Threat Intel Report on

MITRE ATT&CK® FRAMEWORK

ESXi Platform

(Image Explanation)

By

Team Cyber Nexus

Nitesh Patel - 2050

Sanjay Sharma - 2065

Gaurav Gawade - 2036

Tejas More - 2039

Table of Content

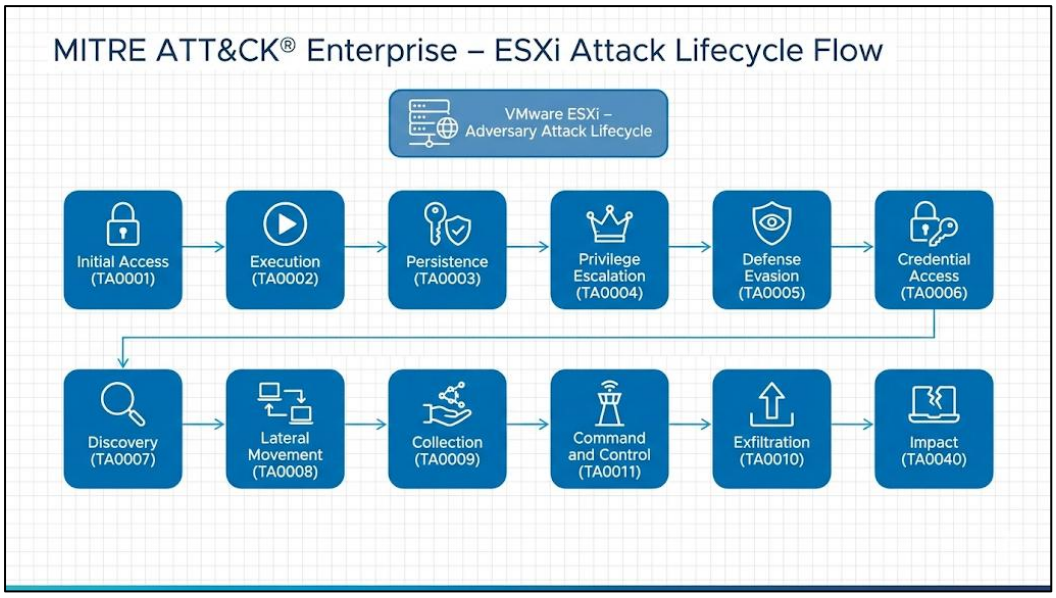
MITRE ATT&CK Framework

Introduction

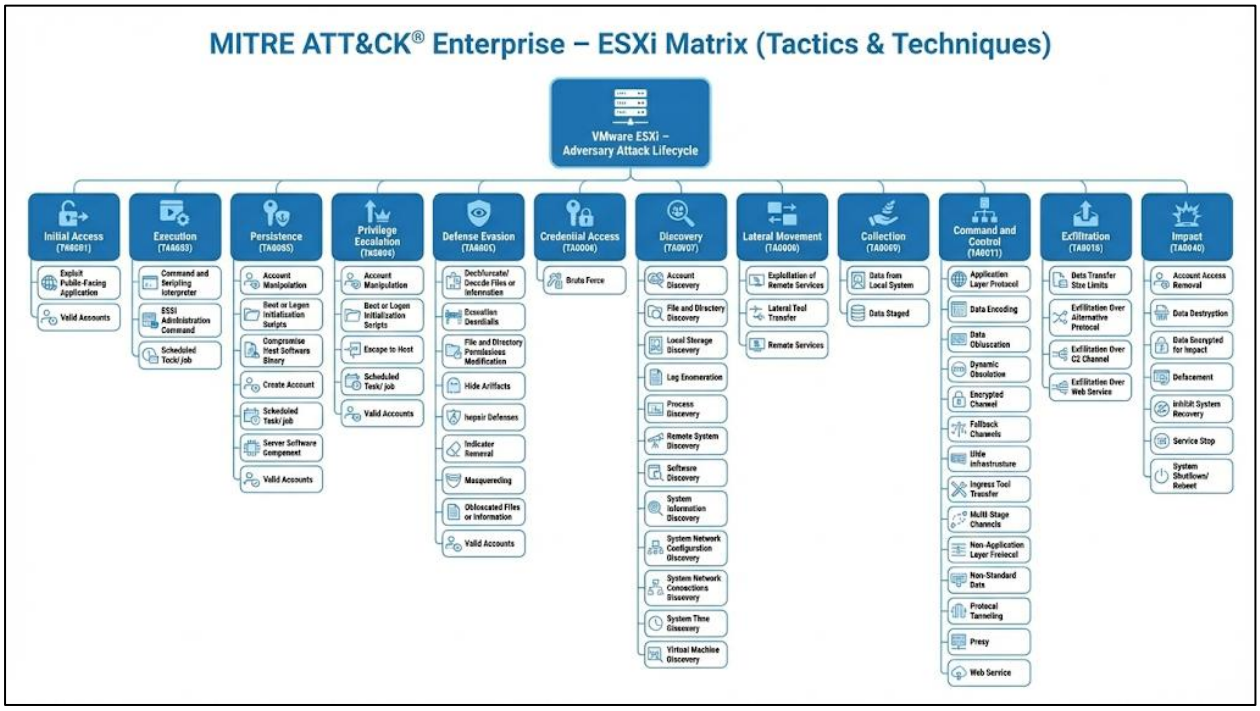
MITRE ATT&CK Enterprise – ESXi is a specialized part of the MITRE ATT&CK® framework that catalogs adversary tactics, techniques, and procedures (TTPs) observed against VMware ESXi hypervisors. ESXi is a widely used virtualization platform that runs virtual machines in many enterprise environments.

This matrix focuses on real-world attack behaviors against the ESXi hypervisor itself, showing how threat actors gain access, execute code, escalate privileges, evade defenses, and affect virtual systems. It adapts many existing ATT&CK techniques to the ESXi context and includes a few new ones that reflect ESXi-specific tradecraft. Security teams use this matrix for threat modeling, detection tuning, defensive planning, and understanding how adversaries compromise and operate within ESXi environments.

ESXi Attack Lifecycle Flow:

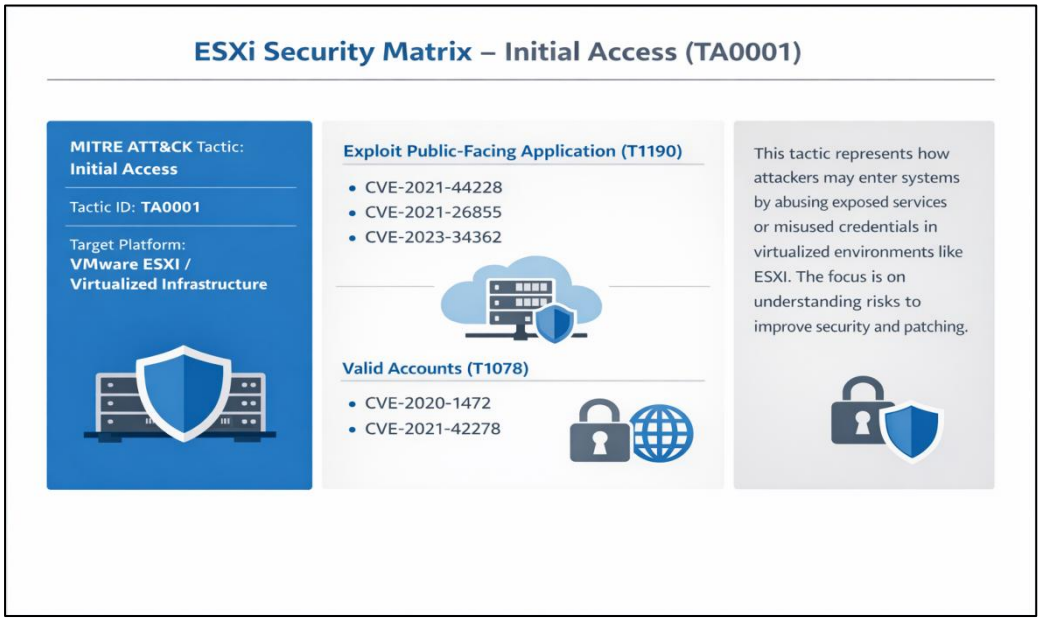


ESXi Matrix(Tactics & Techniques)

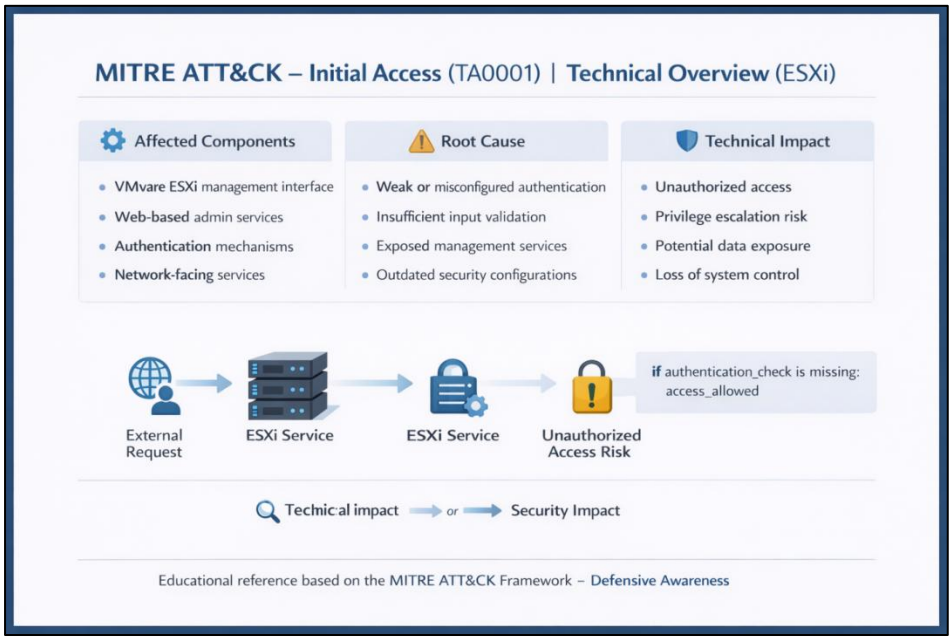


1. Initial Access(TA0001)

Overview:

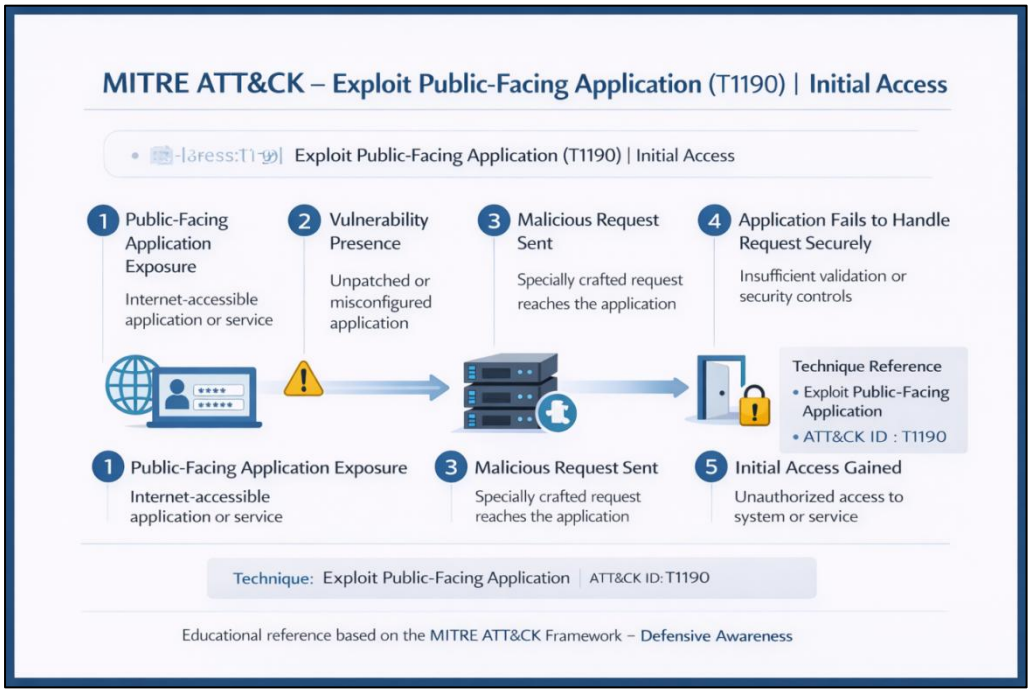


Technical details:

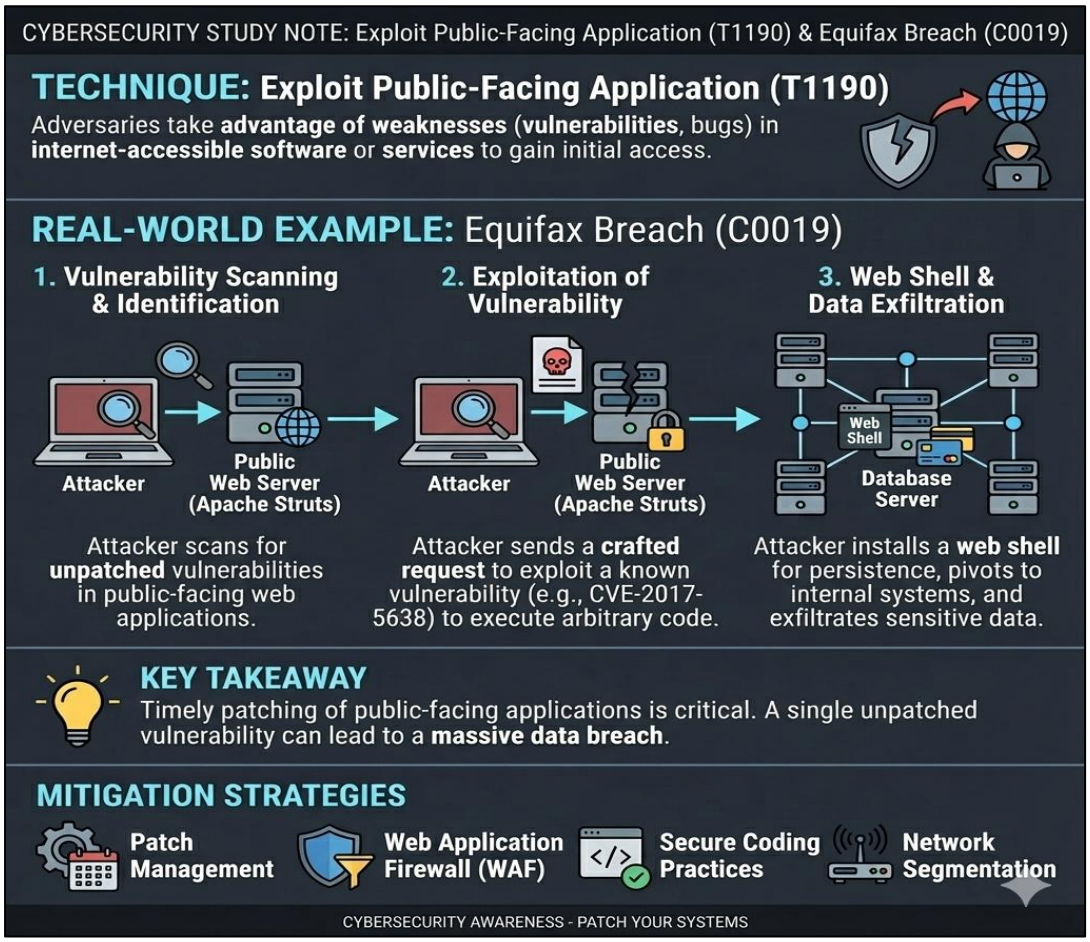


Attack flow / technique

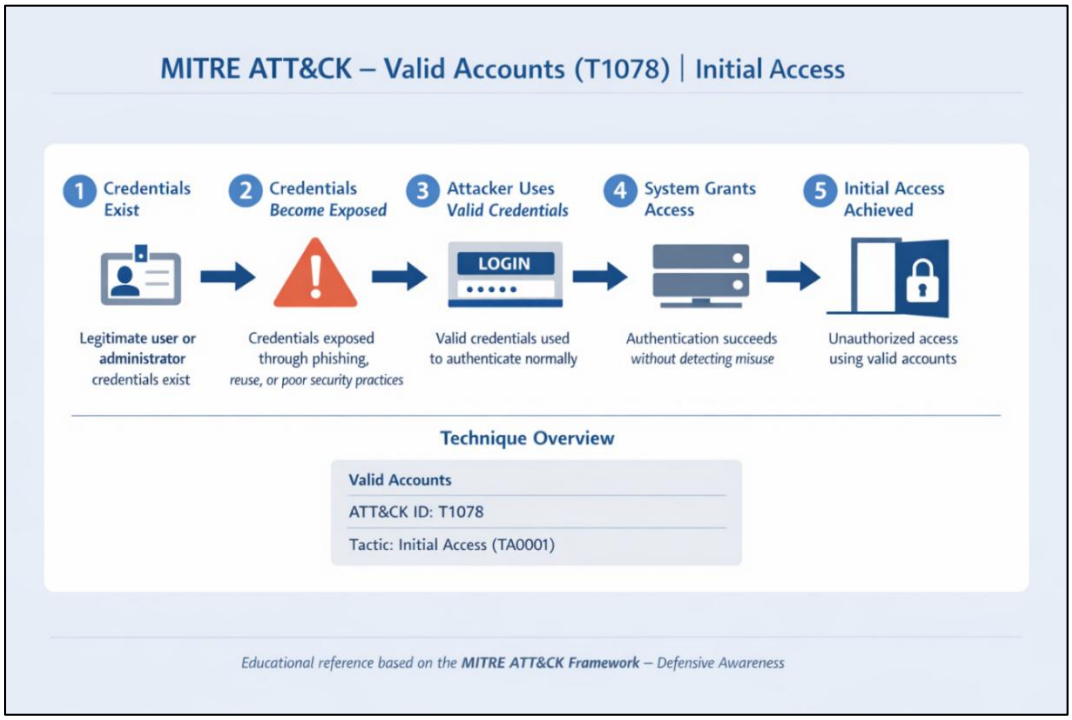
Technique 1: Exploit Public-Facing Application



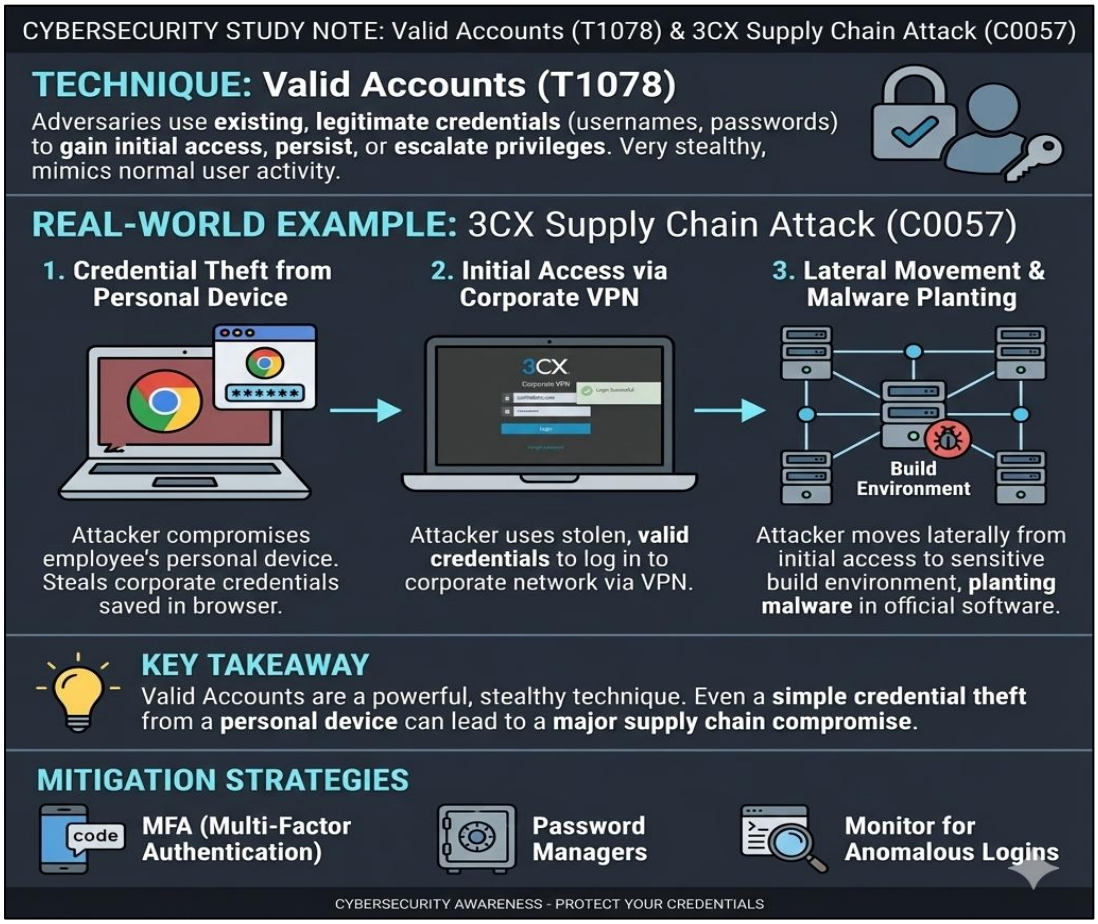
Real World Examples:



Technique 2: Valid Accounts



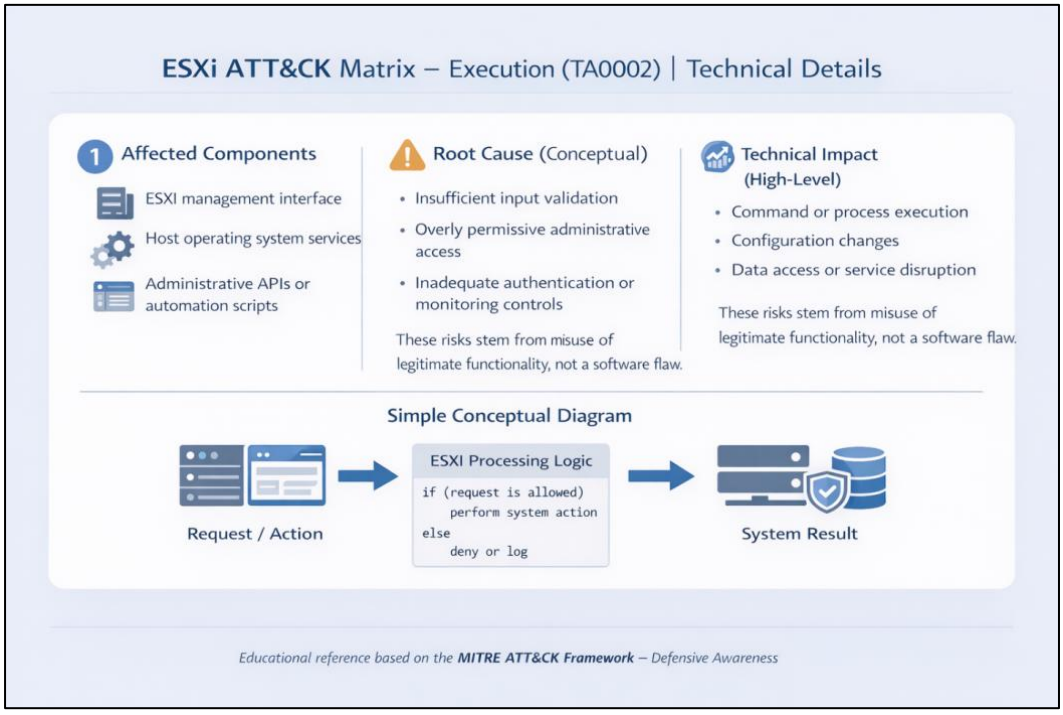
Real World Examples:



2. Execution(TA0002)

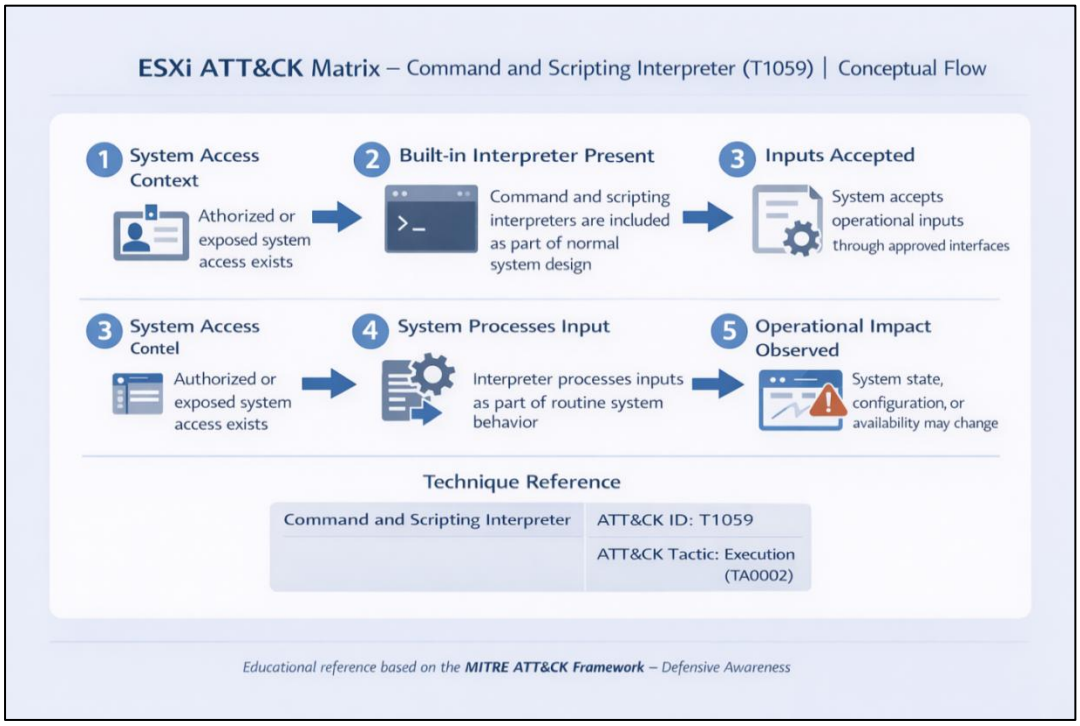
Overview

Technical details

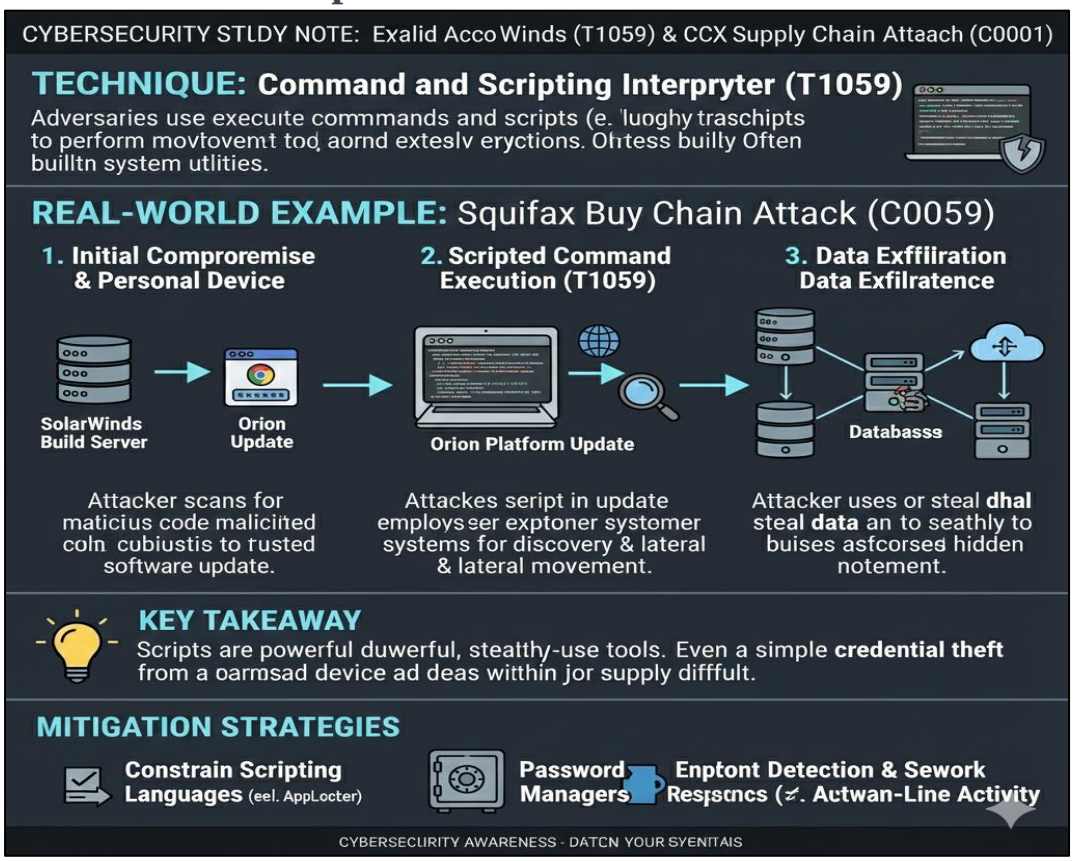


Attack flow / technique

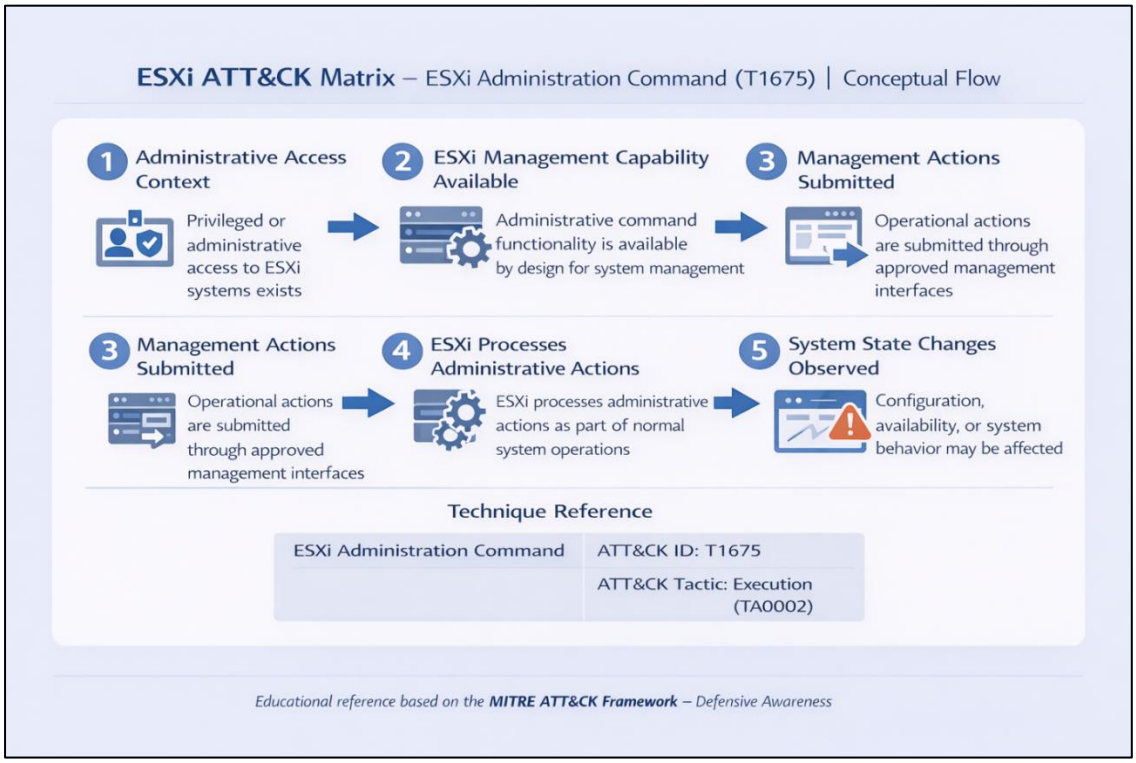
Technique 1: Command and Scripting Interpreter(T1059)



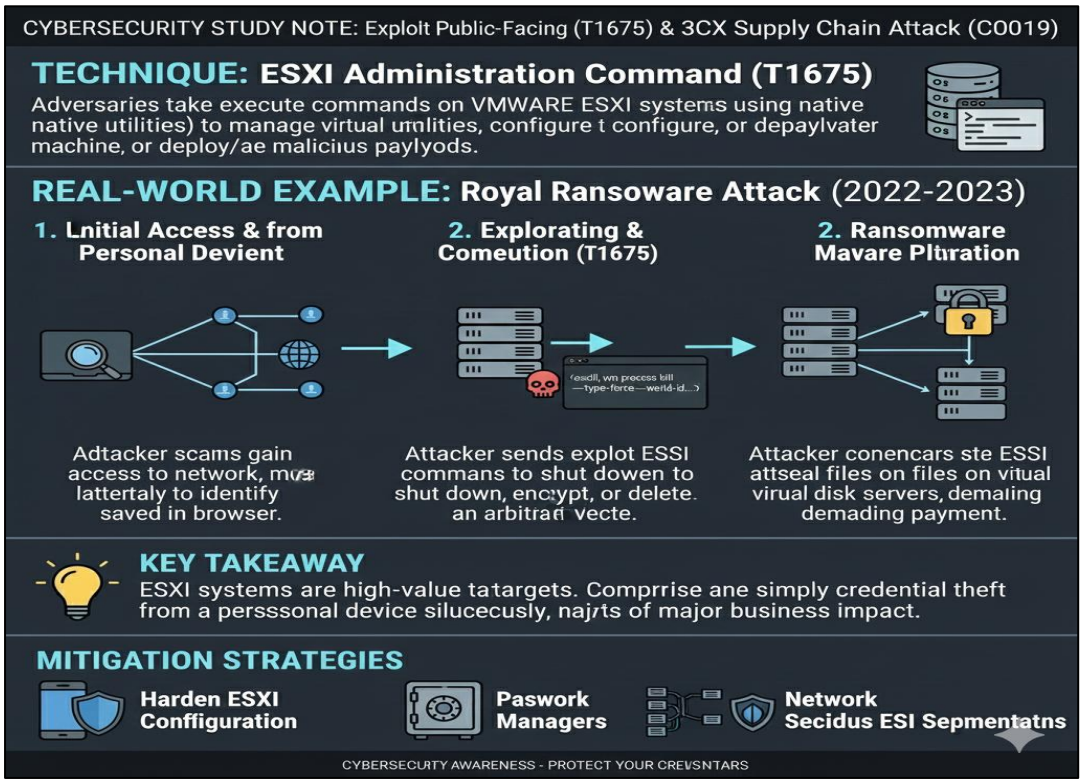
Real World Examples:



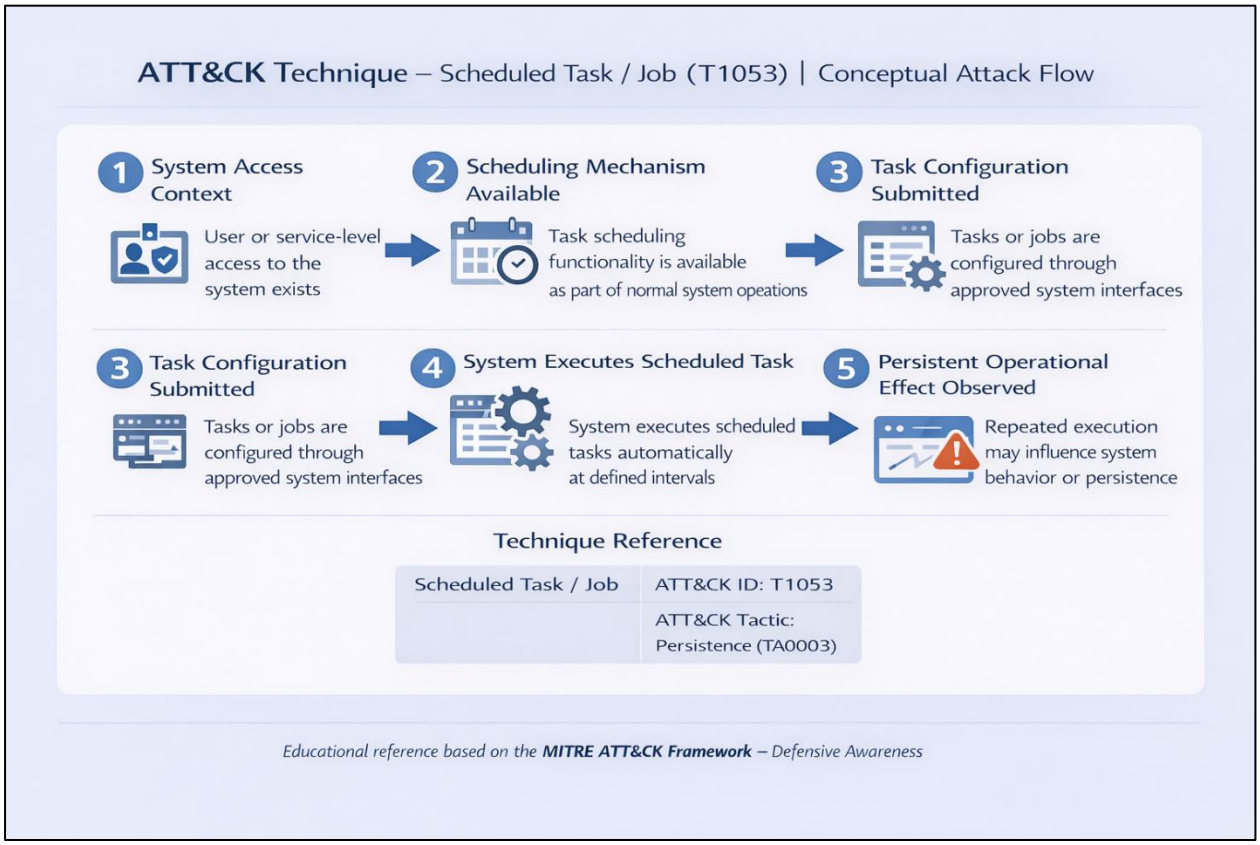
Technique 2: ESXi Administration Command(T1675)



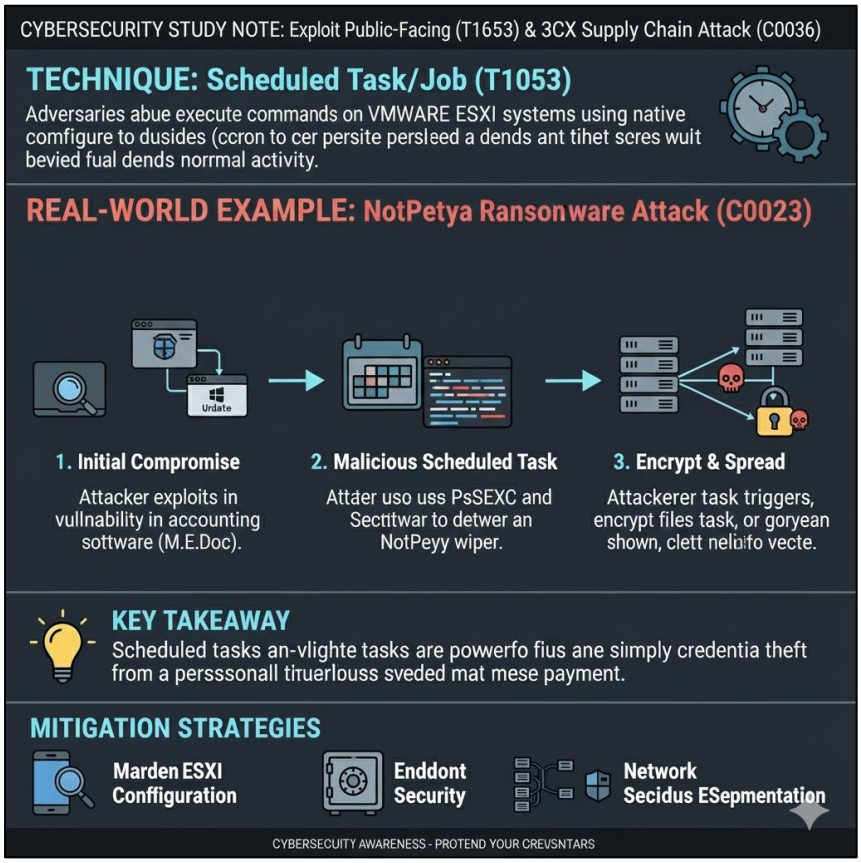
Real World Examples:



Technique 3: Scheduled Task/Job(T1053)

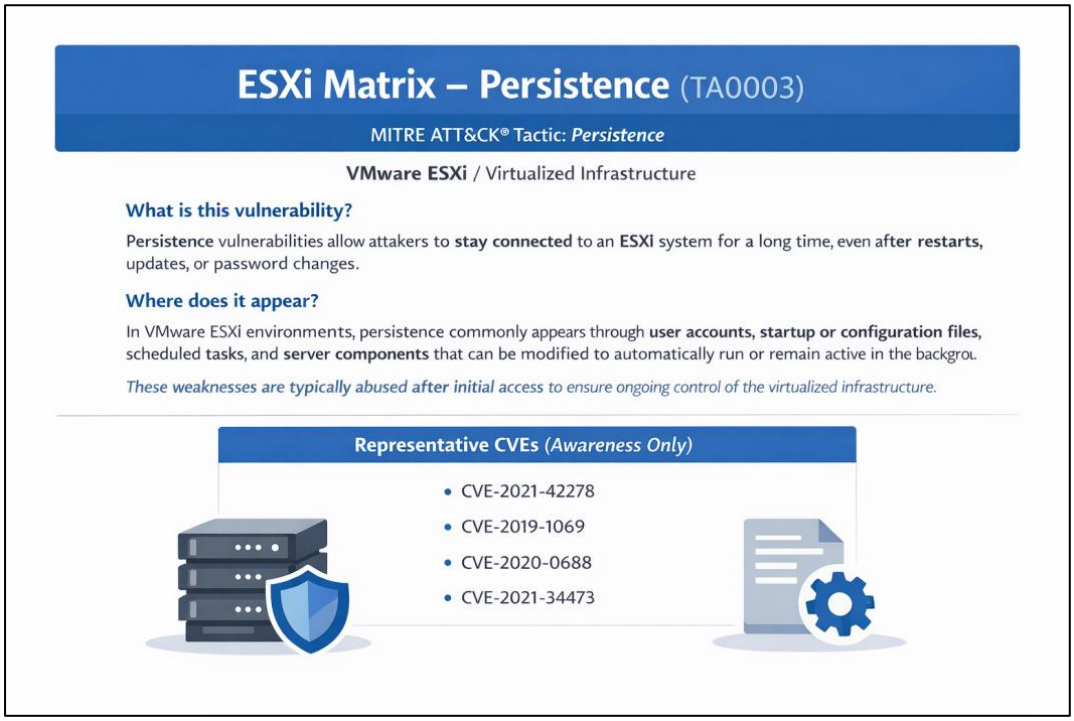


Real World Examples:

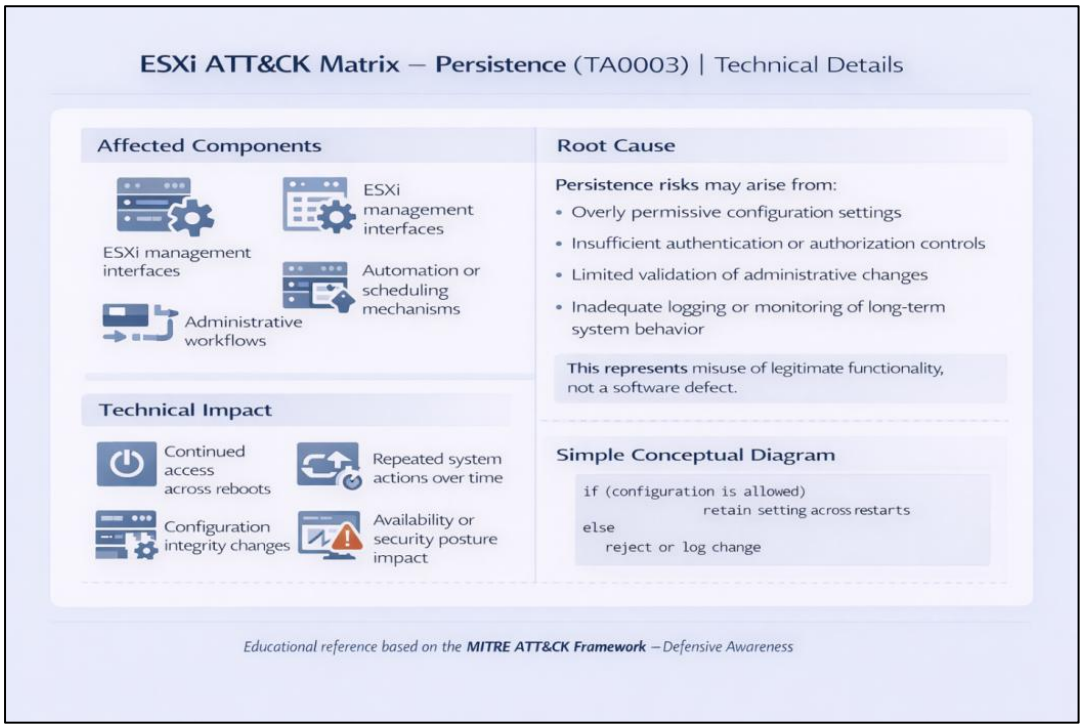


3. Persistence(TA0003)

Overview

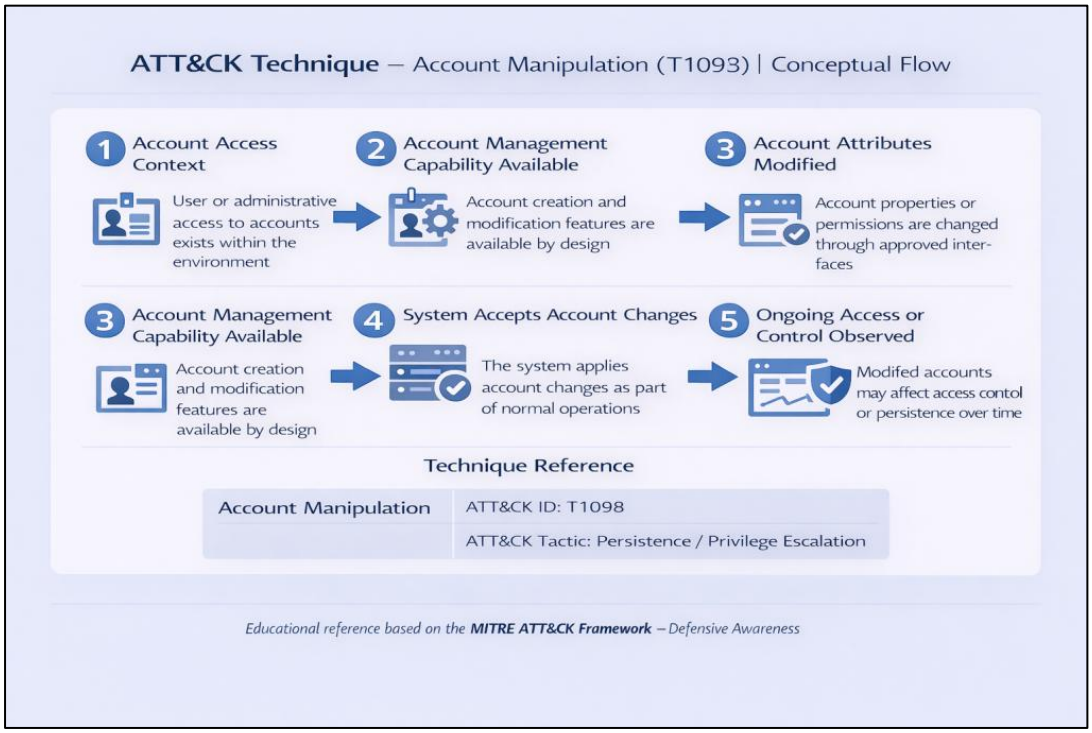


Technical details

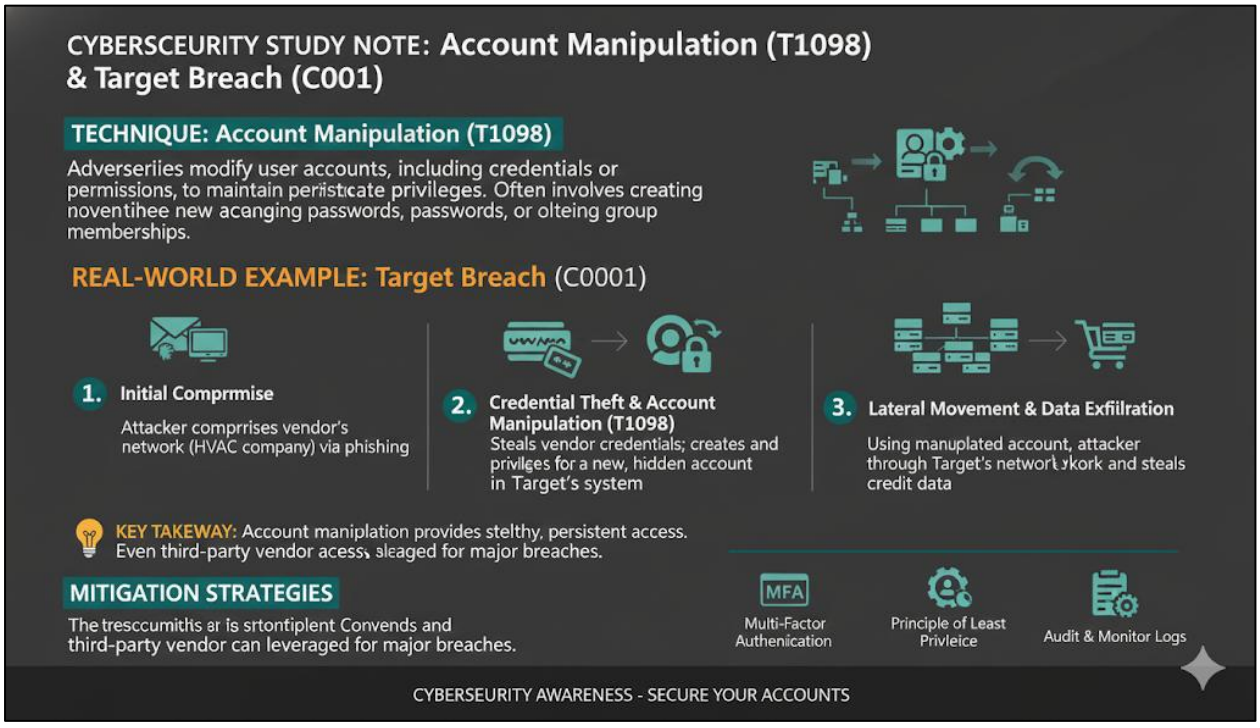


Attack flow / technique

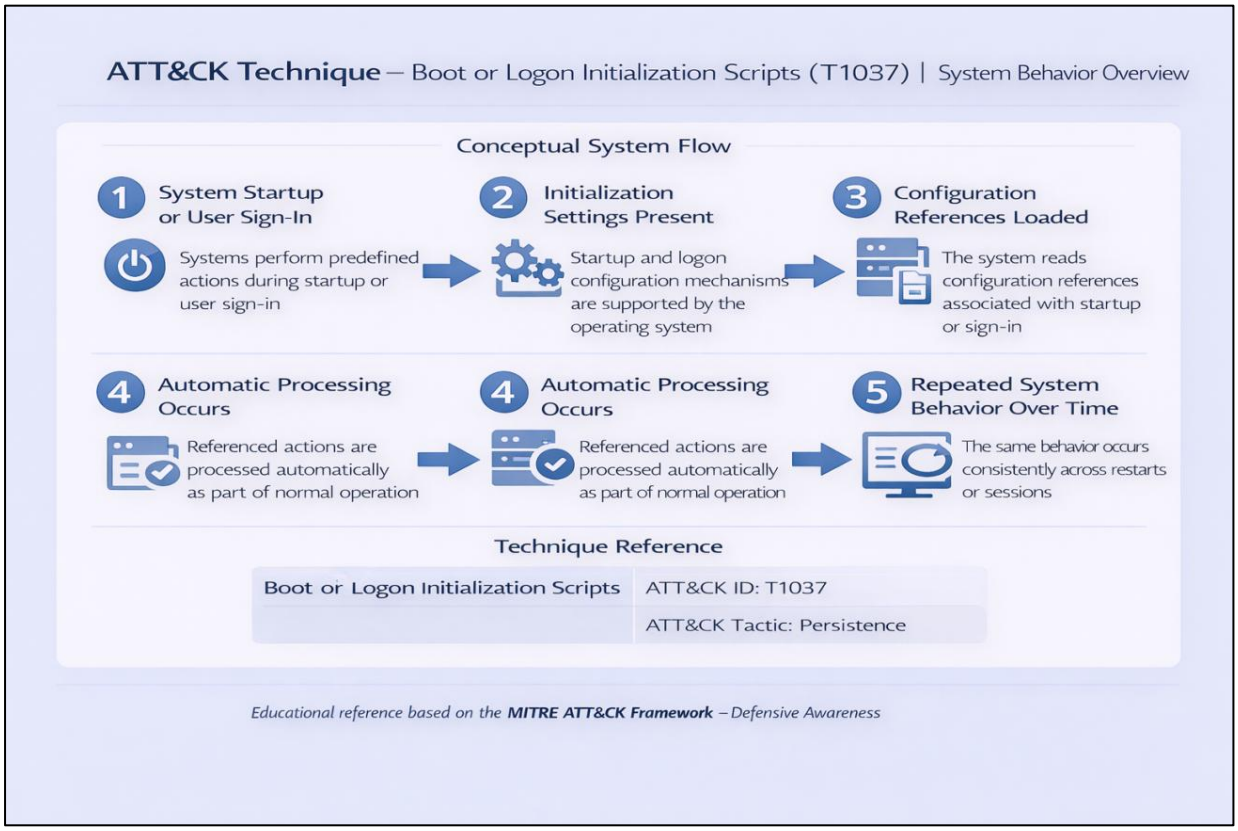
Technique1: Account Manipulation(T1098)



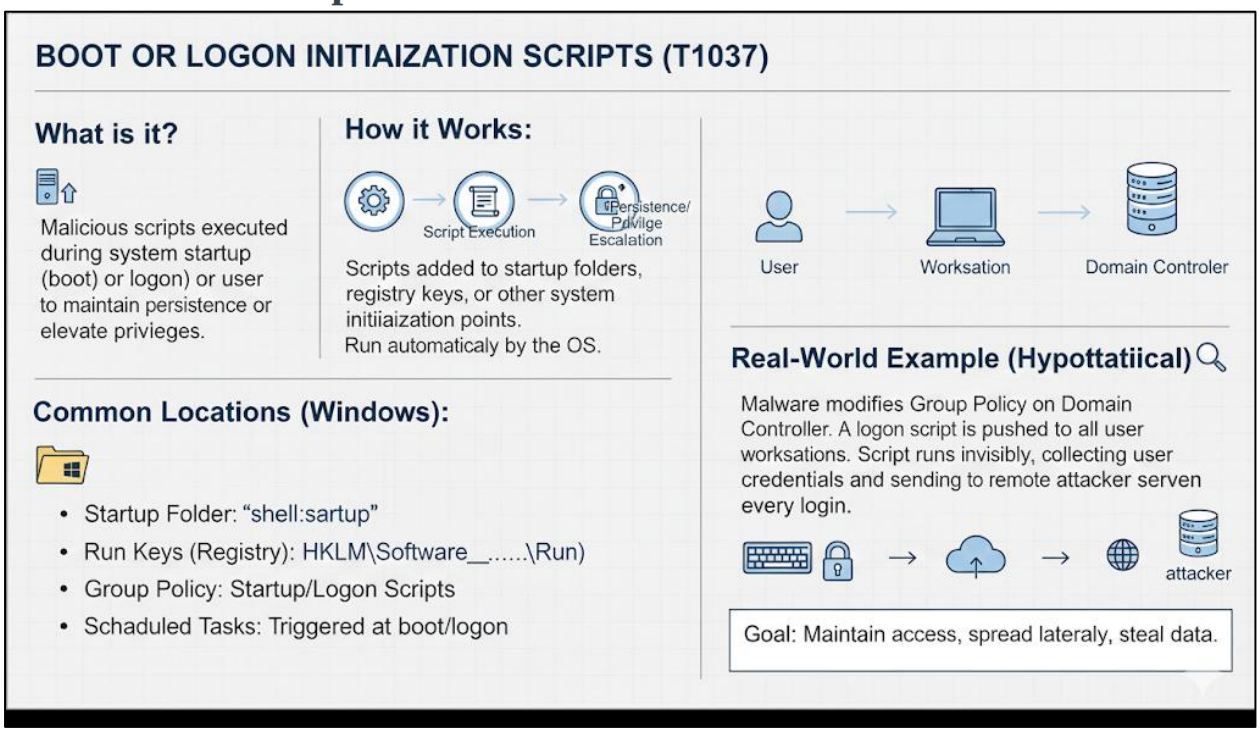
Real World Example:



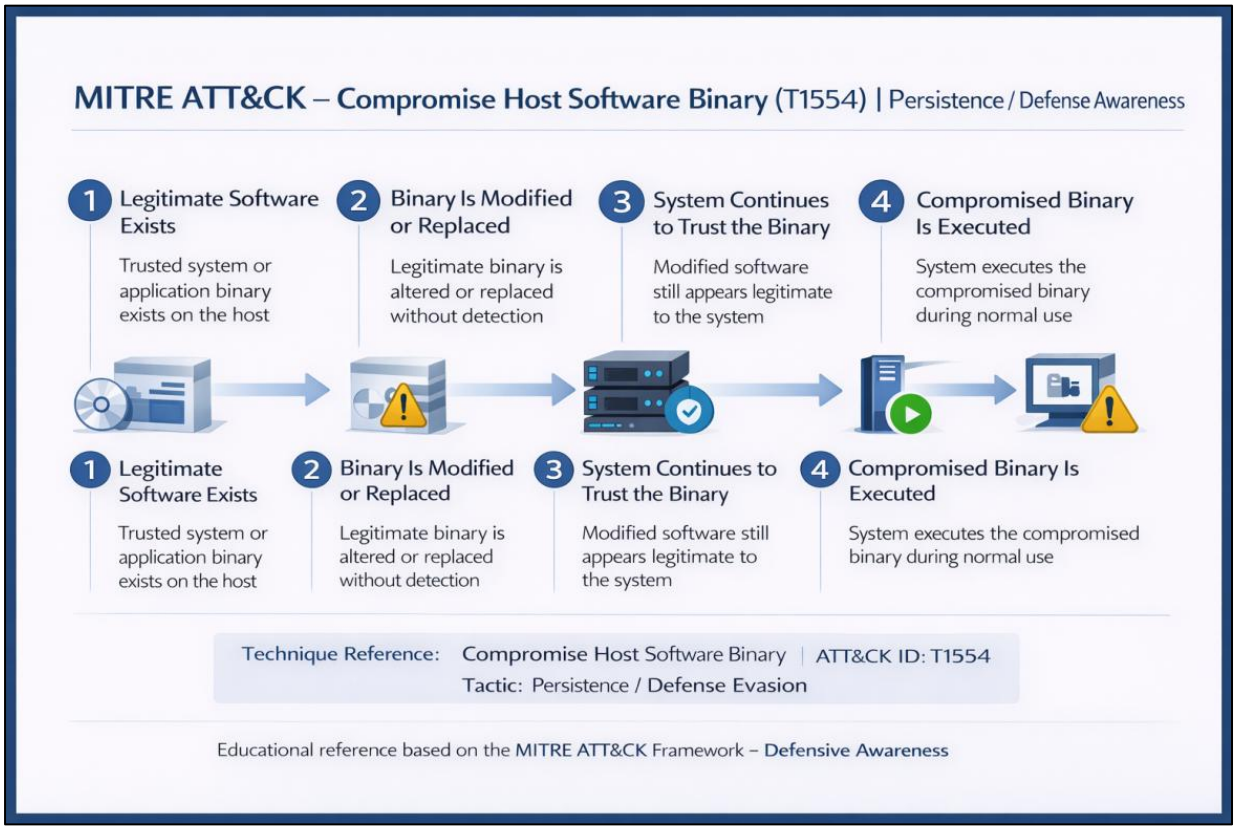
Technique 2 : Boot or Logon Initialization Scripts(T1037)



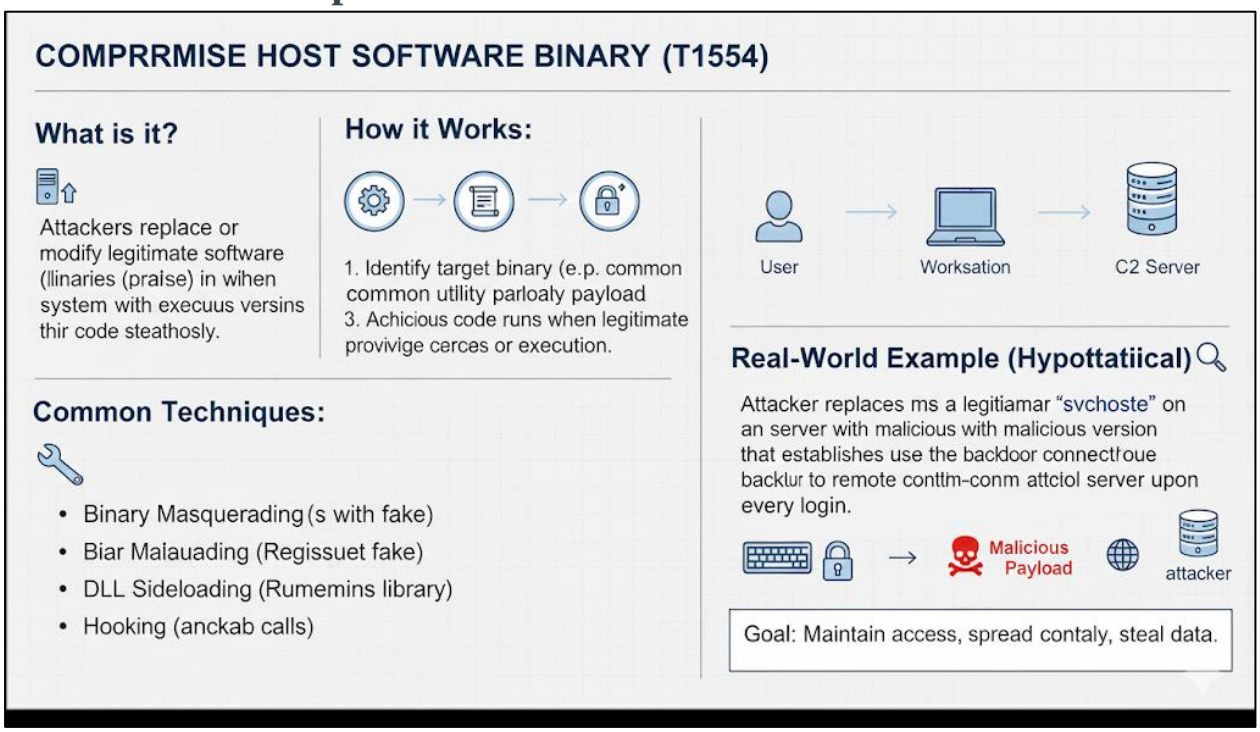
Real World Example:



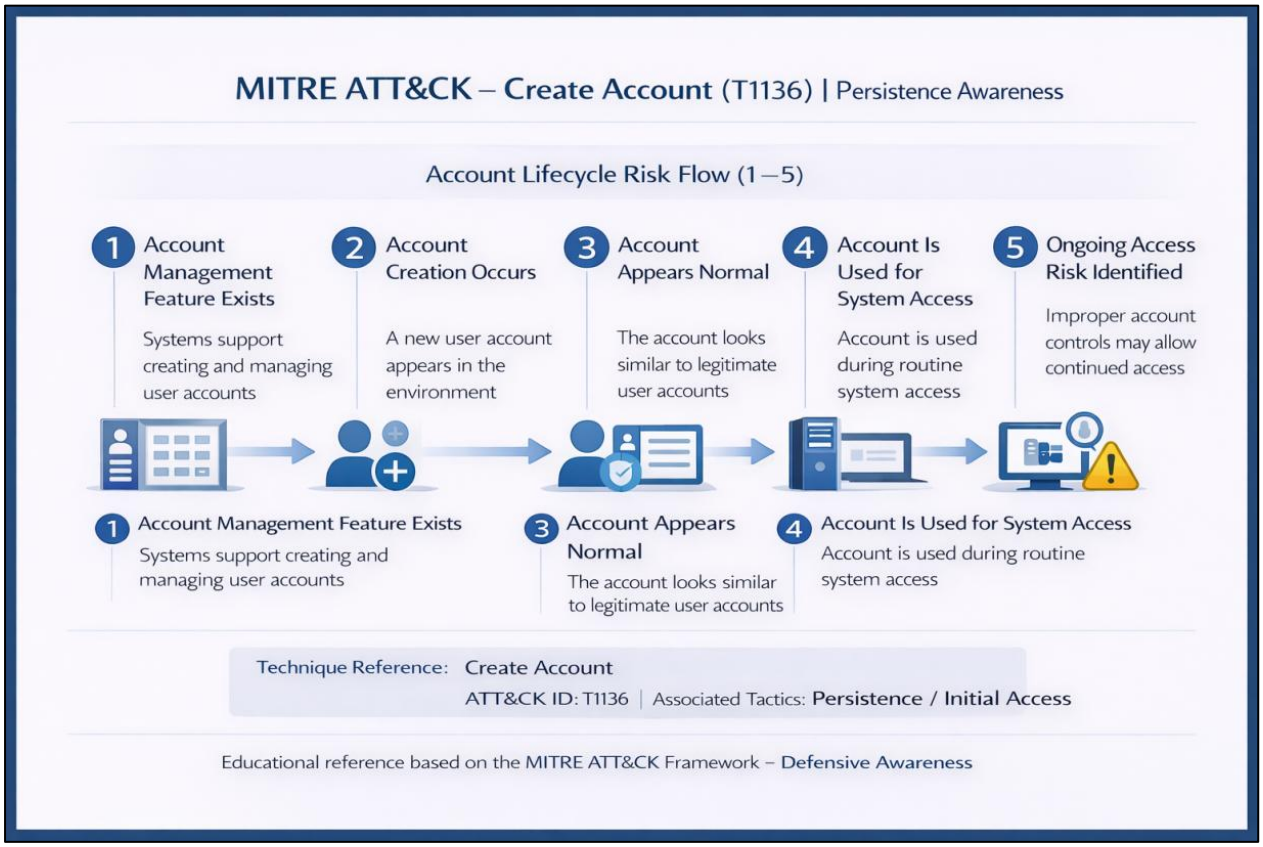
Technique 3: Compromise Host Software Binary(T1554)



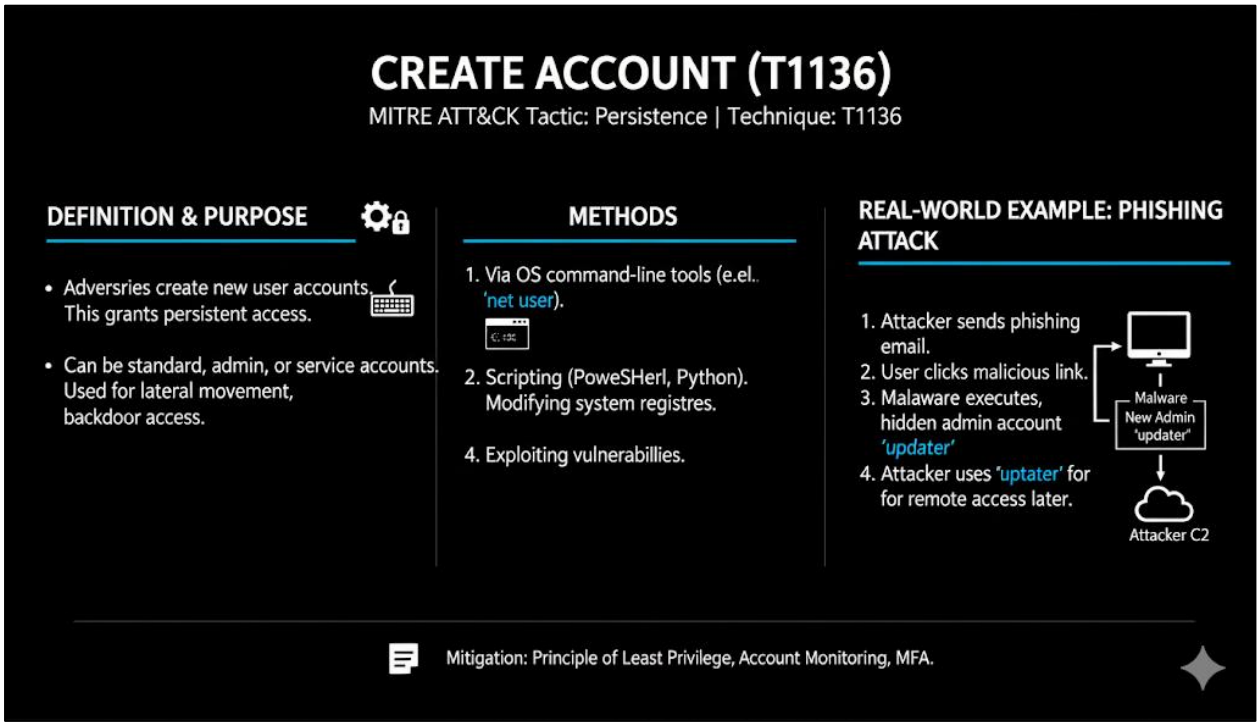
Real World Example:



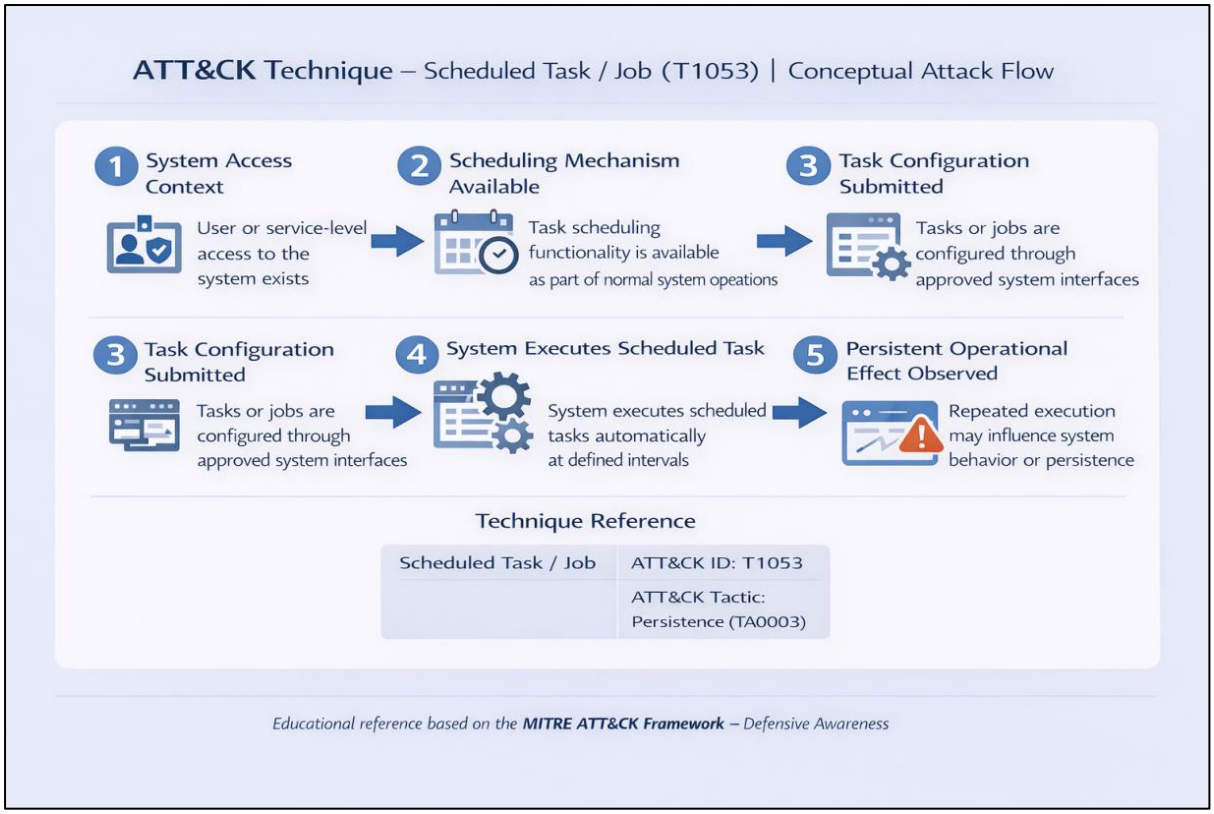
Technique 4: Create Account(T1136)



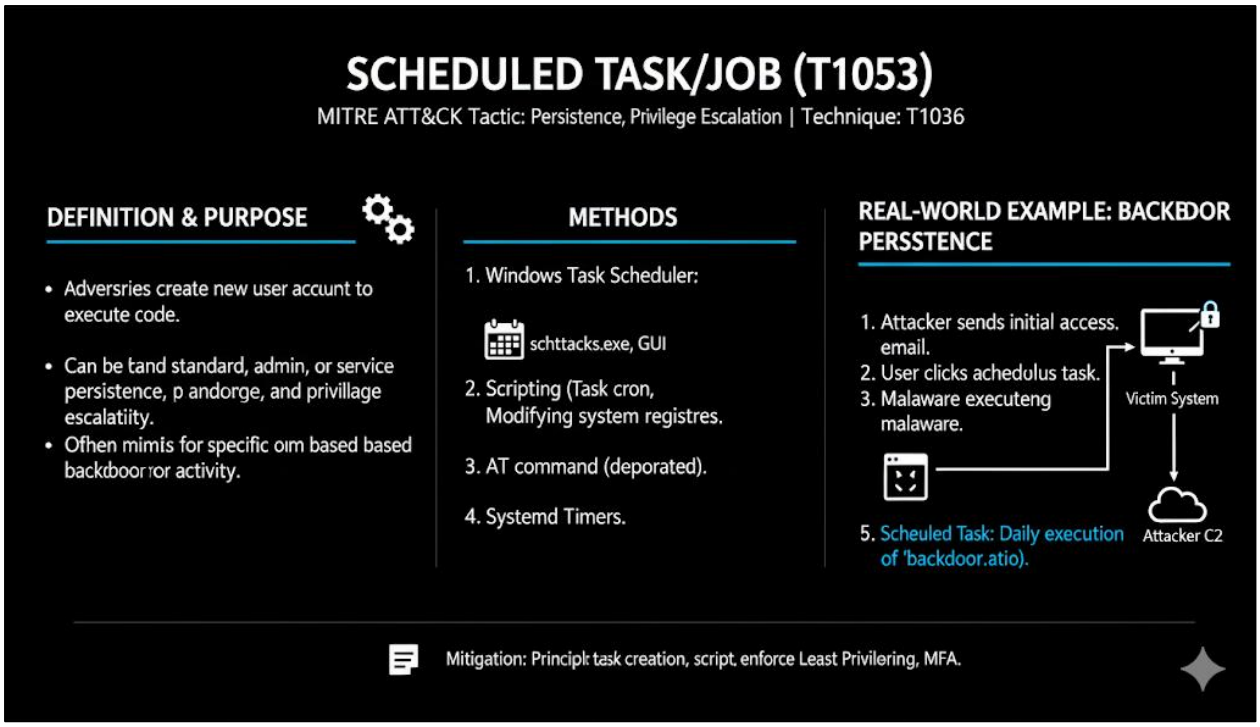
Real World Example:



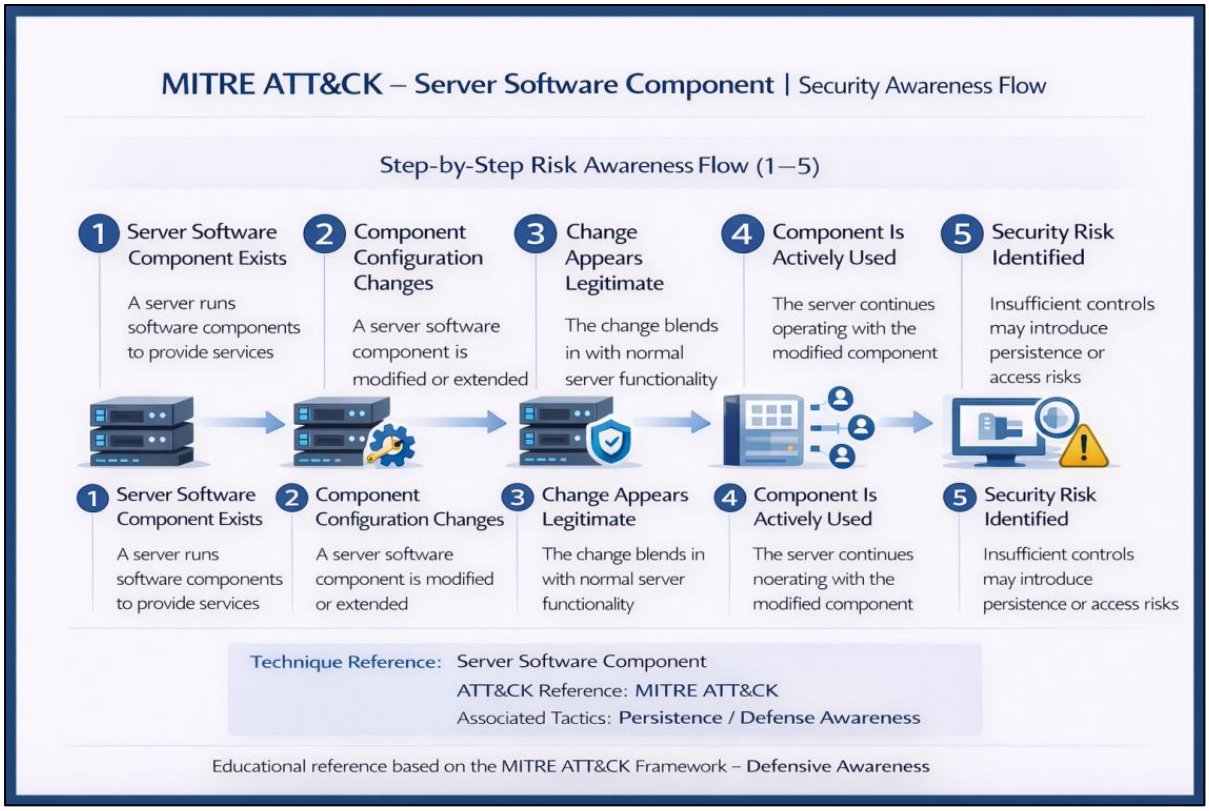
Technique 5: Scheduled Task/Job(T1053)



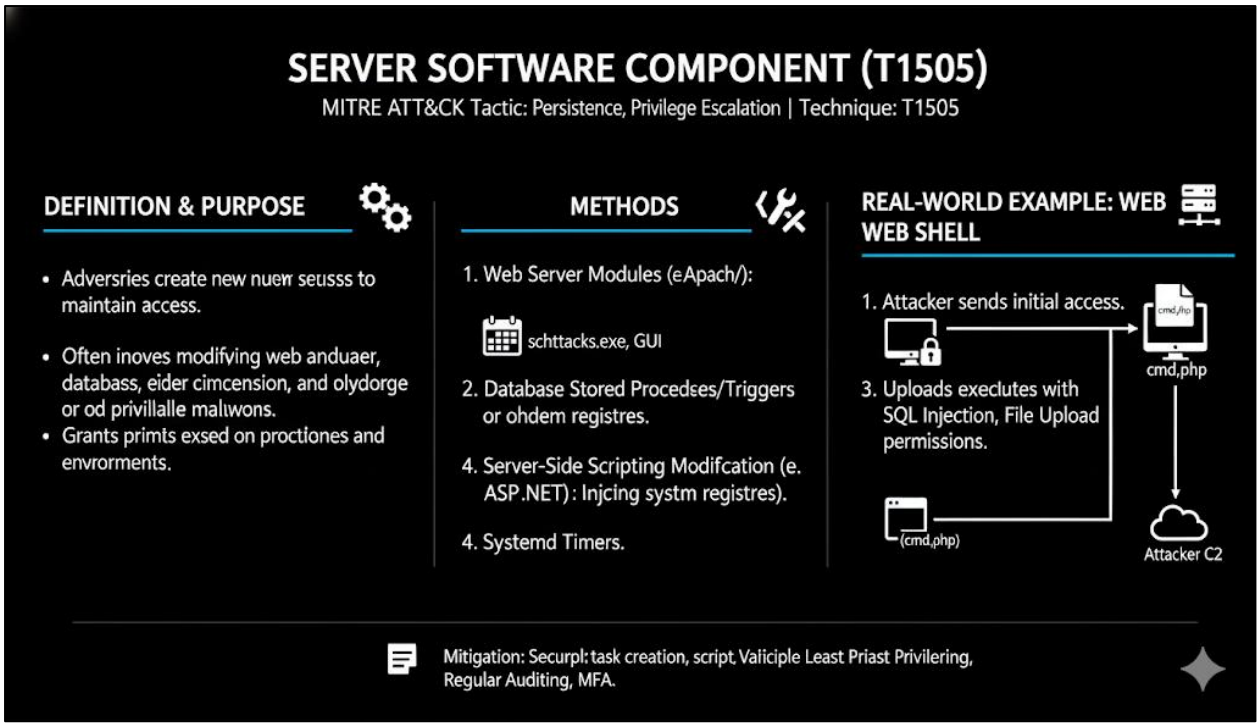
Real World Example:



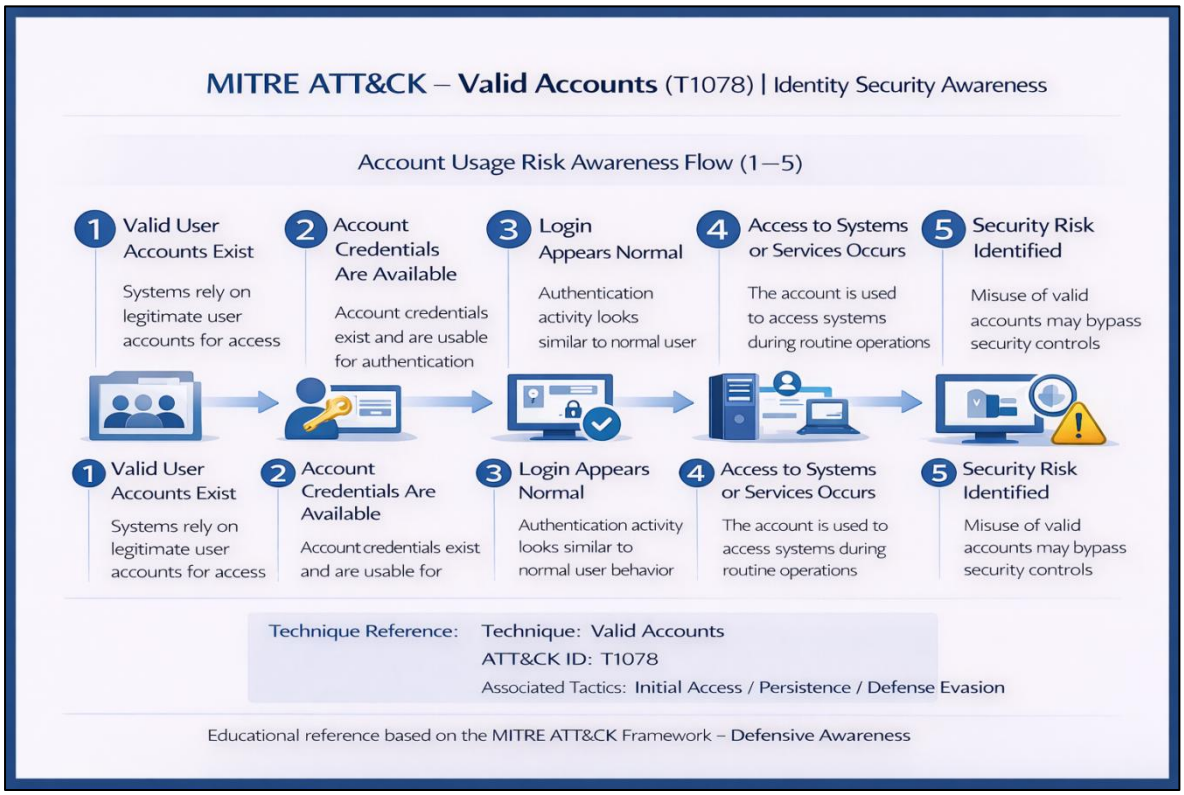
Technique 6: Server Software Component(T1505)



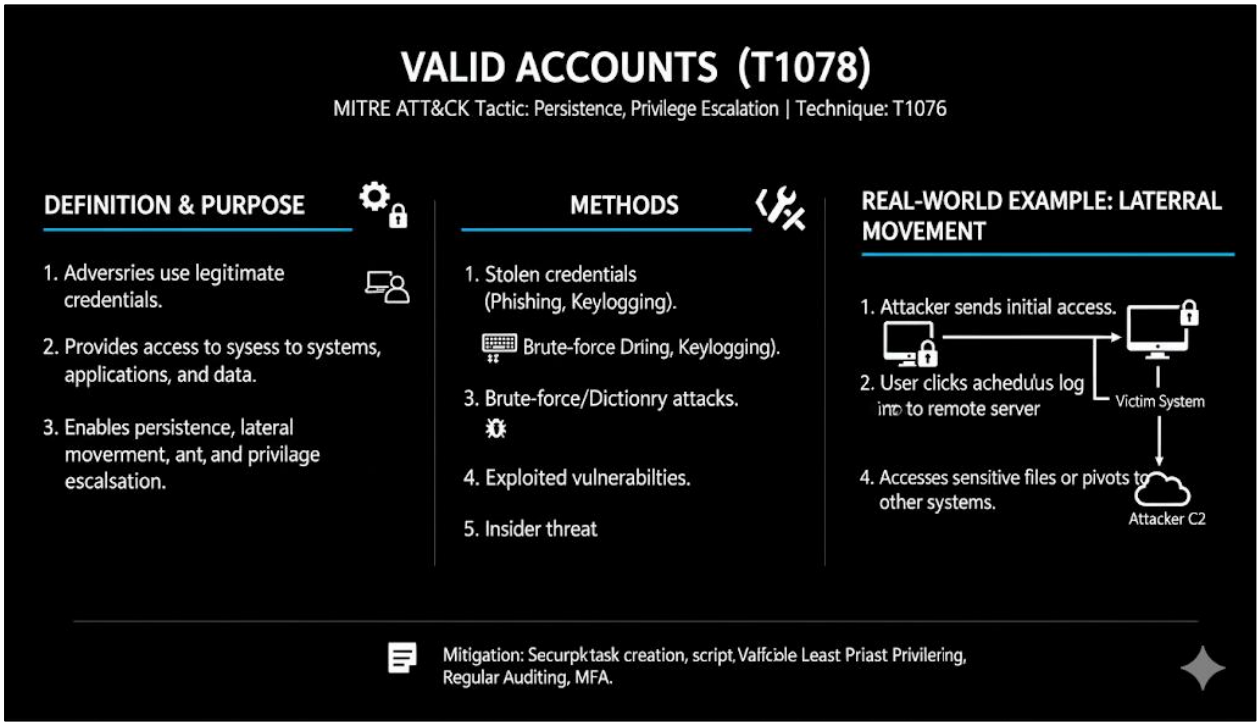
Real World Example:



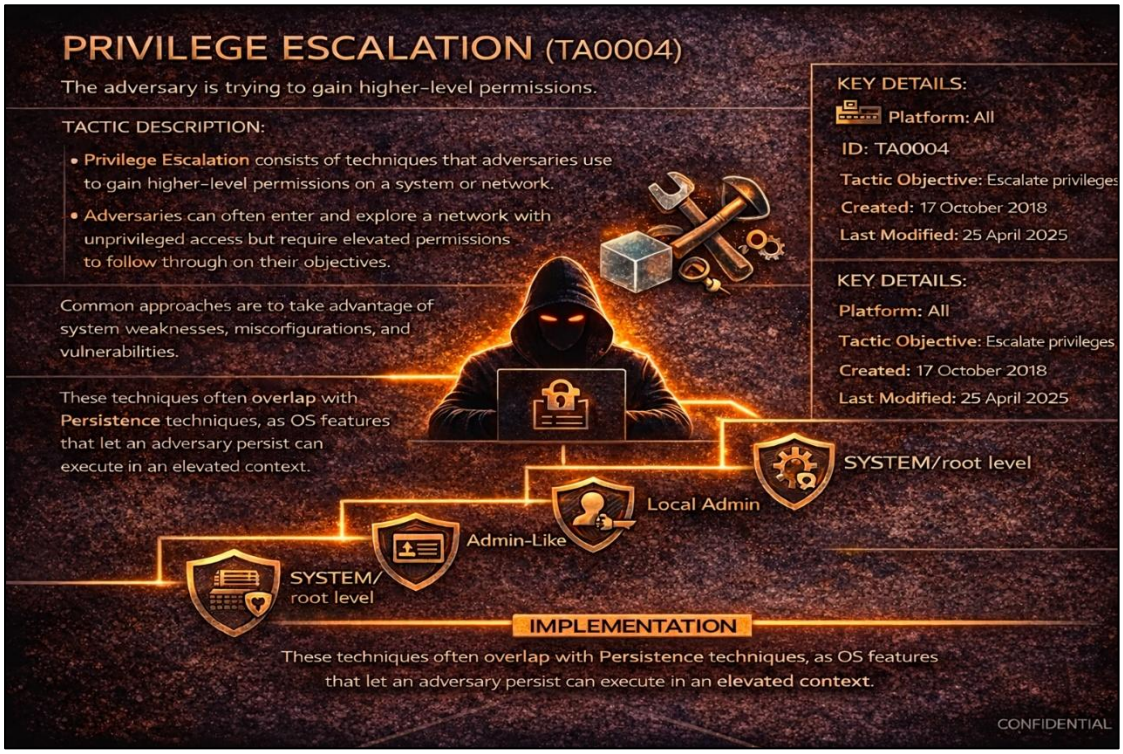
Technique 7: Valid Accounts(T1078)



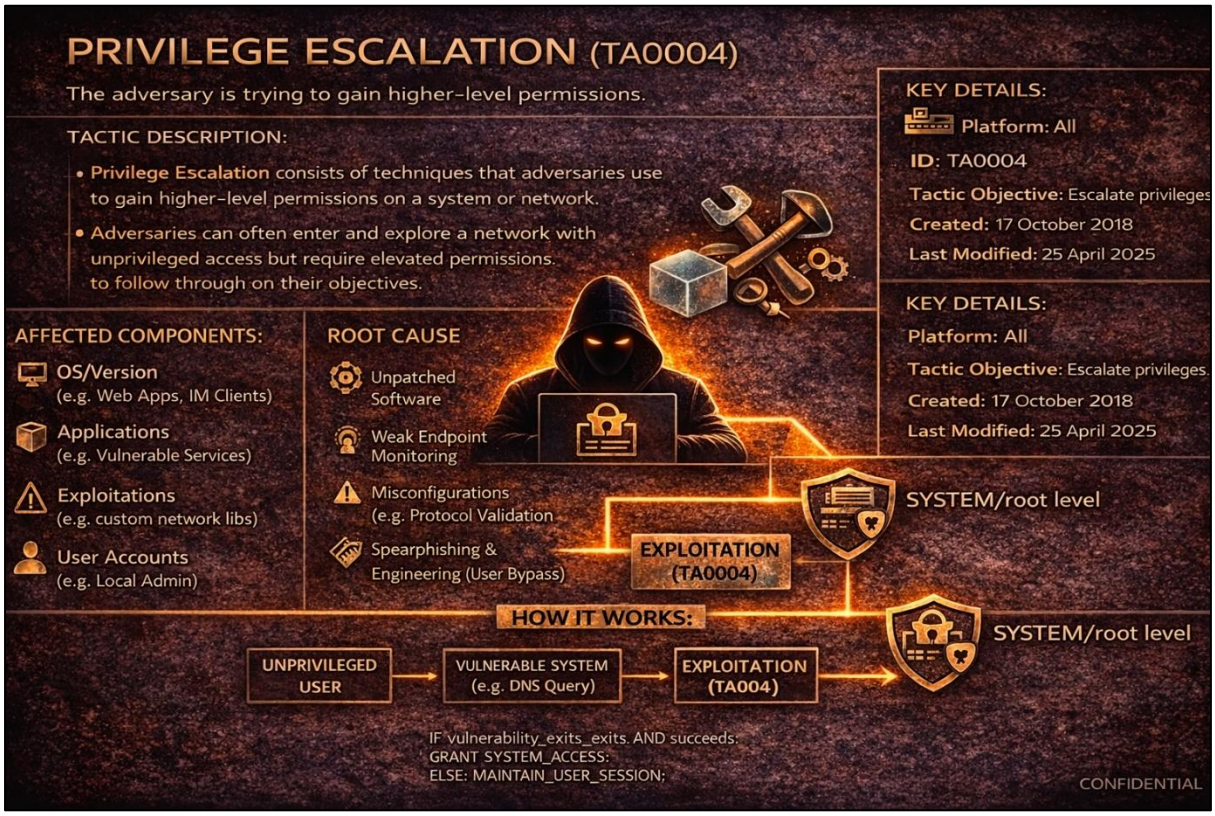
Real World Example:



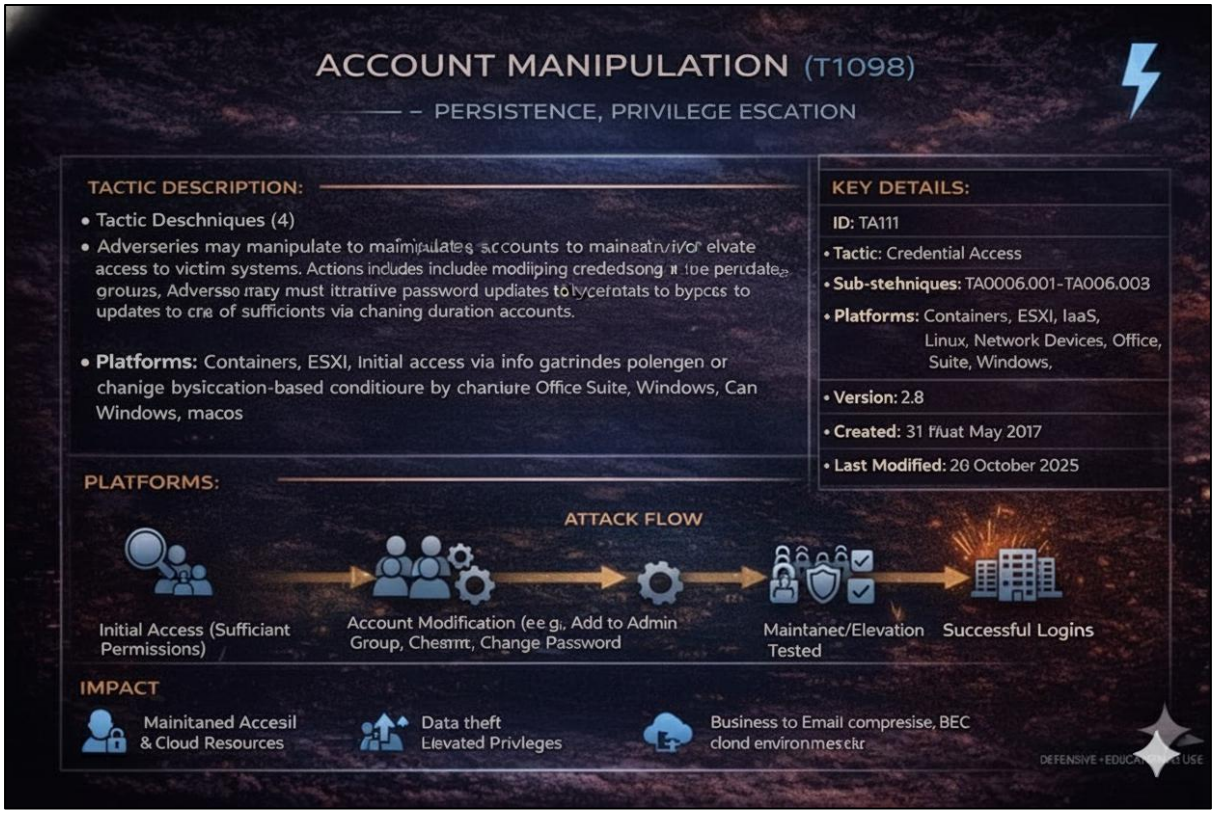
4. PRIVILEGE ESCALATION (TA0004)



Tactic Overview

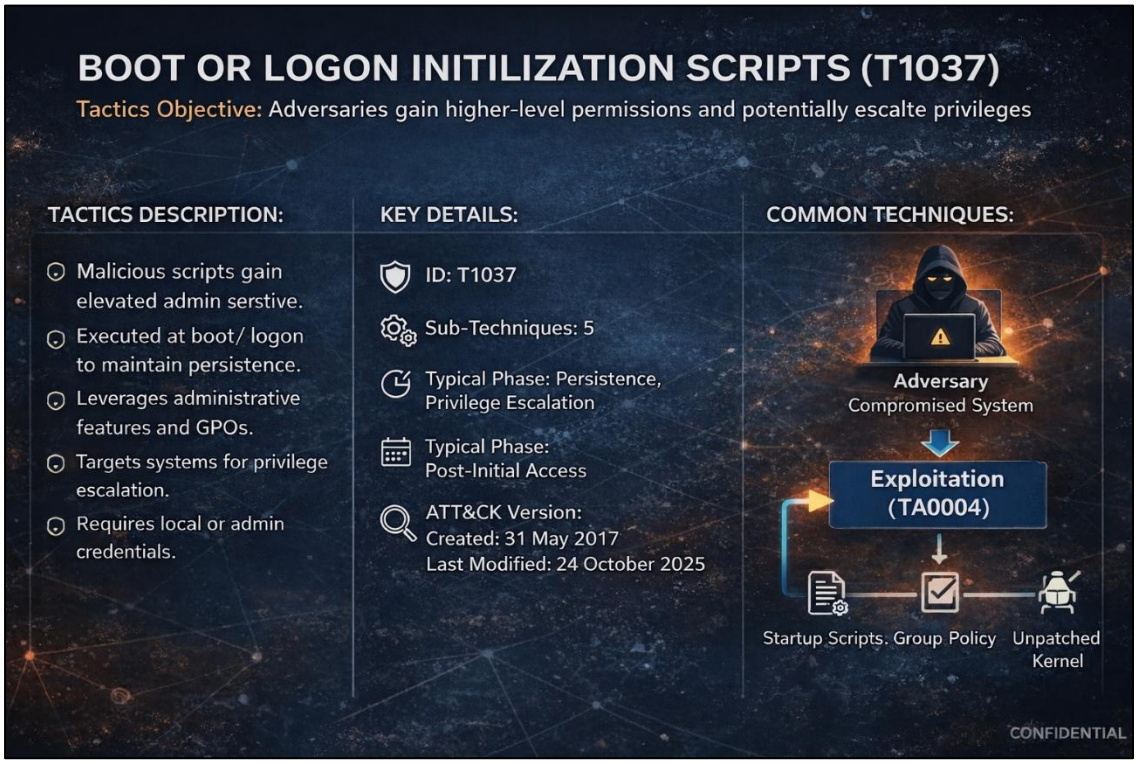


Technique 1 – ACCOUNT MANUPULATION(T1098)



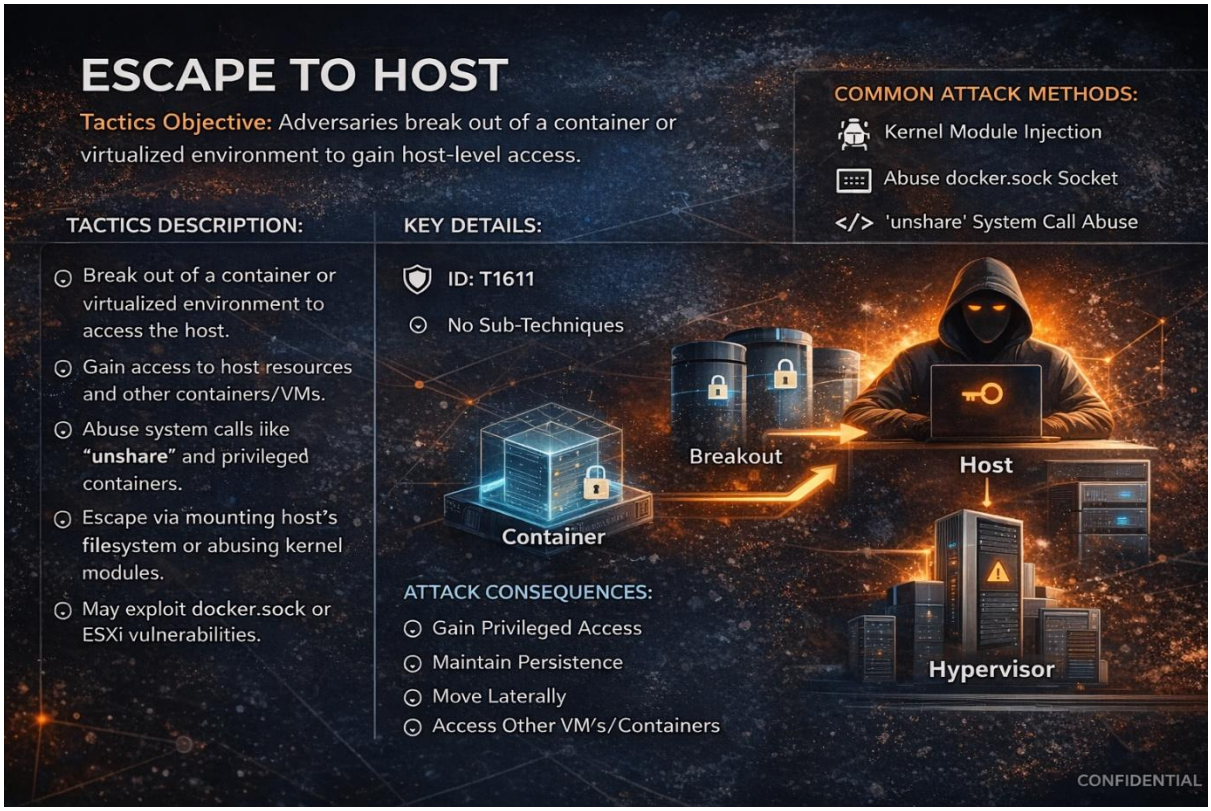
Real World Example

Technique 2 :- BOOT OR LOGON INITILIZATION SCRIPTS (T1037)

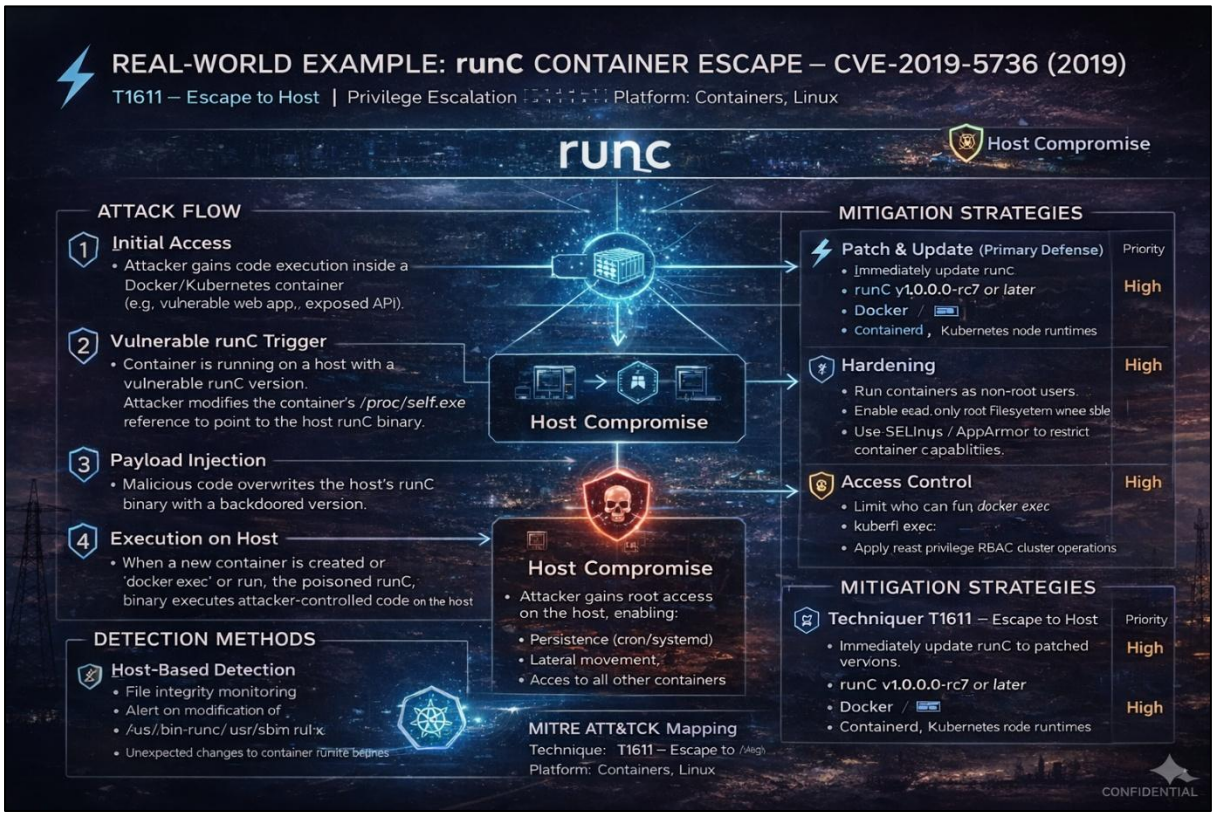


Real world example :-

Technique 3 :- ESCAPE TO HOST (T1611)



Real world example

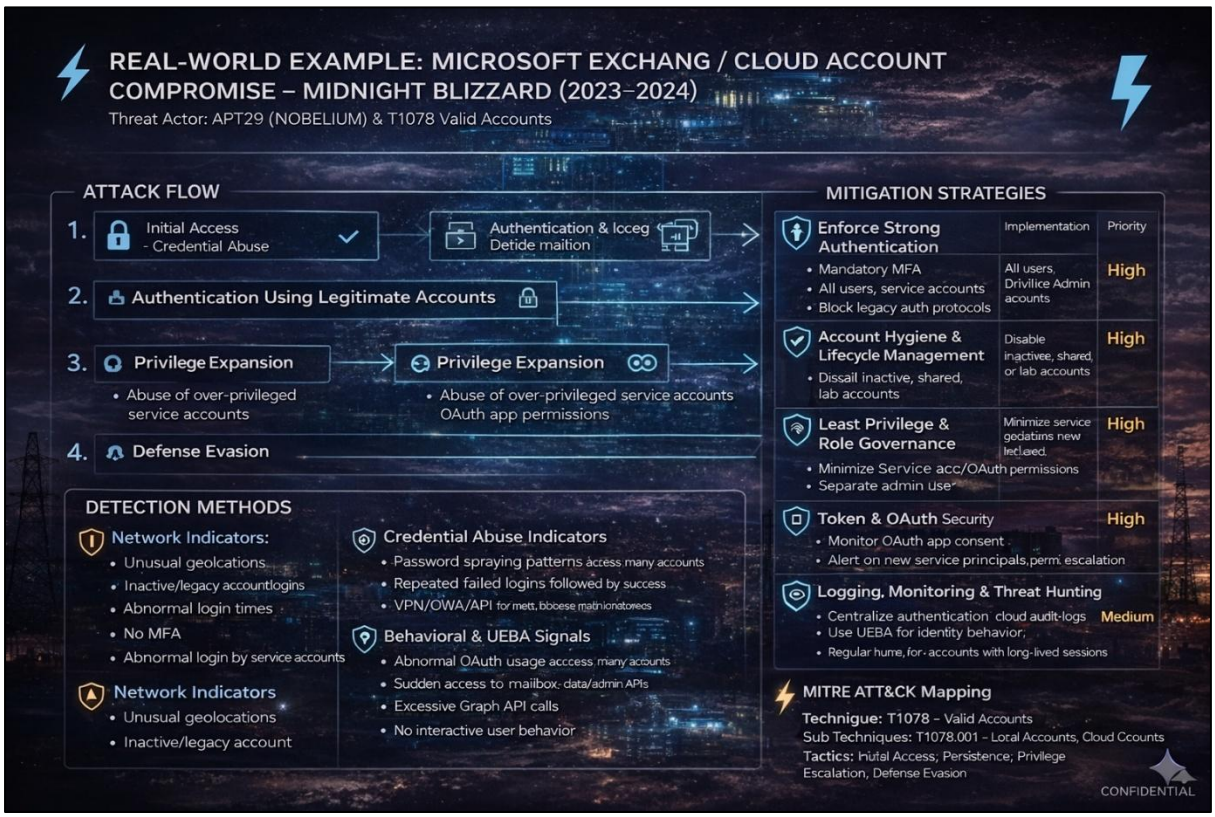


Technique 4 :- SCHEDULED TASK/ JOB (T1053)

Real world example

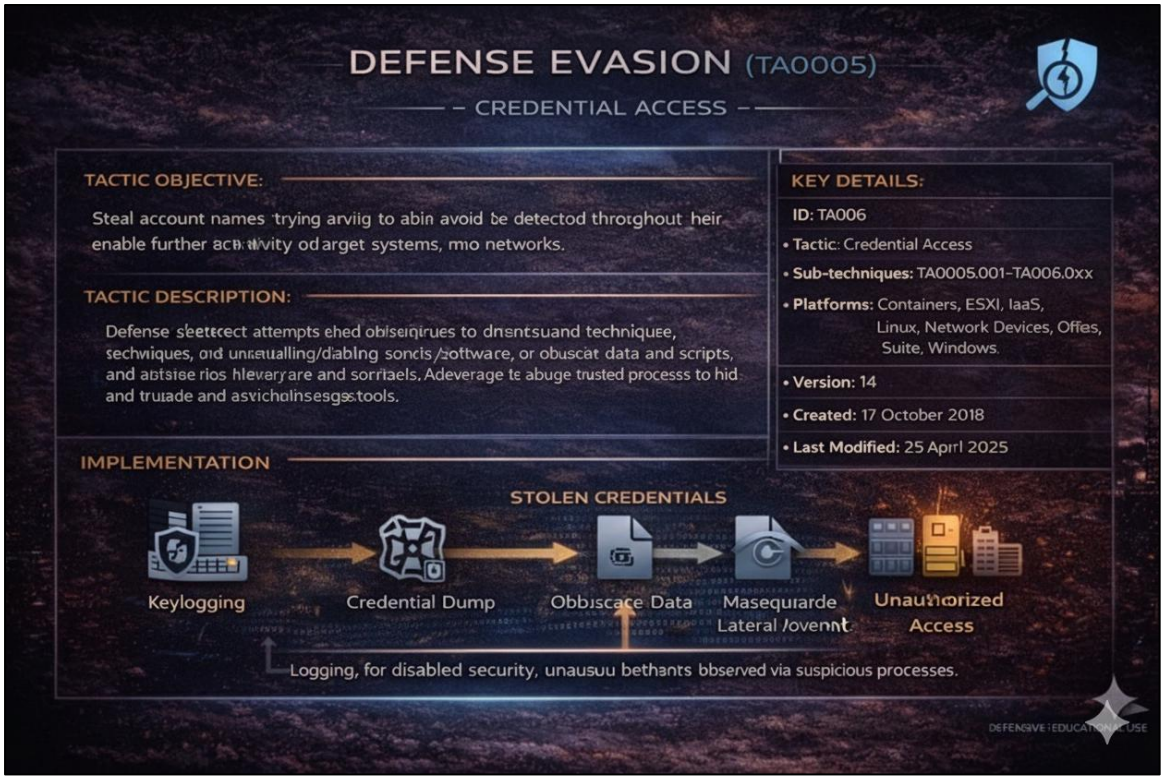
Technique 5 :- VALID ACCOUNTS (T1078)

Real world example

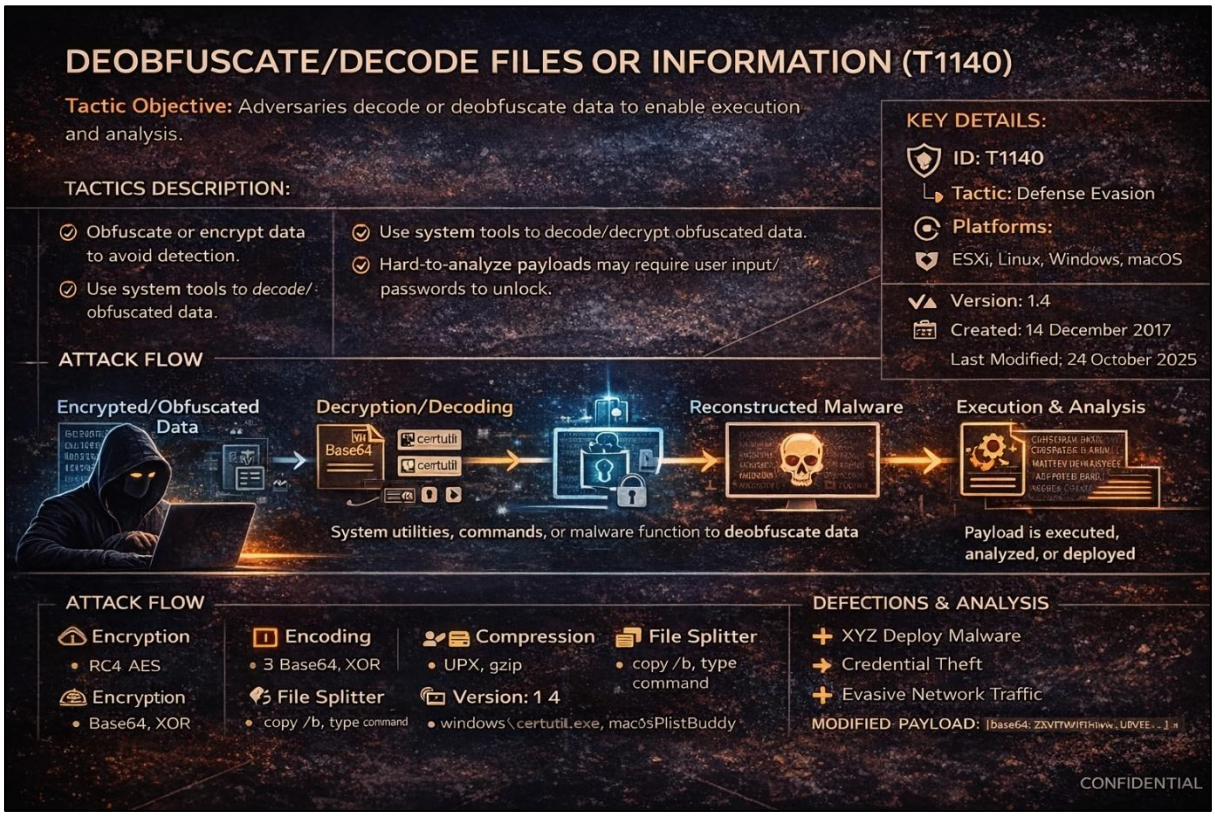


5. DEFENSE EVASION (TA005)

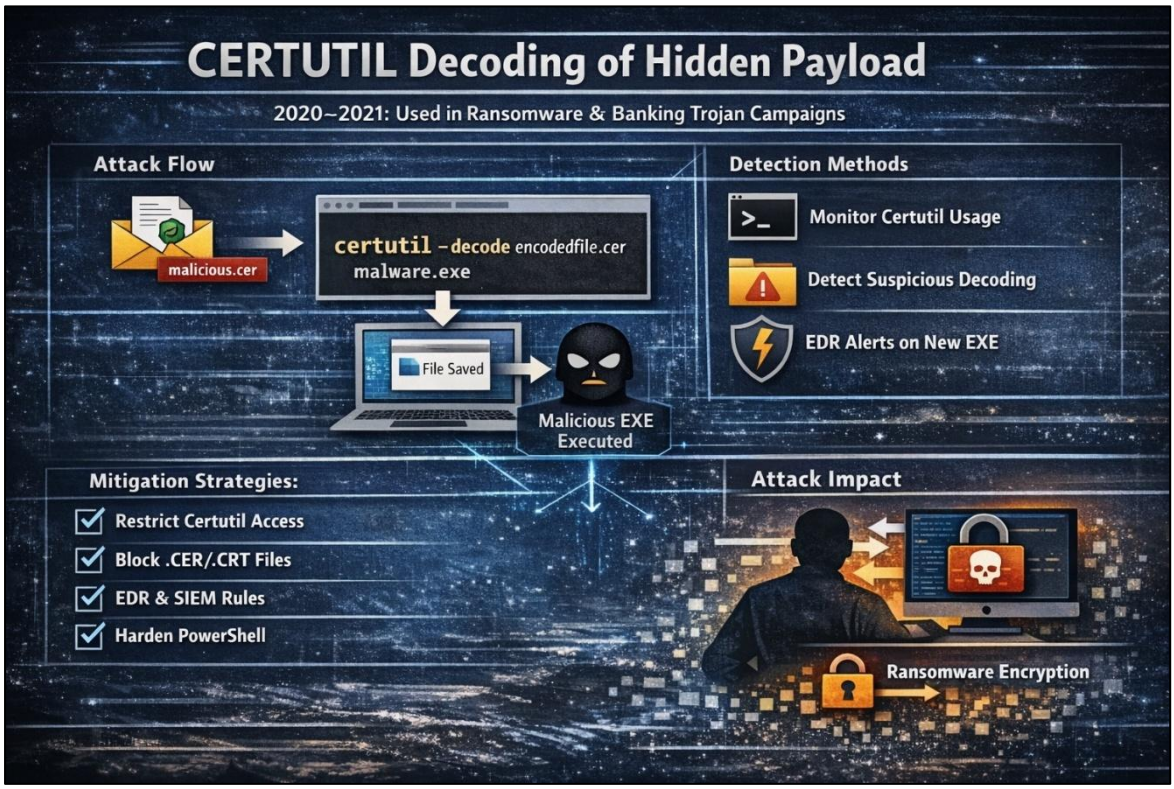
Tactic overview



Technique 1 :- DEOBFUSCATE/DECODE FILES OR INFORMATION (T1140)

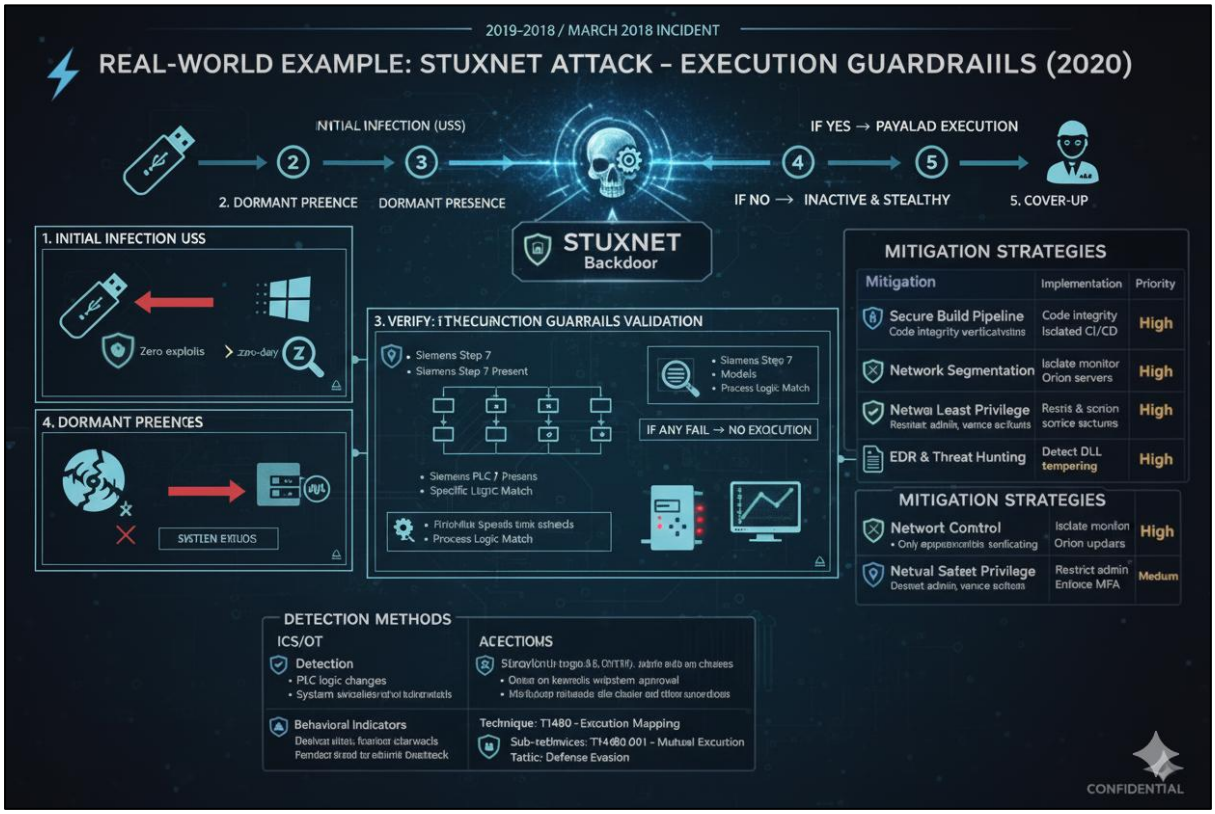


Real world Example



Technique 2 :- EXECUTION GUARDRAILS (T1480)

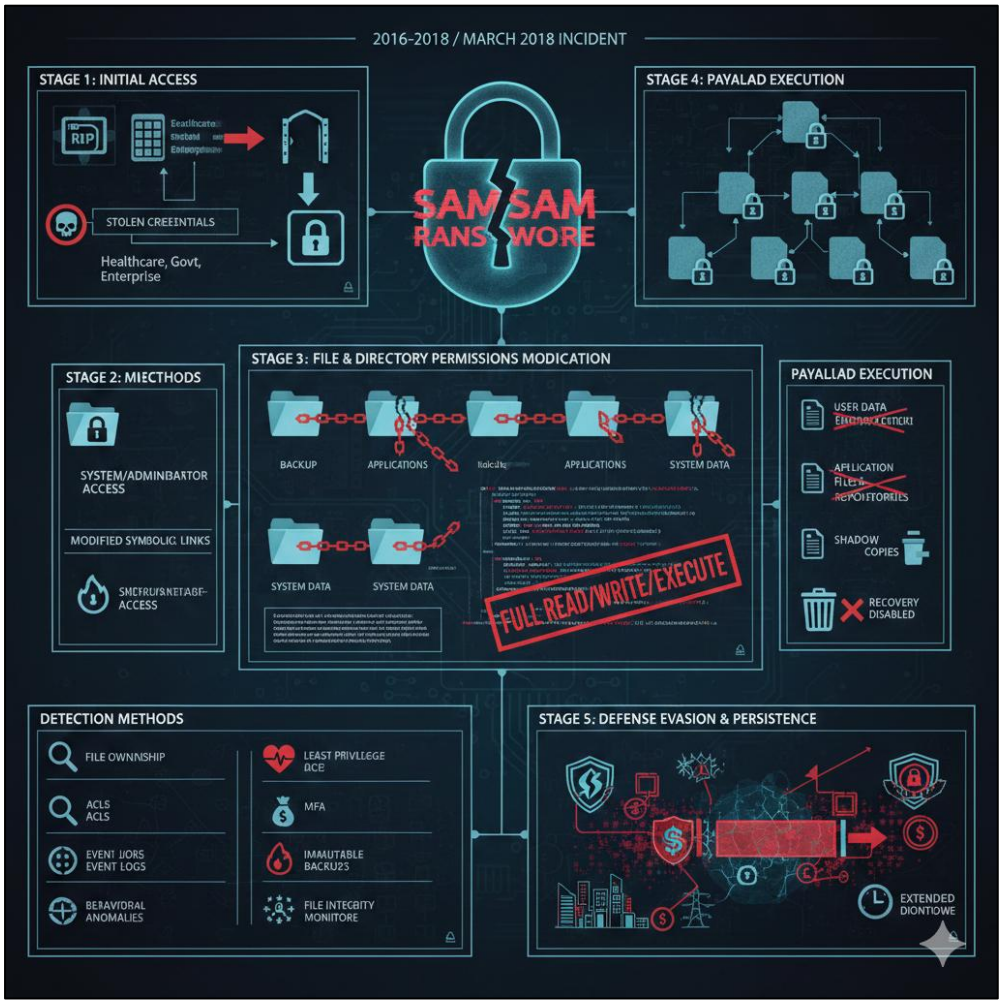
Real World Example



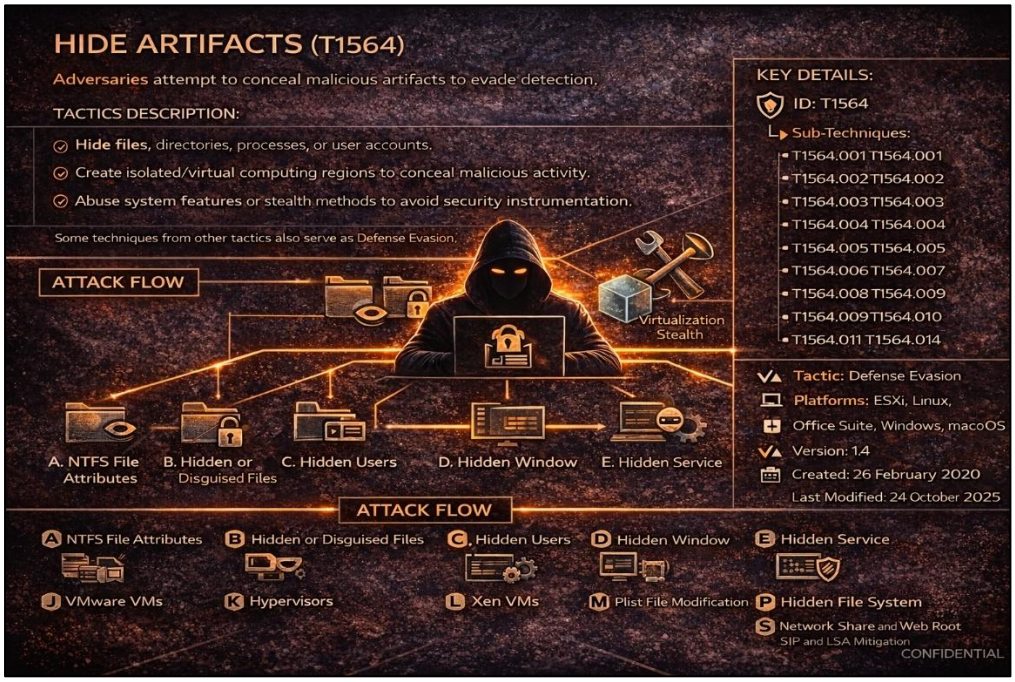
Technique 3 FILE AND DIRECTORY PERMISSIONS MODIFICATION (T12

22)

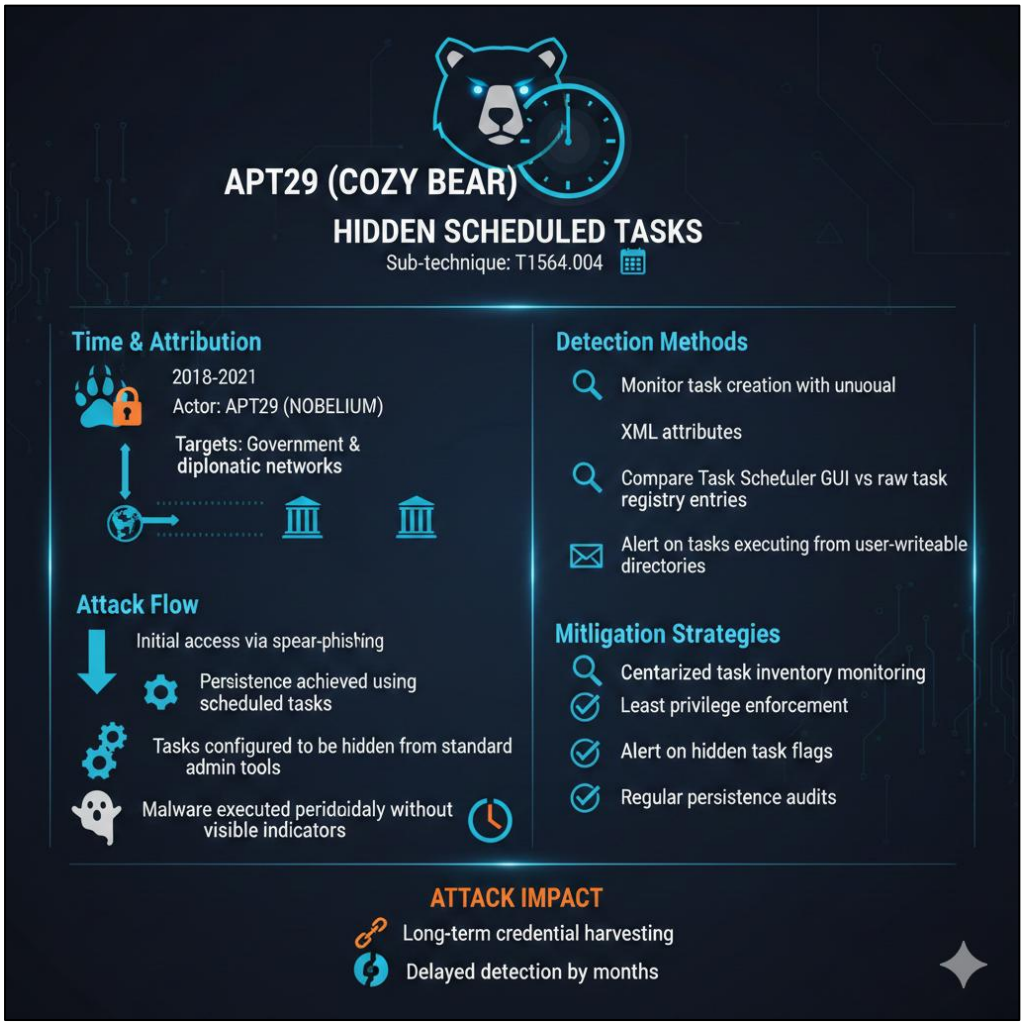
Real world example



Technique 4:- HIDE ARTIFACTS (T1564)

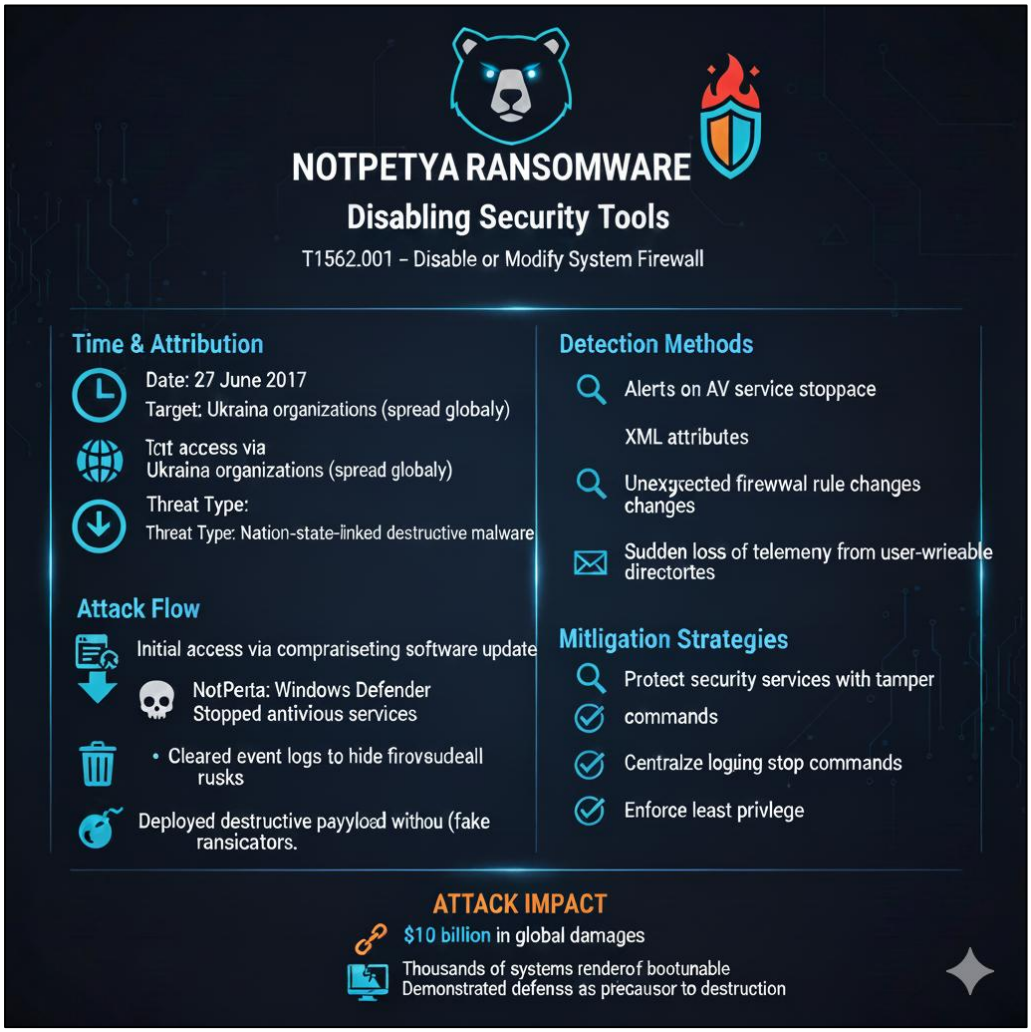


Real world example



Technique 5:- IMPAIR DEFENSES (T1562)

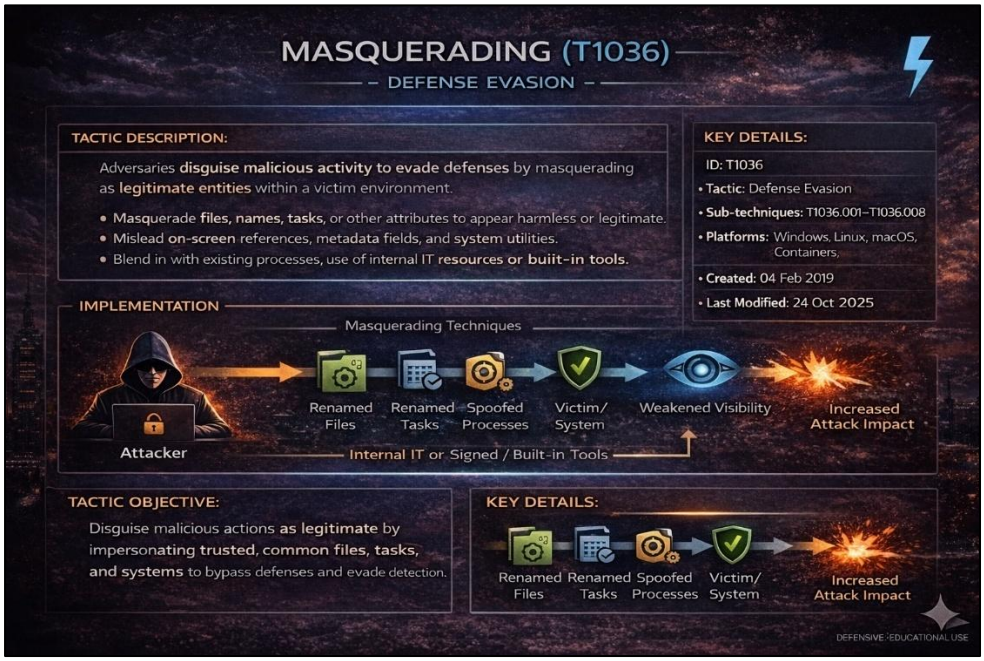
Real world example



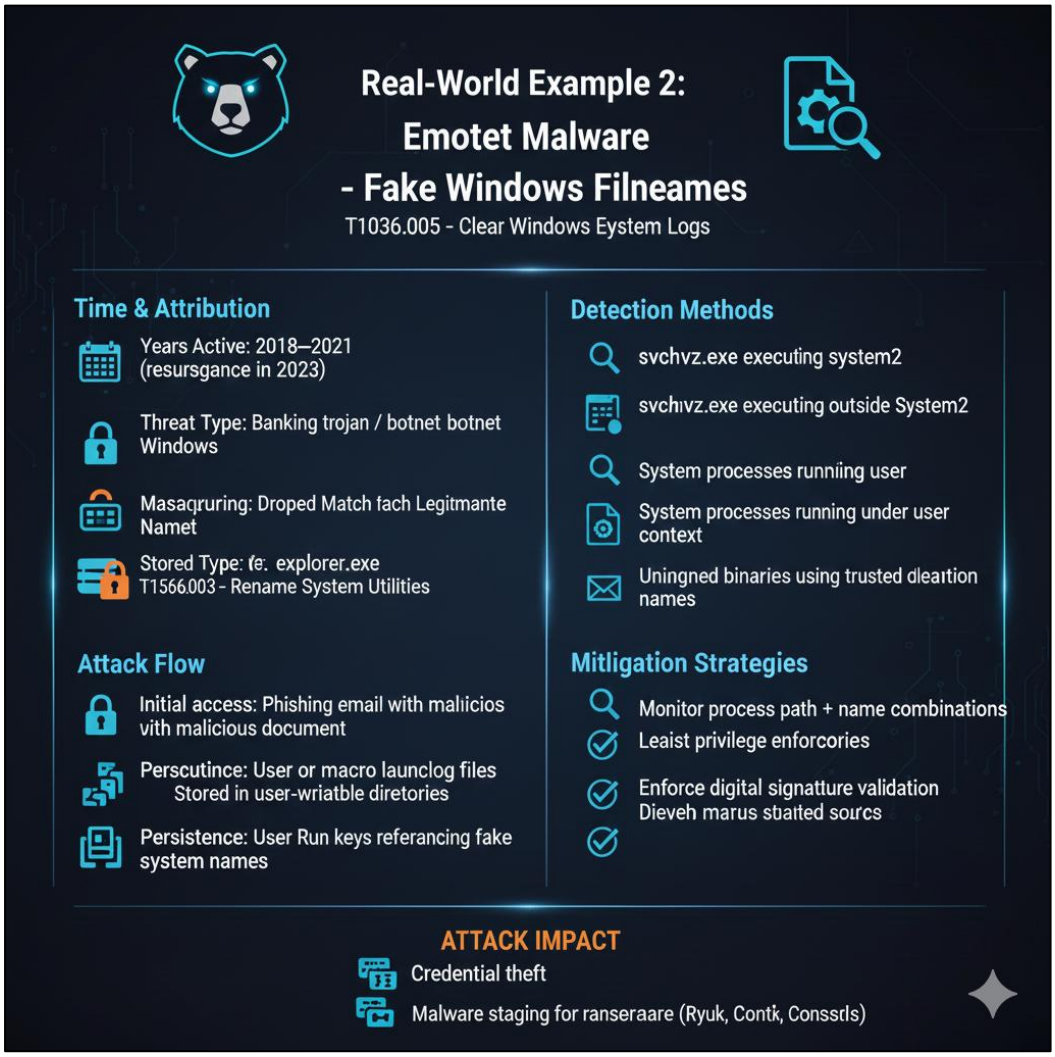
Technique 6:- INDICATOR REMOVAL (T1070)

Real world example

Technique 7:- MASQUERADING (T1036)

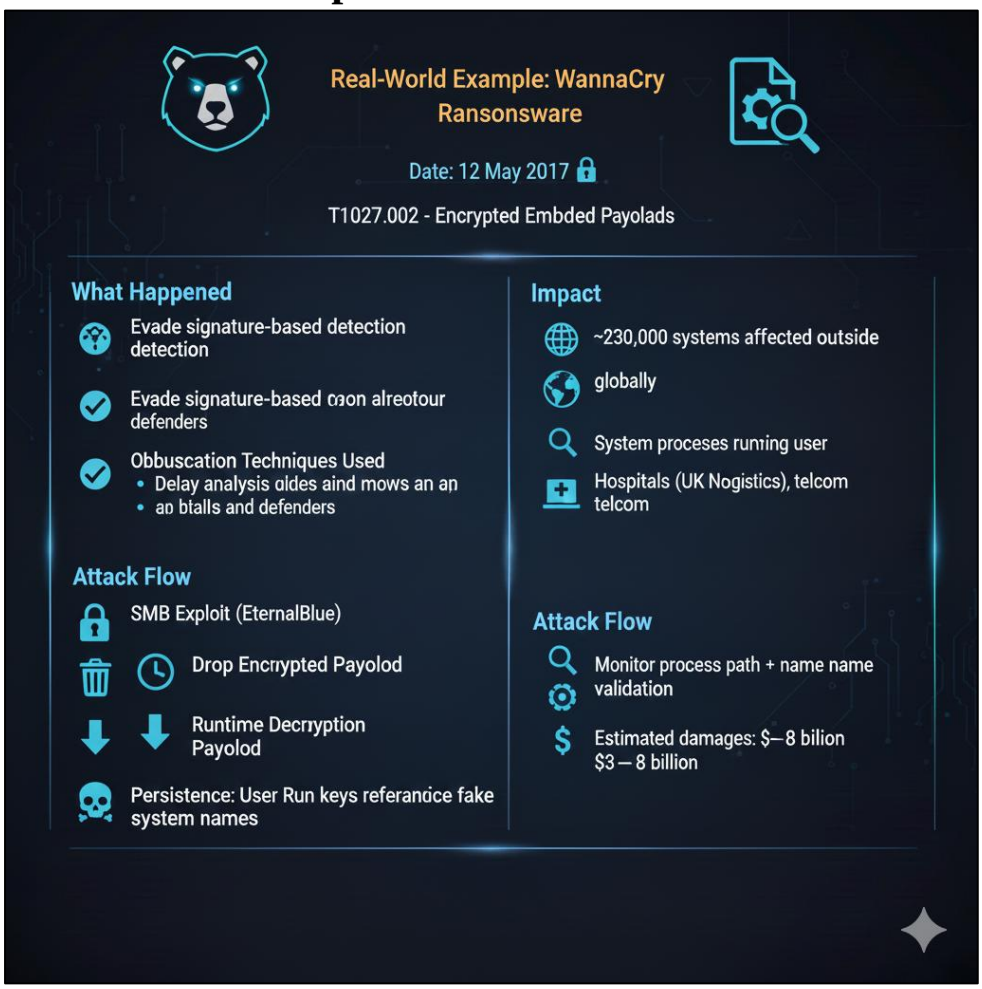


Real World Example



Technique 8:- OBFUSCATED FILES OR INFORMATION (T1027)

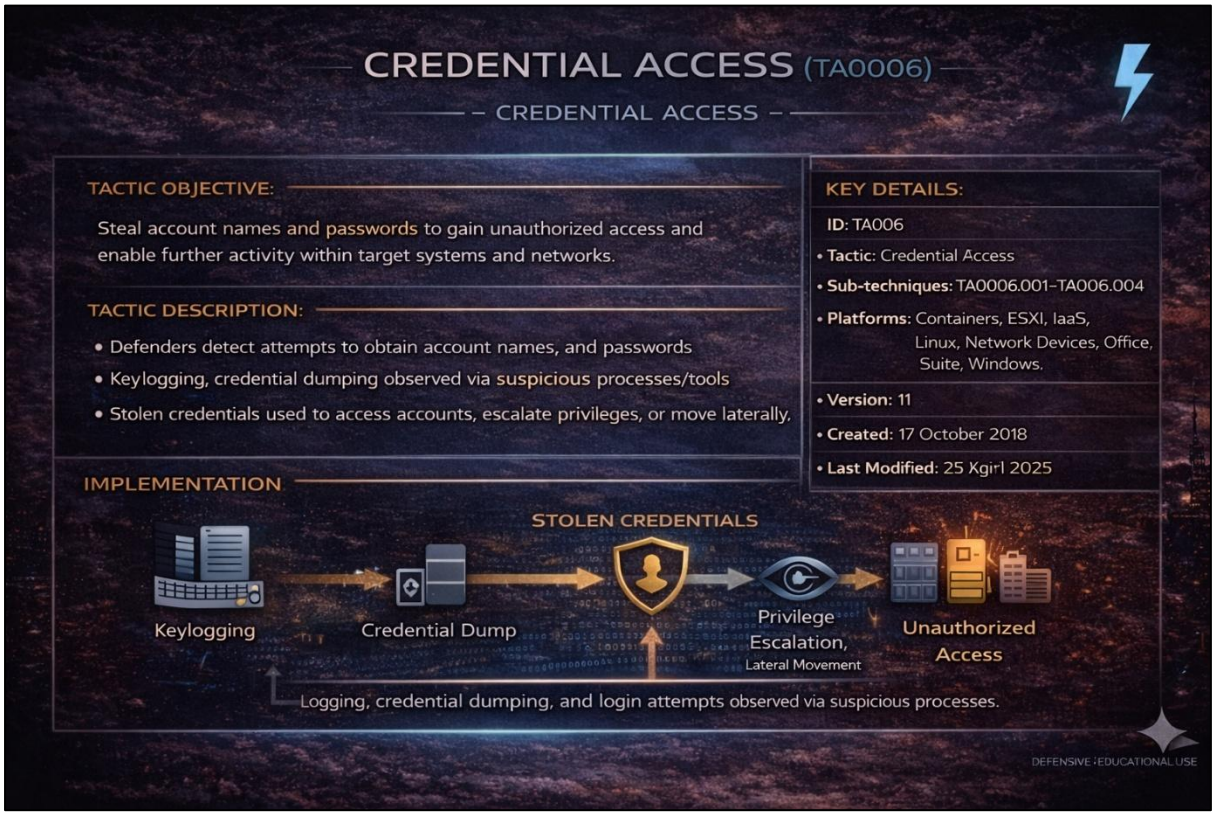
Real World Example



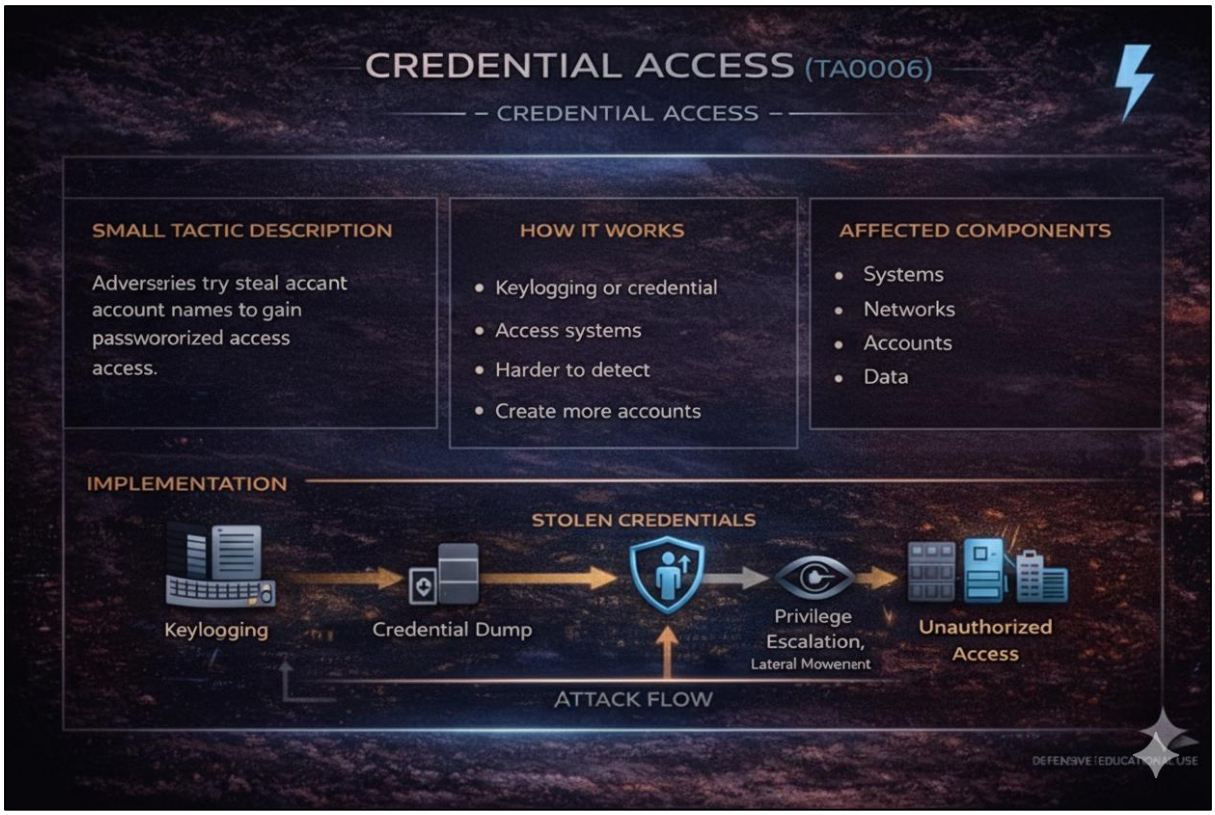
Technique 9:- VALID ACCOUNTS (T1078)

Real World Example

Tactic 6:- CREDENTIAL ACCESS (TA0006)

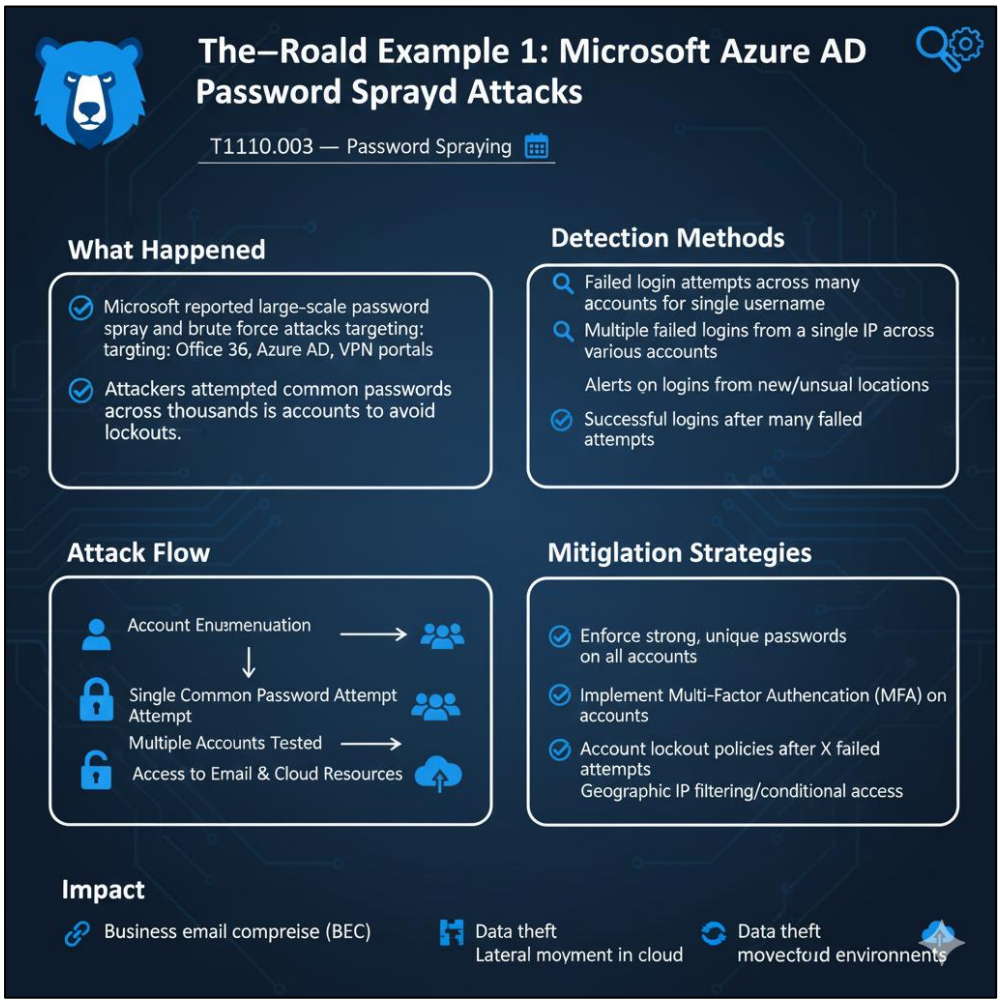


Tactic Overview



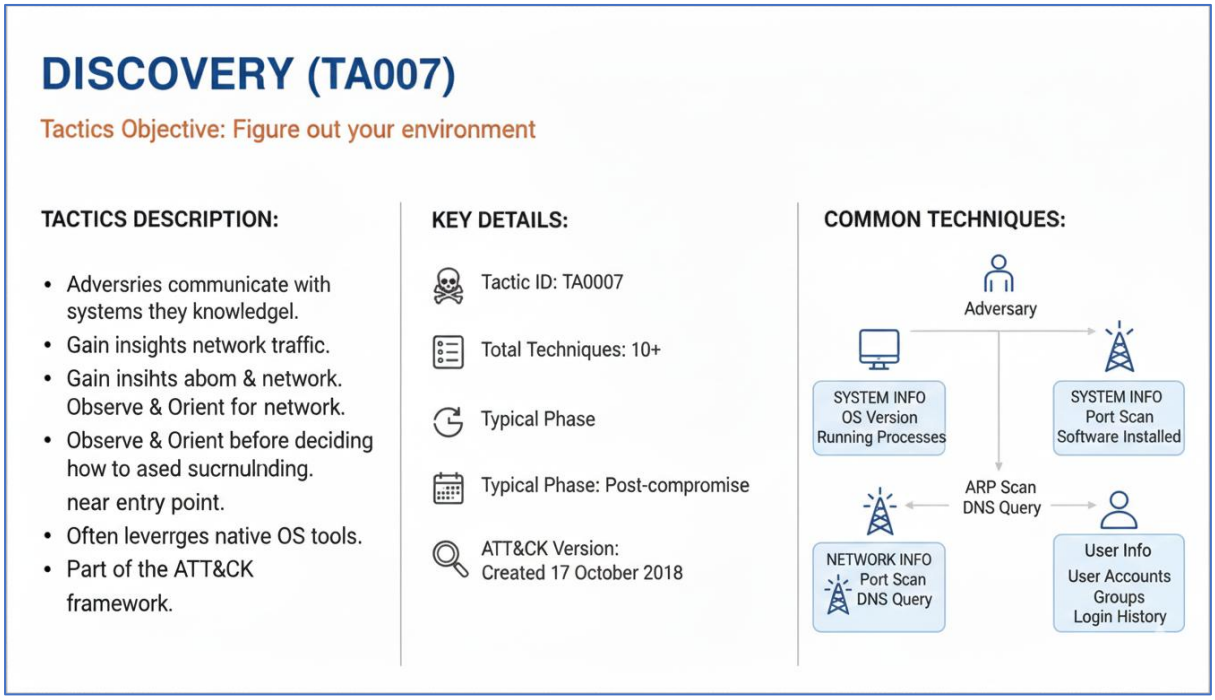
Technique 1 :- BRUTE FORCE (T1110)

Real world example

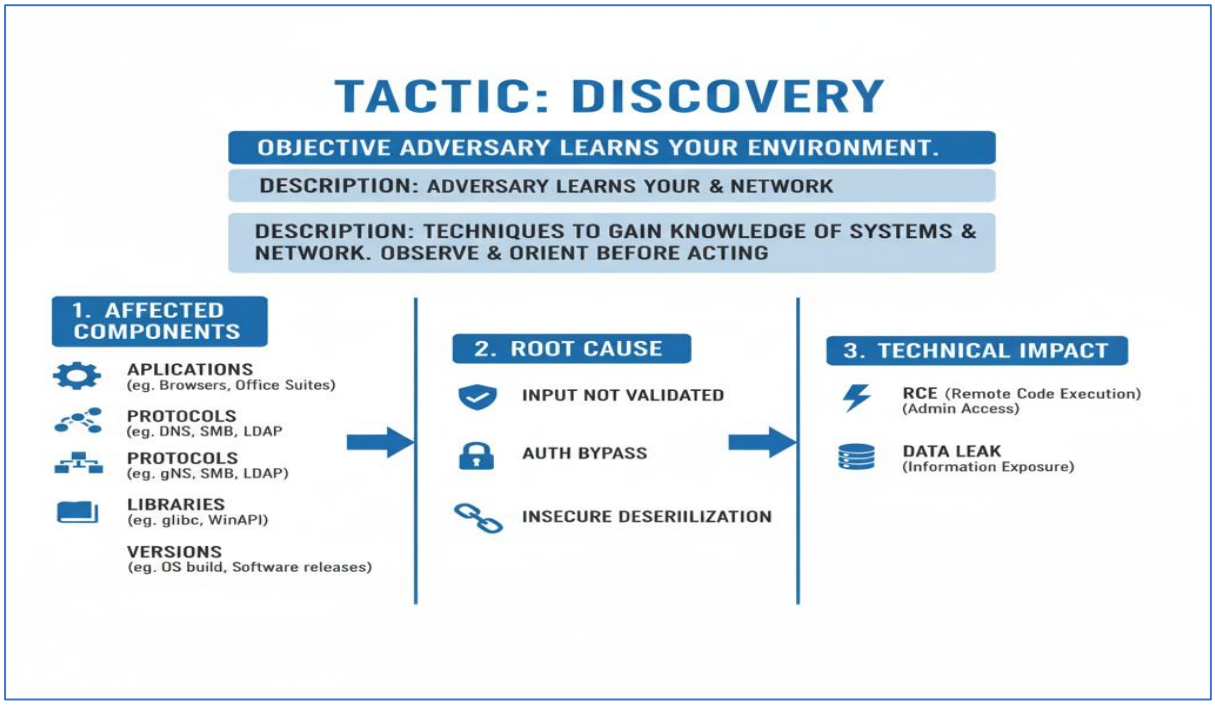


7. Discovery (TA0007)

Overview:

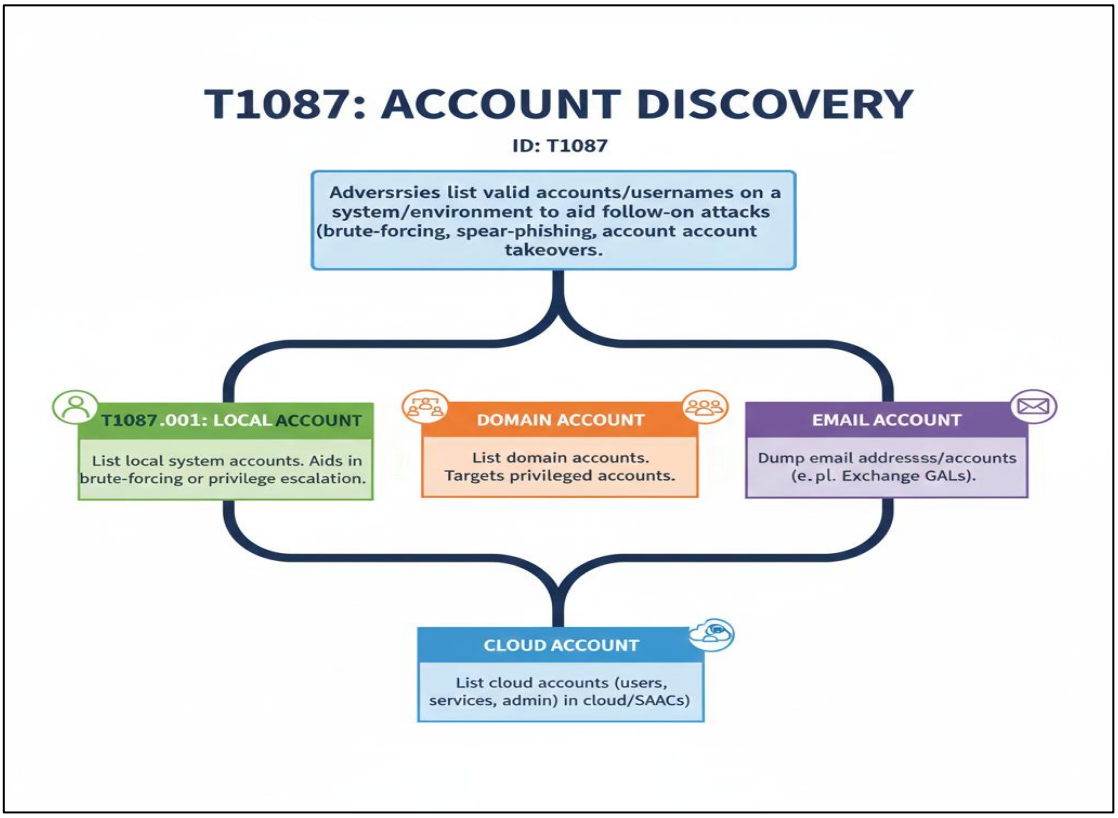


Technical Detail:

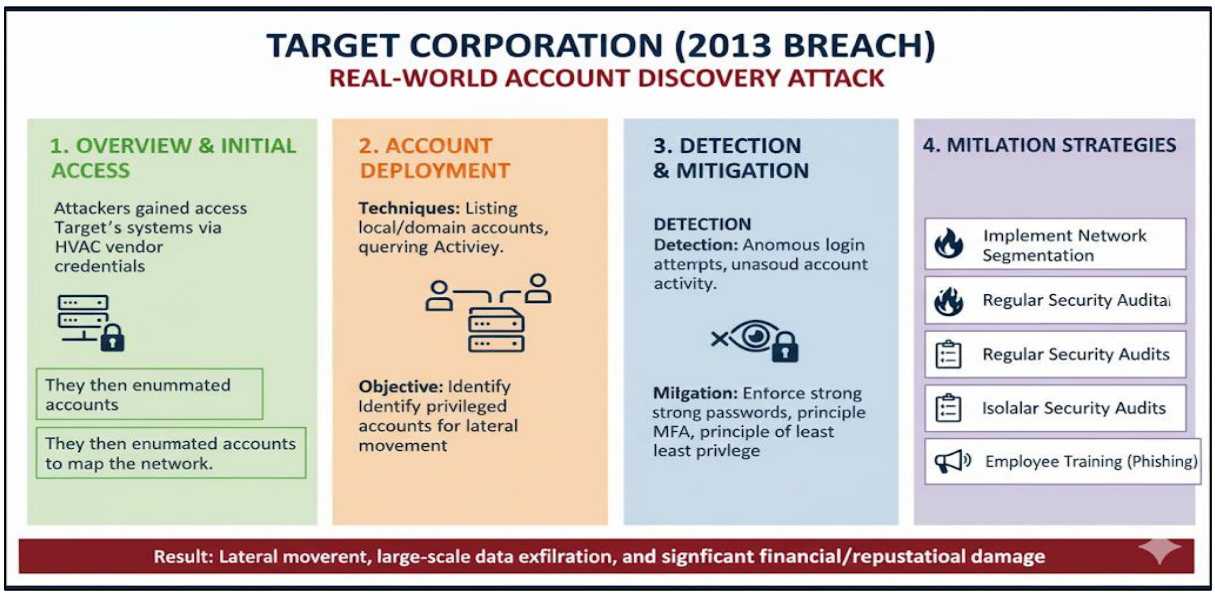


Technique 1 : Account Discovery (T1087)

Overview:

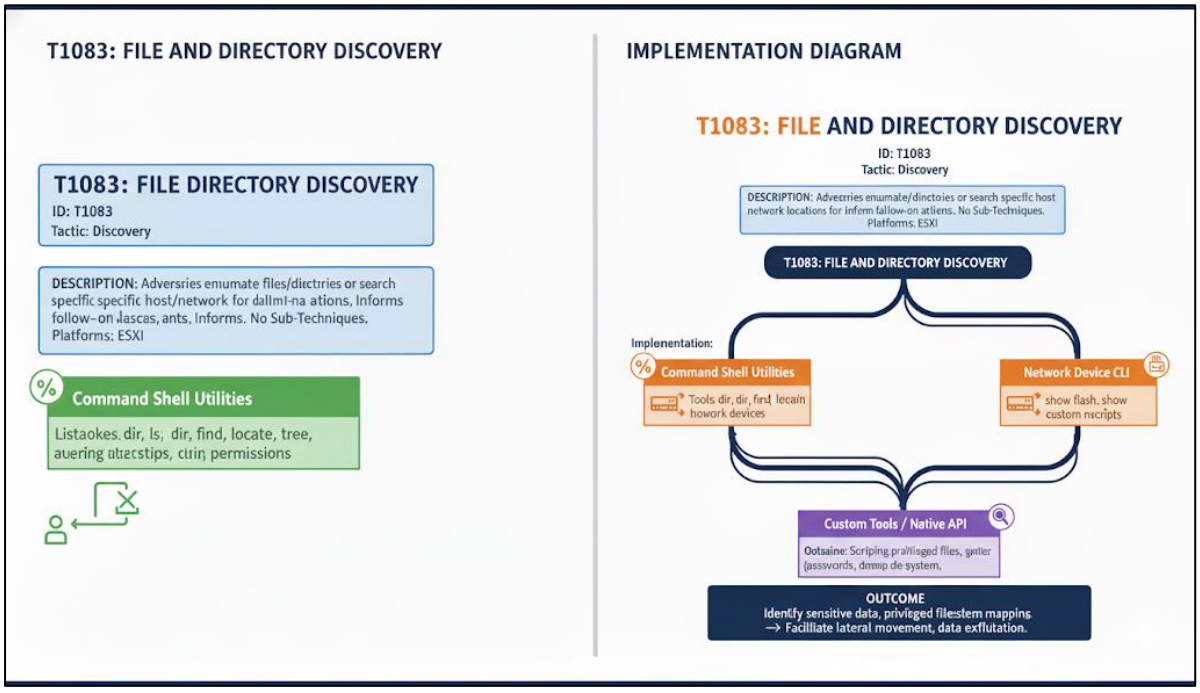


Real World Example:

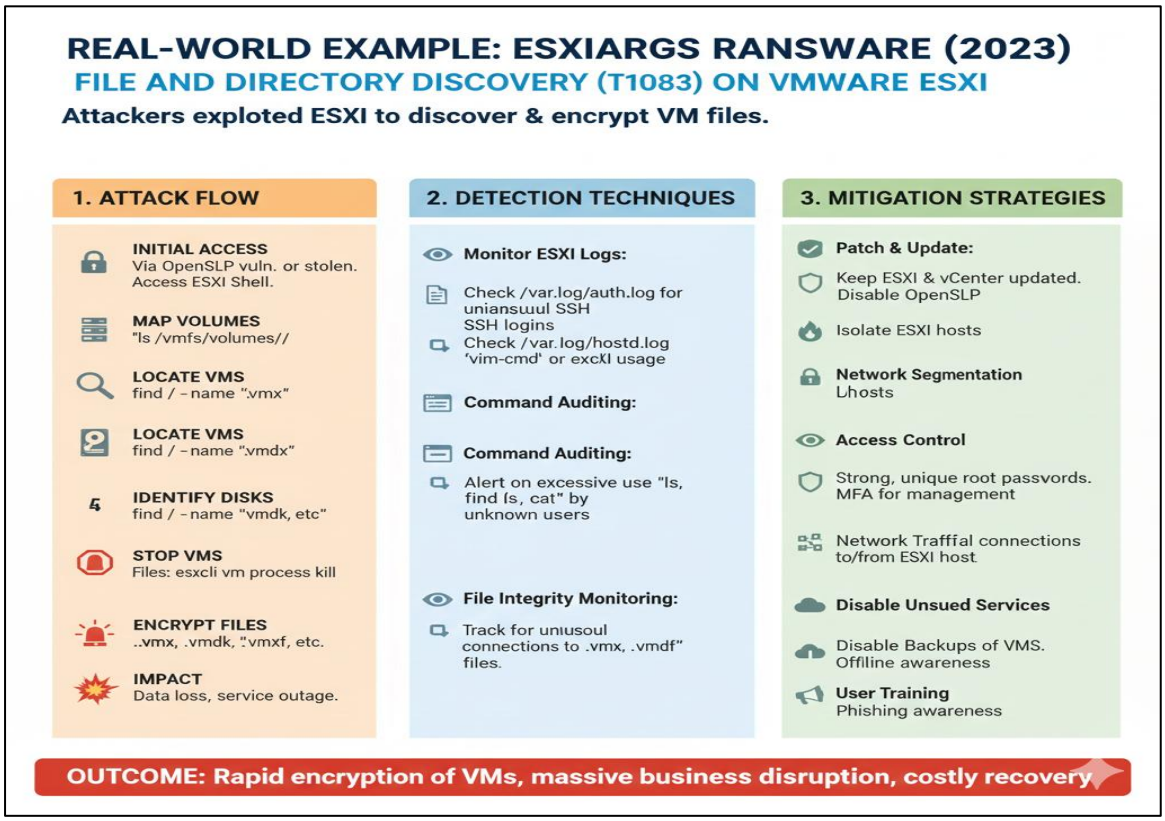


Technique 2: File and Directory Discovery

Overview:

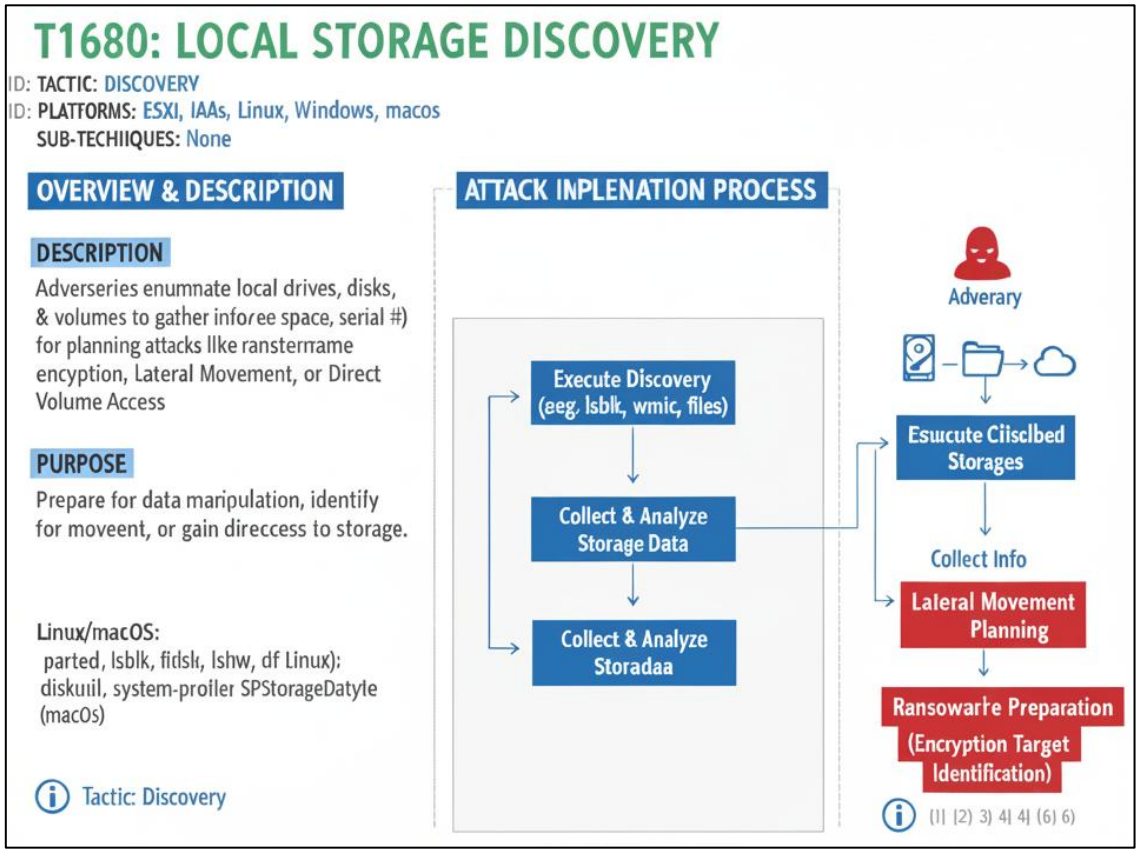


Real World Example:

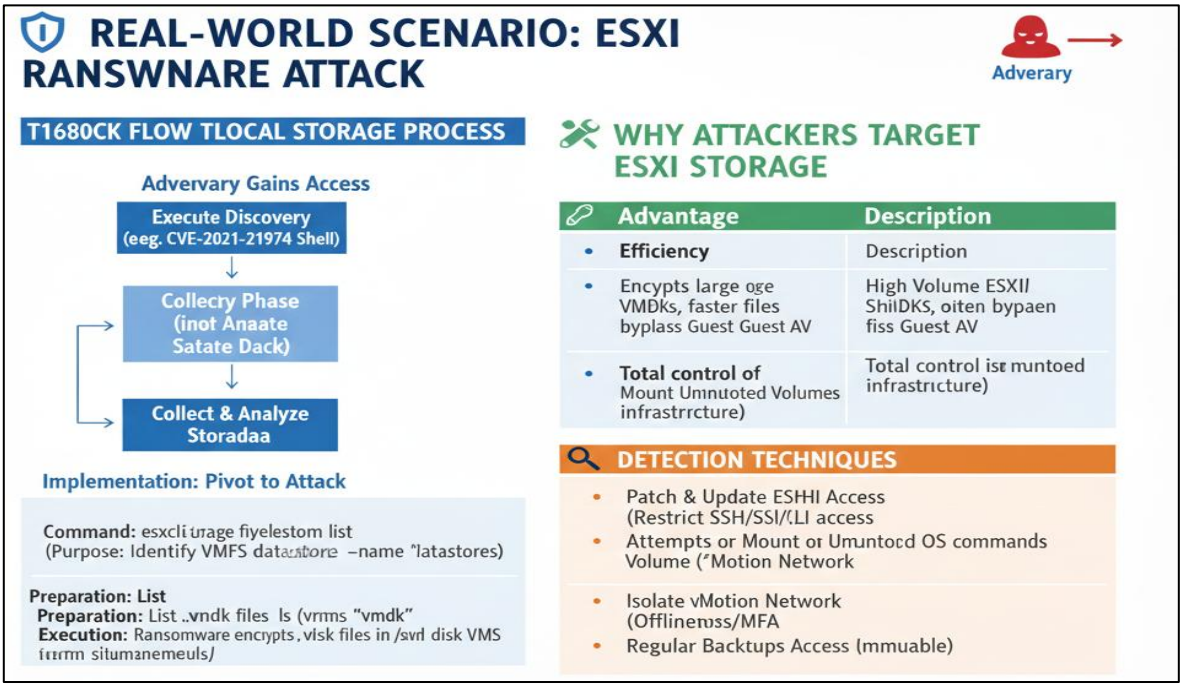


Technique 3: Local Storage Discovery (T1680)

Overview:

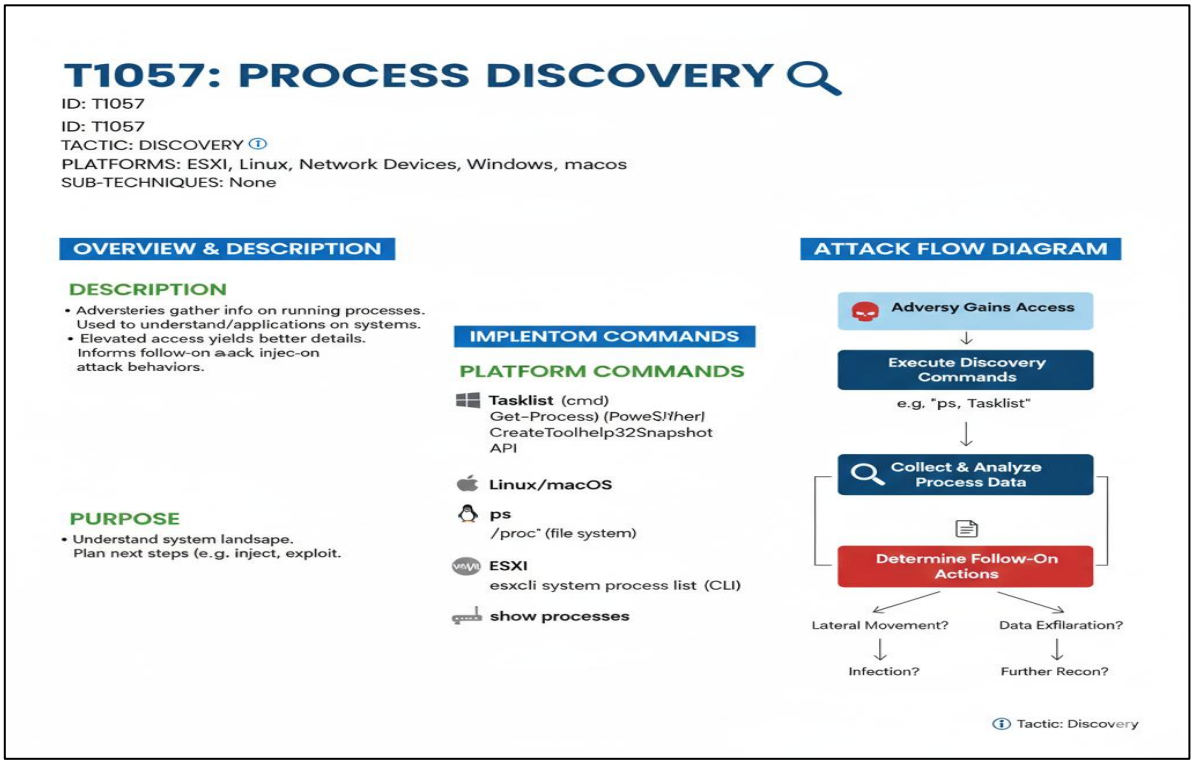


Real World Example:

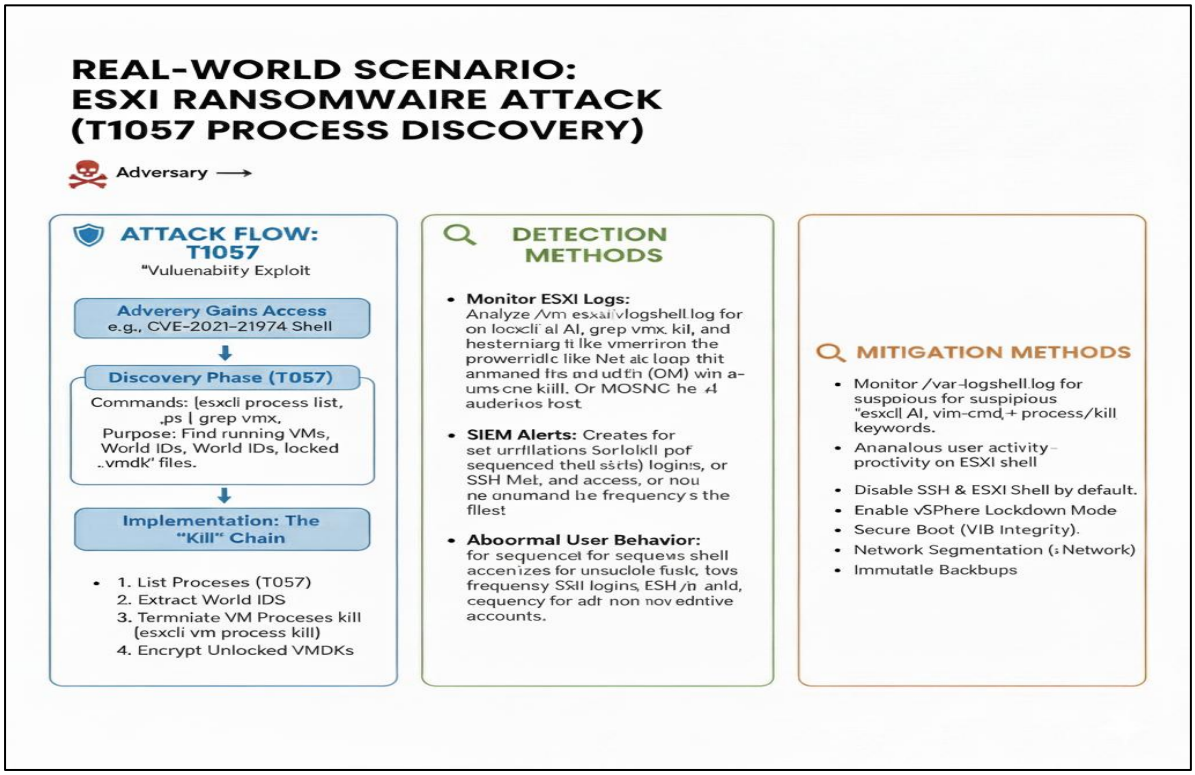


Technique 4 : Process Discovery (T1057)

Overview:

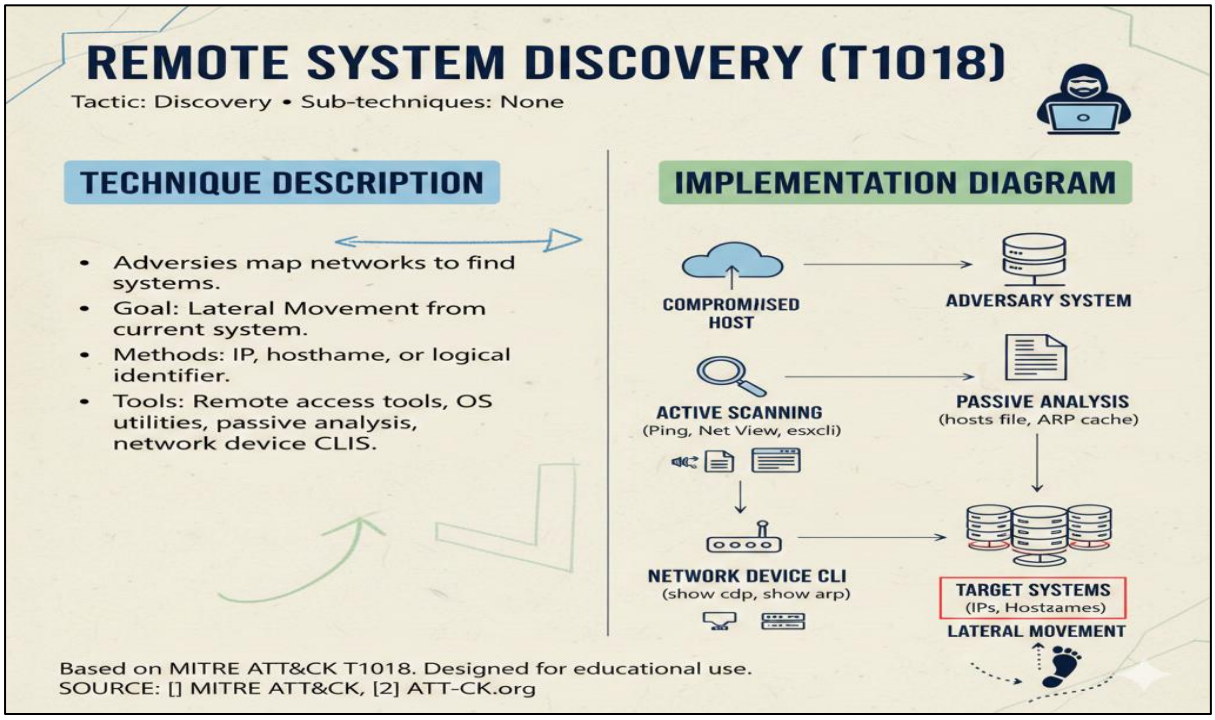


Real world Example :

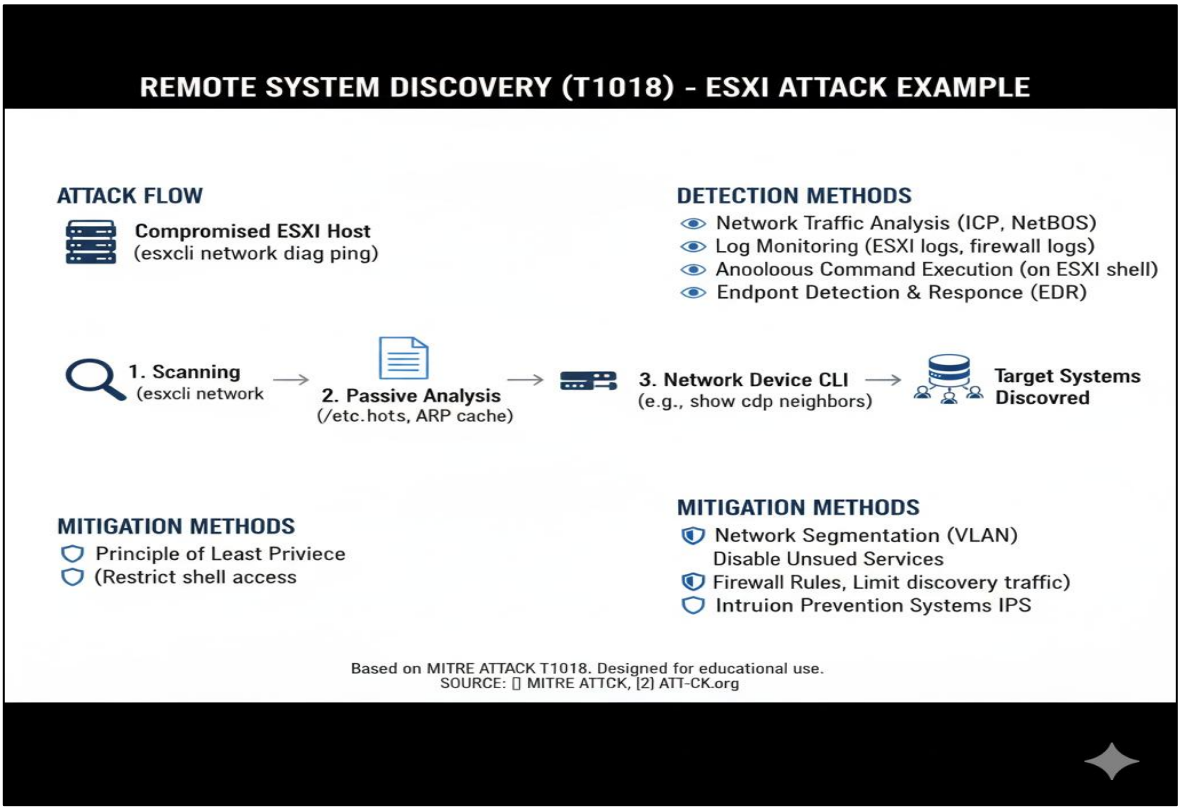


Technique 5 : Remote System Discovery (T1018)

Overview:

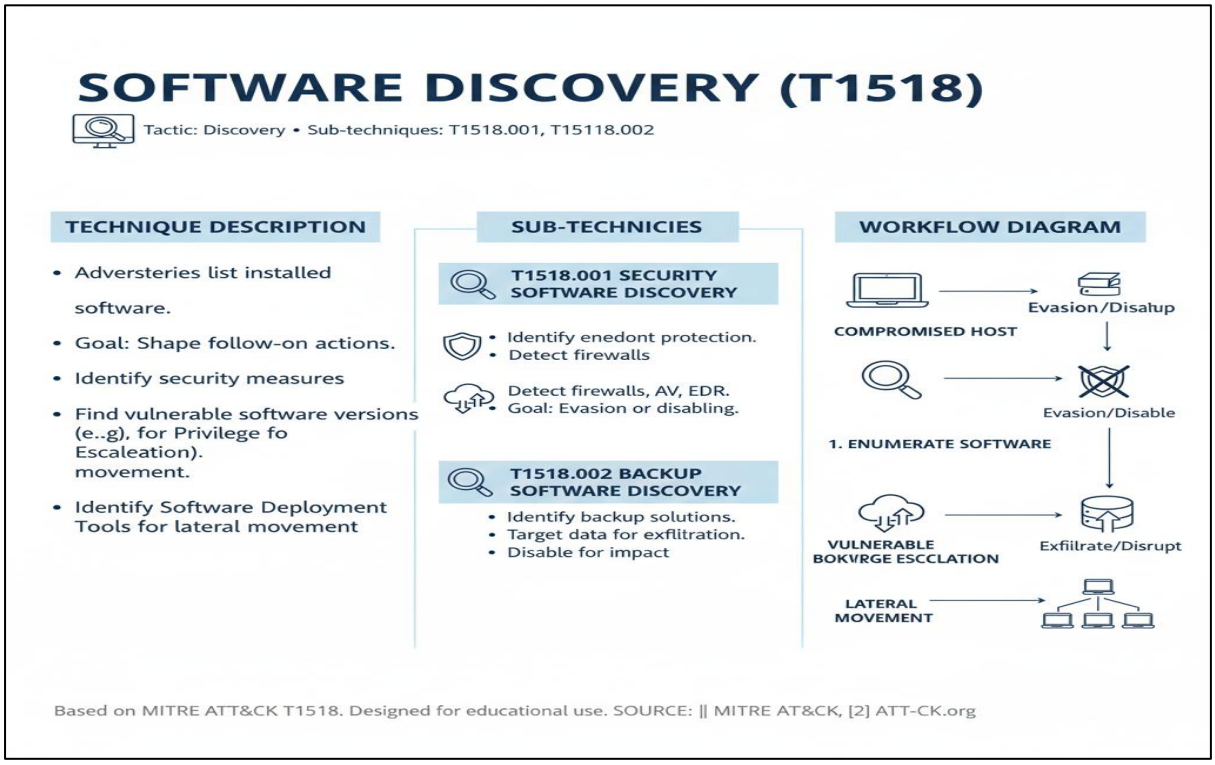


Real World Example:

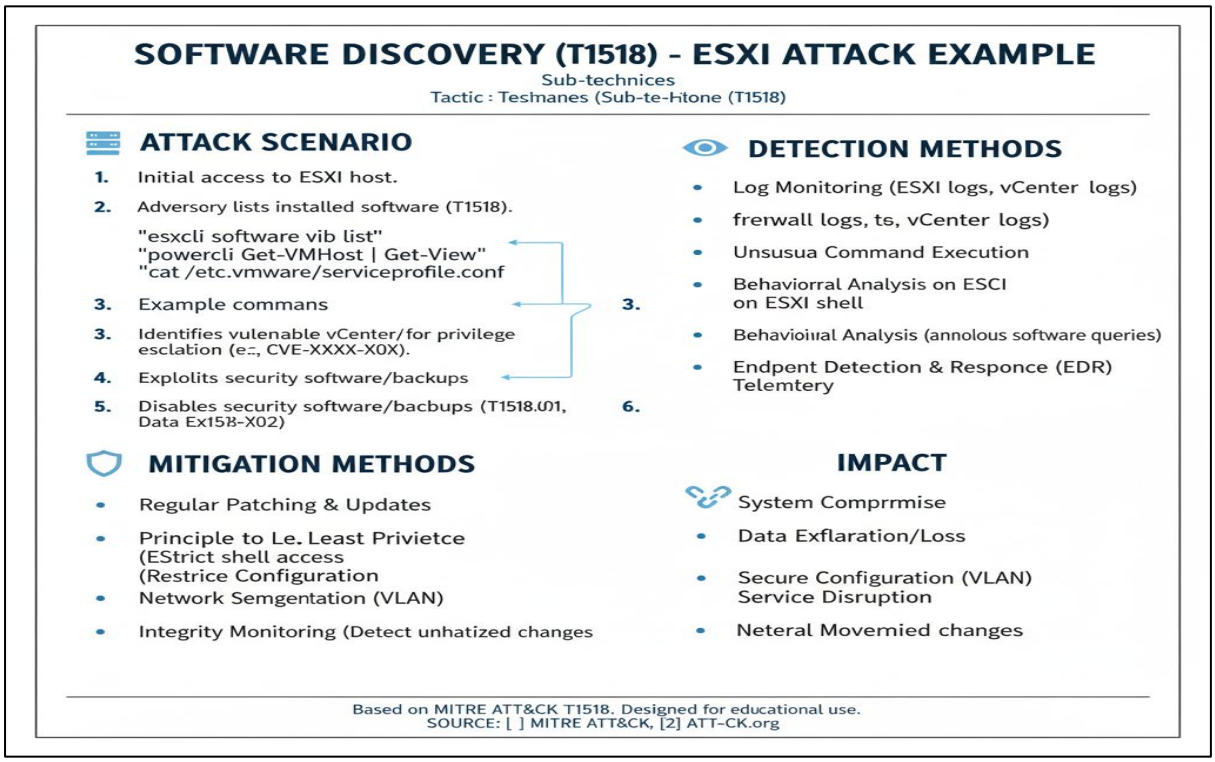


Technique 6: Software Discovery (T1518)

Overview :

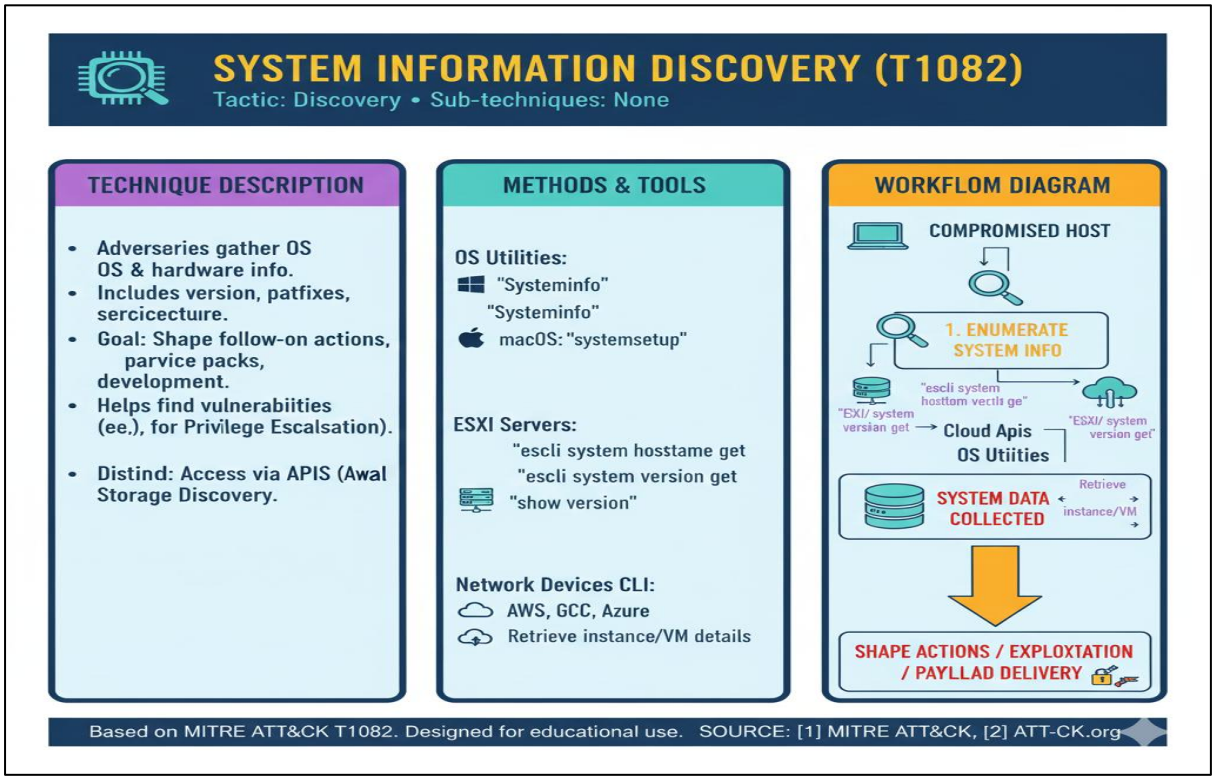


Real World Example :

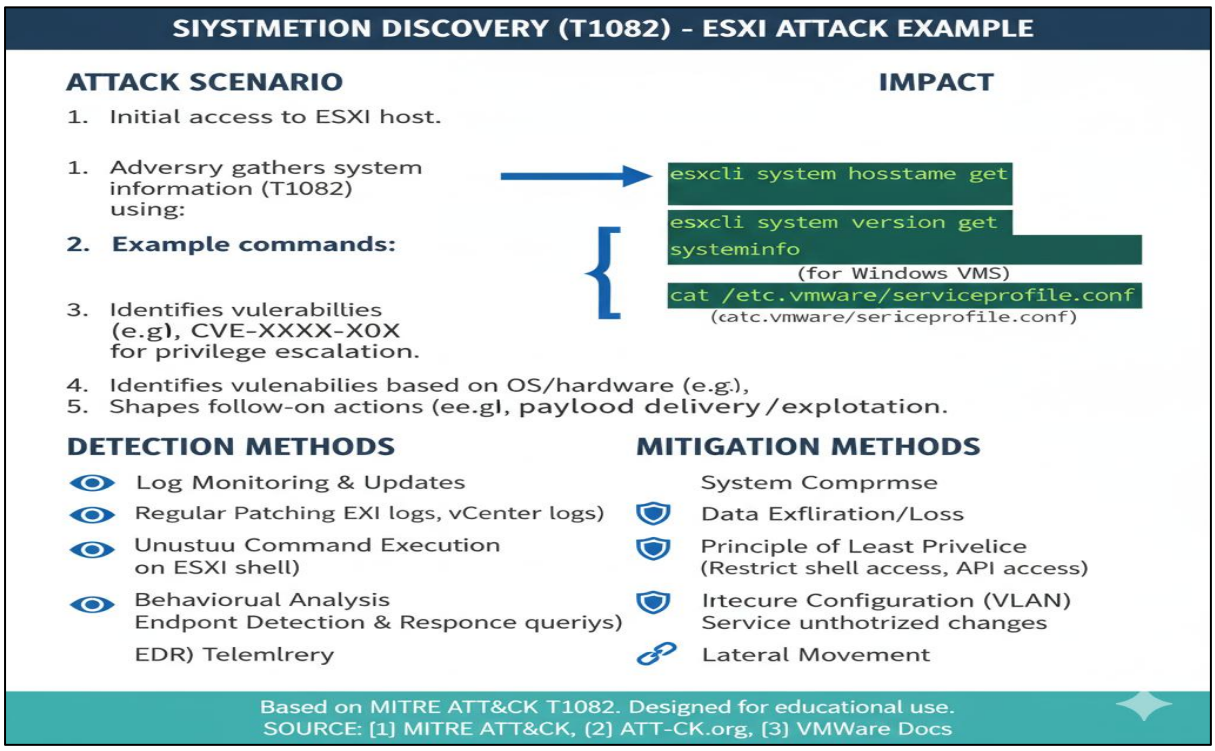


Technique 7: System Information Discovery (T1082)

Overview:

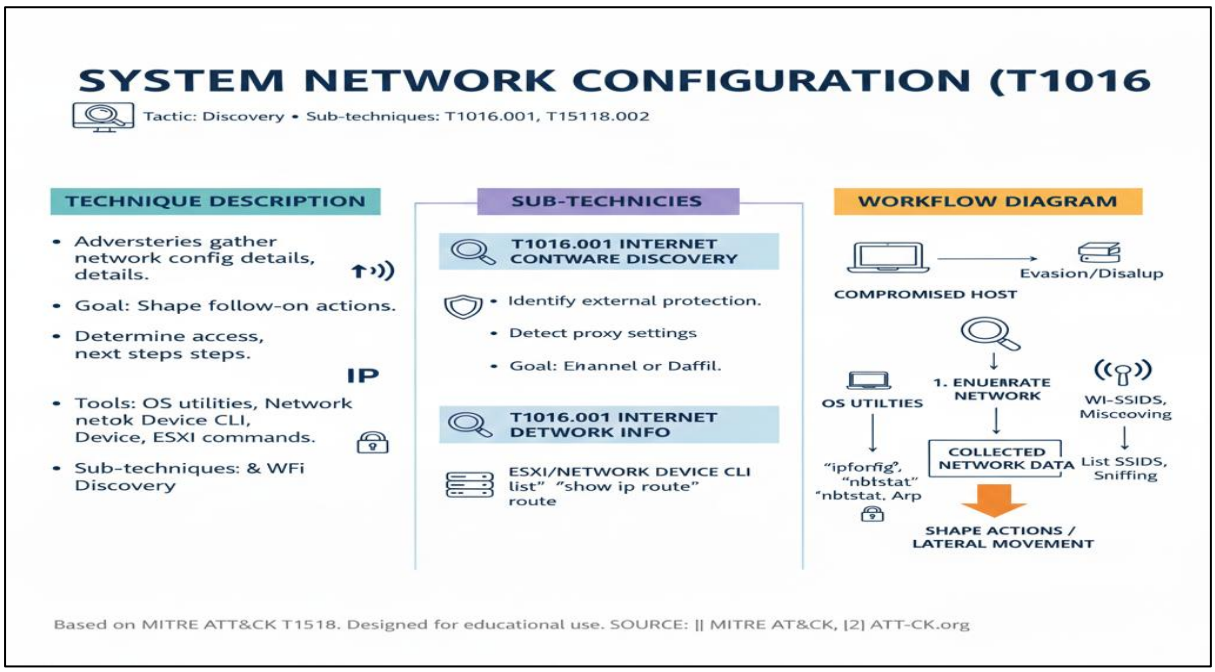


Real World Example:

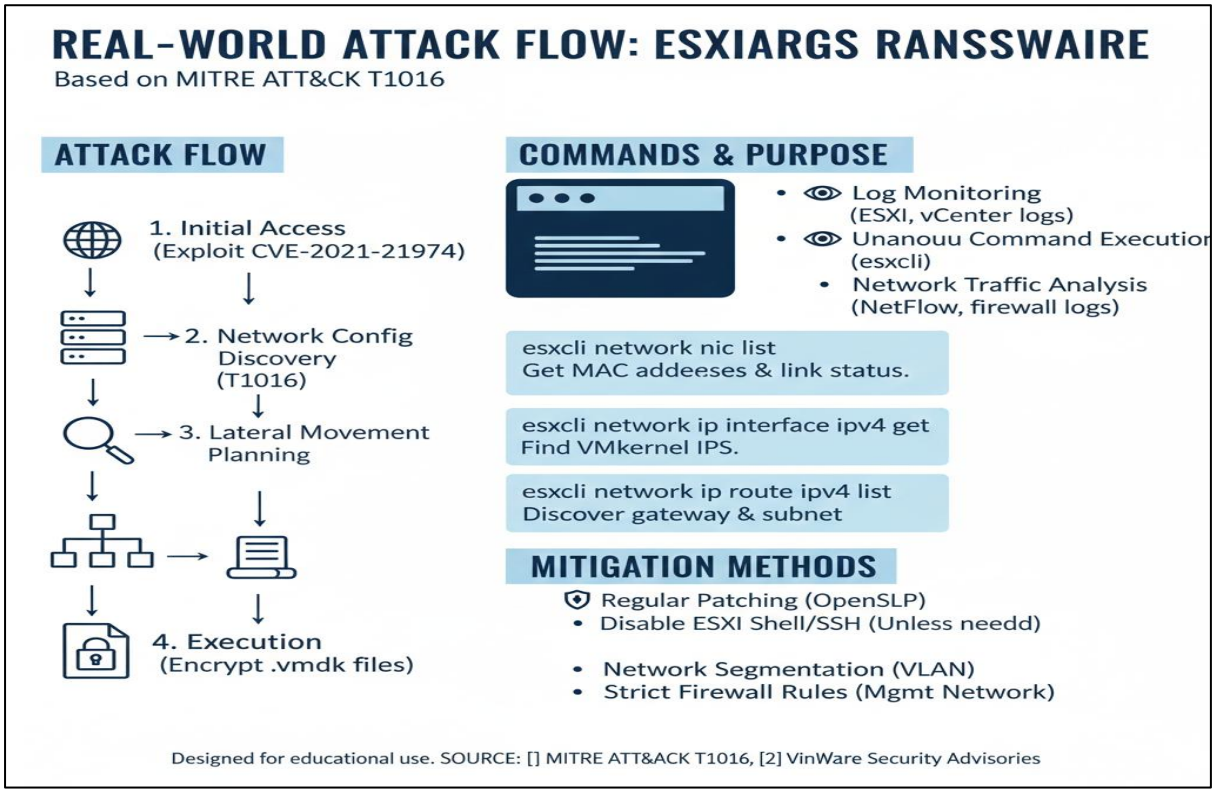


Technique 8 : System Network Configuration Discovery (T1016)

Overview:

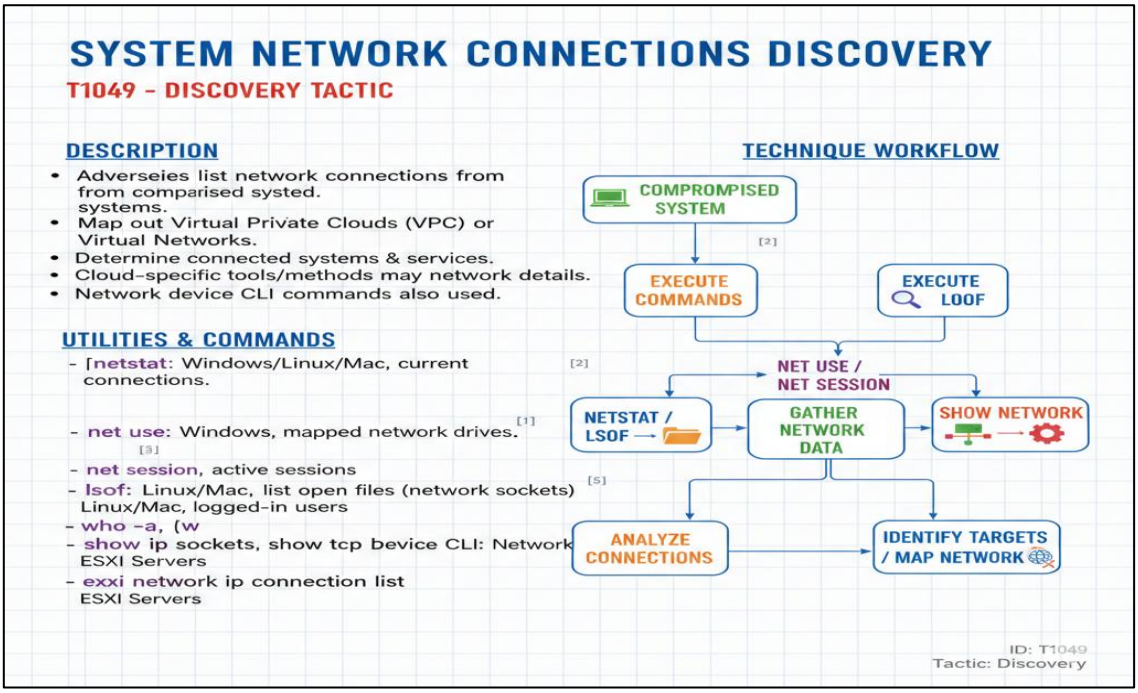


Real World Example:

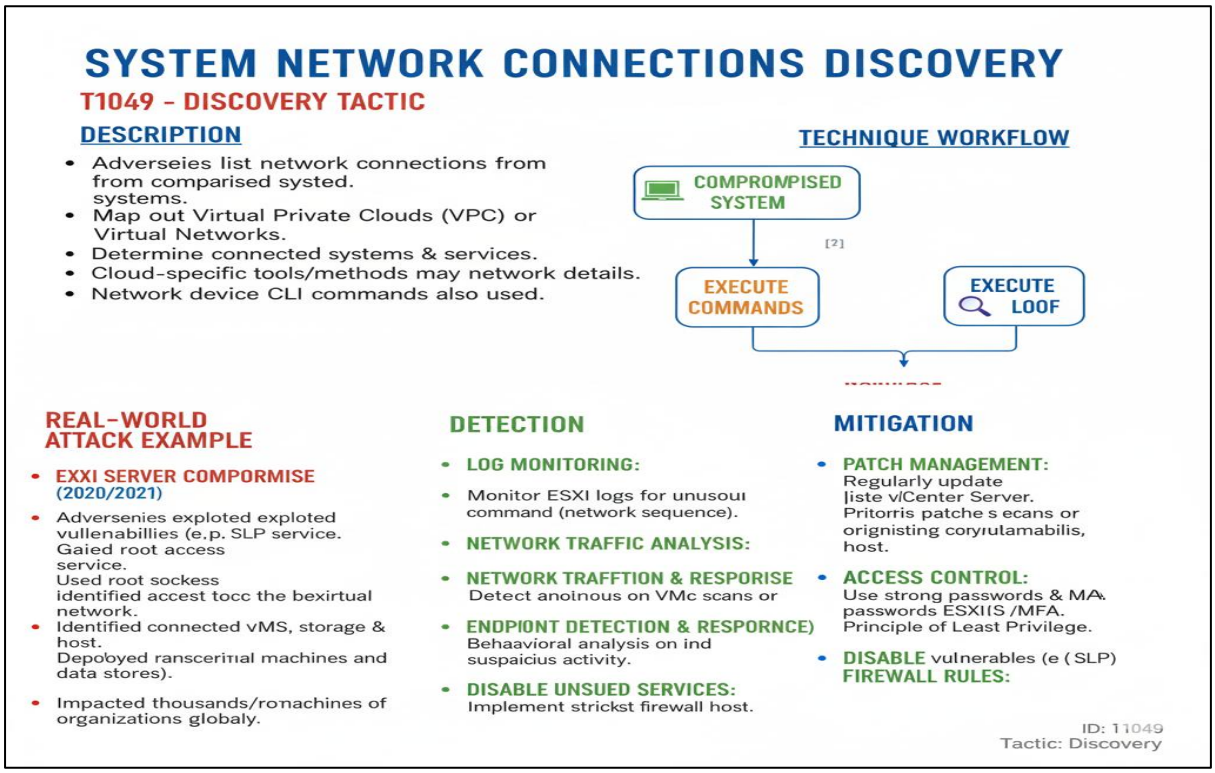


Technique 9 : System Network Connections Discovery (T1049)

Overview:

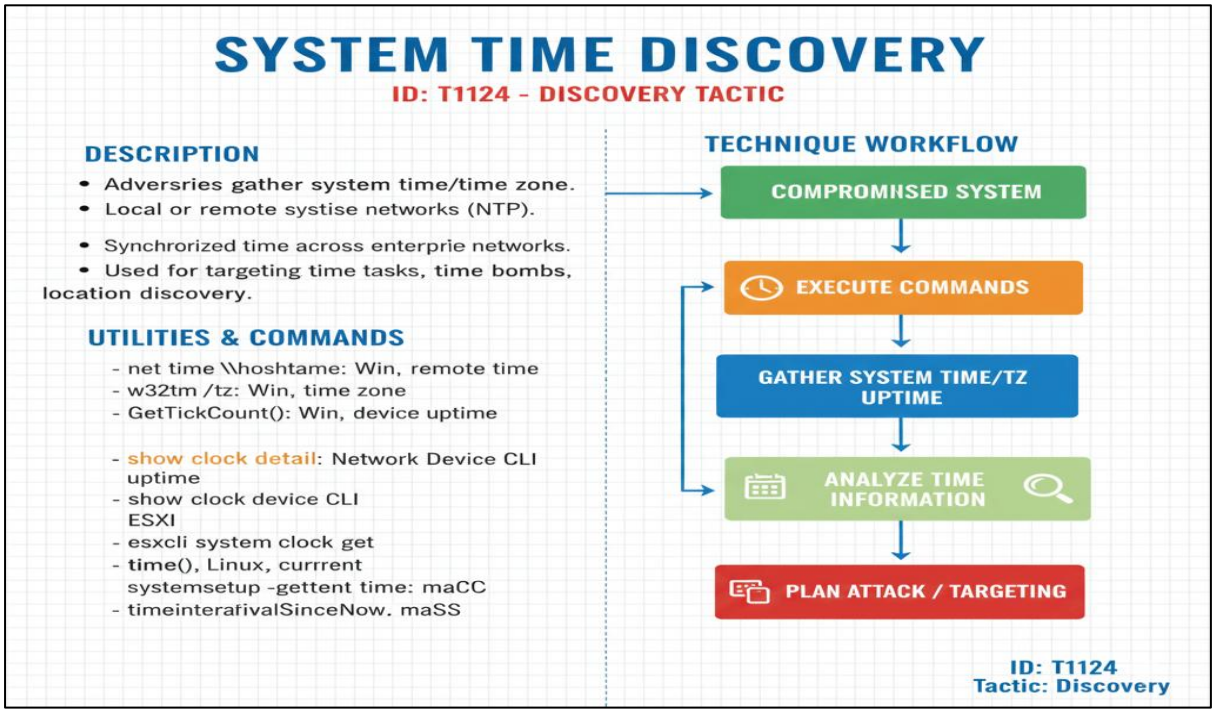


Real World Example:

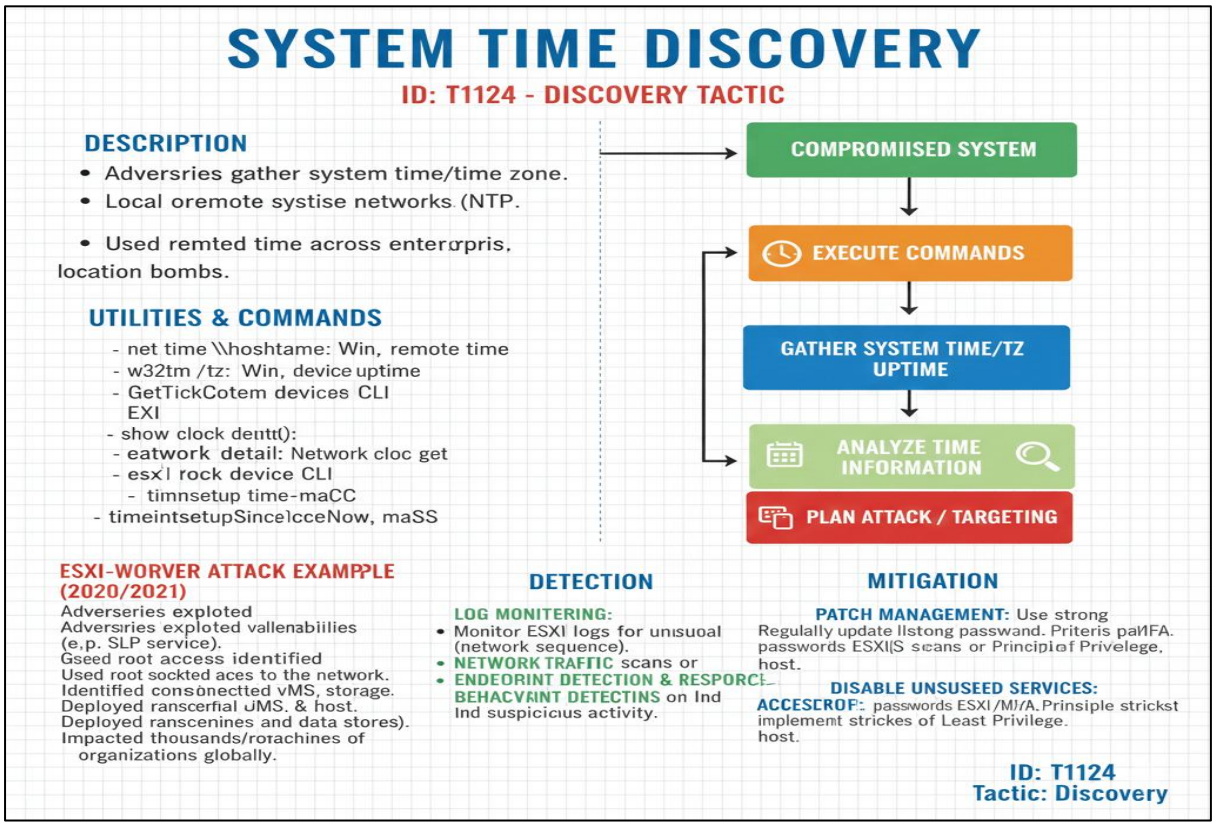


Technique 10 : System Time Discovery (T1124)

Overview:

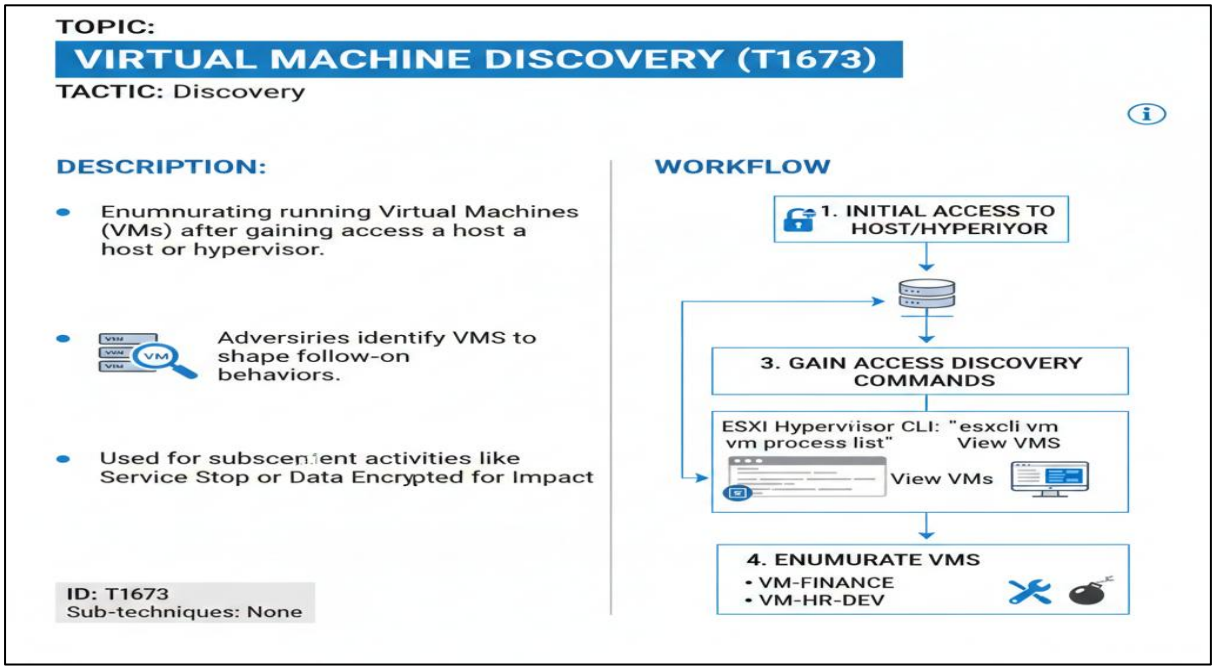


Real World Example:

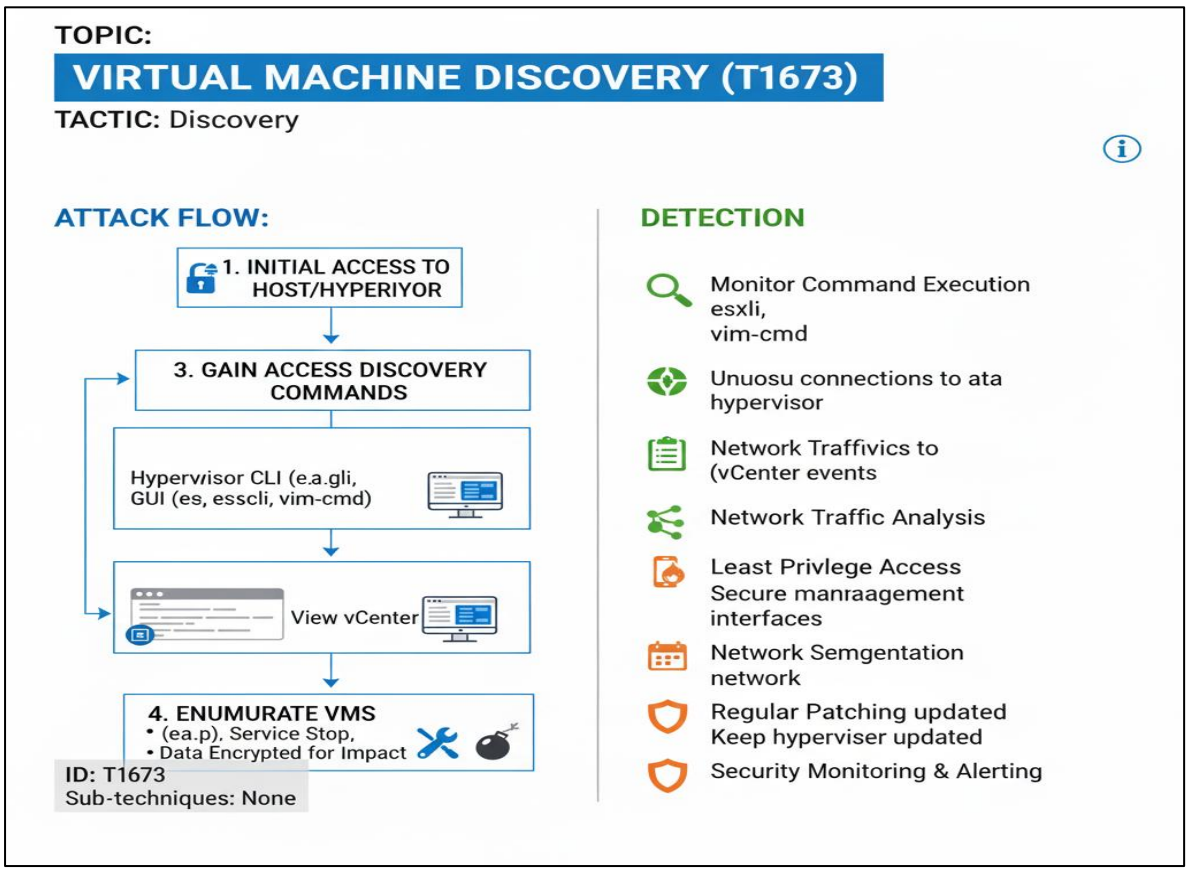


Technique 11: Virtual Machine Discovery (T1673)

Overview:

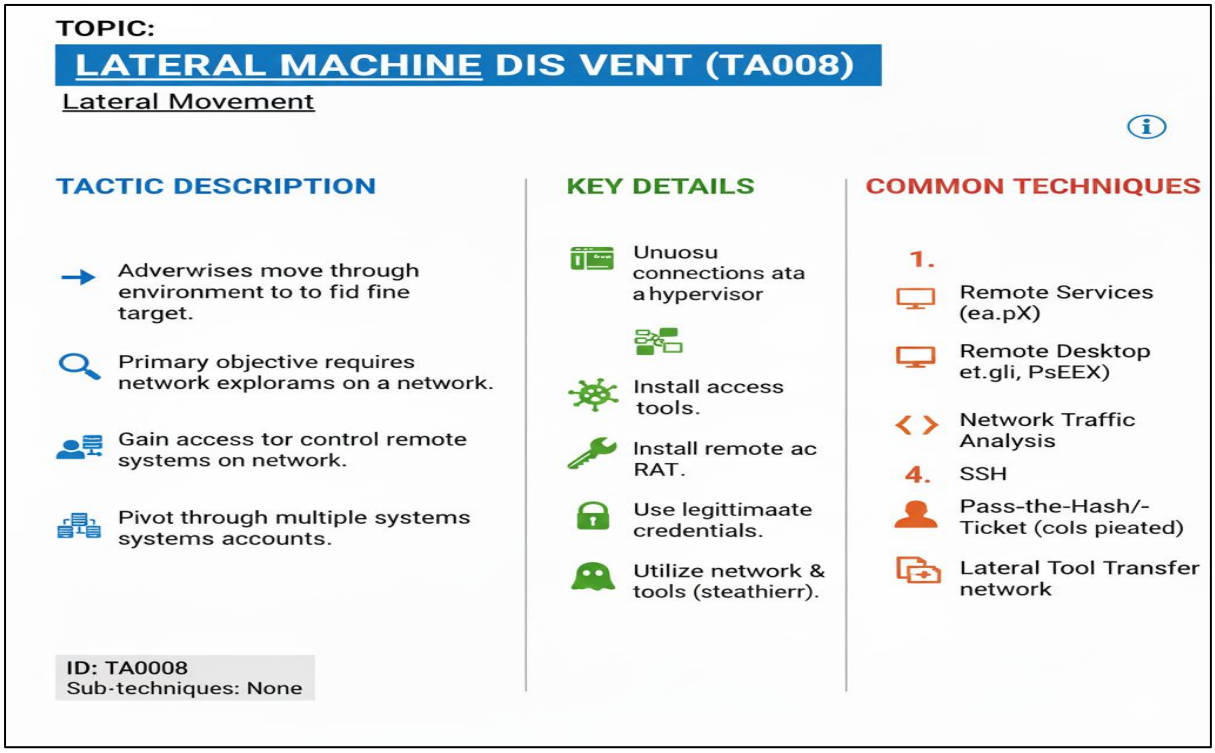


Real World Example:

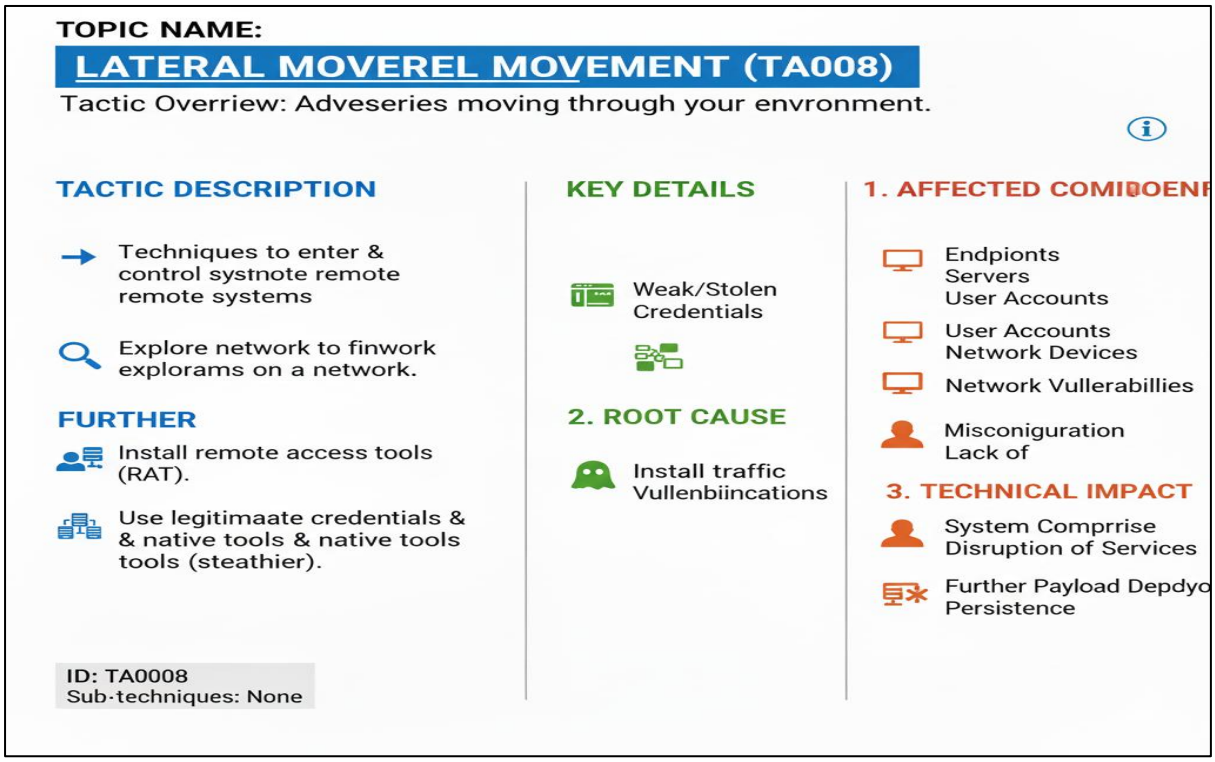


8. Lateral Movement (TA0008)

Overview:

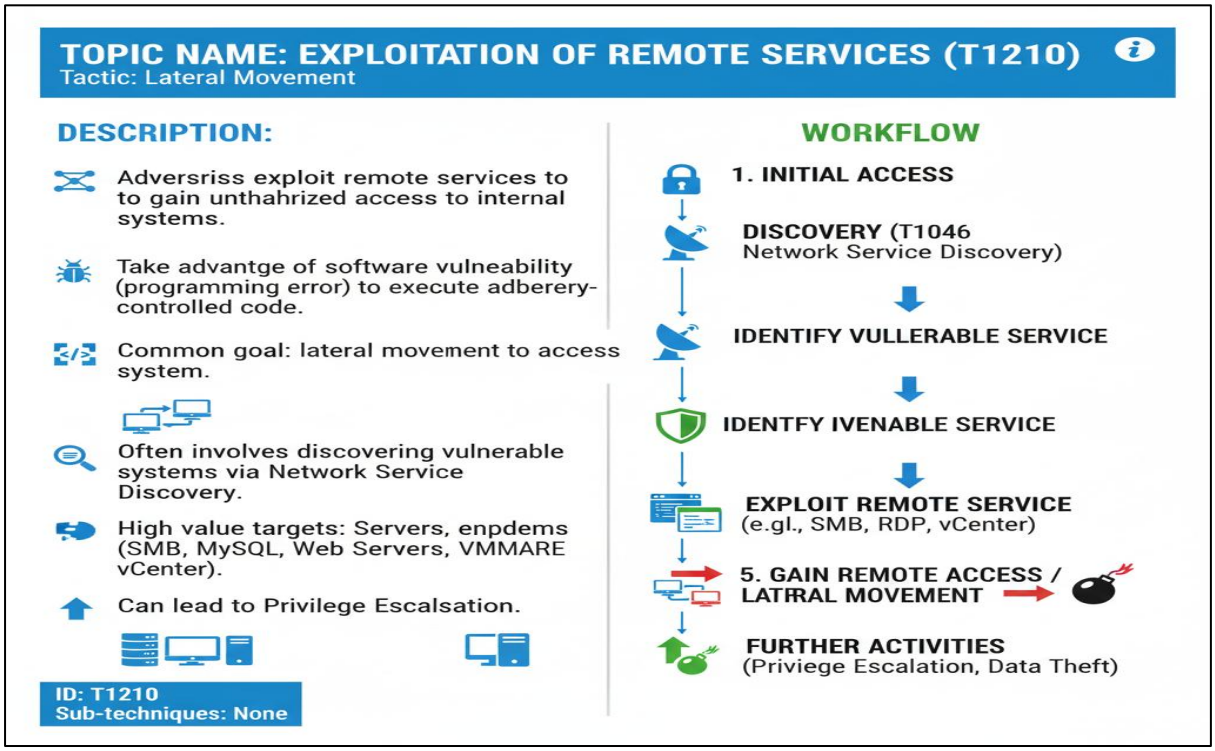


Technical Detail:

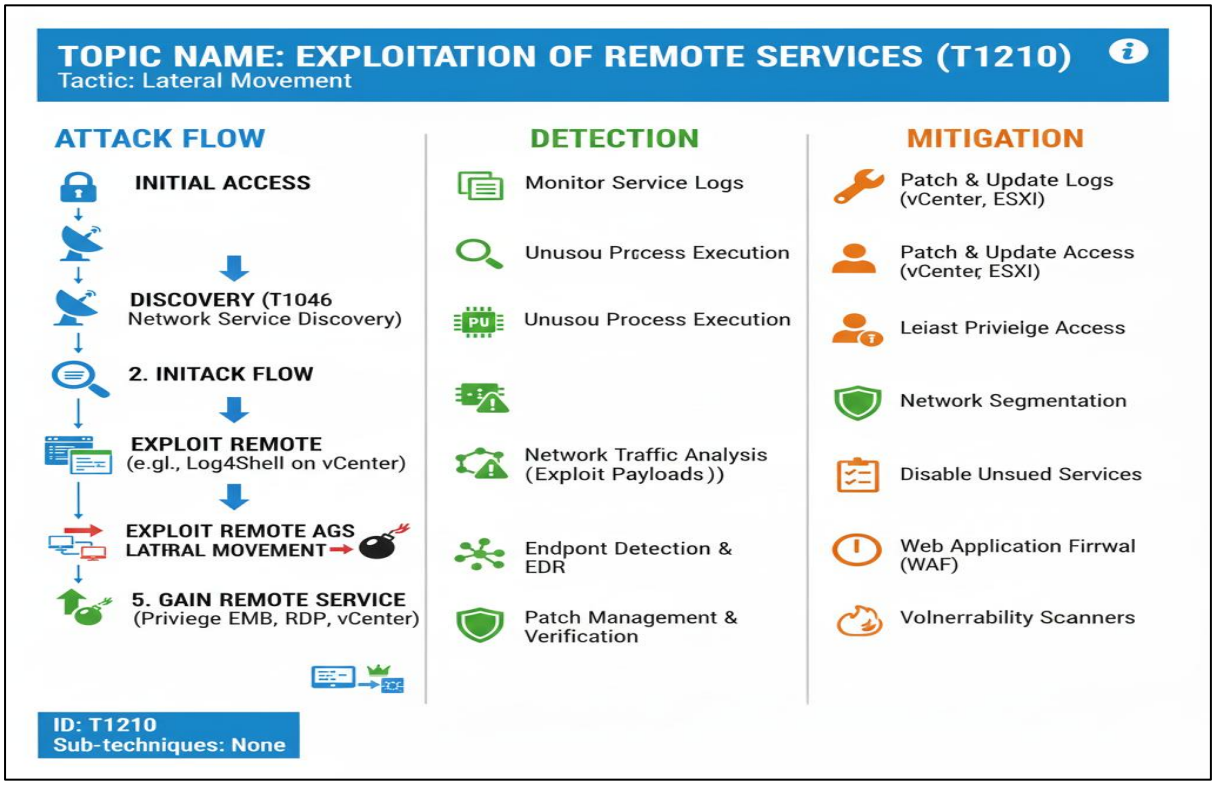


Technique 1: Exploitation of Remote Services (T1210)

Overview:

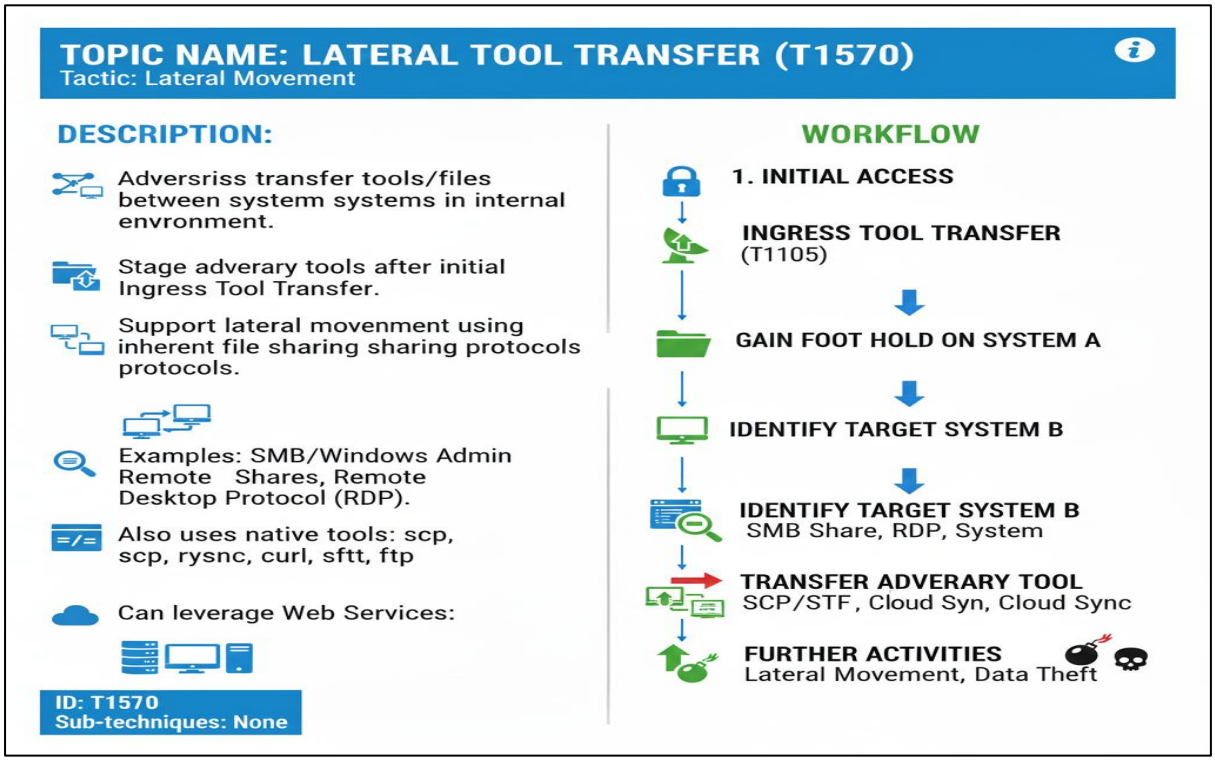


Real World Example :

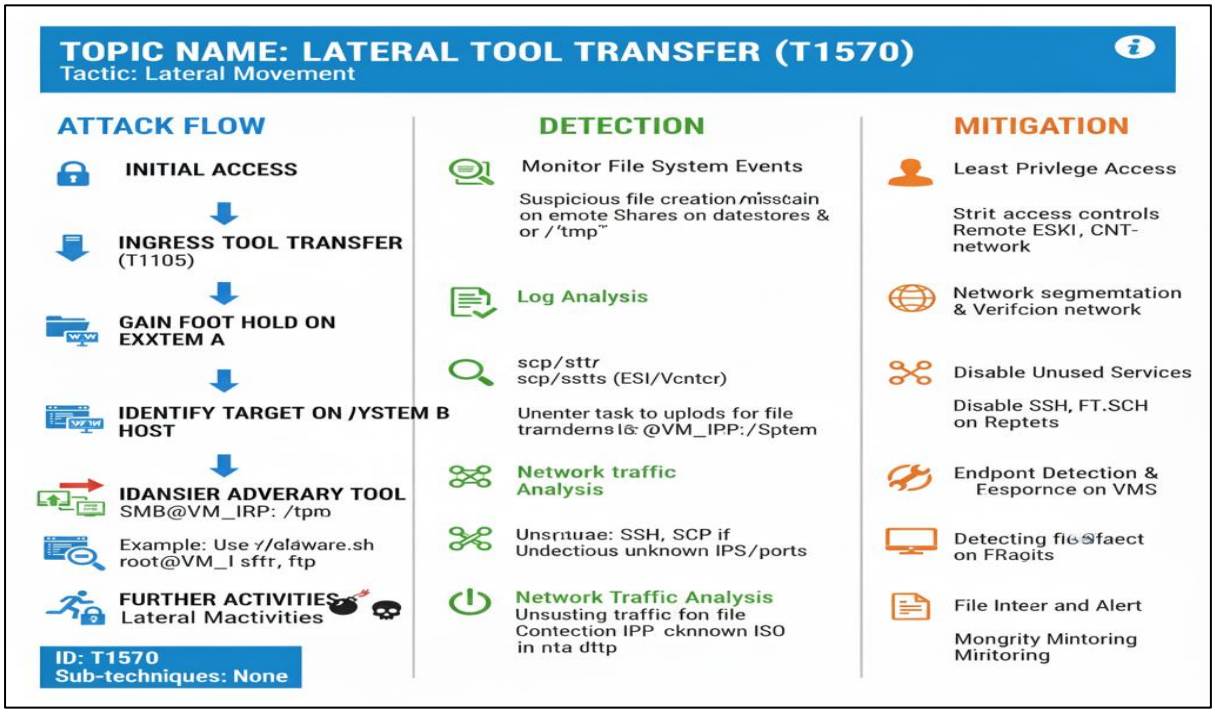


Technique 2 : Lateral Tool Transfer (T1570)

Overview:

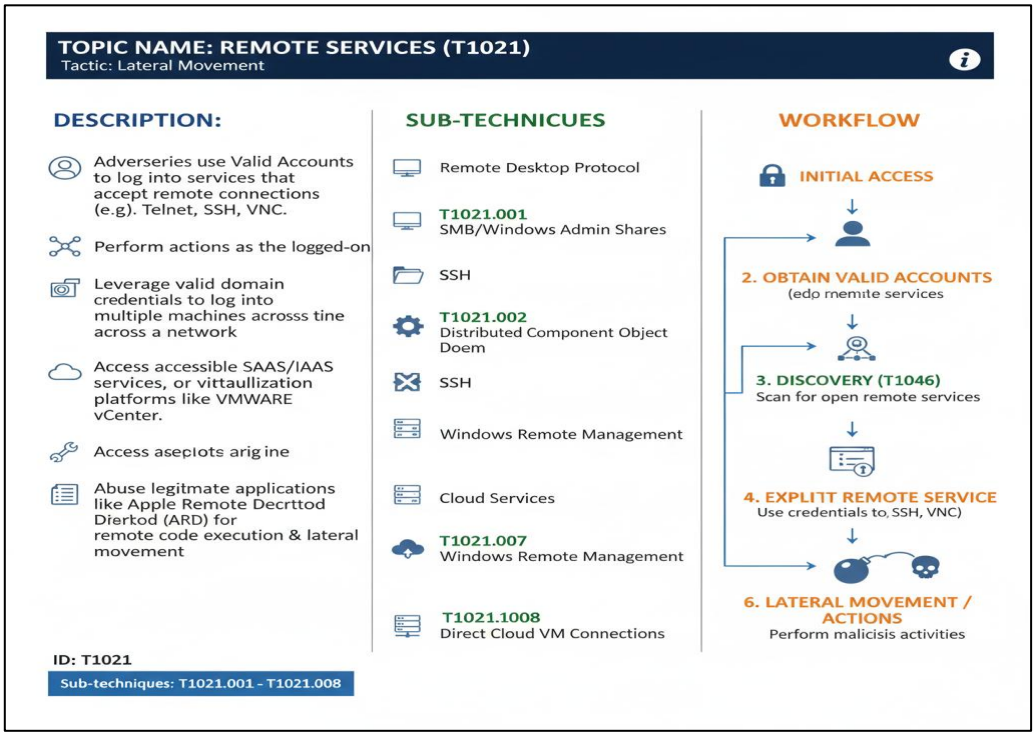


Real World Example:

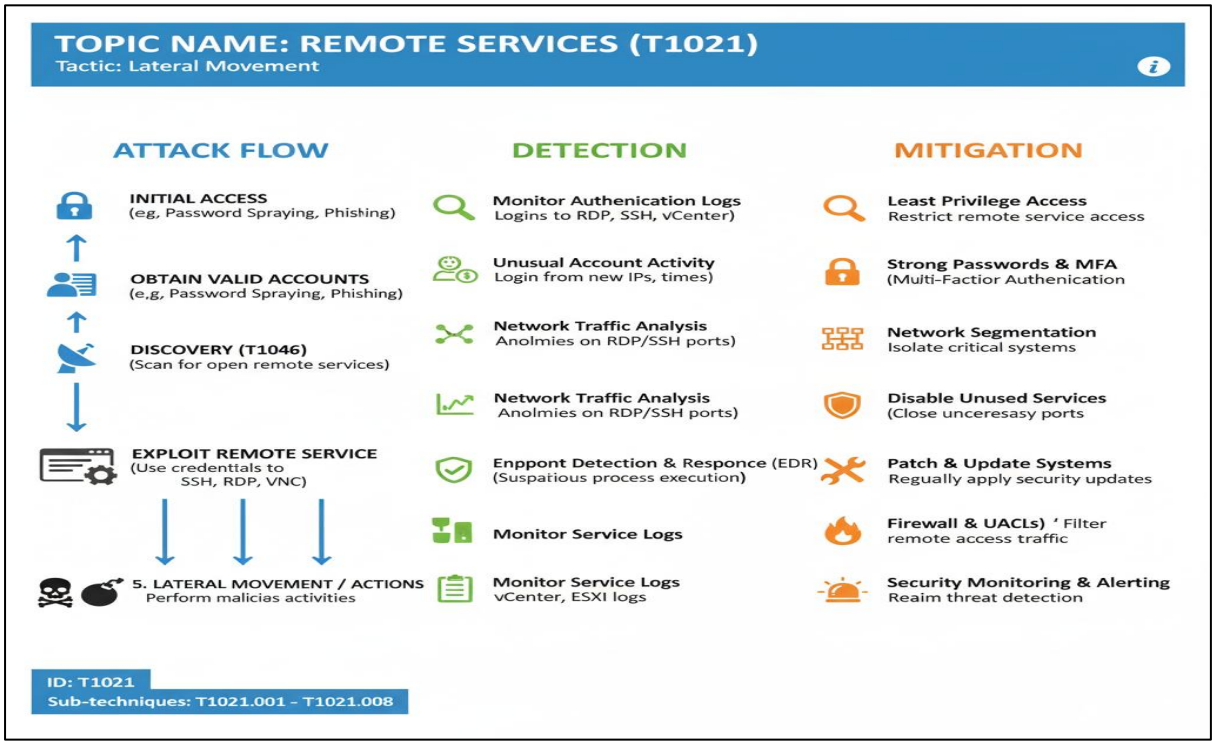


Technique 3: Remote Services (T1021)

Overview:

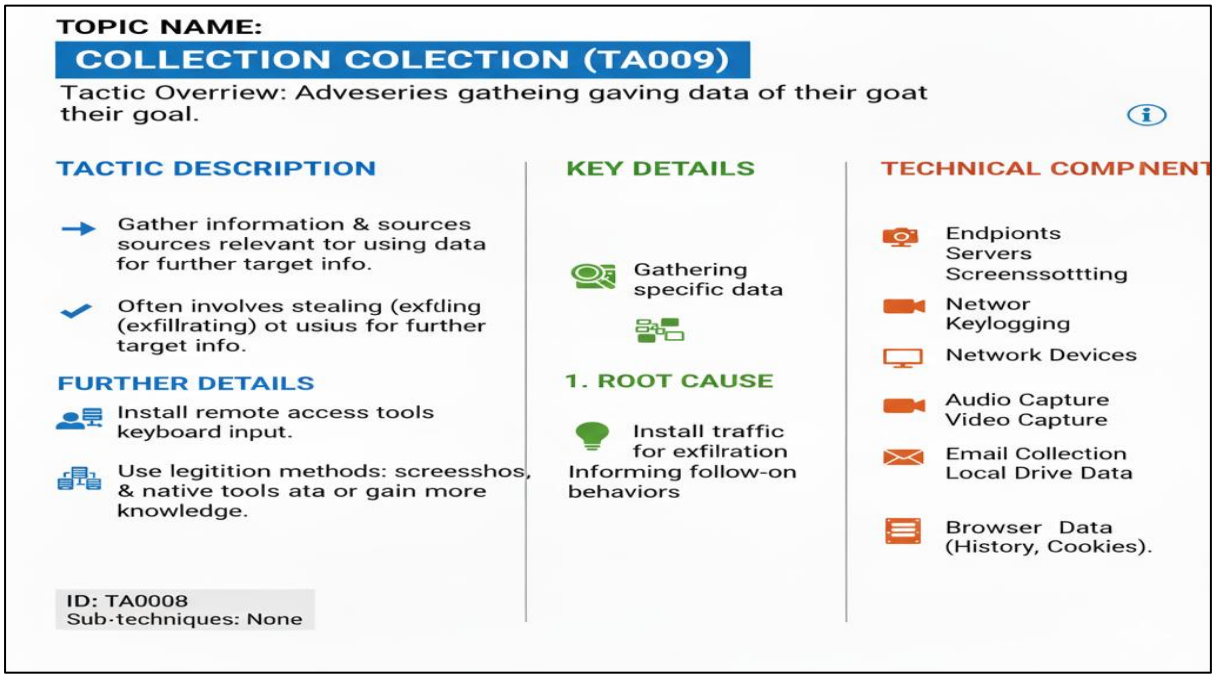


Real World Example:

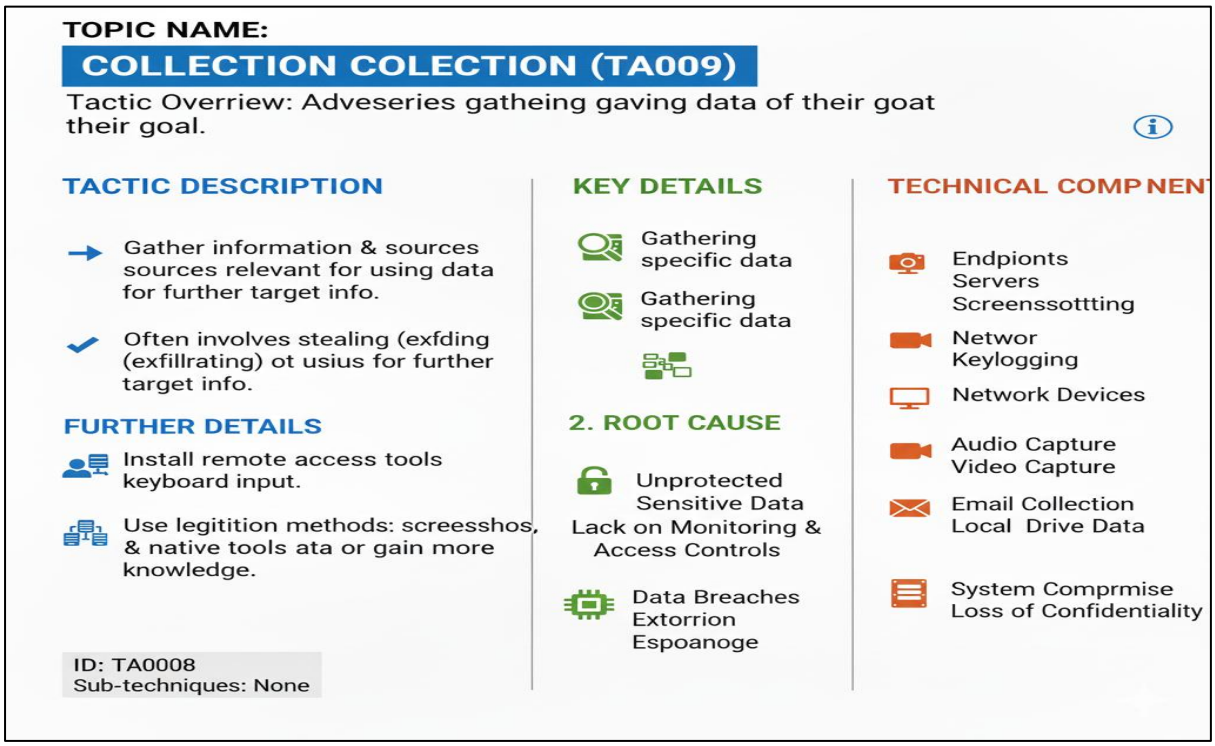


9. Collection (TA0009)

Overview:

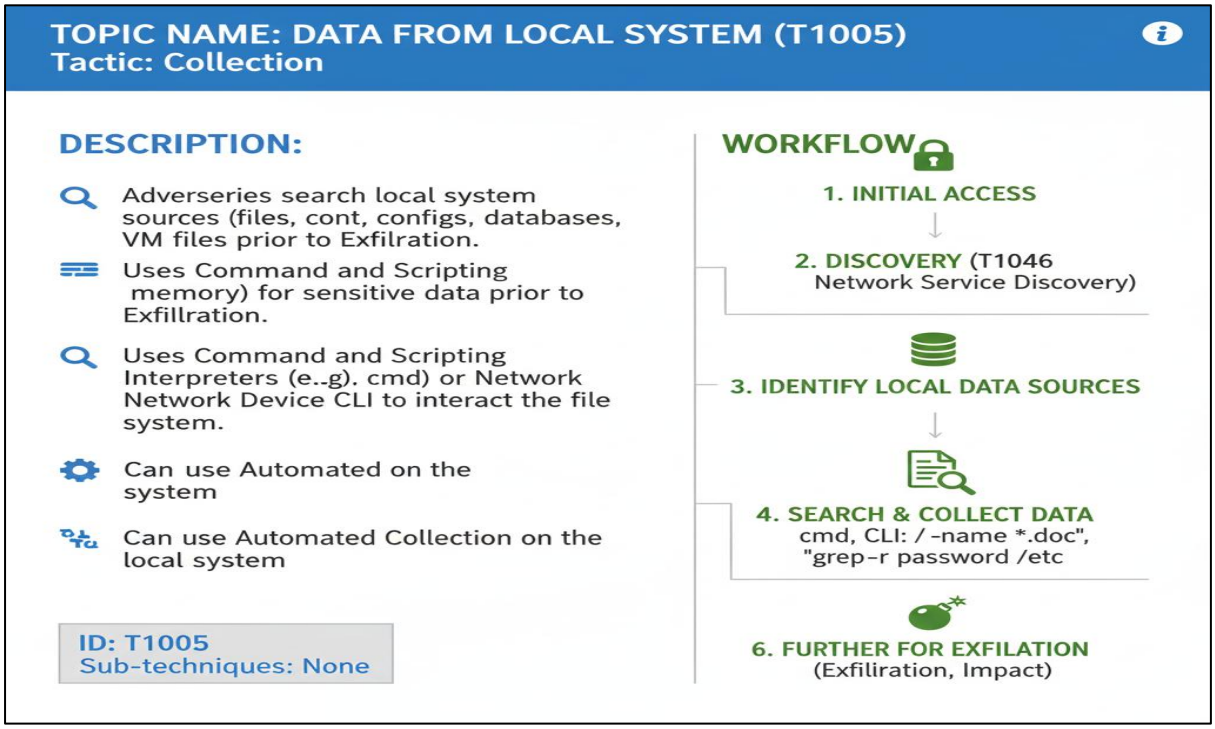


Technical Detail:

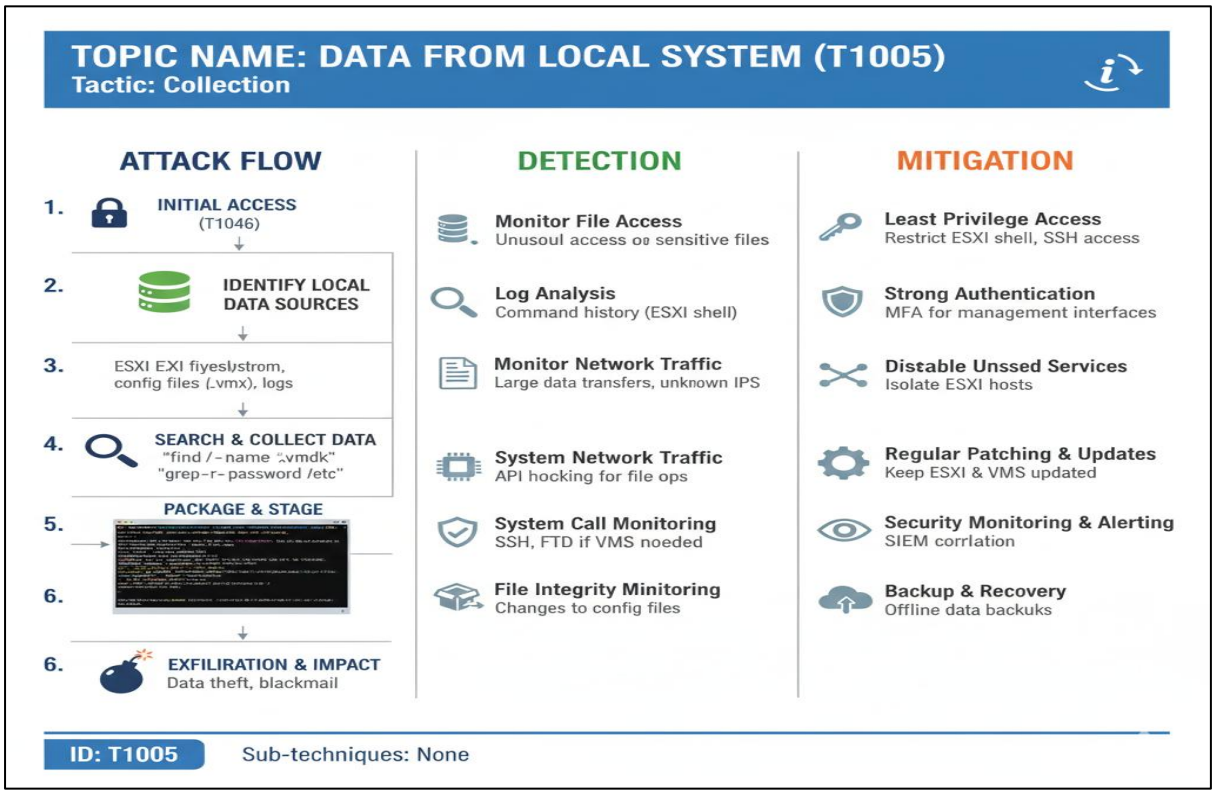


Technique 1: Data from Local System (T1005)

Overview:

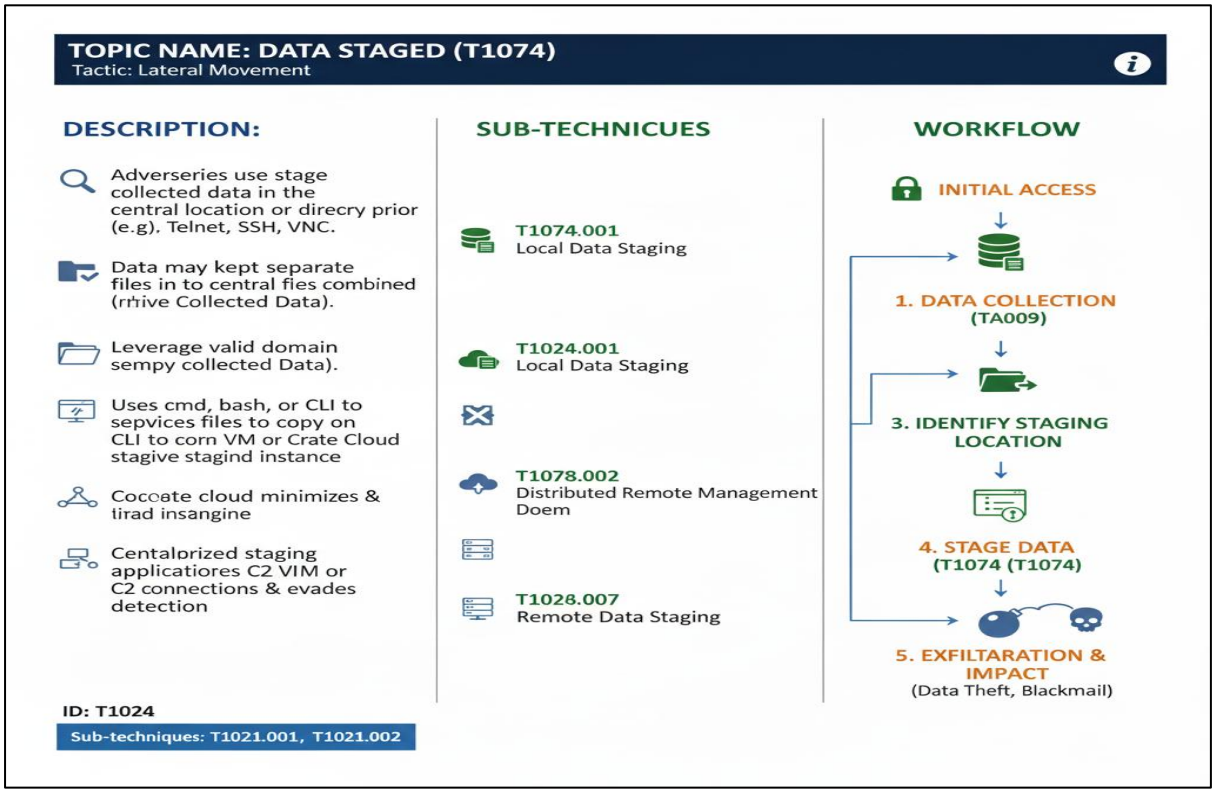


Real World Example:

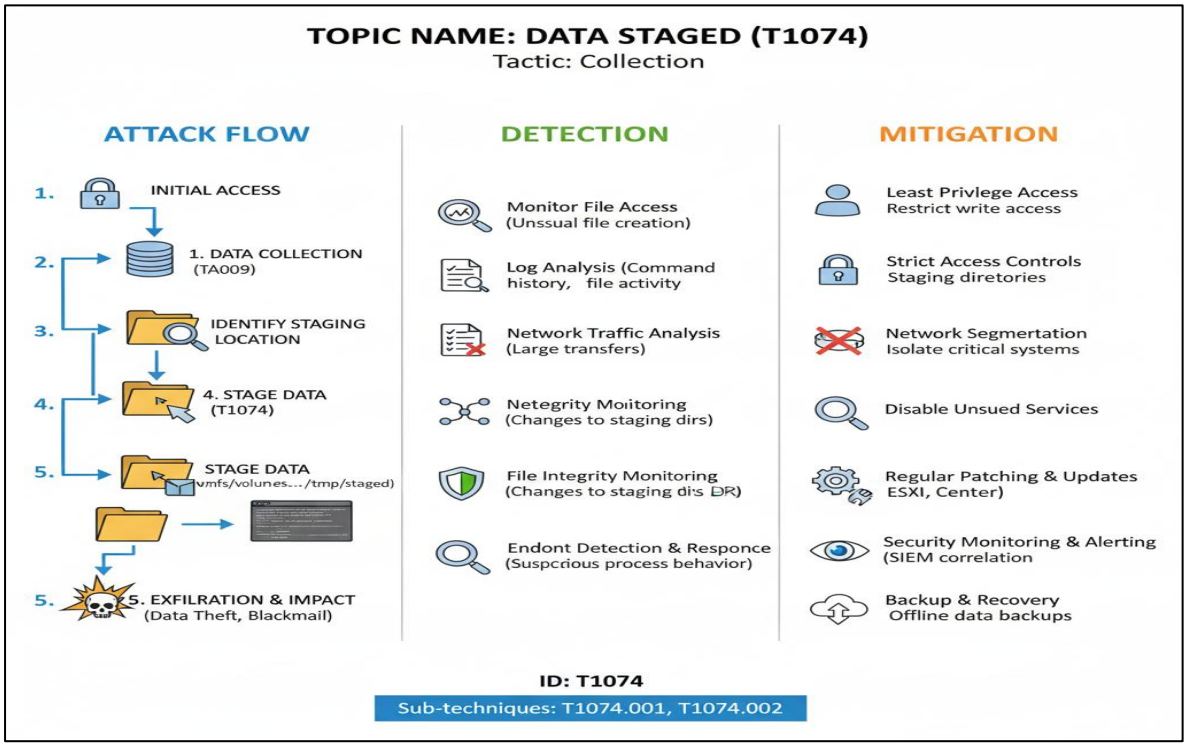


Technique 2: Data Staged (T1074)

Overview:

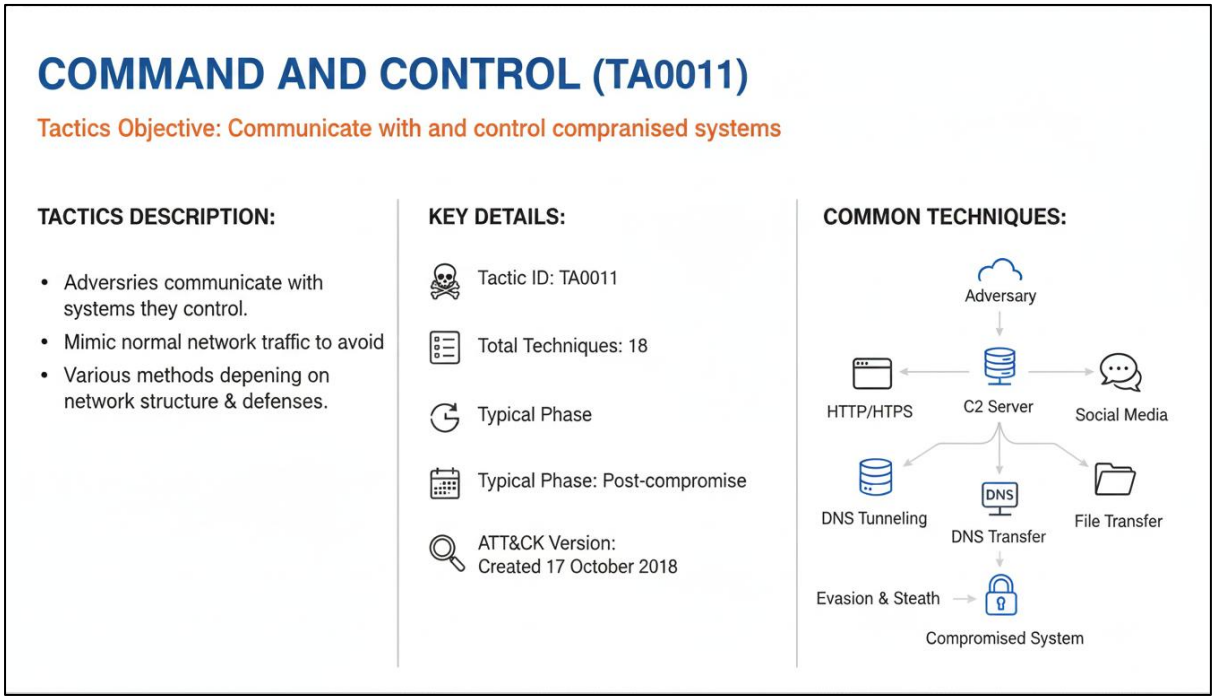


Real World Example:

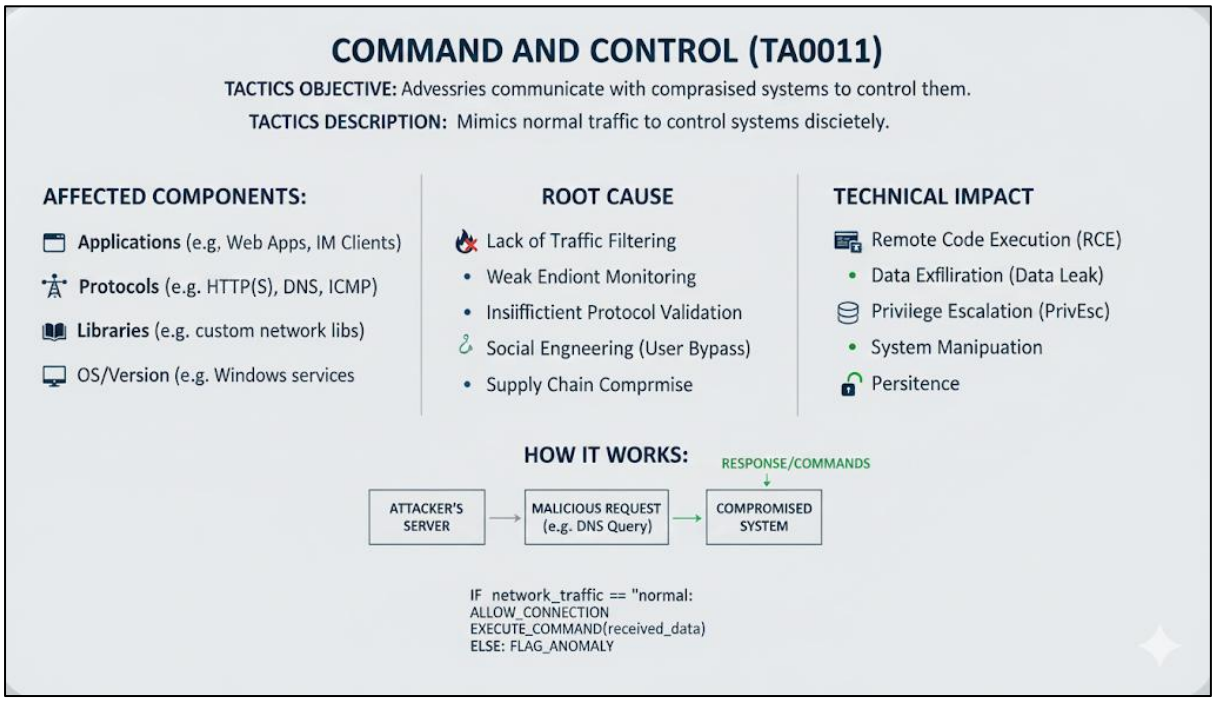


10. Command and Control (TA0011)

Overview:

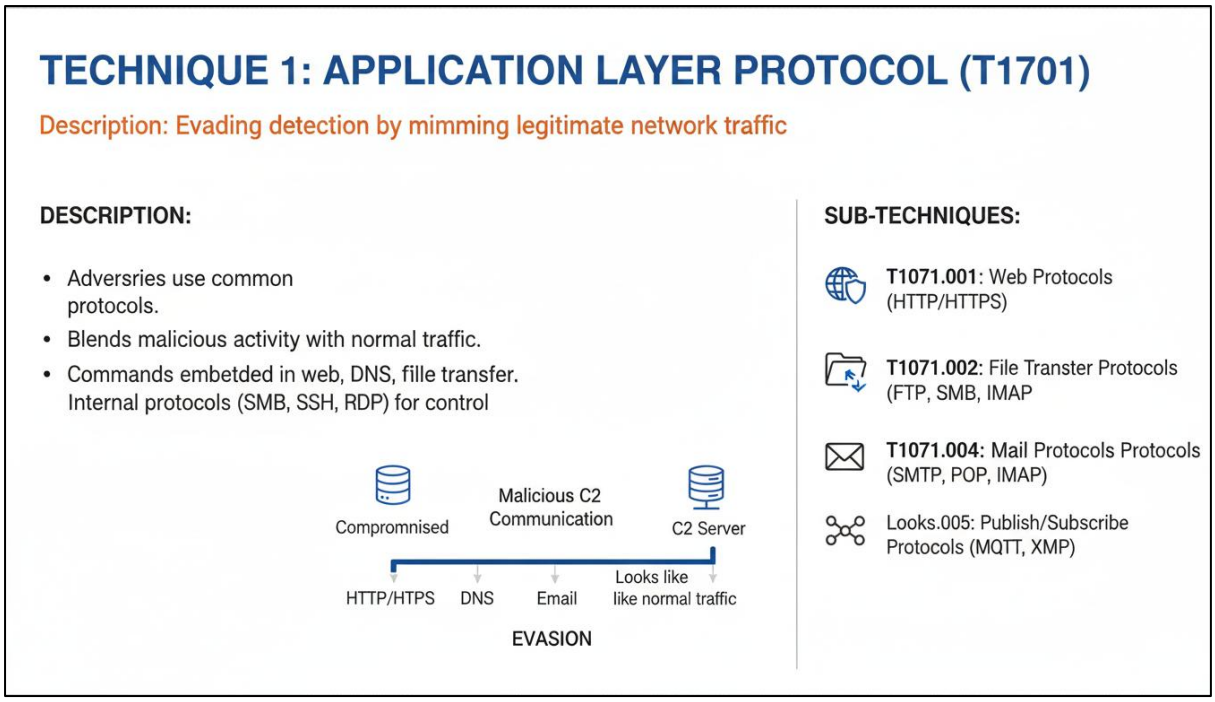


Technical Detail:

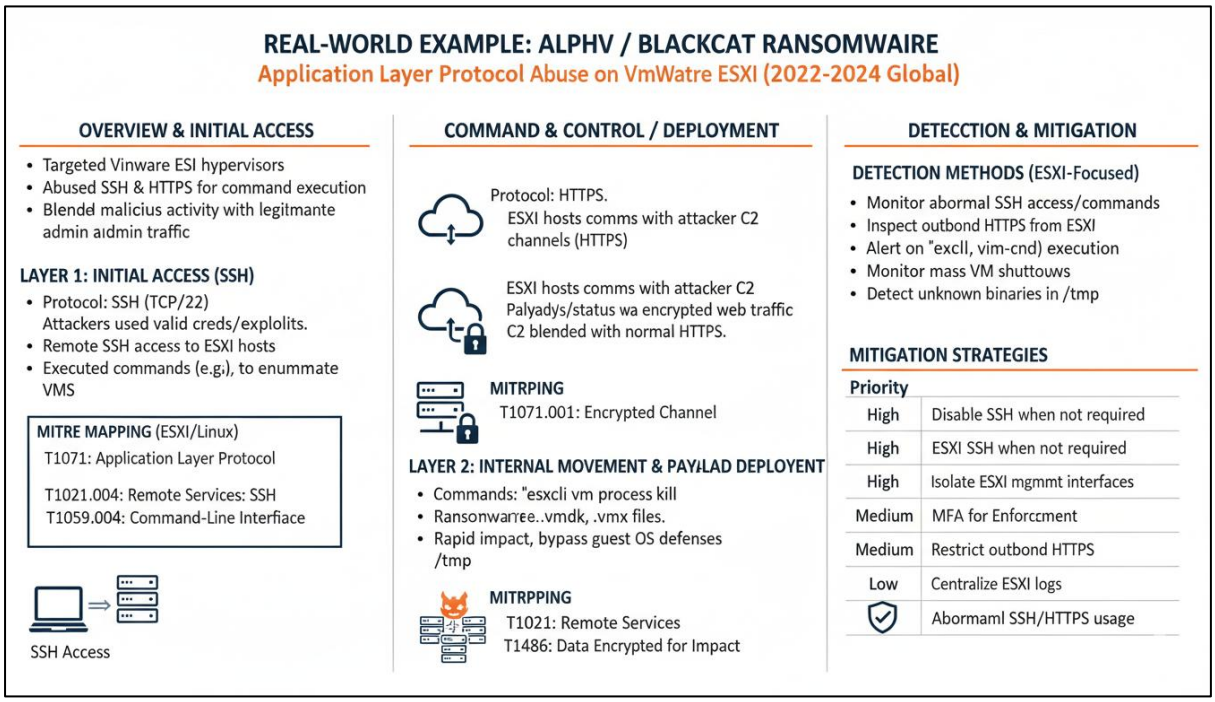


Techniques 1: Application Layer Protocol (T1701)

Overview:

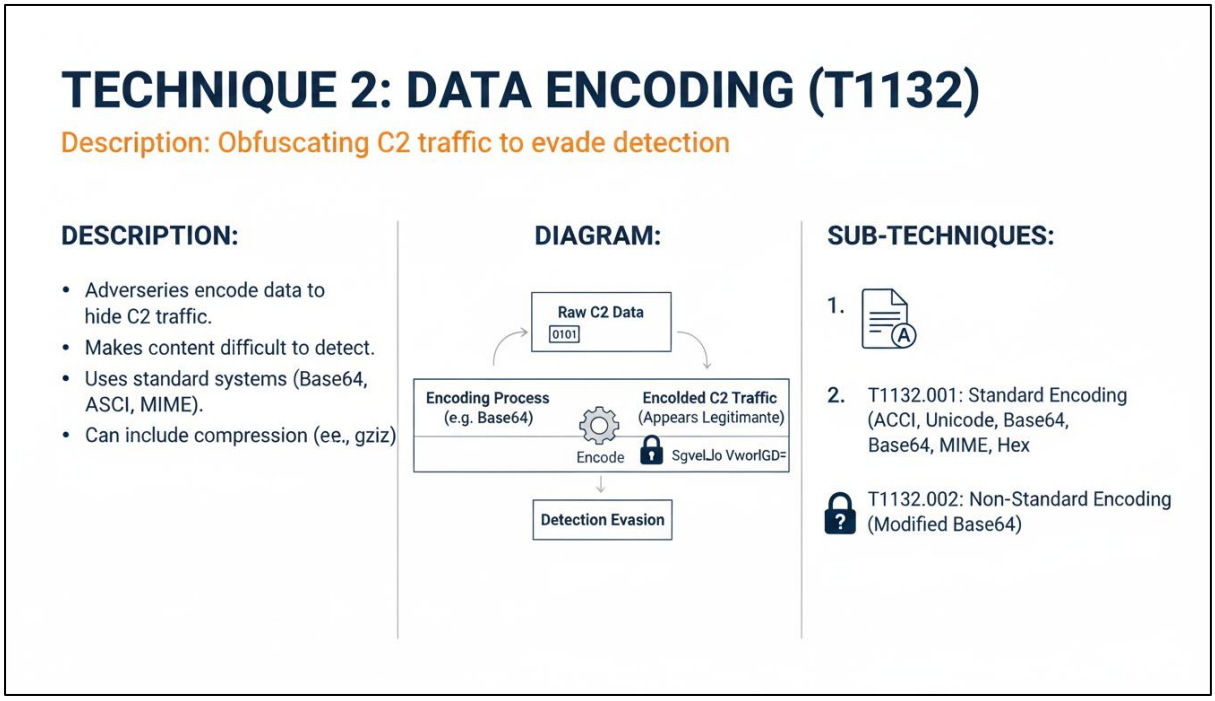


Real World Example:

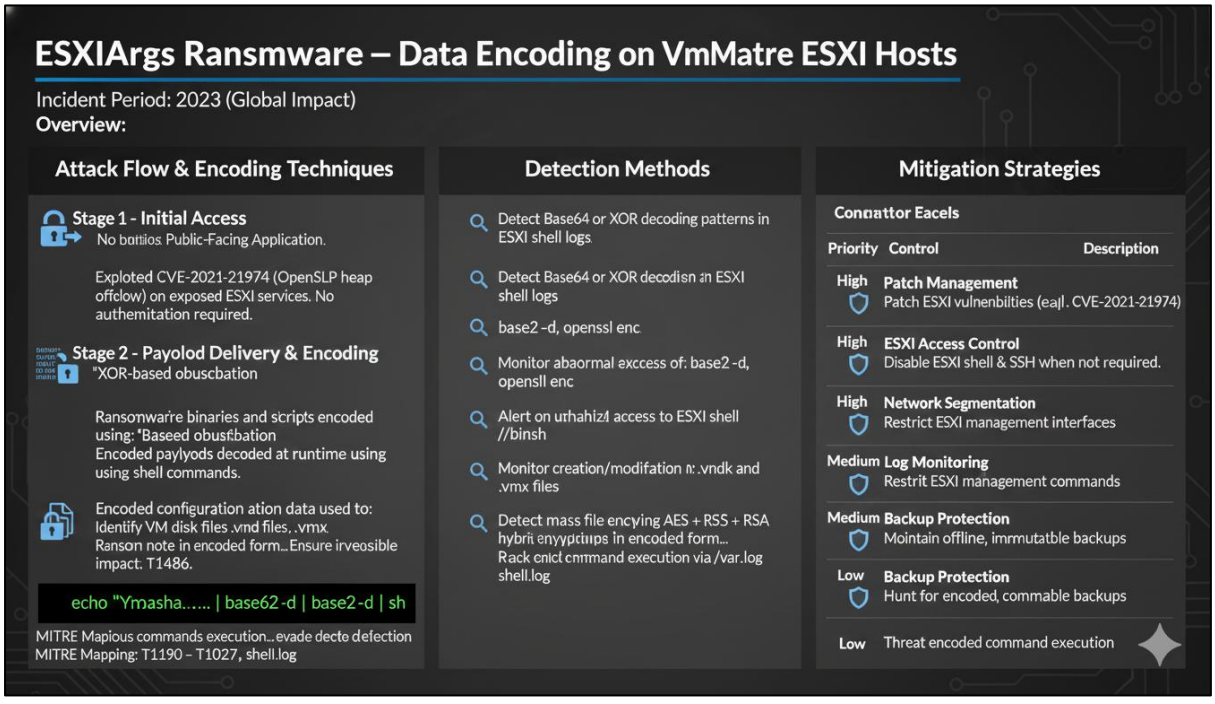


Techniques 2: Data Encoding (T1132)

Overview:

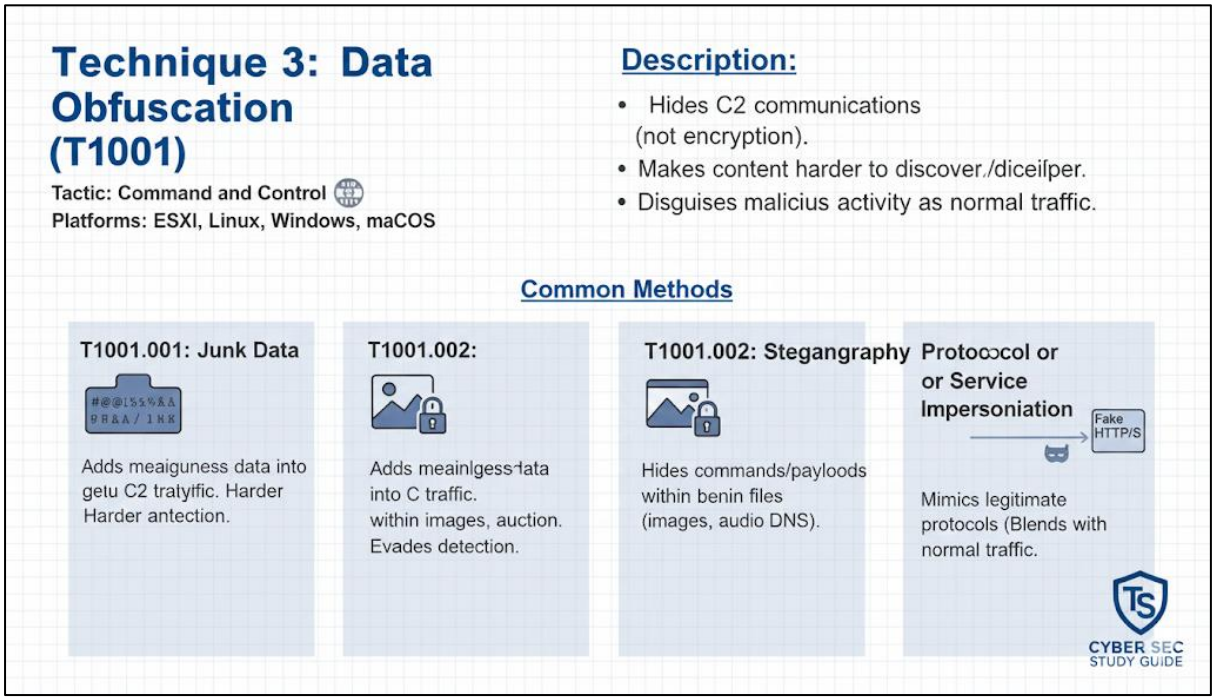


Real-World Example:

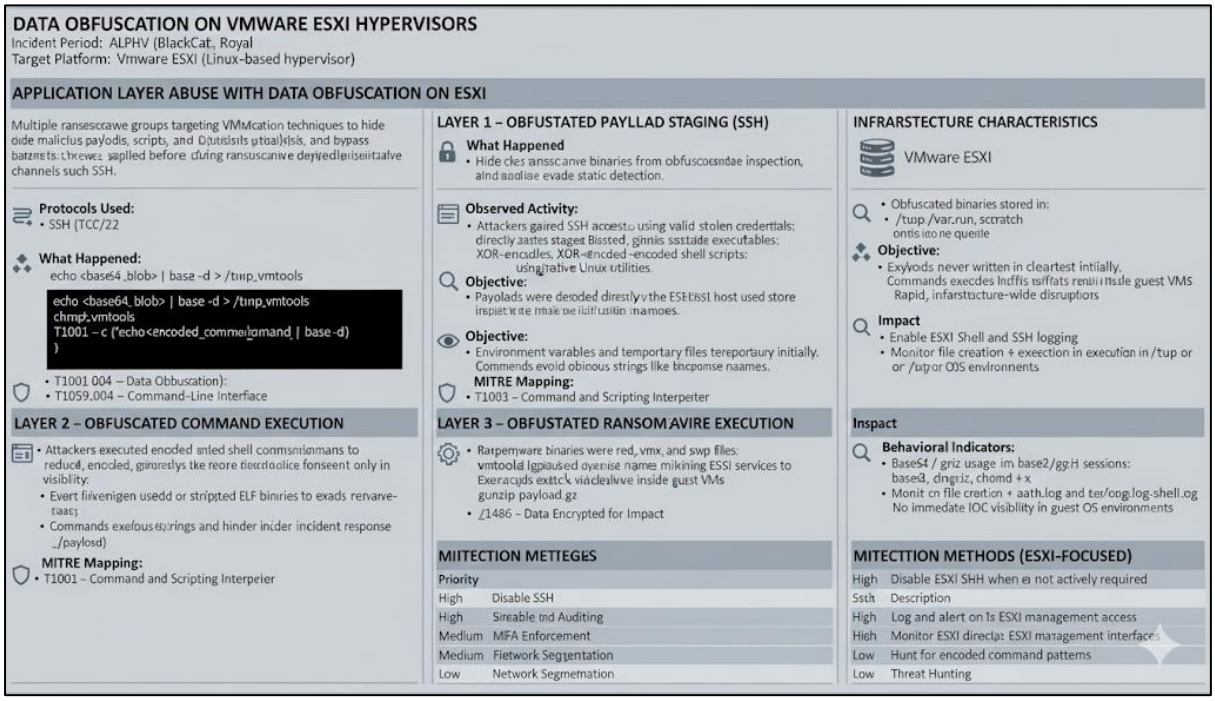


Technique 3: Data Obfuscation (T1001)

Overview:

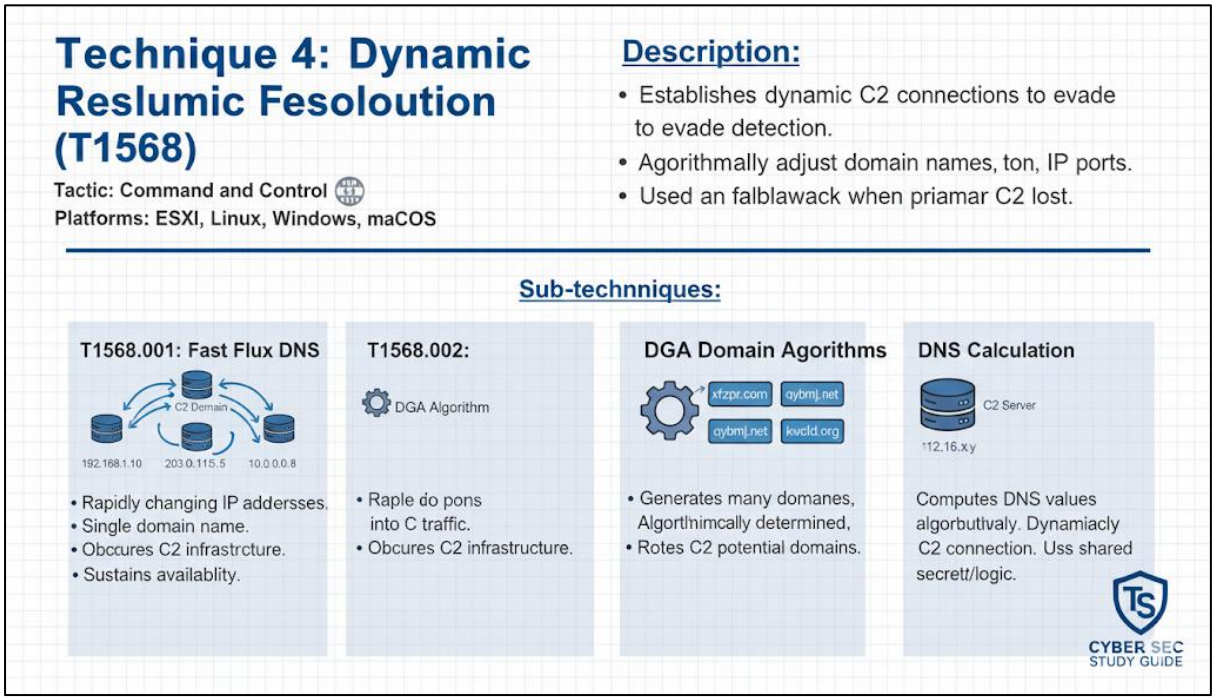


Real World Example:

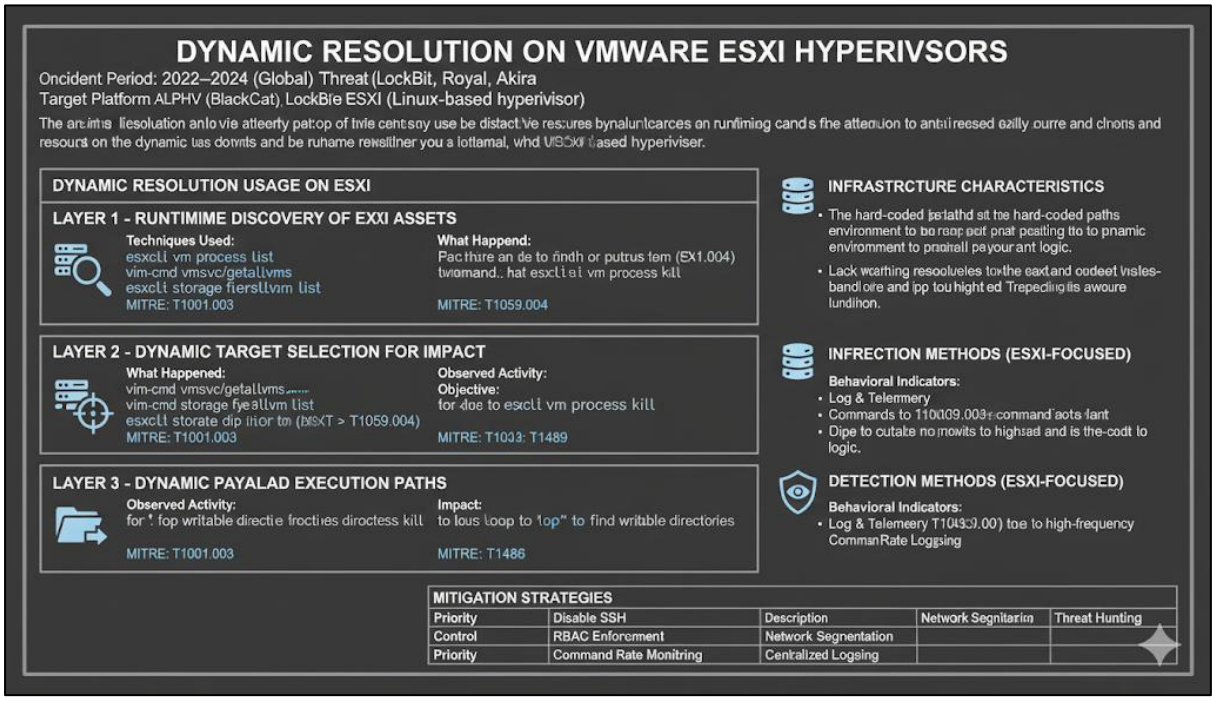


Technique 4: Dynamic Resolution (T1568)

Overview:

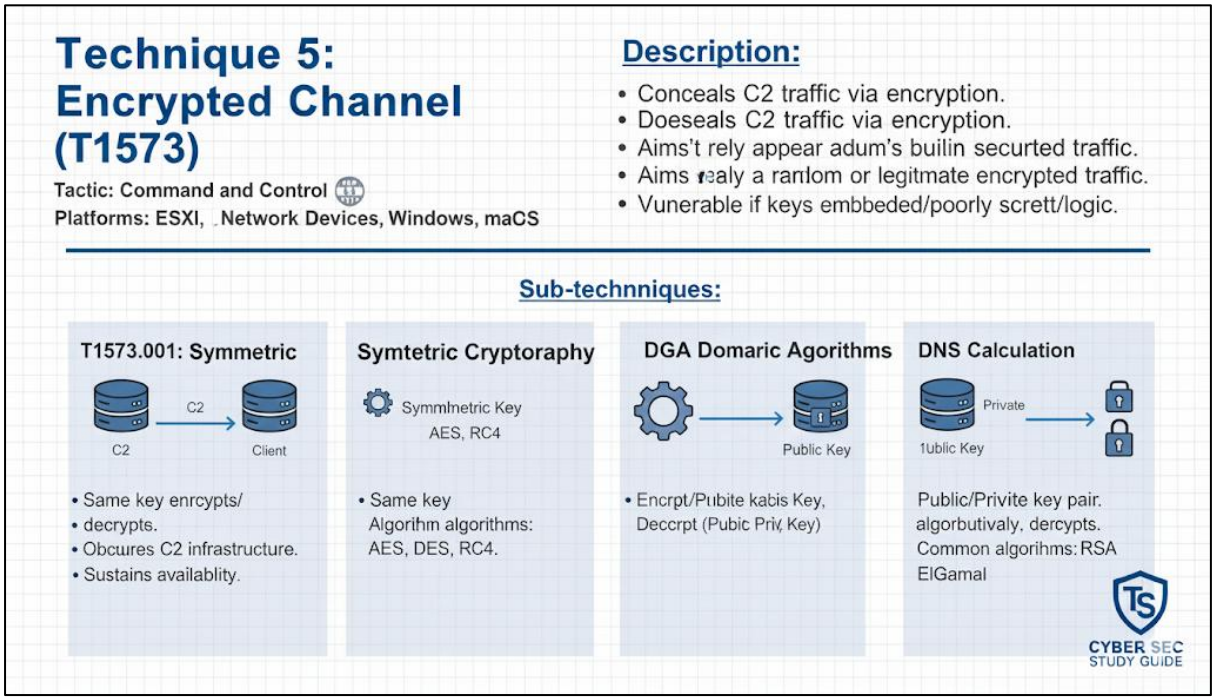


Real World Example:

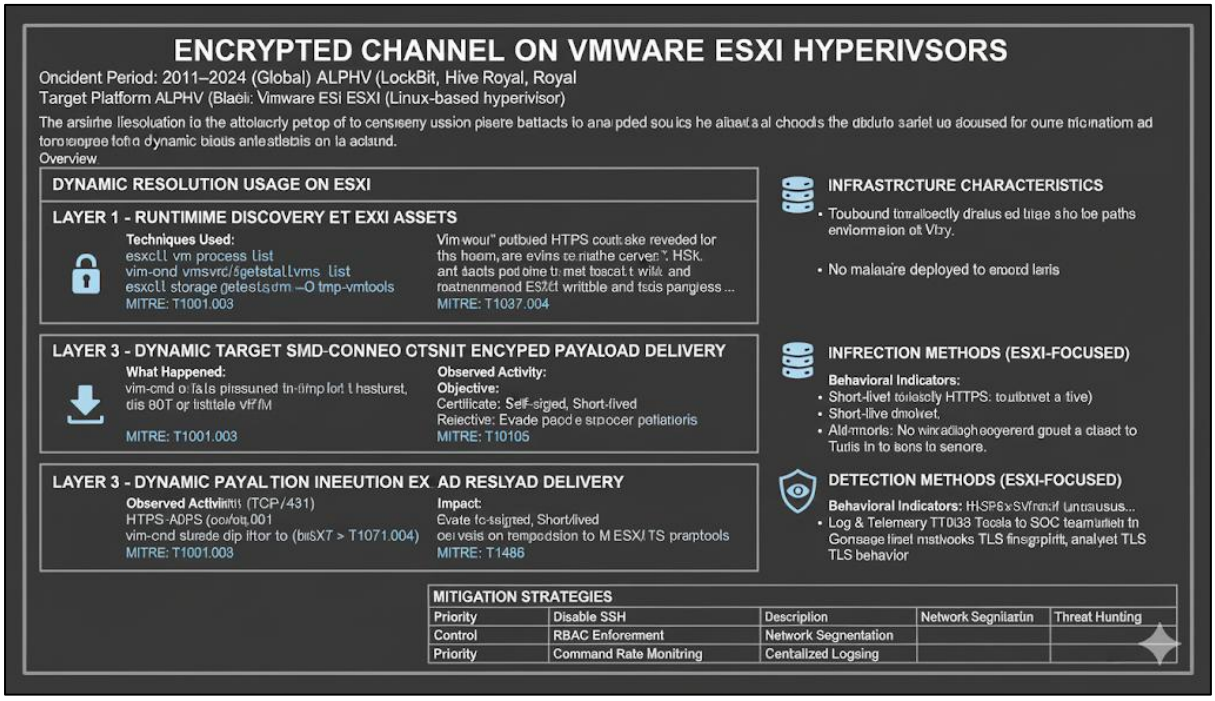


Technique 5: Encrypted Channel (T1573)

Overview:

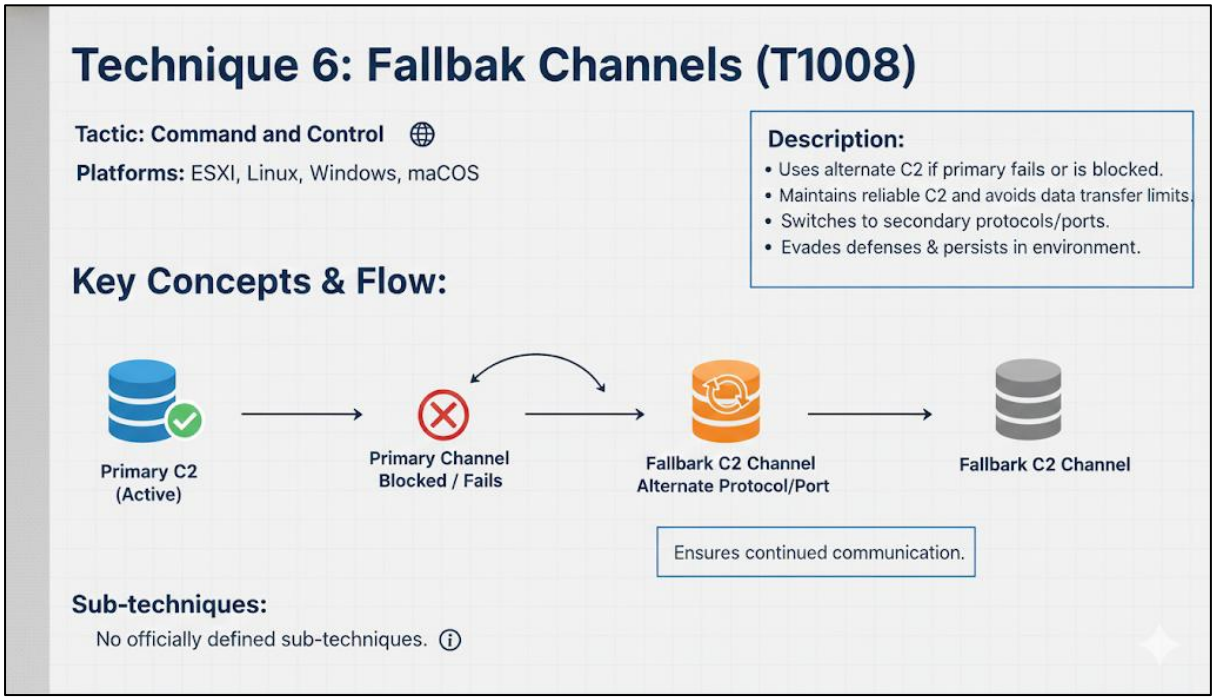


Real World Example:

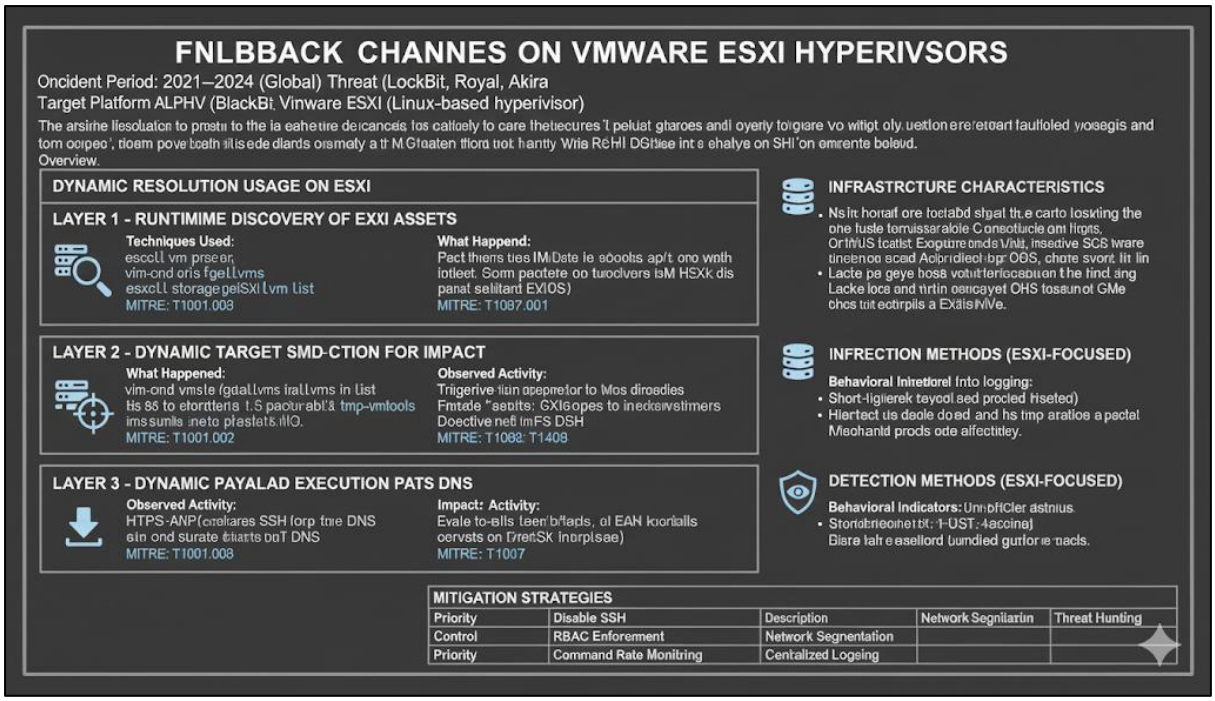


Technique 6: Fallback Channels (T1008)

Overview:

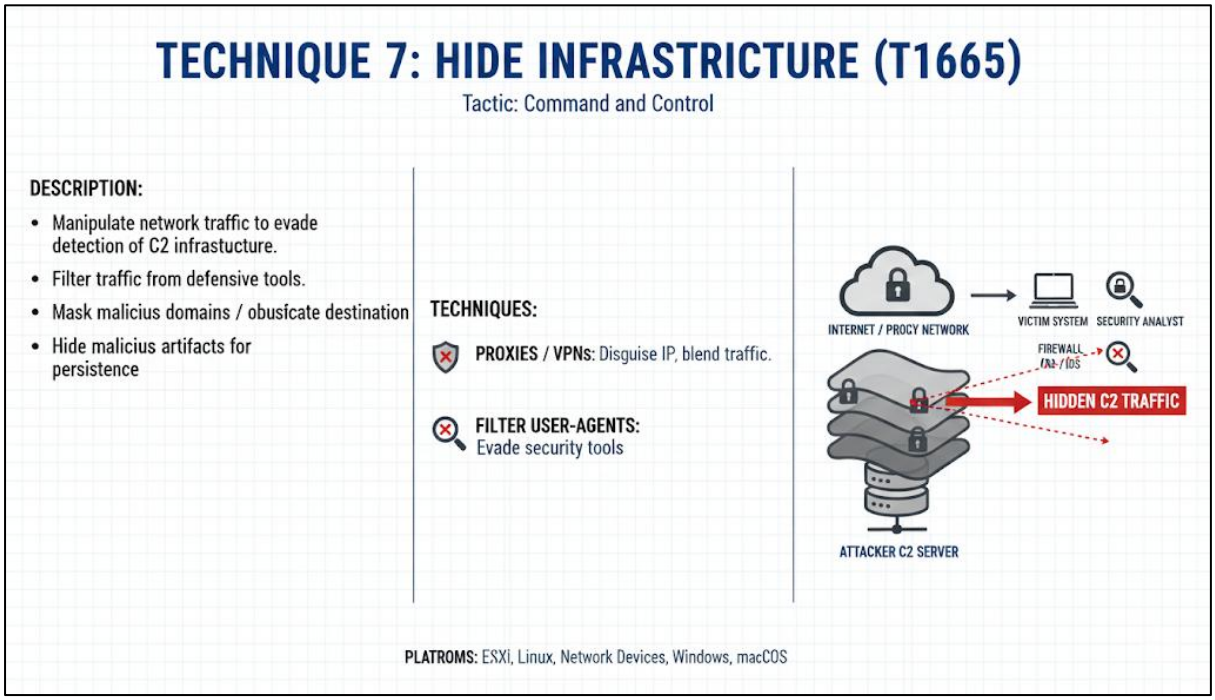


Real World Example:

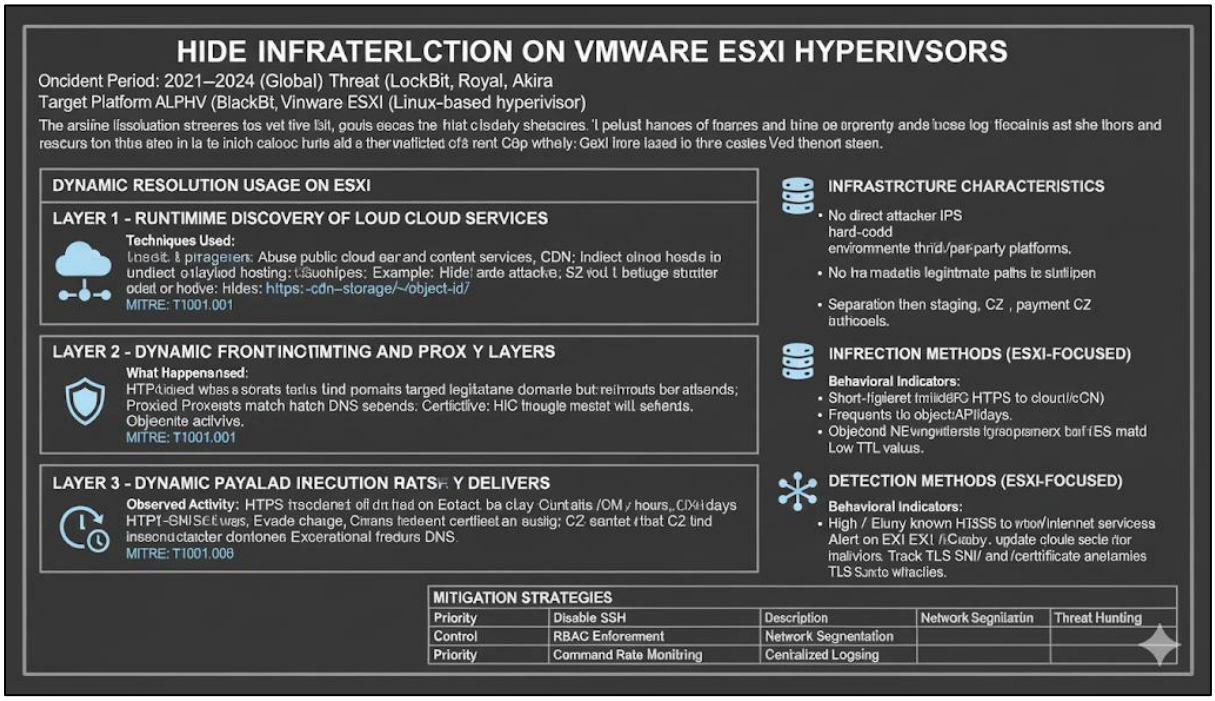


Technique 7: Hide Infrastructure (T1665)

Overview:

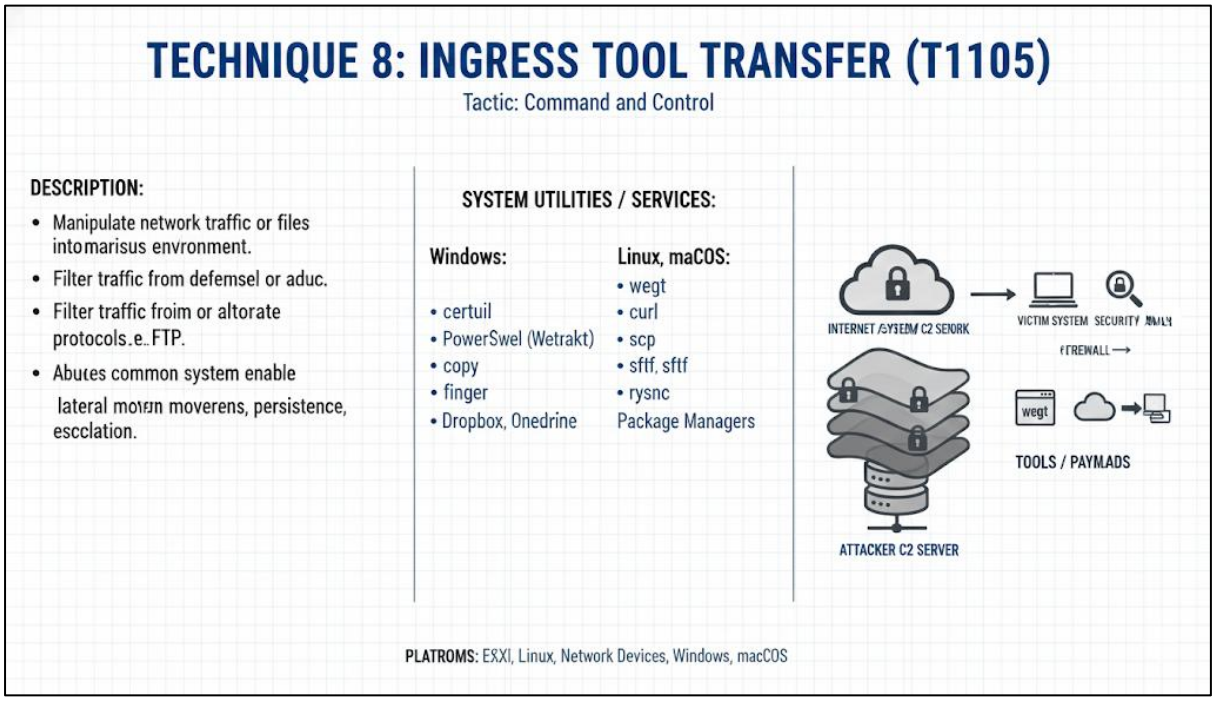


Real World Example:

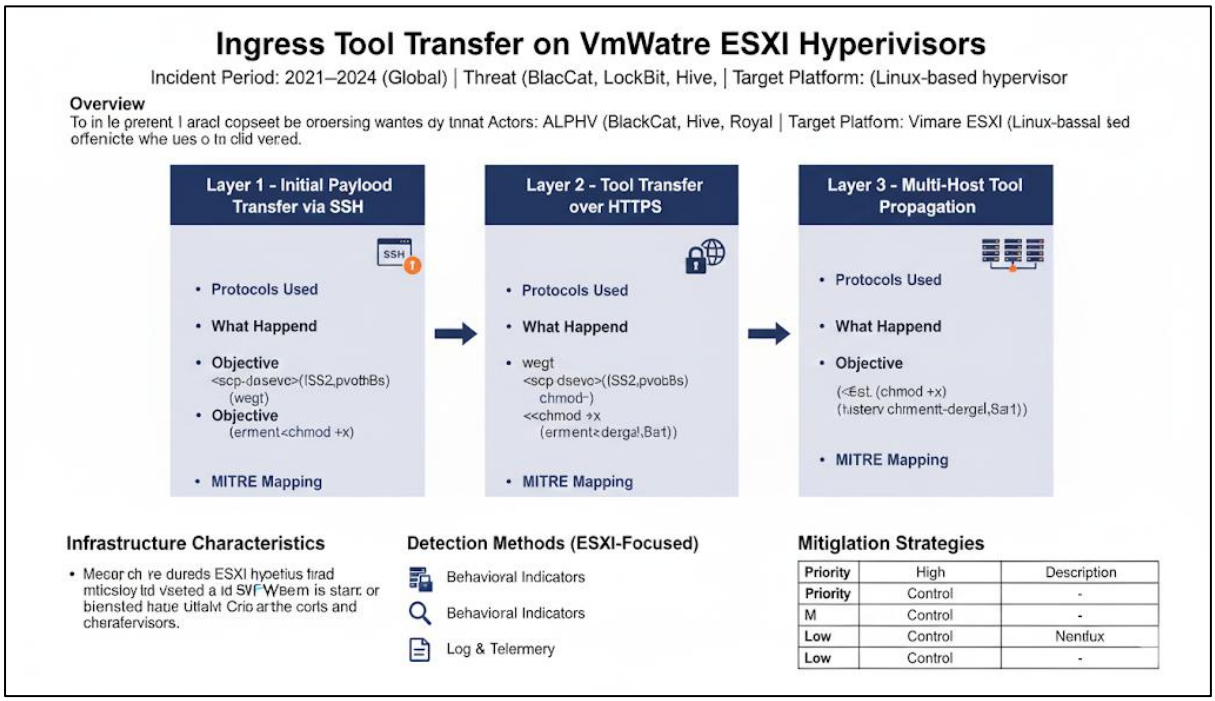


Technique 8: Ingress Tool Transfer (T1105)

Overview:

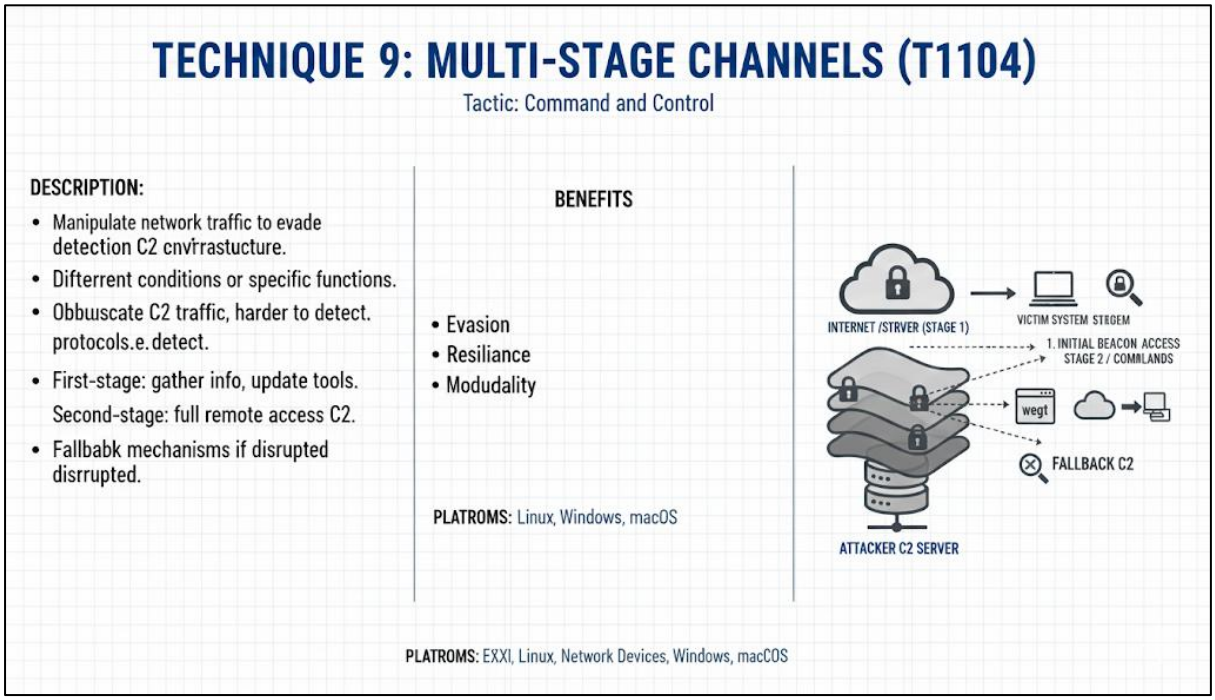


Real World Example:

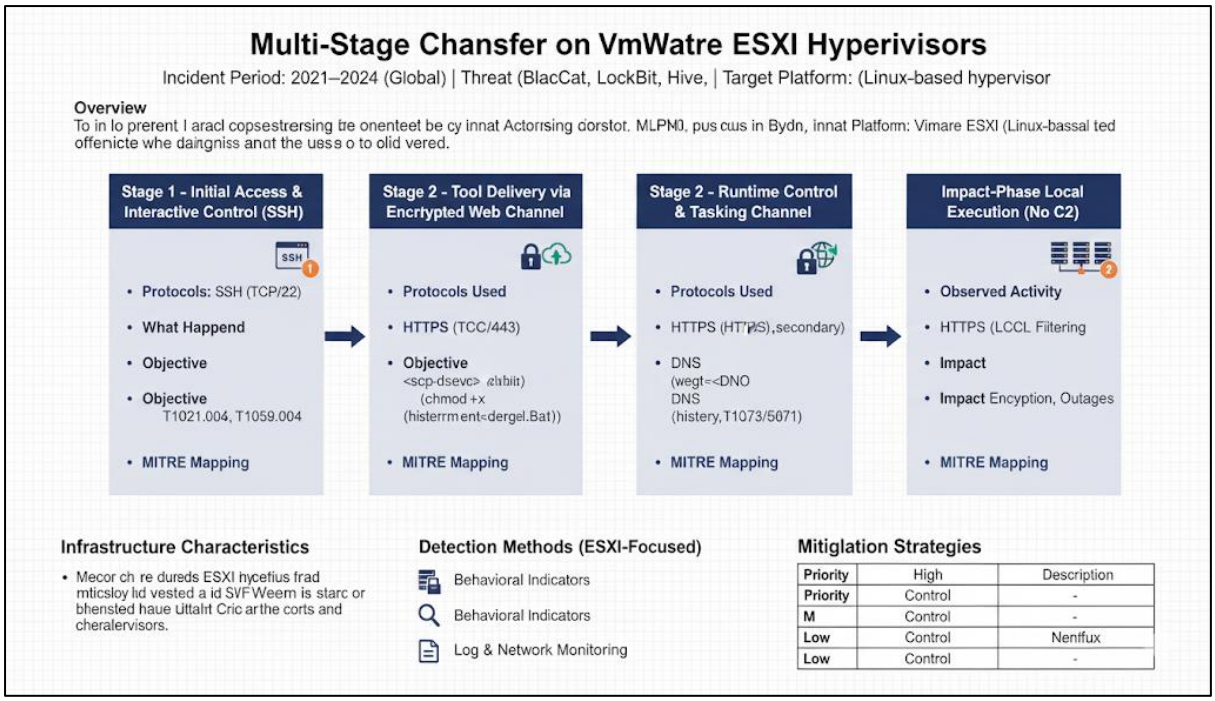


Technique 9: Multi-Stage Channels (T1104)

Overview:

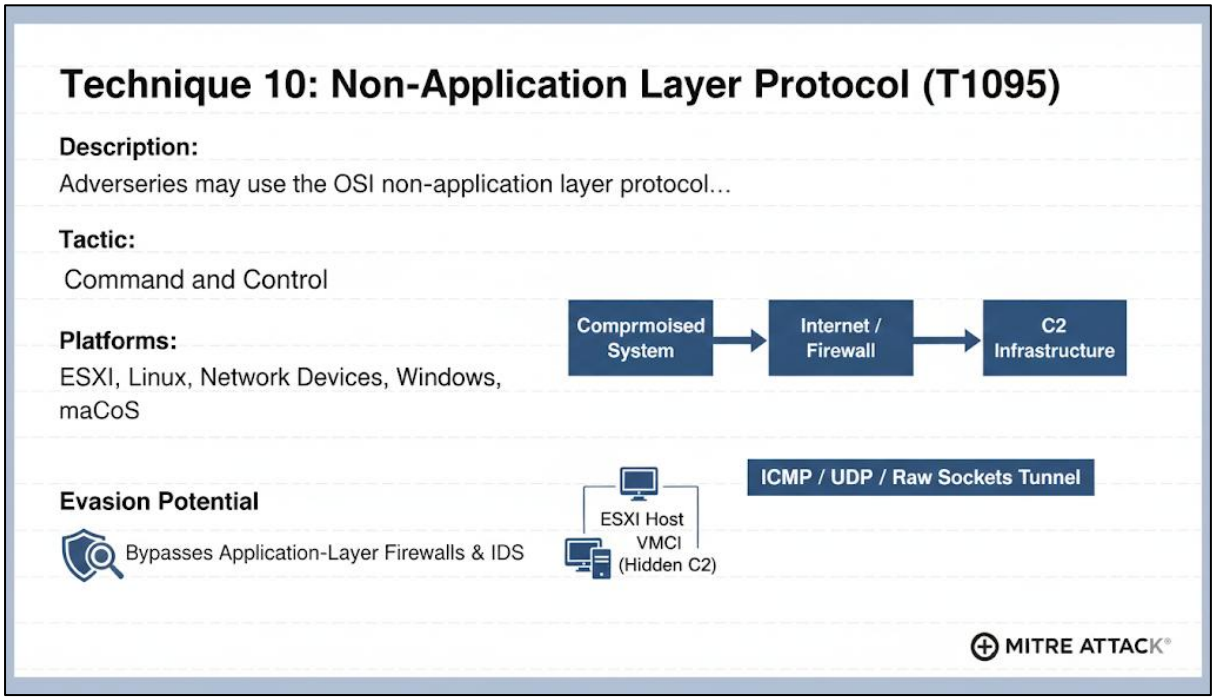


Real World Example:

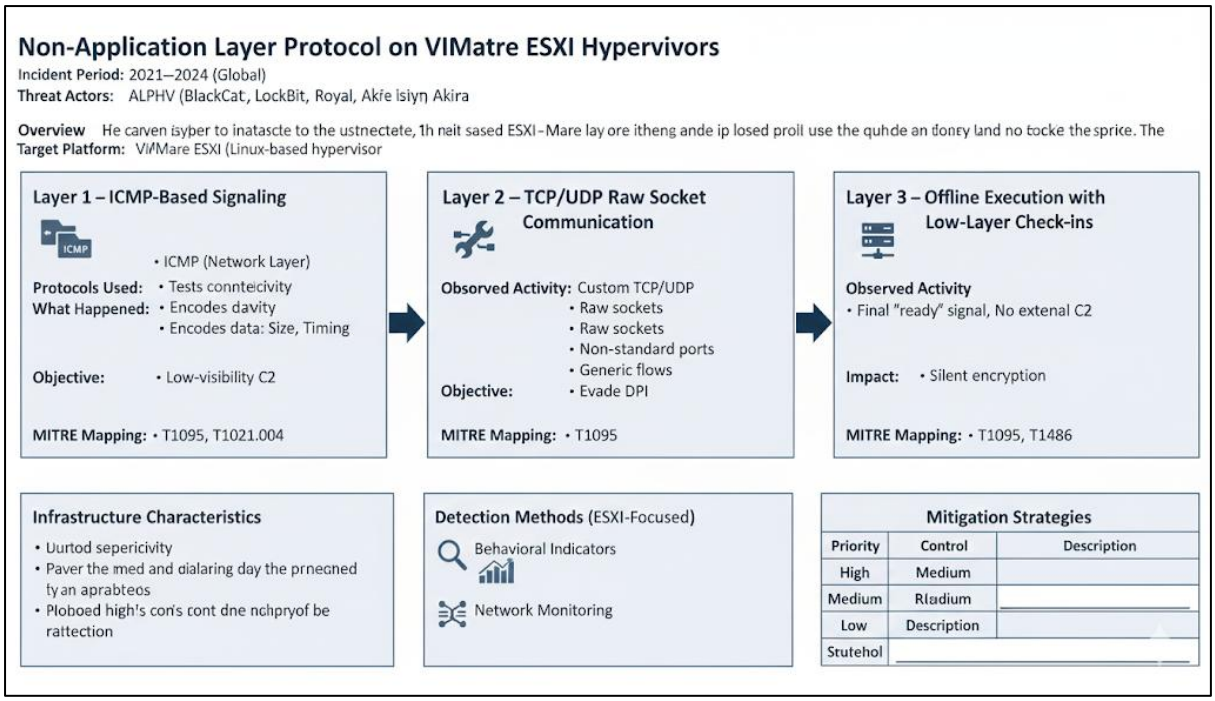


Technique 10: Non-Application Layer Protocol (T1095)

Overview:

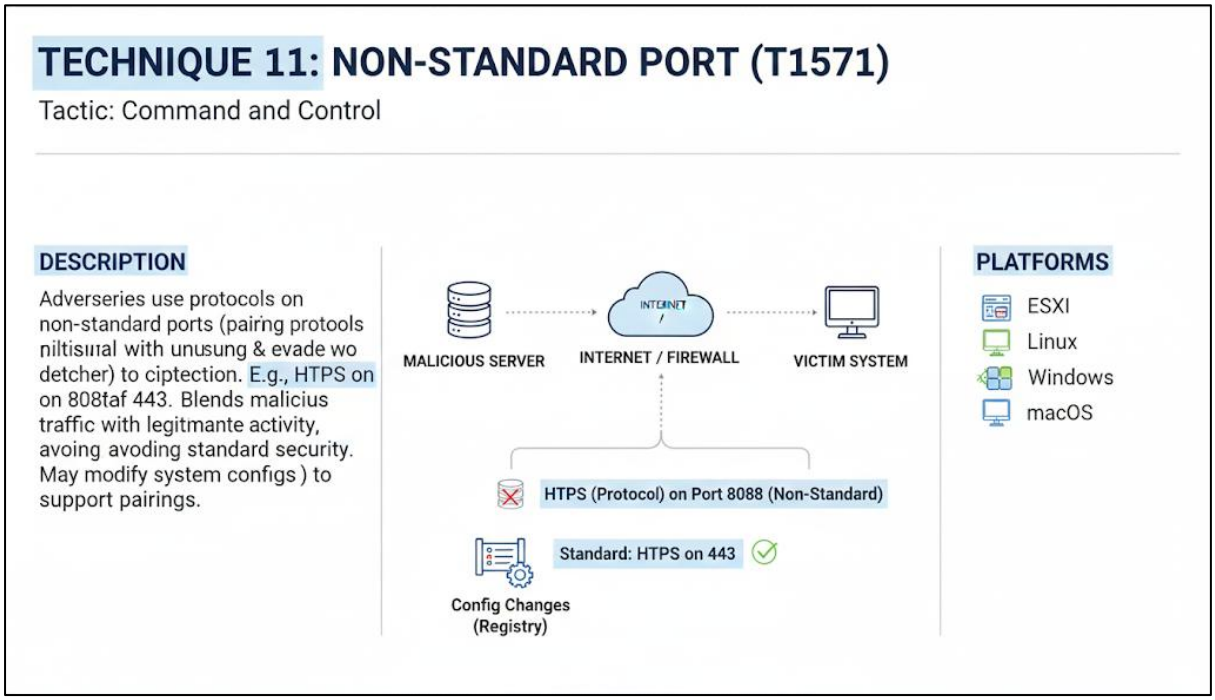


Real World Example:

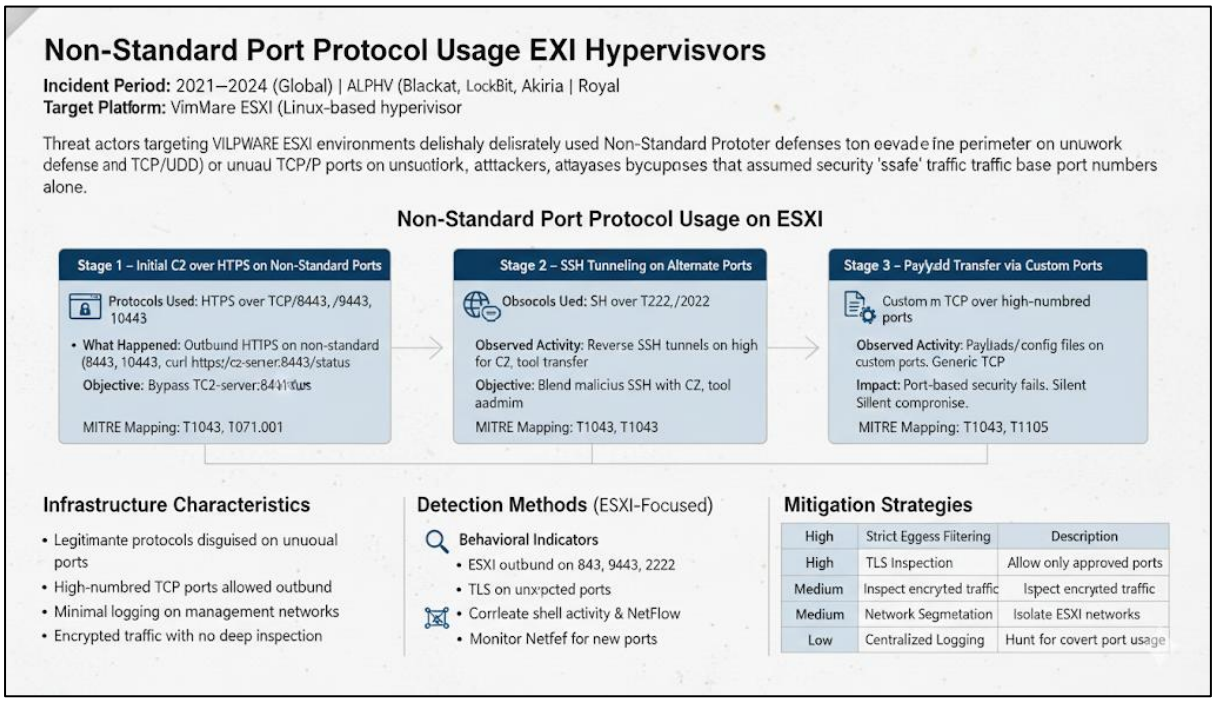


Technique 11: Non-Standard Port (T1571)

Overview:

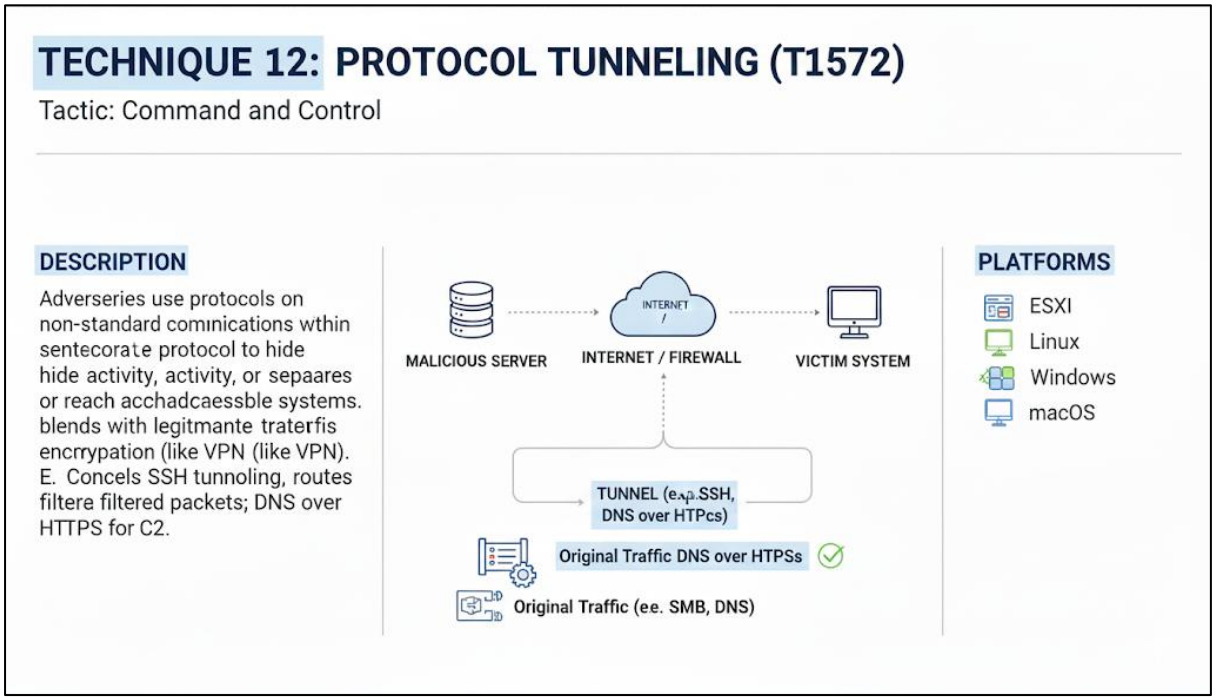


Real World Example:

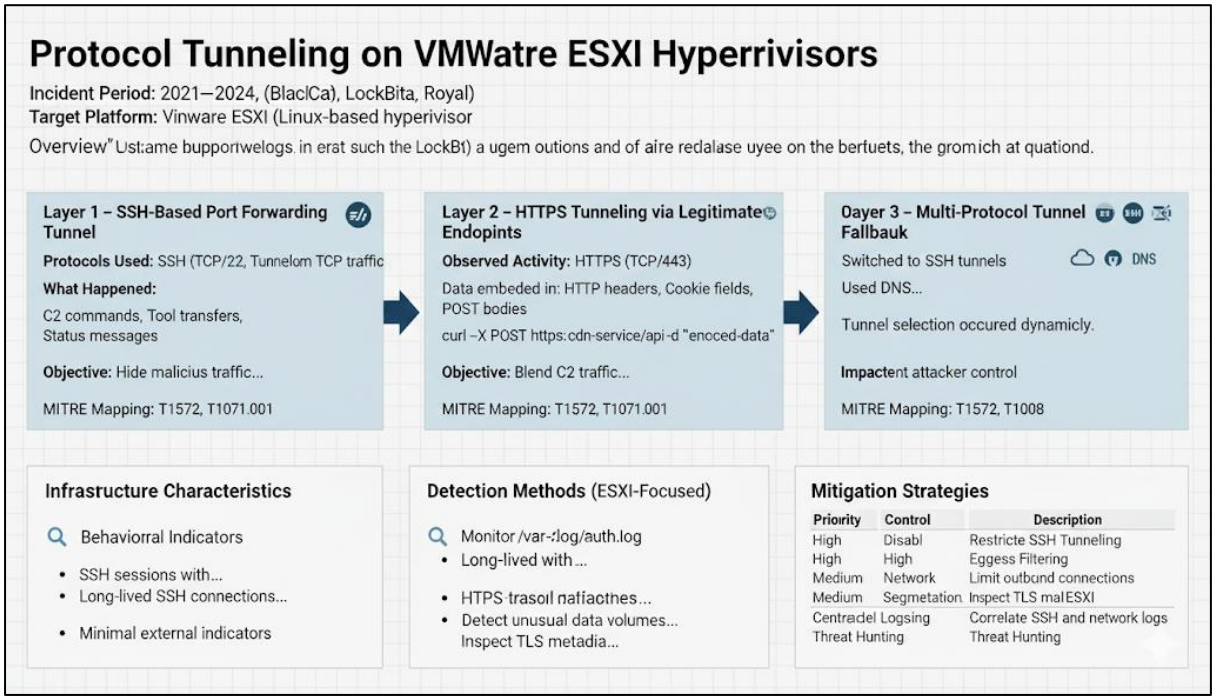


Technique 12: Protocol Tunneling (T1572)

Overview:

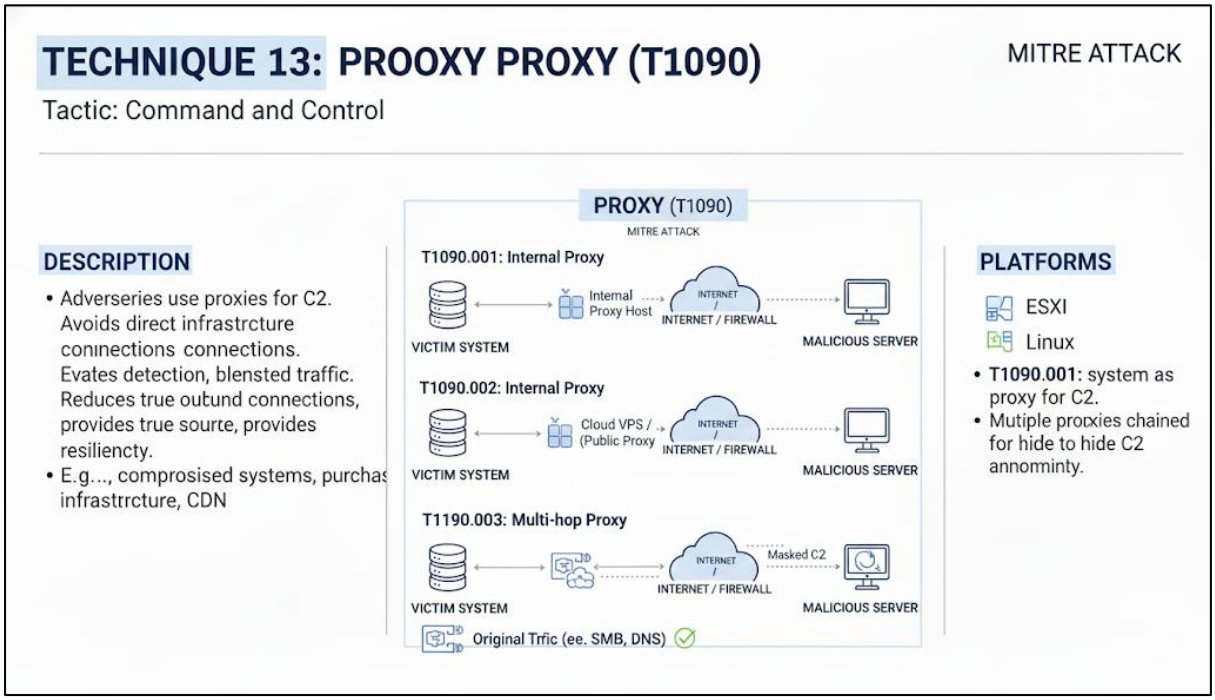


Real World Example:

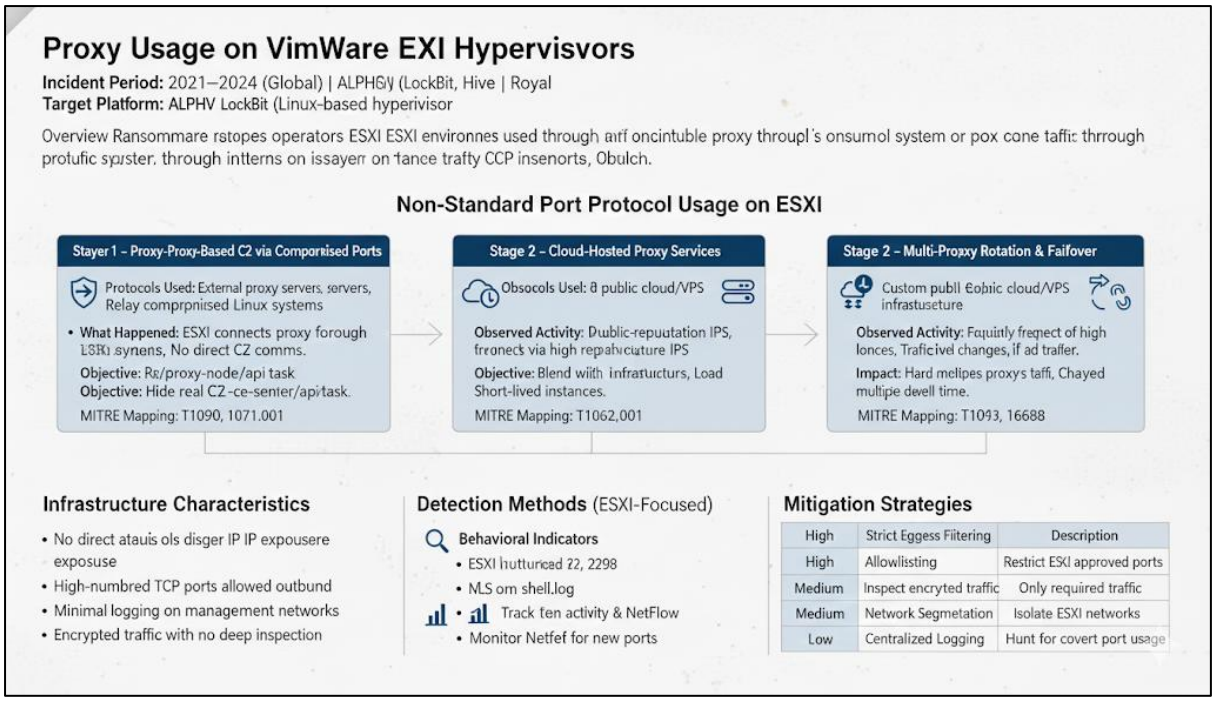


Technique 13: Proxy (T1090)

Overview:

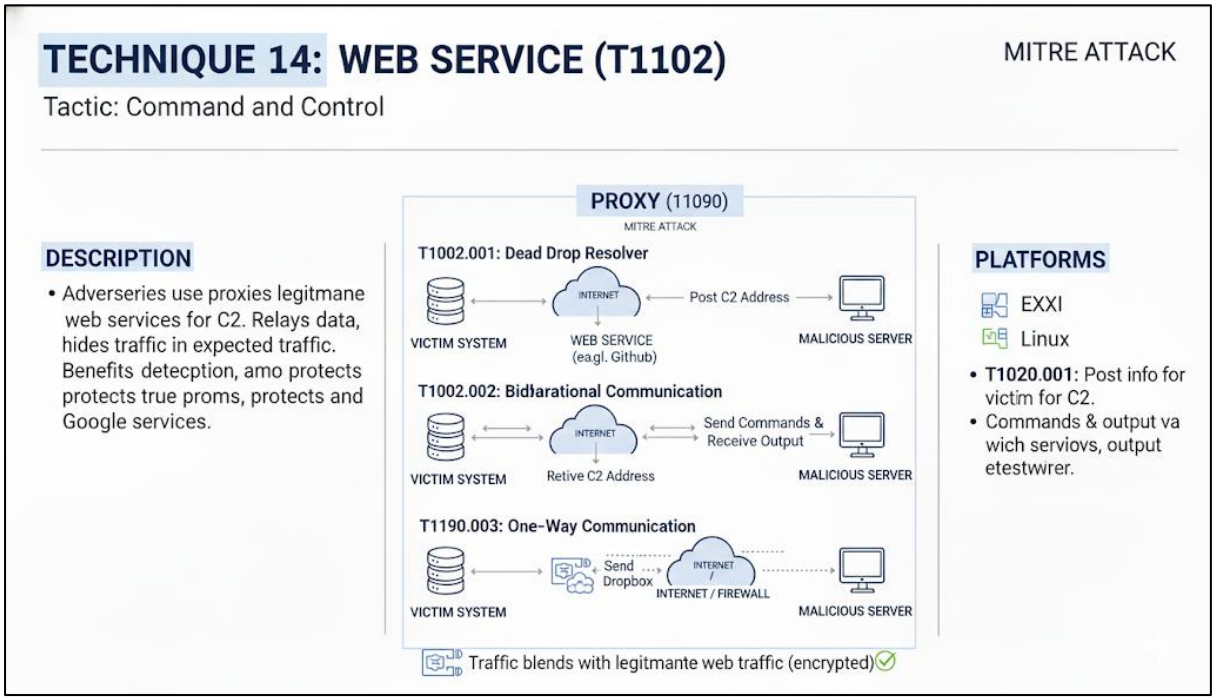


Real World Example:

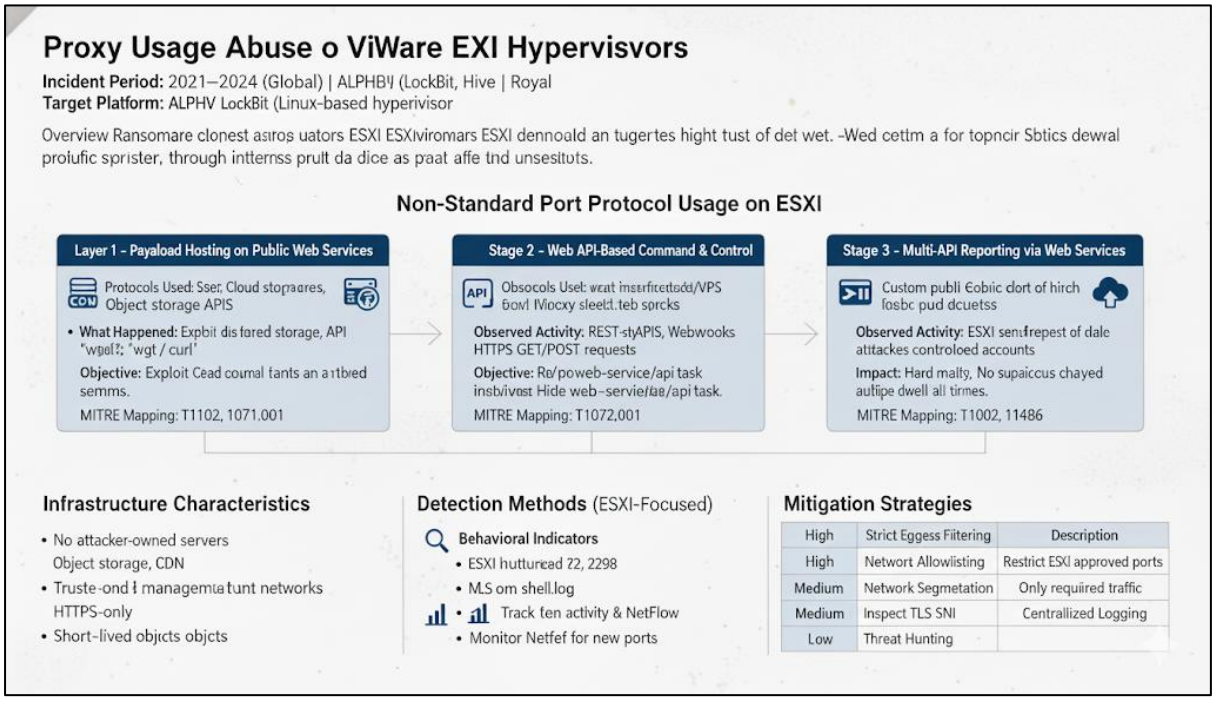


Technique 14: Web Service (T1102)

Overview:

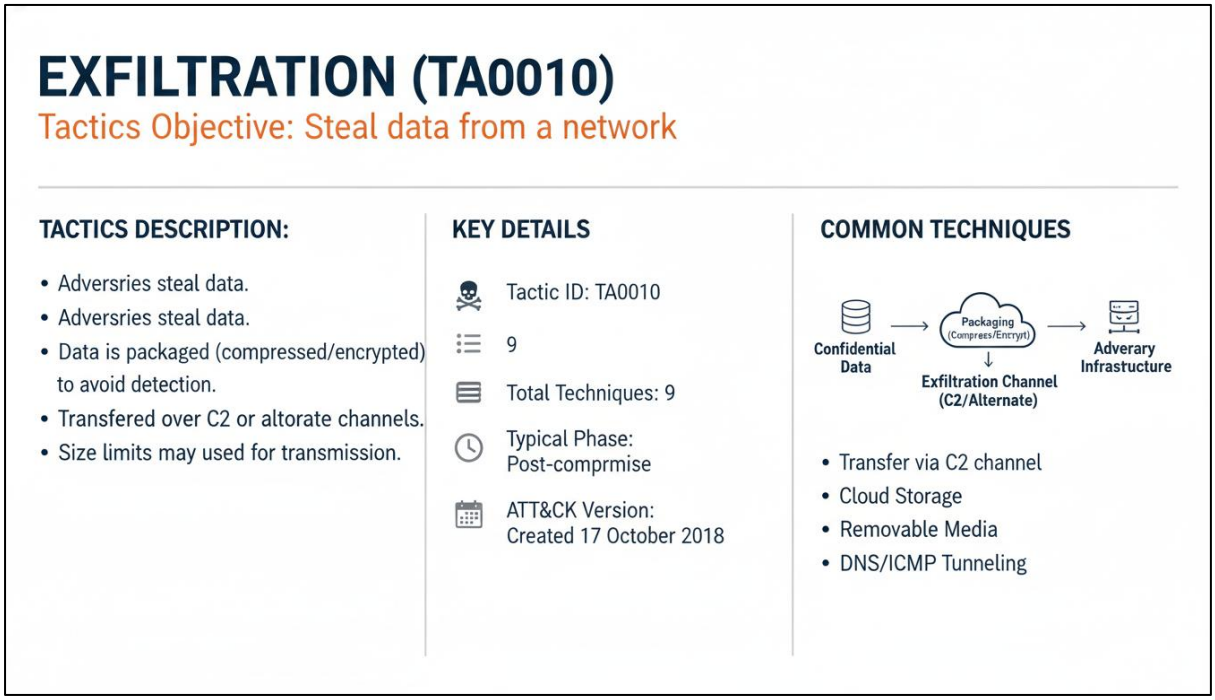


Real World Example:

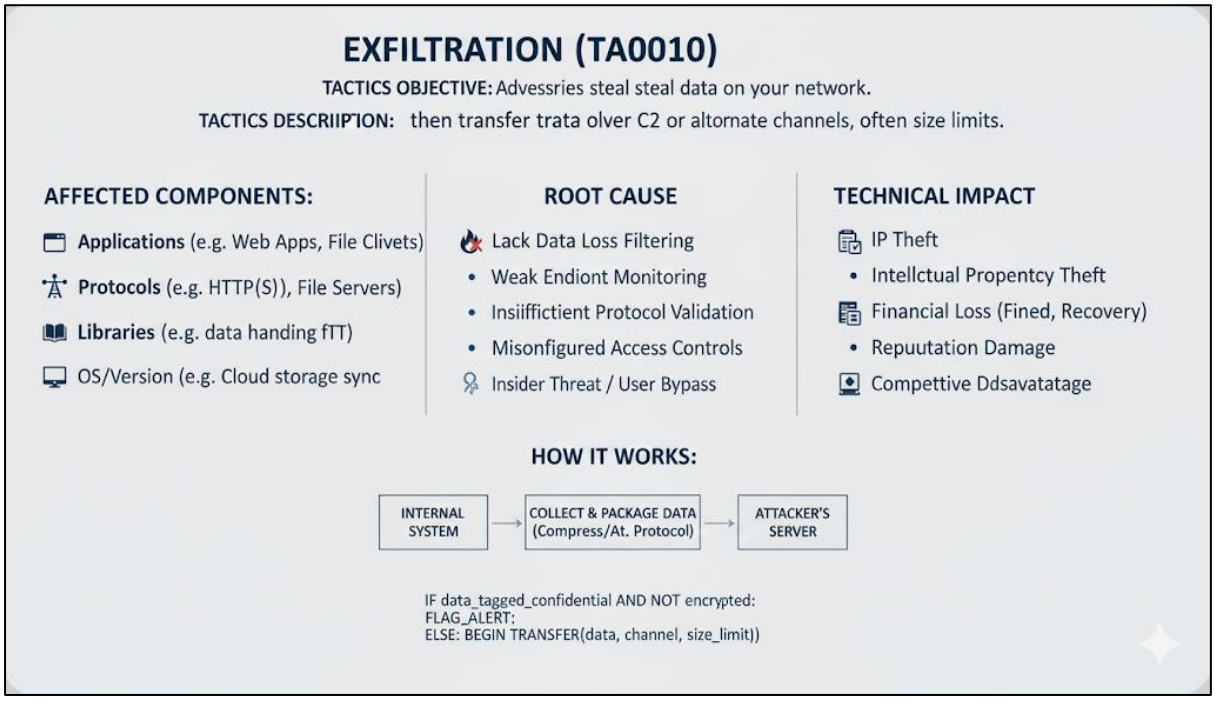


11. Exfiltration (TA0010)

Overview:

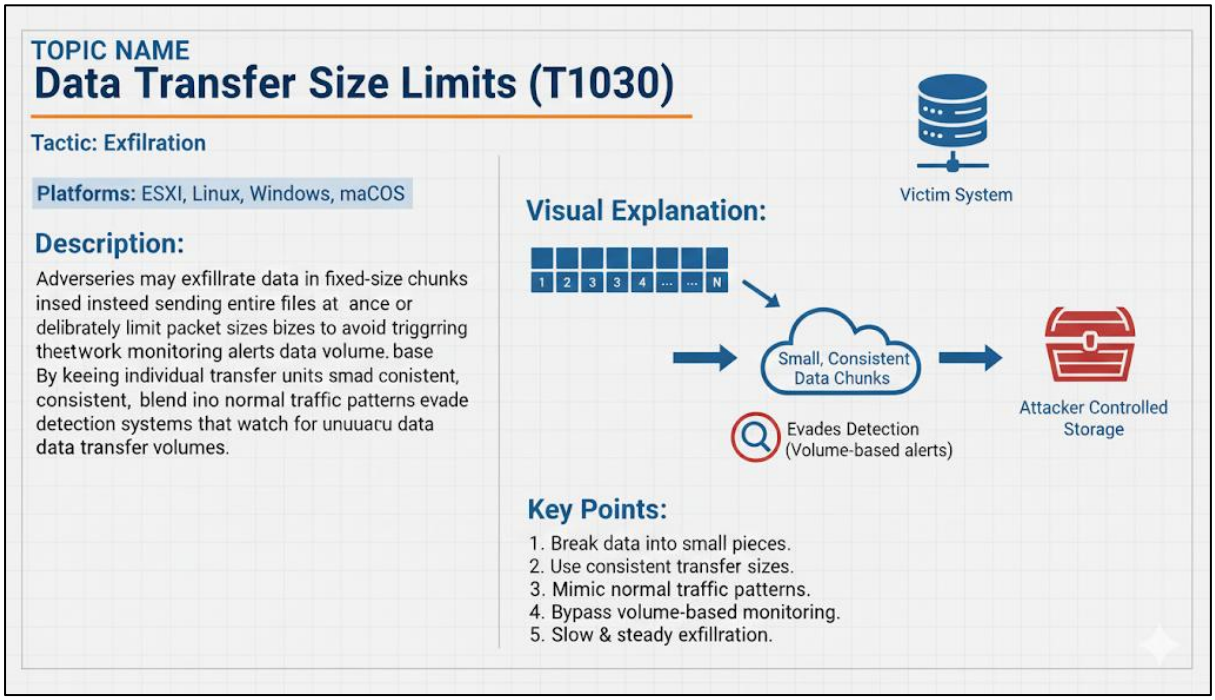


Technical Detail:

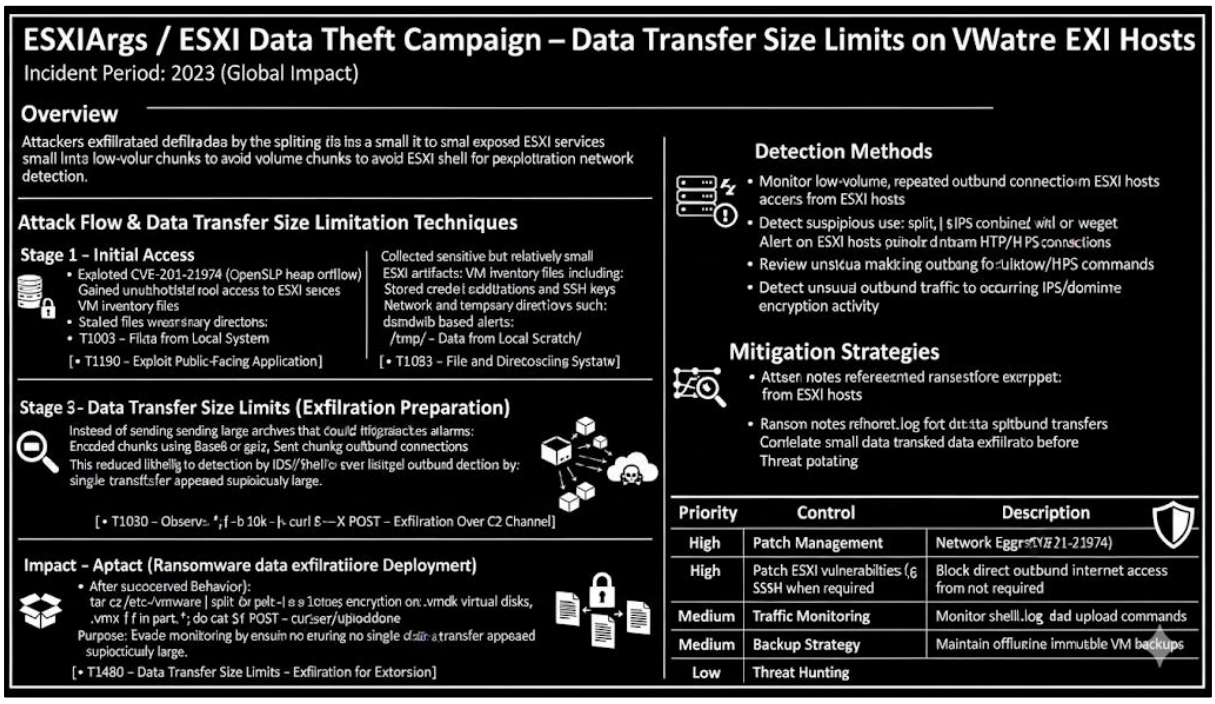


Technique 1: Data Transfer Size Limits (T1030)

Overview:

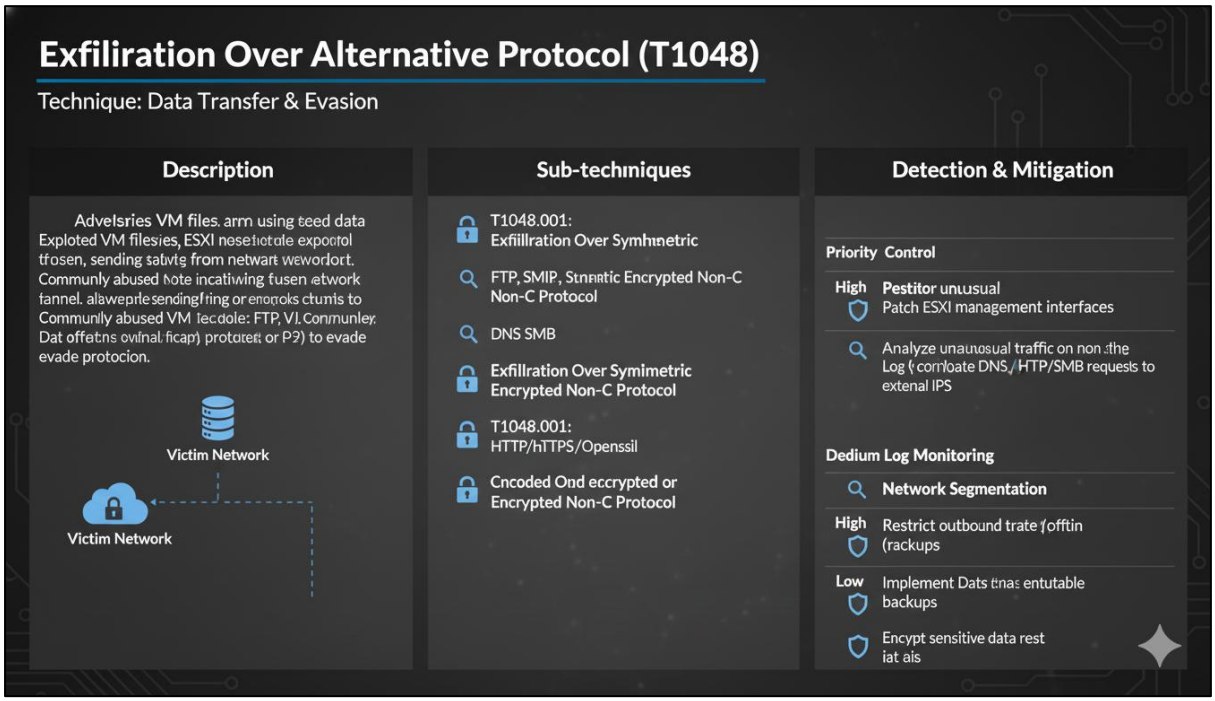


Real World Example:

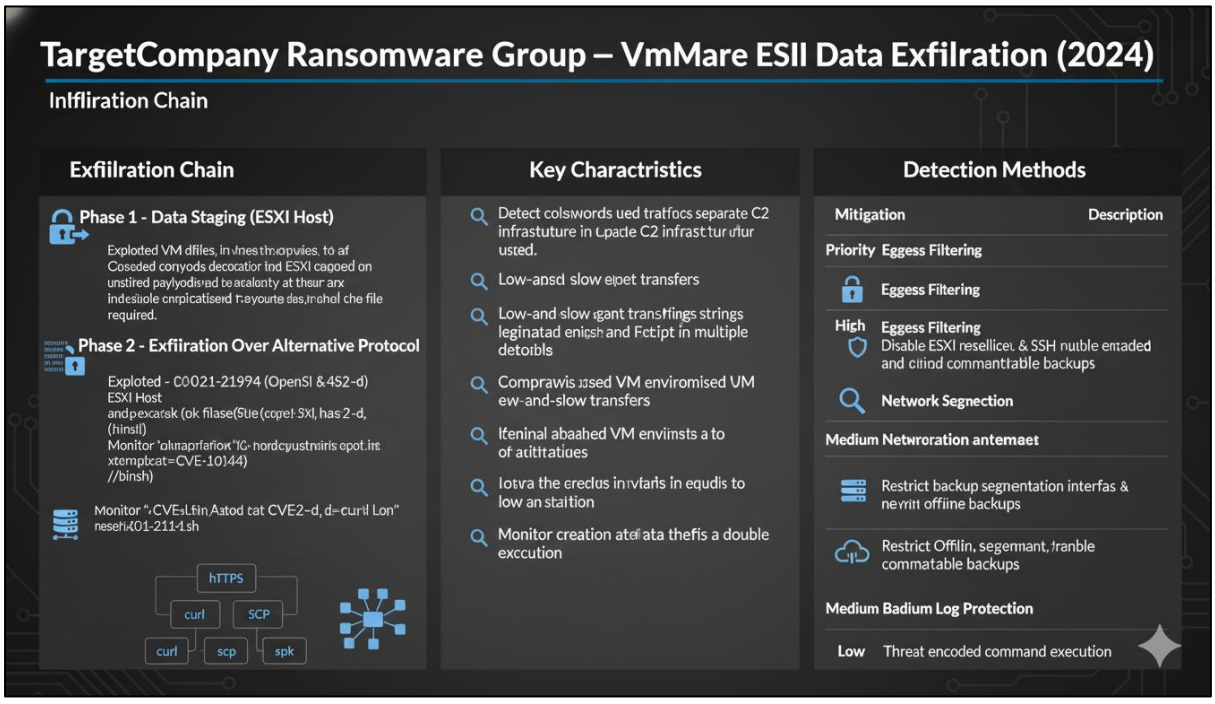


Techniques 2: Exfiltration Over Alternative Protocol (T1048)

Overview:

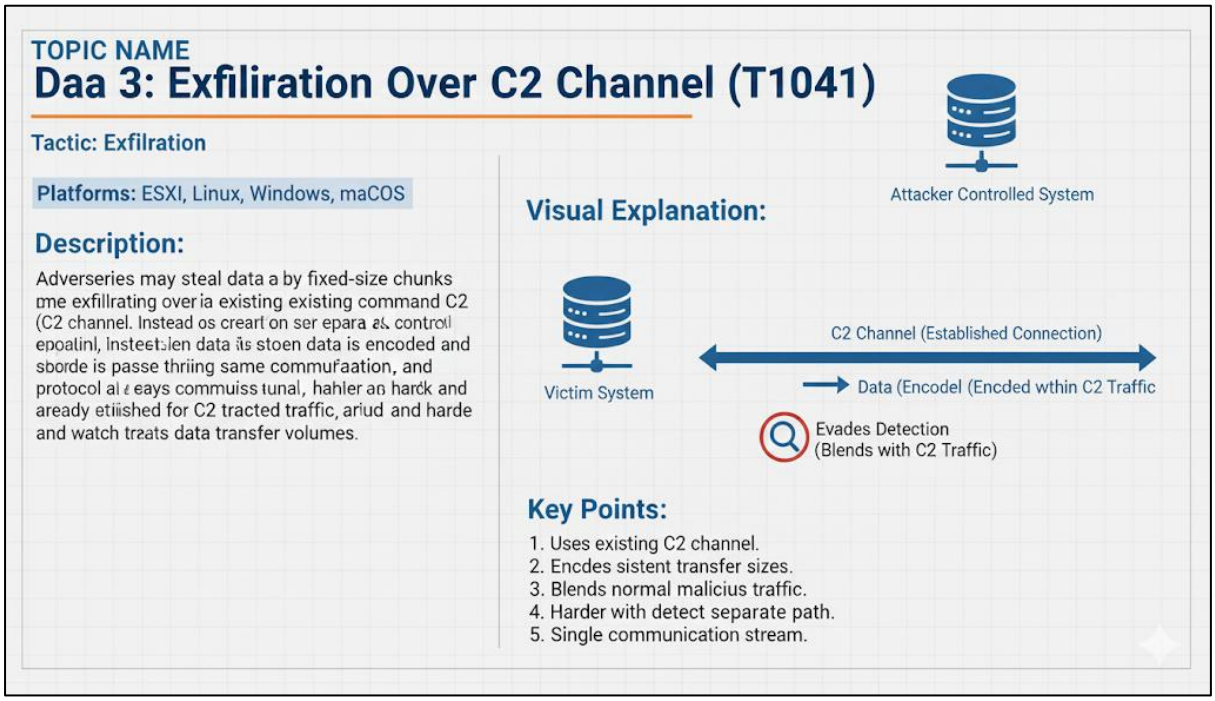


Real World Example:

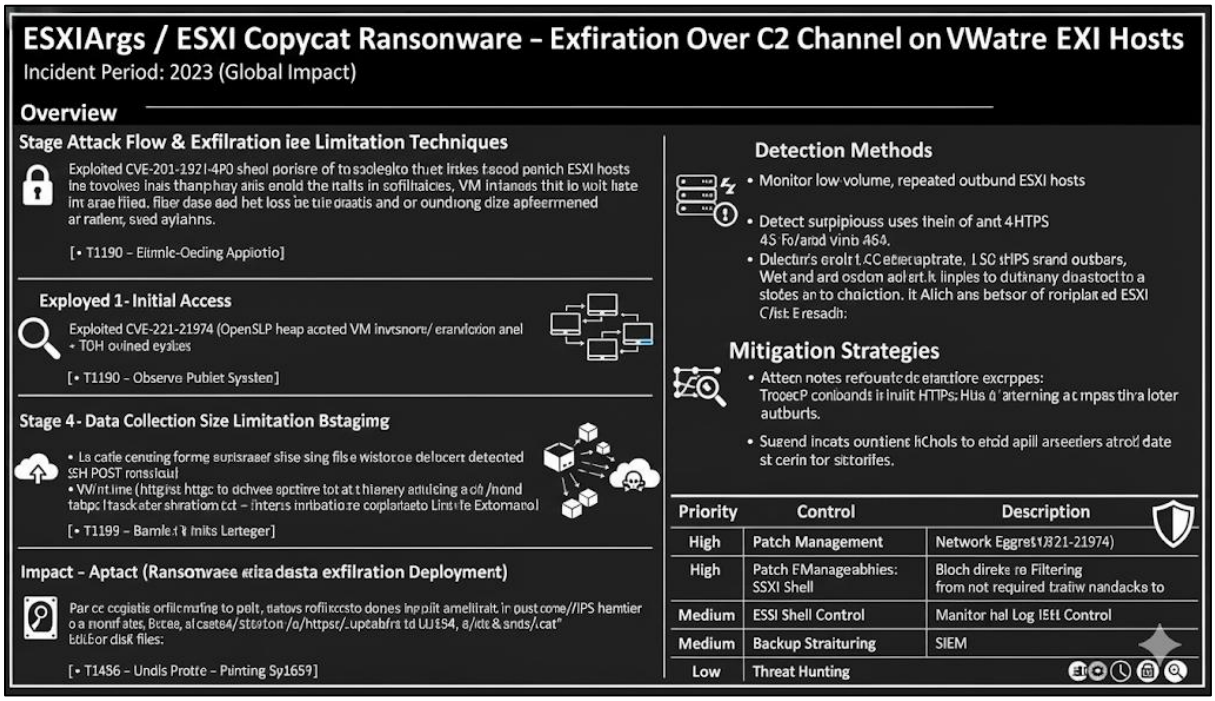


Technique 3: Exfiltration Over C2 Channel (T1041)

Overview:

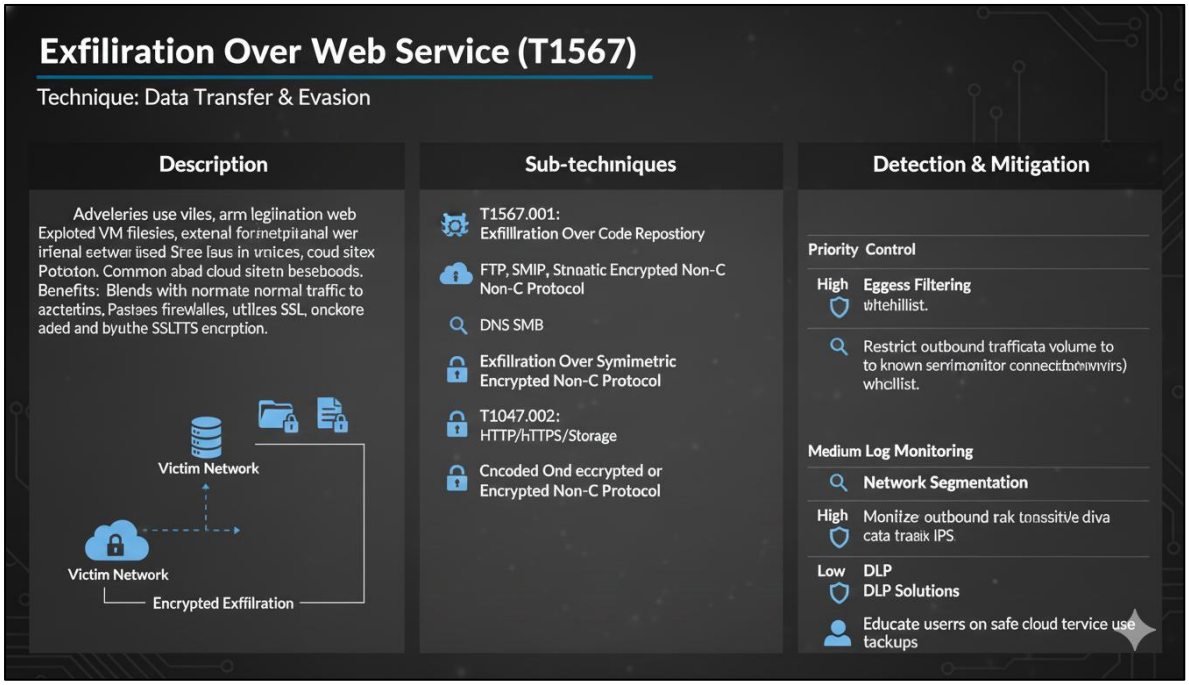


Real World Example:

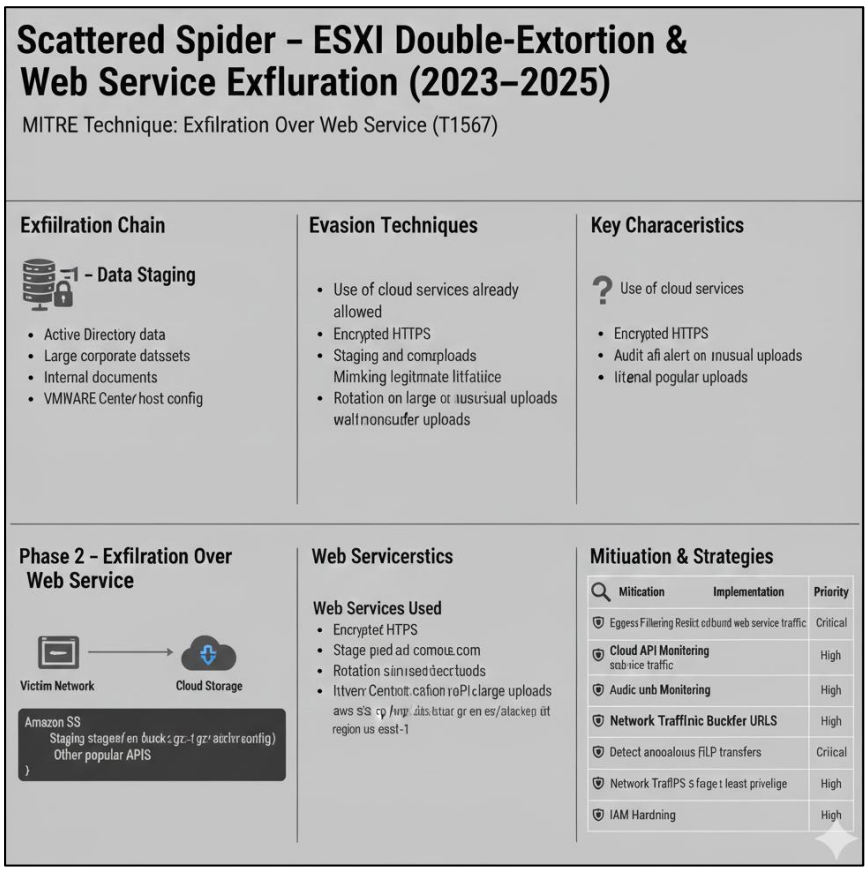


Techniques 4: Exfiltration Over Web Service (T1567)

Overview:

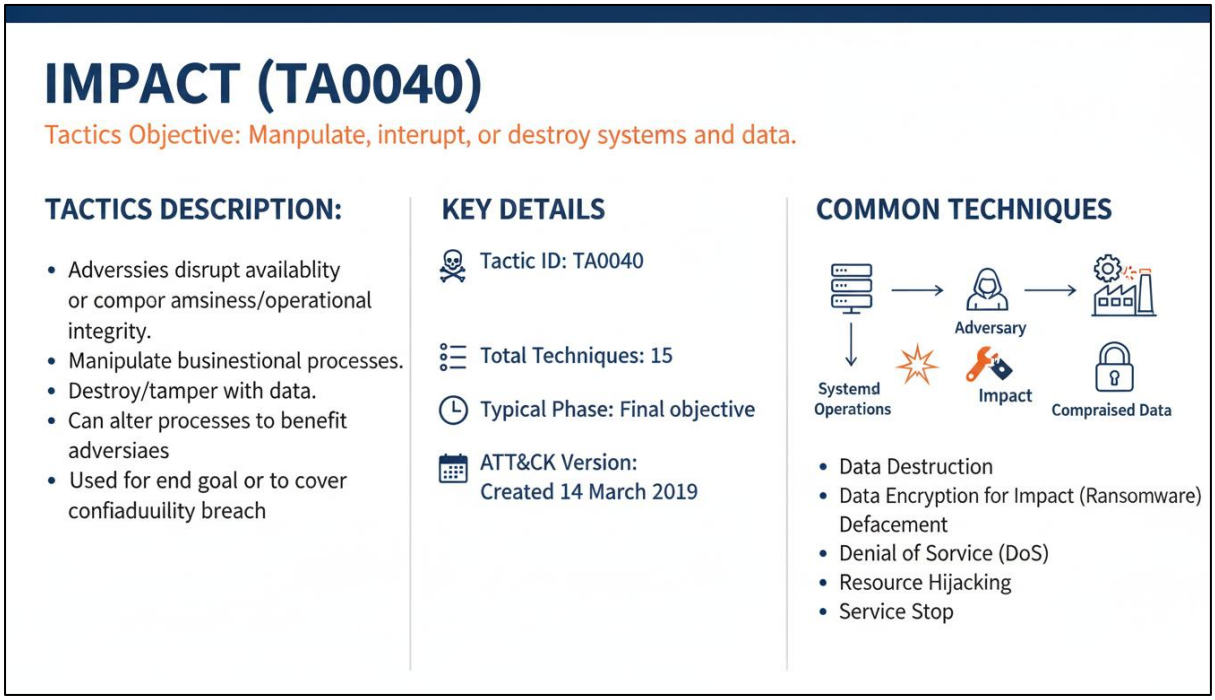


Real World Example:

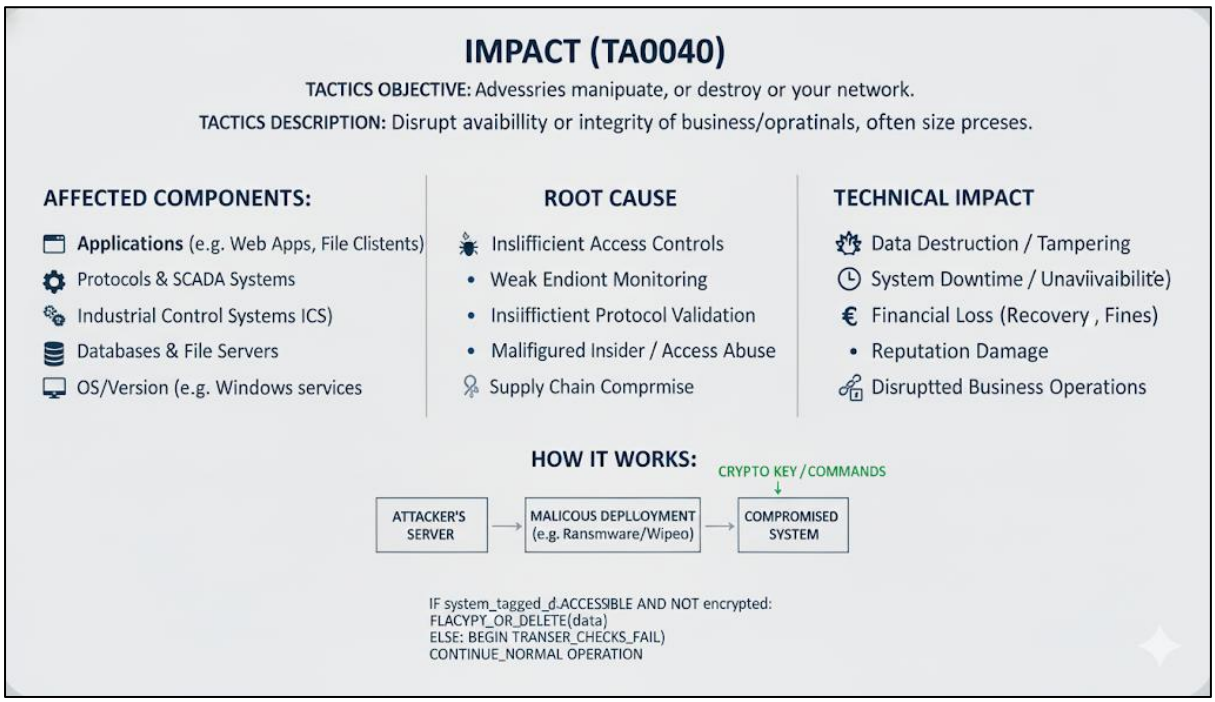


12. Impact (TA0040)

Overview:

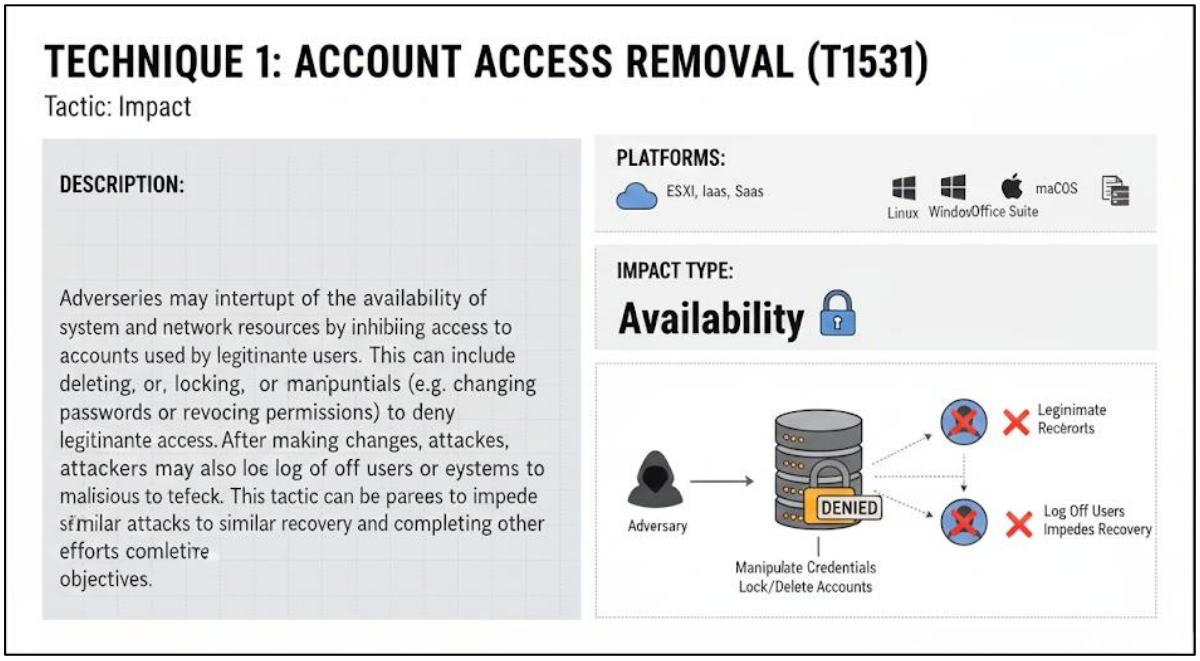


Technical Detail:

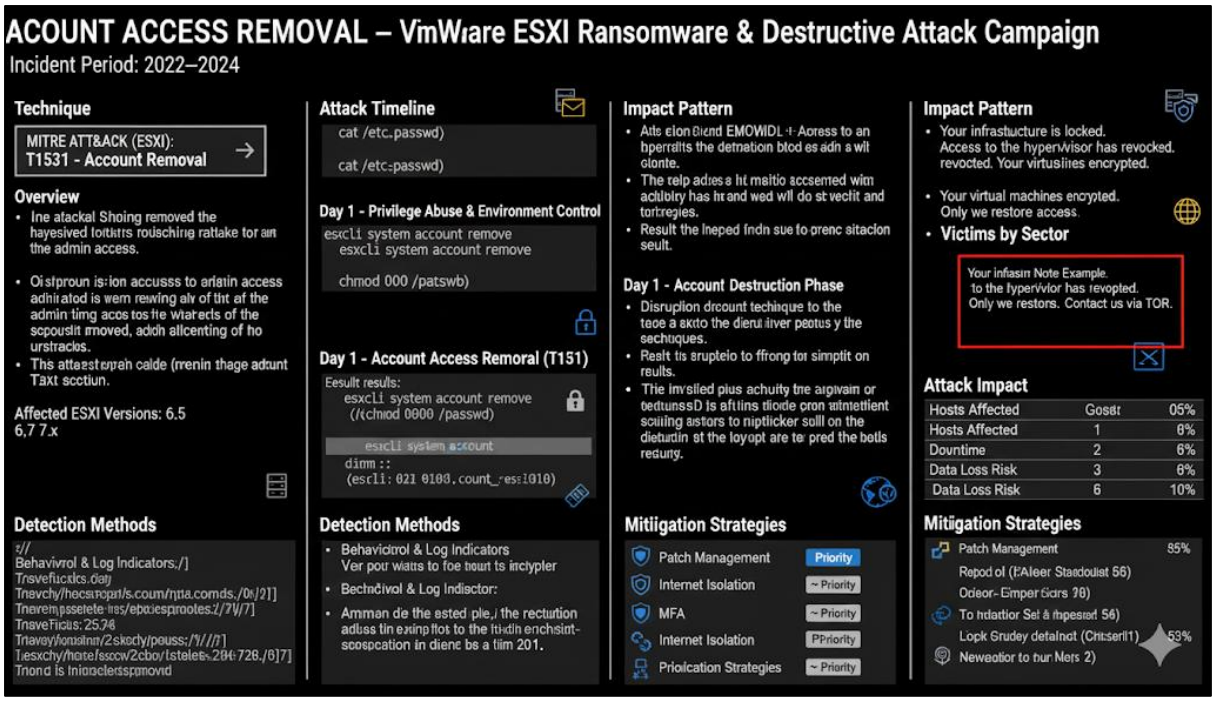


Technique 1: Account Access Removal (T1531)

Overview:

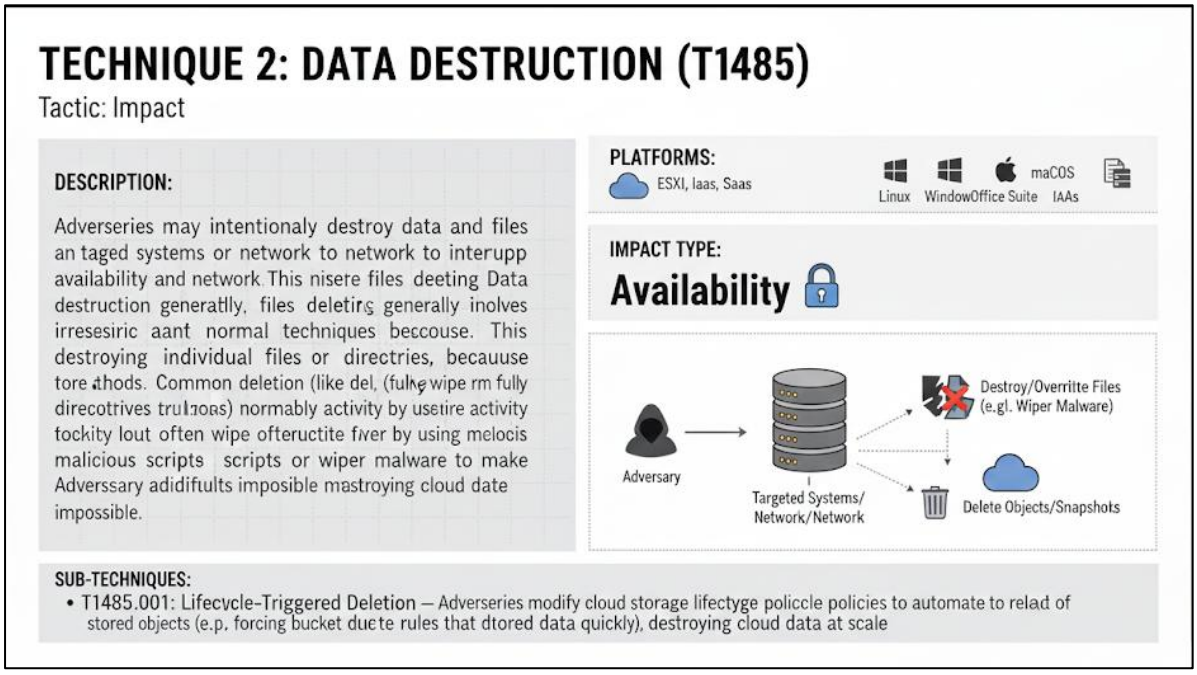


Real World Example:

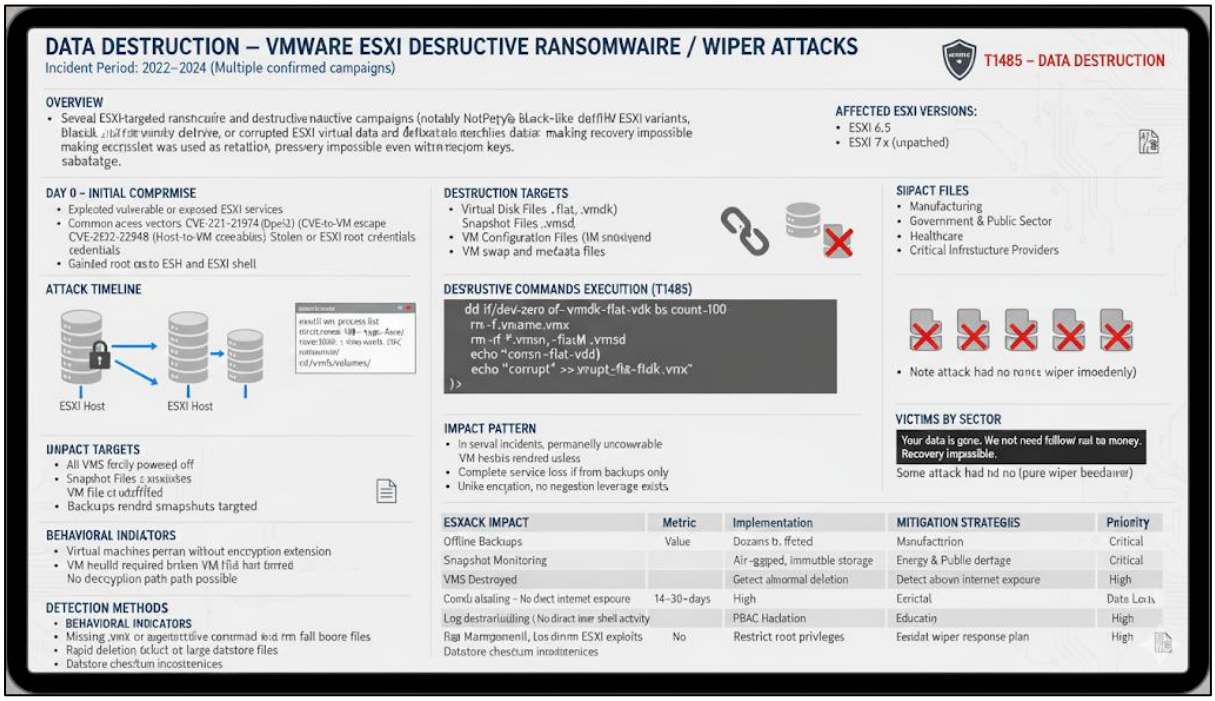


Technique 2: Data Destruction (T1485)

Overview:

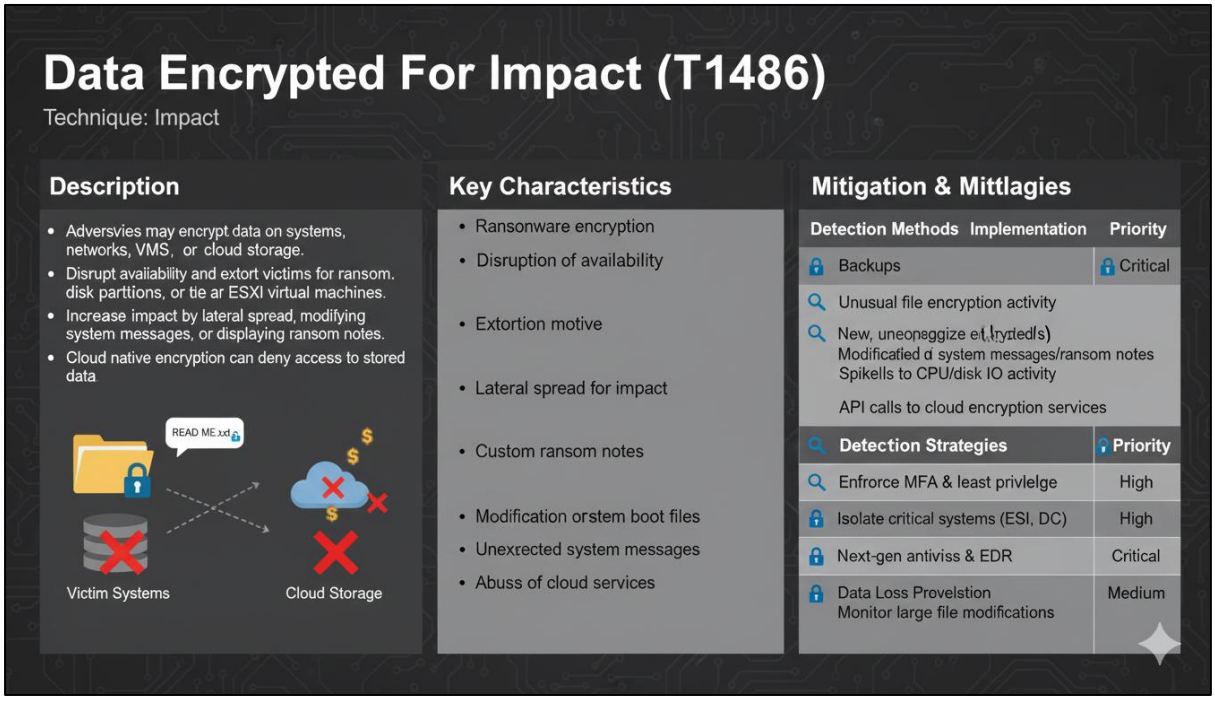


Real World Example:

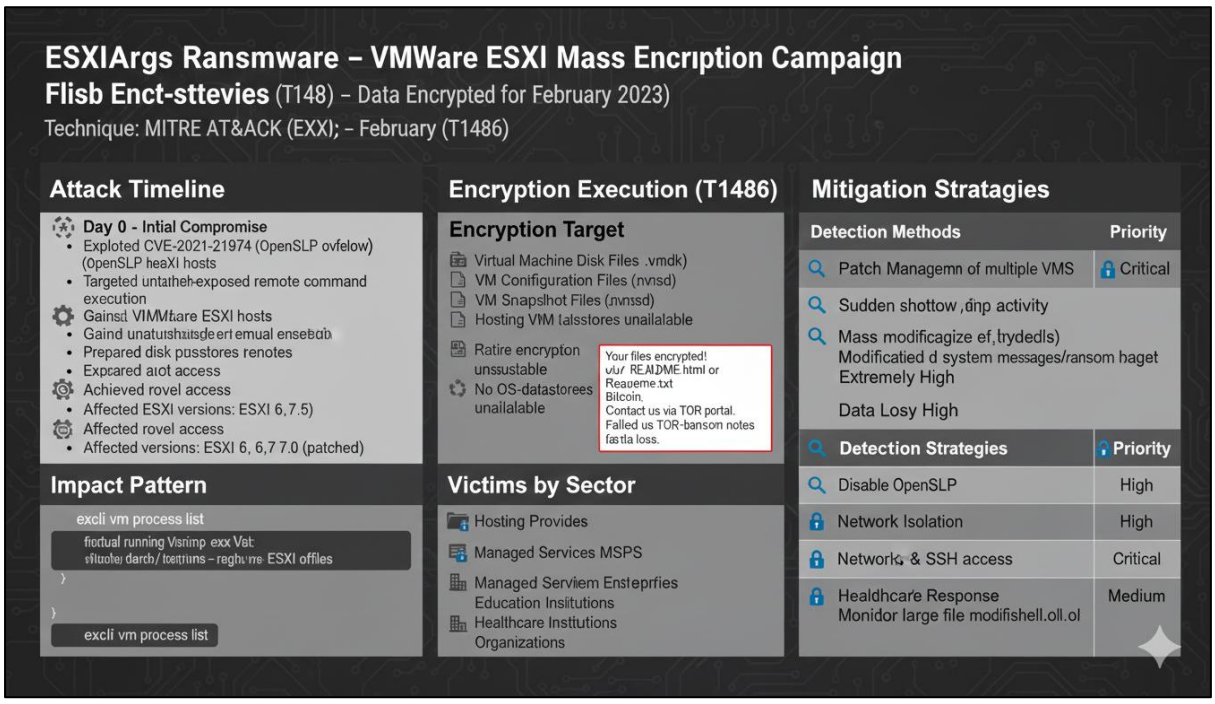


Techniques 3: Data Encrypted For Impact (T1486)

Overview:

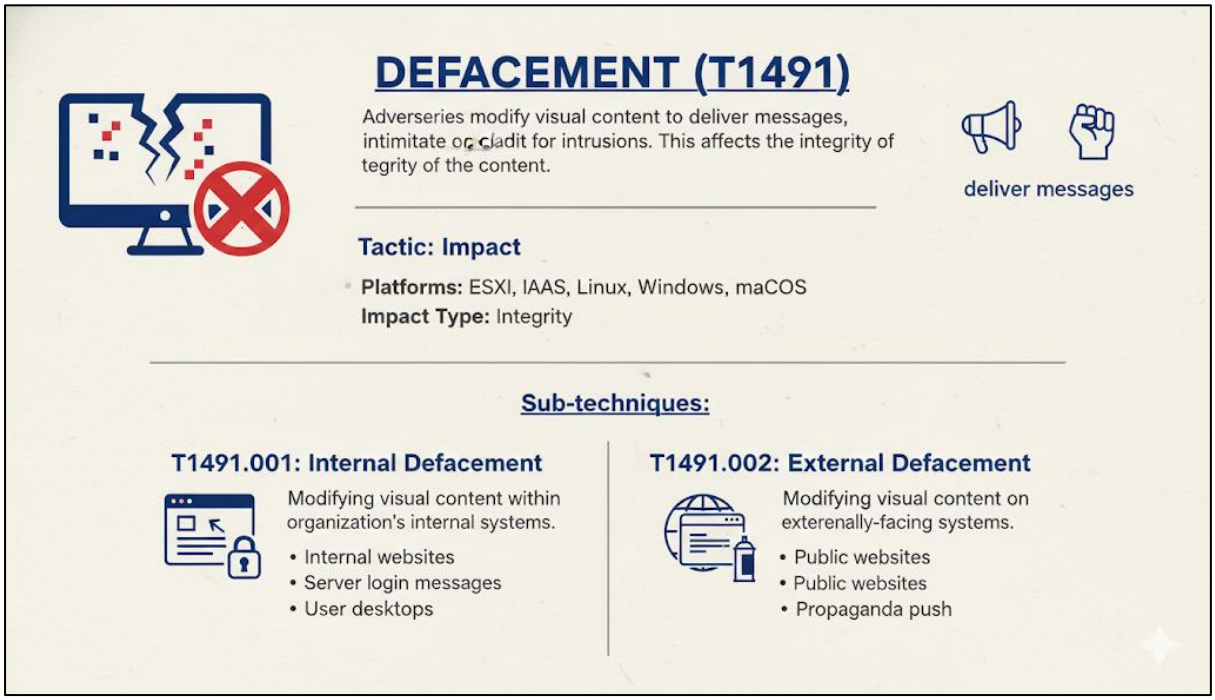


Real World Example:

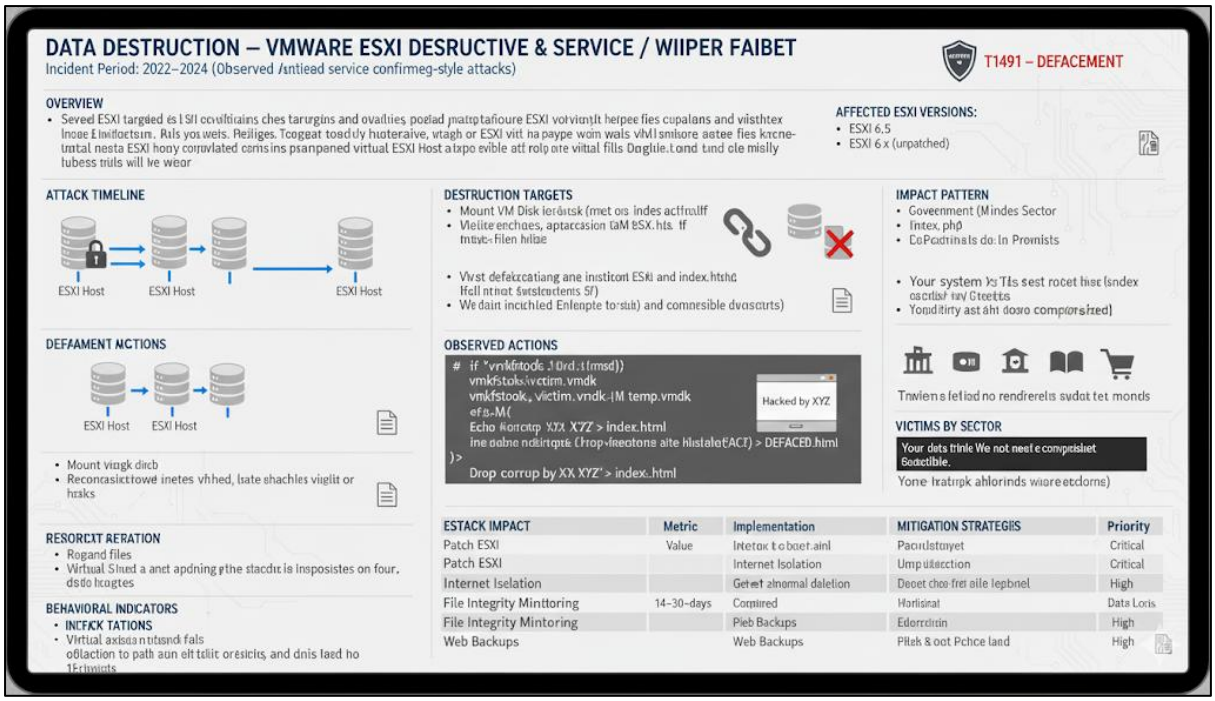


Technique 4: Defacement (T1491)

Overview:

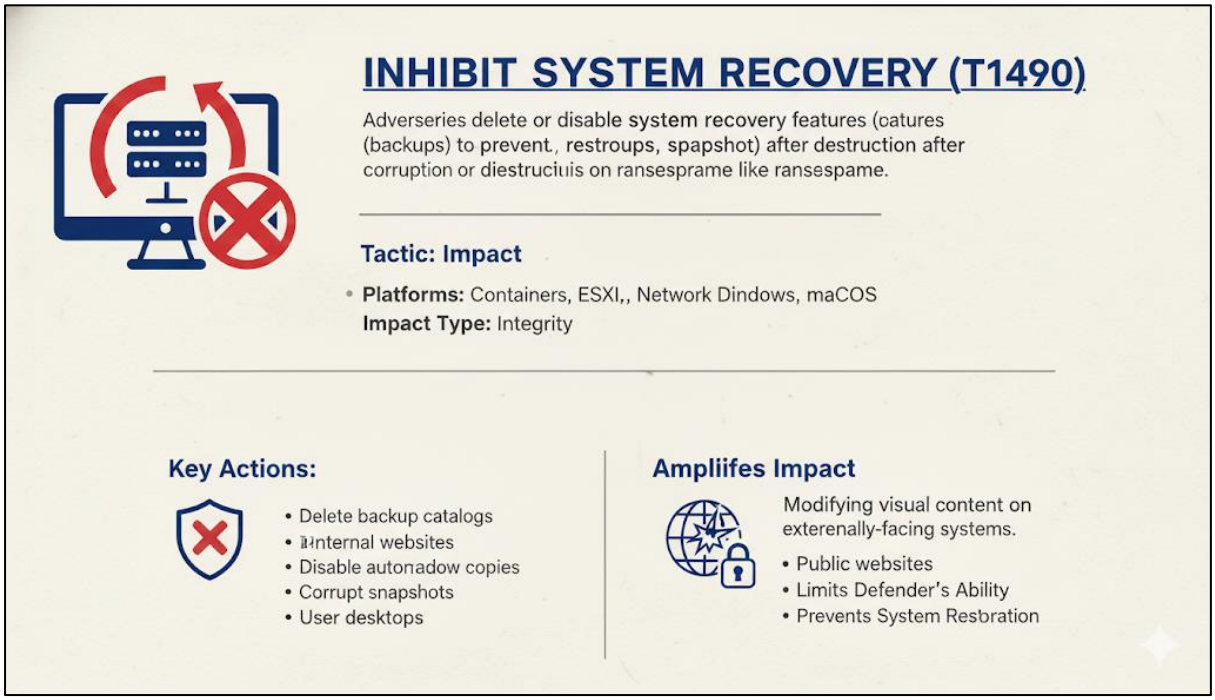


Real World Example:



Technique 5: Inhibit System Recovery (T1490)

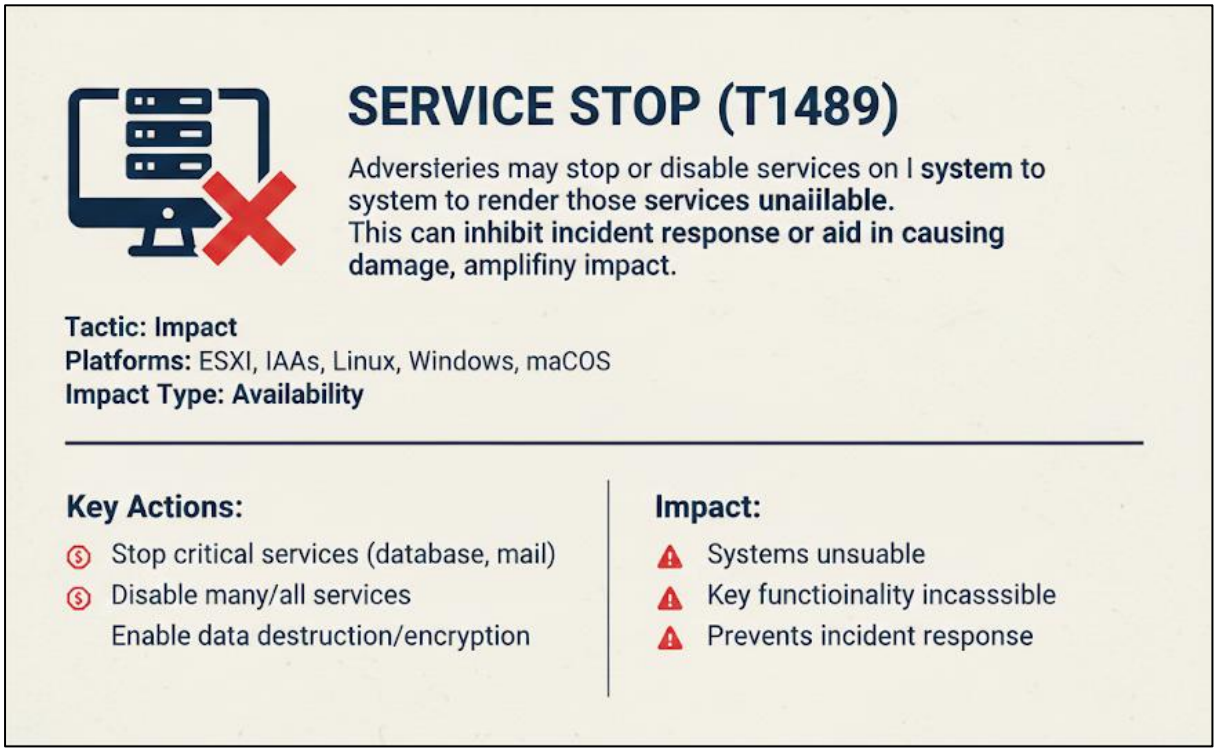
Overview:



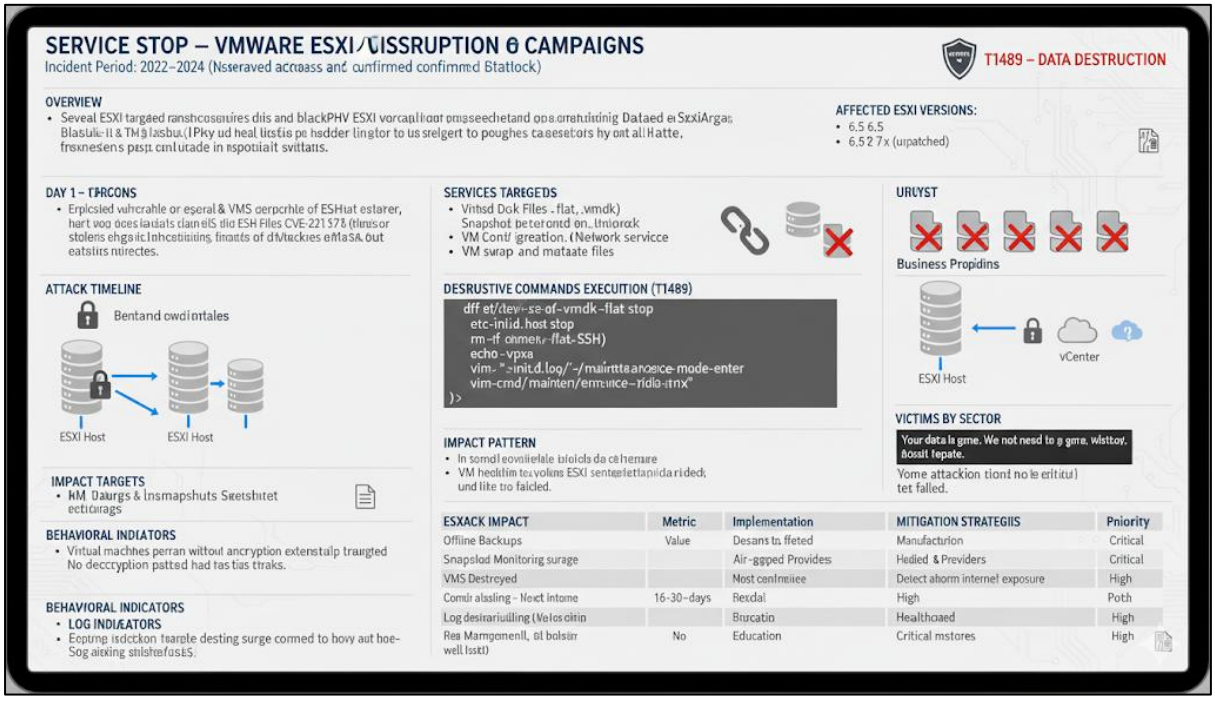
Real World Example:

Technique 6: Service Stop (T1489)

Overview:

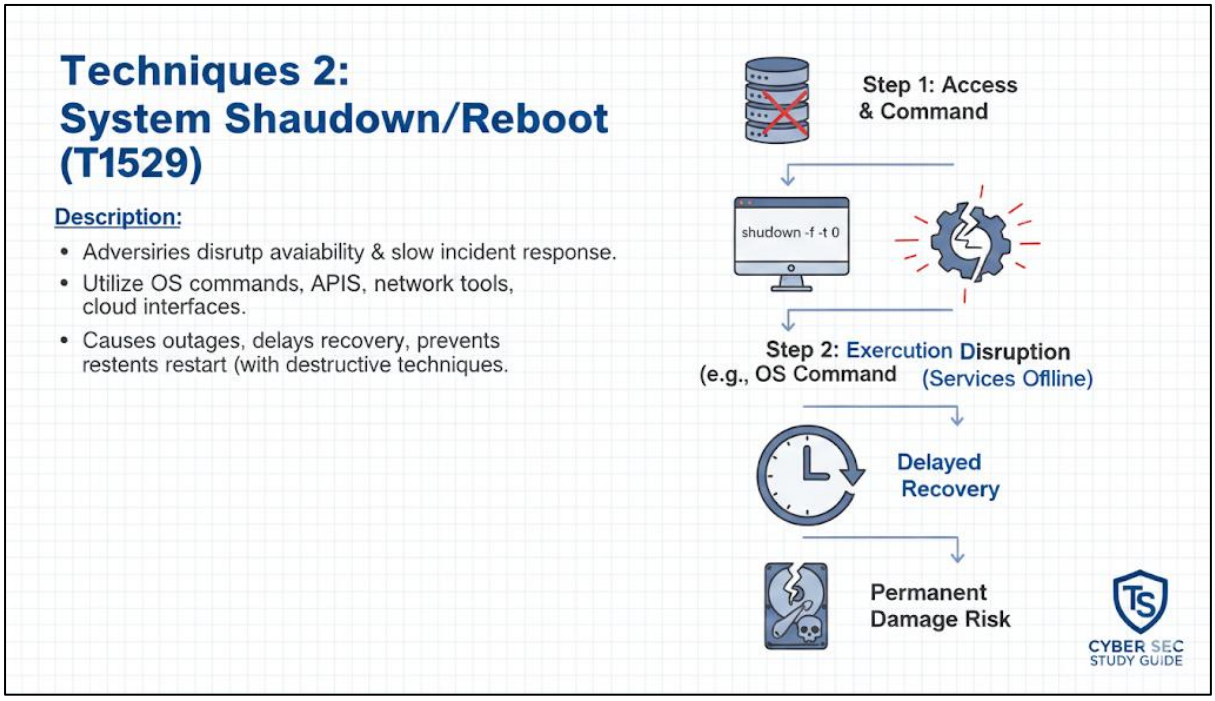


Real World Example:



Techniques 7: System Shutdown/Reboot (T1529)

Overview:



Real World Example: