MITRE ATT&CK Defender: Fundamentals For CTI

LESSON 1 Understanding ATT&CK Fundamentals:

Objectives:

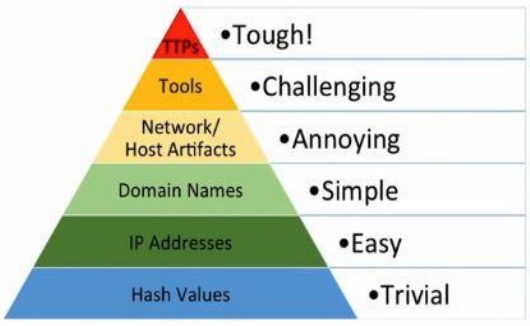
- Understand the background and motivation for ATT&CK – understanding ATT&CK
- Identify what information is captured in ATT&CK – Benefits of using ATT&CK
- Recognize the structure of ATT&CK – Operationalizing ATT&CK

Important References for Analysis of ATTACKS:

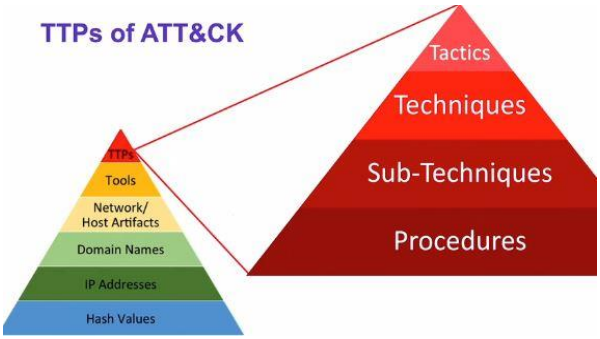
- **MITRE ATT&CK -** https://attack.mitre.org/matrices/enterprise/
- **MITRE Engage -** https://engage.mitre.org/matrix/
- **MITRE Cyber Analytics Repository -** https://car.mitre.org/analytics/
- **MITRE Engenuity -** https://mitre-engenuity.org/attackevaluations/
- **CTID MITRE Engenuity -** https://ctid.mitre-engenuity.org/
- **Adversary Emulation Plans -** https://attack.mitre.org/resources/adversary-emulation-plans/
- **MITRE ATT&CK Data Sources -** https://github.com/mitre-attack/attack-datasources
- **MITRE CTI -** https://github.com/mitre/cti
- **ATT&CK Navigator-** https://mitre-attack.github.io/attack-navigator/

Important to Remember:

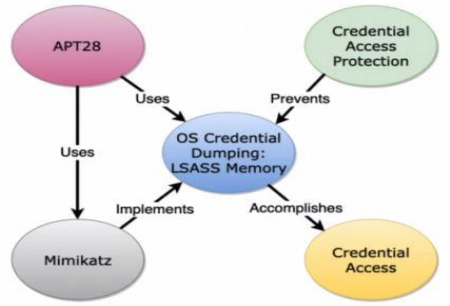
Pyramid of Pain –



This pyramid helps in identifying IOCs along with TTPs of the ATTACK.



A quick Example of APT28 which when analysed using MITRE ATT&CK analysis and pyramid of pain for TTPs, may look something like this mentioned below:



MITRE ATT&CK Matrices:

The matric view captures relationship between tactics, techniques and sub-techniques. Each matric focuses on a specific “technology domain – also available for MacOS, Android, iOS, Cloud, Containers, Linux other than just Enterprise”. ATT&CK matrices are unique, but often overlap.

Tactics: Each tactic is assigned an ID as well as a short and longer description. ATT&CK Tactic is an intermediate objective of the adversary.

Some Examples of Tactics in MITRE ATT&CK are – Initial Access; Persistence; Defense Evasion; Lateral Movement; Collection; etc

Techniques & Sub-Techniques: Techniques means by which adversaries achieve their tactical goal; how an adversary performs each action. List of techniques may differ across platforms, but may grow and evolve over time. Techniques do have a unique identifiers – technique IDs.

Some Examples of Techniques & Sub-Techniques in MITRE ATT&CK are –

Tactics - Execution

Techniques – Command and Scripting Interpreter

Sub-Techniques – Command and Scripting Interpreter: PowerShell

Sub- Techniques: Gives more specific description of the adversarial behaviour used to achieve a goal. It describes behaviour at a lower level than a technique, it is designed to help reduce changes to techniques as new variations and platforms are added.

Mitigations: Configurations, tools, or processes that can prevent a techniques from working or having the desired outcome for an adversary. It is intended to allow you to take an action such as changing a policy or deploying a tool.

Mitigations

Mitigation	Description
Antivirus/Antimalware	Anti-virus can be used to automatically quarantine suspicious files.
Code Signing	Where possible, only permit execution of signed scripts.
Disable or Remove Feature or Program	Disable or remove any unnecessary or unused shells or interpreters.
Execution Prevention	Use application control where appropriate.
Privileged Account Management	When PowerShell is necessary, restrict PowerShell execution policy to administrators. Be aware that there are methods of bypassing the PowerShell execution policy, depending on environment configuration.[1]
Restrict Web-Based Content	Script blocking extensions can help prevent the execution of scripts and HTA files that may commonly be used during the exploitation process. For malicious code served up through ads, adblockers can help prevent that code from executing in the first place.

Below is where this highlighted mitigation is addressed.

Disable or Remove Feature or Program

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

ID: M1042
Version: 1.1
Created: 11 June 2019
Last Modified: 31 March 2020

Techniques Addressed by Mitigation

Domain	ID		Name	Use
Enterprise	T1098	.004	Account Manipulation: SSH Authorized Keys	Disable SSH if it is not necessary on a host or restrict SSH access for specific users/groups using `/etc/ssh/sshd_config`.
Enterprise	T1547	.007	Boot or Logon Autostart Execution: Re-opened Applications	This feature can be disabled entirely with the following terminal command: `defaults write -g ApplePersistence -bool no`.
Enterprise	T1059		Command and Scripting Interpreter	Disable or remove any unnecessary or unused shells or interpreters.
		.001	PowerShell	It may be possible to remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution.
		.005	Visual Basic	Turn off or restrict access to unneeded VB components.
		.007	JavaScript/JScript	Turn off or restrict access to unneeded scripting components.
Enterprise	T1092		Communication Through Removable Media	Disable Autoruns if it is unnecessary.[1]

Data Sources and Detections: Data Sources are source of information collected by a sensor or logging system, it is used to collect information relevant to identifying adversary actions - “where to collect data”.

Detections – High level analytics process, sensors, data and detection strategies. Detection is useful to identify a technique has been used by an adversary – “How to Interpret collected data”.

Data Sources: Command: Command Execution Process: OS API Execution Process: Process Access Process: Process Creation

Detection

Monitor for unexpected processes interacting with LSASS.exe.[66] Common credential dumpers such as Mimikatz access LSASS.exe by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,[67] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Groups and Software:

Procedure – Specific implementation the adversary uses for techniques or sub-technique. This describes the group or software entity with a brief description of how the technique is used.

Groups – Related intrusion activity that are tracked by a common name. Some groups have multiple names associated with similar activities. Example – APT1, APT 38,

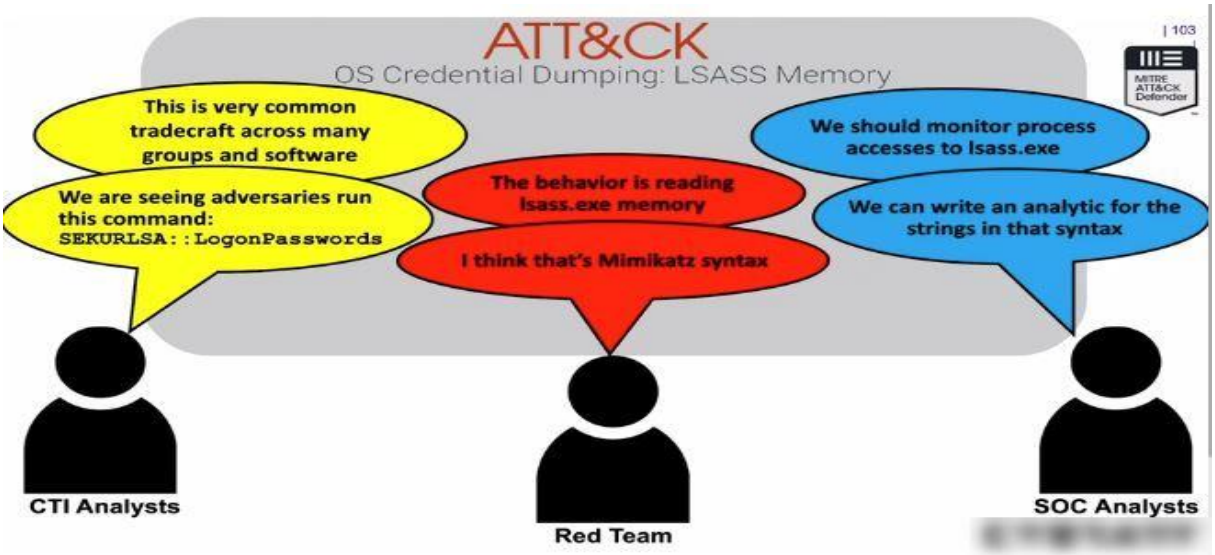
Software – Tools or malware used by an adversary during intrusions (entries may have multiple names). Example – PlugX is a remote access Trojan that uses modular plugins. It has been used by multiple threat groups.

LESSON 2 Benefits of using ATT&CK:

Citations within ATT&CK – also links to references within MITRE ATT&CK. MITRE uses publicly available cyber threat intelligence that anyone can access as the references for ATT&CK.

Collaboration and Communication across resources: Common Language

Example - **ATT&CK provides a language that can be used by:** Defenders; Red Teams; Executives; Intelligence Analysts



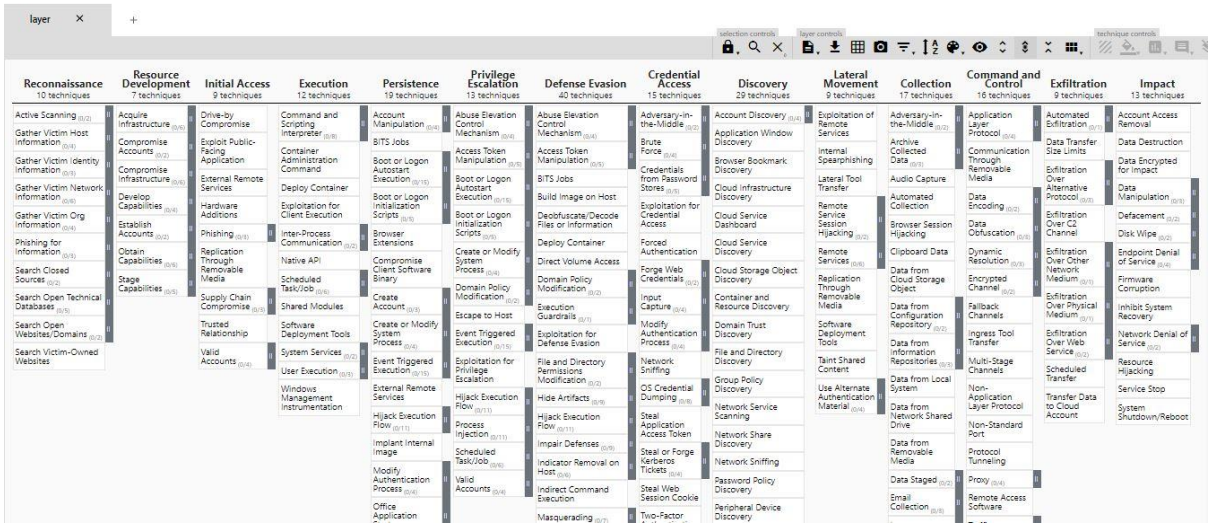
Quantitative Scorecard – This includes Documenting Priorities; Identifying Gaps; Informing Decision making. We can use ATT&CK to build quantitative scorecards for organization defences based on the inputs provided.

ATT&CK Navigator (Most Important) – Is designed to provide basic navigation and annotation of ATT&CK matrices. We can visualize defensive coverage, red/blue team planning, and the frequency of detected techniques. This Navigator manipulates the cells in the matrix (colour coding, adding a comment, assigning a numerical value, etc.)

Reference –

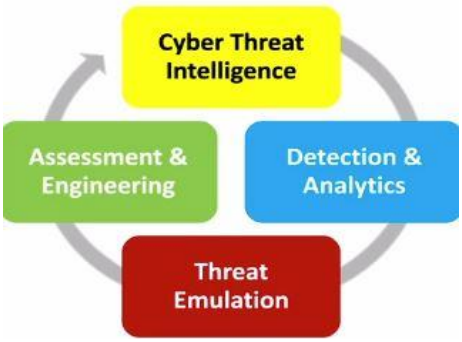
https://github.com/mitre-attack/attack-navigator

https://mitre-attack.github.io/attack-navigator/



LESSON 3 Operationalizing ATT&CK: For Cyber Threat Intelligence

CTI – critical for improving decision-making as well as shaping operations (threat-informed defense). ATT&CK is a great starting point for identifying what behaviours have been reported for specific groups or software.



Detection and Analysis: Let's take for example - OS Credential Dumping: LSASS Memory

Procedure Examples

Name	Description
APT1	APT1 has been known to use credential dumping using Mimikatz.[9]
APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[41][42]
APT3	APT3 has used a tool to dump credentials by injecting itself into lsass.exe and triggering with the argument "dig."[38]
APT32	APT32 used Mimikatz and customized versions of Windows Credential Dumper to harvest credentials.[49][50]
APT33	APT33 has used a variety of publicly available tools like LaZagne, Mimikatz, and ProcDump to dump credentials.[53][54]
APT39	APT39 has used Mimikatz, Windows Credential Editor and ProcDump to dump credentials.[52]

Detection –

OS Credential Dumping: LSASS Memory

Monitor for unexpected processes interacting with LSASS.exe.[66] Common credential dumpers such as Mimikatz access LSASS.exe by opening the process, locating the LSA secrets key, and decrypting the sections in memory where credential details are stored. Credential dumpers may also use methods for reflective Process Injection to reduce potential indicators of malicious activity.

On Windows 8.1 and Windows Server 2012 R2, monitor Windows Logs for LSASS.exe creation to verify that LSASS started as a protected process.

Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module,[67] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

MITRE Cyber Analytics Repository report –

CAR-2019-04-004: Credential Dumping via Mimikatz

Credential dumpers like Mimikatz can be loaded into memory and from there read data from another processes. This analytic looks for instances where processes are requesting specific permissions to read parts of the LSASS process in order to detect when credential dumping is occurring. One weakness is that all current implementations are "overtuned" to look for common access patterns used by Mimikatz.

This requires information about process access, e.g. ... odel mapping, since we currently lack any open/access ... odel requirements.

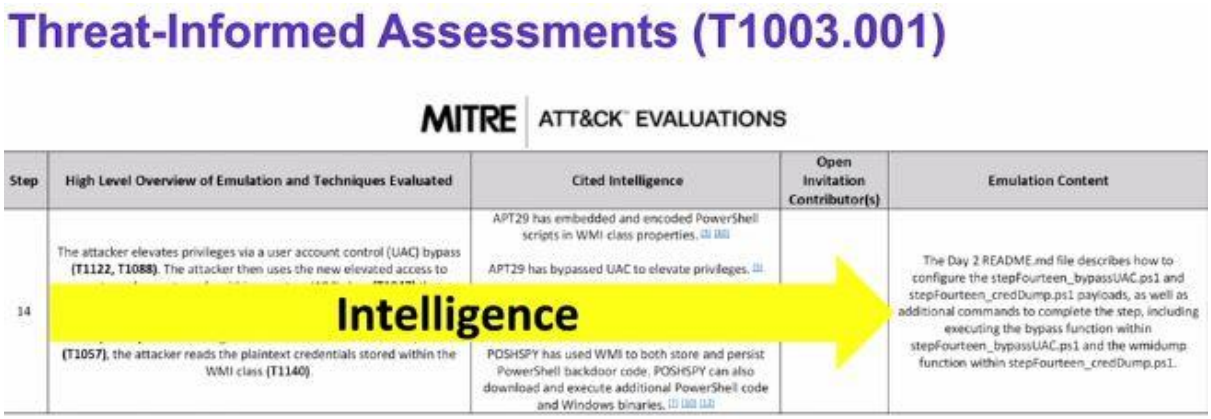
Submission Date: 2019/04/29
Information Domain: Host
Data Subtypes: Process
Analytic Type: TTP
Applicable Platforms: Windows
Contributors: MITRE

Processes that access LSASS

```
EventCode=10
TargetImage="C:\\WINDOWS\\system32\\lsass.exe"
(GrantedAccess=0x1410 OR GrantedAccess=0x1010 OR GrantedAccess=0x1438 OR GrantedAccess=0x143a OR GrantedAccess=0x1418)
CallTrace="C:\\windows\\SYSTEM32\\ntdll.dll+*|C:\\windows\\System32\\KERNELBASE.dll+20edd|UNKNOWN(*)"
```

Threat Emulation – https://github.com/mitre-attack/attack-arsenal

https://github.com/center-for-threat-informed-defense



In short MITRE ATT&CK helps us analyse questions such as what risks are most critical to address?, what risks can be tolerated?, as well as help us understand importance of informed decisions, assessments using threats will lead us towards necessary enhancements.

I hope this is helpful in getting fundaments of MITRE ATT&CK from CTI perspective.

-By Shefali Kumari