IP blocking** process is performed by examining the machines with which it is in communication within the network.

As a result of **detection of malware**, activities are examined with a **threat hunting** approach, machines spreading malware are **isolated** and **necessary actions** are taken.

You can contact us to get detailed information about our ADEO MDR Services and to forward your questions.

info@adeo.com.tr

4. MANAGED DETECTION AND RESPONSE INCIDENT MANAGEMENT STAGES

NUMBER OF INCIDENT RESPONSE:

52

Incident

They are attacker activities that require in-depth analysis and incident response processes as a result of the analysis of a detected real alarm. Incident response procedures are required as a result of some initial access techniques, such as attackers exploiting zero-day vulnerabilities or obtaining employee password/username information. The distribution of first access techniques requiring incident response in 2022 is indicated on page 21.

Incident Management Stages

ADEO MDR team **researches** and **detects compromised machines**.

The MDR detection phase involves detecting and identifying suspicious activity on systems.
The mean detection time (Dwell Time) of possible **high severity** and **critical** anomalies determined by using security products such as **EDR**, **NDR**, **SOAR** and the competencies of MDR Analysts is **3 minutes 37 seconds**.

Suspicious activities detected through various security products are examined in detail by **ADEO MDR** Analysts **7x24x365** days.

The response phase is the actions taken to **stop** and **prevent** the activities detected as malicious as a result of the analysis and to **prevent the activity from spreading** within the organization.
In 2022, the mean **response time** of **ADEO MDR** team to **high severity** and **critical** incidents was **16 minutes 27 seconds.**

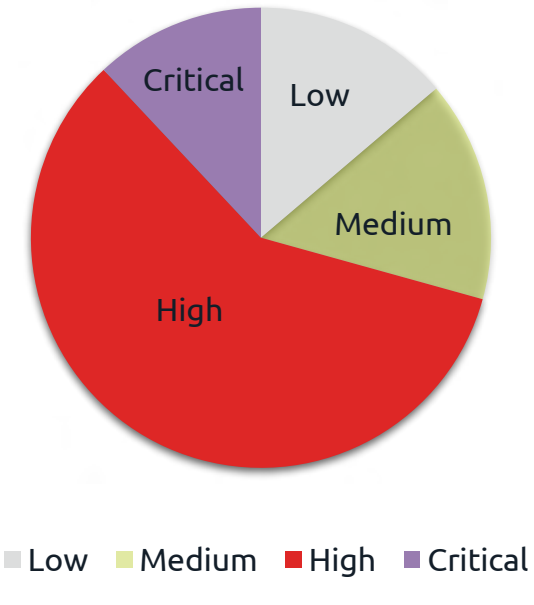
The recovery phase includes measures to **eliminate**, **improve**, and **prevent repetition** of threatening situations.

Security Breach
↓
Detection
↓
Analysis
↓
Response
↓
Remediation

5. NUMBER OF ALARMS AND ITS SEVERITY PER YEAR

ADEO's rule development and improvement efforts continue.

Within the scope of these works, the target for 2023 is to reduce the number of critical and high-level alarms and to increase the number of true positive alarms.



DETECTION AND RESPONSE TIME

MEAN TIME TO DETECTION*

3m 37s

MEAN TIME TO RESPONSE*

16m 27s

The mean detection time of only high severity and critical alarms was 3 minutes 37 seconds, and the mean response time was 16 minutes and 27 seconds.

**DETECTION TIME:*
It is the time elapsed between the realization of the attack and the detection of the attack by the MDR team and defining it as an attack.

**RESPONSE TIME:*
It is the time interval when the attack occurs and the necessary action is taken after the relevant attack is seen and defined by the MDR Team.

6. DISTRIBUTIONS OF ALARMS BY INDUSTRY

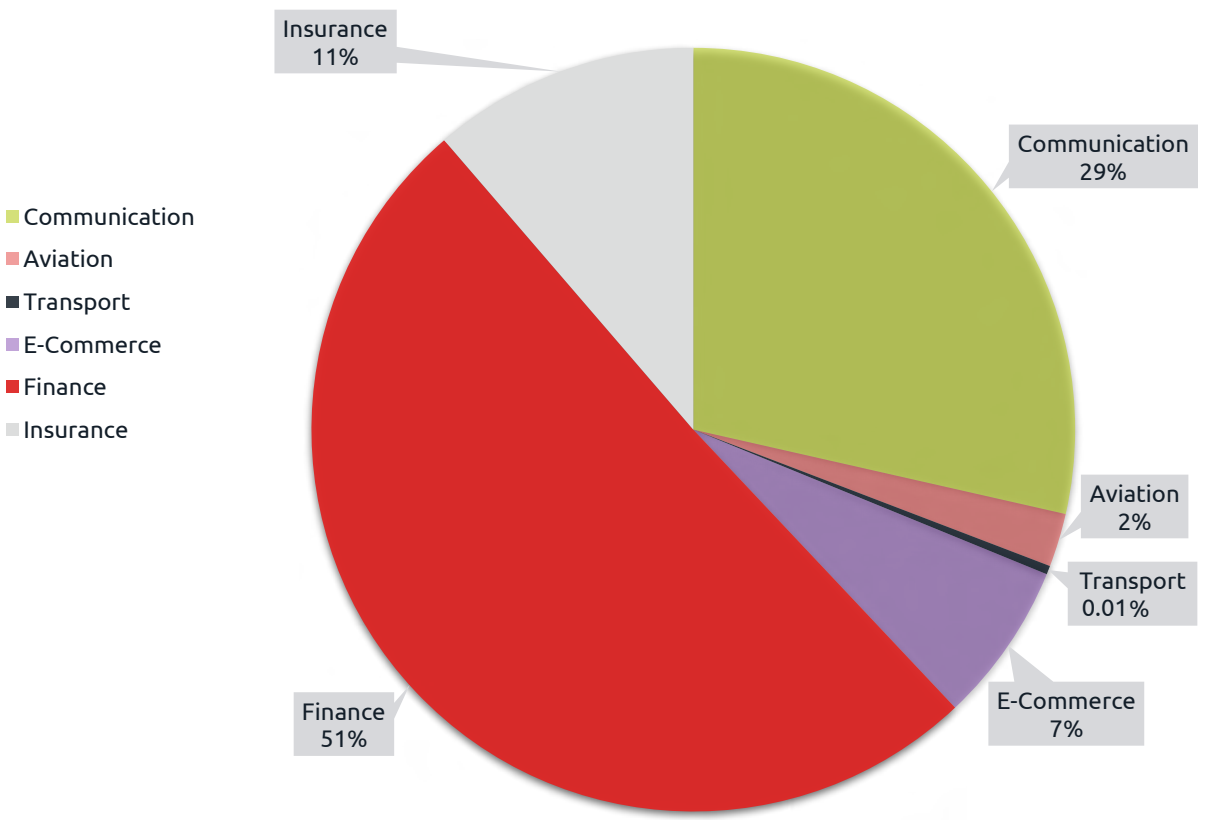
INDUSTRIES WITH MOST ALARM OBSERVATIONS

FINANCE

The strategic importance of the sector is huge and therefore it is the target of cyber attack groups.

COMMUNICATION

It is a distributed sector in which employees are mostly in the field.
The attacks were exposed due to this distributed structure.



7. TOP VICTIM INDUSTRIES

Ransomware groups specifically target the **Manufacturing** sector.

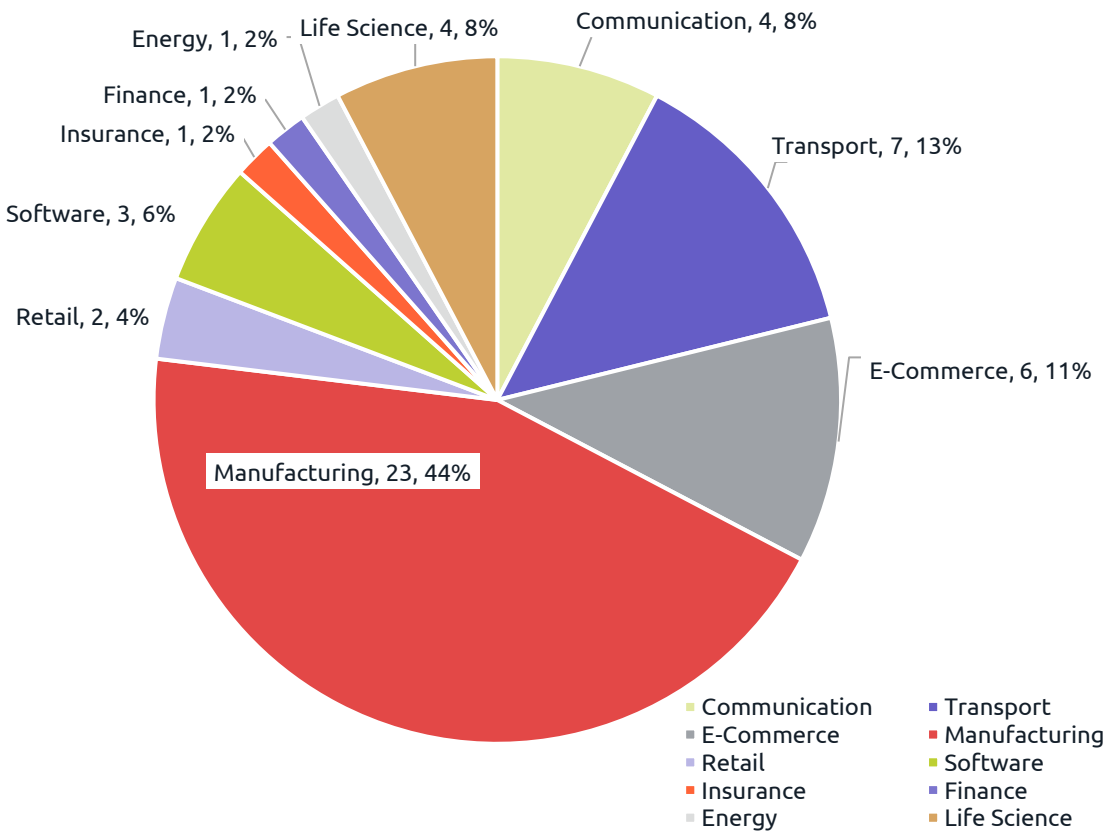
The sector is in a **distributed structure** and the management is not carried out from the center, but by the teams in the region. **Awareness** is low due to local team control.

As a result of this low awareness, **visibility is low** and suspicious movements are detected **lately**.

Due to the **very low** level of visibility in **OT environments**, it has been observed that security standards are not met and awareness or precautions against OT attacks are very weak.

Why Manufacturing?

NUMBER OF INCIDENTS



8. MOST SIGNIFICANT SECURITY VULNERABILITIES IN 2022& ADEO MDR SERVICE'S DETECTION RULES

The rules we wrote as **ADEO MDR** about the important **Top 50+** vulnerabilities published in 2022 and the number of **IOCs we added** are shown in the table. As can be seen here, the number of cyber incidents is increasing day by day.

When we go into the details of the cyber attacks that occurred, the detection rate of these attacks is lower than the detection rate of previous attacks. In addition to the products' own detection capabilities, **proactive security solutions are needed** for the detection of new attacks.

At this point, it is ensured that the threat indicators obtained as a result of regular research from cyber **threat intelligence sources are blocked, the attacks obtained from these sources are analyzed, the rules for the detection of the related attacks are developed and the written rules are tested in our laboratory environments**, added to the ADEO rule database and disseminated on our customers' systems.

Our threat detection and intelligence analysts regularly conduct research on **emerging security vulnerabilities**. After the vulnerabilities are technically examined and tested in laboratory environments, **more than one rule set** is developed to increase the visibility of the attack surface, specific to **the detected IOCs** and the different observed patterns.

"Proactive security solutions are needed for the detection of new attacks."

You can contact us to get detailed information about our ADEO MDR Services and to forward your questions.

info@adeo.com.tr

9. MOST SIGNIFICANT SECURITY VULNERABILITIES IN 2022& ADEO MDR SERVICE'S DETECTION RULES

Security Vulnerability	Number of Rules Written	Number of IOCs Added
SysJoker Backdoor	18	74
Qbot/Qakbot	25	270
CVE-2021-4034 | PwnKit: Local Privilege Escalation Vulnerability	3	97
BazarLoader	4	100
Malware Targeting Ukrainian Organizations	12	4316
ProxyNotShell Exchange Vulnerability (CVE-2022-41082, CVE-2022-41040)	14	400
B1txor20	7	114
Spring4Shell	6	250
CVE-2022-26809 Remote Procedure Call Runtime Remote Code Execution Vulnerability	3	252
CVE-2022-29072 - 7-Zip Local Privilege Escalation	3	32
BPFDoor - An Evasive Linux Backdoor	6	101
MS-MSDT 0-day RCE	6	120
Kingminer Botnet Attack	6	345
Follina Zero-Day Vulnerability (CVE 2022-30190)	3	183
LockBit 3.0 Ransomware	3	210
Domain Privilege Escalation [CVE-2022-26923]	3	229
Windows System hive/sam File Export Process	7	236
SessionManager Exchange Malware	6	194
Microsoft Teams' GIFShell Attack	6	185
Nerbian RAT Malware	6	50
X-Files Stealer – Malware	8	37
HermeticWiper and Destructive Malware Targeting Ukraine	5	63
WhisperGate: A Destructive Malware to Destroy Ukraine Computer Systems	5	70
New BianLian Ransomware	7	129
BlackByte Ransomware	7	108
Lazarus Group's Rootkit Attack	12	840
Ryuk Ransomware	4	72
Zero-day Vulnerabilities in Microsoft Exchange Server	12	1525
BlackCat Ransomware	18	38
BumbleBee Malware	7	351
Cuba Ransomware	25	710
Black Basta Ransomware	20	125

MOST SIGNIFICANT SECURITY VULNERABILITIES IN 2022& ADEO MDR SERVICE'S DETECTION RULES

With the rules developed about the relevant security vulnerabilities and attacks and the competencies of MDR security analysts, **threat hunting** is carried out on our customers' systems at regular intervals. Before potential cyber attacks occur, the relevant vulnerability or attack indicators are detected. After the determination made, the necessary precautions and actions are taken and the institution is informed about the subject. Attack-related rules are added to customer systems and **monitored** by **MDR security analysts** for **7x24x365** days. Details of the findings are shared with our customers through MDR reports on a regular basis.

After a certain period, after the rules are added to the customer systems that are monitored by **security analysts**, the alarms regarding the exploitation of the relevant vulnerability are detected by the analysts. In line with the investigations, after the exploitation of cyber attacks is prevented by the developed rules and IOCs, the **root cause** causing the vulnerability is **investigated by the analysts**.

ADEO threat intelligence resource is updated with the **findings** and **IOC data** obtained after the analysis. The intelligence data sets obtained from the attacks are added to our customers' systems on a regular basis. In this way, with the added IOC and intelligence data, the exploitation of the relevant security vulnerability on all customer systems is prevented.

"Attack-related rules are added to customer systems and monitored by MDR security analysts for 7x24x365 days. "

10. MOST IMPORTANT TOPICS OF THE YEAR #TOP 4

BUSIEST MONTH:
FEBRUARY

NUMBER OF INCIDENTS SEEN:
5

BUSIEST DAY:
7 APRIL

NUMBER OF ALARMS REVIEWED TODAY:
652

"By controlling global trends and following threat intelligence, rules for current vulnerabilities are added quickly."

11. MOST IMPORTANT TOPICS OF THE YEAR- #1 Spring4Shell

What is Spring4Shell? (1)

Spring is a framework for Java. Spring4Shell, identified by the code CVE-2022-22965, is a vulnerability in the Spring Framework that allows remote code execution (RCE). It was named Spring4Shell after the Log4Shell vulnerability that was popular in 2021, but these vulnerabilities are not related to each other.

The zero-day vulnerability was announced in a Twitter post that was later deleted. VMware also officially announced Spring4Shell on March 31, 2022

What Are Spring4Shell Effects? (2)

The vulnerability affects Spring MVC and Spring WebFlux applications running JDK 9 or higher. Webshell allows a web server to be accessed remotely, often for the purpose of cyber attacks. Most exploits for the Spring4Shell vulnerability occur by uploading webshell with a malicious .jsp file to the web server. After the webshell is loaded, attackers can run code remotely.

What are Spring4Shell Activities? (3)

- 4 days after the Spring4Shell vulnerability was published, 16% of organizations worldwide were exposed to exploit attempts.
- In the first week after the Spring4Shell vulnerability was released, there were 37,000 exploit attempts.
- Software vendors were the most affected sector with 28%.
- Europe is the continent most affected by exploitation attempts with an impact of 20%

How long did we update the detection rules we created?

As ADEO MDR Service, we have animated the Spring4Shell vulnerability in our own laboratory environments and used different patterns to detect the related vulnerability. A total of 6 detection rules developed and 250 malicious IOCs collected from various global CTI sources were transferred to all our customers within **4 hours**.

12. MOST IMPORTANT TOPICS OF THE YEAR - #2 ProxyNotShell

What is ProxyNotShell?

On September 30, 2022, Microsoft released two vulnerabilities affecting Exchange email servers. These vulnerabilities were named ProxyNotShell because they resemble the ProxyShell vulnerability.

An attacker must be authenticated to exploit these vulnerabilities. Therefore, CVSSv3 scores were determined as 8.8.

What are ProxyNotShell Effects?

The first published vulnerability, CVE-2022-41040, allows exploiting the Server-Side Request Forgery (SSRF) vulnerability in Exchange Server. Another vulnerability included in ProxyNotShell, CVE-2022-41082, allows remote code execution (RCE).

What are the recommendations published by Microsoft for ProxyNotShell?

Microsoft yayınladığı blog yazısında (4) Exchange Online müşterilerinin herhangi bir işlem yapmasına gerek olmadığını belirtti. Güvenlik açığı ilk açıklandığında Microsoft'un yayınladığı ilk önermeler yetersiz kaldı, sonrasında Exchange sunucuları için güncelleme yayınlandı. Microsoft yayınlanan güncellemelerin uygulanmasını önerdi.

How long did we update the detection rules we created?

As ADEO MDR Service, we have animated the **ProxyNotShell** vulnerability in our own laboratory environments and used different patterns to detect the related vulnerability. A total of **14 detection rules** developed and **400 malicious IOCs collected** from various global CTI sources were transferred to all our customers within **5 hours.**

13. MOST IMPORTANT TOPICS OF THE YEAR - #3 Cuba Ransomware

Let's Get to Know Cuba Ransomware Group

Who is Cuba Ransomware Group?

Cuba ransomware was first observed in December 2019. In November 2021, the FBI increased its awareness when it released an official statement about this ransomware group. (5) Cuba ransomware is thought to be a Russian-based group as it was observed that it did not proceed with the attack when a Russian keyboard layout was noticed.

Most Affected Countries and Sectors?

The countries where Cuba ransomware makes the highest number of attack attempts are the USA (26%) and Turkey (21%). When the sectors targeted by Cuba were investigated, it was observed that the IT sector was in the first place. It is known to target companies with medium-sized (201-1000 employees) in general.

Cuba Ransomware Group targeted organizations affected by ProxyShell ((CVE-2021-34473, CVE-2021-34523 , CVE-2021-31207) and ProxyLogon (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) vulnerabilities, giving them their first access. (6)

Some of Cuba's Attacks in 2022

August: Cuba Ransomware group was found to be using a new malware called ROMCOM RAT with activities such as loading data and a new tool called KerberCache. (7)

September: Cuba attacks the Montenegrin government, blaming Russia for the attack, claiming that some sensitive documents were leaked on the dark web. (8)

October: Cuba ransomware group launched a phishing attack targeting Ukraine. It was detected that when the link from the phishing email was clicked in the attack, the file was downloaded by being directed to PDF Reader and running the ROMCOM malware.

How long did we update the detection rules we created?

As **ADEO MDR Service**, we have animated the Cuba vulnerability in our own laboratory environments and used different patterns to detect the related vulnerability.

A total of **31 detection rules** and **710 IOCs** were delivered to all our customers within **6 hours.**

14. MOST IMPORTANT TOPICS OF THE YEAR- #4 LockBit

What is LockBit?

LockBit ransomware is malicious software designed to prevent users from accessing their computer systems and force them to pay a ransom.

Attacks using LockBit started in September 2019 with the then-named ".abcd virus". To date, the software has targeted organizations in the US, China, India, Indonesia, and Ukraine. In addition, attacks were seen in many countries (France, United Kingdom, Germany) across Europe.

LockBit, Back in the Fied with 3.0

In June 2022, Lockbit ransomware group was found to have started using the latest ransomware variant, LockBit 3.0. The group called this new version “LockBit Black”.

In June 2022, LockBit also launched a bug bounty program by launching a first. They offered $1 million to the security researcher who could identify anyone from LockBit group.

2022 Activities of LockBit 3.0

October: LockBit group publishes British car dealership Pendragon on their blog page in October 2022. LockBit group demanded a ransom of $60 million, but Pendragon refused to pay the ransom.

Lockbit was able to steal 5% of Pendragon data. In October, they attacked a few more large companies.

November: LockBit group attacked the big tech startup Thales in November 2022. When Thales refused to pay the ransom, the data was leaked. (9)

How long did we update the detection rules we created?

As **ADEO MDR Service**, we used different patterns to simulate the LockBit vulnerability in our own laboratory environments and to detect the related vulnerability. A total of **31 detection rules** and **210 IOCs** were transferred to all our customers within **3 hours.**

MOST IMPORTNT TOPICS OF THE YEAR - TOP 4 - Sources

Sources

1 – https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement

2 – https://kb.vmware.com/s/article/88203

3 - https://blog.checkpoint.com/2022/04/05/16-of-organizations-worldwide-impacted-by-spring4shell-zero-day-vulnerability-exploitation-attempts-since-outbreak/

4 - https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

5- https://www.cisa.gov/uscert/ncas/alerts/aa22-335a

6 - https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba

7 - https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

8 - https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/

9 - https://www.avertium.com/resources/threat-reports/an-update-on-lockbit-3.0

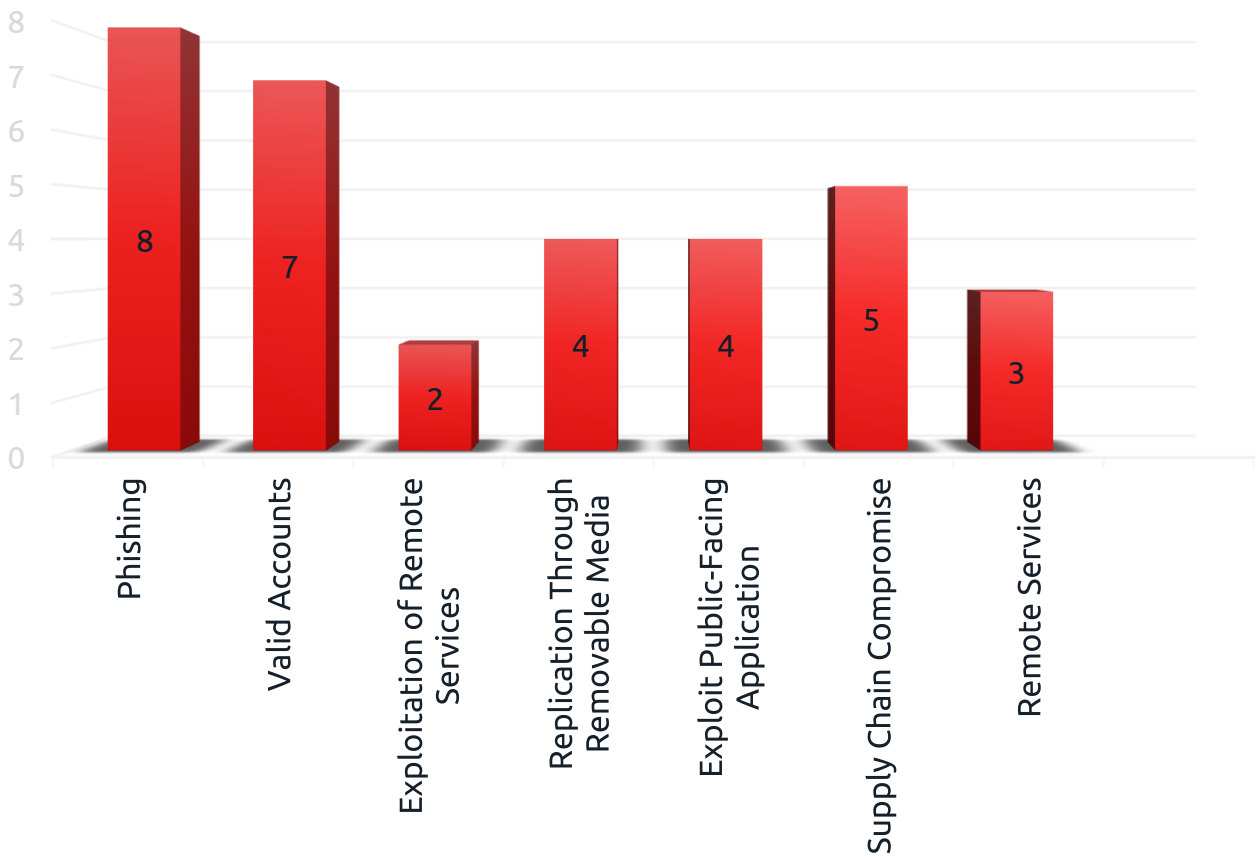
15. MOST POPULAR INITIAL ACCESS TECHNIQUES

An attacker's ability to gain a foothold in the environment begins with initial access.

The credentials of compromised accounts can be compromised by various techniques and used to bypass access controls applied to different resources on systems within the network.

After initial access, the attacker can switch to other tactics and techniques to achieve objectives. Therefore, preventing the first access is important for the security of the system.

"Preventing the first access is important for the security of the system."



ADEO MDR SERVICE

TACTICS*, TECHNIQUES* & DETECTION RULES

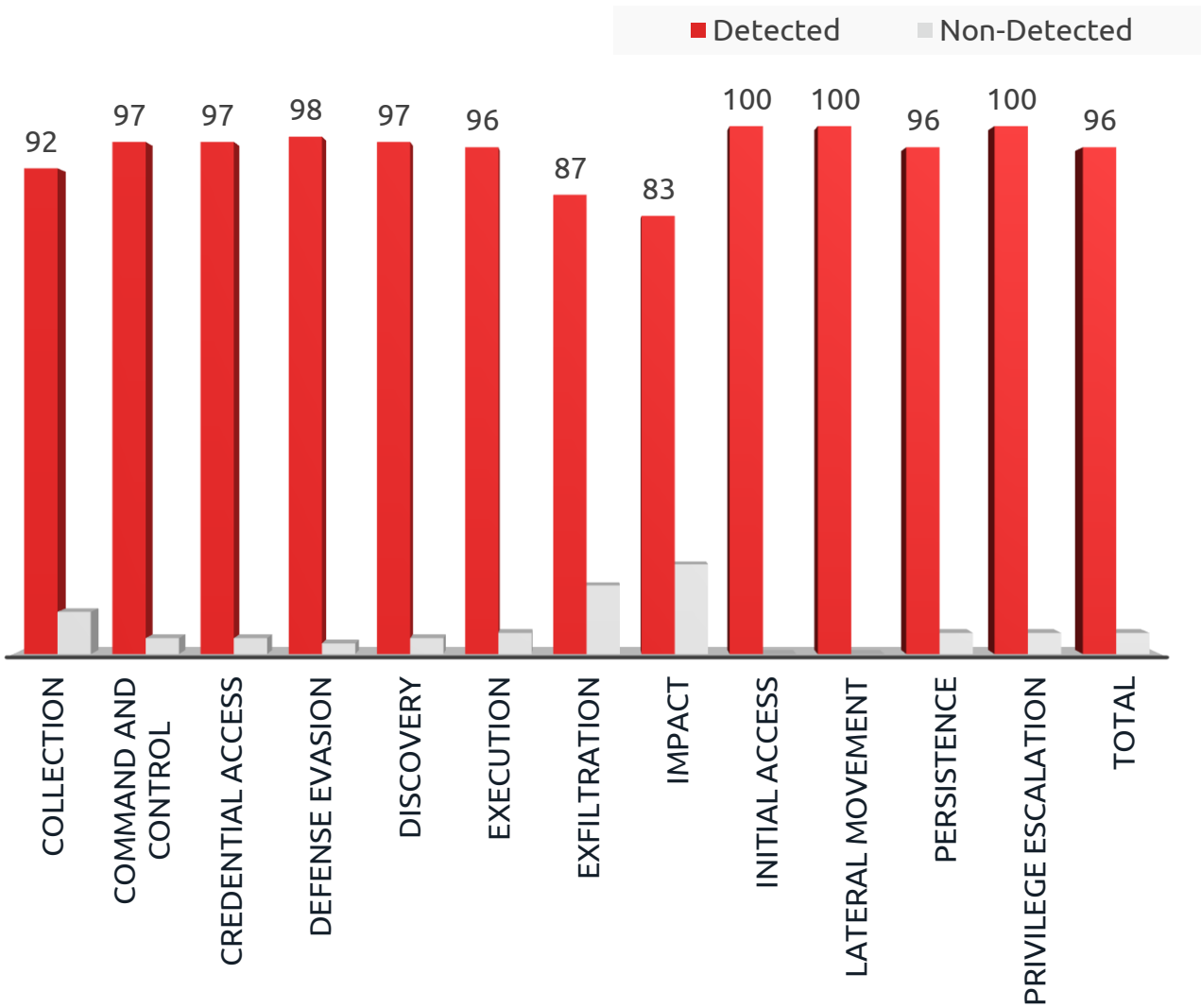
**TACTICS:*
Indicates the purpose of the activities performed by the attacker. It is of great importance in determining the stage of the attack.
**TECHNIQUES:*
The tools, methods, or processes that attackers use to carry out these tactics.

16. OUR DETECTION RULES

As **ADEO MDR Service**, we can detect all the tactics in the MITRE ATT&CK® Framework through the special detection rules we have developed, the IoCs we collect from threat intelligence platforms, and our strong leading product portfolio.

As a result of the security tests performed by MDR Service, it has been reported that **97% of 465 techniques can be detected** via EDR. Of the **18 undetected techniques**, only **5 were observed to be detectable by EDR.**

"As a result of the security tests performed by MDR Service, it has been reported that 97% of 465 techniques can be detected via EDR."



17. TACTICS

1.COLLECTION

The adversary is trying to gather data of interest to their goal.
Collection consists of techniques adversaries may use to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.
Frequently, the next goal after collecting data is to steal (exfiltrate) the data. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input.

92% of the attacks made using the Collection tactic can be detected by our **ADEO MDR Service**.

In addition to **EDR technology**, it is recommended to implement data loss prevention systems for the detection of these and similar attacks.
It is recommended to use **DLP** technology, which is an additional data leakage prevention system, for studies such as planning controls such as reducing the risk, impact and degree of attack and ensuring the continuity of policies.

XDR, **NDR**, **Firewall**, **DLP** technologies are recommended to prevent the leak attempts of **compressed or encrypted** files and to perform user behavior analysis (UBA).

It is important to organize **awareness trainings** at regular intervals in order to increase user awareness.
It is recommended to keep the system images and **software used up-to-date.**

In an **Exchange** environment, **Exchange rules** need to be tightened to prevent administrators from doing potentially malicious automatic forwarding, downloading, and opening.
Using multi-factor authentication (MFA) for externally accessible e-mail servers will greatly reduce attacks.

17. TACTICS

2. COMMAND AND CONTROL

The adversary is trying to communicate with compromised systems to control them.
Command and Control consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.
There are many ways an adversary can establish command and control with various levels of stealth depending on the victim's network structure and defenses.

97% of the attacks made using the Command and Control tactic can be detected by our **ADEO MDR Service.**

Web traffic to/from known **bad or suspicious domains** should **be monitored.**

It is recommended to filter DNS requests to unknown, untrusted or known bad domains and resources through the firewall.

It is recommended to use
- **Firewall, NDR, IDS/IPS in addition to EDR** for the detection of these and similar attacks and
- **UBA-based products** for user behavior analysis.

It is necessary to **monitor the traffic** in the network and to **constantly check** the IP's going from inside to outside and coming from outside with **intelligence services.**

Applications that can be installed on the system must pass through the approval mechanism and must be in the list of allowed applications **(White List).**
Your computer system should not allow any application to be run or installed.
By blocking the installation of applications from unknown sources, **you can prevent malware used to create** C2 channels from being installed on your system.

17. TACTICS

3. CREDENTIAL ACCESS

The adversary is trying to steal account names and passwords.
Credential Access consists of techniques for stealing credentials like account names and passwords.
Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

97% of the attacks made using the Credential Access tactic can be detected by our **ADEO MDR Service.**

WAF is a common **security control** used by organizations to protect web systems from zero-day exploits, remote command execution, and other known and unknown threats and vulnerabilities.
It is recommended **to locate WAF within the organization**.

Passwords should not be used on different platforms, the password should be considered for a maximum of **1 or 3 months**, and it should be considered to have special features. It is important to **avoid unnecessary/over-authorization**, and to close the existing accounts after the staff leaves the job.
File shares should be limited to specific directories that only have access to required users.

It is recommended to place **Privileged Access Management** (**PAM**) products within the organization in order to securely manage the accounts of users with access permissions to critical resources.
It is important **to activate MFA** in all possible logins, especially VPN and E-mail access.

It is important to isolate the departments from each other by using **VLAN** and to minimize the possible dangers.
It is recommended to regularly update the **security updates** of the applications **where the credentials are hosted**, especially the Domain Controller servers.

17. TACTICS

4. DEFENSE EVASION

The adversary is trying to avoid being detected.
Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise.
Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

98% of the attacks made using the Defense Evasion tactic can be detected by our **ADEO MDR Service**.

It is recommended **to save/archive** the logs of the relevant applications in a central point in order to analyze the activities performed via **PowerShell** and **Command Prompt** command line applications.
It is recommended to position **Load Balance, DDoS Protection** products in-house to protect against denial of service attacks **(DoS/DDoS)** and to minimize attack types.

It is recommended to **limit user privileges.**
Only authorized users should be limited to making service changes.
It is recommended to **prevent execution** from user directories such as file download directories and temporary files directories.

Attackers can abuse compiled **HTML files (.chm)** to hide malicious code. CHM files are often distributed as part of the Microsoft HTML help system. CHM files are compressed compilations of various content such as **VBA, JScript, Java and ActiveX.**
With application whitelist software, the execution of such **uncommon script extensions** can be **prevented** or **detected**.

It is recommended to **disable/remove** the security vulnerabilities of applications that are **not needed in-house.**
In order to prevent **phishing attacks** via e-mail, it is important to position **Sandbox-derived** technologies and **Email Security Gateway** products, and to make **security updates** of used **application inventories** at regular intervals

17. TACTICS

5. DISCOVERY

The adversary is trying to figure out your environment.

Discovery consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act. They also allow adversaries to explore what they can control and what's around their entry point in order to discover how it could benefit their current objective.
Native operating system tools are often used toward this post-compromise information-gathering objective.

97% of the attacks made using the Discovery tactic can be detected by our **ADEO MDR Service**.

The existing environment in the institutions (with the help of **Active Directory, Firewall, Network Segmentation** and other security devices, if any) should be tightened in accordance with the needs and **the attack surface should be narrowed.**
It is recommended to tighten and mature the **Audit** and **Log levels** running on the environments.

In order to prevent the risk of discovery and possible exploitation, asset inventories should be examined periodically, making sure that **unnecessary ports, services and services are closed.**
It is recommended to use **IPS/IDS technologies** to detect and prevent remote service scans.

Many important information is also available through Windows Management Instrumentation and Windows system management tools such as PowerShell.
Windows event logs must be configured and collected centrally to identify such actions that can be taken to gather system and network information.

Security updates of applications in asset inventory should be checked periodically.

User account management should be provided and the **minimum privilege policy** should be applied.

17. TACTICS

6. EXECUTION

The adversary is trying to run malicious code.

Execution consists of techniques that result in adversary-controlled code running on a local or remote system.
Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

96% of the attacks made using the Execution tactic can be detected by our **ADEO MDR Service.**

By opening a malicious file or link, the user can be subjected to a social engineering attack to execute malicious code.
In order to prevent such attacks, it is necessary to **regularly check and update the e-mail or internet browser applications** on the end user's side.

Visibility on network traffic should be increased with NGFW or NDR products to prevent or detect attackers from **exploiting RCE vulnerability**.

The existing environment in the institutions **(with the help of Active Directory, Firewall, Network Segmentation and other security devices, if any)** should be tightened in accordance with the needs and the **attack surface** should be narrowed. It is recommended to tighten and mature the **Audit** and **Log** levels working on the environments and to use **SIEM** technologies.

An **RCE vulnerability** that can be found on **open servers** will allow the attacker to easily enter the corporate network.
With the **Zero Trust** security strategy, **access from external servers** to internal or other servers should **be limited and monitored by network access control (NAC) tools.**

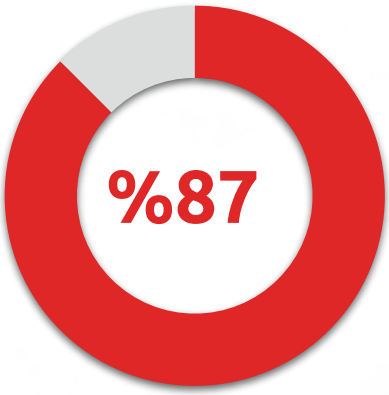
17. TACTICS

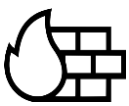
7. EXFILTRATION

The adversary is trying to steal data.

Exfiltration consists of techniques that adversaries may use to steal data from your network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption. Techniques for getting data out of a target network typically include transferring it over their command and control channel or an alternate channel and may also include putting size limits on the transmission.

87% of the attacks made using the Exfiltration tactic can be detected by our **ADEO MDR Service.**





For data to leave the network, it must pass through a designed exit point.
- **A next-generation firewall (NGFW)** with signature-based antivirus features typically useful for C2 detection **can help detect or prevent an infiltration.**
- **A network intrusion prevention system (IPS)** that can see traffic protocols **can help detect and prevent leakage.**

DLP monitors the unauthorized access and use of sensitive data by the user. It is recommended to use it as it **prevents data from coming out.**

Attackers spread over the network by running malicious code **over USB**. In some cases, **data hijacking can occur via a user-identified USB device**. The USB device can be used as the last data evasion point or otherwise to switch between disconnected systems. In order to prevent this, it is recommended to **disable the usb ports** in **low awareness areas**.

Instead of sending data in one piece, an attacker can **send files in pieces.** In this way, it ensures the transmission of data without exceeding the minimum upload size. **Continuous monitoring of network traffic** is recommended to prevent an attack.

17. TACTICS

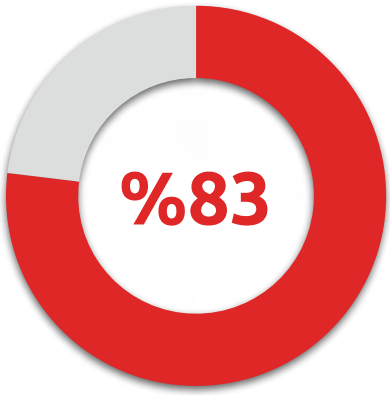
8. IMPACT

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

83% of the attacks made using Impact tactic can be detected by our **ADEO MDR Service.**



Ransomware can encrypt data on target systems or multiple systems in a network **to cut off access** to system and network resources.
In order to prevent attacks, it is recommended to **prepare backups** by preparing **disaster scenarios** and make these backups inaccessible to attackers.

A denial of service attack results in a successful **DDoS** attack when the attacked resource is exposed to requests from multiple machines and does not respond by exceeding its capacity. **To prevent DDOS**, it is recommended to filter traffic and take **DDoS prevention service** provided by **Content Delivery Networks (CDN)** or providers specializing in DoS mitigation.

Data Manipulation: Attackers can add or delete data, hiding their activities with different results. In this way, they may try to influence a business process, organizational understanding, or decision-making by manipulating their competitor's data. It is recommended **to use data encryption, storage method** and **DLP** solutions to prevent financial losses that may occur.

Man in the Middle attack is an attack method that takes place in the form of interception of various data by listening to the communication between two connections in the network or manipulating the data by listening to the communication and creating a misleading communication. In order to prevent **Mitm** attack types, it is important to use **SSH**, **IPSec** protocols, **HTTPS** supported sites, and not to connect to unencrypted **WIFI** networks shared in public environments.

17. TACTICS

9. PERSISTENCE

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

96% of the attacks made using the Persistence tactic can be detected by our **ADEO MDR Service.**

NDR gives you transparency on all connections and protocols. It deeply scans traffic and performs retrospective analysis to analyze connections, streams, packets and metadata in real time.
To minimize the resolution time of a detected threat, it is recommended to use an **integrated network detection and response solution.**

Prevention: It is important to have a weekly **malware scan** for all devices on the network. In addition, **security breach analysis and evaluation (Compromise Assessment)** studies should be carried out at regular intervals.

By running **remote commands on assets** that contain various vulnerabilities, **system shutdown/restart**, attackers can cause data corruption, material damage and loss of life in environments and places such as e-commerce and hospitals.
It is recommended to **use Extended Detection and Response (XDR), Firewall, Backup** technologies to prevent these and similar types of attacks.

Downloads such as **fake/cracked** programs, games operating systems can make your system the target of serious attacks. It may expose institutions to attacks such as ransom, data breach, and backdoor. These and similar attacks are usually caused by **low user awareness**. For this reason, it is recommended to give **basic safety training to employees at regular intervals.**

17. TACTICS

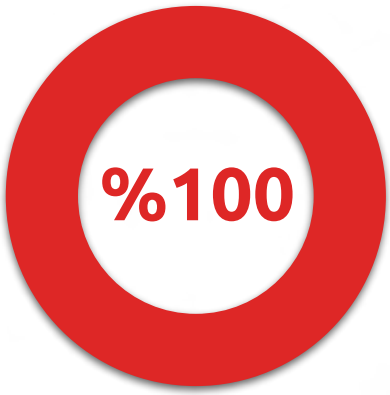
10. PRIVILEGE ESCALATION

The adversary is trying to gain higher-level permissions.
Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Examples of elevated access include:

- SYSTEM/root level
- local administrator
- user account with admin-like access
- user accounts with access to specific system or perform specific function.

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.



100% of the attacks made using the Privilege Escalation tactic can be detected by our **ADEO MDR Service.**

Logs from directory servers such as **Active Directory (AD)** or **LDAP** need to be configured. User rights upgrade or new user creation events need to be followed.
It is necessary to create a list of privileged user account names, authorizations. Privilege Escalation attacks or attacks against privileged users can be detected using **Identity-based Security** products.

Privileged access rights need to be reviewed at appropriate intervals (at least once a month) and the assignment of **privileged permissions should be reviewed regularly.**
All privileged access to files and databases (including local system access) must be monitored. The alarm mechanisms of critical privileged user changes should be **instantly shared with the relevant IT managers** by creating Mail-SMS.

Make sure that users have **directory access control set up** to reduce places where **malicious files** can be placed for execution. It is recommended that all executables be placed in **write protected** directories.

It is important to detect **security vulnerabilities** before attackers take advantage of these vulnerabilities. An effective **scanning process with vulnerability scanning tools; reveals system misconfigurations, weak passwords, and weaknesses in Web Server Security.**

For keeping threat vectors away from institutions with effective vulnerability scanning it is important to **update, patch or deploy additional layers of security.**

17. TACTICS

11. INITIAL ACCESS

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network.

Techniques used to gain a foothold include targeted spear phishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

100% of the attacks made using the Initial Access tactic can be detected by our **ADEO MDR Service.**

It is important that users do not use their passwords on social networks and other platforms when setting a password. The change interval of passwords should be **between 1 and 3 months**. It must contain special characters and have a **minimum of 14 characters.**
Unnecessary authorization should be avoided during **account authorization**. It is important to **close the accounts of the dismissed employee.**

URL analysis (including expanding shortened links) within the email can help detect links to known malicious sites.
Sandbox solutions can be used to detect these links and detect malicious behavior by automatically accessing these sites or to wait and capture content if a user visits the link.

It is necessary to **collect authentication logs** and detect unusual / unauthorized access outside of normal working hours.

It is important to update the used application asset inventories (web browsers, components, plug-ins, office and media etc.) on a **regular basis.**
Network traffic classified as malicious by **threat intelligence sources should be blocked and alerts should be created.**

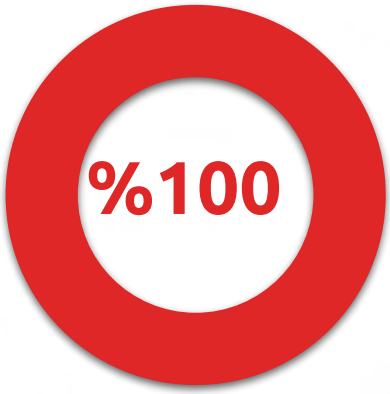
17. TACTICS

12. LATERAL MOVEMENT

The adversary is trying to move through your environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain.
Adversaries might install their own remote access tools to accomplish Lateral Movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

100% of the attacks made using the Lateral Movement tactic can be detected by our **ADEO MDR Service.**

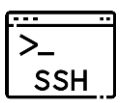


Lateral movement techniques may be legitimate depending on the network environment and how they are used. Factors such as files accessed or activities occurring after a **remote login (RDP)** may indicate suspicious or malicious behavior associated with this activity. It is recommended to monitor user accounts logged into systems that would **normally not be able to access** multiple systems in a relatively short time.

By isolating **VLAN** networks from each other, it prevents the spread of attacks and data breaches.
Restricting the systems or services accessed by **VPN** will keep the internal spread to a minimum in case VPN accounts are compromised.

If the use of **WinRM** is not common by system teams, it should be disabled. If widely used, **Windows event logs** should be configured and centrally collected on **SIEM**.
Suspicious accesses should be detected through these logs collected with the written rules.

The use of **SSH** may be legitimate depending on the network environment and how it is used. Other factors, such as activity after remote login, may indicate **suspicious** or **malicious behavior**. It is **necessary to monitor user accounts** logged into systems that would normally not be able to access multiple systems in a relatively short time.



18. DISTRIBUTION OF ATTACK DETECTION BY OPERATING SYSTEMS

As ADEO MDR Service, we have **4000+** detection rules for **Windows**, **Linux**, **MacOS** operating systems and derivatives (Windows Server, Workstation, Centos, Unix, Debian, Ubuntu based etc.).

The distributions of the developed detection rules are **3563 rules in Windows** operating system, **719 rules in Linux** and **695 rules in MacOS**.

The detection rules we developed cover an average of **94%** of the Tactical, Technical, Procedures (TTP*) created for all Linux, MacOs, Windows-based operating systems in the MITRE ATT&CK® Framework.

In this way, we are able to support all our customers with a detection rate of over **96%** for **3 operating systems** and their derivatives.

"We are able to support all our customers with a detection rate of over 96% for 3 operating systems and their derivatives."

Windows

3500+

LINUX

700+

MacOS

650+

**TTP:*
An abbreviation for Techniques, Tactics and Procedures used to describe/describe the operation of a threat actor. TTPs are used to profile a specific threat actor.

19. PREDICTIONS FOR 2023

OT and IoT Systems*:

The fact that both industrial systems and technology continue to develop without slowing down brings some dangers along with their convenience.

OT (Operational Technology systems) and IoT (Internet of Things) are in a structure that can be dangerous in terms of cyber security.

For example; A cyberattack was conducted in Florida using the remote access platform known as Team Viewer.
Cyber attackers broke into the water treatment system and multiplied the values of various components, such as sodium hydroxide. If the attack had not been noticed, people could have been poisoned.

OT and IoT systems, which are one step behind in security compared to other sectors, according to the motivations of cybercriminals, seem to be the target of attacks in the future.

"It is known that technologies such as OT (Operational Technology Systems) and IoT (Internet of Things) have recently been seriously affected by cyber attacks, and even special attack techniques targeting these technologies have been developed."

**Operational Technology (OT):*
It refers to computer systems used to manage industrial operations as opposed to administrative operations. OT can also be defined as a category of hardware and software that monitors and controls how physical devices work.
Businesses with process systems and/or storage and distribution systems use a completely different network and device structure than IT. It is difficult at first glance to understand the difference of this structure because the same device, switch, cable and routers are used. This structure, which consists of PLCs, controllers, sensors, operator stations, is called OT (Operational Technology).

You can contact us to get detailed information about our ADEO MDR Services and to forward your questions.

info@adeo.com.tr

19. PREDICTIONS FOR 2023

End User Security:

Every new day in cyberspace can herald a vulnerability or a new attack technique.
Although zero-day attacks set the agenda and attract the attention of cyber attackers, traditional methods still remain valid.

The ransomware group, which was newly released in 2022 and became known as "Black Basta" by drawing attention with its attacks, attacked companies using spear phishing as the first access technique.

With phishing attacks, the mail and password information of the employees of the institution are seized and put up for sale on hacker forums.
Ransomware groups also buy this sensitive information about the organization they are targeting and design the attack scenario accordingly.

For this reason, it is of great importance for corporate employees to gain awareness of cyber security today.
Especially ;

- Renewing passwords periodically,
- Conducting social engineering tests in order to raise awareness of the end user and
- Not neglecting two-factor authentication

will help protect against cyber attacks.

"With phishing attacks, the mail and password information of the employees of the institution are seized and put up for sale on hacker forums. Ransomware groups also buy this sensitive information about the organization they are targeting and design the attack scenario accordingly."

You can contact us to get detailed information about our ADEO MDR Services and to forward your questions.

info@adeo.com.tr

19. PREDICTIONS FOR 2023

Zero-Day Vulnerabilities:

In our report, we mentioned some zero-day vulnerabilities that were newly released in 2022 and made a name for itself.

It is very important to follow the agenda, pass the patches released by the manufacturers against new security vulnerabilities, and follow the anomaly activities in systems with vulnerabilities.

Even after the patch is released for the security vulnerabilities affecting the email servers, we see that various bypass methods are used.

Attackers target servers while providing access to unpatched, vulnerable systems and will try to access the patched systems with various bypass methods.

In addition to e-mail servers, new vulnerabilities can also be exploited in Active Directory certificate services, which can be used to ensure post-access persistence and increase authority.

We think that the use of security vulnerabilities related to e-mail servers and certificate services may increase in 2023.

"We think that the use of security vulnerabilities related to e-mail servers and certificate services may increase in 2023."

19. PREDICTIONS FOR 2023

What ChatGPT Says?

a What cyber security attacks can happen in 2023

As an AI language model, I cannot predict future events with complete accuracy, and the nature and severity of cyber attacks cannot be foreseen. However, based on current trends and emerging threats, some potential cybersecurity attacks that could occur in 2023 could include:

1. Zero-day exploits: These are vulnerabilities in software that are unknown to the software vendor and therefore unpatched. Cyber attackers could use such exploits to gain unauthorized access to systems or steal sensitive information.
2. Internet of Things (IoT) attacks: As more devices become connected to the internet, the risk of IoT-based attacks increases. These attacks could exploit vulnerabilities in IoT devices to gain access to networks and steal data.
3. AI-powered attacks: Cyber attackers could use artificial intelligence to launch sophisticated attacks that bypass traditional security measures. AI could be used to automate attacks, evade detection, and identify vulnerabilities in target systems.
4. Supply chain attacks: These are attacks that target the software or hardware supply chain, with the aim of compromising the security of a larger network. For example, attackers could inject malware into a legitimate software update that is then distributed to multiple users.
5. Phishing and social engineering attacks: These are attacks that exploit human behavior to trick users into giving away sensitive information or granting access to systems. Cyber attackers could use increasingly sophisticated techniques to create convincing phishing emails or other social engineering tactics.

To mitigate the risk of these and other cyber attacks, it's essential to implement strong security measures, stay informed about emerging threats, and continuously monitor and improve cybersecurity practices.

“The important thing is to continue to take cybersecurity measures and be vigilant during your online activities.”

20. RECOMMENDATIONS #TOP5

1 In order to prevent a possible attack, the institution must be monitored **7x24x365** days with the **MSSP*** or **MDR** service.

2 It is important to **activate dual authentication MFA**, avoid unnecessary authorization, and take preventive measures in places where awareness is low.

3 In order to increase detection capabilities, it is primarily important to **increase visibility**. The **rules and correlations** that will detect the relevant attacks must be **constantly updated.**

4 Despite possible cyber incidents, an up-to-date action plan should be created and the **simulations** should be repeated periodically to keep **awareness** and preparations **up-to-date.**

5 It is necessary to examine the **asset inventories** at certain periods and provide the control of **outsourced services.**

20. RECOMMENDATIONS

- It is **important to fully monitor** the visibility and tightening of all **IT and OT systems.**
- Rather than purchasing automated products and software, systems, **human-based services** or **investments in people** in cyber security teams need to be increased.
- It should be ensured that the **Red Team** and **Penetration Test** activities are carried out by expert teams at regular intervals.
- It should be kept in mind that most of the attacks are caused by newly discovered vulnerabilities. Starting from here, it is important that the **"Vulnerability Management"** procedures are applied continuously and that they are strictly followed.
- Giving **practical awareness training** to users and employees against **phishing attacks** at certain intervals is beneficial in preventing human-induced attacks.
- It should be ensured that the **Purple Team*** actions for measuring the maturity level of cyber security teams are taken by expert teams.
- The existing **environment** in the institutions (Active Directory, Firewall, Network Segmentation and other security devices, if any) should be tightened in accordance with the needs and **the attack surface should be narrowed.**

**PURPLE TEAM:*
The Purple Team is the cooperation and collaboration of the Red Team and the Blue Team. It is aimed to develop the skills and processes of both the Red Team and the Blue Team.

21. NEW MEMBERS OF THE PRODUCT FAMILY

New Member of Product Family Crowdstrike

Rules were developed for Crowdstrike, which was added to the product family of ADEO MDR Service.
500+ rules were added to the product.

MDR is Stronger with SOAR

SOAR (Security Orchestration Automation and Response) technology is at the heart of our MDR service.

This product, which enables to execute, coordinate and automate tasks among various tools on a single platform; at the same time, is a solution that helps us to use our existing human power more effectively.

Resilience with SIMSPACE

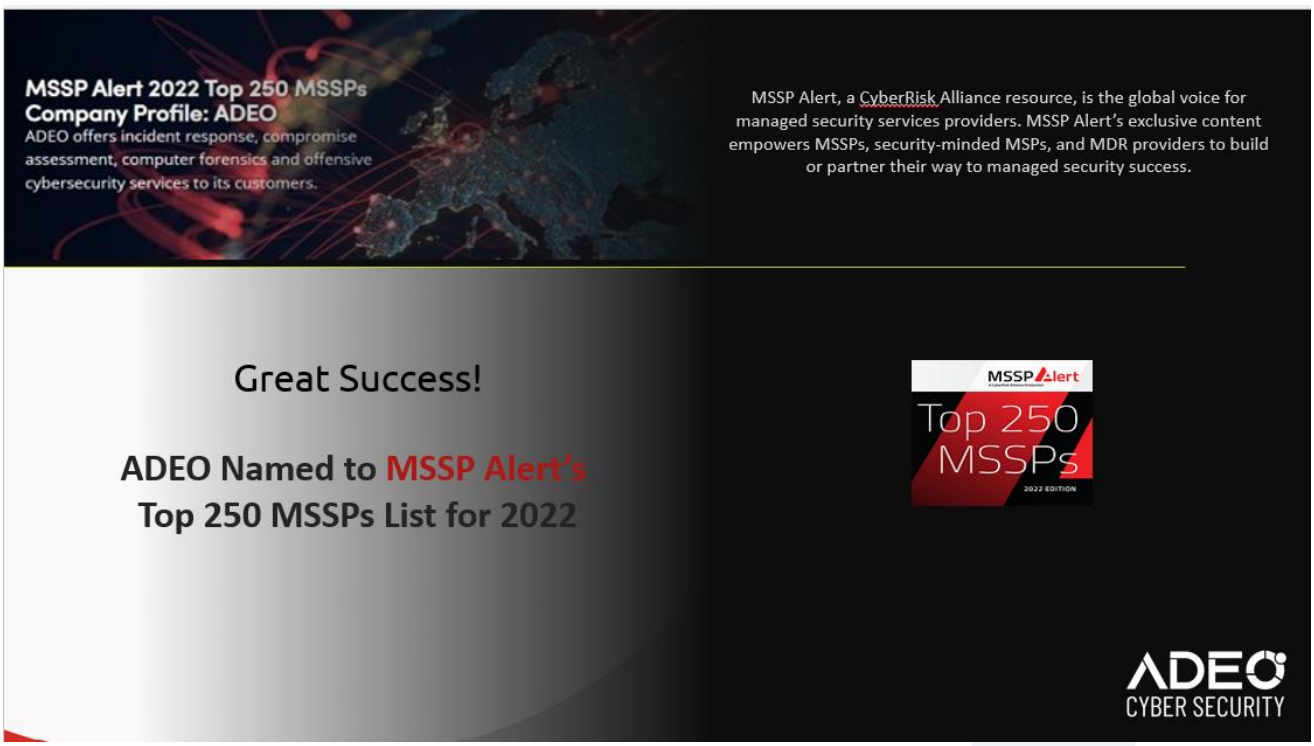
ADEO cyber security teams conduct drills against known and current threats on the Simspace Training Simulation and drill environment with which they have partnered. Build tools, processes and teams against advanced attacks and provide optimized cyber resilience with Simspace.

New Member of Product Family Cybereason

Rules have been developed for Cybereason, which has been added to the Product family of ADEO MDR Service.
Developed **50+ rules** have been added to the Product.

22. ADEO in 2022

**MANAGED SECURITY SERVICE PROVIDERS(MSSP):*
MSSP is a type of service provider that provides remote software/hardware-based information or network security services to an organization. An MSSP hosts, deploys, and manages a security infrastructure by providing information security (IS) services to one or more clients simultaneously.



22. ADEO in 2022

ADEO Cyber Security became a member of the Microsoft Intelligence Security Association (#MISA), led by Microsoft, which brings together manufacturers and service providers who have a say in the cyber security industry.

"Thanks to our MISA membership, we have the chance to publish our 2 important services to Marketplace. Our managed SOC and MDR services have become available to regions that we can deliver through the Marketplace."

22. ADEO in 2022

23. Contact Information

For detailed information about our MDR Service

You can contact as via

mdr@adeo.com.tr

Istanbul

Fetih Mah. Tahralı Sk.
Tahralı Sitesi Kavakyeli Plaza
C Blok D16/17
Ataşehir / İSTANBUL / TÜRKİYE

Phone: +90 (216) 472 35 35
Fax: +90 (216) 472 35 36

Ankara

Kabil Cad. (Eski 4.Cad)
1335. Sokak No:58 D:9-10
Aşağı Öveçler
Çankaya / ANKARA / TÜRKİYE

Phone: +90 (312) 482 12 35
Fax: +90 (312) 482 12 36

Email: info@adeo.com.tr

adeo.com.tr
mxdrturkiye.com

/adeosecurity /adeodfir
/adeocomtr

/ADEOcomtr

/ADEO Cyber Security Services

/adeocomtr

ADEO CYBER SECURITY