Threat Inelligence Task

Name : Lavanya Chilukamari **Inter ID :** 308

Tactic Name : TA0043 – Reconnaissance

Tactic Link : https://attack.mitre.org/tactics/TA0043

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

Goal: Gather information for planning attacks.

Techniques of Reconnaissance :

- **T1595 - Active Scanning**
  Procedure: Use network scanner to map open ports.
  - Step 1: Run Nmap scan on target IP range.
  - Step 2: Collect and analyze open ports and services.
- **T1589 - Gather Victim Identity Information**
  Procedure: Search LinkedIn for employee roles.
  - Step 1: Query organization name on LinkedIn.
  - Step 2: Export and analyze job roles and hierarchy.
- **T1592 - Gather Victim Host Information**
  Procedure: Use Shodan to gather exposed device info.
  - Step 1: Search target IP/domain on Shodan.
  - Step 2: Note device types, banners, and software versions.

Tactic Name : TA0042 – Resource Development

Tactic Link : https://attack.mitre.org/tactics/TA0042

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

Goal: Build and maintain resources for attacks.

Techniques of Resource Development :

- **T1583.001 - Acquire Infrastructure: Domains**
  Procedure: Register domain for phishing.
  - Step 1: Choose a domain mimicking the target.
  - Step 2: Register and configure DNS records.

- **T1584.001 - Compromise Infrastructure: Web Servers**
  Procedure: Exploit vulnerable web server.
    - Step 1: Scan for outdated CMS versions.
    - Step 2: Upload web shell for persistent access.
- **T1585.002 - Establish Accounts: Cloud Accounts**
  Procedure: Create fake cloud account for staging tools.
    - Step 1: Sign up on a cloud platform with stolen ID.
    - Step 2: Deploy storage bucket for tool hosting.

Tactic Name : TA0001 – Initial Access

Tactic Link : https://attack.mitre.org/tactics/TA0001

Description of the Tactic :The adversary is trying to get into your network.

Goal: Gain access to target systems.

Techniques of Initial Access :

- **T1566.001 - Phishing: Spearphishing Attachment**
  Procedure: Email malicious doc to HR employee.
    - Step 1: Craft Word doc with macro payload.
    - Step 2: Send via spoofed HR-related email.
- **T1190 - Exploit Public-Facing Application**
  Procedure: Exploit SQL injection in login page.
    - Step 1: Identify injectable input field.
    - Step 2: Dump user table via SQL injection.
- **T1133 - External Remote Services**
  Procedure: Connect using stolen VPN credentials.
    - Step 1: Steal credentials from prior phishing.
    - Step 2: Log in to VPN portal and access internal network.

Tactic Name : **TA0002 – Execution**

Tactic Link : https://attack.mitre.org/tactics/TA0002

Description of the Tactic :The adversary is trying to run malicious code.

Goal: Run malicious code on a target system.

Techniques of Execution:

- **T1059.003 - Command and Scripting Interpreter: Windows Command Shell**
  Procedure: Drop and run batch script.
    - Step 1: Copy malicious script to temp folder.
    - Step 2: Execute using cmd.exe.
- **T1203 - Exploitation for Client Execution**
  Procedure: Use exploit in Adobe Reader.
    - Step 1: Craft malicious PDF.
    - Step 2: Send to user via email for execution.
- **T1047 - Windows Management Instrumentation (WMI)**
  Procedure: Use WMI to run remote payload.
    - Step 1: Access WMI via PowerShell.
    - Step 2: Invoke payload execution remotely.

Tactic Name : **TA0003 – Persistence**

Tactic Link : https://attack.mitre.org/tactics/TA0003

Description of the Tactic :The adversary is trying to maintain their foothold.

Goal: Maintain access after reboot/logoff.

Techniques of Persistence :

- **T1547.001 - Registry Run Keys/Startup Folder**
  Procedure: Add malware to Run key.
    - Step 1: Write malware path to HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
    - Step 2: Reboot system to auto-launch.
- **T1053.005 - Scheduled Task**
  Procedure: Create a hidden task for malware execution.
    - Step 1: Register task using schtasks.
    - Step 2: Set trigger on user login.
- **T1543.003 - Create or Modify System Process: Windows Service**
  Procedure: Install malware as service.
    - Step 1: Use sc.exe to create new service.
    - Step 2: Start service to activate payload.

Tactic Name : **TA0004 – Privilege Escalation**

Tactic Link : https://attack.mitre.org/tactics/TA0004

Description of the Tactic :The adversary is trying to gain higher-level permissions.

Goal: Gain higher-level privileges.

Techniques of Privilege Escalation :

- **T1068 - Exploitation for Privilege Escalation**
  Procedure: Exploit Windows vulnerability (e.g., PrintNightmare).
    - Step 1: Deliver and run exploit code.
    - Step 2: Spawn elevated shell.
- **T1548.002 - Bypass User Access Control**
  Procedure: Use UAC bypass tool.
    - Step 1: Drop fodhelper.exe UAC bypass script.
    - Step 2: Execute to elevate process without prompt.
- **T1134.001 - Access Token Manipulation: Token Impersonation**
  Procedure: Impersonate SYSTEM token.
    - Step 1: Enumerate tokens via Incognito tool.
    - Step 2: Use stolen token to spawn elevated process.

Tactic Name : **TA0005 – Defense Evasion**

Tactic Link : https://attack.mitre.org/tactics/TA0005

Description of the Tactic :The adversary is trying to avoid being detected.

Goal: Evade detection by security tools.

Techniques of Defence Evasion :

- **T1027 - Obfuscated Files or Information**
  Procedure: Base64 encode payload.
    - Step 1: Encode malware script in Base64.
    - Step 2: Decode and execute at runtime.
- **T1070.004 - File Deletion**
  Procedure: Clean up execution traces.
    - Step 1: Delete dropped payloads.
    - Step 2: Clear logs from temp folders.
- **T1562.001 - Disable or Modify Tools**
  Procedure: Disable Windows Defender.
    - Step 1: Modify registry or use PowerShell to disable Defender.
    - Step 2: Confirm status via Get-MpPreference.

Tactic Name : Tactic Name : **TA0006 – Credential Access**

Tactic Link : https://attack.mitre.org/tactics/TA0006

Description of the Tactic :The adversary is trying to steal account names and passwords.

Goal: Steal credentials like usernames and passwords.

Techniques of Credential Access :

- **T1003.001 - LSASS Memory**
  Procedure: Dump LSASS to extract creds.
  - Step 1: Use procdump on lsass.exe.
  - Step 2: Analyze dump with Mimikatz.
- **T1056.001 - Keylogging**
  Procedure: Install keylogger on user machine.
  - Step 1: Drop and install keylogger silently.
  - Step 2: Monitor and collect typed credentials.
- **T1555.003 - Credentials from Web Browsers**
  Procedure: Extract saved passwords.
  - Step 1: Access browser's login data file.
  - Step 2: Decrypt stored passwords using DPAPI.

Tactic Name : **TA0007 – Discovery**

Tactic Link : https://attack.mitre.org/tactics/TA0007

Description of the Tactic : The adversary is trying to figure out your environment**.**

Goal: Understand the environment.

Techniques of Discovery :

- **T1087.001 - Local Account Discovery**
  Procedure: List local users.
  - Step 1: Run net user command.
  - Step 2: Note admin or privileged users.
- **T1018 - Remote System Discovery**
  Procedure: Scan network for live hosts.
  - Step 1: Ping sweep using script.
  - Step 2: Log reachable hosts.

- **T1069.002 - Permission Groups Discovery: Domain Groups**
  Procedure: Enumerate AD groups.
    - Step 1: Use net group /domain.
    - Step 2: Identify high-privilege groups.

Tactic Name : **TA0008 – Lateral Movement**

Tactic Link : https://attack.mitre.org/tactics/TA0008

Description of the Tactic :The adversary is trying to move through your environment.

Goal: Move across systems.

Techniques of Lateral Movement :

- **T1021.002 - Remote Services: SMB/Windows Admin Shares**
  Procedure: Access C$ share on remote system.
    - Step 1: Connect using stolen creds.
    - Step 2: Drop and execute payload.
- **T1075 - Pass the Hash**
  Procedure: Authenticate using NTLM hash.
    - Step 1: Capture NTLM hash.
    - Step 2: Use tool like pth-winexe to connect.
- **T1550.002 - Use Alternate Authentication Material: Pass the Ticket**
  Procedure: Use Kerberos TGT ticket.
    - Step 1: Extract ticket with Mimikatz.
    - Step 2: Use kerberos::ptt to impersonate user.

Tactic Name : **TA0009 – Collection**

Tactic Link : https://attack.mitre.org/tactics/TA0009

Description of the Tactic :The adversary is trying to gather data of interest to their goal.

Goal: Collect valuable data.

Techniques of Collection :

- **T1114.001 - Email Collection: Local Email Clients**
  Procedure: Extract emails from Outlook.
    - Step 1: Access PST files.
    - Step 2: Parse and export sensitive emails.

- **T1005 - Data from Local System**
  Procedure: Copy sensitive files.
    - Step 1: Locate documents folder.
    - Step 2: Archive for exfiltration.
- **T1113 - Screen Capture**
  Procedure: Take screenshots of user desktop.
    - Step 1: Use script to capture screen.
    - Step 2: Save and store image.

Tactic Name : **TA0011 – Command and Control**

Tactic Link : https://attack.mitre.org/tactics/TA0011

Description of the Tactic :The adversary is trying to communicate with compromised systems to control them.

Goal: Control infected systems.

Techniques of Command and Control :

- **T1071.001 - Web Protocols**
  Procedure: Use HTTPS to communicate with C2.
    - Step 1: Send beacon to C2 over HTTPS.
    - Step 2: Receive commands.
- **T1095 - Non-Application Layer Protocol**
  Procedure: Use raw TCP for C2.
    - Step 1: Open TCP socket to remote server.
    - Step 2: Transmit encoded commands.
- **T1105 - Ingress Tool Transfer**
  Procedure: Download payload from C2.
    - Step 1: Send GET request to C2 server.
    - Step 2: Save payload to disk.

Tactic Name : **TA0010 – Exfiltration**

Tactic Link : https://attack.mitre.org/tactics/TA0010

Description of the Tactic :The adversary is trying to steal data**.**

Goal: Steal data from target network.

Techniques of Exfiltration:

- **T1041 - Exfiltration Over C2 Channel**
  Procedure: Send ZIP over HTTPS to C2.
    - Step 1: Compress data.
    - Step 2: Upload via beacon channel.
- **T1567.002 - Exfiltration to Cloud Storage**
  Procedure: Upload to Dropbox.
    - Step 1: Authenticate to fake Dropbox.
    - Step 2: Upload stolen documents.
- **T1052.001 - Exfiltration Over USB**
  Procedure: Copy data to USB device.
    - Step 1: Mount USB.
    - Step 2: Transfer files to drive.

Tactic Name : **TA0040 – Impact**

Tactic Link : https://attack.mitre.org/tactics/TA0040

Description of the Tactic :The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Goal: Damage or disrupt operations.

Techniques of Impact :

- **T1486 - Data Encrypted for Impact (Ransomware)**
  Procedure: Encrypt user files.
    - Step 1: Drop encryption module.
    - Step 2: Execute and drop ransom note.
- **T1499 - Endpoint Denial of Service**
  Procedure: Overload system resources.
    - Step 1: Launch infinite loop script.
    - Step 2: Consume CPU and crash system.
- **T1561.001 - Disk Wipe: Disk Content Wipe**
  Procedure: Wipe disk sectors.
    - Step 1: Access disk with raw write permissions.
    - Step 2: Overwrite disk with random bytes.