

MITRE ATT&CK Defender: Fundamentals For CTI



LESSON 1 Understanding ATT&CK Fundamentals:

Objectives:

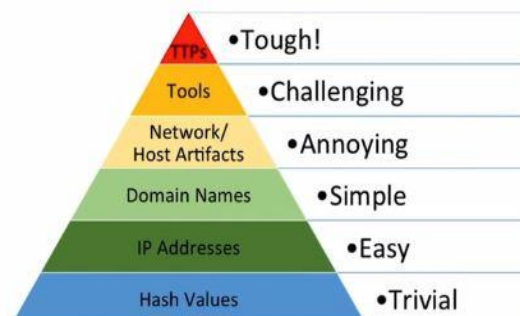
- Understand the background and motivation for ATT&CK – understanding ATT&CK
- Identify what information is captured in ATT&CK – Benefits of using ATT&CK
- Recognize the structure of ATT&CK – Operationalizing ATT&CK

Important References for Analysis of ATTACKS:

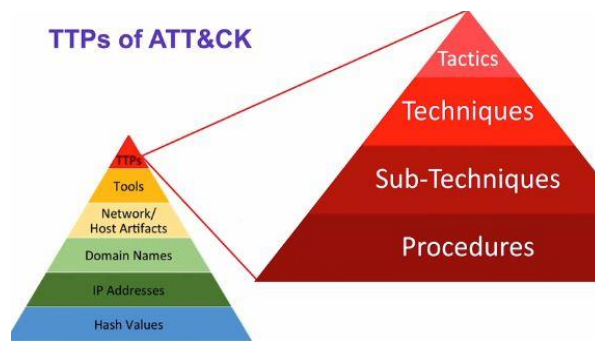
- MITRE ATT&CK - <https://attack.mitre.org/matrices/enterprise/>
- MITRE Engage - <https://engage.mitre.org/matrix/>
- MITRE Cyber Analytics Repository - <https://car.mitre.org/analytics/>
- MITRE Engenuity - <https://mitre-engenuity.org/attackevaluations/>
- CTID MITRE Engenuity - <https://ctid.mitre-engenuity.org/>
- 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:

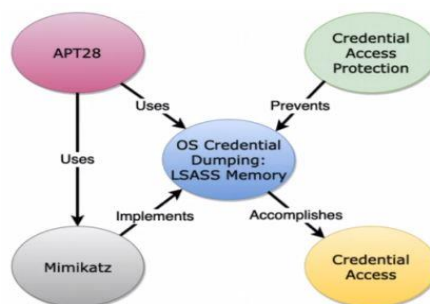
Pyramid of Pain –



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 matrix view captures relationship between tactics, techniques and sub-techniques. Each matrix 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.

Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side show sub-techniques hide sub-techniques help

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (3)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (3)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)
Gather Victim Identity Information (2)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (3)	Develop Infrastructure (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (3)	Boot or Logon Initialization Scripts (3)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Boot or Logon Initialization Scripts (3)	Deploy Container	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking
Phishing for Information (2)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Direct Volume Access	Forge Web Credentials (2)	Cloud Service Discovery	Clipboard Data	
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (2)	Scheduled Task/Job (6)	Create Account (3)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage Object
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Execution Guardrails (1)	Modify Authentication Process (4)	Container and Resource Discovery	Software Deployment Tools	Data from Configuration Repository (2)
Search Open Websites/Domains (2)		Valid Accounts (4)	System Services (2)	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery	Taint Shared Content	Data from Information Repositories (2)
Search Victim-Owned Websites			User Execution (2)	External Remote Services	Hijack Execution Flow (11)	Hide Artifacts (2)	OS Credential Dumping (3)	File and Directory Discovery	Use Alternate Authentication Material (4)	Data from Local System
			Windows Management Instrumentation	Hijack Execution Flow (11)	Process Injection (11)	Hijack Execution Flow (11)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive
				Implant Internal Image	Scheduled Task/Job (6)	Impair Defenses (2)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media
				Modify Authentication Process (4)	Valid Accounts (4)	Indicator Removal on Host (4)	Steal Web Session Cookie	Network Share Discovery		Data from Staged (2)
						Indirect Command Execution		Network Sniffing		Email Collection
						Masquerading (7)		Password Policy Discovery		
								Peripheral Device Discovery		

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 <code>/etc/ssh/sshd_config</code> .
Enterprise	T1547	.007 Boot or Logon Autostart Execution: Re-opened Applications	This feature can be disabled entirely with the following terminal command: <code>defaults write org.Apple.Preferences.NBOSD -bool no</code> .
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.

Turla

Turla is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and malware. Turla's espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#)

APT REPORTS

The Epic Turla Operation

Solving some of the mysteries of Snake/Uroboros
<https://securelist.com/the-epic-turla-operation/93542/>

Meet CrowdStrike's Adversary of the Month for March: VENOMOUS BEAR

<https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-march-venomous-bear/>

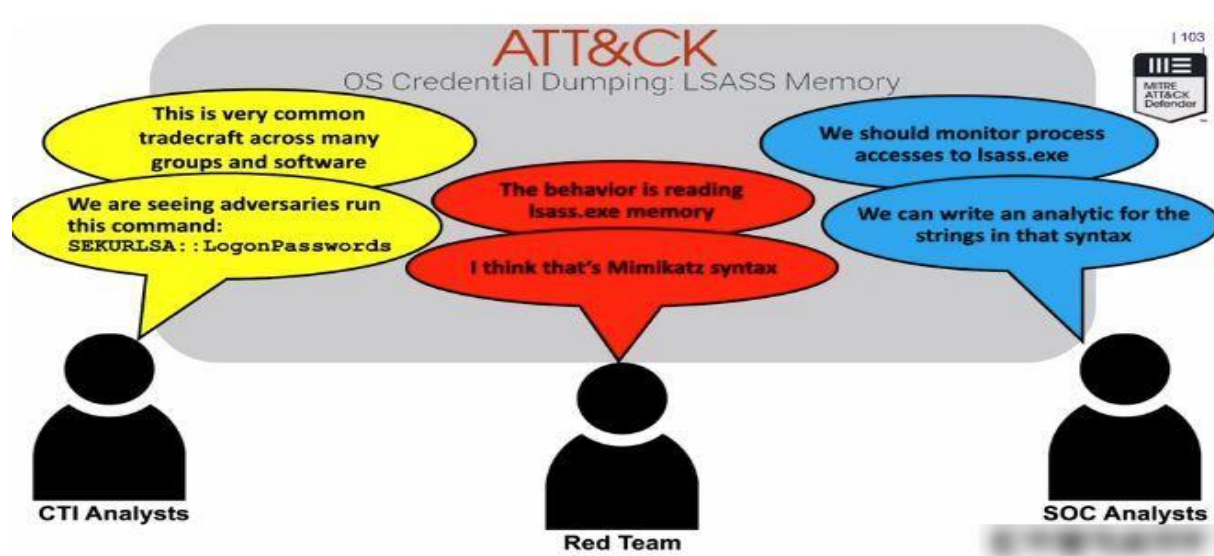
Gazing at Gazer

Turla's new second stage backdoor

Diplomats in Eastern Europe bitten by a Turla mosquito

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/>

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning (0.2)	Acquire Infrastructure (0.1)	Drive-by Compromise (0.1)	Command and Scripting Interpreter (0.1)	Account Manipulation (0.1)	Abuse Elevation Control Mechanism (0.1)	Abuse Elevation Control Mechanism (0.1)	Adversary-in-the-Middle (0.2)	Account Discovery (0.1)	Exploitation of Remote Services (0.1)	Adversary-in-the-Middle (0.2)	Application Layer Protocol (0.1)	Automated Exfiltration (0.1)	Account Access Removal (0.1)
Gather Victim Host Information (0.1)	Compromise Accounts (0.2)	Exploit Public-Facing Application (0.2)	Container Administration Command (0.1)	BITS Jobs (0.1)	Access Token Manipulation (0.1)	Access Token Manipulation (0.1)	Brute Force (0.1)	Application Window Discovery (0.1)	Internal Spearphishing (0.1)	Archive Collected Data (0.1)	Communication Through Removable Media (0.1)	Data Transfer Size Limits (0.1)	Data Destruction (0.1)
Gather Victim Identity Information (0.1)	Compromise Infrastructure (0.1)	External Remote Services (0.1)	Deploy Container (0.1)	Boot or Logon Autostart Execution (0.1)	Boot or Logon Autostart Execution (0.1)	Boot or Logon Autostart Execution (0.1)	Credentials from Password Stores (0.1)	Browser Bookmark Discovery (0.1)	Lateral Tool Transfer (0.1)	Audio Capture (0.1)	Data Encoding (0.1)	Exfiltration Over Alternative Protocol (0.1)	Data Encrypted for Impact (0.1)
Gather Victim Network Information (0.1)	Develop Capabilities (0.1)	Hardware Additions (0.1)	Exploitation for Client Execution (0.1)	Boot or Logon Initialization Scripts (0.1)	Boot or Logon Initialization Scripts (0.1)	Boot or Logon Initialization Scripts (0.1)	Cloud Infrastructure Discovery (0.1)	Cloud Service Dashboard (0.1)	Remote Service Session Hijacking (0.1)	Automated Collection (0.1)	Data Obfuscation (0.1)	Defacement (0.1)	Data Manipulation (0.1)
Gather Victim Org Information (0.1)	Establish Accounts (0.2)	Phishing (0.1)	Inter-Process Communication (0.1)	Browser Extensions (0.1)	Create or Modify System Process (0.1)	Create or Modify System Process (0.1)	Cloud Service Discovery (0.1)	Cloud Service Discovery (0.1)	Remote Services (0.1)	Clipboard Data (0.1)	Dynamic Resolution (0.1)	Endpoint Denial of Service (0.1)	Denial of Service (0.1)
Phishing for Information (0.1)	Obtain Capabilities (0.1)	Replication Through Removable Media (0.1)	Native API (0.1)	Compromise Client Software Binary (0.1)	Domain Policy Modification (0.1)	Domain Policy Modification (0.1)	Cloud Storage Object Discovery (0.1)	Cloud Storage Object Discovery (0.1)	Replication Through Removable Media (0.1)	Data from Cloud Storage Object (0.1)	Encrypted Channel (0.1)	Exfiltration Over Physical Medium (0.1)	Firmware Corruption (0.1)
Search Closed Sources (0.2)	Stage Capabilities (0.1)	Supply Chain Compromise (0.1)	Scheduled Task/Job (0.1)	Create Account (0.1)	Execution Guardrails (0.1)	Execution Guardrails (0.1)	Input Capture (0.1)	Container and Resource Discovery (0.1)	Software Deployment Tools (0.1)	Data from Information Repositories (0.1)	Failback Channels (0.1)	Ingress Tool Transfer (0.1)	Network Denial of Service (0.1)
Search Open Technical Databases (0.1)	Trusted Relationship (0.1)	Software Deployment Tools (0.1)	User Execution (0.1)	Event Triggered Execution (0.1)	Exploitation for Defense Evasion (0.1)	Exploitation for Defense Evasion (0.1)	Modify Authentication Process (0.1)	File and Directory Discovery (0.1)	Taint Shared Content (0.1)	Data from Local System (0.1)	Non-Application Layer Protocol (0.1)	Transfer Data to Cloud Account (0.1)	System Shutdown/Reboot (0.1)
Search Open Websites/Domains (0.2)	Valid Accounts (0.1)	System Services (0.1)	Windows Management Instrumentation (0.1)	External Remote Services (0.1)	Hijack Execution Flow (0.1)	Hijack Execution Flow (0.1)	OS Credential Dumping (0.1)	Group Policy Discovery (0.1)	Use Alternate Authentication Material (0.1)	Data from Removable Drive (0.1)	Non-Standard Port (0.1)	Service Stop (0.1)	
Search Victim-Owned Websites (0.1)					Process Injection (0.1)	Process Injection (0.1)	Steal Application Access Token (0.1)	Network Service Scanning (0.1)		Data from Network Shared Drive (0.1)	Protocol Tunneling (0.1)		
					Scheduled Task/Job (0.1)	Scheduled Task/Job (0.1)	Steal or Forge Kerberos Tickets (0.1)	Network Sniffing (0.1)		Data Staged (0.1)	Proxy (0.1)		
					Valid Accounts (0.1)	Valid Accounts (0.1)	Steal Web Session Cookie (0.1)	Password Policy Discovery (0.1)		Email Collection (0.1)	Remote Access Software (0.1)		
					Office Application (0.1)	Office Application (0.1)	Two-Factor (0.1)	Peripheral Device Discovery (0.1)					

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. ^[49]
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.

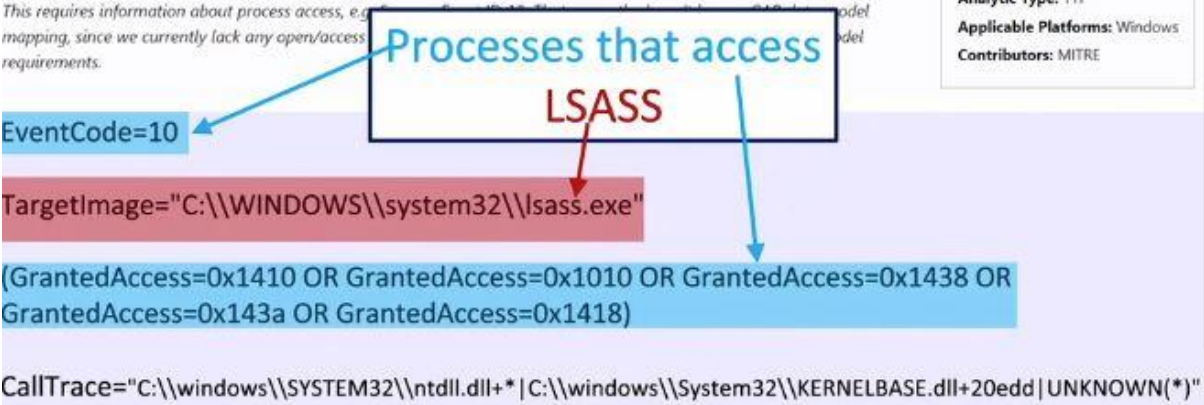
Monitor processes and command-line arguments for program execution that may be indicative of credential dumping. Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's 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. mapping, since we currently lack any open/access requirements.



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

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

Threat-Informed Assessments (T1003.001)

MITRE ATT&CK [™] EVALUATIONS				
Step	High Level Overview of Emulation and Techniques Evaluated	Cited Intelligence	Open Invitation Contributor(s)	Emulation Content
14	The attacker elevates privileges via a user account control (UAC) bypass (T1122, T1088). The attacker then uses the new elevated access to (T1057), the attacker reads the plaintext credentials stored within the WMI class (T1140).	APT29 has embedded and encoded PowerShell scripts in WMI class properties. [1] [2] APT29 has bypassed UAC to elevate privileges. [3] POSHSPY has used WMI to both store and persist PowerShell backdoor code, POSHSPY can also download and execute additional PowerShell code and Windows binaries. [4] [5] [6]		The Day 2 README.md file describes how to configure the stepFourteen_bypassUAC.ps1 and stepFourteen_credDump.ps1 payloads, as well as additional commands to complete the step, including executing the bypass function within stepFourteen_bypassUAC.ps1 and the wmidump function within stepFourteen_credDump.ps1.

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 fundamentals of MITRE ATT&CK from CTI perspective.

-By Shefali Kumari