GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Ekran System

Title: "How Can MITRE ATT&CK Help You Mitigate Cyber Attacks?S"

Website: EkranSystem.com

Organization: Ekran System

Date: 21 February 2019

URL: https://www.ekransystem.com/en/blog/mitre-attack-mitigate-cyber-attacks

Accessed: 21 Oct 2019

Synopsis: The number of cyber attacks and data breaches is increasing with every passing day, but security teams are often not ready to detect all security gaps in their organizations. The scope of their monitoring is usually so broad that it's difficult to anticipate where a potential threat might come from.

However, identifying security gaps is easier if the security team can understand the logic of adversaries. Fortunately, the MITRE ATT&CK framework provides a comprehensive approach to better detect and mitigate adversarial behavior.

The MITRE ATT&CK model

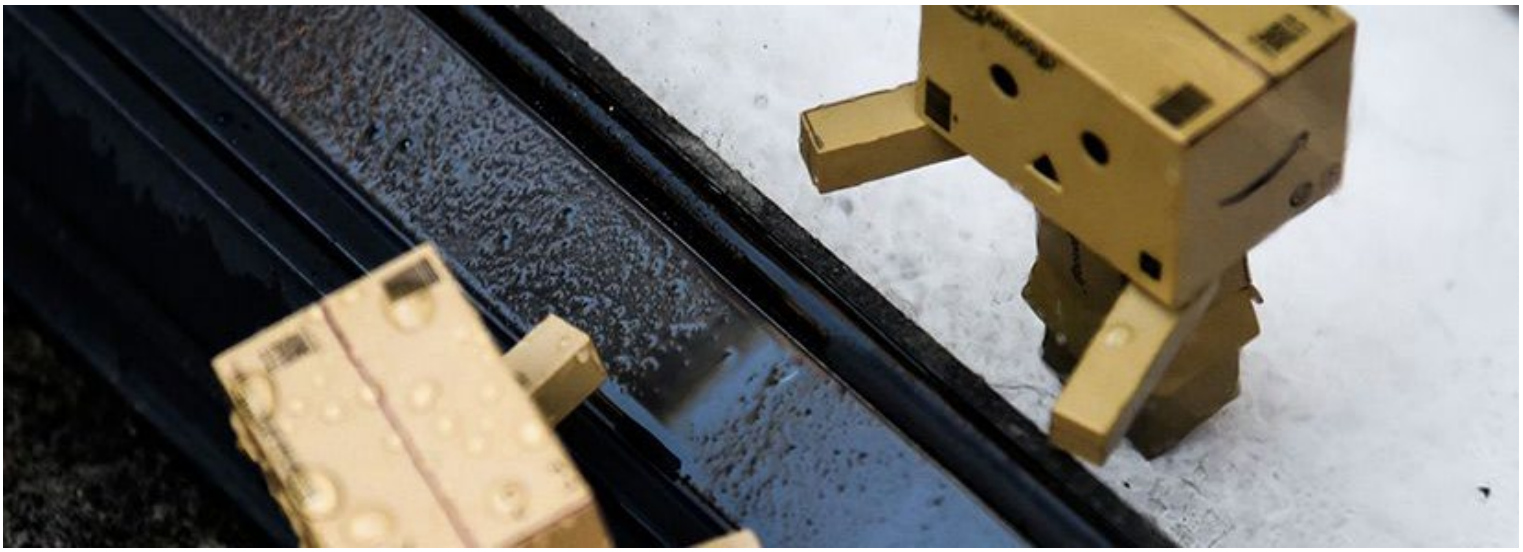
ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. It's a knowledge base of adversarial tactics, techniques, and procedures that reflect various phases of a hacker attack lifecycle. The framework was initially designed to structure adversarial behavior for conducting penetration testing. But using ATT&CK to advance cyber threat models, security officers can understand an attacker's actions better and ensure timely incident detection and mitigation.

Particularly, the ATT&CK framework allows you to go beyond traditional indicators of compromise and move to behavioral detection analytics. It provides security teams with prior knowledge of how adversaries interact with particular platforms to achieve their malicious goals.

February 21, 2019

How Can MITRE ATT&CK Help You Mitigate Cyber Attacks?

Category: Security



The number of cyber attacks and data breaches is increasing with every passing day, but security teams are often not ready to detect all security gaps in their organizations. The scope of their monitoring is usually so broad that it's difficult to anticipate where a potential threat might come from.

However, identifying security gaps is easier if the security team can understand the logic of adversaries. Fortunately, the MITRE ATT&CK framework provides a comprehensive approach to better detect and mitigate adversarial behavior.

The MITRE ATT&CK model

ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge. It's a knowledge base of adversarial tactics, techniques, and procedures that reflect various phases of a hacker attack lifecycle. The framework was initially designed to structure adversarial behavior for conducting penetration testing. But using ATT&CK to advance cyber threat models, security officers can understand an attacker's actions better and ensure timely incident detection and mitigation.

Particularly, the ATT&CK framework allows you to go beyond traditional indicators of compromise and move to behavioral

The MITRE ATT&CK model structures adversarial behavior into matrices to show relations between different tactics and techniques used by attackers and the ways you can effectively mitigate these attacks.

As of today, MITRE has created three collections of matrices associated with different subject matters:

PRE-ATT&CK showcases an attacker's behavior before an actual attack happens. The described techniques can be applied to any platform.
ATT&CK for Enterprise contains data on adversarial tactics and techniques used during the post-exploit stages for Windows, Linux, and Mac.
ATT&CK for Mobile unites pre- and post-exploit knowledge for iOS and Android.

So let's look closer at how these matrices are organized.

Each matrix includes a set of tactics and techniques that attackers may use for achieving their malicious goals at a particular stage of an attack. Tactics describe what an adversary is trying to achieve, while techniques explain how they accomplish their goals. Each tactic includes a range of techniques that can be used by an attacker.

All information on techniques is structured in the following way:

The **data sources** section specifies digital data sources where you can identify the execution of a particular technique.
The **examples** section lists all known incidents when this particular technique was used by adversaries.
The **mitigation** section provides advice on what measures you should take to prevent the execution of a certain technique.
The **detection** section suggests what kind of processes should be monitored in order to detect this technique.
The **references** section provides links to additional resources for deeper analysis.

Adversaries won't necessarily use all the tactics described in the ATT&CK matrices. Probably, an adversary will execute the minimum number of tactics and techniques in order to remain unnoticed while achieving their goals.

ATT&CK for enterprise

In this section, we'll discuss how you can use the ATT&CK Enterprise matrix to enhance the security of your organization. However, MITRE has recently worked on **integrating some of the PRE-ATT&CK techniques into ATT&CK** for Enterprise in order to add more clarity about how adversaries get initial access to a network, increasing the potential of network defense teams.

By mastering the MITRE ATT&CK matrix for enterprises, you can find answers to the following questions:

What adversarial behaviors are common across most attacks?
What is the evidence of adversarial behavior?

How do attackers act?
What user behaviors can be considered abnormal and suspicious?

The answers to these questions will help you understand what you need to look for to detect users who behave suspiciously and how to mitigate their malicious actions. The ATT&CK framework can be used as a starting tool for an organization to develop behavioral analytics for detecting malicious behavior within an organization's environment.

Currently, the ATT&CK for Enterprise matrix contains 11 tactics and more than 200 techniques adversaries use for compromising an organization's network and operating within it. Understanding these tactics can allow security officers to prioritize their corporate network defense strategies.

Here is what the ATT&CK Enterprise matrix looks like:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

Image credit: MITRE ATT&CK

Initial access refers to the vectors hackers exploit to access the targeted network or system.
Execution contains techniques aimed at executing malicious code after penetrating the network.
Persistence allows attackers to execute their malicious activity on the network.
Privilege escalation is necessary for adversaries to get permissions that allow them to access sensitive data.
Defense evasion allows penetrators to go unnoticed by intrusion detection software.
Credential access includes techniques aimed at obtaining credentials of privileged users for establishing an attacker's control over the system or network.
Discovery tactic lets adversaries orient themselves in the targeted system.
Lateral movement is used by hackers to ensure remote system access and control.
Collection includes techniques that attackers use for gathering targeted data across the system.
Exfiltration allows adversaries to remove sensitive data from the targeted system.
Command and control shows how attackers establish communication between the compromised network and the system under their control.

Let's consider one of these tactics, initial access. In order for an adversary to access the targeted system or network, they will apply one or more of the techniques listed in the initial access column, such as using a spearphishing link or a valid account. You may think that this ATT&CK matrix works only for outsider threats, but it is also used for behavioral analytics inside your organization.

Applying the ATT&CK matrix for cyber threat detection

Let's take a detailed look at how the ATT&CK tactics and techniques work for detecting and mitigating data beaches. For example, let's say that a malicious insider wants to send trade secrets to a competitor by email. In order to accomplish this

goal, the **opportunistic employee** needs to successfully execute several intermediate actions.

First, an insider will need to obtain access to sensitive data. This may be done using the **privilege escalation** tactic, for example. Now, they can use a technique such as *bypassing user account control* to elevate their privileges to administrator. If an attacker knows the credentials for an account with administrator privileges, they can also bypass user account control through some **lateral movement** techniques. To detect the account control bypass technique, security analysts should apply the following types of monitoring:

> Identification monitoring: Failed multi-factor authentication attempts
> Activity monitoring: Anomalies in session context (time, location, IP and host addresses, “leapfrog” connections, activity anomalies)

To mitigate this attack, you can use high-risk alerts for privilege elevation commands and user account manipulations.

Collection is the next tactic that an insider needs to use. For instance, they may use the *data from local system* technique for collecting sensitive data from local system sources, such as the file system or databases. At this stage, an adversary can be detected by monitoring sensitive files, including access to and operations on them.

If the previous tactic was successfully executed by a malicious insider, they come to the **exfiltration** tactic. To transmit data to a competitor, an insider may use *data compression* to make the data more portable by reducing its size and possibly renaming it to complicate tracking. To transfer trade secrets over the network, an adversary may use the *scheduled transfer* technique and send small portions of data at certain intervals. File compression can be detected through process monitoring, while sending fixed-size data packets at regular intervals can be detected by analyzing network traffic for uncommon data flows.

Data breach arranged by an insider

Tactics

Privilege escalation	
Techniques	Bypass user accounts control by using valid accounts: use a colleague's privileged credentials OR misuse granted privileged credentials OR perform unauthorized privilege elevation operation
Attacker's actions	*Elevating user privileges*
Detection	Identification monitoring: failed multi-factor authentication attempts Activity monitoring: anomalies in the session context (time, location, IP and host addresses, "leapfrog" connections, activity anomalies) high-risk alerts (privilege elevation commands, user account manipulations)
Lateral movement	

Collection	
Techniques	Data from the local system
Attacker's actions	*Collecting sensitive data from the local system*
Detection	File monitoring
Exfiltration	
Techniques	Data compression
Attacker's actions	*Reducing the size of sensitive data*
Detection	Process monitoring
Scheduled transfer	
Techniques	*Email monitoring, network traffic analysis*
Attacker's actions	Sending mall portions of stolen data at certain intervals

Benefit from combining Ekran System and ATT&CK

The ATT&CK matrix for enterprises describes what an attacker usually does after they enter your corporate network. Ekran System, in turn, provides you with a set of helpful tools for both preventing and mitigating cybersecurity threats. Using these two solutions together, you can enhance your organization’s defenses to counteract adversarial actions at any stages of the attack lifecycle.

Ekran System includes identity management and access management tools to prevent Bypassing of User Control and similar techniques. Ekran System also provides you with a number of monitoring and alerting (incident response) tools that you can set up the way you need to ensure full visibility of your infrastructure. With the help of these tools, you can transparently address adversarial tactics described in MITRE ATT&CK for enterprises.

For instance, with Ekran System’s multi-factor authentication feature, you can make sure that users logging into your network are who they claim to be. In case any malicious action is detected, you’ll be immediately notified with a well-tuned alert system. Using the MITRE recommendations, you can configure Ekran’s flexible and transparent alert system to respond to suspicious events better. The incident response module provided by Ekran System allows you to terminate suspicious actions or block a compromised user account altogether.

All collected data is recorded in the form of indexed video, which makes Ekran System a comprehensive and easy-to-use tool for researching adversarial tactics, applying the honeypot technique, mitigating cyber attacks, detecting their sources, and preventing new security incidents from happening.

Conclusion

The MITRE ATT&CK framework is a useful knowledge base that systematizes information about tactics and techniques used by cyber attackers for penetrating enterprise networks. ATT&CK has already proven to be a trusted data source for

security officers who work on behavioral analytics. Using this framework in addition to Ekran System will help you define what user behavior and system security gaps to focus on to improve the cybersecurity of your corporate network.

Rating:

Average: 5 (1 vote)

YOU MAY ALSO LIKE

How to Build an Insider Threat Program [12-step Checklist]

February 19, 2019

A functional insider threat program is a core part of any modern cybersecurity strategy. Having controls in place to prevent, detect, and remediate insider attacks and inadverte…

Ekran System, Inc. Goes West, Continues North American Expansion

February 06, 2019

Ekran System, Inc., a leading insider threat prevention software vendor, is happy to announce the opening of a new sales support office in Texas. Since 2013, Ekran System…