MITRE ATT&CK®: BEST AND WORST PRACTICES

A BEST PRACTICE: MAPPING CYBER THREAT INTELLIGENCE TO ATT&CK

Cyber analysts use the MITRE ATT&CK framework to map real-world TTPs as part of their cyber threat intelligence strategies. The steps below are from CISA's "Best Practices for MITRE ATT&CK Mapping," which outlines key steps to successfully map CTI reports to ATT&CK. https://www.cisa.gov/uscert/best-practices-mitre-attckr-mapping

STEP 00 — UNDERSTAND MITRE ATT&CK

Ensure you know what ATT&CK is (and isn't) and how you can use it to understand adversary behavior. Visit **attack.mitre.org** to learn more about the framework.

STEP 01 — FIND THE BEHAVIOR

Search for signs of adversaries interacting with platforms or apps to help find a chain of suspicious behavior. Work to understand what led to the initial compromise and how the adversary performed the post-compromise activity.

STEP 02 — RESEARCH THE BEHAVIOR

Perform additional research to understand the context of suspicious behaviors. This may include reviewing the original source reporting, looking at technical details to better understand overall adversary behavior, or searching the ATT&CK website for key terms that help identify behaviors.

STEP 03 — IDENTIFY THE TACTICS

Review your report to identify tactics: the adversary's goals. Try to figure out what the adversary was trying to accomplish and why. Review tactic definitions in ATT&CK and compare them to the adversary's behaviors. Identify all the tactics in the report to help understand specific techniques or sub-techniques they can use to achieve that goal.

STEP 04 — IDENTIFY THE TECHNIQUES

Review the technical details in your report to understand how the adversary tried to achieve their goals. Compare this behavior with ATT&CK techniques listed under the tactic you've identified. Remember that techniques and sub-techniques are not isolated activities, but elements in the adversary's larger playbook.

STEP 05 — IDENTIFY THE SUB-TECHNIQUES

Once you've identified techniques, review sub-technique descriptions in ATT&CK and compare them to behavior outlined in the report. If one aligns, it is probably the right sub-technique. How effectively you can identify a sub-technique depends on the detail in your report.

WORST PRACTICES: AVOID THESE ATT&CK PITFALLS

MITRE ATT&CK is one tool in a cyber analyst's toolbox, but it can take some care to use. All too often, defenders try to use ATT&CK in ways in ways that might even hurt their defenses. Here are three common mistakes ATT&CK users make, along with steps you can take to avoid these pitfalls.

TRYING TO ACHIEVE 100% COVERAGE

Every organization faces its own unique cyber threats. Not every tactic or technique will apply to everyone. Instead of trying to defend against every tactic or technique in the matrix, prioritize the ones that are most relevant to you and ensure you are prepared for them.

SHOUTING "BINGO" WHEN YOU HAVE ONE TECHNIQUE

Just because you've identified a single way an adversary has done technique doesn't mean it's time to declare success and color a box green. Adversaries have multiple ways they can perform most ATT&CK techniques. It's great that you've found one, but be sure you're looking for and understand other possible ways a technique might be accomplished.

LIMITING YOURSELF TO THE MATRIX

Remember, the ATT&CK matrix only documents observed real-world, in-the-wild behaviors. But adversaries may (and probably do) have a series of other behaviors they use that have not yet been documented in ATT&CK. To get a full picture of the threats your organization faces:

1. Leverage your own intelligence sources
2. Create and document your own observed techniques
3. Don't limit yourself to behaviors, a timely indicator can still catch an adversary

MITRE | ATT&CK® Resources

attack.mitre.org

- Access ATT&CK technical information
- Contribute to ATT&CK
- Follow our blog
- Watch ATT&CK presentations

@MITREattack

mitre-att&ck

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

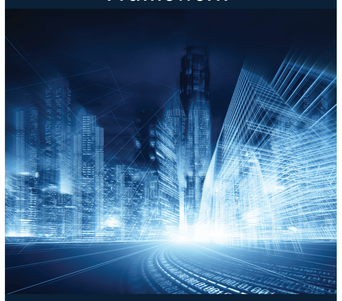
To help cyber defenders gain a common understanding of the threats they face, MITRE developed the ATT&CK framework. It's a globally-accessible knowledge base of adversary tactics and techniques based on real world observations and open source research contributed by the cyber community.

Used by organizations around the world, ATT&CK provides a shared understanding of adversary tactics, techniques and procedures and how to detect, prevent, and/or mitigate them.

ATT&CK is open and available to any person or organization for use at no charge.

For more than 60 years, MITRE has worked in the public interest. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | ATT&CK® Enterprise Framework



MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

MITRE ATT&CK® ENTERPRISE FRAMEWORK

RECONNAISSANCE
10 techniques

- Active Scanning ☰
- Gather Victim Host Information ☰
- Gather Victim Identity Information ☰
- Gather Victim Network Information ☰
- Gather Victim Org Information ☰
- Phishing for Information ☰
- Search Closed Sources ☰
- Search Open Technical Databases ☰
- Search Open Websites/Domains ☰
- Search Victim-Owned Websites

RESOURCE DEVELOPMENT
7 techniques

- Acquire Infrastructure ☰
- Compromise Accounts ☰
- Compromise Infrastructure ☰
- Develop Capabilities ☰
- Establish Accounts ☰
- Obtain Capabilities ☰
- Stage Capabilities ☰

INITIAL ACCESS
9 techniques

- Valid Accounts ☰
- Replication Through Removable Media
- Trusted Relationship
- Supply Chain Compromise ☰
- Hardware Additions
- Exploit Public-Facing Application
- Phishing ☰
- External Remote Services
- Drive-by Compromise

EXECUTION
13 techniques

- Scheduled Task/Job ☰
- Windows Management Instrumentation
- Software Deployment Tools
- Shared Modules
- User Execution ☰
- Exploitation for Client Execution
- System Services ☰
- Command and Scripting Interpreter ☰
- Native API
- Inter-Process Communication ☰
- Container Administration Command
- Deploy Container
- Serverless Execution

PERSISTENCE
19 techniques

- Valid Accounts ☰
- Hijack Execution Flow ☰
- Boot or Logon Initialization Scripts ☰
- Create or Modify System Process ☰
- Event Triggered Execution ☰
- Boot or Logon Autostart Execution ☰
- Account Manipulation ☰
- External Remote Services
- Office Application Startup ☰
- Create Account ☰
- Browser Extensions
- Traffic Signaling ☰
- BITS Jobs
- Server Software Component ☰
- Pre-OS Boot ☰
- Compromise Client Software Binary
- Internal
- Modify Authentication Process ☰

PRIVILEGE ESCALATION
13 techniques

- Process Injection ☰
- Access Token Manipulation ☰
- Abuse Elevation Control Mechanism ☰
- Domain Policy Modification ☰
- Escape to Host
- Exploitation for Privilege Escalation

DEFENSE EVASION
42 techniques

- Modify Authentication Process ☰
- Direct Volume Access
- Rootkit
- Obfuscated Files or Information ☰
- Indicator Removal on Host ☰
- Modify Registry
- Trusted Developer Utilities Proxy Execution ☰
- Traffic Signaling ☰
- Signed Script Proxy Execution ☰
- Rogue Domain Controller
- Indirect Command Execution
- BITS Jobs
- XSL Script Processing
- Template Injection
- File and Directory Permissions Modification ☰
- Virtualization/Sandbox Evasion ☰
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material ☰
- Impair Defenses ☰
- Hide Artifacts ☰
- Masquerading ☰
- Deobfuscate/Decode Files or Information
- Signed Binary Proxy Execution ☰
- Exploitation for Defense Evasion
- Execution Guardrails ☰
- Modify Cloud Compute Infrastructure ☰
- Pre-OS Boot ☰
- Subvert Trust Controls ☰
- Build Image on Host
- Deploy Container
- Modify System Image ☰
- Network Boundary Bridging ☰
- Weaken Encryption ☰
- Reflective Code Loading
- Debugger Evasion
- Plist File Modification

CREDENTIAL ACCESS
17 techniques

- Network Sniffing
- OS Credential Dumping ☰
- Input Capture ☰
- Brute Force ☰
- Two-Factor Authentication Interception
- Exploitation for Credential Access
- Steal Web Session Cookie
- Unsecured Credentials ☰
- Credentials from Password Stores ☰
- Steal or Forge Kerberos Tickets ☰
- Forced Authentication
- Steal Application Access Token
- Adversary-in-the-Middle ☰
- Forge Web Credentials ☰
- Multi-Factor Authentication Request Generation
- Steal or Forge Authentication Certificates

DISCOVERY
30 techniques

- System Service Discovery
- Application Window Discovery
- System Network Configuration Discovery ☰
- System Owner/User Discovery
- System Network Connections Discovery
- Permission Groups Discovery ☰
- File and Directory Discovery
- Peripheral Device Discovery
- Network Share Discovery
- Password Policy Discovery
- Browser Bookmark Discovery
- Virtualization/Sandbox Evasion ☰
- Cloud Service Dashboard
- Software Discovery ☰
- Query Registry
- Remote System Discovery
- Network Service Scanning
- Process Discovery
- System Information Discovery
- Account Discovery ☰
- System Time Discovery
- Domain Trust Discovery
- Cloud Service Discovery
- Container and Resource Discovery
- Cloud Infrastructure Discovery
- System Location Discovery ☰
- Cloud Storage Object Discovery
- Group Policy Discovery
- Debugger Evasion

LATERAL MOVEMENT
9 techniques

- Remote Services ☰
- Software Deployment Tools
- Replication Through Removable Media
- Internal Spearphishing
- Use Alternate Authentication Material ☰
- Lateral Tool Transfer
- Taint Shared Content
- Exploitation of Remote Services
- Remote Service Session Hijacking ☰

COLLECTION
17 techniques

- Data from Local System
- Data from Removable Media
- Input Capture ☰
- Data Staged ☰
- Screen Capture
- Email Collection ☰
- Clipboard Data
- Automated Collection
- Audio Capture
- Video Capture
- Browser Session Hijacking
- Data from Information Repositories ☰
- Adversary-in-the-Middle ☰
- Archive Collected Data ☰
- Data from Network Shared Drive
- Data from Cloud Storage Object
- Data from Configuration Repository ☰

COMMAND AND CONTROL
16 techniques

- Data Obfuscation ☰
- Fallback Channels
- Application Layer Protocol ☰
- Proxy ☰
- Communication Through Removable Media
- Web Service ☰
- Multi-Stage Channels
- Ingress Tool Transfer
- Data Encoding ☰
- Traffic Signaling ☰
- Remote Access Software
- Dynamic Resolution ☰
- Non-Standard Port
- Protocol Tunneling
- Encrypted Channel ☰
- Non-Application Layer Protocol

EXFILTRATION
9 techniques

- Exfiltration Over Other Network Medium ☰
- Scheduled Transfer
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Physical Medium ☰
- Exfiltration Over Web Service ☰
- Automated Exfiltration ☰
- Exfiltration Over Alternative Protocol ☰
- Transfer Data to Cloud Account

IMPACT
13 techniques

- Data Destruction
- Data Encrypted for Impact
- Service Stop
- Inhibit System Recovery
- Defacement ☰
- Firmware Corruption
- Resource Hijacking
- Network Denial of Service ☰
- Endpoint Denial of Service ☰
- System Shutdown/Reboot
- Account Access Removal
- Disk Wipe ☰
- Data Manipulation ☰

☰ Has sub-techniques

MITRE | ATT&CK®

attack.mitre.org

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®