INTE1130- Industry Awareness Project - Advanced Persistent Threats

Dr.Graham Clarke (Mentor)
Dr.Mahshid Sadeghpour (Supervisor)
Gaurav Jain (s4036068)
Ram Kishore Marimuthuraj Nandini (s3974637)
Taha Kasim Rupawala (s4038149)

October 18, 2024

RMIT UNIVERSITY

ACKNOWLEDGEMENT

We gratefully thank **Dr. Mahshid Sadeghpour,** for her support throughout the course of this project. I express my sincere gratitude to our mentor, **Dr. Graham Clarke,** for their sagacious guidance, scholarly advice and inspiration offered in an amiable and pleasant manner in helping me complete the project successfully. Their commitment towards work, sincerity, and hardworking nature motivated us to do the project sincerely and elegantly. We would like to take this opportunity to thank all the faculty members of the school for their support and their wisdom imparted to us throughout the course. Special thanks to my parents, family, and friends for supporting me throughout the course of our project and for the opportunity they provided in undergoing this course in such a prestigious institution.

RAM KISHORE MARIMUTHURAJ NANDINI – S3974637
GAURAV JAIN – S4036068
TAHA KASIM RUPAWALA – S4038149

Contents

1 Introduction

1.1 Overview of Advanced Persistent Threat

An APT, or Advanced Persistent Threat, is a highly complicated and coordinated cyberattack that allows anonymous individuals to acquire undetected access to a network for extended periods (Chen et al., 2014). Unlike ordinary cyber attacks, which are abrupt, APTs focus on remaining undetected for as long as possible until their objectives are realized. Such operations are typically carried out by state-sponsored hackers or criminal enterprises with vast financial resources to obtain secret information, infiltrate servers, or achieve other political, social, or military goals.

To target a specific network, APTs frequently use reconnaissance and social engineering strategies. For example, one of the most well-known APTs, the Stuxnet worm, was designed to destroy Iran's nuclear facilities by directly attacking their industrial control systems (Zetter, 2014). This style of attack emphasizes the strategic aspect of APTs, which are typically used for political or economic advantage beyond simply stealing money or inflicting short disruptions.

1.2 Impact and Importance of APT in Security

APTs pose a serious challenge to global security due to their scale, sophistication, and potential for long-term impact. Organizations across sectors—such as government, finance, healthcare, and critical infrastructure—are prime targets for APT campaigns. The extended nature of these attacks allows adversaries to siphon off sensitive data, ranging from trade secrets to personal information, leading to significant financial loss, reputational damage, and even geopolitical consequences.

For example, APTs may steal classified data or intellectual property intended for government agencies, influencing national security decisions. Similarly, attacks on organizations can result in the theft of secret technologies or financial data, damaging their competitive advantage. APT victims are frequently unaware that they are compromised due to their clandestine nature, which makes them vulnerable until significant harm has been done. As a result, ongoing monitoring and enhanced detection techniques are required (Tankard, 2011).

Furthermore, APTs have a greater impact on national and international cybersecurity initiatives. As attackers develop new ways to circumvent established security safeguards, there is an urgent need for innovation in both defensive strategies and regulatory frameworks.(Conteh & Schmick, 2016)

1.3 Scope and Objective

The purpose of this paper is to provide an in-depth examination of Advanced Persistent Threats by investigating their lifecycle, technical frameworks used to analyze them, and the tactics employed by attackers to carry out APT operations. This paper will also explore detection and preventive strategies, providing insights into the current and future state of APTs.

Key areas covered will include:

1. An overview of the APT lifecycle, explaining how attackers move through different stages, from reconnaissance to exfiltration.
2. Exploration of frameworks, such as the MITRE ATTACK framework, that categorize APT tactics and techniques ("Mitre ATT&CK®", 2020).
3. Detailed discussion of how APTs are implemented through social engineering, software vulnerabilities, and other backdoor techniques.
4. A review of current detection and prevention techniques, including the role of artificial intelligence in enhancing security.
5. Case studies illustrating real-world APT campaigns and their consequences.
6. An examination of future trends in APTs, focusing on the advancements in prevention techniques and governance.

The paper aims to provide a comprehensive understanding of APTs, emphasizing the importance of staying ahead of attackers by implementing cutting-edge technology, robust incident response systems, and policy changes that prioritize cybersecurity. Through this analysis, readers will gain insight into how APTs operate and the critical measures needed to mitigate their threat.

2 APT Technical Framework

2.1 Cyber Kill Chain Framework

Cyber Kill Chain is a framework model used for detecting, identifying, and preventing different intrusion activities. This framework is developed by Lockheed Martin. This seven-step framework helps security experts understand how attackers will try and exploit the system and help create a defense system for large organizations (Tarun & Arvind Mallari, n.d.)

According to Lockheed Martin, an attacker might attack in seven different areas starting from reconnaissance in which the attacker will find as much information as he can to the final accomplishment of their objectives.(Lockheed Martin, n.d.)

In recent years, many attacks have been held in different organizations, and identifying how the attacker exploited the system could be very difficult to find. Hence, by using this framework, security experts can start identifying at what stage an attacker is and try to stop them from further exploiting along with understanding how and when the attacker exploited the system. (Tarun & Arvind Mallari, n.d.) To understand the framework better, let's understand the seven stages of the Cyber Kill Chain Framework:

Figure 1: Cyber Kill Chain (Lockheed Martin, n.d.)

2.1.1 Reconnaissance

The first step Reconnaissance simply means gathering information about potential targets. The attacker simply looks for gathering information by simply looking on the internet and finding specific information about network details, social network IDs, and other different organization details.(*Certified Ethical Hacker (CEH) version 12*, n.d.) There are two ways to perform Reconnaissance:

1. Passive Reconnaissance: This means gathering information about the target organization without letting the target know anything. Examples like Searching the Internet, Social Media Networks, Different Public documents, surfing through the target website, gathering information through whois, Domain names, and many more. Tools such as Shodan, Nmap, and Google can be used for Passive Reconnaissance. (Tarun & Arvind Mallari, n.d.)

2. Active Reconnaissance: Active means gathering information with deeper profiling which might trigger an alert on IDS. Techniques like Ping sweep, Phishing Mail, Social engineering techniques, Port scanning, etc.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

By finding this information, the attacker will know information about the target, and the attacker can understand what attack they need to exploit and understand what kind of malware to install, what ways to further exploit, and how to stay in the system.

After successfully entering the network, the attacker will try to create an outbound connection to get access to other vulnerable computers and try to perform other attacks. Outbound connections will help attackers create a backdoor through which they can send data to their server from the target. There are different Malware attacks according to the specific vulnerability(Jenna, n.d.). Some of them are as follows:

2.1.2 Weaponization

In the weaponization stage, an attacker tries to find vulnerabilities and ways to exploit the system to gain unauthorized access. After finding different vulnerabilities, an attacker can create a custom malware or Distributed Denial of Service attack with botnets. An attacker can create custom malware such as trojans, and worms which will spread through the whole server. Weaponization can be done through a Remote Access Tool (RAT) which is a payload for cyber weapons. (*Certified Ethical Hacker (CEH) version 12*, n.d.)

RAT (Remote Access Tool): Remote access tools are used to give attackers unauthorized remote access. Through creating custom malware, attackers use these tools to get undetected to their computers and monitor their actions.(Tarun & Arvind Mallari, n.d.) There are two types of RAT:

1. Client-side RAT: Client-side RAT executing remote connection through pieces of code. After establishing a connection, one can simply perform any action on the target server. Ventir Trojans, Poison Ivy, Carberp, and Njrat are examples of Client-side RAT. (*Certified Ethical Hacker (CEH) version 12*, n.d.)

2. Server-side RAT : These rats come with a proper UI and instead of a code, there could be a button through which you can perform various actions. This could trigger an alert in the target computer because these RATs come with security features and in other way, server

RATs are also easier to use. TeamViewer is an example of server-side RAT.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.1.3 Delivery

As expected, after finding vulnerabilities, we will send malicious attachments to the targeted servers. The most popular ways to transmit cyber weapons are through websites and emails. This is the most important step as this will rely that the attack will work or not. (*Certified Ethical Hacker (CEH) version 12*, n.d.)

Delivery is a very high-risk step because through delivering malicious attachments, there are high chance that the attacker can easily be detected or could be trapped in a Honey Pot attack. Along with that, this stage takes a long time because not a single method gives 100 percent success and an attacker group may have to again reconsider the previous steps.(Tarun & Arvind Mallari, n.d.)

Delivering attachments through emails, various phishing attacks, USB/removal media, DNS cache poisoning, and Driven by Download are mechanisms of the Delivering stage.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.1.4 Exploitation

After successfully delivering malicious attachments to the targeted server, this step is as its name suggests, exploiting the target server. In this stage, the target organization may face threats like various authentication and authorization attacks, brute force attacks, XSS, and many more.(Tarun & Arvind Mallari, n.d.)

This step is to simply trigger the exploit by executing RAT on target computers, and install various payloads for certain escalation of attacks. Vulnerabilities like outdated operating systems, not updating software, and not having a popular Anti-virus help an attacker gain easy access. Attackers use different vulnerabilities publicly available CVE. These vulnerabilities are various software bugs that bring threats to the system. Another reason is not having sanitation in their code which will create threats for different XSS attacks. (Tarun & Arvind Mallari, n.d.)

Exploitation is the most crucial part of the cyber chain. After getting inside the server, attackers have to find certain ways to escalate inside the server. For example, if an attacker successfully exploits an employee's computer through a phishing attack, the amount of authorization employee could not be useful for the attacker groups. Hence, in this step, an attacker will try to search and exploit more ways to get more access to the system.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.1.5 Installation

In this step, after entering the system target installs additional programs like trojans, and worms, or creates a backdoor for extended remote access. After successfully installing additional malware programs, the attacker can exploit different areas of the target network and also try to hide in the system and stay undetected for a long time and see all actions of the target network. (*Certified Ethical Hacker (CEH) version 12*, n.d.)These two methods are used to install programs:

- **Dropper**: This is a program that installs and runs malware in the target system. Before installing the malware, Dropper also disables host security controls and stays hidden in the system.(Tarun & Arvind Mallari, n.d.)

- **Downloader**: Downloaders work the same as Dropper but in small cases and can be used to exploit a specific area of the network.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.1.6 Command and Control

In this stage, the attacker gets command and control access to the target server and establishes a two-way connection between the target server and the attacker server which helps the attacker get access back and forth. An attacker can also leverage various communication channels like email communication, IRC chats, and DNS, and also apply privilege escalation. There are three types of communication structures mainly known as centralized structure, decentralized structure, and social network-based structures. Steganography is also used to get C&C access easily. Steganography means simply injecting malicious malware in a picture and video through email or any other attachments. (Tarun & Arvind Mallari, n.d.)

2.1.7 Action on objectives:

After successfully getting remote command and control access to the target system, the attacker group will fully perform a targeted attack and accomplish their intended goals. This could be blackmailing the organization by blocking access to the whole system which is called Ransomware, executing big Data breaches and selling data to the black market, getting all funds access, and many more. Hence. If the attacker comes into this stage, it gets really hard for an organization to prevent the attack.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.2 MITRE Framework

Another well-known Framework is called MITRE ATT&CK which stands for Adversarial Tactics, Techniques, and Common Knowledge, which was created by MITRE in 2013. MITRE framework is a knowledge base that describes tactics, techniques, and procedures of cyber adversaries to help organizations detect and prevent Cyber Attacks. To understand MITRE ATT&CK, Let's understand TTP.("Mitre ATT&CK®", 2020)

2.2.1 Tactics, Techniques, and Procedure

The terms 'Tactics, techniques, and Procedures are used to understand the pattern of different threat actors of the group, This process can help strengthen the security of an Organization.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

- **Tactics**: Tactics are termed as various actions taken by threat actors to perform an attack. This consists of performing different tactics used for gathering information, performing initial exploitation, lateral movements, and privilege escalation to stay hidden in the system. Most APT groups don't change their tactics, but they could differ according to what vulnerabilities they find in the targeted system.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

- **Techniques**: Techniques are termed as various steps and methods used for performing various intermediate attacks in the whole APT attack. These techniques can be analyzed according to the different stages of an attack. For example, let's take the example of the initial phase of an attack where they need to gather information and initially exploit using certain tools that are publicly available.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

  In comparison, Techniques used in the middle phase will differ from the initial phase where and mostly depend on technical tools to perform privilege escalation, lateral movement in the system, and many more.

  Now, in the last stage, APT attack groups use different technical and non-technical tools to accomplish their objectives. By aggregating these stages, an organization can detect and prevent different stages of attacks and help strengthen their cyber defense.

- **Procedure**: Procedures involve a proper sequence of actions performed by the attackers to implement attacks at different stages. These procedures can be dependent on different threat actors and APT groups, and they can also change in various parts of the attack life cycle. An understanding of procedures can help the organization understand its next step and help prevent large attacks.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

After understanding the TTP, let's understand the tactics and techniques of MITRE ATTCK which are as follows:

2.2.2 Reconnaissance

This step involves gathering as much information as they can about victims' organizations through active and passive reconnaissance. It is the same as the first step in the cyber kill chain. This information will help the attacker plan and execute the initial attack.("Mitre ATT&CK®", 2020)

Techniques used in reconnaissance are Active scanning, gathering victim host, identity, network, and org information, Phishing, scanning target organization and open domains.

2.2.3 Resource Developing

This step involves techniques used to steal, purchase, or create different resources that can be used for further exploitation. These resources include public reports, account information, or capabilities. For example, an attacker can purchase a domain name for an XSS attack to support command and control, and for phishing attacks. ("Mitre ATT&CK®", 2020)

According to the MITRE, Acquire Access. Acquire Infrastructure, Compromise Accounts, Compromise Infrastructure, develop capabilities, establish accounts, and obtain capabilities. ("Mitre ATT&CK®", 2020)

THE MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	Command-Line Interface	AppCert DLLs	Accessibility Features	BITS Jobs	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Control Panel Items	AppInit DLLs	AppCert DLLs	Binary Padding	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Dynamic Data Exchange	Application Shimming	AppInit DLLs	Bypass User Account Control	Credentials in Files	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Execution through API	Authentication Package	Application Shimming	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryp-tographic Protocol
Spearphishing Link	Execution through Module Load	BITS Jobs	Bypass User Account Control	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Exploitation for Client Execution	Bootkit	DLL Search Order Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Permission Groups Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	LSASS Driver	Component Firmware	File System Permis-sions Weakness	DCShadow	Kerberoasting	Process Discovery	Replication Through Removable Media	Input Capture		Multi-Stage Channels
	Mshta	Component Object Model Hijacking	Hooking	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	Query Registry	Shared Webroot	Man in the Browser		Multi-hop Proxy
	PowerShell	Create Account	Image File Execution Options Injection	DLL Side-Loading	Network Sniffing	Remote System Discovery	Taint Shared Content	Screen Capture		Multiband Communication
	Regsvcs/Regasm	DLL Search Order Hijacking	New Service	Deobfuscate/ Decode Files or Information	Password Filter DLL	Security Software Discovery	Third-party Software	Video Capture		Multilayer Encryption
	Regsvr32	External Remote Services	Path Interception	Disabling Security Tools	Private Keys	System Information Discovery	Windows Admin Shares			Remote Access Tools
	Rundll32	File System Permissions Weakness	Port Monitors	Exploitation for Defense Evasion	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Remote File Copy
	Scheduled Task	Hidden Files and Directories	Process Injection	Extra Window Memory Injection		System Network Connections Discovery				Standard Application Layer Protocol
				Network Share Connection Removal						
				Obfuscated Files or Information						
				Plist Modification						
				Port Knocking						
				Process Doppelgänging						
				Process Hollowing						
				Process Injection						
				Redundant Access						
				Regsvcs/Regasm						
				Regsvr32						
				Rootkit						
				Rundll32						
				SIP and Trust Provider Hijacking						

Figure 2: MITRE Attack Matrix with Tactics and Techniques("Mitre ATT&CK®", 2020)

2.2.4 Initial Access

After gathering the required information and resources, attackers will try to enter the system through unauthorized access and establish an initial foothold. By establishing these footholds, the attacker may gain remote access and get continued access. Techniques used for Initial Access are Content Injection, Drive-by Compromise, Exploit public Applications, Phishing, Spear phishing attachments, supply chain compromise, and many more.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.2.5 Exploitation

After establishing an initial foothold, in the exploitation step, attackers use malicious code in the compromised system. Techniques used in exploitations are Cloud Administration Command, Command and Scripting Interpreter, Container Administrative Command, Service Execution, and many more.("Mitre ATT&CK®", 2020)

2.2.6 Persistence

In this step, an attacker tries to maintain their exploitation. To keep persistence, different techniques are used to keep access to the system even after the computer is restarted, rebooted, or any other action that could cut off their access. Techniques used are Account Manipulation, BITS Jobs, Boot or Logon AutoStart Execution, Boot or Logon Initialization Scripts, and many more.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.2.7 Privilege Escalation

In the privilege escalation step, an attacker tries to escalate their access by gaining higher-level access through a compromised system. For example, it could be that an attacker has exploited an employee and knows to use techniques to gain access to the SYSTEM/root level, accounts with admin access, and many more. Techniques used are Abuse Elevation Control Mechanism, Access Token manipulation, Account Manipulation, Domain or Tenant Policy Modification, Event Triggered Execution, and many more.("Mitre ATT&CK®", 2020)

2.2.8 Defense Evasion

Defense Evasion consists of staying hidden in the network and avoiding detection throughout the process. Techniques used for defense evasion are disabling software, encrypting different data, and staying hidden through custom malware. Techniques used in this step are the same as the previous step but with little added benefits for staying hidden in the system.("Mitre ATT&CK®", 2020)

2.2.9 Credential Access

As its names suggest, the Credential Access stage is where an attacker tries to steal user credentials like account details, passwords, and sensitive information. Techniques used are Adversary-in-the-middle, Brute Force, Exploitation for Credential Access, Forced Authentication, forging web Credentials, Input Capture, and Modifying the Authentication Process.("Mitre ATT&CK®", 2020)

2.2.10 Discovery

After gaining credential access, exploiting the system server, and finding a way to stay hidden, the Discovery phase consists of techniques used by attackers to gather information about internal systems and networks. This will allow the attacker to understand what control they have and what it will take to accomplish their objective. Various operating systems tools are used for information gathering in this step. Techniques used are Account Discovery, Application Window Discovery, Browser Information Discovery, Cloud Infrastructure Discovery, and Cloud Infrastructure Discovery.(*Certified Ethical Hacker (CEH) version 12*, n.d.)

2.2.11 Lateral Movement

Lateral Movement means using techniques for entering the remote system of the compromised host and further pivoting to other multiple networks by using their remote access server or operating system tools. Techniques used are Internal Spear phishing, Exploitation of Remote Services, Lateral Tools Transfer, Remote Service Session Hijacking, Replication through Removable media, and many more.("Mitre ATT&CK®", 2020)

2.2.12 Collection

In this stage, after getting the required remote access, attackers try to collect as much information as they need to accomplish their goals. Common targets include email accounts, phone numbers, screenshots, bank details, audio, video, and keyboard input. Techniques used are Adversary in the middle, Archive collected data, Audio Capture, Automated Collection, Browser Server Collection, Data from Removable Media, and Data Staged. ("Mitre ATT&CK®", 2020)

2.2.13 Command and Control

In this stage, the attacker creates a communication channel between their server and compromised victim servers to get proper command and control access. Various protocol techniques are used to mimic normal, expected traffic and avoid detection. The techniques used are the Application Layer protocol, communication through removal media, content injection, Data encoding, and many more.("Mitre ATT&CK®", 2020)

2.2.14 Exfiltration

This step is used to steal as much data as possible and required. Once the data is collected, they copy or remote the data from the system without getting detected. Data will be transferred through the command-and-control channels. Techniques used are Exfiltration over symmetric and asymmetric C2 protocol, over Bluetooth, physical medium, and many more.("Mitre ATT&CK®", 2020)

2.2.15 Impact

This step is the last step of MITRE ATT&CK in which the attacker tries to accomplish their objective and destroy their system and data. Techniques like Account Access Removal, Data Destruction, Data Encrypted, Defacement, and many more.("Mitre ATT&CK®", 2020)

3 APT Implementation

3.1 Reconnaissance Techniques in Advanced Persistent Threat (APT's)

APT29, also known as Cozy Bear, is recognized for its spear-phishing campaigns aimed at gathering sensitive information about its targets. This group often employs deceptive emails to trick individuals into revealing confidential data.

In contrast, APT28, also referred to as Fancy Bear, frequently relies on active scanning and network reconnaissance to gain a deeper understanding of target infrastructure. This approach allows them to gather critical insights that facilitate their attacks.

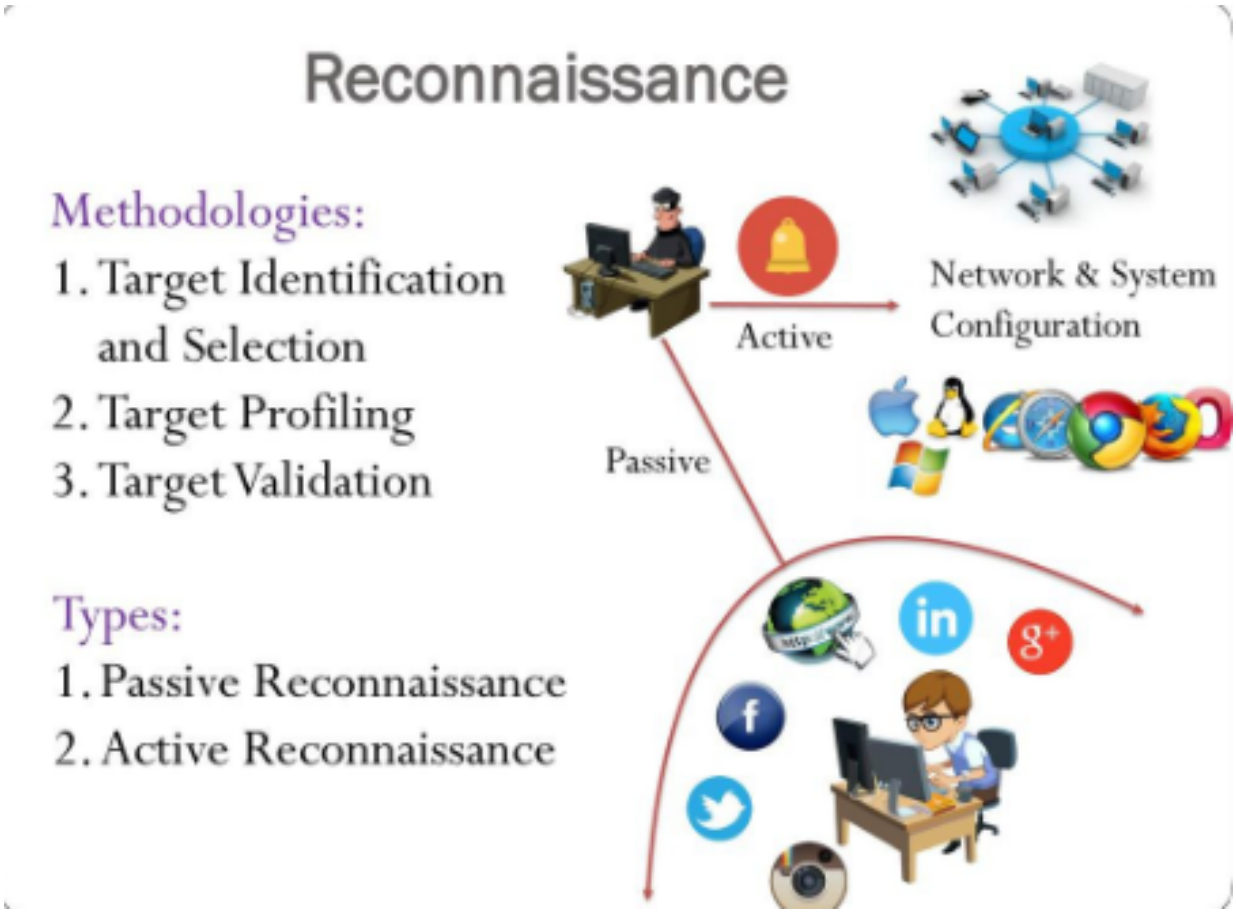

Figure 3: Reconnaissance
(Alam Zeb, n.d.)

3.1.1 Active Scanning (T1595)

Description: Active scanning involves systematically sending data packets to servers across the internet to discover open ports, services, software versions, and potential vulnerabilities. Attackers may use tools like Nmap or Acunetix to gather information about the victim's environment. This process generates large volumes of log data and may go unnoticed amidst normal internet traffic.

Real-life Example: APT groups like Deep Panda use active scanning techniques to identify vulnerabilities in corporate networks. For example, Acunetix scans were used by this group to test several servers for software versions and potential exploits (Steffens, 2020).

Mitigation Strategies: To strengthen security, organizations can implement network segmentation to isolate critical systems from those exposed to the internet, thereby reducing the attack surface. Additionally, deploying Intrusion Detection Systems (IDS) enables the detection of abnormal scanning behaviors, allowing security teams to respond promptly to potential threats. Regular patch management is also essential, as it keeps software updated to address and minimize vulnerabilities that could be exploited through scanning activities.

3.1.2 Gather Victim Identity Information (T1589)

Description: Attackers gather personal information such as usernames, email addresses, and credentials to facilitate further exploitation. This may be done through open-source intelligence (OSINT) or phishing campaigns.

Real-life Example: The APT28 group registered multiple malicious domains designed to appear legitimate, using techniques such as phishing emails that contained malicious links to gather credentials from targets. The domain *worldpostjournal[.]com* was used in one such campaign, and a reverse search identified other domains linked to the same email (Steffens, 2020).

Mitigation Strategies: To enhance security against social engineering attacks, users should be educated on social media awareness to limit the amount of personal information they share online, reducing potential exposure. Employing advanced email filtering can block phishing attempts and flag suspicious domains, adding another layer of protection. Additionally, implementing multi-factor authentication (MFA) ensures that even if credentials are compromised, attackers cannot access systems without the second authentication factor, making it significantly harder for unauthorized users to gain access.

3.1.3 Gather Victim Network Information (T1590)

Description: Adversaries seek to gather detailed information about a target's network, including IP addresses, domain names, and system architecture. This can involve passive techniques (e.g., WHOIS lookups) or active probing of external-facing systems.

Real-life Example: During the Witchcoven campaign, the Snake group used network fingerprinting techniques to gather information about visitors to compromised websites, specifically targeting government networks through IP whitelisting (Steffens, 2020).

Mitigation Strategies: Traffic analysis involves monitoring outbound traffic for anomalies, such as unexpected queries or spikes in traffic, which could indicate scanning or probing activities by attackers. This proactive approach helps in detecting potential threats early. Another key measure is restricting public information. By minimizing the exposure of sensitive network details, such as DNS records and IP addresses, organizations can reduce the risk of attackers gathering information that could be used to exploit vulnerabilities. Internal network segmentation is also an essential security practice. By limiting access to sensitive parts of the network, segmentation helps restrict lateral movement within the system, preventing attackers from easily navigating through the network if they gain initial access.

3.1.4 Phishing for Information (T1598)

Description: Phishing for information is a widely used technique to deceive users into providing sensitive information, often through emails or fake websites designed to look legitimate. Attackers trick users into clicking malicious links or downloading harmful attachments.

Real-life Example: The Lotus Blossom APT group used fake conference invitations via email, embedding malicious exploits within Word documents. This form of spear-phishing is common for targeted attacks on individuals (Steffens, 2020).

Mitigation Strategies: To protect against phishing threats, organizations should conduct regular security awareness training, helping employees recognize and avoid suspicious emails. Email security solutions are also essential, as they can filter out known phishing signatures and detect malware attachments, reducing the chances of harmful content reaching users. Furthermore, implementing browser isolation and web filtering prevents access to malicious websites and restricts script execution, adding an extra layer of defense against web-based attacks.

3.2 Resource Development Techniques using Advanced Persistent Threat

APT41, also known as Double Dragon, is notorious for acquiring infrastructure and establishing accounts to facilitate a wide range of financially and politically motivated attacks. This group has been observed purchasing virtual private servers (VPS) and domains to launch phishing campaigns.

Similarly, APT28, also referred to as Fancy Bear, frequently compromises third-party infrastructure, such as websites or VPNs, to carry out stealthy operations. Their tactics have been particularly noted in attacks against European institutions.

On the other hand, APT33, an Iranian-backed group, often focuses on compromising social media and email accounts. They use these compromised platforms to gather intelligence and conduct espionage activities.

3.2.1 Acquire Access (T1583)

Description: Adversaries acquire access to victim systems, services, or accounts through various means, including purchasing access from underground markets or directly stealing credentials. This access often serves as an entry point into victim networks ("Mitre ATT&CK®", 2020).

Example: Attackers acquire stolen credentials from underground forums to gain unauthorized access to corporate networks.

Mitigation Strategies: To safeguard critical systems, enforcing multi-factor authentication (MFA) ensures that even if credentials are compromised, attackers cannot access sensitive areas without an additional authentication factor. Additionally, threat intelligence monitoring allows organizations to detect when corporate credentials appear on underground markets, enabling a timely response to prevent unauthorized access and mitigate potential security breaches.

3.2.2 Acquire Infrastructure (T1583.002)

Description: Adversaries acquire or rent infrastructure, such as servers or domains, to carry out their operations. This infrastructure is often used for command-and-control (C2), phishing campaigns, or launching attacks ("Mitre ATT&CK®", 2020).

Example: The APT28 group used rented VPS (Virtual Private Servers) to manage C2 servers and coordinate attacks without exposing their true origin (Steffens, 2020).

Mitigation Strategies: To detect potential threats, organizations can use domain and IP monitoring to track new domain registrations and infrastructure associated with suspicious activities. Additionally, analyzing outbound network traffic helps identify communications with known malicious infrastructures, allowing for early detection and mitigation of potential security breaches.

3.2.3 Compromise Accounts (T1586)

Description: Attackers compromise legitimate accounts by stealing login credentials via phishing, social engineering, or other methods. These accounts can then be used to gain unauthorized access to target systems ("Mitre ATT&CK®", 2020).

Example: The APT33 group compromised corporate email accounts and used them to spread malware internally (Steffens, 2020).

Mitigation Strategies: To reinforce account security, organizations should enforce strong password policies and regularly rotate credentials to minimize the risk of compromise. Continuous access logging and monitoring further enhance security by enabling the detection of suspicious access patterns or unusual login times, allowing for rapid response to potential threats.

3.3 Compromise Infrastructure (T1584)

3.3.1 Description

Adversaries may take over third-party infrastructure to further obfuscate their activities. This could involve compromising web servers or VPN systems, which allow attackers to operate without exposing their infrastructure ("Mitre ATT&CK®", 2020). **Example**: In the Witchcoven campaign, attackers compromised government web servers to stage further attacks without leaving traces back to their original infrastructure.

Mitigation Strategies: To minimize security risks, organizations should conduct regular audits of third-party services and infrastructure to identify and address any vulnerabilities. Additionally, consistent patch management across all systems is essential to prevent the exploitation of known vulnerabilities, ensuring that infrastructure remains resilient against emerging threats.

3.3.2 Establish Accounts (T1585)

Description: Attackers create fake accounts on social media platforms, email providers, or other services to blend in and conduct malicious activities. These accounts can be used to launch phishing attacks or establish a presence in the victim environment ("Mitre ATT&CK®", 2020).

Example: APT29 created fake social media accounts to gather intelligence and initiate phishing attacks (Steffens, 2020).

Mitigation Strategies: To enhance security against unauthorized access, organizations should deploy tools that detect and block the creation of fake accounts on critical systems. Additionally, enforcing stronger identity verification mechanisms during account creation adds an extra layer of protection, ensuring that only legitimate users can establish access to corporate systems.

3.4 Initial Access Techniques using Advanced Persistent Threats (APTs)

APT29, also known as Cozy Bear, has been observed using valid accounts to infiltrate networks, often through phishing campaigns that steal legitimate credentials. Once they gain access, these stolen credentials allow them to acquire privileged access within the network, further deepening their infiltration.

APT41, or Double Dragon, has displayed a high level of sophistication in compromising supply chains, particularly targeting the software supply chain. Their campaigns have been aimed at healthcare and technology organizations, leveraging these compromises to achieve broader objectives.

Meanwhile, APT28 also referred to as Fancy Bear has frequently employed external remote services, exploiting vulnerabilities in VPN systems to access target systems. This tactic has been evident in their campaigns against political entities across Europe.

3.4.1 Supply Chain Compromise (T1195)

Description: Supply chain compromises involve infiltrating a supplier or third-party service provider with access to the target organization. Attackers can compromise the software or hardware being delivered to the target, injecting malicious code or altering configurations to later exploit the target's systems.

Sub-techniques:

1. **Compromise Software Supply Chain (T1195.002)**: Attackers modify software updates, such as in the SolarWinds attack, to inject malicious code.
2. **Compromise Hardware Supply Chain (T1195.003)**: Altering the hardware, such as routers or storage devices, before it is delivered to the target ("Mitre ATT&CK®", 2020).

Mitigation Strategies: To strengthen defenses against supply chain attacks, organizations should implement thorough vendor risk management by conducting due diligence on vendors and embedding security requirements within contracts. Using software integrity verification tools and checksums ensures that software from vendors is authentic and untampered. Additionally, network segmentation is crucial, as it minimizes the exposure of critical systems by isolating them from external and third-party infrastructures. Staying updated on emerging threats through threat intelligence enables proactive responses to potential supply chain compromises, further enhancing overall security (Zhang et al., 2024).

3.4.2 External Remote Services (T1133)

Description: Attackers frequently utilize external remote access services, such as Remote Desktop Protocol (RDP), VPNs, or other remote management tools, to gain unauthorized entry into systems. They often exploit weak or default credentials or take advantage of vulnerabilities within these services to infiltrate networks.

One sub-technique is RDP Exploitation (T1133.001), where attackers use stolen or weak RDP credentials to access systems. Another common method is VPN Exploitation (T1133.002), where attackers exploit vulnerabilities in VPN services or use stolen credentials to penetrate internal networks ("Mitre ATT&CK®", 2020).

Mitigation Strategies: To secure remote access services, organizations should implement multi-factor authentication (MFA) for all remote connections to reduce the risk of compromised credentials. Regular vulnerability management, including patching and updating VPN and RDP servers, is essential to protect against exploitation. Remote access should be limited to approved and secured gateways, with internet-facing services minimized to reduce exposure. Additionally, continuous logging and monitoring of remote access activity allow for the detection of anomalies and unauthorized access attempts, enabling a rapid response to potential threats (Zhang et al., 2024).

3.4.3 Valid Accounts (T1078)

Description: Attackers use legitimate accounts to gain access to systems. These valid credentials may be obtained through phishing, password spraying, credential stuffing, or other means, allowing attackers to bypass many traditional security defenses.

Sub-techniques:

1. **Local Accounts (T1078.001)**: Using local user credentials to access systems.
2. **Domain Accounts (T1078.002)**: Using domain credentials to move laterally across the network.

Mitigation Strategies: To reduce the risk of password spraying and brute force attacks, enforcing strong password policies is crucial. Regular account monitoring helps identify unusual login behavior and detect suspicious activity early on. Additionally, implementing regular credential rotation and requiring unique passwords across systems enhances security by minimizing the likelihood of password reuse. Adhering to the principle of least privilege further safeguards systems by ensuring users have access only to the resources necessary for their roles, reducing potential points of exploitation (Zhang et al., 2024).

3.4.4 Drive-by Compromise (T1189)

Description: A drive-by compromise occurs when a victim unknowingly visits a malicious website that exploits vulnerabilities in the browser, plugins, or underlying operating system. The attacker can execute malicious code on the victim's system through these exploits. **Sub-techniques:**

1. **Browser Exploits (T1189.001)**: Leveraging browser vulnerabilities to compromise a system when a user visits a malicious site.

2. **Malicious Ads (T1189.002)**: Using malvertising (malicious advertisements) that deliver exploits to the user's browser without needing them to click ("Mitre ATT&CK®", 2020).

Mitigation Strategies: To protect against drive-by attacks, organizations should employ browser isolation techniques, running internet browsers in sandboxed environments to contain potential threats. Regularly updating and patching browsers, plugins, and related software helps minimize exposure to vulnerabilities. Additionally, implementing web filtering blocks access to known malicious sites and harmful content, while script-blocking extensions, such as NoScript, limit the execution of potentially malicious code within web browsers, adding further layers of security (Zhang et al., 2024).

3.5 Persistence in Advanced Persistent Threats (APTs)

Persistence is a critical tactic employed by Advanced Persistent Threat (APT) actors to maintain access to compromised systems over extended periods. Once inside a target network, attackers use various methods to ensure their continued presence, even in the face of system reboots or credential changes. The *MITRE ATT&CK* framework offers a detailed taxonomy of these persistence techniques, enabling defenders to map, detect, and mitigate such activities ("Mitre ATT&CK®", 2020). Persistence techniques such as *Account Manipulation*, *Hijacking Execution Flow*, and *Modification of Authentication Processes* are crucial for adversaries to blend in with legitimate processes and evade detection. Research has also demonstrated the growing complexity of APTs and persistence tactics in modern cybersecurity (Alshamrani et al., 2019).

Key Persistence Techniques

3.5.1 Account Manipulation (T1098)

Description: Account manipulation refers to the act of creating or modifying user accounts, particularly those with administrative privileges, to maintain unauthorized access within a compromised system. Attackers may reset passwords or escalate privileges to ensure long-term control over critical systems. This method is commonly used by Advanced Persistent Threats (APTs) to persist within a network while bypassing traditional security defenses(Alshamrani et al., 2019).

For example, APT28, also known as Fancy Bear, a Russian cyber espionage group, is known for creating backdoor administrative accounts to sustain access over time. Similarly, FIN6 has employed account manipulation tactics in retail environments, allowing them to maintain privileged access across system reboots.

Several mitigation techniques can help counter this threat. Regular account auditing can detect unauthorized account creation or privilege escalation. Privileged Access Management (PAM) can monitor and control administrative accounts, reducing the risk of unauthorized changes. Additionally, implementing Multi-Factor Authentication (MFA) makes it more difficult for attackers to successfully take over accounts.

Mitigation Techniques

Account auditing involves conducting regular reviews to detect unauthorized account creation or privilege escalation within a system. This process helps identify potential security breaches and ensures that only authorized users have the necessary access. Privileged Access Management (PAM) is another important technique, designed to monitor and control administrative accounts, thereby preventing unauthorized changes and limiting attackers' ability to manipulate privileged accounts. Additionally, Multi-Factor Authentication (MFA) plays a crucial role in reducing the likelihood of successful account takeovers by adding an extra layer of security, making it harder for attackers to gain access using compromised credentials.

3.5.2 Hijack Execution Flow (T1574)

Description: Hijacking execution flow allows adversaries to manipulate how code is executed within a system. Techniques such as DLL Injection or Process following enable attackers to piggyback on legitimate processes, making detection significantly more challenging ("Mitre ATT&CK®", 2020). Advanced Persistent Threat (APT) groups often employ these methods to ensure their malicious payloads run with higher privileges, allowing them to maintain persistence within compromised systems.

For instance, APT29, also known as Cozy Bear, is notorious for using DLL Injection to execute malicious payloads within trusted system processes, effectively evading detection. Similarly, the Lazarus Group used Process Hollowing during the Sony Pictures breach, running malicious code within legitimate processes to avoid detection.

Mitigation Techniques

Several mitigation techniques can help prevent these types of attacks. Code Signing Enforcement ensures that only trusted, signed code is permitted to run, minimizing the chances of malicious code being executed. Memory Scanning, through Endpoint Detection and Response (EDR) solutions, can monitor system memory for suspicious behavior, such as process hollowing. Additionally, tools like Microsoft AppLocker can be used for Application Control, restricting unauthorized scripts and binaries from executing within the system.

3.5.3 Modify Authentication Process (T1556)

Description: Modifying the authentication process allows attackers to bypass or exploit vulnerabilities in user authentication systems. Techniques such as Credential Dumping and Passing the Hash enable attackers to gain unauthorized access to systems without the need for valid passwords (Alshamrani et al., 2019). These methods are crucial for attackers to maintain ongoing access, even after security teams attempt remediation efforts.

For example, APT33 is known for using Pass the Hash techniques, which allow them to authenticate without requiring valid credentials. Similarly, APT41 has employed Golden Ticket attacks, forging Kerberos tickets to ensure long-term access to domain resources.

Mitigation Techniques

To mitigate these risks, several techniques can be implemented. Credential Guard can help protect against credential dumping while enforcing secure authentication protocols like Kerberos can reduce the likelihood of pass-the-hash attacks. Additionally, Active Directory Auditing plays an important role in detecting and preventing unauthorized changes to authentication mechanisms, thereby enhancing overall system security.

3.6 Privilege Escalation in Advanced Persistent Threats (APTs)

Privilege escalation is a critical tactic used by Advanced Persistent Threat (APT) actors to gain higher-level permissions or execute commands with elevated privileges. This allows attackers to perform unauthorized actions that would otherwise be restricted. The *MITRE ATT&CK* framework categorizes various privilege escalation techniques, helping defenders identify and mitigate these methods ("Mitre ATT&CK®", 2020). Some of the prominent techniques include *Access Token Manipulation*, *Abuse Elevation Control Mechanisms*, and *Process Injection*. These techniques allow attackers to bypass security controls and gain administrative-level access to the system, thereby broadening the scope of their attack.

Key Privilege Escalation Techniques:

3.6.1 Access Token Manipulation (T1134)

Description: Access token manipulation involves exploiting Windows access tokens to impersonate other users or processes and escalate privileges. Tokens represent the security context of a process or thread and are used to determine access to system resources. Attackers manipulate these tokens to impersonate privileged users, such as administrators, enabling them to execute commands with higher privileges.

Procedure Examples

APT29, also known as Cozy Bear, has utilized access token manipulation to impersonate local administrators, allowing them to gain control of critical systems while bypassing standard security measures. By manipulating these tokens, they can operate under the guise of legitimate administrators, making detection more difficult. Similarly, FIN6 has been known to manipulate access tokens to gain elevated privileges, enabling them to execute malware under the context of privileged system processes. This tactic allows them to maintain a high level of access and control within the compromised systems while evading security protocols.

Mitigation Techniques

Token integrity monitoring involves the continuous observation of access tokens to detect any unusual activity that could indicate manipulation. This proactive monitoring helps identify potential security threats early, ensuring that any signs of token tampering are promptly addressed. Additionally, applying the principle of least privilege access is crucial. By ensuring that tokens are assigned only the minimum level of privilege necessary for specific tasks, organizations can significantly reduce the impact of token manipulation if it occurs. Deploying behavioral detection tools further enhances security by identifying abnormal behaviors in processes attempting to manipulate or impersonate tokens. These tools can help detect and prevent malicious actions, thereby reinforcing overall system security.

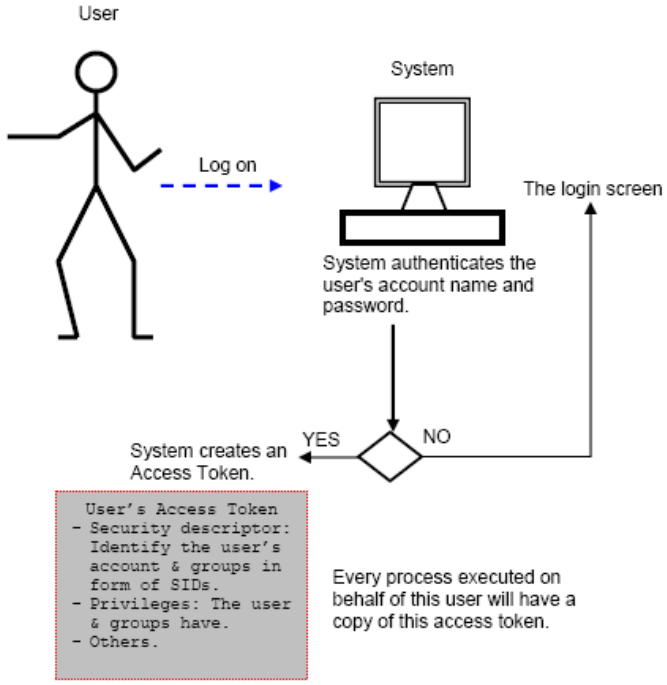

Figure 4: Access Token Manipulation(Anusthika Jeyashankar, 2022)

3.6.2 Abuse Elevation Control Mechanisms (T1548)

Description: Abusing elevation control mechanisms refers to the exploitation of features like User Account Control (UAC) in Windows or sudo in Unix/Linux systems to gain elevated privileges. Attackers can bypass or abuse these controls to execute commands or processes with administrative privileges without alerting the security system.

Procedure Examples
APT33 has employed User Account Control (UAC) bypass techniques to escalate privileges, allowing them to maintain persistence within high-value systems. By circumventing UAC restrictions, this group can gain elevated access, making it easier to execute malicious actions while remaining undetected.

APT32, also known as OceanLotus, has exploited sudo misconfigurations on Linux systems to gain root-level access. This allows them to take complete control of the system, enabling them to conduct a wide range of activities with the highest level of privilege within the compromised environment.

Mitigation Techniques: To minimize the risk of privilege escalation, organizations should enforce strict User Account Control (UAC) settings, configuring it to prompt for credentials on all sensitive actions, thereby reducing the likelihood of unauthorized bypasses. Additionally, regular audits of sudo configurations on Unix/Linux systems are essential to ensure they adhere to the principle of least privilege. For further security, using multi-factor authentication (MFA) for administrative actions adds an extra layer, requiring attackers to overcome additional authentication factors before they can escalate privileges.

3.6.3 Process Injection (T1055)

Description: Process injection involves injecting malicious code into legitimate running processes to escalate privileges or execute commands under the context of trusted system processes. This technique allows attackers to hide their activities within legitimate processes, making it harder for security tools to detect malicious behavior.

Procedure Examples
The Lazarus Group is known for utilizing process injection techniques to evade detection and execute malware within trusted system processes. This method enables them to move laterally across networks, spreading their malicious activities while avoiding security measures.

Similarly, APT28, also known as Fancy Bear, frequently employs DLL injection and process hollowing techniques to escalate privileges. These methods allow them to operate stealthily within compromised environments, making it difficult for security systems to detect their presence as they carry out their attacks.

Mitigation Techniques
To prevent unauthorized code injection and suspicious memory modifications, organizations can deploy Endpoint Detection and Response (EDR) solutions with memory scanning capabilities, which detect signs of code injection or unexpected changes in system memory. Enforcing code integrity ensures that only signed and trusted code can execute within system processes, blocking unauthorized code from running. Additionally, using behavioral analysis tools helps identify unusual process behaviors, such as code execution from unexpected sources, providing early detection of potential threats.

3.7 Defense Evasion in Advanced Persistent Threats (APTs)

Defense evasion is a critical phase in APT attacks, where adversaries focus on avoiding detection and weakening the victim's security mechanisms. *MITRE ATT&CK* provides detailed techniques used by APTs to evade detection. Some of the most significant methods include *Impairing Defenses*, *Weakening Encryption*, *Masquerading*, and *Impersonation*. These techniques allow adversaries to remain undetected and continue their malicious activities while bypassing robust security measures ("Mitre ATT&CK®", 2020). Research further highlights that evading defense mechanisms is crucial for adversaries to conduct prolonged operations without being discovered (Alshamrani et al., 2019).

Key Defense Evasion Techniques

3.7.1 Impair Defenses (T1562)

Description: Impairing defenses involves disabling, modifying, or tampering with security tools to avoid detection and allow attackers to persist on the target system. This can include disabling antivirus software, firewalls, or other security measures that monitor for malicious activity. By impairing defenses, adversaries ensure that their malicious activities go unnoticed by system administrators.

Procedure Examples

APT28 also referred to as Fancy Bear, is notorious for disabling endpoint security tools and tampering with Windows Defender. This allows them to operate within a victim's network undetected, effectively bypassing protective measures and maintaining their malicious activities.

Similarly, APT41 is known for exploiting vulnerabilities to disable antivirus systems. By doing so, they create an environment where their malware can execute without interference, furthering their ability to compromise systems while avoiding detection.

Mitigation Techniques: To enhance security against tampering, continuous monitoring of security tools and processes is essential, as it helps detect when defenses are disabled or altered. Implementing tamper protection mechanisms further prevents unauthorized modifications to security settings, safeguarding the integrity of critical defenses. Additionally, Privileged Access Management (PAM) limits administrative access to crucial security functions, restricting attackers' ability to disable protective measures and ensuring that only authorized personnel can make changes.

3.7.2 Weaken Encryption (T1600)

Description: Weakening encryption involves tampering with encryption algorithms or encryption settings, allowing attackers to bypass or intercept secure communications. Adversaries may weaken the encryption methods in use or exploit vulnerabilities in cryptographic protocols to decrypt sensitive data or communicate without detection.

Procedure Examples

APT29, also known as Cozy Bear, has been observed renaming their malware to mimic legitimate system processes. This tactic makes it difficult for administrators to identify the threat, as the malicious software blends in with regular system activities, evading detection.

Similarly, the Lazarus Group is known for disguising their malware as legitimate applications. For instance, they have been seen renaming malicious executables to resemble antivirus software, making it even more challenging for security teams to detect and remove the threat from compromised systems.

Mitigation Techniques: To protect against encryption-based attacks, organizations should adopt strong encryption standards, such as TLS 1.3, to ensure that only the latest and most secure protocols are used, effectively minimizing the risk of exploiting outdated algorithms. Regular cryptographic audits are crucial to verify that encryption implementations follow current best practices and remain free from vulnerabilities. Additionally, implementing certificate

pinning adds another layer of security by preventing man-in-the-middle attacks that attempt to exploit weakened encryption, thus ensuring the authenticity of communications.

3.7.3 Masquerading (T1036)

Description: Masquerading is the act of disguising malicious activity or code as legitimate files, users, or processes to evade detection. Attackers may rename files or processes to mimic system components or trusted software, reducing the likelihood of raising alarms with security tools. This technique is commonly used to blend malicious activities with regular system functions.

Procedure Examples

APT29, also known as Cozy Bear, has been observed renaming their malware to mimic legitimate system processes, making it challenging for administrators to identify the threat. By disguising malicious software as common system files, they can evade detection and continue their activities unnoticed.

The Lazarus Group employs a similar tactic, disguising their malware as legitimate applications. For instance, they have been known to rename malicious executables to resemble antivirus software, further complicating efforts to detect and eliminate the threat within compromised systems.

Mitigation Techniques: To enhance security and detect potential threats, organizations should continuously monitor running processes and file activities to identify unusual or unexpected changes, such as the renaming of critical files. Behavioral detection tools further strengthen defenses by identifying malicious activities based on behavior patterns rather than solely relying on file names or signatures, enabling more dynamic threat detection. Additionally, implementing application whitelisting restricts the execution of unauthorized applications and processes, ensuring that only trusted software can operate within the system.

3.7.4 Impersonation (T1056)

Description: Impersonation involves attackers posing as legitimate users or systems to bypass authentication controls and gain unauthorized access. Adversaries can steal credentials or session tokens, enabling them to assume the identity of legitimate users and perform malicious actions while avoiding detection.

Procedure Examples

APT33 has employed spear-phishing and credential-harvesting tactics to impersonate high-ranking officials within targeted organizations. This approach allows them to gain access to sensitive systems by using the credentials of individuals with significant authority, making it easier to infiltrate critical areas of the organization.

APT10, on the other hand, is known for impersonating trusted third-party vendors during supply chain attacks. By masquerading as legitimate partners, they can infiltrate target networks, exploiting the trust placed in these third parties to gain unauthorized access and compromise key systems.

Mitigation Techniques: To reduce the risk of successful impersonation attacks, implementing multi-factor authentication (MFA) ensures that stolen credentials alone are insufficient for access. User Behavior Analytics (UBA) enhances security by monitoring for any unusual user activity, such as logins from unfamiliar locations or at unusual times, which may indicate impersonation. Additionally, session monitoring with enforced session timeouts prevents attackers from exploiting stolen session tokens for extended periods, helping to limit unauthorized access.

3.8 Credential Access in Advanced Persistent Threats (APTs)

Credential access is a vital tactic in APT campaigns that involves stealing or exploiting credentials to gain unauthorized access to systems and sensitive data. Adversaries use various methods to capture login credentials or authentication tokens, which can then be used to move laterally across the network. The *MITRE ATT&CK* framework outlines multiple techniques for credential access, including *Adversary-in-the-Middle*, *Brute Force*, *Unsecured Credentials*, and *Steal/Forge Authentication Certificates or Force Web Credentials* ("Mitre ATT&CK®", 2020). Gaining access to credentials enables attackers to execute further malicious actions under the guise of legitimate users.

Key Credential Access Techniques

3.8.1 Adversary-in-the-Middle (T1557)

Description: The adversary-in-the-middle (AiTM) attack involves intercepting communication between a user and a legitimate system to steal credentials or session tokens. Adversaries position themselves between the user and a trusted service, capturing sensitive information such as login credentials, or modifying the communication to gain access.

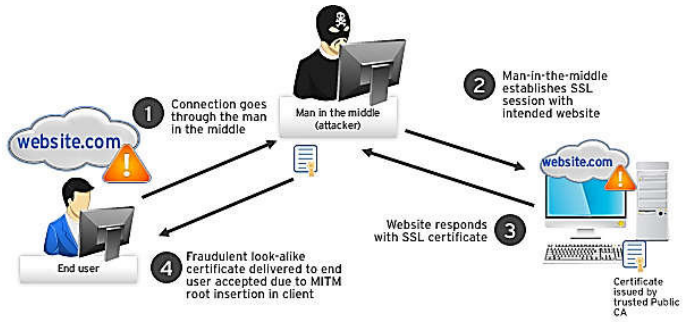

Figure 5: Adversary-in-the-Middle
(Dr. Yusuf Perwej et al., n.d.)

Procedure Examples

APT34, also known as OilRig, is infamous for executing man-in-the-middle (MiTM) attacks to intercept credentials during VPN connections. By capturing this sensitive information, they can gain unauthorized access to internal systems, allowing them to infiltrate networks undetected.

Similarly, APT29, or Cozy Bear, has conducted adversary-in-the-middle (AiTM) attacks to steal session cookies during web-based communications. By hijacking these session cookies, attackers can take control of user sessions, bypassing authentication mechanisms and gaining access to the victim's online accounts and sensitive information.

Mitigation Techniques: To ensure secure communication and protect against session hijacking, organizations should use encrypted protocols like TLS to secure data between users and services, making it resistant to interception. Actively monitoring session activity and enforcing session timeouts can further prevent adversaries from exploiting ongoing sessions. Additionally, multi-factor authentication (MFA) enhances security by ensuring that a stolen session token alone cannot provide unauthorized access, as additional verification is required.

3.8.2 Brute Force: Credentials from Password Stores (T1110)

Description: Brute force attacks involve systematically guessing login credentials or exploiting weaknesses in password storage to obtain valid user credentials. Attackers may target password hashes stored in password stores or configuration files, which can then be cracked to obtain plaintext credentials. Password stores can often be vulnerable if they are improperly secured or if weak hashing algorithms are used.

Procedure Examples
APT32, also known as OceanLotus, is known for brute-forcing credentials stored in password managers and browser password stores. By targeting these repositories, they aim to retrieve passwords for high-value targets, giving them unauthorized access to sensitive systems.

APT41, on the other hand, has used brute-force attacks against Active Directory and password vaults. Their goal is to gain access to administrative credentials, which allows them to escalate privileges and further infiltrate the target's network with elevated access.

Mitigation Techniques
Using strong hashing algorithms, such as bcrypt or Argon2, is essential for securely storing passwords. These modern algorithms make brute force attacks significantly more difficult by adding computational complexity to the hashing process, protecting passwords from being easily cracked.

Account lockout policies provide another layer of security by locking user accounts after a certain number of failed login attempts. This prevents automated brute-force attacks from continuously attempting to guess passwords.

Additionally, salting passwords enhances security by adding a unique random value, or "salt," to each password before hashing. This makes it much harder for attackers to crack stored password hashes, even if they manage to access the database.

3.8.3 Unsecured Credentials (T1552)

Description: Unsecured credentials refer to sensitive login information such as usernames and passwords that are left exposed in configuration files, scripts, or logs. Attackers can easily obtain these credentials if they are not properly secured, allowing them to gain unauthorized access to systems or services.

Procedure Examples
APT33 has been observed actively searching for plaintext credentials left in configuration files and scripts on compromised servers. By locating these unsecured credentials, they can easily gain unauthorized access to sensitive systems and resources within the targeted environment.

Similarly, APT10 is notorious for exploiting unsecured credentials left in development environments and cloud service configurations. This practice allows them to access sensitive resources and infiltrate networks, capitalizing on weak security practices in the development and deployment stages of software and cloud services.

Mitigation Techniques: To ensure the secure storage of credentials, organizations should use encrypted vaults or other secure storage solutions, rather than plaintext files or scripts, to prevent unauthorized access. Conducting regular audits of code repositories and servers helps identify and eliminate any exposed credentials that may be inadvertently included in these environments. Additionally, isolating development, testing, and production environments minimizes the risk of sensitive credentials being exposed in less secure or public-facing systems, further safeguarding critical information.

3.8.4 Steal/Forge Authentication Certificates or Force Web Credentials (T1606)

Description: Adversaries can steal or forge authentication certificates force the acquisition of web credentials through man-in-the-middle attacks or exploit vulnerabilities in certificate management. By gaining access to authentication certificates or compromising web-based authentication, attackers can impersonate legitimate users and access sensitive systems or data.

Procedure Examples

APT28, also known as Fancy Bear, is notorious for stealing authentication certificates during phishing campaigns. By acquiring these certificates, they can bypass two-factor authentication mechanisms, gaining unauthorized access to secure systems with greater ease.

APT41, on the other hand, has been observed using forged authentication certificates to impersonate trusted systems, particularly during supply chain attacks. This tactic allows them to infiltrate networks by presenting themselves as legitimate entities, making it difficult for security measures to detect their malicious activities.

Mitigation Techniques: To protect stored passwords against brute-force attacks, organizations should use strong hashing algorithms like bcrypt or Argon2, which are specifically designed to resist such attacks by making password cracking computationally intensive. Implementing account lockout policies that temporarily disable accounts after a set number of failed login attempts can further prevent automated brute-force attempts. Additionally, salting passwords before hashing them enhances security by adding unique values to each password, making it more challenging for attackers to crack stored password hashes, even if they obtain the hash data.

3.9 Discovery

After gaining credential access from different techniques, the attacker will try to discover different resources and networks and gain knowledge about the system.(Cyber Security & Infrastructure Security Agency, 2020) Let's dive into different techniques:

3.9.1 Permission Groups Discovery

After gaining credential access from different techniques, the attacker will try to discover different resources and networks and gain knowledge about the system. Let's dive into different techniques:

- *Local Groups*: Attackers can investigate different local groups and their permission settings. This information will help them understand what users exist in each group and how they are categorized. Tools like BloodHound, Chimera, Cobalt Strike, and many more. (Cyber Security & Infrastructure Security Agency, 2020)
- *Domain Groups*: Attackers can investigate domain groups and their permissions. This will help the attacker understand what domain groups exist and the users belonging to those groups. The main motive is to find users with domain administrator rights. Tools users are Adfind, BlackCat, CrackMapExec, and Inception to help enumerate Domain groups. (Cyber Security & Infrastructure Security Agency, 2020)
- *Cloud Groups*: Attackers investigate cloud user groups and their permissions to find certain users with cloud infrastructure rights. The cloud providers use API for providing permission groups. For example, the command "az ad user get-member-groups" will list all user groups. Tools like ROADTools, AADInternals, and Pacu are used for enumerating Cloud Domains.("Mitre ATT&CK®", 2020)

3.9.2 System network Configuration Discovery

Through this technique, attackers will discover different network settings and configurations, by looking at their MAC and IP addresses, ARP table, Net BIOS, nbstat, and many more.("Mitre ATT&CK®", 2020)

As an attacker has already access to many networks, they could easily discover network information by using different Linux commands like Arp, ifconfig/config, nbstat, TCP, and routing table.("Mitre ATT&CK®", 2020)

3.9.3 File and Directory Discovery

The attacker could enumerate different files and directories by searching different locations in the network. Commands like tree, ls, find, locate, and dir to gather files. Attackers investigate these files to try to discover more sensitive information and user permissions which will help them impact the system.("Mitre ATT&CK®", 2020) Different procedures like:

- *AcidRain*: Linux command is used to find files related to storage devices.
- *Action RAT*: Tool to collect files and drive on the infected machine.
- *Babuk*: Ability to enumerate files and folders on the targeted system
- *BlackCat*: Can enumerate files used for encryption.

3.9.4 Cloud Infrastructure Discovery

In this technique, an attacker tries to discover resources and information that are available in the Cloud Infrastructure environment known as IaaS known as Infrastructure-as-a-service. Different network resources such as virtual machines, snapshots, instances, and other database and storage devices.("Mitre ATT&CK®", 2020)

Cloud Providers offer various Infrastructure information through API and command through CLI. For example, AWS provides different commands that could be used by attackers to discover different instances and files about the cloud Infrastructure:

- *Describe Instances*: Amazon EC2 API that returns information about two or more instances in an account.
- *List Buckets*: Returns all sets of buckets by the authenticated servers. ("Mitre ATT&CK®", 2020)
- *HeadBucket*: Shows all permissions about the user and existent buckets.("Mitre ATT&CK®", 2020)
- *GetPublicAccessBlock*: Getting public Access Block for an existent bucket.
- *DescibeDBInstances*: Help determine all database information like size, owner, networks, and permissions. ("Mitre ATT&CK®", 2020)

Through this information, an attacker can enumerate more resources by compromising different access keys of cloud infrastructure and get resources for further attack. Tools like Pacu enumerate EC2 instances which are crucial in AWS Infrastructure. Along with Scattered Spider used to identify access resources, containers, and backup management. ("Mitre ATT&CK®", 2020)

3.10 Lateral movement

Let's go through some of the sub-techniques used for lateral Movement:

3.10.1 Exploitation of Remote Services

Attackers will gain unauthorized access by exploiting internal systems of the network and doing lateral movement inside the target. Exploitation of software can be done by finding vulnerabilities like no sanitization of code, or multiple programming errors in software or kernel. By exploiting this software, an attacker can easily move in the system by doing lateral movement inside the network.("Mitre ATT&CK®", 2020)

There are many vulnerabilities found in different services such as MYSQL, SMB, and RDP which can be exploited by attacks like XSS, Cross-site request forgery, and SQL Injection. There are different tools and procedures used for exploiting Remote services:

- *Bad Rabbit*: SMB exploit which spreads through victim networks.
- *Lucifer*: Exploit multiple vulnerabilities like (CVE-2019-0708) Eternal Blue and many more.("Mitre ATT&CK®", 2020)
- *Fox Kitten*: Exploits well-known vulnerabilities including RDP.("Mitre ATT&CK®", 2020)
- *Stuxnet*: Propagates using Print Spooler MS10-061 and MS08-067 and other Windows server service vulnerabilities.("Mitre ATT&CK®", 2020)

3.10.2 Remote Service Session Hijacking

This technique means hijacking an existing section of Remote services to smoothly move laterally from one place to another. In Credential Access, attackers use valid credentials and use them to hijack these existing sessions.("Mitre ATT&CK®", 2020) Session hijacking can be

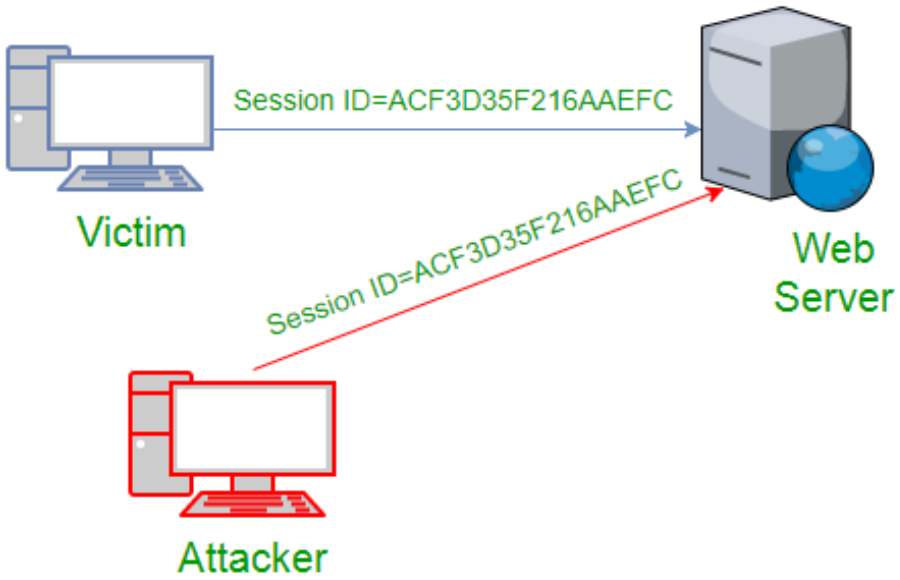

Figure 6: Remote Service Session Hijacking
(GeeksforGeeks, n.d.)

done in two parts:

- *SSH Hijacking*: SSH stands for Secure Shell which is a standard means of remote access in Linux and MacOS. SSH helps a user connect to another system remotely through a symmetric or asymmetric encryption tunnel, or commonly through a digital certificate and credentials. By SSH hijacking, an attacker can laterally move into the system without getting detected and also get access to other third parties' servers as well.(Adam Boileau, n.d.)
- *RDP Hijacking*: RDP stands for Remote Desktop, which means the software used for providing remote access to different systems. By Hijacking the RDP session, attackers can move laterally in the system without the use of stolen credentials.("Mitre ATT&CK®", 2020) This hijacking can be done by 2 procedures mainly:
  Axiom: Target specific victims with remote desktops. **WannaCry**: executes malware through enumerating existing remote desktops.

3.10.3 Remote Services

This technique is done by logging into valid accounts and then without getting caught, doing lateral movement to the system. In an enterprise, an attacker can convert workstations and servers into domains. ("Mitre ATT&CK®", 2020)

They could also enter secure shell and remote desktops by exploiting different remote services. There are many ways to use Remote Services such as:

- *SMB/Windows Admin Share*: SMB is a file in Windows used for serial port sharing in the same network or domain. Through using SMB, attackers can easily move into the system through file sharing.

- *RDP Hijacking*: VNCs are remote desktops but only share screens with other systems, and valid credentials can be exploited.("Mitre ATT&CK®", 2020)
  Axiom: Target specific victims with remote desktops. **WannaCry**: executes malware through enumerating existing remote desktops.

- *DCOM*: COM stands for Component Object Model which is a Windows API and helps interact with different interfaces and executables. DCOM (Distributed Component Object Model) is an extended functionality of COM that uses remote procedure call technology. By getting privileged user access, one can obtain all shellcode executions through Microsoft Office and macros from documents, and all other executable files. Cobalt Strike, Empire, and SILENTTRINITY are procedures used for DCOM.("Mitre ATT&CK®", 2020)

- *Software Deployment Tools*: By using different tools, attackers can gain access to the software already installed in the enterprise to move laterally in the system by executing different commands. Some of the software might also be used for administrative purposes and integrated with CI/CD pipelines. Altiris, AWS, Microsoft, Intune, and Azure are some of the examples of Software solutions mainly used in Enterprise.("Mitre ATT&CK®", 2020) Different Procedures used are as follows:
  Sandworm team: Uses Remote Exec for remote code execution and moves into the system. **Silence**: uses RAdmin, and remotely executes workstations and ATM. **Threat Group − 1314**: This group exploited the victim's Altiris, which is an endpoint management platform. **APT32**: This group exploited McAfee ePO for Lateral Movement in the system.

3.11 Collection

After successfully moving throughout the system, Attackers will try to collect as much data and resources as possible for goal accomplishment. ("Mitre ATT&CK®", 2020)Different techniques used to collect data are:

- *Adversary-in-the-middle*: Using this technique, the Attacker tries to position himself between multiple networks and tries to perform network sniffing and Data manipulation. It is also called Man in the Middle Attack. ARP cache poisoning and DHCP snooping can also help in (AiTM) attack.
- *Audio Capture*: Collecting data by leveraging different multimedia devices like webcams, microphones, phone cameras, and other applications to get sensitive information.
- *Archive Collected Data*: After collecting all data, the Attacker can encrypt and compress the data. Archive can be done through utility, Library, and custom methods.
- *Data from Cloud Storage*: Collecting data from Cloud storage.
- *Code Repositories*: Attackers may leverage source code and software with automated software builds, Attackers can leverage git files, internal hosts, and other third-party interference.

3.12 Command & Control

In this tactic, Attackers will try to communicate through the target system with a focus on controlling them and staying undetected. Attackers will try to communicate with normal traffic to stay undetected. ("Mitre ATT&CK®", 2020)Different techniques used for Command and Control are as follows:

3.12.1 Application Layer Protocol

Attackers may communicate through the OSI Application layer and bind through normal traffic to avoid detection. Any commands given through the remote system will be embedded within different protocols used for web browsing, file transfer, emails, and DNS.(Doug Bienstock et al., 2020) Let's dig deep into some of the protocols:

- **Web Protocols**: These protocols are the ones used for web trafficking which include HTTPS, TLS, and Web sockets that carry common traffic. Procedures like 3PARA RAT, 4H RAT, ABK, and Action RAT use HTTP for command and control.
- **File Transfer Protocol**: FTP Protocols include file transfer protocols such as FTP, FTPS, TFTP, and SMB which could be common traffic environments used to avoid detection. Procedures like BADHATCH, CARROTBALL, Disco, and Dragonfly have used FTP protocols for command and control.("Mitre ATT&CK®", 2020)
- **Mail Protocol**: SMTP, IMAP. POP3 are protocols used for electronic mail which include normal traffic used for detection. Procedures like BadPatch, Cannon, CHOPSTICK, COMRat, and Kimsuky use mail protocol for C2. ("Mitre ATT&CK®", 2020)
- **DNS Protocol**: These are protocols used for the Domain name system, along with administrative functions in the network. This could be the most used protocol because DNS traffic could be allowed before getting authenticated by using various methods like DNS tunneling. Procedures like Anchor, Chimera, Cobalt Group and Strike, and Cobian RAT use DNS tunneling for Command and Control.("Mitre ATT&CK®", 2020)

3.12.2 Data Obfuscation

Data obfuscation means hiding data from the network in such a way that it is not possible to detect it in the network. These commands are hidden in an extra layer of data or security so that it is not detected by the common traffic.(Draco Team - Bitefinder, n.d.) Techniques used for Data obfuscation are:

- **Junk Data**: The attacker can add junk data within significant commands to confuse network traffic to not get detected. This could be done by prepending junk data, adding a junk file under a significant file, methods for deciphering, and many more. Procedures like GoldMax, Kevin, Mori, and P8RAT use different Junk data techniques for command and control.(Draco Team - Bitefinder, n.d.)
- **File Transfer Protocol**: Steganography means hiding malware or commands inside an image, txt file, or pdf file to make detection more difficult. This technique can be also used for compromising a system by adding malware into an image file or adding a command to a document file. Procedures like Axiom, Daserf, LightNeuron, and RDAT are used for hiding malware and commands in images and document files.(Draco Team - Bitefinder, n.d.)
- **Protocol Impersonation**: This technique is to impersonate legitimate protocols to not get detected. Attackers can create fake SSL and TLS handshake, and make it look legitimate for not getting detected. Procedures like FakeM, FALLCHILL, and Higaisa are used for impersonating protocols.(Draco Team - Bitefinder, n.d.)

3.12.3 Proxy

: Attackers can use a proxy network to be undetected in the network traffic, Many tools like ZXPortMap, HTRAN, and ZXProxy. Attackers mostly use proxies for managing C2 channels, redirecting, and reducing numbers of outbound connections, and can also ride over existing trusted communications. They can also create multiple proxies and create a pathway for malicious traffic.(Draco Team - Bitefinder, n.d.)

Procedure:

- **Aria-body**: Ability to communicate through reverse SOCKS proxy.
- **BADCALL**: SProxy server between victim network and attacker network.
- **Blue Mockingbird**: Use ssf, Venom, and frp for establishing a SOCKS proxy.
- **Earth Lucasa**: Successfully adopted Cloudflare as a proxy for compromised servers.

3.12.4 Encrypted Channel

Instead of relying on different ways to stay undetected in normal traffic, Attackers will create an encryption channel to hide command and control traffic.("Mitre ATT&CK®", 2020) There are 2 Encryption channels as follows:

- **Symmetric Cryptography**: These encryption channels use a single key for encryption and decryption. DES, 3DES, AES, and RC4 are examples of Symmetric Cryptography. Procedures like ADVSTORESHELL, APT28, Attor, Bandook, and Bazar used different symmetric cryptosystems like AES, XOR, and custom encryption for communication.

- **Asymmetric Cryptography**: Also known as public key cryptography uses two keys, one public key and one private key. A sender encrypts with the public key and the receiver decrypts the message on the private key. RSA and El-Gamal are popular asymmetric cryptography. Procedures like Cobalt group, ComRAT, COATHANGER, carbon, and BISCUIT use asymmetric cryptography for communication.

3.13 Exfiltration

This tactic uses different techniques to steal data from the target network. After collecting the data, Attackers avoid detecting it while removing it.("Mitre ATT&CK®", 2020)
Techniques:

3.13.1 Exfiltration on Alternate method

After stealing the data, the Attacker exfiltrates data to another protocol. This could be an encrypted or non-encrypted protocol. SMTP, FTP, DNS, TLS handshake, and SMB are alternate protocols that can be used to exfiltrate data. Different procedures like:

- **Chaes**: Exfiltrates collected data using MIME protocol.

- **Kobalos:**: Exfiltrated data and credentials over the UDP network.

- **Hydraq:**:Exfiltrated data through port 443.

- **AADInternals:**: Directly downloads cloud user's data such as AWS and One drive files.

3.13.2 Exfiltration over Web Services:

Attackers can use different web services for exfiltrating the data. These services provide an added layer of protection along with helping bypass firewalls as well.("Mitre ATT&CK®", 2020)

Procedures like Appleseed, DropBook, Magic Hound, and ngrok used web services for exfiltrating data.

3.13.3 Transfer Data to Cloud Account

Attackers can exfiltrate the data including backup, sharing, and syncing to a cloud account to which they have access in the system. Attackers would avoid external network interfaces and look to utilize existing cloud users' accounts in the same cloud provider to blend in with the normal system.("Mitre ATT&CK®", 2020)

3.14 Impact

This is the last tactic of the MITRE Attack in which attackers accomplish their goal by disrupting the system or asking for ransomware and many more. This impact differs on whether attackers have some personal agenda or monetary gains.(“Mitre ATT&CK®”, 2020)Some of the Impacts done by APT attacks are :

3.14.1 Network Denial of Service

: A network DOS attack is when an attacker sends malicious traffic to the target way larger than the bandwidth capacity with a motive to disrupt the target network. For example, an attacker would send 8gbps of traffic to a network with a bandwidth capacity of 800mbps.(“Mitre ATT&CK®”, 2020)

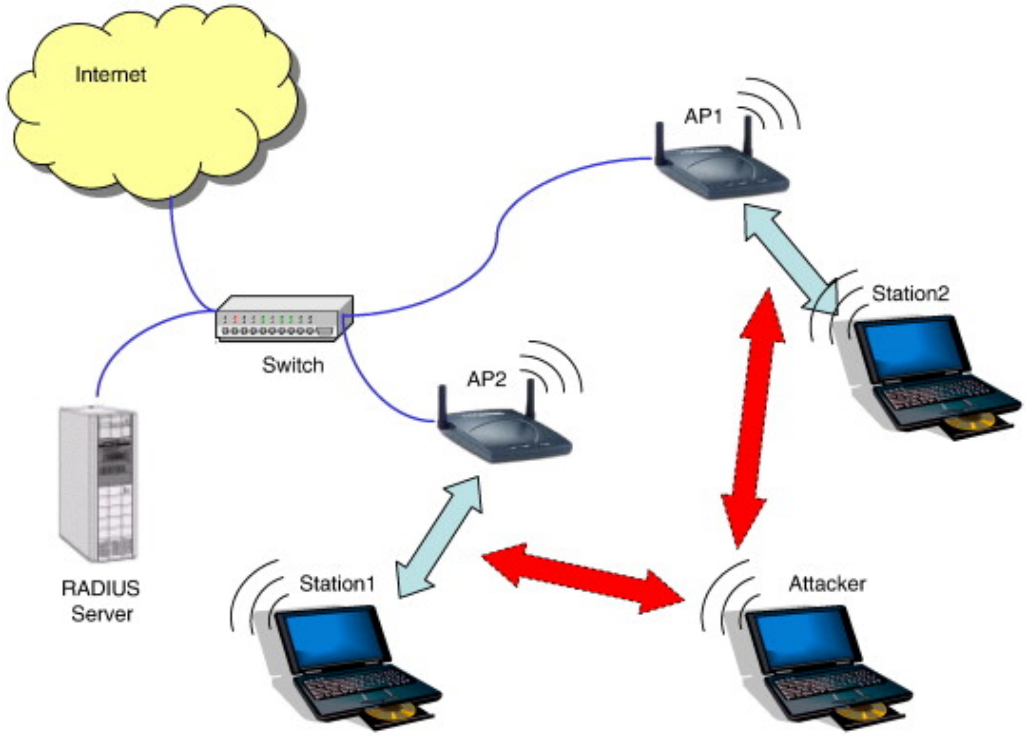

Figure 7: Network Denial of Service
(Kemal Bicakci & Bulent Tavli, n.d.)

Network Flood Attack and Reflection Amplification are two techniques used for DOS attacks. (“Mitre ATT&CK®”, 2020)

3.14.2 Data Manipulation

: An attacker can manipulate the integrity of the company by updating, adding, or deleting data with a motive to influence internal and external outcomes and hide certain activities. ("Mitre ATT&CK®", 2020)

For example, attackers will try to manipulate data to change company planning strategies, decision-making, and other organizational activities. ("Mitre ATT&CK®", 2020)An attacker can manipulate data in three ways:

- **Stored Data Manipulation**: Manipulating stored data such as Microsoft Office files, database files, source code files, and many more.
- **Transmitted Data Manipulation:**: Manipulating data on a network or between two connections by adding a tool and changing the response. Burp-suite is a good example of transmitting data.
- **Runtime Data Manipulation:**: Manipulating data by altering application binaries on runtime.

3.14.3 Data Encrypted for Impact

Attackers may encrypt most parts of impact areas to disrupt the availability of the target system. This impact can be done to gain monetary compensation for a decrypt key. Key. An attacker may reboot the system which can be opened with a decryption key or change different data files like PDFs, and office files and encrypt them to disrupt availability to users.("Mitre ATT&CK®", 2020)

Procedures like Babuk, Avaddon, BlackCat, and Akira used Encryption to impact their target system.

4 Mitigation Framework

4.1 Mitigation through Social Engineering

Social Engineering plays an important role as a key element of Advanced Persistent Threats (APT), manipulating human psychology to infiltrate networks and systems to bypass initial safeguards. By employing trust, authority, and manipulation, attackers mislead others into behaviors that jeopardize security. According to Santhosh Kumar, social engineering attacks follow a structured lifecycle comprising phases such as investigation, manipulation, execution, and exit. Understanding this lifecycle is essential for preventing victimization, as attackers often employ sophisticated methods to deceive their targets (Birthriya et al., n.d.).

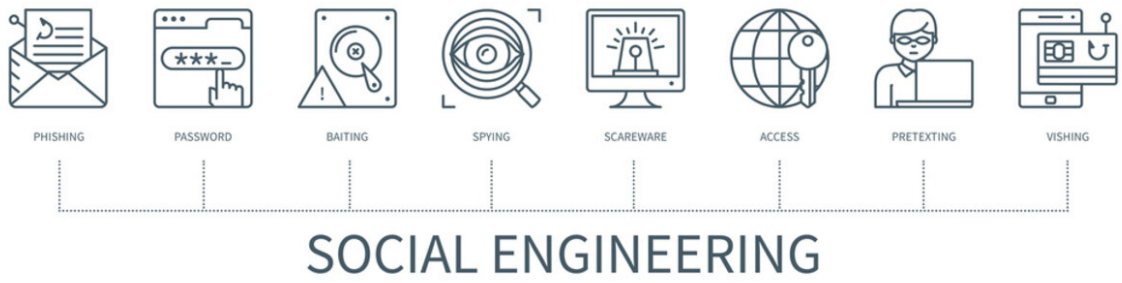

Figure 8: Social Engineering

Social engineering assaults rely heavily on exploiting human vulnerabilities, using psychological tactics to coerce individuals into divulging private information, or performing actions that compromise security. Birthriya et al. emphasize that social engineering attacks are "particularly dangerous due to their ability to bypass technical defenses by targeting human nature." Severe cases, like a CEO authorizing a fraudulent payment resulting in a financial loss of approximately $ 37 million, highlight the effectiveness of trust-based exploitation. The authors stress that "the ripple effects of a single social engineering incident can lead to significant financial and reputational damage" (Birthriya et al., n.d.). The prevalence and growth of social engineering attacks further emphasize the need to address these risks. The APWG (2022) noted a 500% increase in social engineering incidents within a single quarter in 2018, underscoring the rapid escalation of these threats in the cyber environment (apwg2022). Social engineering tactics were involved in a significant percentage of cyberattacks, with 43% of IT workers reporting targeted attacks in 2021 alone. This highlights the susceptibility of organizations to these techniques.

Birthriya et al. also discuss the structured lifecycle of social engineering attacks, which includes research, manipulation, execution, and exit phases. Understanding these phases is crucial, as "the cyclical nature of these attacks allows threat actors to adapt and refine their methods, making early detection and intervention vital." This lifecycle perspective reinforces the need for a comprehensive, layered strategy combining proactive protection with constant vigilance. Ultimately, Birthriya et al. conclude that social engineering attacks are not only prevalent but also highly successful due to their reliance on human psychology. This makes them a top cybersecurity priority, as they can bypass even advanced technical defenses. The authors advocate for a "multi-layered defense, combining technical measures with comprehensive security awareness training" to mitigate the ongoing threat posed by social engineering (Birthriya et al., n.d.).

Organizations should implement robust network segmentation and intrusion detection systems to mitigate reconnaissance tactics and monitor exposure. Techniques such as active scanning (T1595), regular patch management, and IDS can help in identifying and mitigating potential threats. When adversaries gather victim identification information (T1589), educating employees on social media awareness and using multi-factor authentication (MFA) can prevent exploitation. Monitoring outbound traffic and segmenting internal networks help reduce lateral movement during network information gathering (T1590). Phishing attacks (T1598) can be mitigated with security awareness training, advanced email filtering, and web filtering systems that block malicious websites and scripts ("Mitre ATT&CK®", 2020; Steffens, 2020).

During the resource development phase, strategies like MFA and threat intelligence monitoring are crucial when adversaries attempt to gain access (T1583). To detect compromised infrastructure (T1584), monitoring domains and IPs and maintaining patch management are essential to address vulnerabilities. Compromised accounts (T1586) can be safeguarded through strong credential policies and access monitoring, while the creation of fake accounts (T1585) requires tools to detect and enforce identity verification ("Mitre ATT&CK®", 2020; Steffens, 2020)

Mitigating initial access tactics requires rigorous vendor risk management to address supply chain compromises (T1195), particularly by conducting integrity checks on third-party software and isolating critical systems. Implementing MFA and vulnerability management on external remote services (T1133) reduces unauthorized access, while strong password policies, regular credential rotation, and access controls help prevent unauthorized use of valid accounts (T1078). Browser isolation, web filtering, and script-blocking extensions can protect against drive-by compromises (T1189), safeguarding against browser-based attacks and malicious ads (Zhang et al., 2024).

4.2 Mitigation Through Authentication Control

Advanced Persistent Threats (APTs) represent a significant challenge to organizations by exploiting vulnerabilities to infiltrate systems and persist within networks. Combatting such threats requires a layered defense strategy, with authentication control playing a central role. Proper authentication control, which encompasses the processes and technologies that verify user identities and secure access to critical systems, can significantly mitigate the techniques used by APT actors in areas such as persistence, privilege escalation, defense evasion, and credential access. By deploying comprehensive authentication mechanisms, organizations can enhance their defense posture and limit the scope of potential breaches.

Authentication control is particularly crucial in preventing persistence techniques used by APTs to maintain long-term access. According to Ross Anderson, in his seminal work *Security Engineering*, "secure system design should not rely on just one layer of defense but rather a multi-faceted approach that incorporates strong authentication, access control, and real-time monitoring" (Anderson, 2020). Anderson's emphasis on layered defenses resonates well with the idea of using multi-factor authentication (MFA) as a central component of preventing persistence. MFA ensures that even if attackers create or modify accounts, they will require additional factors beyond credentials, such as biometric verification or one-time passcodes, to access the system. This approach contrasts with Bruce Schneier's more cryptography-focused perspective. In *Applied Cryptography*, Schneier advocates for securing authentication through strong cryptographic protocols, stating that "properly designed cryptographic systems make it

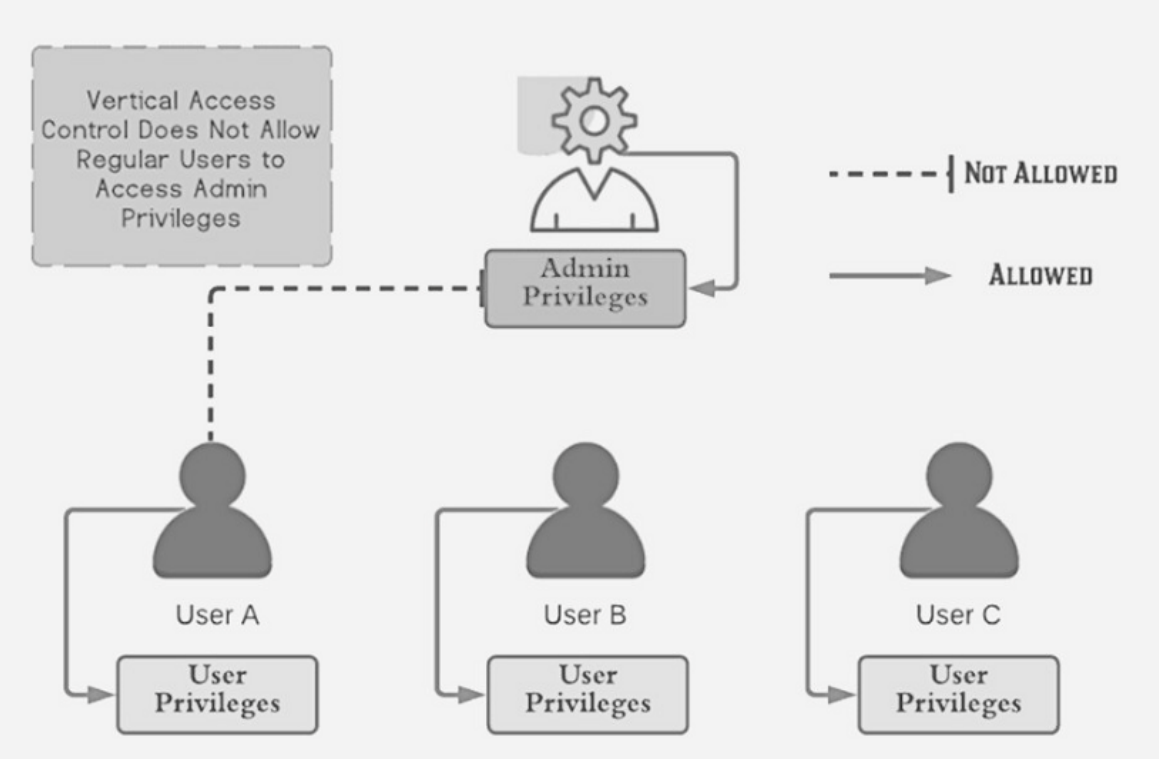

Figure 9: Broken Authentication Control
(Alessandro Parisi, n.d.)

nearly impossible for adversaries to persist undetected" (Schneier, 2015). While cryptography is vital in securing communications, Anderson's broader view of layered authentication mechanisms, including session timeouts and privileged access management (PAM), offers a more comprehensive solution to combatting APT persistence.

Privilege escalation is another key tactic used by APTs, where attackers seek to gain higher-level permissions within a compromised system. Richard Bejtlich, in *The Practice of Network Security Monitoring*, emphasizes the importance of continuous monitoring for privilege abuse, arguing that "real-time detection is essential for identifying when attackers are attempting to elevate their privileges"(Bejtlich, 2013). While Bejtlich focuses on detecting and responding to suspicious activities as they occur, Anderson advocates for a proactive approach, stating that "role-based access control (RBAC) should be used to limit users and processes to only the permissions necessary for their tasks" (Anderson, 2020). This preventative method reduces the opportunities for attackers to escalate privileges in the first place. The least privilege principle, which both Anderson and Bejtlich agree on, is crucial for minimizing the attack surface for privilege escalation attempts(Bejtlich, 2013). By comparing these perspectives, it becomes evident that combining both proactive access control measures and real-time monitoring offers the strongest defense against privilege escalation.

When it comes to defense evasion, attackers often attempt to bypass security mechanisms by disabling security tools, weakening encryption protocols, or disguising their activities as legitimate processes. Michal Zalewski, in *The Tangled Web*, stresses the importance of securing authentication at the web application level, noting that "robust authentication mechanisms, such as certificate pinning and secure API gateways, are critical in preventing attackers from masquerading as legitimate users" (Zalewski, 2012). Zalewski's focus on securing the application layer complements Anderson's broader emphasis on tamper-resistant authentication controls. Meanwhile, Schneier's evasion approach revolves around using encryption to secure data flows, stating that "encryption serves as the first and last line of defense in protecting sensitive information" (Schneier, 2015). While encryption is essential, it is clear that a more holistic approach—one that includes tamper-proof authentication and continuous logging of authentication events—is needed to combat the diverse methods of defense evasion that APTs employ.

Credential access, often achieved through techniques such as adversary-in-the-middle attacks, brute force, or exploiting unsecured credentials, can be effectively mitigated through strong authentication practices. Yuri Diogenes and Erdal Ozkaya, in *Cybersecurity Attack and Defense Strategies*, argue that "multi-factor authentication and strong password policies are the backbone of any strategy to prevent credential theft and exploitation" (Diogenes & Ozkaya, 2018). Their focus on robust password policies aligns with Schneier's recommendation for using cryptographic measures like secure hashing and salted passwords to protect stored credentials. Diogenes and Ozkaya, however, go further by advocating for the use of password vaults and credential vaulting solutions to ensure that credentials are not exposed in plaintext in configuration files or scripts. Anderson supports this perspective by stating that "secure storage of credentials should be treated with the same priority as securing network access itself" (Anderson, 2020). Together, these approaches highlight the need for a combination of cryptographic protections, strong password policies, and secure storage mechanisms to mitigate credential access.

4.3 Mitigation using Machine Learning Model and Encryption

As discussed the two techniques of Mitigating APT, the Authors C.N.S Vinoth Kumar and U.Sakthivelu in their article "Advanced Persistent Threat Detection Using Machine Learning Model". They talked about various techniques used for detecting and mitigating like Combination with Malware detectors, Adverbial ML-Based Attack Detection methods, and many more, and found a lot of limitations. Their main focus is to detect attackers when they are in the Lateral Movement process and use Cryptography and Machine Learning to detect Remote Desktop Movements during the Lateral Movement Process.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)
The authors' focus was to look into limitations in the log event datasets from the Internet which are used to depict the real user. These datasets are taken from a laboratory called Los Alamos National Laboratory. To train and test the machine learning algorithms, we need significant datasets. Hence, certain limitations were found for generic intrusion datasets like not effectively detecting attackers in the Internal network, normal attacking behavior being surmised, data imbalance, and many more.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

4.3.1 The Lateral Movement Detection Algorithm

To remove all limitations, the author came up with a solution to combine a comprehensive and unified dataset without changing real users' behavior. The comprehensive dataset is host-based public telemetry records datasets that are publicly available. Unified datasets are sets of data formats lowered for further research, quantitative comparisons, and reproduction of data. However, to overcome the limitations mentioned before, they added malicious code from a comprehensive to the unified dataset to see the attack patterns and different properties within the enterprise. To understand properly. In a comprehensive dataset, let's term malicious logon events as 'LE', and RDP logon events could be termed as 'P' in the unified set. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Now Source host 'Slea' is directly mapped for every element 'e' belongs LE on Snj, which randomly selected unique hosts from event ej belongs to P. For event e Ui, Dk, represents tuple username and it mapped to Uk, Dk,, a randomly selected tuple which belongs to P. After successfully implementing this equation, the malicious event is inserted into datasets chronologically. Below is the proper algorithm for injection of the malicious event of RDP known as Remote Desktop Protocol Authentication events where is the mean of session duration, 2 is the variance x is the set of different source hosts, and y is the set of the malicious source host. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

4.3.2 Defense Mechanism

Hence, they came up with a defense mechanism that acts as soon as attackers move into the system and limits their presence by introducing a dynamic deception model that uses two methods, 1. Synchronizing Sockets and 2. Generating IP Address. These processes use cryptography like hybrid encryption and symmetric block cipher encryption, along with the Hidden Markov Model, which is used for time selection, and DHCP will help enable dynamic policy allocation.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

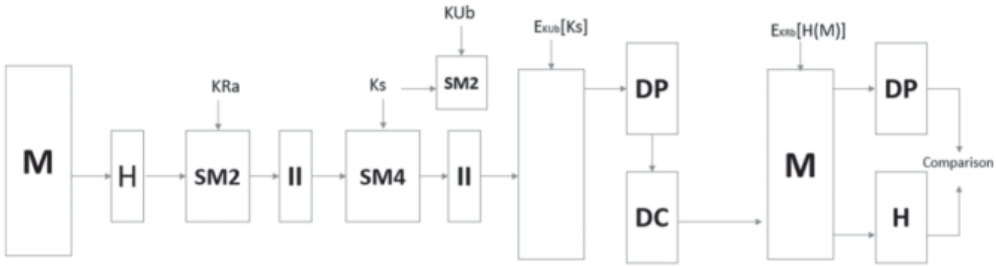

Figure 10: Encryption Method(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

4.3.3 Socket Synchronization and IP Address Generation

The reason for choosing socket is because it is easier for synchronizing and is divided into two protocols, TCP and UDP. Sockets also don't require any fixed port, which makes it difficult for attackers to penetrate.

The Author designed a hybrid encryption based on the socket synchronizing communication

Algorithm 1: Malicious Remote Desktop Protocol authentication events injection

Initialize: μ, σ^2, x and y/malicious and benign variables
1: Malicious_AuthTuple ← ("username" + "destination event")/in benign
2: Benign_AuthTuple ← ("username" + "destination event")/in malicious
/Dictionary mapping malicious and benign data from source
3: Source ← dict{}
4: **for each** host ∈ y
5: Source[host] ← x.randomPop()
6: **End**
/Dictionary mapping malicious and benign data from the tuple
7: AuthTuple ← dict{}
8: **for each** tuple ∈ Malicious_AuthTuple **do**
9: AuthTuple[tuple] ← Benign_AuthTuple.randomPop()
10: **End**
/Rewrite malicious event fields and insert them in benign
11: **for each** event ∈ Malicious, **do**
12: new source ← Source[event.Host]
13: newuser ← AuthTuple[event.Tuple]username
14: newdestination ← AuthTuple[event.Tuple]destination
15: session ← GaussianRandom(μ, σ^2)
16: modified ← newEvent
17: append.Benign(modified)
18: **End**
19: **return** Benign

Figure 11: Algorithm 1(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

technology. The figure shows the encryption and identification process where M stands for plaintext, and H stands for hash algorithm. The message and Hash value sign the SM2 and package II value and further processing SM4 Algorithm. At the receiver part, decrypting the sender's public key is used for SM4 Hashing.

A total of 32 rounds in non-linear iterations are carried out through SM4 encryption and key expansion, generated through pseudo-random and incorporated by the dynamically generated IP Address Table. Along with this process, block cipher chaining is done where the previous iteration is XORed with the initial round. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Hidden Markov Model:
This Model is used to determine the proper transition probability in a way, such as qi termed as the current state, and qi+1 is termed as the future state.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023) In simple terms, HMM can be described as :
= (A, B,)

4.3.4 Update Algorithms

Update Algorithms is a heuristic search algorithm used for identifying the defense action in real time. This algorithm will help give a security alert whenever there is a movement from the attacker using attacker using a security model structure. Below is the Algorithm used for Update Algorithm.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Algorithm 2: Belief Update Algorithm

Initialize: n_k, $\propto_{t+1}= U_{a(r,f)}$, added_num=0
1. **procedure** Belief_Update ($\propto_t, u_r, y_r$)
2: **while** added_num $<n_k$ **do**
3: $(s, \varphi) \sim \propto_t$
4: $(s, \varphi, y, -) \sim G(s, \varphi, u_r)$
5: if $y^{Z(s)} = y_r^{Z(s)}$ then
6: $\propto_{t+1} \leftarrow \propto_{t+1} U \{s', \varphi'\}$
7: added_num←added_num+1

Figure 12: Update Algorithm(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

After the author explained all these terms, they evaluated experiments with different Mathematical modeling, in which there are different equations from the arrival of attack to detecting malicious payloads, delays, and defender optimum action. Then they did Evaluation Metrics in which they used an Intel Laptop with 32 GB RAM, Azure VM for training supervised learning, and unsupervised learning worked in Intel Xeon with AVX enabled core and 1TB memory. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Different Machine learning techniques are also used which are as follows:

malicious RDP sessions.

$$Accuracy = \frac{TP + TN}{Total\ subjects} \times 100\%$$

$$Precision = \frac{TP}{TP + FP} \times 100\%$$

$$F1\ score = 2 \times \frac{TP}{TP + FN}$$

$$Sensitivity/Recall = \frac{TP}{TP + FN} \times 100\%$$

$$AP\ score = \sum_n (Recall_n - Recall_{n-1}) \times Precision$$

$$Sepcificity = \frac{TN}{FP + TN} \times 100\%$$

$$GMeean = \sqrt{Sensitivity + Specificity}$$

Figure 13: ML Metrics(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

TP refers to True Positive, TN means True Negative, FP is False Positive, and FN is False Negative. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Table 2: Estimation of performance metrics during detection of RDP session with ML classifiers

Classifier	Accuracy	Precision	F1 score	Recall
RF	99.8%	99.6%	0.96	96.0%
LR	98.4%	10.7%	0.03	1.3%
GNB	99.4%	86.3%	0.85	83.1%
FNN	96.6%	0%	0	0%
DTC	99.9%	99%	0.95	92.6%
AdaBoost	99.9%	99.9%	0.99	99.8%

Figure 14: Research table(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

By using these ML metrics, different mathematics equations, and evaluations, the author came up with a table that shows that the detection of RDP sessions using these ML classifiers helps get good results as shown in the table Figure. (U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

Hence, we can see this encryption algorithm and Machine learning Model, an enterprise can detect and mitigate attackers, whenever they try to move into the system internally.(U. Sakthivelu & C. N. S. Vinoth Kumar, 2023)

4.4 Comparative Analysis

A multifaceted strategy that integrates the advantages of encryption, social engineering defenses, and authentication management is needed to mitigate Advanced Persistent Threats (APTs). Each of these strategies has its advantages and disadvantages. Authentication control, such as multi-factor authentication (MFA) and role-based access control (RBAC), provides a strong defense at system entry points by ensuring that only authorized users are granted access. While it is effective at limiting privilege escalation and monitoring access in real-time, it can be time-consuming to implement and may not handle all insider risks. Social engineering defenses, which rely on educating employees to recognize and reject manipulation techniques such as phishing, are critical in addressing human vulnerabilities. However, even well-trained personnel can make mistakes, and this strategy is strongly reliant on human behavior, which is naturally unpredictable. Encryption techniques, on the other hand, secure data in transit and at rest, safeguarding critical information even if hackers gain access to systems. While encryption is extremely successful at avoiding data breaches and lateral movement, it does impose computational costs and necessitates complex key management to be entirely effective.

Considering the advantages and disadvantages of each method, the most complete defense against APTs is provided by an integrated mitigation framework that incorporates all three. Authentication control should serve as the foundation, with robust entry barriers and ongoing monitoring for suspicious activities. Social engineering defenses, such as regular training and awareness programs, assist limit human error and vulnerability to manipulation. Encryption techniques add an important layer of data security by assuring that even if attackers breach the system, they cannot simply access or modify sensitive information. Organizations may develop a strong defense strategy that tackles both the technological and human components of APT threats by combining these tactics, as well as continuous monitoring and real-time incident response capabilities. This multi-layered technique greatly decreases the danger posed by sophisticated adversaries while also improving the overall security posture of the organization.

Ultimately, the most effective mitigation technique against APTs involves a combination of the strategies discussed by these authors. A multi-layered authentication control system, as advocated by Anderson, forms the core of an organization's defense. This system should be enhanced by cryptographic protections as detailed by Schneier, ensuring that communication channels and credential stores are encrypted and secure(Schneier, 2015). Finally, continuous monitoring and real-time response capabilities, as recommended by Bejtlich, provide a crucial safety net, ensuring that any breaches are quickly detected and mitigated before they cause significant damage(Bejtlich, 2013). By integrating these approaches, organizations can build a robust defense against APTs, ensuring that their authentication controls are both resilient and adaptive to evolving threats.

5 Future Trends and Emerging Technologies

5.1 Use of AI

In the future, there are a lot of ways through which we can use Artificial Intelligence in detecting and preventing Advanced Persistent Threats and in comparison to that, an attacker can also use AI to perform more complex Attacks. To use AI, mostly one needs to give a piece of certain information like datasets for making them detect and prevent attacks. Let's see different ways to use AI in Advanced Persistent Threats:

5.1.1 Detecting APT in Mobile Devices

A lot of APT attacks happen through the mobile phones of employees, customers, and top authorities. The main focus of attacking is Social Engineer, other techniques like Watering Holes attack like MIMT, cross-site Scripting, SQL Injection, Application Repackaging attacks, and adding Malware into Mobile devices. Below is the figure showing different attacks.(Amjed Ahmed Al-Kadhimi et al., 2023)

These attacks happen because of different mobile vulnerabilities like downloading different third-party apps, stolen devices, different sensor vulnerabilities, employees clicking malicious links, and vulnerabilities in the Mobile Security Reference Architecture. (Amjed Ahmed Al-Kadhimi et al., 2023)
To mitigate these attacks, the Author came up with detecting APT attacks using AI techniques like gaming theory, machine learning, and deep algorithms. The author suggests that AI can benefit organizations to solve problems with different attacks. APT attacks mostly are very hard for a small team to prevent and mitigate, hence, AI can help easily process an enormous information about the APT system and then detect the Attack with proper accuracy. Author speculations are that False positive alerts will be reduced if we use AI.(Amjed Ahmed Al-Kadhimi et al., 2023)

5.1.2 Different Techniques Used With AI:

The first tool for detecting APT attacks was the use of OmniDroid, which is a collection of over 20,000 genuine malware samples that are used for modern attacks, which helps developers create an anti-malware system and also detect and prevent Android malware. (Amjed Ahmed Al-Kadhimi et al., 2023)

After that, there is the use of deep learning with AI using an application called DDefender which helps detect any malicious app on the device with 50 percent accuracy. Other tools like Betalogger which helps prevent the leaking of personal information using deep learning, DeepAMD used for detecting Android Malware, and 5G security architecture used for identifying threats and malware in 5G Networks.(Amjed Ahmed Al-Kadhimi et al., 2023)

5.1.3 Detecting Phishing Emails using AI

Phishing emails are one of the most common ways to perform an Initial stage attack. Hence detecting will help prevent attacks. Hence, AI can be used for detecting Phishing emails, the author talks about detecting spam emails through Perceptron, detecting spam images with SVM(Support vector Machines), logistics regression and decision trees, and adopting NLP.

Perceptron uses the method same as Neural networks used in the brain. It successfully implements neurons in AI. Just like neurons in the human brain, Perceptron will help give certain outputs of one or more levels of input. Because of this algorithm, one can easily detect phishing emails by looking at the outputs.

Hence, Perceptron can only detect through certain routes and is not flexible with a fixed margin. SVM is an extension, which can help detect emails using a support vector and use image instead of text. Along with that linear and regression methods are also used for detecting phishing emails by using scititk-learn and UCI-Machine learning and a technique known as one-hot encoding.

6 Recommendation

A comprehensive and multi-layered approach to cybersecurity is necessary for enterprises to reduce the threats posed by Advanced Persistent Threats (APTs). Strengthening detection, prevention, and response skills is the main goal of the following suggestions:

6.1 Boost Employee Awareness and Training

Organizations should make regular cybersecurity training for all staff a top priority because APTs usually use social engineering techniques like phishing to obtain access. Phishing attack simulations and real-time incident response exercises ought to be a part of this training. APTs frequently take advantage of human weaknesses, which can be lessened by training staff members to spot shady emails and websites.

6.2 Boost Authentication Mechanisms

To stop unwanted access, it is crucial to put in place robust authentication measures. All sensitive accounts, particularly those with administrative rights, ought to be required to use multi-factor authentication (MFA). This requires users to confirm their identification over several channels, adding degree of protection. To lower the risk of privilege escalation, role-based access control, or RBAC, should be used to make sure users have just the minimal access required for their function.

6.3 Deploy Advanced Machine Learning Models for Threat Detection

To detect and stop APTs during their lateral movement phase, machine learning techniques must be incorporated into the security framework. The detection of suspicious actions, such as odd login patterns, attempts at data exfiltration, or unexpected access to sensitive resources, can be improved with the application of machine learning models. Malicious activity during lateral movement can be detected and remote desktop motions can be monitored using machine learning and cryptography.

6.4 Implement Robust Encryption

It's critical to encrypt sensitive data both in transit and at rest. Even in the case of a security compromise, valuable assets should be protected by using advanced encryption standards. By preventing unwanted individuals from accessing or altering data, encryption lessens the impact of an APT. To prevent the system as a whole from being compromised if keys are compromised, encryption technologies must be supported by appropriate key management procedures.

6.5 Implementing Dynamic Deception Models

A dynamic deception model that simulates environments can perplex attackers and impede their advancement in addition to static defenses. To deceive attackers and restrict their capacity to conduct reconnaissance or escalate privileges, deception technologies may use socket synchronization, create fictitious IP addresses, or insert misleading data.

Organizations can use both preventive measures and enhanced detection techniques to create a more robust defense system against APTs by including these ideas. This all-encompassing strategy lowers the possibility of attacks while getting ready for the constantly changing cybersecurity threats.

7 Conclusion

This research concludes by examining the complex and multidimensional nature of Advanced Persistent Threats (APTs), a type of cyberattack that still poses a threat to organizations in a variety of industries. APTs are one of the most severe threats to global cybersecurity because of their tenacity, intelligence, and ability to go unnoticed while accomplishing their goals. By targeting susceptible systems and exploiting security flaws, APT attackers frequently get extended, unauthorized access to networks, allowing them to steal valuable information, modify data, and disrupt operations.

Analysis of technical frameworks, such as MITRE ATT&CK and the Cyber Kill Chain, has shed light on how APTs function and the steps attackers take to accomplish their goals. These frameworks enable security experts to identify and address the many techniques used by attackers, including reconnaissance and weaponization, command and control, exfiltration, and impact. Understanding these stages is critical for establishing effective defense measures that detect and mitigate APT attacks before they do irreversible damage.

The application of particular APT strategies, including active scanning, phishing for information, and compromise of third-party infrastructure, has been covered in length in this paper along with the lifecycle and stages of APT assaults. The employment of these approaches by well-known APT groups, such as APT29, APT28, and APT41, emphasizes the significance of both proactive and reactive actions. Security solutions must be updated and enhanced regularly to keep up with APT actors' changing tactics. Furthermore, the human component remains one of the most critical vulnerabilities, as many APT operations, particularly those that use phishing or social engineering, rely on human error to acquire early access.
To counter the risks posed by APTs, organizations must take a multifaceted approach to security, which includes advanced detection systems, regular vulnerability assessments, and complete threat intelligence plans. The use of machine learning models and encryption techniques can also help an organization detect and respond to lateral movement and other APT-related actions. The lateral movement detection technique, for example, shows how machine learning

may increase the detection of suspicious behavior within a network, lowering the possibility of an attacker going undetected.

Even though APT assaults are becoming more sophisticated, cybersecurity has a bright future. Emerging technologies, like as artificial intelligence (AI) and automation, have the potential to significantly improve the detection and mitigation of APT attacks. AI-based systems can increase real-time monitoring and incident response capabilities, lowering the time required to detect and neutralize APTs. Furthermore, ongoing changes to encryption mechanisms and authentication controls might provide a more durable defense against cyber adversaries' expanding arsenal of strategies.

However, our security strategy must change along with APTs. Organizations must be attentive and proactive, not only by adopting cutting-edge technological defenses but also by cultivating a cybersecurity-aware culture. Employee training programs that focus on detecting phishing attempts, safeguarding credentials, and adhering to best practices can dramatically minimize the likelihood of APTs acquiring a foothold in the first place.

In essence, the continued fight against APTs necessitates a combination of improved technology, intelligent security policy, and human awareness. Understanding the lifecycle of APTs, utilizing technical frameworks, and staying ahead of evolving threats can help organizations create a more secure environment that is better able to deal with the mounting problems of advanced cyber attacks.

References

Adam Boileau. (n.d.). Trust Transience: Post Intrusion SSH Hijacking. *Black Hat Briefings*.

Alam Zeb. (n.d.). Reconnaissance in cyber security. https://www.linkedin.com/pulse/reconnaissance-cyber-security-alam-zeb-m3cjf/

Alessandro Parisi. (n.d.). *Hands-On Artificial Intelligence for Cybersecurity : Implement Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies*. https://ebookcentral.proquest.com/lib/rmit/detail.action?docID=5847212#

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. *IEEE Communications Surveys & Tutorials*, *21*(2), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891

Amjed Ahmed Al-Kadhimi, Manmeet Mahinderjit Singh, & Mohd Nor Akmal Khalid. (2023). A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques. *MDPI*. https://doi.org/https://doi.org/10.3390/app13148056

Anderson, R. (2020). *Security Engineering:
*. John Wiley; Sons.

Anusthika Jeyashankar. (2022, January). Account Manipulation and Access Token Theft Attacks. https://www.socinvestigation.com/account-manipulation-and-access-token-theft-attacks/

Bejtlich, R. (2013). *The practice of network security monitoring: Understanding incident detection and response*. No Starch Press.

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (n.d.). A Comprehensive Survey of Social Engineering Attacks: Taxonomy of Attacks, Prevention, and Mitigation Strategies [Publisher: Routledge _eprint: https://doi.org/10.1080/19361610.2024.2372986]. *Journal of Applied Security Research*, *0*(0), 1–49. https://doi.org/10.1080/19361610.2024.2372986

Certified Ethical Hacker (CEH) version 12 (12th ed.). (n.d.). EC-Council.

Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats [Series Title: Lecture Notes in Computer Science]. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, C. Salinesi, M. C. Norrie, & Ó. Pastor (Eds.), *Advanced Information Systems Engineering* (pp. 63–72, Vol. 7908). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44885-4_5

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research*, *6*(23), 31–38. https://doi.org/10.19101/IJACR.2016.623006

Cyber Security & Infrastructure Security Agency. (2020, April). Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices. Retrieved September 21, 2024, from https://www.cisa.gov/news-events/alerts/2018/04/16/russian-state-sponsored-cyber-actors-targeting-network-infrastructure

Diogenes, Y., & Ozkaya, E. (2018). *Cybersecurity, attack and defense strategies: Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing.

Doug Bienstock, Melissa Derr, Josh Madeley, & Tyler McLellan. (2020, May). UNC3524: Eye Spy on Your Email - Threat Intelligence. Retrieved October 1, 2024, from https://cloud.google.com/blog/topics/threat-intelligence/unc3524-eye-spy-email/

Dr. Yusuf Perwej, Nikhat Akhtar, & Dr.Firoj Parwej. (n.d.). A Technological Perspective of Blockchain Security. *ResearchGate*. https://doi.org/DOI:10.24327/ijrsr.2018.0911.2869

Draco Team - Bitefinder. (n.d.). *Dissecting a Chinese APT Targeting South Eastern Asian government Institutions* (BiteFender Whitepaper).

GeeksforGeeks. (n.d.). Session Side Hijacking Vulnerability in Ethical Hacking. https://www.geeksforgeeks.org/session-side-hijacking-vulnerability-in-ethical-hacking/

Jenna, P. (n.d.). Reconnaissance in Cybersecurity: Types & Prevention.

Kemal Bicakci & Bulent Tavli. (n.d.). Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *ScienceDirect*. https://doi.org/https://doi.org/10.1016/j.csi.2008.09.038

Lockheed Martin. (n.d.). Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mitre ATT&CK®. (2020, April). https://attack.mitre.org/

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th anniversary edition). Wiley.

Steffens, T. (2020). *Attribution of Advanced Persistent Threats: How to Identify the Actors Behind Cyber-Espionage*. Springer. https://doi.org/10.1007/978-3-662-61313-9

Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. *Network Security*, *2011*(8), 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

Tarun, Y., & Arvind Mallari, R. (n.d.). Technical Aspects of Cyber Kill Chain. Retrieved October 27, 2024, from https://link.springer.com/content/pdf/10.1007/978-3-319-22915-7_40

U. Sakthivelu & C. N. S. Vinoth Kumar. (2023). Advanced Persistent Threat Detection and Mitigation Using Machine Learning Model. *Tech Science Press*. https://doi.org/DOI:10.32604/iasc.2023.036946

Zalewski, M. (2012). *The tangled Web: A guide to securing modern Web applications*. No Starch Press.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon* (First Edition). Crown Publishers.

Zhang, J., Zheng, J., Zhang, Z., Chen, T., Tan, Y.-a., Zhang, Q., & Li, Y. (2024). ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. *Computer Networks*, *245*, 110376. https://doi.org/10.1016/j.comnet.2024.110376

Appendices

Appendix A.1: Team Assignments

1. Gaurav Jain (s4036068) – Team Leader
2. Ram Kishore (s3972281) – Team Secretary
3. Taha Kasim Rupawala (s4038149) – Team Member
4. Dr. Graham Clarke - Team Mentor

Appendix A.2: Team Contract

We, as a team, agree to:

1. Have equal task division with weekly workload reviews to mitigate uneven contribution risks.
2. Adhere to the agreed research methodology, conducting regular check-ins to prevent inconsistent approaches.
3. Use MS Teams for formal communication, with mandatory weekly summaries to avoid information silos and a WhatsApp group for real-time communication.
4. Compile final submission in Overleaf, implementing change freeze 24 hours before the deadline to manage last-minute alterations.
5. Address conflicts promptly, using majority voting and an escalation protocol to resolve persistent disputes.
6. Set internal deadlines 48 hours before official ones, using a shared calendar with reminders to prevent missed deadlines.
7. Rotate proofreading responsibilities and implement a two-person review system for each section to ensure quality.
8. Document and review individual contributions weekly to maintain accountability and acknowledge all work fairly.

Appendix A.3: Project Management

Purpose

To successfully research, develop, and submit a comprehensive report on Advanced Persistent Threats (APT), focusing on the identification, technical aspects, implementation, mitigation frameworks, and emerging trends in APT.

Objectives

Complete all tasks within the defined timeline.

Produce a high-quality report that meets project rubrics and technical standards.

Foster effective communication and collaboration within the team to ensure all aspects of the APT topic are covered in-depth.

Team Roles and Responsibilities

Gaurav Jain (Team Leader):

Oversee the project execution, ensure tasks are completed as per schedule, and manage the team's progress.

Lead the research on APT technical frameworks, drafting sections 3.5 to 3.9, and contributing to mitigation strategies.

Ram Kishore (Secretary):

Document all meetings, track task completion, and manage communication between the team and the mentor, Dr. Graham Clarke.

Lead the work on social engineering aspects of APT, drafting sections 3.1 to 3.4, and assisting in report compilation.

Taha Kasim Rupawala (Team Member):

Focus on the machine learning models and encryption related to APT.

Responsible for drafting sections 3.10 to 3.14, working on future trends, and assisting with final report editing.

Team Communication

Weekly Checkpoints:

- All team members will attend weekly checkpoints to discuss progress, assess challenges, and review the report status. Checkpoints are scheduled on 14th August, 21st August, 28th August, 11th September, 18th September, 25th September, 9th October, and 14th October.

Communication Channels:

- Primary: MS Teams for formal communication and document sharing, and WhatsApp for real-time updates.
- Meetings: Zoom or in-person meetings, as required, will be facilitated weekly.

Meeting Frequency: Weekly meetings with Dr. Graham Clarke and additional team meetings during critical stages, such as before submission deadlines.

Decision-Making Process

Consensus-Based:

- Decisions will be made by consensus within the team. In case of disagreements, Gaurav Jain will have the final say after discussions.
- Adjustments to task allocations will be made during team meetings.

Conflict Resolution

Mediation:

- Any conflicts will be addressed promptly during weekly meetings, mediated by Gaurav Jain to find a resolution.
- **Escalation:** If the issue remains unresolved, it will be escalated to Dr. Graham Clarke for further guidance.

Milestones and Deliverables

Week 4-7:

- Complete the initial research and draft individual sections based on the technical aspects of APT.
- Submit work for review by Dr. Graham Clarke during each checkpoint.

Week 8-12:

- Finalize the detailed sections, including real-world examples, mitigation strategies, and future trends.
- Ensure consistency across sections and submit the report for quality reviews.

Final Deliverable:

- Submit the final APT report by 18th October 2024, with report submission led by Gaurav Jain.

Performance Metrics

Timeliness:

- All team members are expected to meet the deadlines outlined in the project schedule and agreed upon in meetings.

Quality:

- The report will be evaluated based on its alignment with project rubrics, technical depth, and clarity.

Participation:

- Active participation in weekly meetings and contributing to assigned tasks is mandatory for all members.

Resource Allocation

Research Resources:

- Utilize academic databases, research journals, cybersecurity forums, and other reputable online sources for gathering data on APTs.

Tools:

- Use Overleaf for collaborative report writing, MS Teams for communication, and Zotero for citation management.

Sign-Off

Agreement

All team members agree to the roles, responsibilities, and processes outlined in this charter.

Approval

The charter is approved by Gaurav Jain (Team Leader) and will be revisited as needed throughout the project lifecycle.

Weekly Task Register

Team Member	Week	Task	Completion Status	Date of Completion
Gaurav Jain (Team Leader)	Week 4	Topic selection, research on advanced threats	Completed	05/08/2024
	Week 5	Arrange meeting with a mentor, discuss with the team about the researched threats and brainstorming	Completed	10/08/2024
	Week 6	Creation of Overleaf account and started with the report drafting. Started with APT technical framework	Completed	17/08/2024
	Week 7	Report finalization according to 1D report rubrics	Completed	24/08/2024
	Week 8	Research on APT implementation	Completed	31/09/2024
	Week 8	Start with researching and writing from 3.5 to 3.9 assigned	Completed	07/09/2024
	Week 9	Further drafting and fine-tuning of 3.5 to 3.9 and working on references	Completed	14/09/2024
	Week 10	Research on real-world examples and case studies	Completed	21/09/2024
	Week 11	Future trends and emerging tech related to authentication control	Completed	28/09/2024
	Week 12	Work on mitigation framework through authentication control	Completed	05/10/2024
	Week 13	Final document editing and submitted	Completed	12/10/2024
Ram Kishore (Secretary)	Week 4	Topic selection, research on advanced threats	Completed	05/08/2024
	Week 5	Researched on other authors and lit review	Completed	10/08/2024
	Week 6	Start with APT technical framework, social engineering techniques	Completed	17/08/2024
	Week 7	Report drafting and meeting with team and finalizing for 1D	Completed	24/08/2024
	Week 8	Research on APT implementation	Completed	31/09/2024
	Week 8	Start with researching and writing from 3.1 to 3.4 assigned	Completed	07/09/2024
	Week 9	Further drafting and fine-tuning of 3.1 to 3.4 and working on references	Completed	14/09/2024
	Week 10	Research on real-world examples and case studies	Completed	21/09/2024
	Week 11	Future trends and emerging tech related to social engineering	Completed	28/09/2024
	Week 12	Work on mitigation framework through social engineering	Completed	05/10/2024
	Week 13	Final document editing	Completed	12/10/2024
Taha Kasim Rupawala	Week 4	Topic selection, research on advanced threats	Completed	05/08/2024

	Week 5	Discuss with the team about the researched threats and brainstorming	Completed	10/08/2024
	Week 6	Started with APT technical framework	Completed	17/08/2024
	Week 7	Report finalization according to 1D report rubrics	Completed	24/08/2024
	Week 8	Research on APT implementation	Completed	31/09/2024
	Week 8	Start with researching and writing from 3.10 to 3.14 assigned	Completed	07/09/2024
	Week 9	Further drafting and fine-tuning of 3.10 to 3.14 and working on references	Completed	14/09/2024
	Week 10	Research on real-world examples and case studies	Completed	21/09/2024
	Week 11	Future trends and emerging tech related to machine learning model and encryption	Completed	28/09/2024
	Week 12	Work on mitigation framework through machine learning model and encryption	Completed	05/10/2024
	Week 13	Final document editing	Completed	12/10/2024

Table 1: Task Assignment and Completion Status

Task Register

Week	Tasks
Week 4	- Meeting to choose a topic (Advanced Persistent Threats). - Approval meeting with Dr. Graham for the project topic. - Initial research on APTs.
Week 5	- Weekly meeting with Dr. Graham to decide on the meeting schedule. - Review of rubrics for requirements clarity. - Index creation and discussion with the mentor. - Finalization of the index with a focus on the technical aspects of APT. - Contributed work on the draft.
Week 6	- Group members began their assigned tasks. - Meeting with a mentor to clarify doubts. - Creation of Overleaf account for report structuring and Zotero for citation management.
Week 7	- Finalization of work according to 1D Progress Report rubrics. - Mentor meeting for assignment approval and project management clarification. - Continued research on additional topics.
Week 8	- Research on APT implementation, writing sections 3.5 to 3.9. - Research on APT implementation, writing sections 3.1 to 3.4. - Research on APT implementation, writing sections 3.10 to 3.14.
Week 9	- Further drafting and fine-tuning sections 3.5 to 3.9, worked on references. - Further drafting and fine-tuning sections 3.1 to 3.4, worked on references. - Further drafting and fine-tuning sections 3.10 to 3.14, worked on references.
Week 10	- Research on real-world examples and case studies.
Week 11	- Research on future trends and emerging tech related to authentication control. - Research on future trends and emerging tech related to social engineering. - Research on future trends and emerging tech related to machine learning models and encryption.
Week 12	- Worked on mitigation framework through authentication control. - Worked on mitigation framework through social engineering. - Worked on mitigation framework through machine learning models and encryption.
Week 13	- Final document editing and submission.

Table 2: Weekly Tasks Summary

Minutes of Meeting

Week 4 (05/08/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. Finalization of the project topic (Advanced Persistent Threats).
2. Initial research on APTs.
3. Discussion about meeting with Dr. Graham for project approval.

Discussion:

1. Gaurav suggested "Advanced Persistent Threats" as the project topic, and the team unanimously agreed.
2. All members were assigned to conduct initial research on APTs.
3. Gaurav scheduled the meeting with Dr. Graham for topic approval.

Action Items:

All members are to complete initial research on APTs by the next meeting.

Gaurav to meet with Dr. Graham for topic approval.

Take Home Message:

The project will focus on Advanced Persistent Threats, and research should begin immediately to prepare for future discussions with the mentor.

Week 5 (10/08/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. Review of research findings on APT.
2. Set up a meeting schedule with Dr. Graham.
3. Rubric review and index creation.

Discussion:

All members shared their initial research findings, focusing on the technical and social aspects of APTs.

Gaurav proposed scheduling regular weekly meetings on Fridays with Dr. Graham.

The team reviewed the project rubric and agreed to create an index covering technical aspects of APT.

Action Items:

Ram to conduct a further literature review.

Gaurav to create the index and discuss it with Dr. Graham for feedback.

Take Home Message:

Finalized the structure of the report focusing on the technical aspects of APT and aligned it with the rubric requirements.

Week 6 (17/08/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. Review assigned tasks and Overleaf setup.
2. Discuss Overleaf and Zotero setup for collaboration.
3. Clarify questions with Dr. Graham on the technical framework of APT.

Discussion:

Overleaf account creation was completed, and all members had access to report drafting.

Zotero was set up for managing references.

The team discussed the APT technical framework and prepared questions for Dr. Graham on areas requiring clarification.

Action Items:

Each member is to start drafting their assigned sections in Overleaf.

Gaurav to organize the report structure.

Take Home Message:

The report structure is set up in Overleaf, and Zotero is ready for citations. Task assignment for sections has started, with each member taking ownership of specific parts.

Week 7 (24/08/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. Finalize work based on 1D Progress Report rubrics.
2. Discussion with Dr. Graham for assignment approval.
3. Research additional topics.

Discussion:

Each team member finalized their section according to the 1D rubrics.

The mentor provided feedback on the current progress and clarified questions regarding report management.

Additional research topics were allocated to ensure coverage of APT implementation and future trends.

Action Items:

- Continue drafting based on mentor feedback.

- Research additional topics assigned for upcoming sections.

Take Home Message:

The team is on track, and the initial sections are aligned with the rubrics. Further research is needed for the next stages of the project.

Week 8 (31/08/2024 & 07/09/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. - Review APT implementation research.
2. - Writing assigned sections: 3.5 to 3.9 (Gaurav), 3.1 to 3.4 (Ram), 3.10 to 3.14 (Taha).

Discussion:

- Each member presented their findings on APT implementation and started drafting their respective sections.

- The team reviewed their progress and coordinated to ensure consistency across different parts of the report.

Action Items:

- Complete the assigned sections by next week and review references for accuracy.

Take Home Message:

Each member is progressing well in drafting their assigned sections on APT implementation. Consistency in writing style and content should be maintained across sections.

Week 9 (14/09/2024)

Attendees: Gaurav Jain, Ram Kishore, Taha Kasim Rupawala
Duration: 45 minutes

Agenda:

1. Fine-tuning and drafting of sections 3.1 to 3.14.
2. Review of references.

Discussion:

- Team members worked on fine-tuning their sections (3.5 to 3.9, 3.1 to 3.4, and 3.10 to 3.14) based on the feedback and added relevant references.

- All references were reviewed and compiled using Zotero.

Action Items:

- Finalize the drafted sections with references for mentor review.

Take Home Message:

Drafts are nearing completion, and referencing is being handled carefully. The report is progressing according to plan.

Team Dynamics

The team has implemented several mechanisms to ensure active participation and smooth collaboration throughout the project. Weekly meetings with mentor Dr. Graham Clarke are scheduled on the following dates: 14th August, 21st August, 28th August, 11th September, 18th September, 25th September, 9th October, and 14th October. During these meetings, progress is reviewed, and each member's contributions are evaluated.

Gaurav Jain, as the team leader, monitors deadlines, ensures task completion, and guides the overall direction of the report. Ram Kishore, as the secretary, documents meeting minutes, tracks task progress, and manages communication between the team and mentor. Taha Kasim Rupawala leads the research on machine learning and encryption, ensuring those areas are thoroughly addressed in the report.

Task assignments are clear and based on each member's designated sections. For example:

- Gaurav Jain is working on Sections 3.5 to 3.9.
- Ram Kishore is focusing on Sections 3.1 to 3.4.
- Taha Kasim Rupawala is covering Sections 3.10 to 3.14.

This ensures accountability and specialization within the team.

Challenges Overcome

One major challenge the team overcame was aligning schedules for weekly meetings. Initially, finding a common time for all members and Dr. Graham was difficult due to conflicting commitments. However, the team addressed this by agreeing on times outside of normal working hours, ensuring that everyone could attend. This flexibility fostered improved communication and teamwork, leading to more effective collaboration.

Another challenge was aligning the team's understanding of the technical aspects of APT, particularly when integrating different frameworks. After discussions and feedback from Dr. Graham, the team synchronized their understanding of key concepts, ensuring consistency across the report sections.

Challenges and How They Were Solved

1. Conflict in Research Approaches

Given the complexity of APTs, there could be differences in opinions or approaches to certain aspects of the project, such as technical frameworks or mitigation strategies. The team plans to address any potential conflicts by following a consensus-based decision-making process, with Gaurav Jain mediating disagreements. If unresolved, Dr. Graham will be consulted for guidance.

2. Ensuring High-Quality Contributions

Maintaining a high standard of research and analysis across all sections of the report could present a challenge. To overcome this, the team has introduced peer reviews during the weekly meetings. This allows each member to review and provide constructive feedback on the other members' work. This process helps to identify gaps, inconsistencies, or areas that need improvement early on, ensuring that the final submission meets high-quality standards.