



## Page 2 – MITRE ATT&CK Mapping + Detection Engineering

By: Kim Lien Chu

**Title:** MITRE ATT&CK Mapping: Step-by-Step Cheat Sheet for SOC Analysts

**Focus Area:** Translating threat intel into actionable defense for healthcare SOCs

---



### Summary

This artifact is a hands-on guide for mapping raw adversary behaviors to MITRE ATT&CK techniques, contextualizing them for healthcare environments, and aligning them with federal cybersecurity frameworks. It empowers SOC analysts to operationalize threat intelligence, build detection logic, and support defense planning in clinical settings.

---



### Skills Demonstrated

- Threat intelligence parsing and technique mapping
  - MITRE ATT&CK fluency and sector contextualization
  - Detection logic development for SIEM/XDR platforms
  - Risk alignment with HHS 405(d), CISA SRMA, and NIST CSF
  - Scenario design for tabletop exercises and staff training
- 



### Tools & Frameworks Used

- MITRE ATT&CK Navigator
  - CrowdStrike, Mandiant, CISA threat reports
  - Splunk/Sysmon detection logic references
  - HHS 405(d) Practices #4, #9, #10
  - CISA SRMA Sector Risk Profiles
-

## Artifact Walkthrough

### Step 1: Extract Adversary Behaviors

Start with threat intel and pull out raw actions:

- “Fake IT candidates gaining insider access”
  - “Use of ORB networks to mask infrastructure”
  - “Abuse of AnyDesk for persistence”
  - “Callback phishing targeting help desk”
- 

### Step 2: Identify the MITRE Technique

Use MITRE ATT&CK Navigator to map each behavior to a technique.

Behavior	Mapped Technique	Technique ID
Fake IT candidates gaining insider access	Valid Accounts	T1078
Abuse of AnyDesk for persistence	Remote Access Software	T1219
Use of ORB networks to mask infrastructure	Acquire Infrastructure: Domains	T1583.001
Callback phishing targeting help desk	Phishing: Spearphishing via Service	T1566.001

**MITRE | ATT&CK**

Metrics ▼ Tactics ▼ Techniques ▼ Defenses ▼ CTI ▼ Resources ▼ Benefactors ▼ Blog ▼ Search

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!

**TECHNIQUES**

- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts**
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts

**Sub-techniques (4)**

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.<sup>[1]</sup> Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

**ID:** T1078  
**Sub-techniques:** T1078.001, T1078.002, T1078.003, T1078.004  
**Tactics:** Defense Evasion, Persistence, Privilege Escalation, Initial Access  
**Platforms:** Containers, ESXi, IaaS, Identity Provider, Linux, Network Devices, Office Suite, SaaS, Windows, macOS  
**Contributors:** Jon Sternstein, Stern Security, Mark

*Figure 1: MITRE ATT&CK technique T1078 – Valid Accounts, confirming mapping for insider access via fake IT hires.*

**anyDesk**

Network Traffic, Data Source DS0029

... y\_time, src\_ip, dest\_ip, dest\_domain, url\_path| sort \_time desc .002 Remote Desktop Software Monitor for Outbound connections to known RMM service endpoints (e.g., teamviewer.com, anydesk.com)New connections from internal systems to unexpected IPs on:TCP 5938 (TeamViewer)TCP 7070-7071 [AnyDesk]TCP 5650 (Ammyy Admin)TCP/UDP 443, 80, or randomized ports Analytic 1 - Detect net...

Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise

... e to establish persistence.[30][31] G1043 BlackByte BlackByte modified multiple services on victim machines to enable encryption operations.[32] BlackByte has installed tools such as AnyDesk as a service on victim machines.[33] S0089 BlackEnergy One variant of BlackEnergy creates a new service using either a hard-coded or randomly generated name.[34] G0108 Blue Mockingbird Blue...

Obtain Capabilities: Tool, Sub-technique T1588.002 - Enterprise

... tained multiple publicly-available tools, including METASPLOIT, UNICORN, and NorthStar C2.[28] C0015 C0015 For C0015, the threat actors obtained a variety of tools, including AdFind, AnyDesk, and Process Hacker.[29] C0017 C0017 For C0017, APT41 obtained publicly available tools such as YSoSerial.NET, ConfuserEx, and BadPotato.[30] C0018 C0018 For C0018, the threat actors acquire...

Remote Access Tools: Remote Desktop Software, Sub-technique T1219.002 - Enterprise

... ling another computer, transmitting the display output, keyboard input, and mouse control between devices using various protocols. Desktop support software, such as VNC, Team Viewer, AnyDesk, ScreenConnect, LogMein, AmmyyAdmin, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application con...

*Figure 2: MITRE search results for “AnyDesk” confirming technique T1219 – Remote Access Software.*

**acquire infrastructure**

**Acquire Infrastructure:** Technique T1583 - Enterprise

Acquire Infrastructure Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure can be used for command and control, persistence, and data exfiltration. Examples include cloud services, virtual machines, and physical servers.

**Acquire Infrastructure:** DNS Server, Sub-technique T1583.002 - Enterprise

Acquire Infrastructure: DNS Server Adversaries may set up their own Domain Name System (DNS) servers that can be used during targeting. During post-compromise activity, adversaries may utilize DNS traffic for various tasks, such as domain resolution, reverse shell delivery, and domain fronting.

**Acquire Infrastructure:** Botnet, Sub-technique T1583.005 - Enterprise

Acquire Infrastructure: Botnet Adversaries may buy, lease, or rent a network of compromised systems that can be used during targeting. A botnet is a network of compromised systems that can be instructed to perform coordinated actions, such as distributed denial-of-service (DDoS) attacks or data exfiltration.

**Acquire Infrastructure:** Serverless, Sub-technique T1583.007 - Enterprise

Acquire Infrastructure: Serverless Adversaries may purchase and configure serverless cloud infrastructure, such as Cloudflare Workers, AWS Lambda functions, or Google Apps Scripts, that can be used during targeting. By utilizing serverless functions, adversaries can quickly spin up and tear down infrastructure without managing physical hardware.

**Acquire Infrastructure:** Domains, Sub-technique T1583.001 - Enterprise

Acquire Infrastructure: Domains Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, registered through domain registrars.

**Collection** ▼ **Command and Control** ▼ **.002** **Bypass User Account Control** Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by running the program with elevated privileges or bypassing the UAC dialog.

*Figure 3: MITRE sub-technique T1583.001 – Domains, used to mask C2 infrastructure via ORB networks.*

The screenshot shows the MITRE ATT&CK website's search interface. The search term 'callback phishing' is entered in the search bar. Below the search bar, there are several search results listed under the heading 'Techniques'.

- Phishing for Information, Technique T1598 - Enterprise**  
... shers bring along their own web pages. Retrieved October 20, 2020. Ryan Hanson. (2016, September 24). phishey. Retrieved October 23, 2020. Avertium. (n.d.). EVERYTHING YOU NEED TO KNOW ABOUT CALLBACK PHISHING. Retrieved February 2, 2023. Proofpoint. (n.d.). What Is Email Spoofing?. Retrieved February 24, 2023. Itkin, Liora. (2022, September 1). Double-bounced attacks with email spoofing. Retrieved Februa...
- Phishing for Information: Spearphishing Voice, Sub-technique T1598.004 - Enterprise**  
... ne number while also posing as a trusted entity, such as a business partner or technical support staff.[1] Victims may also receive **phishing** messages that direct them to call a phone number ('**callback phishing**') where the adversary attempts to collect confidential information.[2] Adversaries may also use information from previous reconnaissance efforts (ex: Search Open Websites/Domains or Search Victim-Own...
- Phishing Technique T1566 - Enterprise**  
... SCAMS. Retrieved February 2, 2023. CISA. (n.d.). Protecting Against Malicious Use of Remote Monitoring and Management Software. Retrieved February 2, 2023. Kristopher Russo. (n.d.). Luna Moth **Callback Phishing** Campaign. Retrieved February 2, 2023. Esler, J., Lee, M., and Williams, C. (2014, October 14). Threat Spotlight: Group 72. Retrieved January 14, 2016. Novetta. (n.d.). Operation SMN: Axiom Threat Act...
- Phishing: Spearphishing Voice, Sub-technique T1566.004 - Enterprise**  
... SCAMS. Retrieved February 2, 2023. CISA. (n.d.). Protecting Against Malicious Use of Remote Monitoring and Management Software. Retrieved February 2, 2023. Kristopher Russo. (n.d.). Luna Moth **Callback Phishing** Campaign. Retrieved February 2, 2023. Proofpoint. (n.d.). What Is Vishing?. Retrieved September 8, 2023. Parisi, T. (2022, December 2). Not a SIMulation: CrowdStrike Investigations Reveal Intrusion C...

Figure 4: MITRE technique T1566.001 – Phishing via Service, used in callback phishing targeting help desks.

### Step 3: Contextualize the Mapping

Technique ID	Name	Use Case
T1078	Valid Accounts	Insider access via fake IT hires in healthcare SOC
T1219	Remote Access Software	RMM abuse during callback phishing to maintain persistence
T1583.001	Acquire Infrastructure: Domains	ORB networks used to mask C2 targeting hospital help desks
T1566.001	Phishing: Spearphishing via Service	Callback phishing targeting help desk to reset credentials

### Step 4: Align to Sector Risks

Risk Vector	Technique	Mitigation Strategy
Insider Threat	T1078	Enhanced vetting, behavioral analytics
Remote Access Abuse	T1219	Restrict RMM usage, monitor anomalies

Infrastructure Obfuscation	T1583.001	Threat hunting, DNS anomaly detection
Social Engineering	T1566.001	Training, MFA, call-back verification

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors ▾

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!

Home > Mitigations > User Training

## User Training

User Training involves educating employees and contractors on recognizing, reporting, and preventing cyber threats that rely on human interaction, such as phishing, social engineering, and other manipulative techniques. Comprehensive training programs create a human firewall by empowering users to be an active component of the organization's cybersecurity defenses. This mitigation can be implemented through the following measures:

Create Comprehensive Training Programs:

- Design training modules tailored to the organization's risk profile, covering topics such as phishing, password management, and incident reporting.
- Provide role-specific training for high-risk employees, such as helpdesk staff or executives.

Use Simulated Exercises:

- Conduct phishing simulations to measure user susceptibility and provide targeted follow-up training.
- Run social engineering drills to evaluate employee responses and reinforce protocols.

Leverage Gamification and Engagement:

- Introduce interactive learning methods such as quizzes, gamified challenges, and rewards for successful detection and reporting of threats.

Incorporate Security Policies into Onboarding:

- Include cybersecurity training as part of the onboarding process for new employees.
- Provide easy-to-understand materials outlining acceptable use policies and reporting procedures.

Regular Refresher Courses:

- Update training materials to include emerging threats and techniques used by adversaries.
- Ensure all employees complete periodic refresher courses to stay informed.

ID: M1017  
Version: 1.3  
Created: 06 June 2019  
Last Modified: 24 December 2024

Version Permalink

MITIGATIONS

- Operating System Configuration
- Out-of-Band Communications Channel
- Password Policies
- Pre-compromise
- Privileged Account Management
- Privileged Process Integrity
- Remote Data Storage
- Restrict File and Directory Permissions
- Restrict Library Loading
- Restrict Registry Permissions
- Restrict Web-Based Content
- Software Configuration
- SSL/TLS Inspection
- Threat Intelligence Program
- Update Software
- User Account Control
- User Account Management
- User Training**
- Vulnerability Scanning
- Mobile

Figure 5: MITRE M1017 – User Training mitigation strategy for phishing and social engineering.

## Step 5: Apply in Defense Planning

Use these mappings to:

- Build SIEM/XDR detection rules
- Create tabletop scenarios for SOC teams
- Train staff on specific TTPs and red flags
- Align with HHS 405(d), CISA SRMA, and NIST CSF practices



## Use Case Scenario

During a simulated callback phishing attack at a regional hospital, analysts used this cheat sheet to rapidly identify RMM abuse, map it to T1219, and deploy detection logic in Splunk. The artifact also supported tabletop planning and staff training aligned with HHS 405(d) Practice #10.

---



## Reflection

This artifact reflects my commitment to bridging the gap between threat intelligence and operational defense. By translating raw behaviors into standardized techniques and aligning them with healthcare-specific risks, I help SOC teams move faster, smarter, and in sync with national guidance.

---



## References

1. MITRE ATT&CK Framework – <https://attack.mitre.org>
  2. MITRE M1017: User Training – <https://attack.mitre.org/mitigations/M1017>
  3. HHS 405(d) Cybersecurity Practices – <https://405d.hhs.gov>
  4. CISA Sector Risk Management Agency Guidance – <https://www.cisa.gov/srma>
  5. CrowdStrike 2025 Threat Hunting Report – Referenced for adversary behaviors and technique validation
  6. Mandiant Threat Intelligence Briefs – Used for mapping callback phishing and infrastructure tactics
  7. Sysmon + Splunk Detection Logic – Applied in simulation context for T1219 and T1078
-