Understanding MITRE ATT&CK

Attack Campaign vs MITRE ATT&CK ?

- **14** phases (called "**Tactics**")
- Several ways for executing each phase ("**Techniques**")

- Given a specific attack campaign
- How is it **mapped** on MITRE ATT&CK Tactics and Techniques?

Keep in mind

- Given a specific attack campaign
- How is it **mapped** on MITRE ATT&CK Tactics and Techniques?

- Mapping:
  - Process **Not** automatic / immediate / easy
  - Result **Not** algorithmic / exact

  - Result sometimes counterintuitive
  - In practice: Textual report + List of Techniques

Our next steps

- Outline **a few** common scenarios for "**entering an organization**"
- Illustrate their mapping on MITRE ATT&CK

- Key points:
  - Each scenario might appear as a "single step"
  - …yet it corresponds to **several** techniques in **two** different tactics
  - Mapping **not** obvious

Example 1

- **Phishing**
- User opens attachment (that contains **macros**)
- Macros executed by program that opens attachment

- Requirements:
  - User involvement
  - Program that opens that attachment type has scripting capabilities (e.g., Excel)
  - Scripting capabilities are enabled

Excel Macros = Visual Basic Script

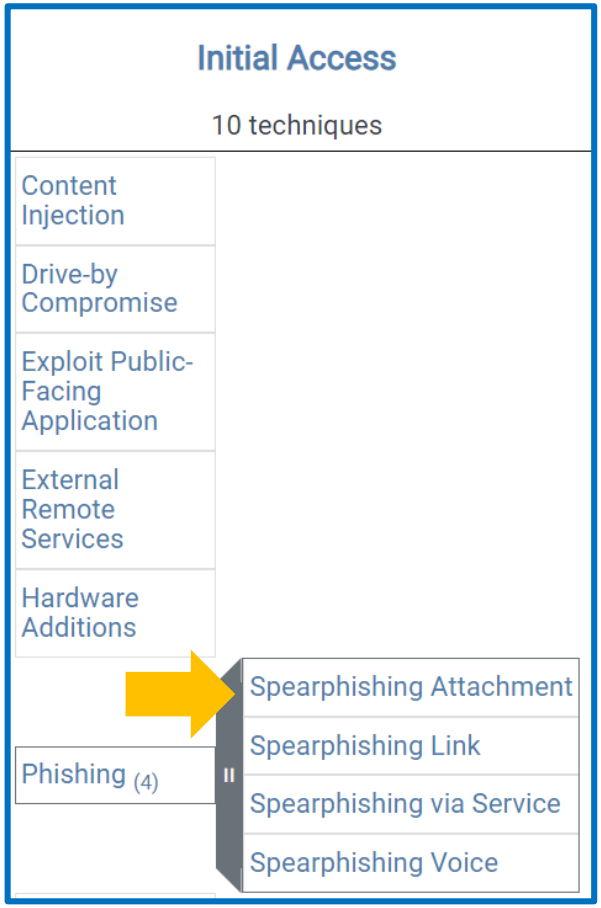
To insert a macro in Excel, you can follow these general steps:

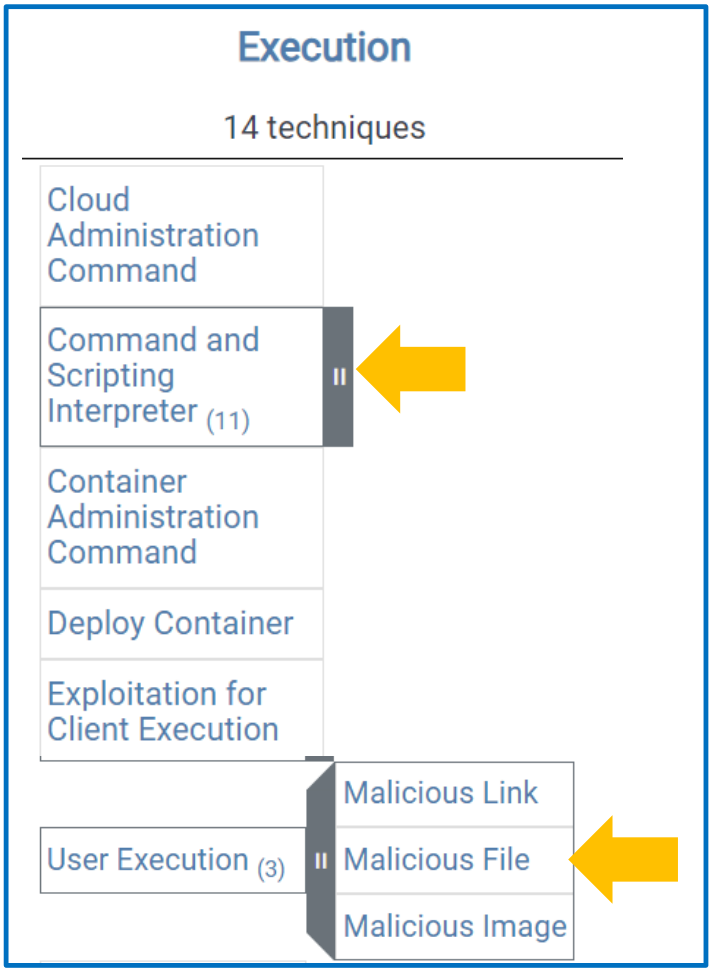
- **Record a Macro**: Go to the **View** tab, click on **Macros**, and select **Record Macro**. Perform the actions you want to automate.
- **Write a Macro**: Press `ALT + F11` to open the **Visual Basic for Applications (VBA)** editor. Here, you can write or paste your macro code.
- **Assign a Macro**: You can assign your macro to a button, shape, or shortcut key for easy access.
- **Run a Macro**: Access the macro via the **Macros** dialog box under the **View** tab or use the assigned button or shortcut.

To run an Excel macro automatically, you can use the following methods:

- **Event Procedures**: Assign the macro to an event like opening the workbook or changing a cell.
- **Auto_Open Macro**: Create a macro named `Auto_Open` to run it when Excel starts.
- **VBA Project Settings**: Adjust the settings in the VBA project to trigger the macro upon certain actions.

Mapping


Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice

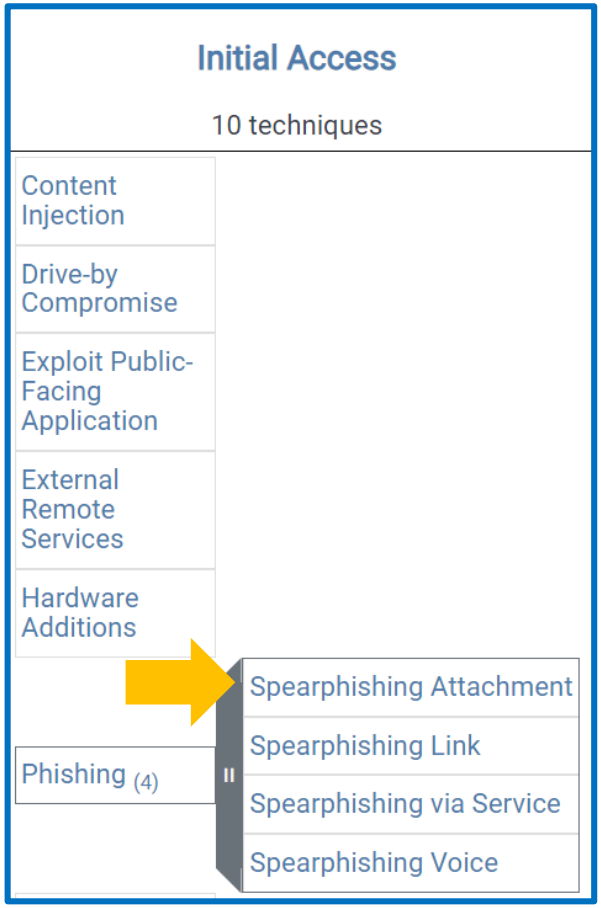

Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (11)
Container Administration Command
Deploy Container
Exploitation for Client Execution
User Execution (3)
Malicious Link
Malicious File
Malicious Image

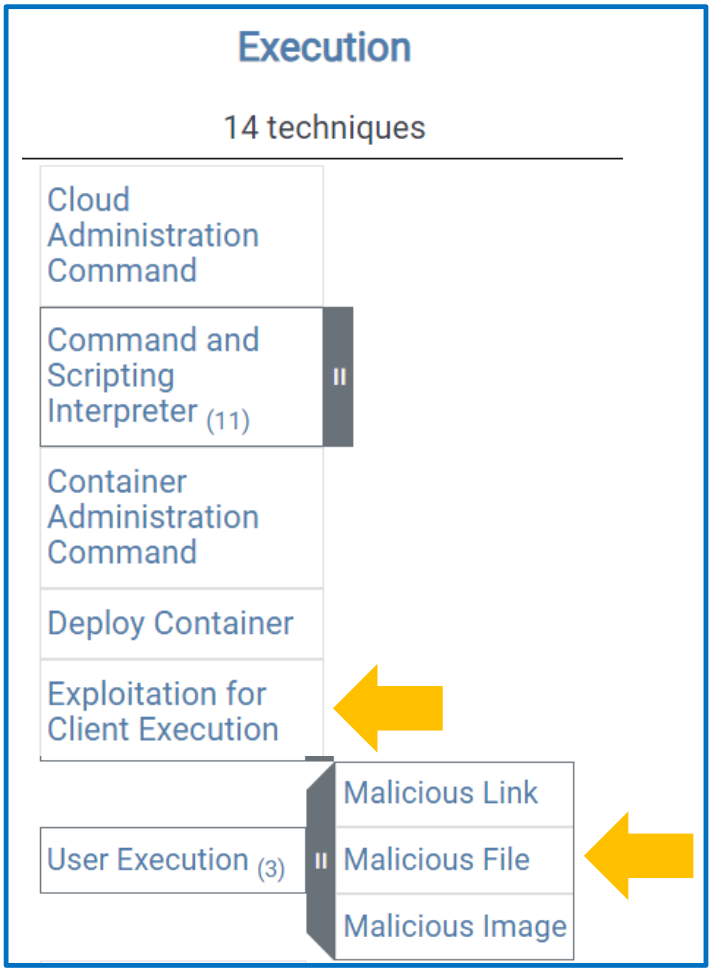
Example 2

- Phishing
- User opens attachment (that contains an exploit)
- RCE exploitation in **program that opens attachment**

- Requirements:
  - User involvement
  - Program that opens certain attachments (client program) has **RCE vulnerability**
  - Adversary has exploit for that vulnerability

Mapping


Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice

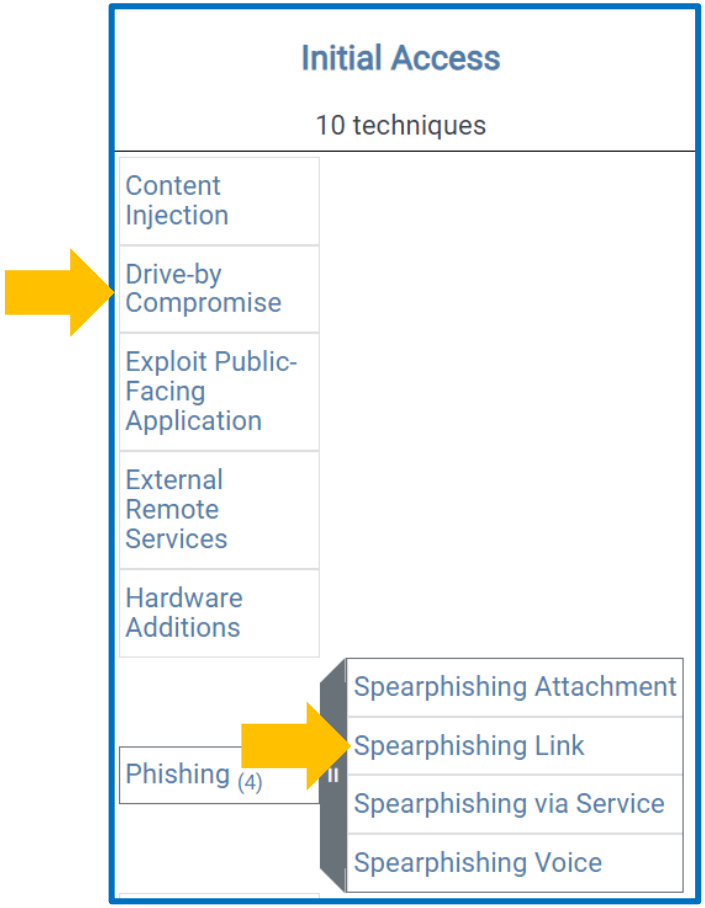

Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (11)
Container Administration Command
Deploy Container
Exploitation for Client Execution
User Execution (3)
Malicious Link
Malicious File
Malicious Image

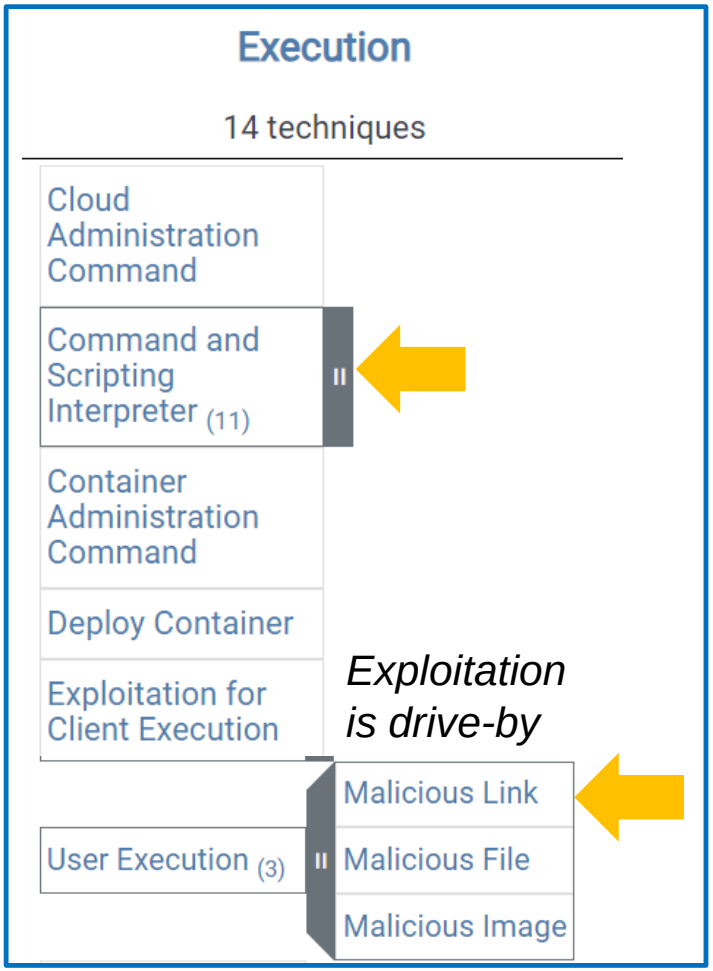
Example 3

- Phishing
- User clicks on a link
- RCE exploitation in **Browser that fetches document** (drive-by)

- Requirements:
  - User involvement
  - Browser (client program) has **RCE vulnerability**
  - Adversary has exploit for that vulnerability (and a website that serves that exploit)

Mapping


Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Spearphishing Voice

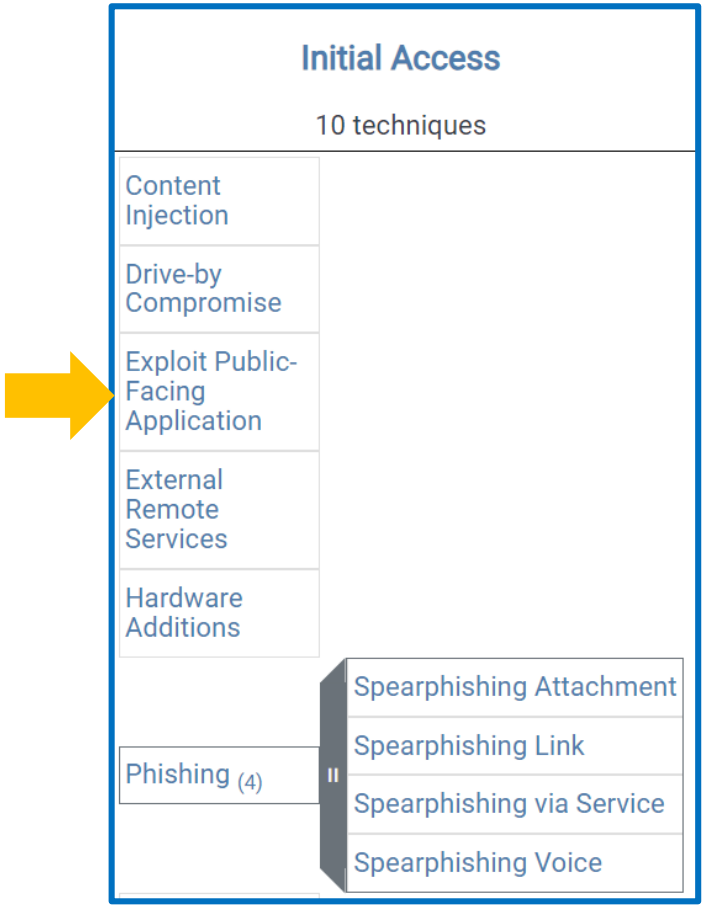

Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (11)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Exploitation is drive-by
User Execution (3)
Malicious Link
Malicious File
Malicious Image

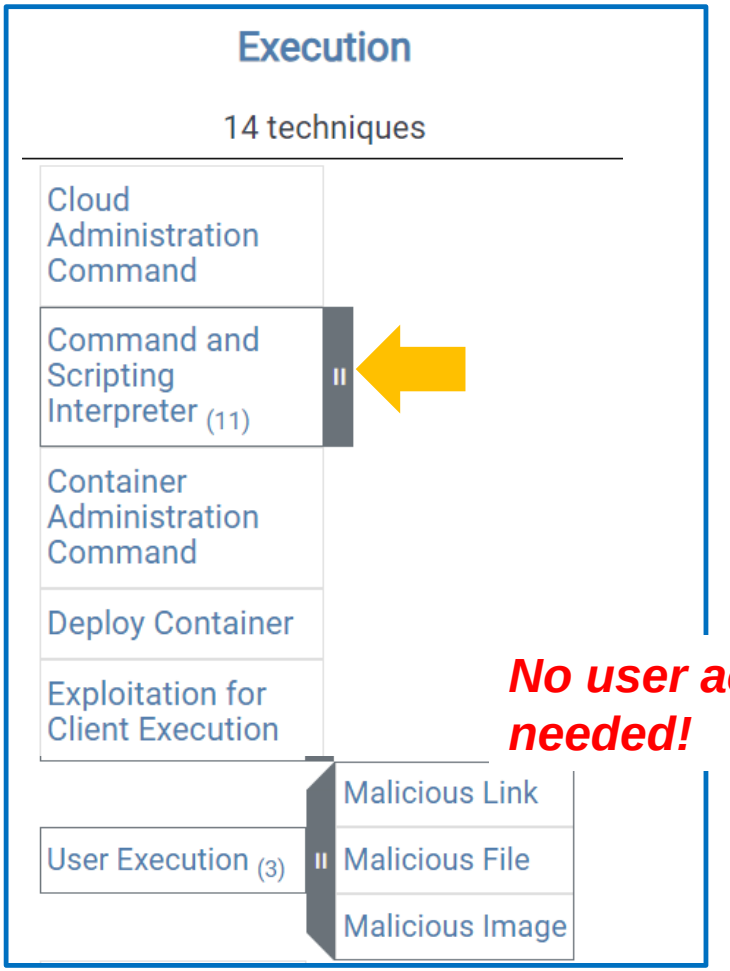
Example 4

- Server has RCE vulnerability

- Requirements:
  - Server accessible to Adversary
  - Adversary has exploit for that vulnerability

Mapping





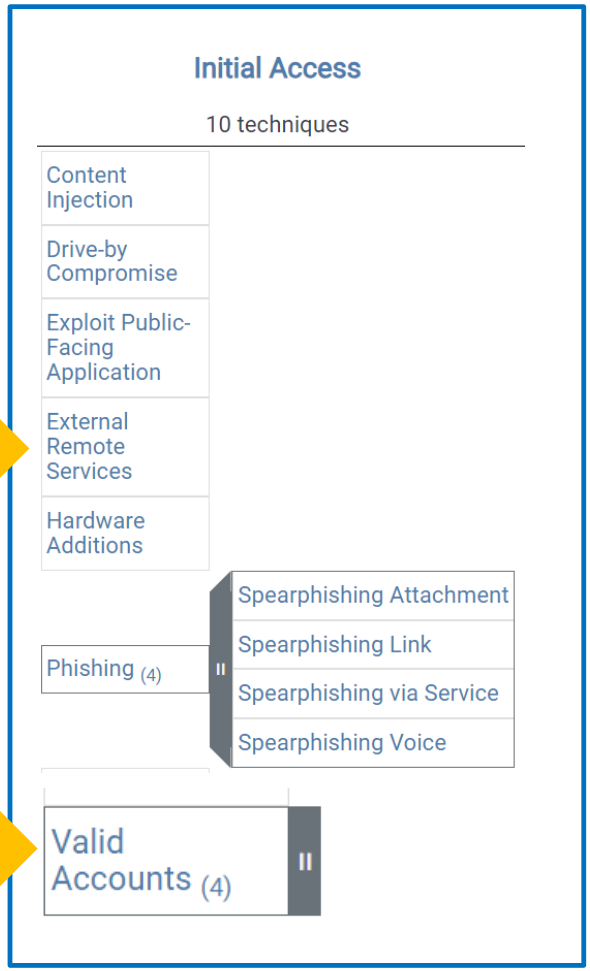
No user action needed!

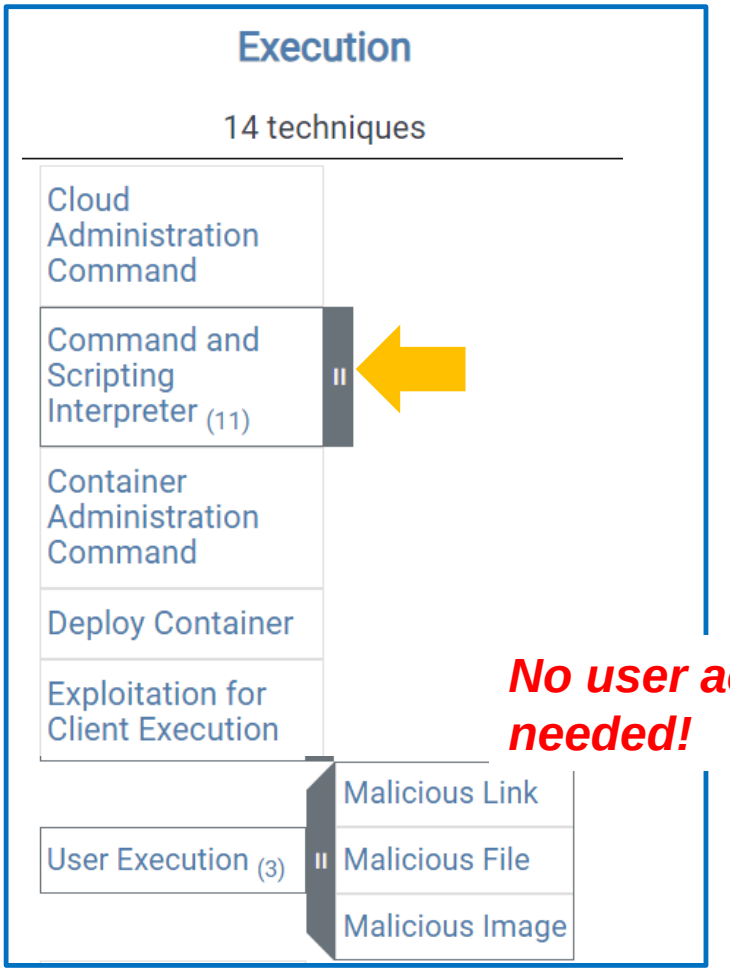
Example 5

- Server allows command execution through **credentials** (e.g., ssh, VPN, ...)

- Requirements:
  - Server accessible to Adversary
  - Adversary has valid credentials

Mapping





No user action needed!

What MITRE ATT&CK is (and is NOT)

What MITRE ATT&CK is NOT (I)

- For any given **technique**, we do **not** have any clue about:
  - **Frequency** / **Probability** of usage

- There are statistics
- But in cybersecurity we **never** know their **coverage**
  - How many incidents missing from the statistics?

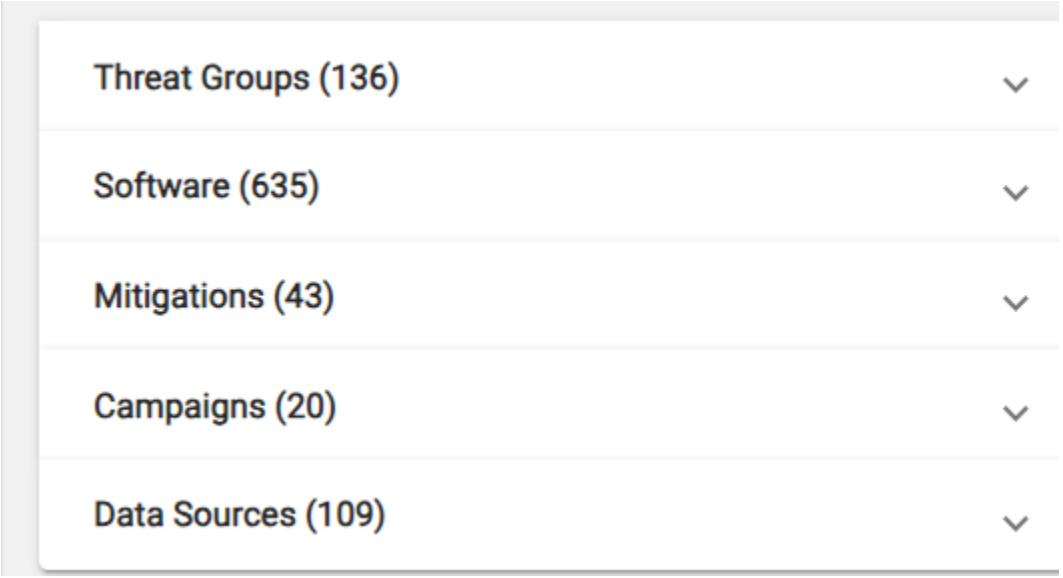
- ...nor their **bias**
  - Is the sample really relevant for "our" environment?

What MITRE ATT&CK is NOT (II)

- For any given **technique**, we do **not** have any clue about:
  - **Frequency** / **Probability** of usage
  - Whether it is **absolutely essential** for a given attacker
    - Stopping this technique stops the attack?

What MITRE ATT&CK is

- **Database** (with "links and navigation") for associating **tactics** / **techniques** with:



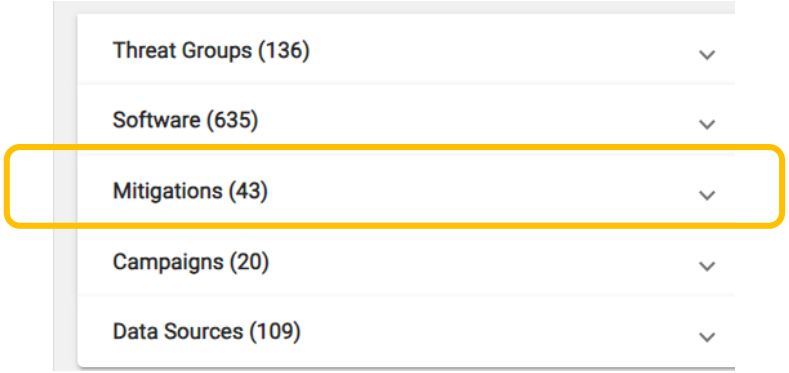
- Coverage obviously incomplete

Example: Mitigations

Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.

- Which **techniques** are covered by a certain **mitigation**?
- Which **mitigations** exist for a certain **technique**?

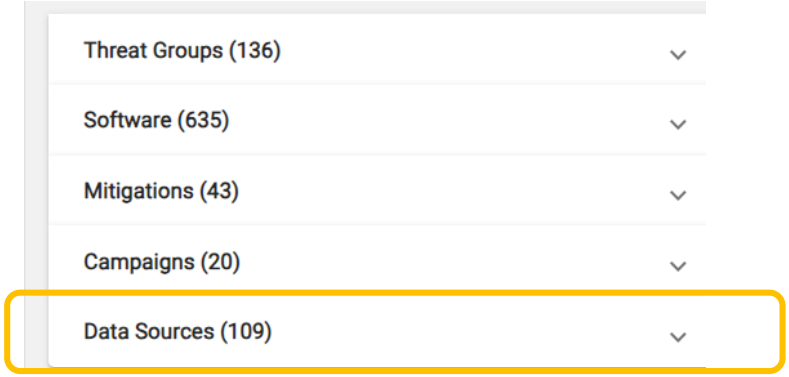


Example: Data Sources (≈"log")

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.

ID	Name	Domain	Description
DS0026	Active Directory	Enterprise	A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)
DS0015	Application Log	Enterprise ICS	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)

- Which **techniques** could be detected by a certain **data source**?
- Which **data source** could enable detecting a certain **technique**?

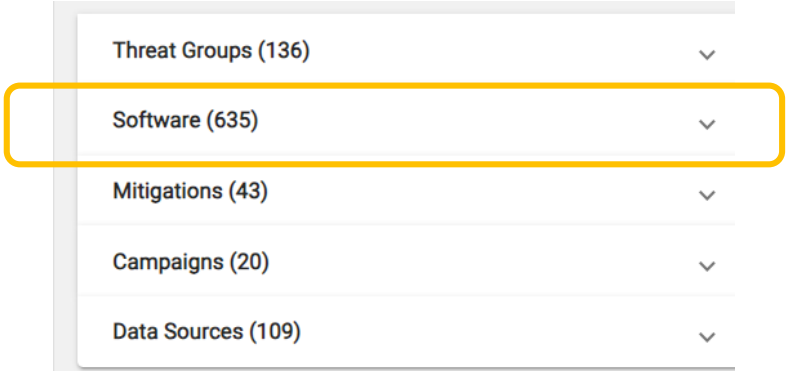


Example: Software (I)

CrackMapExec

CrackMapExec, or CME, is a post-exploitation tool developed in Python and designed for penetration testing against networks. CrackMapExec collects Active Directory information to conduct lateral movement through targeted networks.[1]

- ≈20 **techniques**



Example: Software (II)

- **Identify** all machines in an IP address range
  `cme smb IP-range`

Discovery

- **Attempt credentials** on all machines
  `cme smb IP-range -u username -p password`
  `(-H password-hash)`

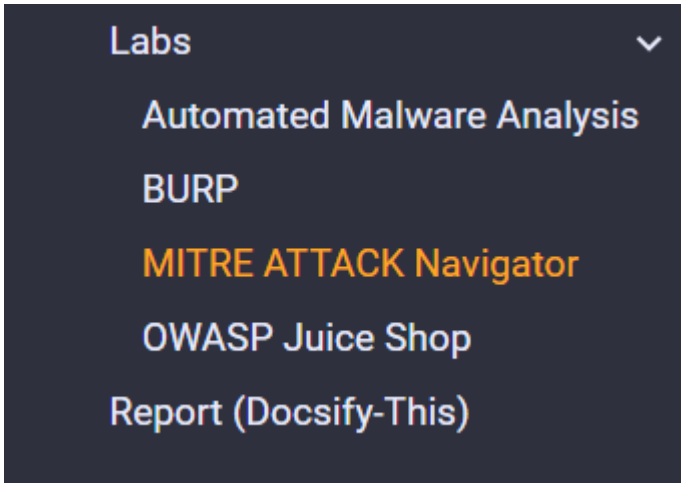
Lateral Movement

- **Extract password hashes** from all machines where local admin
  `cme smb IP-range -u username -p password`
  `-M mimikatz`

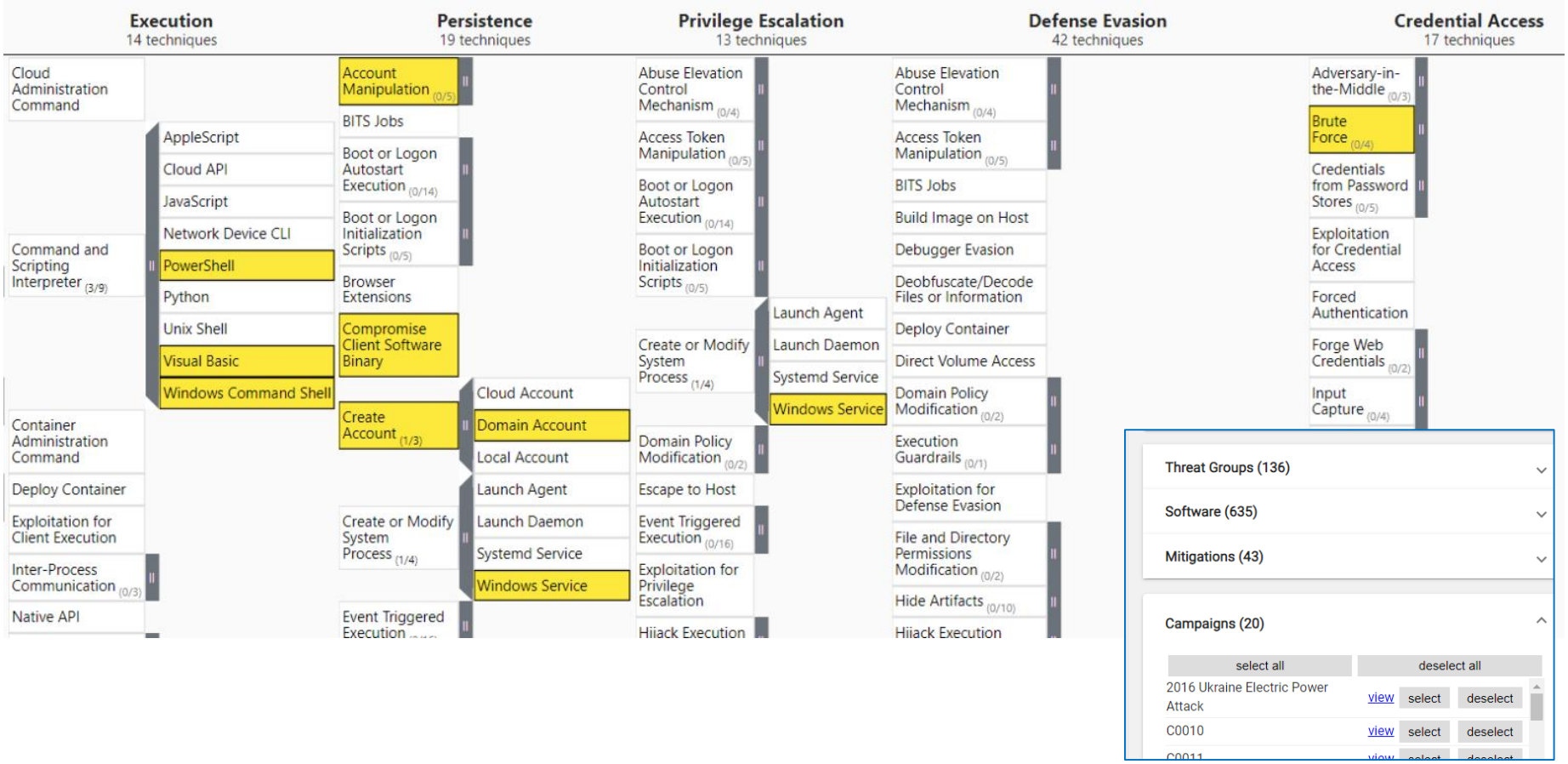
Credential Access

Example: Navigator

- Which **techniques** are covered by **my mitigations**?
- Which **techniques** are used by a certain **threat group**?
- Which techniques am I **missing** w.r.t. to a certain threat group?



Ukraine – Power Grid 2016 Campaign



WARNING

- ATT&CK® Navigator (mitre-attack.github.io)
  (the software)
- Matrix - Enterprise | MITRE ATT&CK®
  (the official database)

- **Not** aligned perfectly

Common Usage

- **Framework** for:
  - **Describing** attack campaigns
    (de facto standard in reports)
  - **Reasoning** about attacks and attack campaigns

- **Very powerful (conceptual) tool**

My suggestion

- For each **topic** covered in the course:
  1. Try to understand which **Tactic ("Why")** it relates to
  2. Then try to search it in Matrix / Navigator

- From our point of view, 1 is **more important** than 2
  - The "Why" (Tactic) helps to understand the "How" (Technique)
  - Many Techniques…impossible to know them all

Misconceptions

How you should think of MITRE ATT&CK

- An **attack campaign** corresponds to **a set** of "switched on cells"
- All **at the same time** and **with the same intensity**
- Distributed in some unpredictable way (i.e., not one in every column)

Misconception (I)

- **NO**:
  - An attack campaign involves **all** the Tactics

- **YES**:
  - One or more Tactics may be **absent** (or **not observed**)

Misconception (II)

- **NO**:
  - Each Technique is used for **one** Tactic
- **YES**:
  - A Technique may be used for **multiple** Tactics

Example

Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques
Valid Accounts (0/4)	Windows Management Instrumentation	Valid Accounts (0/4)	Valid Accounts (0/4)	XSL Script Processing
Trusted Relationship	User Execution (0/3)	Traffic Signaling (0/2)	Scheduled Task/Job (0/5)	Weaken Encryption (0/2)
Supply Chain Compromise (0/3)	System Services (0/2)	Server Software Component (0/5)	Process Injection (0/12)	Virtualization/Sandbox Evasion (0/3)
Replication Through Removable Media	Software Deployment Tools	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/12)	Valid Accounts (0/4)
Phishing (0/4)	Shared Modules	Pre-OS Boot (0/5)	Exploitation for Privilege Escalation	Use Alternate Authentication Material (0/4)
Hardware Additions		Power Settings		Unused/Unsupported Cloud

Valid Accounts

Sub-techniques (4)

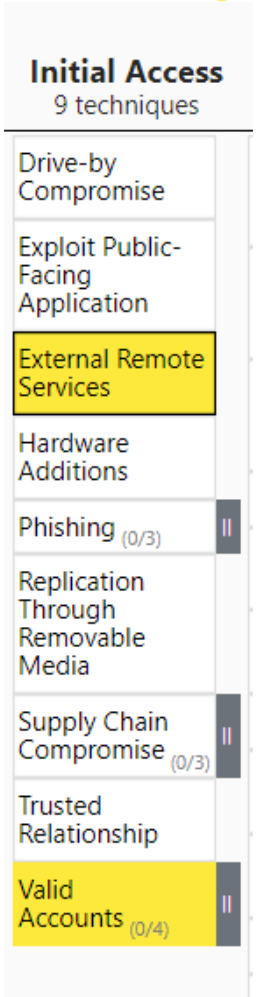
Adversaries may obtain and abuse credentials of existing accounts

Misconception (III)

- **NO**:
  - What we consider **one** "attack step" clearly corresponds to **one** specific Technique

- **YES**:
  - What we consider **one** "attack step" may correspond to one or **more** Techniques

Example (I)



- Campaign that used **multiple** techniques for Initial Access

Example (II)

Initial Access

11 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (4)

Defense Evasion

45 techniques

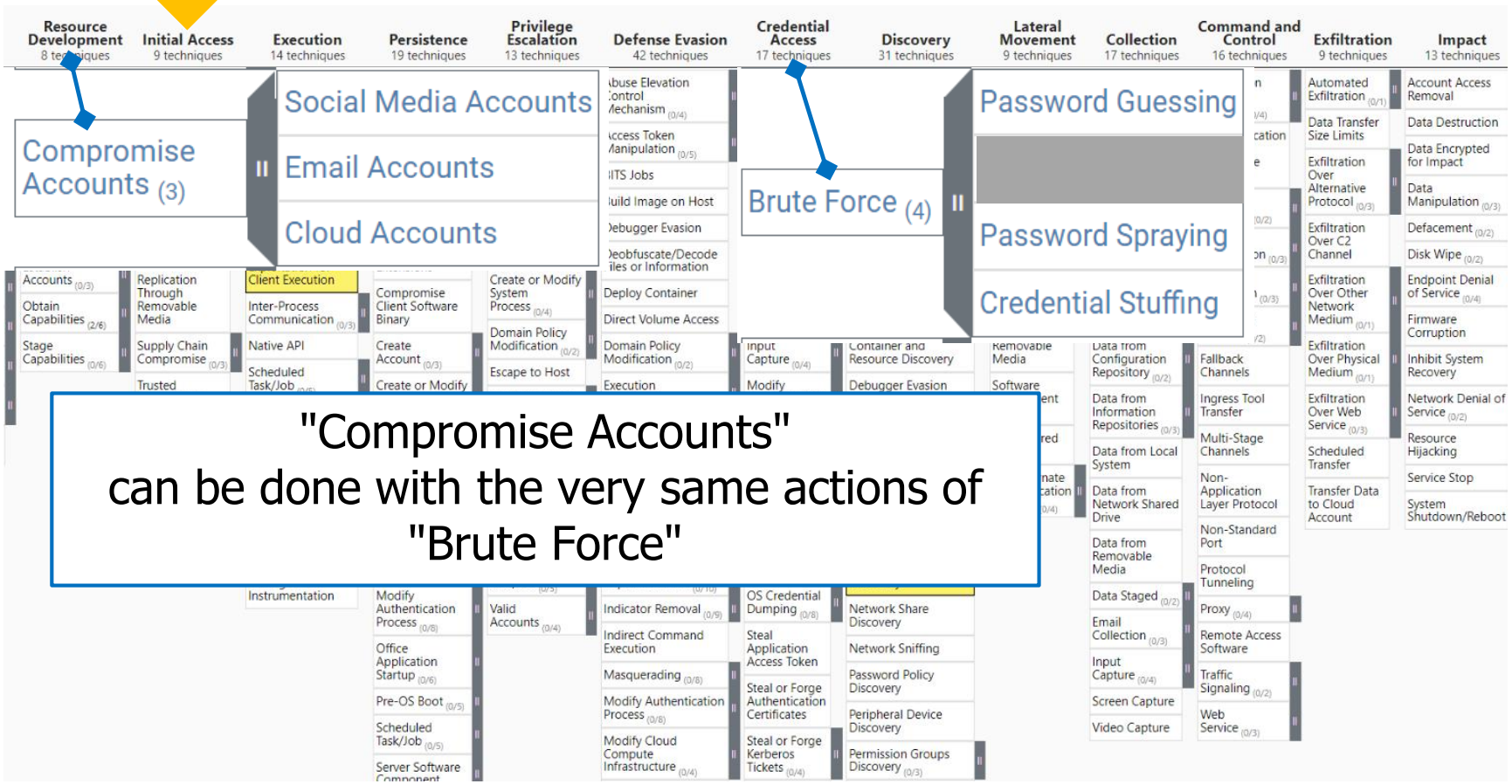
- Abuse Elevation Control Mechanism (6)
- Access Token Manipulation (5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (2)
- Email Spoofing
- Impersonation

Misconception (IV)

- **NO**:
  - What we consider "**the same actions**" corresponds to **the same Technique**

- **YES**:
  - What we consider "the same actions" **might** correspond to **different** Techniques

Example


Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact
Compromise Accounts (3)
Social Media Accounts
Email Accounts
Cloud Accounts
Brute Force (4)
Password Guessing
Password Spraying
Credential Stuffing
"Compromise Accounts"
can be done with the very same actions of
"Brute Force"

Misconception (V)

- **NO**:
  - **Single** flow of Tactics, left to right

- **YES**:
  - **Multiple** flows/loops of Tactics, **back and forth**

  - Left to right arrangement is mostly (but **not** completely) **logical**, not time-based

Example (I)

- …
- Discovery
- Lateral movement
- …
  - Machine M1 entered and controlled
  - Executing Discovery **again** usually provides further information…which may enable discovering M2
  - Machine M2 entered and controlled
  - Executing Discovery **again** usually provides further information…which may enable discovering M3

  - And in M2 / M3 you might need to execute Persistence again

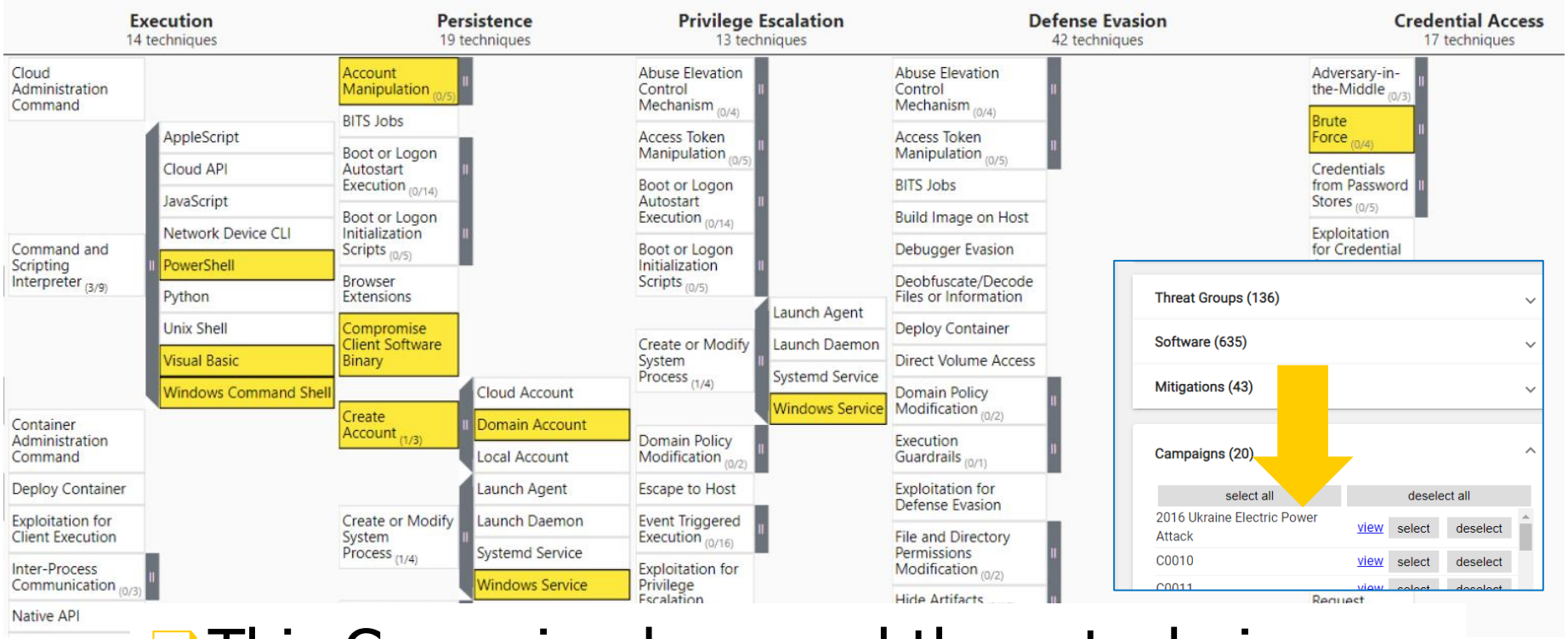
Example (II)

Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques

The **time** ordering might **not** be this one

The technique used for Persistence
(or for Privilege Escalation)
may have required Defense Evasion first

Example (III)



- This Campaign has used these techniques
- Order **not** apparent from the mapping