MANAGED DETECTION AND RESPONSE SERVICE REPORT 2021

TABLE OF CONTENTS

1) SCOPE OF WORK

Managed Detection and Response Services (MDR) are efforts to detect and respond to cyber attacks as quickly as possible.

With the help of technologies that are positioned in-house within the scope of MDR service which increase visibility at the end point, all the details of a cyber incident that may occur can be obtained and the damage can be minimized.

These tools ensure that the attacks detected by the MDR team are highly accurate and it provides a detailed view of what happened before and after the relevant cyber incident. Using these technologies help to plan what to do immediately after a cyber attack to prevent it quickly.

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 great importance in the response of advanced cyber attacks.

Through to the detailed records provided by the technologies used by the MDR teams and the processes operated, the root cause of a cyber attack can be determined very quickly.
This situation plays a key role in quickly preventing the current attack and determining the actions to be taken to prevent similar ones from happening.

ADEO MDR SERVICE

WHAT WE DID IN 2021?

3) 2021 STATISTICS

Busiest Day: **17 December**
Number of Alarms reviewed today:

485

Percentage of Alarms Resolved Without Incident Response

%99

ALARM

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

Most Targeted Industries and Their Total Number of Incident

Manufacturing
9 Incident

Communication
5 Incident

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.

Busiest week:**13-19 December**
Number of Incident seen this week:

5

2021 STATISTICS

The number of Detection Rules was increased from **600** in January 2021 to **2,000** at the end of the year.

The number of IOCs, which was **5,000** in January 2021, increased to **20,000** at the end of the year.

Total Number of Rules Developed

2000+

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.

Number of IOCs scanned with threat intelligence provided internally and externally

20K+

Most Used Initial Access Technique Exploit Public Facing Applications

%41

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.

4) DAILY ROUTINE OF MDR SERVICE

96% 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 work flows. The analyzes made and the actions taken are reported and communicated to the customers at certain periods.

An average of **20** 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.

4% 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.

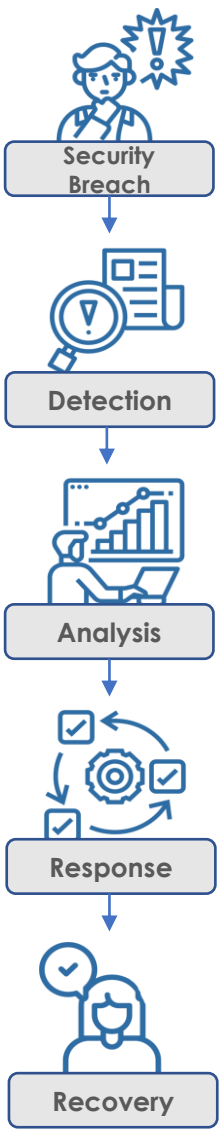
As a result of **detection of malware**, activities are examined with a **threat hunting** approach, machines spreading malware are **isolated** and **necessary actions** are taken.

5) MANAGED DETECTION AND RESPONSE INCIDENT MANAGEMENT STAGES

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 2021 is indicated on page 20.

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 **~4 minutes**.
According to the report published by the Mandiant company in 2021, the average detection time in global incidents was determined as 24 days [1].

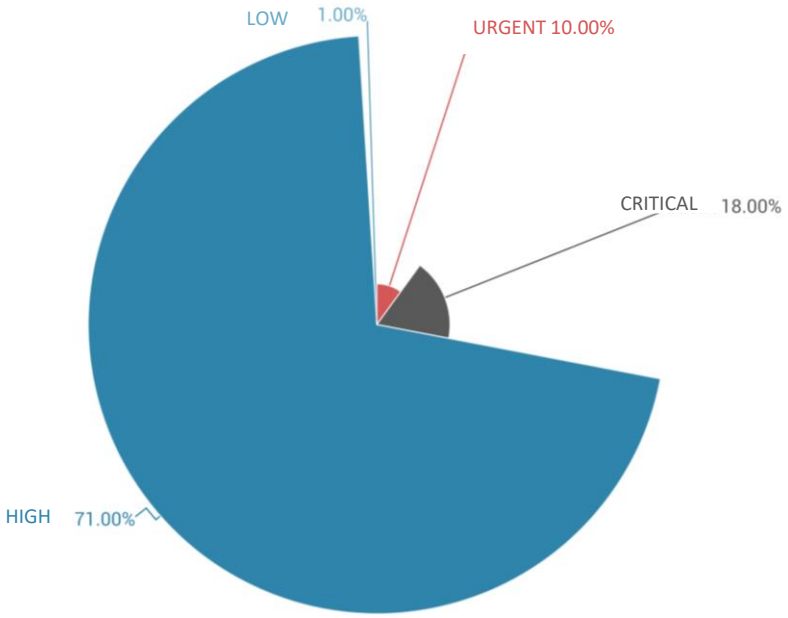
Suspicious activities detected through various security products are examined in detail by **ADEO MDR Analysts 7x24x365 days**.

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 2021, the mean **response time** of ADEO MDR team to **high severity** and **critical** incidents was **1 hour 37 minutes**. According to the report published by IBM in 2021, this period is seen as an average of 287 days in global cases[2].

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

[1] M-Trends 2021, Mandiant
[2] Cost of Data Breach 2021, IBM

6) 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 2022** 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

4m 8s

MEAN TIME TO RESPONSE

1h 37m 8s

While **the mean detection time** of all alarms in 2021 was **1 hour 15 minutes**, **the mean response time** was **4 hours 39 minutes**; the **mean detection time** of only high severity and critical alarms was **4 minutes**, and **the mean response time** was **1 hour and 37 minutes**.

7) DISTRIBUTION OF ALARMS BY INDUSTRY

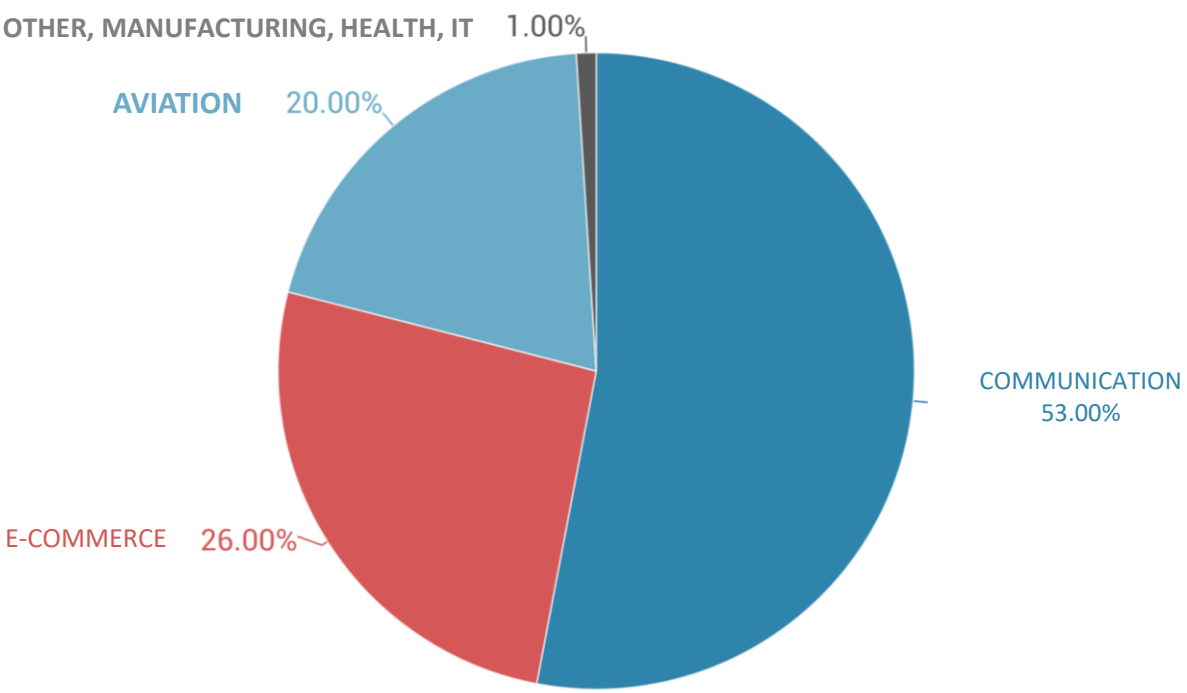
INDUSTRIES WITH MOST ALARM OBSERVATIONS

AVIATION

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.



8) TOP VICTIM INDUSTRIES

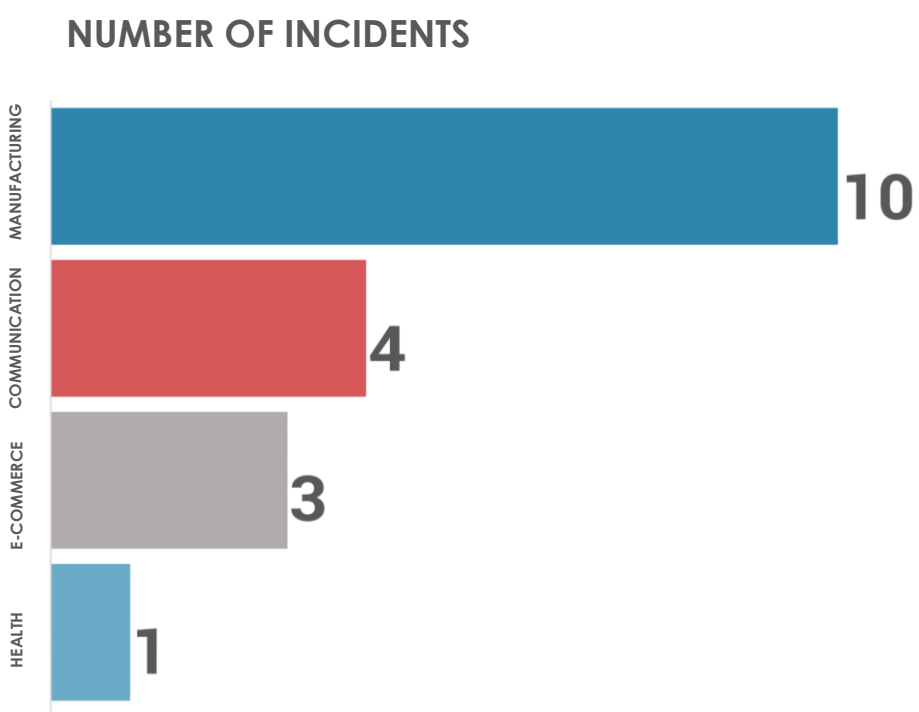
Why Manufacturing

- 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.



9) MOST SIGNIFICANT SECURITY VULNERABILITY IN 2021 & ADEO MDR SERVICE'S DETECTION RULES

The rules we wrote as **ADEO MDR** about the important Top 20+ vulnerabilities published in 2021 and the **number** of **IOCs we added** are shown in the table below. 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.

9) MOST SIGNIFICANT SECURITY VULNERABILITY IN 2021 & ADEO MDR SERVICE'S DETECTION RULES

SECURITY BUG	NUMBER OF CUSTOM RULES WRITTEN	NUMBER OF IOCs ADDED TO PRODUCTS
Apache Log4j Zero-Day Vulnerability	16	3000+
LockBit Ransomware	13	122
Possible InstallerFileTakeOver LPE | Zero-Day Vulnerability	13	4
PetitPotam - NTLM Relay Attack	13	5
Emotet Botnet | TrickBot Malware	12	300
Microsoft Exchange ProxyShell Attack	11	39
LockFile Ransomware & ProxyShel	10	13
Web Shell Attack	10	48
Microsoft MSHTML Remote Code Execution Vulnerability	10	235
PrintNightmare aka SeriousSAM Vulnerability	9	24
macOS Finder RCE Zero-Day	9	4
Coronavirus Phishing & Malware	7	233
Windows Print Spooler Remote Code Execution Vulnerability	7	340
FiveHands Ransomware	6	50
Angry Conti Ransomware	5	30
Cobalt Strike Defender's	5	120
Revil Kaseya Ransomware Attack	5	1282
Razer MauseCVE-2021-30494	5	5
DarkSide Ransomware	4	28
BazarLoader Malware	3	50
Ryuk Ransomware	3	545

10) MOST SIGNIFICANT SECURITY VULNERABILITY IN 2021& AVERAGE EXPOSURE TIME OF VULNERABILITY IN ORGANIZATIONS

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.

The table below shows **statistical data showing** that the relevant security vulnerability is attempted to be exploited on existing customer systems within a **minimum of 1 day** and a **maximum of 1 week.**

SECURITY BUG	AVERAGE EXPOSURE TIME OF VULNERABILITY IN ORGANİZATIONS
Apache Log4j Zero-Day Vulnerability	2 DAYS
Possible InstallerFileTakeOver LPE | Zero-Day Vulnerability	3 DAYS
PetitPotam - NTLM Relay Attack	2 DAYS
Emotet Botnet | TrickBot Malware	4 DAYS
Microsoft MSHTML Remote Code Execution Vulnerability	3 DAYS
PrintNightmare aka SeriousSAM vulnerability	1 WEEK
Coronavirus Phishing & Malware	1 DAY
Razer MauseCVE-2021-30494	1 WEEK
macOS Finder RCE Zero-Day	2 DAYS

MOST SIGNIFICANT SECURITY VULNERABILITY IN 2021& AVERAGE EXPOSURE TIME OF VULNERABILITY IN ORGANIZATIONS

Apache Log4j Zero-Day Vulnerability

2 DAYS

Possible Installer File Take Over LPE | Zero-Day Vulnerability

3 DAYS

PetitPotam - NTLM Relay Attack

2 DAYS

Emotet Botnet TrickBot Malware

4 DAYS

Emotet

Microsoft MSHTML Remote Code Execution Vulnerability

3 DAYS

Microsoft MSHTML

PrintNightmare aka SeriousSAM Vulnerability

1 WEEK

Coronavirus Phishing & Malware

1 DAY

Razer Mause CVE-2021-30494

1 WEEK

macOS Finder RCE Zero-Day

2 DAYS

11) MOST IMPORTANT TOPIC OF THE YEAR #1 LOG4J

MOST IMPORTANT TOPIC OF THE YEAR #1 LOG4J

ADEO MDR SERVICE

1

Why were we so busy during the week of 13-19 December?

It was the week that Log4j was released, and due to the wide attack surface of this vulnerability, threat hunting works were carried out based on the asset inventories of all customers, and special reports were prepared for our customers.

A total of 5 cases were seen this week. These 5 cases correspond to approximately 25% of the annual number of cases.

2

What kind of research has been done for the log4j vulnerability?

In order to detect Log4j, ~3000 IOCs were collected and analyzed from globally published reports and threat intelligence platforms and added to our customers' products.

3

How long did we update the detection rules we created?

As the MDR service, we animated the Log4j vulnerability in our own laboratory environments and used different patterns to detect the related vulnerability. A total of **16 detection rules** were written and transferred to all our customers within **5 hours**.

4

What is the time of occurrence of Log4j vulnerability in institutions and what are the actions taken?

Two days after we added the custom rule sets we created for Log4j and the IOCs we gathered from threat intelligence platforms to our customers; real positive alarms were received about the related vulnerability and MDR Analysts took action to **prevent exploitation of the vulnerability**.

12) MOST IMPORTANT TOPIC OF THE YEAR #2 Lockbit Ransomware

ADEO MDR SERVICE

1

LOCKBIT ?

LockBit ransomware is malware 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"**. The software has so far targeted organizations in the **US**, **China**, **India**, **Indonesia**, and **Ukraine**. In addition, attacks were seen in many countries (France, United Kingdom, Germany) across Europe.

2

Lockbit Back in the Field with 2.0

In July 2021, LockBit 2.0 released an update that enables automatic encryption of devices in Windows domains by abusing Active Directory group policies. According to the FBI statement, **in August 2021**, LockBit 2.0 agreed with the employees of the institution to establish **the initial access** to the potential victim networks, **promising to share a portion of the profit with the people who support the group** if the attack was successful.

3

2021 Activities of Lockbit 2.0

June: Observed the creation and use of StealBit, the malware that automates data exfiltration with the fastest and most efficient encryption.

August: Creation and exploitation of StealBit, the malware that automates data exfiltration with the fastest and most efficient encryption, observed.

October: Release of LockBit targeting Linux and VMware ESXI hypervisor admin platforms.

4

How long did we update the detection rules we created?

As the MDR service, we animated the Lockbit 2.0 vulnerability in our own laboratory environments and used different patterns to detect the related vulnerability. A total of **13 detection rules and 122 IOCs** were transferred to all our customers within **6 hours**.

LOCKBIT 2.0

13) MOST IMPORTANT TOPIC OF THE YEAR #3 PrintNightmare

ADEO MDR SERVICE

1

What is PrintNightmare Vulnerability?

On June 29, 2021, a Windows **ZeroDay** vulnerability, codenamed **PrintNightmare**, was mistakenly disclosed on the public GitHub repository by security researchers at Sangfor Technologies.
Print Nightmare is a critical vulnerability that affects the Microsoft Windows operating system.

2

What are the effects of the PrintNightmare vulnerability?

The vulnerability occurs in the print spooler service and allows a remote authenticated login with SYSTEM-level privileges to execute malicious code. This vulnerability allows **creating new users, installing malware, and modifying or deleting data on systems with full user rights**.

3

How long did we update the detection rules we created?

As the MDR service, we used different patterns to simulate the PrintNightmare vulnerability in our own laboratory environments and to detect the related vulnerability. A total of **9 detection rules** developed and **364 malicious IOCs** collected from various global CTI sources were transferred to all our customers within **4 hours**.

4

When was the PrintNightmare vulnerability discovered and what are the actions taken?

One week after we added the custom rule sets we created for PrintNightmare and the IOCs we collected from threat intelligence platforms to our customers, we received real positive alerts about the related vulnerability and MDR Analysts took action to prevent exploitation of the vulnerability.

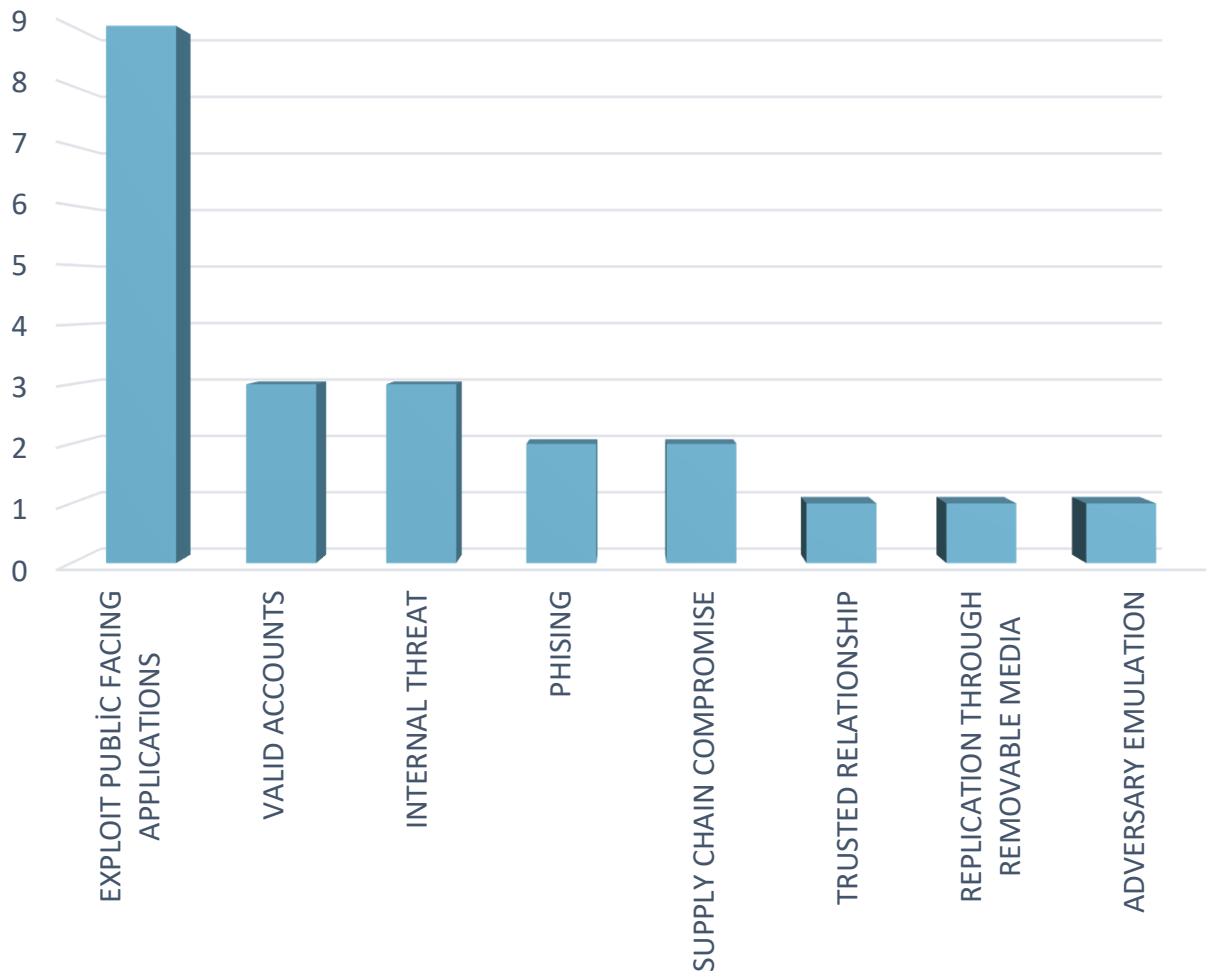
14) MOST POPULAR INITIAL ACCESS TECHNIQUES

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.

The Attack Simulation title in the graphic below refers to the Red/Purple Team activity. Therefore, it does not include a real first access tactic.



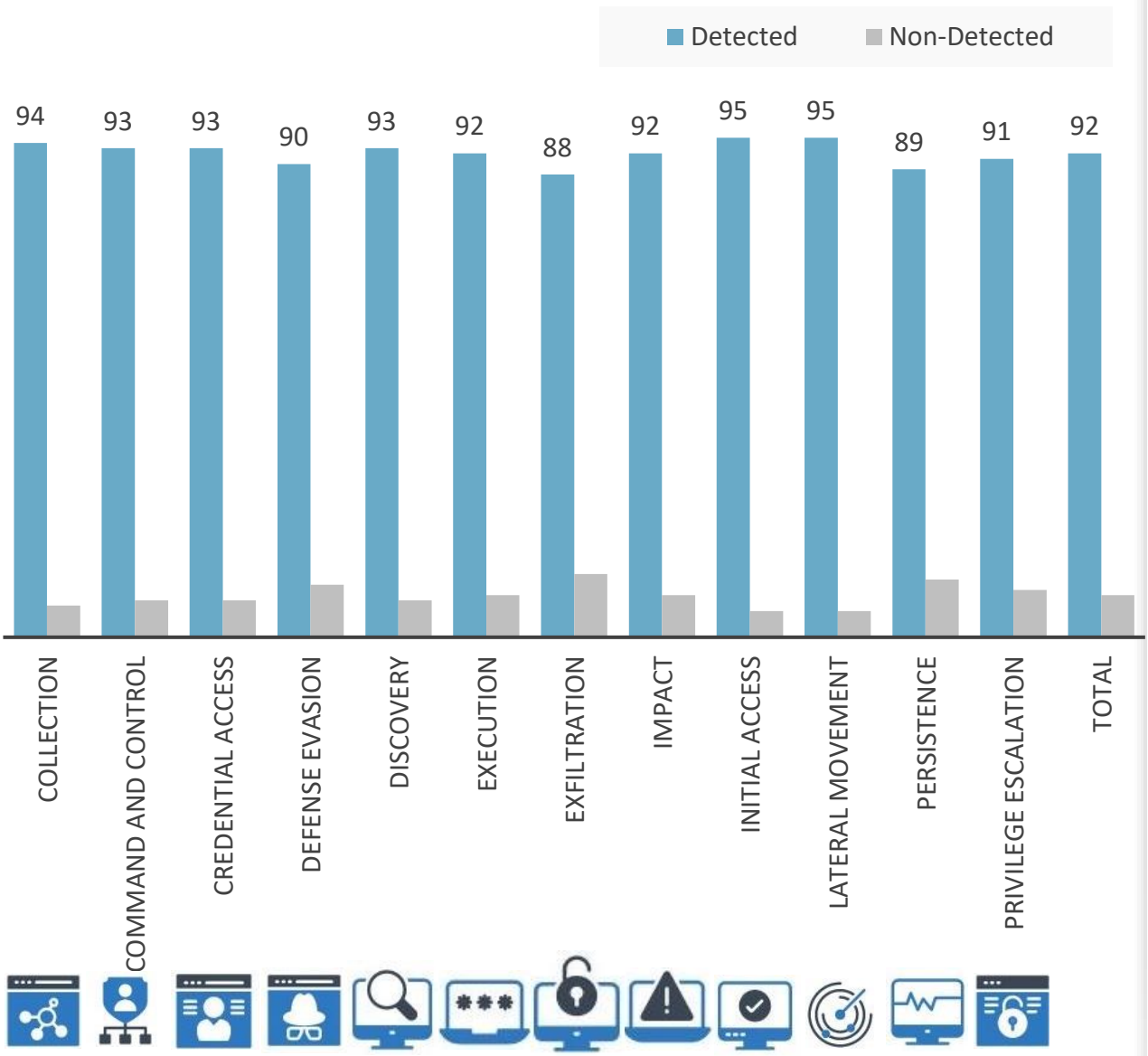
ADEO MDR SERVICE

TACTICS, TECHNIQUES&DETECTION RULES

16) OUR ATTACK 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.

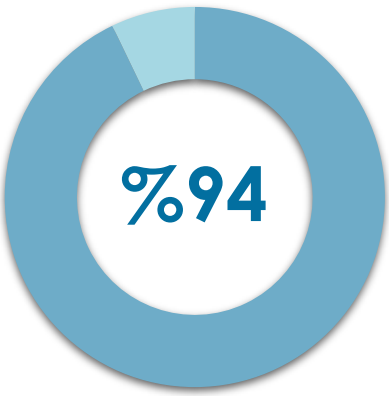
As a result of the security tests performed by MDR Service, it has been reported that **96.6% of ~1000 techniques can be detected** via **EDR**. Of the ~100 undetected techniques, **only 30 were observed to be detectable by EDR.**



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.



94% 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).

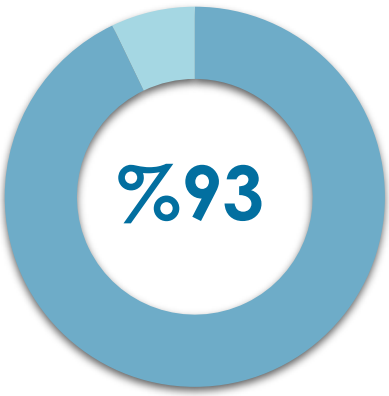
It is important to organize **awareness trainings** at regular intervals in order to increase user awareness.
It is recommended to keep the **system images and software used up-to-date.**

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.

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.



93% of 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.

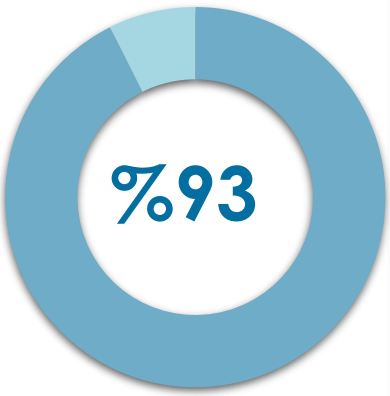
It is necessary to **monitor the traffic** in the network and to **constantly check** the IP's going from inside to outside and coming from outside with **intelligence services**.

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.

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.



93% of attacks 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.

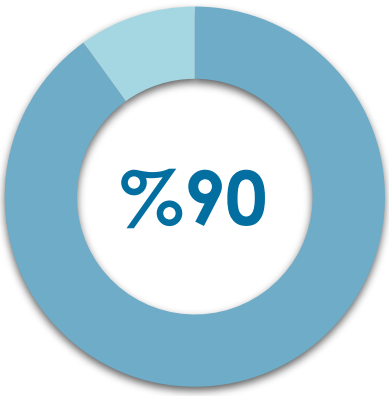
It is recommended to place **Privileged Access Management (PAM)** products within the organization in order to securely manage the accounts of users with access permissions to critical resources.
It is important to **activate MFA** in all possible logins, especially VPN and E-mail access.

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.

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.



90% 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**.

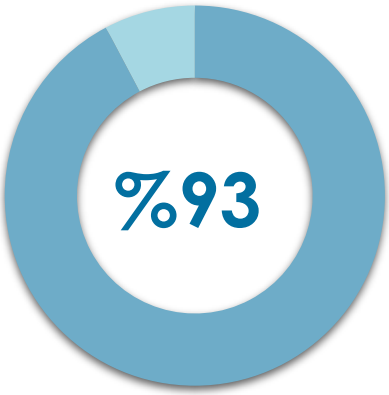
It is recommended to **disable/remove** the security vulnerabilities of applications that are **not needed in-house**.
In order to prevent **phishing attacks** via e-mail, it is important to position **Sandbox-derived** technologies and **Email Security Gateway** products, and to make **security updates**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

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.



93% of attacks 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.

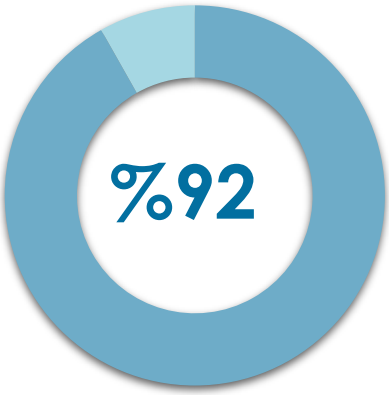
User account management should be provided and the **minimum privilege policy** should be applied.

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.



92% of attacks 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.

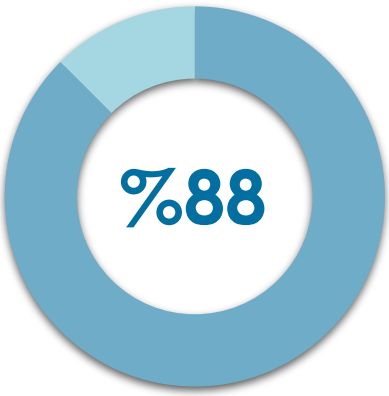
An **RCE vulnerability** that can be found on **open servers** will allow the attacker to easily enter the corporate network.
With the **Zero Trust** security strategy, **access from external servers** to internal or other servers should **be limited and monitored by network access control (NAC) tools.**

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.



88% of 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.

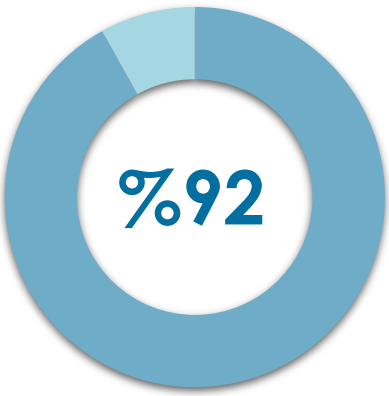
TACTICS

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.



92% of attacks 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.

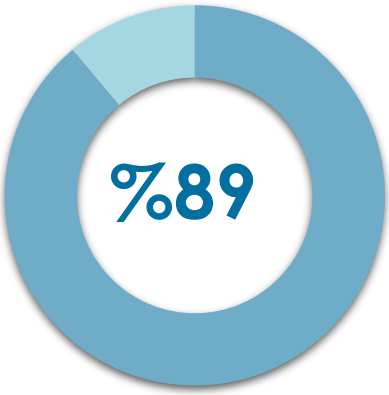
TACTICS

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.



89% of attacks 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.

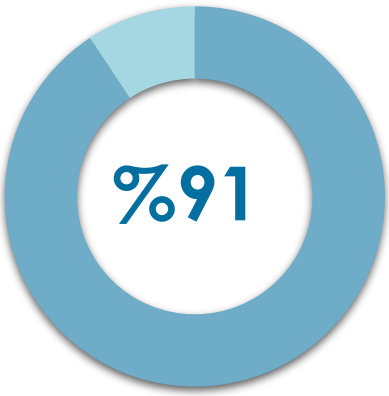
By running **remote commands on assets** that contain various vulnerabilities, **system shutdown/restart**, attackers can cause data corruption, material damage and loss of life in environments and places such as e-commerce and hospitals.
It is recommended to **use Extended Detection and Response (XDR),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

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.

91% of attacks 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.**

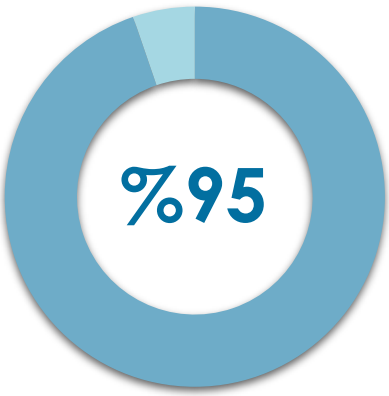
TACTICS

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 spearphishing 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.



95% of attacks 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.

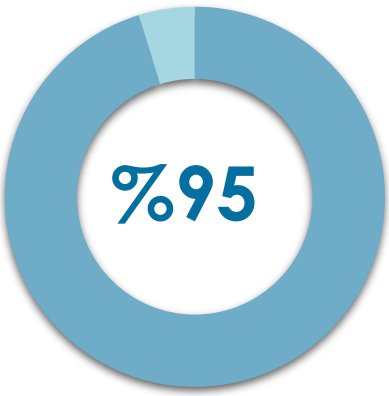
It is important to update the used application asset inventories (web browsers, components, plug-ins, office and media etc.) on a **regular basis.**
Network traffic classified as malicious by **threat intelligence sources** should be **blocked** and **alerts should be created**.

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.



95% of attacks 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 **2000+** 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 **1632 rules in Windows** operating system, **411 rules in Linux** and **407 rules in MacOS**.

The detection rules we developed cover an average of **93%** 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 **95%** for **3 operating systems** and their derivatives.

1600+ **400+** **400+**

19) RECOMMANDATIONS

- In order to prevent a possible attack, the institution **must be monitored 7x24x365** days with the **MSSP** or **MDR** service.
- It is important to **activate** dual authentication **MFA**, avoid unnecessary authorization, and take preventive measures in places where awareness is low.
- 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**.
- 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.
- 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**.
- It should be ensured that the **Purple Team** actions for measuring the maturity level of cyber security teams are taken by expert teams.
- It is necessary to examine **the asset inventories** at certain periods and provide **the control** of **outsourced services**.
- 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**.

20) DEFINITIONS

MDR (Managed Detection and Response)

MDR is the service where the processes required to detect and respond to cyber attacks as quickly as possible are determined and managed.

It covers real-time detection of cyber incidents, taking quick action regarding these attacks, and revealing what needs to be done to prevent similar ones from happening.

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.

ALARM

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

DEFINITIONS

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.

TRUE POSITIVE ALARM

These are alarms that indicate a real attack or unwanted/illegal behavior.

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.

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.

TACTIC

Indicates the purpose of the activities performed by the attacker. It is of great importance in determining the stage of the attack.

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.

DEFINITIONS

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.

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.

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.

OT (OPERATIONAL TECHNOLOGY)

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).

MANAGED DETECTION AND RESPONSE

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