THE MITRE ATT&CK FRAMEWORK EXPLAINED

The MITRE ATT&ACK framework is a free, globally-accessible resource that can help guide organizations through assumed security breach incidents—and it can shift the organizational culture around risk management.

The MITRE ATT&CK framework is based on documented knowledge around:

- Adversary/attacker behaviors
- Threat models
- Techniques
- Mitigation tactics

The idea is that by understanding the myriad ways that attackers actually attack, organizations can better prepare for the risks.

In this article, we will discuss what the MITRE ATT&CK Framework is and how the framework can support your security initiatives.

What is the MITRE ATT&CK framework?

The ATT&CK framework provides the attacker perspective on each stage of the cyberattack lifecycle, from end to end.

MITRE | ATT&CK®

MITRE ATT&CK was developed by the non-profit organization MITRE in 2013 as a community-led initiative. Its name derives from the acronym for Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

The concept—using an end-to-end cyberattack taxonomy as a reference to gain intruder perspective—is not new. (The Lockheed Martin Cyber Kill Chain is another popular framework to model and understand attacker behavior.)

Previously, such extensive information was only available in two ways:

- Through expert cybersecurity incident responders with vast experience.
- As classified documentation in large enterprises regularly addressing Advanced Persistent Threats (APTs) with a dedicated, internal security workforce.

But the ATT&CK framework is unique for the way it drills down into the various attack techniques and procedures used in specific examples, suggesting appropriate mitigation strategies and standardizing language. So, the value proposition of using the MITRE ATT&CK framework has three key points:

1. In-depth real-life examples of relevant and appropriate adversary behaviors
2. Environment-specific attack techniques and methods
3. Standardized language for various attacker methodologies

The framework enables visibility and access, enabling cybersecurity personnel to identify and react to a variety of cybersecurity risks with the right risk management approach. The ATT&CK framework covers several cybersecurity disciplines, including:

- Detection
- Intelligence
- Containment
- Risk management
- Security engineering

The MITRE ATT&CK framework covers mobile, enterprise (cloud), and pre-exploit stages for a variety of cybersecurity disciplines, including:

Who can use the ATT&CK framework?

In terms of who uses this framework, the knowledge can help guide any organization, be it private, non-profit, or government.

The MITRE ATT&CK framework has supports for both mobile and enterprise environments. The true separation, though, is by operating system. The currently supported operating systems are:

- **Enterprise:** PRE, Windows, macOS, Linux, Cloud & Network
- **Mobile:** Android & iOS

Other operating systems, including z/OS, aren't available but may be added in the future.

The ATT&CK Matrix for Enterprise

The ATT&CK Matrix categorizes various tactics that adversaries use across different stages of the attack. Think of the matrix as a reference spreadsheet that describes how these techniques can accomplish a specific task or goal across the various stages of an attack.

What follows are the 14 categories of enterprise tactics across the attack lifecycle. We've included a few examples, though the full matrix categories offer comprehensive techniques.

Reconnaissance (10 techniques)

The first step of the attacker lifecycle is collecting information to facilitate targeting. Example techniques the attackers might use here include:

- Active scanning
- Phishing
- Gathering victim-related information

Resource Development (6 techniques)

In the resource development phase, the adversary establishes resources and capabilities necessary to execute a cyberattack. Some techniques here include:

- Acquiring and/or compromising infrastructure
- Compromising or establishing accounts
- Developing capabilities

Initial Access (9 techniques)

This stage is about the adversary's initial attempts to access an IT network. Common techniques to gain foothold within the network, such as:

- Drive-by compromise
- Spearphishing
- Exploiting external remote services and weak passwords

Attackers can use these compromised accounts and vulnerabilities to execute wider attacks later.

Execution (10 techniques)

In the execution phase, adversaries run malicious code on the target network. They may do this by compromising built-in scripting environments and interpreters to run custom code for network exploration, stealing data and credentials.

Common target interpreters include:

- PowerShell, Windows Command Shell and Unix Shell
- Python and JavaScript installations

Persistence (18 techniques)

Here, the adversary tries to maintain a foothold and evade defense attempts.

Once a code script is executed, the adversaries can prevent defensive actions (from your organization) that would interrupt the attack lifecycle. These interruptions may be caused by system restarts, credential changes, and configuration resets.

Adversaries persist using techniques such as:

- Manipulating accounts
- Modifying SSH authentication keys, authentication packages, services, and registry

weaknesses

Privilege Escalation (12 techniques)

Privilege escalation occurs when the attackers obtain access to elevated permissions in the network, such as root and admin access privileges. Techniques include:

- Sudo caching
- Bypassing user access controls
- Port monitoring

Defense Evasion (37 techniques)

Now, the adversaries avoid detection by disabling or uninstalling security systems and scripts. They masquerade malicious activities under known and trusted processes that go under the radar, subverting potential defenses.

Common techniques in this phase include:

- Abuse elevation control mechanism
- Elevated execution
- Token impersonation

Credential Access (15 techniques)

Credential access is the stage when attackers steal account credentials.

Attackers use techniques like keylogging, brute force, password cracking—even guessing—to access systems and approve rogue accounts within the network.

Discovery (25 techniques)

Adversaries discover the wider network and understand which entry points and corresponding network environments are most suitable for their objectives post-compromise.

Examples here include:

- Accounts discovery
- Infrastructure and cloud service discovery
- Network sniffing
- Policy and permission groups discovery

Lateral Movement (9 techniques)

In this stage, the adversaries move laterally across the network environment, pivoting between systems and accounts for stealthier operations. The process involves compromising more legitimate credentials as well as network and default OS tools.

Techniques include:

- Internal spearphishing
- Remote service exploitation

- SSH hijacking

Collection (17 techniques)

Adversaries gather information and sources necessary to steal and exfiltrate data, including but certainly not limited to emails, keyboard input, databases, and archives.

Command & Control (16 techniques)

At this stage, the attackers control the network and systems with various levels of stealth. The systems act upon commands from the adversary and mimic normal network behavior to avoid possible detection.

The attackers communicate the commands using:

- Existing application layer protocols
- Data encoding
- Data obfuscation
- Multi-stage channels

Exfiltration (9 techniques)

In this phase, the attackers finally exfiltrate relevant data from the compromised network. The data is often compressed and encrypted before transferring it outside the network.

Common techniques in this phase include:

- Automated exfiltration
- Exfiltration over web services or physical medium

Impact (13 techniques)

The attack lifecycle ends with manipulating, disrupting, or destroying compromised systems, network components, accounts, and data. Techniques in this stage can include:

- Account access removal
- Data destruction
- Data encryption and manipulation
- Disk wipes
- Denial of Service attacks on the network
- Resource hijacking

MITRE ATT&CK and the mainframe

Although the ATT&CK matrix doesn't yet include the mainframe, organizations can leverage the framework's knowledge of behaviors. The mainframe is like any other system in your environment—it is susceptible to attacks from within and outside your perimeter. The behaviors and methods of attackers share many characteristics, no matter the system they are attempting to compromise.

By being aware of these behaviors and methods, you can harden your defenses and determine when a potential threat event should be rapidly investigated by your operations and security teams.

(Learn how a truly self-managing mainframe is possible.)

Related reading

- BMC Security & Compliance Blog
- Connecting the Mainframe to Your XDR Strategy
- Digital Forensics & Incident Response (DFIR): An Introduction
- Forrester: A False Sense of Mainframe Security