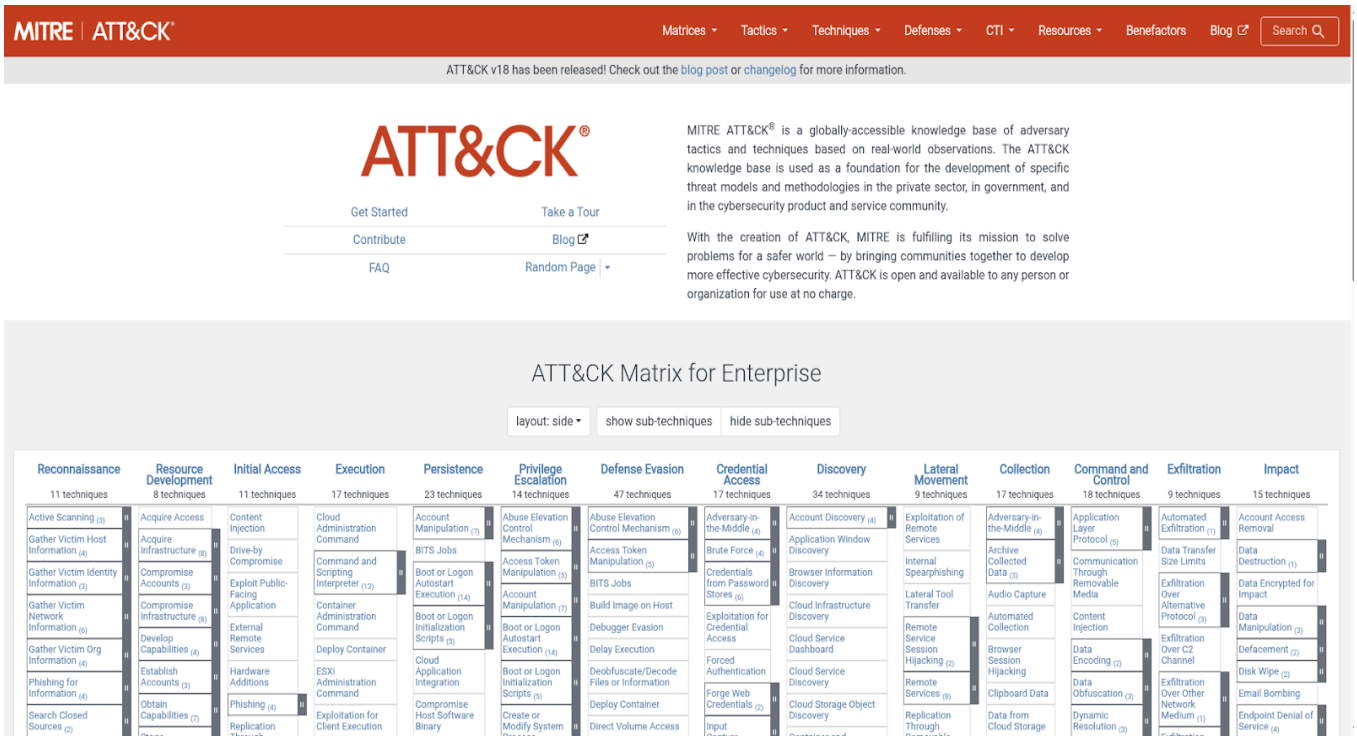
MITRE ATT&CK

MITRE Adversarial Tactics, Techniques, and Common Knowledge



What is MITRE ATT&CK?

MITRE ATT&CK is a **global knowledge base of real-world cyber attacker behavior.**

In simple words:

- It shows **how attackers think**
- What **steps they follow**
- Which t**echniques they use during an attack**

It is **NOT a tool**, it is a **framework.**

ATT&CK = Adversarial Tactics, Techniques, and Common Knowledge

Why MITRE Created ATT&CK

Before ATT&CK:

- Attackers reused the same techniques
- Defenders described attacks inconsistently
- There was no **common language** for attacker behavior

In **2013**, MITRE began documenting **repeatable patterns used by APT groups**, leading to the creation of ATT&CK.

The goal was to:

- Standardize how attacks are described
- Improve detection and defense
- Enable collaboration across the security community

Core Structure of MITRE ATT&CK

MITRE ATT&CK is built around **TTPs**:

1 .Tactic – *The "Why"*

A **tactic** represents the **goal or objective** of the attacker.

Examples:

- Reconnaissance
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Command and Control
- Exfiltration

2.Technique – *The "How"*

A **technique** describes **how** the attacker achieves a tactic.

Examples:

- Phishing
- PowerShell
- Credential Dumping
- Active Scanning

Each technique has a unique **Technique ID** (e.g., T1059).

3.Procedure – *The "How Exactly"*

A **procedure** is the **real-world implementation** of a technique.

Examples:

- Using PowerShell with encoded commands
- Running Nmap to scan IP ranges
- Using Mimikatz to dump credentials

Procedures vary by attacker, tool, and environment.

Tactic: Reconnaissance

Technique: Active Scanning

Procedure: Using Nmap to scan 10.0.0.0/24

Evolution of the ATT&CK Framework

ATT&CK initially focused only on **Windows environments**. Over time, it expanded to cover modern infrastructures.

Current ATT&CK Matrices:

- **Enterprise**
  - Windows
  - Linux
  - macOS
  - Cloud (AWS, Azure, GCP)
- **Mobile**
- **ICS (Industrial Control Systems)**

This evolution ensures ATT&CK remains relevant for:

- Traditional IT environments
- Cloud-native organizations
- OT and critical infrastructure

The MITRE ATT&CK Matrix

The **ATT&CK Matrix** is a **visual representation** of all tactics and techniques.

Structure:

- **Tactics** are displayed across the top
- **Techniques** are listed beneath each tactic
- **Sub-techniques** expand from techniques for deeper detail

The matrix helps defenders:

- Visualize attacker progression
- Identify detection gaps
- Understand attack chains

Example: Reconnaissance in ATT&CK

Tactic:

Reconnaissance
The attacker's goal is to gather information about the target.

Technique:

Active Scanning (T1595)
The attacker actively probes the target's infrastructure.

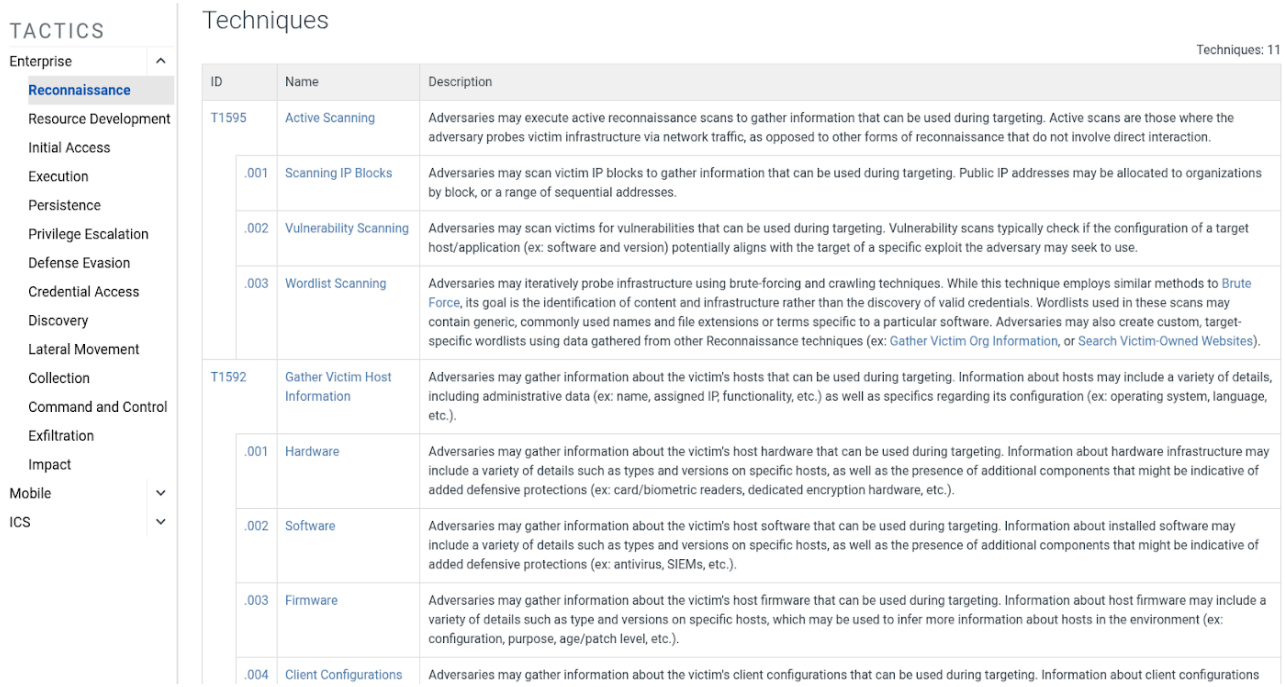
Sub-techniques:

- Scanning IP Blocks
- Vulnerability Scanning
- Wordlist Scanning

This breakdown shows how ATT&CK moves from **high-level intent** to **specific actions**.

Reconnaissance

Technique:



TACTICS

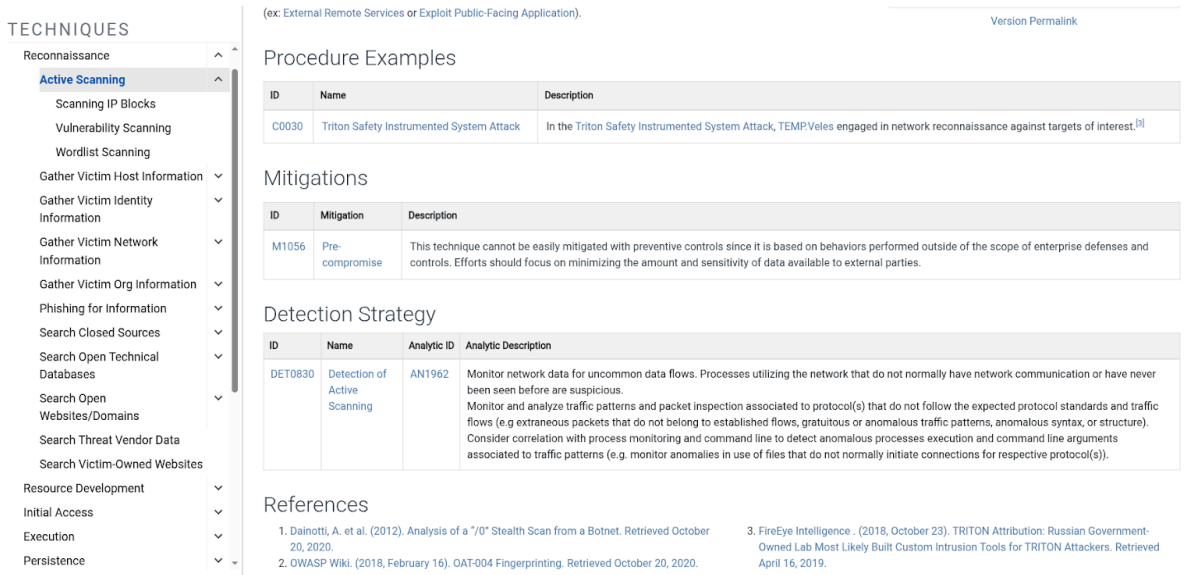
- Enterprise
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
- Mobile
- ICS

Techniques

Techniques: 11

ID	Name	Description
T1595	Active Scanning	Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
.001	Scanning IP Blocks	Adversaries may scan victim IP blocks to gather information that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses.
.002	Vulnerability Scanning	Adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.
.003	Wordlist Scanning	Adversaries may iteratively probe infrastructure using brute-forcing and crawling techniques. While this technique employs similar methods to Brute Force, its goal is the identification of content and infrastructure rather than the discovery of valid credentials. Wordlists used in these scans may contain generic, commonly used names and file extensions or terms specific to a particular software. Adversaries may also create custom, target-specific wordlists using data gathered from other Reconnaissance techniques (ex: Gather Victim Org Information, or Search Victim-Owned Websites).
T1592	Gather Victim Host Information	Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.).
.001	Hardware	Adversaries may gather information about the victim's host hardware that can be used during targeting. Information about hardware infrastructure may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: card/biometric readers, dedicated encryption hardware, etc.).
.002	Software	Adversaries may gather information about the victim's host software that can be used during targeting. Information about installed software may include a variety of details such as types and versions on specific hosts, as well as the presence of additional components that might be indicative of added defensive protections (ex: antivirus, SIEMs, etc.).
.003	Firmware	Adversaries may gather information about the victim's host firmware that can be used during targeting. Information about host firmware may include a variety of details such as type and versions on specific hosts, which may be used to infer more information about hosts in the environment (ex: configuration, purpose, age/patch level, etc.).
.004	Client Configurations	Adversaries may gather information about the victim's client configurations that can be used during targeting. Information about client configurations

Sub-techniques:



TECHNIQUES

- Reconnaissance
  - Active Scanning
    - Scanning IP Blocks
    - Vulnerability Scanning
    - Wordlist Scanning
  - Gather Victim Host Information
  - Gather Victim Identity Information
  - Gather Victim Network Information
  - Gather Victim Org Information
  - Phishing for Information
  - Search Closed Sources
  - Search Open Technical Databases
  - Search Open Websites/Domains
  - Search Threat Vendor Data
  - Search Victim-Owned Websites
- Resource Development
- Initial Access
- Execution
- Persistence

(ex: External Remote Services or Exploit Public-Facing Application).

Version Permalink

Procedure Examples

ID	Name	Description
C0030	Triton Safety Instrumented System Attack	In the Triton Safety Instrumented System Attack, TEMP.Veles engaged in network reconnaissance against targets of interest.[3]

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.

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0830	Detection of Active Scanning	AN1962	Monitor network data for uncommon data flows. Processes utilizing the network that do not normally have network communication or have never been seen before are suspicious. Monitor and analyze traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)).

References

1. Dainotti, A. et al. (2012). Analysis of a "/0" Stealth Scan from a Botnet. Retrieved October 20, 2020.
2. OWASP Wiki. (2018, February 16). OAT-004 Fingerprinting. Retrieved October 20, 2020.
3. FireEye Intelligence . (2018, October 23). TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers. Retrieved April 16, 2019.

Active Scanning

Technique

Sub-techniques (3)

Sub-techniques

ID	Name
T1595.001	Scanning IP Blocks
T1595.002	Vulnerability Scanning
T1595.003	Wordlist Scanning

ID & Related Information

ID: T1595

Sub-techniques: T1595.001, T1595.002, T1595.003

ⓘ Tactic: Reconnaissance

ⓘ Platforms: PRE

Version: 1.0

Created: 02 October 2020

Last Modified: 15 April 2025

Description

Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.

Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).

Technique Detail Pages

Each technique page in ATT&CK provides:

- Technique ID and description
- Sub-techniques
- Real-world procedure examples
- Associated threat groups and software
- Detection guidance
- Mitigation strategies
- External references

This makes ATT&CK useful not only for detection, but also for **investigation and response planning**.

ATT&CK Navigator

The **ATT&CK Navigator** is an interactive tool that allows users to:

- Highlight techniques
- Track detection coverage
- Create heat maps
- Compare threat actors
- Plan red and blue team exercises

It is commonly used to measure **security maturity** and **coverage gaps**.

ATT&CK in Operation

- Now that we understand what **MITRE ATT&CK** is, let's see **how it is actually used in real life** and **why it is important** for cyber security teams.
- **MITRE ATT&CK** contains a **lot of information**, so organizations use it as a **structured guide** to understand attacks instead of getting confused by raw data

Why ATT&CK Matters

In cybersecurity, the **same attacker activity is often called by different names**.

Example:

- One tool says: *Suspicious PowerShell*
- Another says: *Script-based attack*
- A report says: *Living-off-the-land technique*

This creates confusion.

ATT&CK solves this by:

- Giving **standard names**
- Assigning **unique technique IDs** (like T1059)
- Creating a **common language** for everyone

Because of this:

- Teams communicate better
- Incidents are easier to compare
- Reports are easier to understand

ATT&CK and Threat Intelligence

Threat reports often explain **what the attacker did**, but not **how defenders should detect it**.

ATT&CK helps convert **threat intelligence into action**.

How?

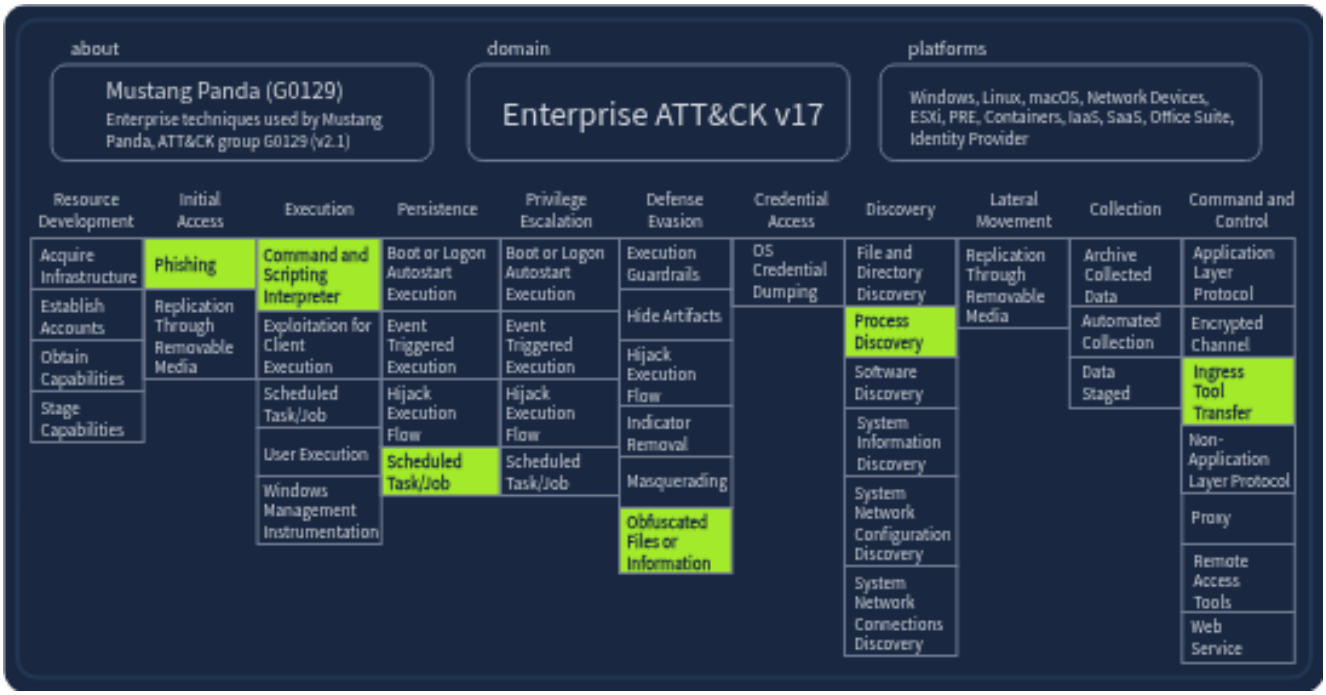
- Threat behavior is mapped to **ATT&CK tactics and techniques**

- Defenders use this mapping to:
  - Write detection rules
  - Create SIEM queries
  - Build SOC playbooks

This makes threat intelligence **useful and actionable**.

Who Uses ATT&CK

- Cyber Threat Intelligence (CTI) Teams-Understand attackers
- SOC Analysts- Investigate alerts
- Detection Engineers- Improve detections
- Incident Responders-Handle security incidents
- Red & Purple Teams-Test defenses



Mapping in Action

After an attack, teams need to understand **how the attacker moved step by step**.

ATT&CK helps by mapping each step clearly.

Example: Mustang Panda (APT Group)

Mustang Panda is a known attacker group.

Based on past attacks, they usually:

- Start with **phishing emails**
- Stay persistent using **scheduled tasks**
- Hide malware using **obfuscation**
- Communicate with servers using **tool transfer**

Using ATT&CK:

- Each action is mapped to a technique
- Teams can prepare detections in advance
- Future attacks are easier to spot

Cyber Analytics Repository (CAR)

What is CAR?

- The **Cyber Analytics Repository (CAR)** is a **collection of detection analytics** created by **MITRE** using the **MITRE ATT&CK framework**.

In simple words:

- **ATT&CK tells you *what attackers do***
- **CAR tells you *how to detect it***

CAR helps defenders turn ATT&CK techniques into **real detection rules**.

Why CAR Exists

ATT&CK explains attacker behavior, but it does **not directly give detection rules**.

Security teams often ask:

- What logs should I look at?
- What pattern indicates this attack?
- How do I write a SIEM rule for this technique?

CAR answers these questions.

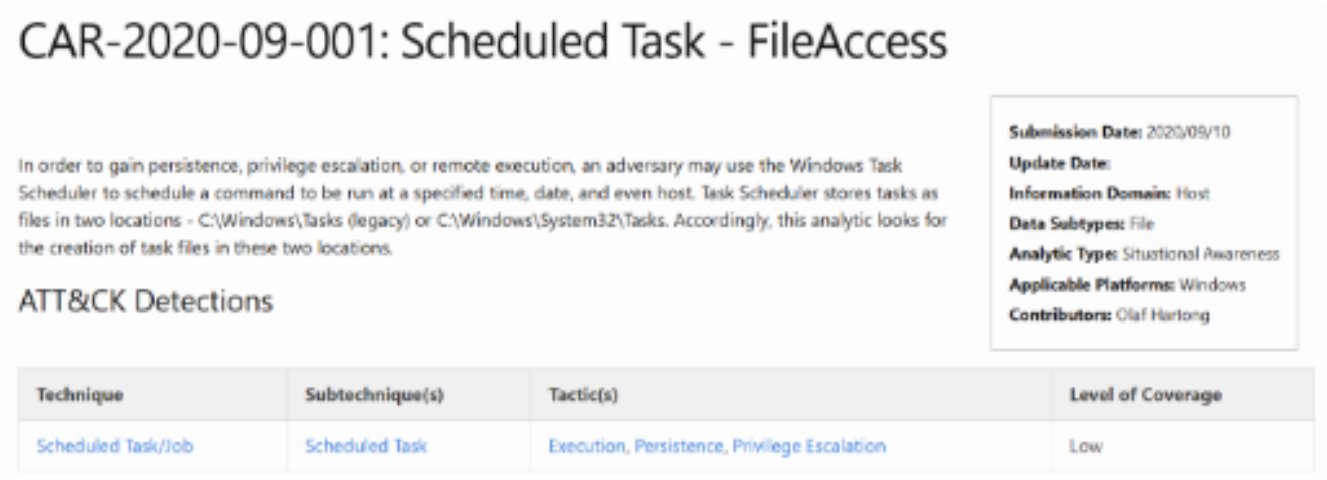
What CAR Provides

Each CAR analytic includes:

- A **description** of the attacker behavior
- The **related ATT&CK tactic and technique**
- **Detection logic** explained clearly
- **Example implementations** for SIEM tools
- Sometimes **unit tests** to validate detection

This makes CAR very useful for:

- SOC analysts
- Detection engineers
- Blue teams
- Students learning detection engineering



CAR-2020-09-001: Scheduled Task - FileAccess

In order to gain persistence, privilege escalation, or remote execution, an adversary may use the Windows Task Scheduler to schedule a command to be run at a specified time, date, and even host. Task Scheduler stores tasks as files in two locations - C:\Windows\Tasks (legacy) or C:\Windows\System32\Tasks. Accordingly, this analytic looks for the creation of task files in these two locations.

Submission Date: 2020/09/10
Update Date:
Information Domain: Host
Data Subtypes: File
Analytic Type: Situational Awareness
Applicable Platforms: Windows
Contributors: Olaf Hartong

ATT&CK Detections

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
Scheduled Task/Job	Scheduled Task	Execution, Persistence, Privilege Escalation	Low

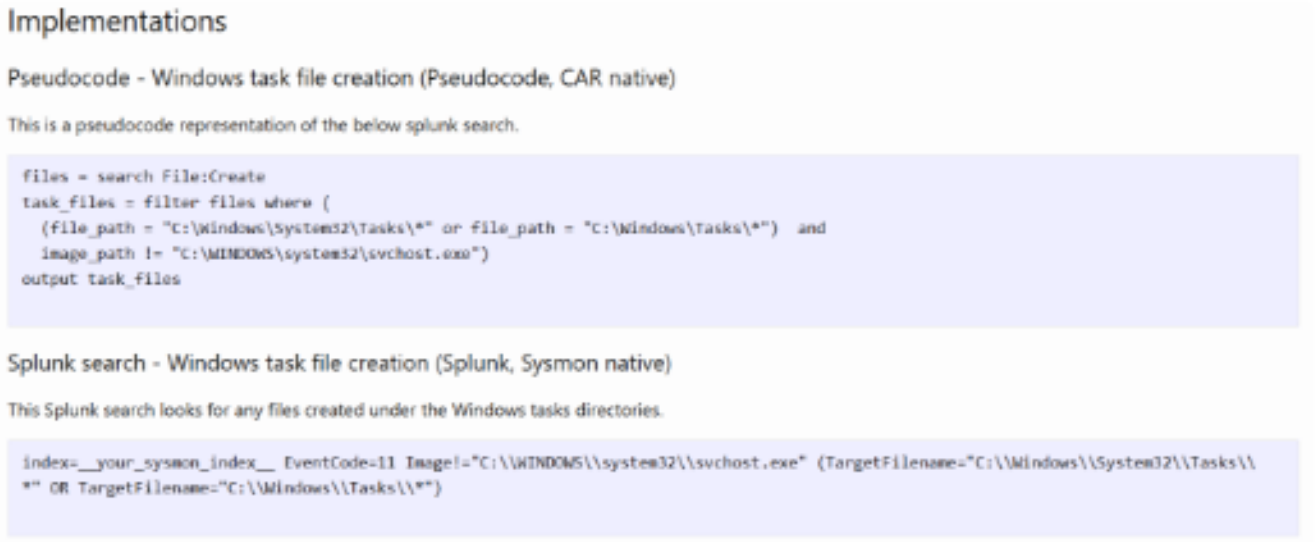
How CAR Is Used in Real SOCs

Typical workflow:

1. Identify an ATT&CK technique
2. Check if a CAR analytic exists
3. Read detection logic and rationale
4. Adapt SIEM query
5. Test and tune detection
6. Deploy in SOC

This makes detection:

- Faster
- More structured
- More reliable



Implementations

Pseudocode - Windows task file creation (Pseudocode, CAR native)

This is a pseudocode representation of the below splunk search.

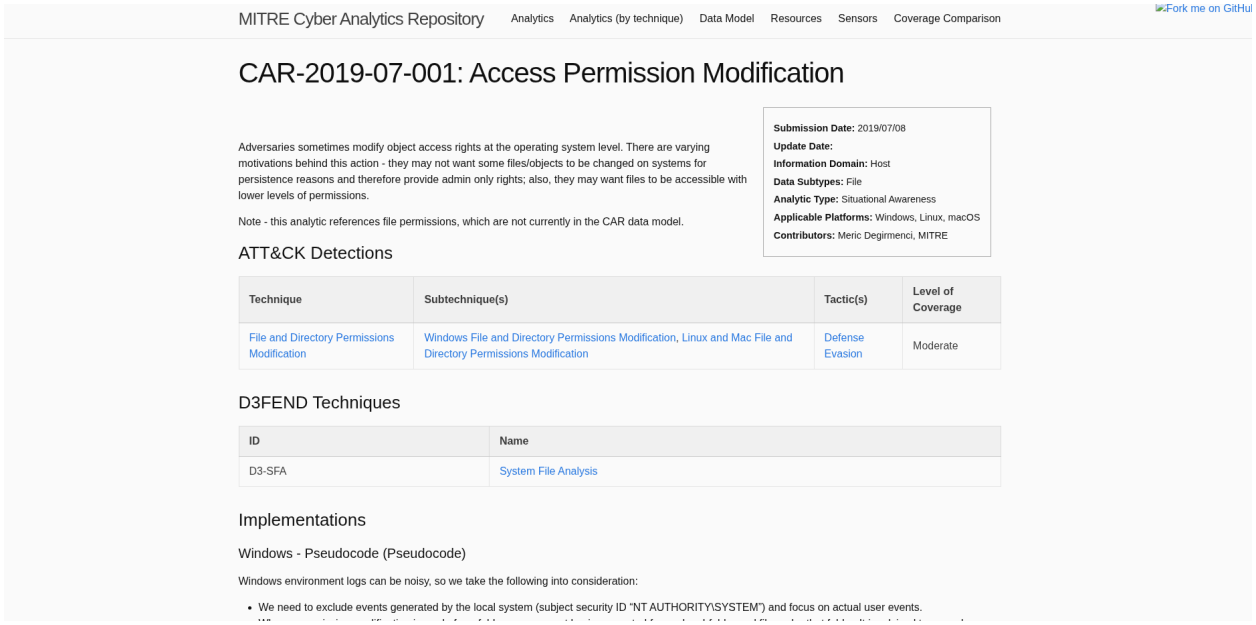
```
files = search File:Create
task_files = filter files where (
  (file_path = "C:\Windows\System32\Tasks\*" or file_path = "C:\Windows\Tasks\*")  and
  image_path != "C:\WINDOWS\system32\svchost.exe")
output task_files
```

Splunk search - Windows task file creation (Splunk, Sysmon native)

This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\
*" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

CAR - for ACCESS PERMISSION MODIFICATION



MITRE Cyber Analytics Repository Analytics Analytics (by technique) Data Model Resources Sensors Coverage Comparison

Fork me on GitHub

CAR-2019-07-001: Access Permission Modification

Adversaries sometimes modify object access rights at the operating system level. There are varying motivations behind this action - they may not want some files/objects to be changed on systems for persistence reasons and therefore provide admin only rights; also, they may want files to be accessible with lower levels of permissions.

Note - this analytic references file permissions, which are not currently in the CAR data model.

Submission Date: 2019/07/08
Update Date:
Information Domain: Host
Data Subtypes: File
Analytic Type: Situational Awareness
Applicable Platforms: Windows, Linux, macOS
Contributors: Meric Degirmenci, MITRE

ATT&CK Detections

Technique	Subtechnique(s)	Tactic(s)	Level of Coverage
File and Directory Permissions Modification	Windows File and Directory Permissions Modification, Linux and Mac File and Directory Permissions Modification	Defense Evasion	Moderate

D3FEND Techniques

ID	Name
D3-SFA	System File Analysis

Implementations

Windows - Pseudocode (Pseudocode)

Windows environment logs can be noisy, so we take the following into consideration:

- We need to exclude events generated by the local system (subject security ID "NT AUTHORITY\SYSTEM") and focus on actual user events.

Implementation in SIEM,EDR

Implementations

Windows - Pseudocode (Pseudocode)

Windows environment logs can be noisy, so we take the following into consideration:

- We need to exclude events generated by the local system (subject security ID "NT AUTHORITY\SYSTEM") and focus on actual user events.
- When a permission modification is made for a folder, a new event log is generated for each subfolder and file under that folder. It is advised to group logs based on handle ID or user ID.
- The Windows security log (event ID 4670) also includes information about the process that modifies the file permissions. It is advised to focus on uncommon process names, and it is also uncommon for real-users to perform this task without a GUI.

```
log_name == "Security" AND
event_code == "4670" AND
object_type == "File" AND
subject_security_id != "NT AUTHORITY\SYSTEM"
```

Windows - Splunk (Splunk)

Splunk version of the above pseudocode.

```
index=__your_windows_security_log_index__ EventCode=4670 Object_Type="File" Security_ID!="NT AUTHORITY\\SYSTEM"
```

Linux - Pseudocode (Pseudocode)

This looks for any invocations of chmod. Note that this is likely to be more noisy than the Windows-specific implementation, although Linux does not generate logs for system triggered activities like in Windows. In addition, it may be necessary to whitelist cron jobs that regularly run and execute `chmod`.

```
processes = search Process:Create
chmod_processes = filter processes where command_line == "chmod *"
output chmod_processes
```

Logpoint, LogPoint native

LogPoint version of the above pseudocode for Windows.

```
norm_id=WindowsSysmon channel="Security" event_id=4670 object_type="File" -user_id="S-1-5-18"
```

Unit Tests

Why MITRE ATT&CK Is Critical in Modern Security

- Provides a **common language** for cyber defense
- Vendor-neutral and globally adopted
- Improves detection, response, and resilience
- Essential for SOC operations and threat hunting
- Widely referenced in security research and tooling

Writing a detection rules and implementation idea using MITRE ATT&CK

SIEM Rule -SPLUNK

MITRE: **T1059.001 – PowerShell (Execution)**

Detect encoded PowerShell execution (very common in attacks).

```
index=windows EventCode=4688

Process_Name="*powershell.exe"

(CommandLine="*-enc*" OR
CommandLine="*EncodedCommand*")
```

Why This Works

- Attackers hide commands using Base64
- Legit admins rarely use -enc

SOC Use

- Execution stage detection
- High-severity alert
- Correlate with phishing or C2 alerts

EDR Rule-Microsoft Defender

MITRE: **T1003 – Credential Dumping**

Detect LSASS memory access.

Process accesses lsass.exe memory

AND Process NOT signed by Microsoft

Example Processes

- mimikatz
- procdump
- renamed tools

SOC Response

- Isolate endpoint
- Reset credentials
- Block process hash

IDS / IPS Rule -SNORT

MITRE: **T1071 – Command and Control (c2 server)**

Detect suspicious PowerShell download over HTTP/s.

```
alert tcp any any -> any 80 (
 msg:"MITRE T1071 - PowerShell C2 Download";
 content:"powershell";
 nocase;
 sid:1000001;
 rev:1;
)
```

Why This Works

- Malware often downloads payloads using PowerShell
- Clear network indicator

SOC Use

- Early malware detection
- Network-level visibility

Malware Detection- YARA rule

MITRE: **T1027 – Obfuscated Files**

MITRE**: T1059 – PowerShell**

Detect **encoded PowerShell in malware files**.

```
rule MITRE_T1059_Encoded_PowerShell
{
   meta:
      mitre = "T1059.001"
      description = "Detect encoded PowerShell commands"
   strings:
      $ps1 = "powershell -enc" nocase
      $ps2 = "FromBase64String" nocase
   condition:
      any of them
}
```

SOC Use

- File scanning
- Memory scanning
- Incident response

Microsoft Sentinel (Cloud SIEM – KQL)

MITRE: T1566 – Phishing (Initial Access)

Detects users clicking malicious links.

```
EmailEvents
| where ThreatTypes has "Phish"
| where DeliveryAction == "Delivered"
```

SOC Use

- Early attack detection
- Prevent payload execution
- User awareness & response

Web Application Firewall (WAF – ModSecurity)

MITRE: **T1190 – Exploit Public-Facing Application**

Detects SQL Injection attempts.

SecRule ARGS "@rx (?i)(union select|or 1=1|sleep\()"

"id:10001,phase:2,deny,msg:'MITRE T1190 SQL Injection Attempt'"

SOC Use

- Web attack prevention
- Protect critical apps
- Reduce breach risk

How SOC Writes Rules Using MITRE

Choose ATT&CK Technique

↓

Understand attacker behavior

↓

Pick log source (SIEM / EDR / IDS)

↓

Write detection logic

↓

Map to MITRE ID

↓

Tune and deploy

“We detect attacker behavior, not tools. MITRE ATT&CK is the backbone of all SOC detections.”

Reference

https://attack.mitre.org/

https://en.wikipedia.org/wiki/ATT%26CK

https://github.com/mitre-attack

https://en.wikipedia.org/wiki/Common_Attack_Pattern_Enumeration_and_Classification

-yuvaraj.D