Attacks

Attacks

- Motivations
- Target categories
- Attacking each target category

Motivations

1. Money
2. Stealing of information
3. Disruption of operations

- Money is by far the **most frequent** motivation

How to obtain money (I)

- **MANY** (creative) ways
  - Banking credentials stolen and used
  - Credentials stolen and sold
  - Long term cookies stolen and sold
  - ...
  - Remote Access Trojans (remotely controllable malware) installed and sold / rented
  - ...

- Victim **not** aware of what happened

How to obtain money (II-a)

- Many (very creative) ways
  - ...
  - Steal data and ask ransom for not making it public
  - Encrypt data and ask ransom for decrypting it (**ransomware**)

How to obtain money (II-b)

- Steal data and ask ransom for not making it public
- Encrypt data and ask ransom for decrypting it (ransomware)
- **Huge** societal problem
  - Attack cost relatively low
  - Potential ROI (Return on Investment) huge

  ⇒ Lot of potential attackers

  - Anonymous payments worldwide
  - Data is crucial to "every organization"
  - Worldwide connectivity

  ⇒ Every organization is a potential target

Target Categories (I)

1. Organizations
2. Industrial Control Systems (ICS)
3. Single individuals

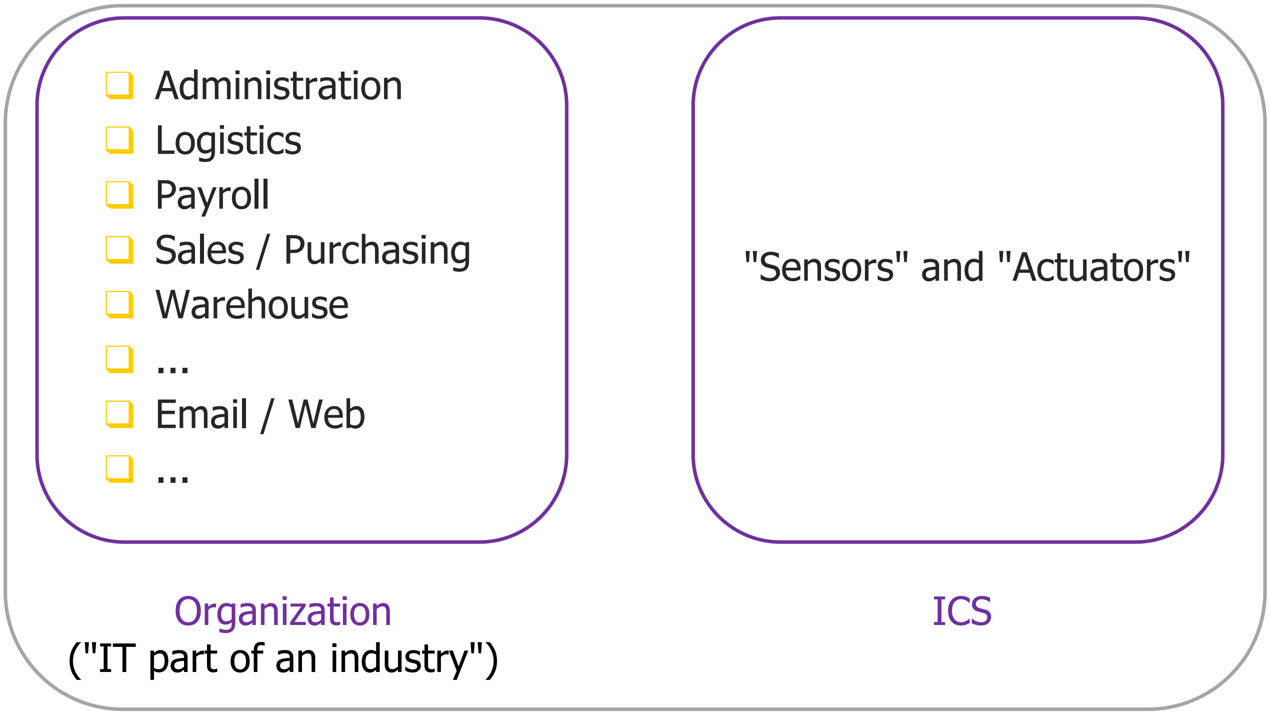
- Organization = "wherever there are servers and data"
- ICS = "sensors and actuators"

Organization

1. Organizations
   ("wherever there are servers and data")

- **Any** kind of organization
  - Hospitals
  - Administrative part of manufacturing companies
  - ...

Organization vs ICS



- Administration
- Logistics
- Payroll
- Sales / Purchasing
- Warehouse
- ...
- Email / Web
- ...

"Sensors" and "Actuators"

Organization
("IT part of an industry")

ICS

Target Categories (II)

- You can make **lot of money** with
  one Organization / lot of Single individuals
- Making money by attacking an ICS is much more difficult

- Attacks to Organizations / Single individuals
  ⇒**very frequent**
- Attacks to ICS
  ⇒ **rare**

Keep in mind

- Attacks are a **professional** activity
- Huge gains justify **huge investments**

- `search "conti diaries part 2"`
  - Tens of people hierarchically structured
  - Work around the clock
  - Teams update malware every 4 hours (update time of Windows Defender)

"Conti Tech Start-up"

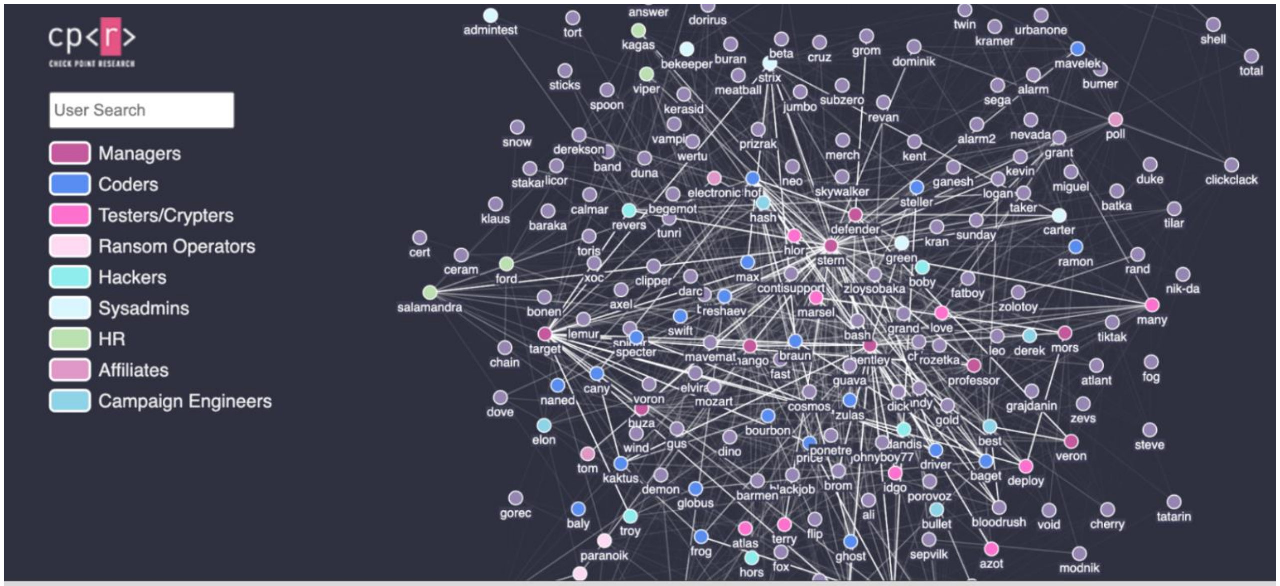


Immagine da research.checkpoint.com

Our next steps

- Attacks against **organizations**
  - Lateral movement
- ...against **single individuals**
- ...against **ICS**

Attacking an Organization

Attacking an Organization

- Several **phases**, each of several **steps**
- From **minutes** to **months**

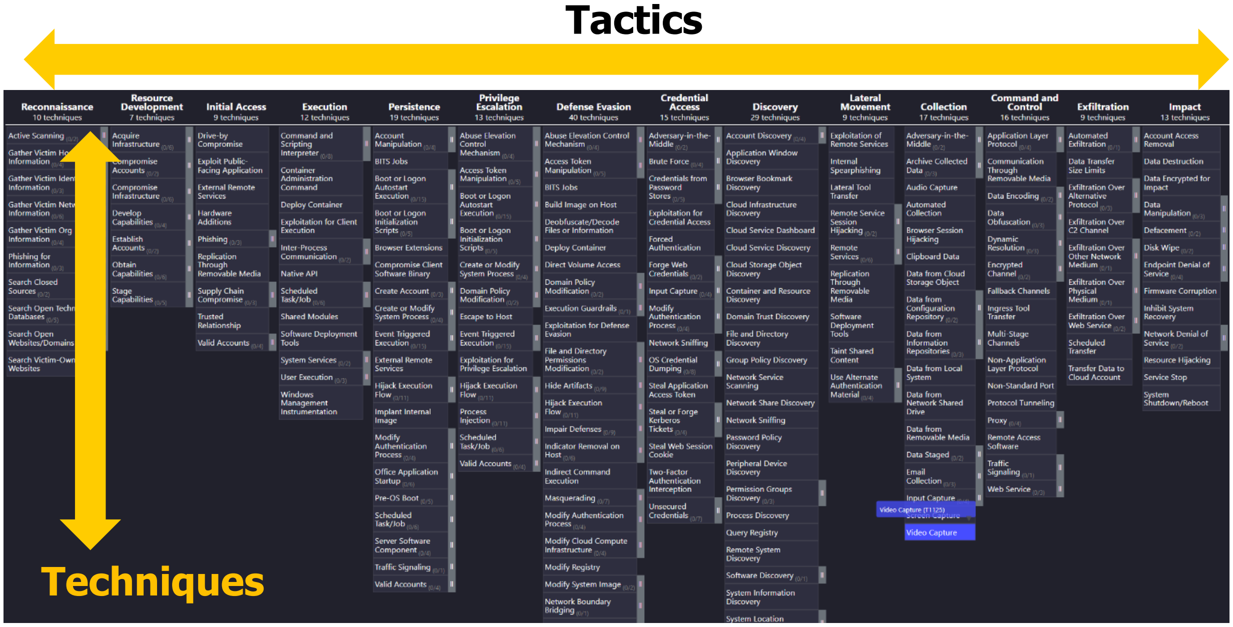
- Several **models** for **describing** attack phases
  - Kill chain (first widely used)
  - ...
  - MITRE ATT&CK ("the" model today)

MITRE ATT&CK (I)

- Currently **the** reference framework
- Built upon **observations** of **many real attacks**

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

MITRE ATT&CK Matrix

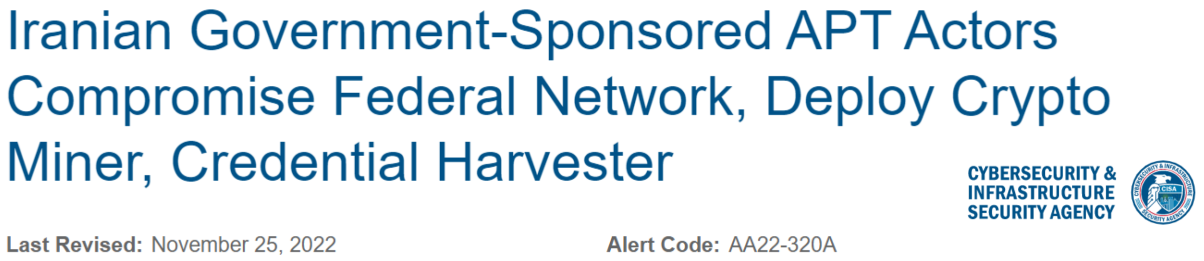


Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/2)	Acquire Infrastructure (0/6)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/4)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/2)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/2)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Ho Information (0/4)	ompromise Accounts (0/2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Ident Information (0/3)	Compromise Infrastructure (0/6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/15)	Boot or Logon Autostart Execution (0/15)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Netw Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Inter-Process Communication (0/2)	Browser Extensions	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deploy Container	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/5)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/6)	Create Account (0/3)	Escape to Host	Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Techn Databases (0/5)		Trusted Relationship	Shared Modules	Create or Modify System Process (0/4)	Event Triggered Execution (0/15)	Domain Policy Modification (0/2)	Modify Authentication Process (0/4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains		Valid Accounts (0/4)	Software Deployment Tools	Event Triggered Execution (0/15)	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Own Websites			System Services (0/2)	External Remote Services	Hijack Execution Flow (0/11)	Exploitation for Defense Evasion	OS Credential Dumping (0/8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			User Execution (0/3)	Hijack Execution Flow (0/11)	Process Injection (0/11)	File and Directory Permissions Modification (0/2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (0/6)	Hide Artifacts (0/9)	Steal or Forge Kerberos Tickets (0/4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (0/4)	Valid Accounts (0/4)	Hijack Execution Flow (0/11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
				Office Application Startup (0/6)		Impair Defenses (0/9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (0/3)	Remote Access Software		
				Pre-OS Boot (0/5)		Indicator Removal on Host (0/6)	Unsecured Credentials (0/7)	Password Policy Discovery		Input Capture (0/4)	Traffic Signaling (0/1)		
				Scheduled Task/Job (0/6)		Indirect Command Execution		Peripheral Device Discovery		Screen Capture	Web Service (0/3)		
				Server Software Component (0/4)		Masquerading (0/7)		Permission Groups Discovery (0/3)		Video Capture			
				Traffic Signaling (0/1)		Modify Authentication Process (0/4)		Process Discovery					
				Valid Accounts (0/4)		Modify Cloud Compute Infrastructure (0/4)		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (0/2)		Software Discovery (0/1)					
						Network Boundary Bridging (0/1)		System Information Discovery					
								System Location					

MITRE ATT&CK (II)

- Periodically **updated** to reflect more recent/accurate knowledge
  - October 2022: v12
  - April 2023: v13
  - October 2023: v14
- Three variants
  - Enterprise (may be specialized for Windows, Linux, Cloud,...)
  - Mobile (may be specialized for Android / iOS)
  - ICS
- Reports describe campaigns in terms of MITRE ATT&CK

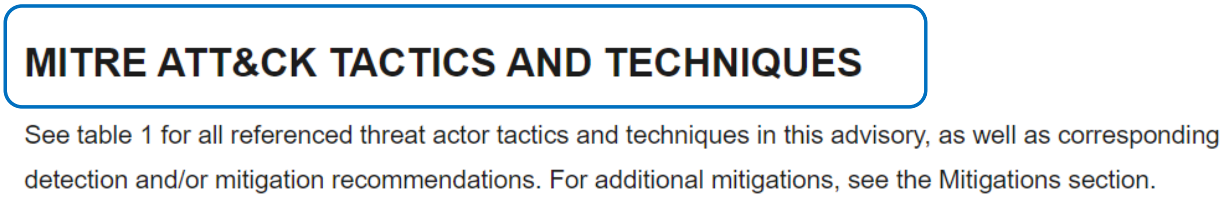
Example



Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Last Revised: November 25, 2022 **Alert Code:** AA22-320A

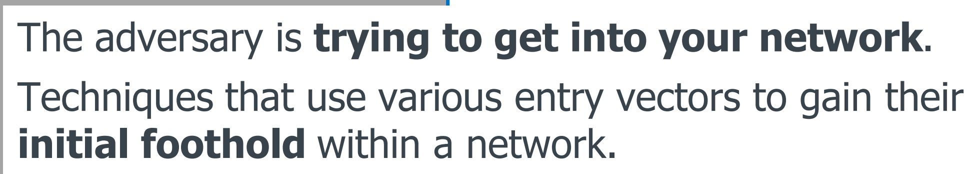


MITRE ATT&CK TACTICS AND TECHNIQUES

See table 1 for all referenced threat actor tactics and techniques in this advisory, as well as corresponding detection and/or mitigation recommendations. For additional mitigations, see the Mitigations section.

"Gain foothold" (I-a)

- Initial Access



The adversary is **trying to get into your network**.

Techniques that use various entry vectors to gain their **initial foothold** within a network.

"Gain foothold" (I-b)

- Initial Access

- **Drive-by Compromise** User visiting a website over the normal course of browsing. Vulnerability exploitation.
- **Exploit Public-Facing Application** Vulnerability exploitation in an Internet-facing computer or program (e.g., web site)
- **Phishing**. Malicious attachments or links in emails
- **Valid Accounts**. Abuse of compromised credentials

(+5 Techniques) MITRE ATT&CK

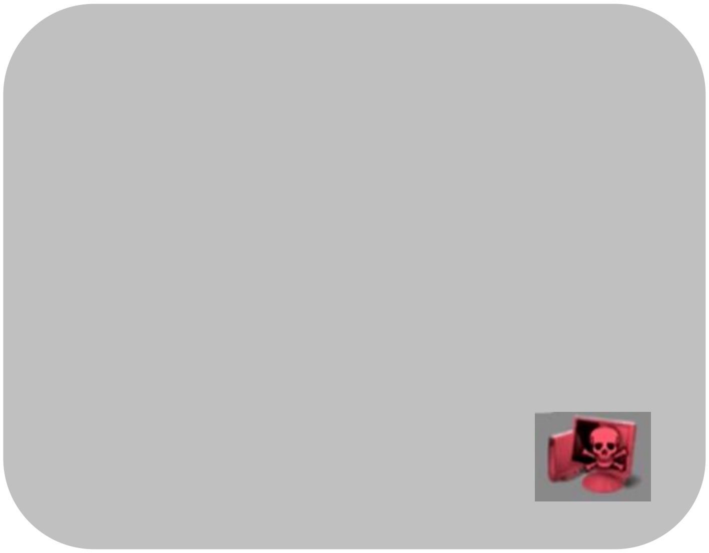
"Gain foothold" (II)

- Initial Access
- Execution
- Persistence

Execution techniques that result in **adversary-controlled** code running within the organization
(12 techniques)

Persistence techniques for **keeping access** to systems **across restarts**, **changed credentials**, and other interruptions that could cut off their access.
(19 techniques)

Scenario so far



Command & Control (C&C)

- ❑ Initial Access
- ❑ Execution
- ❑ Persistence
- ❑ C&C (**Command** & **Control**)

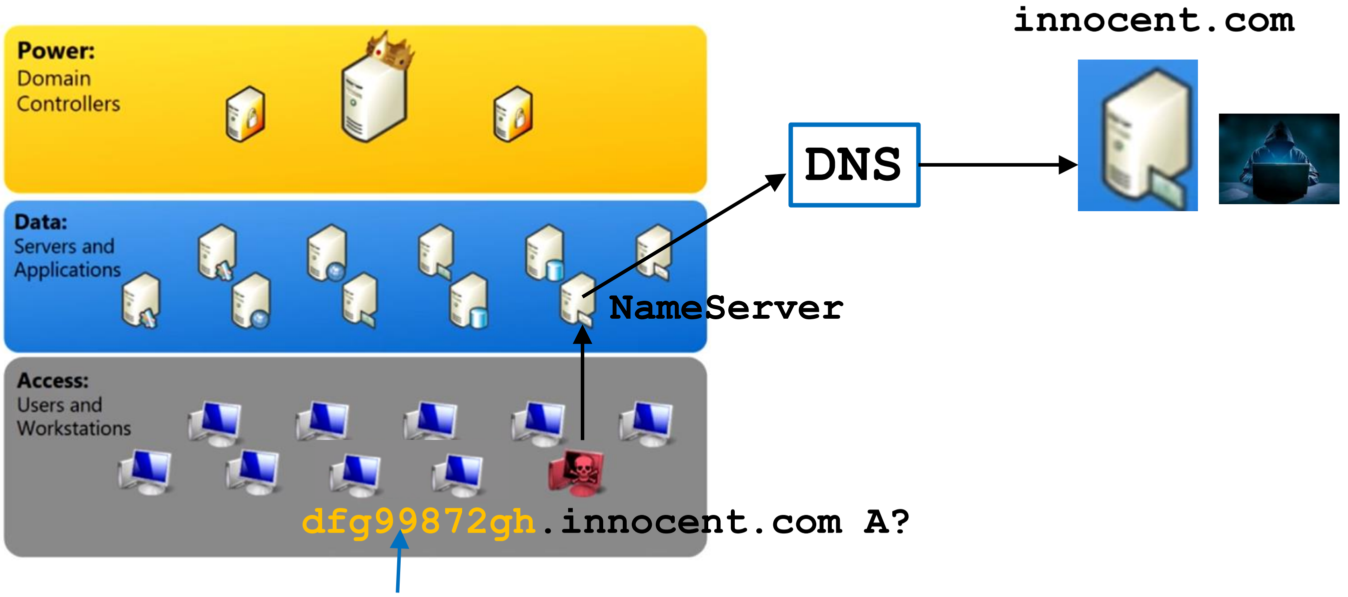
Techniques that adversaries may use to **communicate with systems under their control** within a victim network.

Adversaries commonly attempt to **mimic normal**, expected traffic to **avoid detection**.

Location of the adversary must be **obfuscated**.

(16 Techniques)

Example (outline): DNS Tunneling (I)



innocent.com

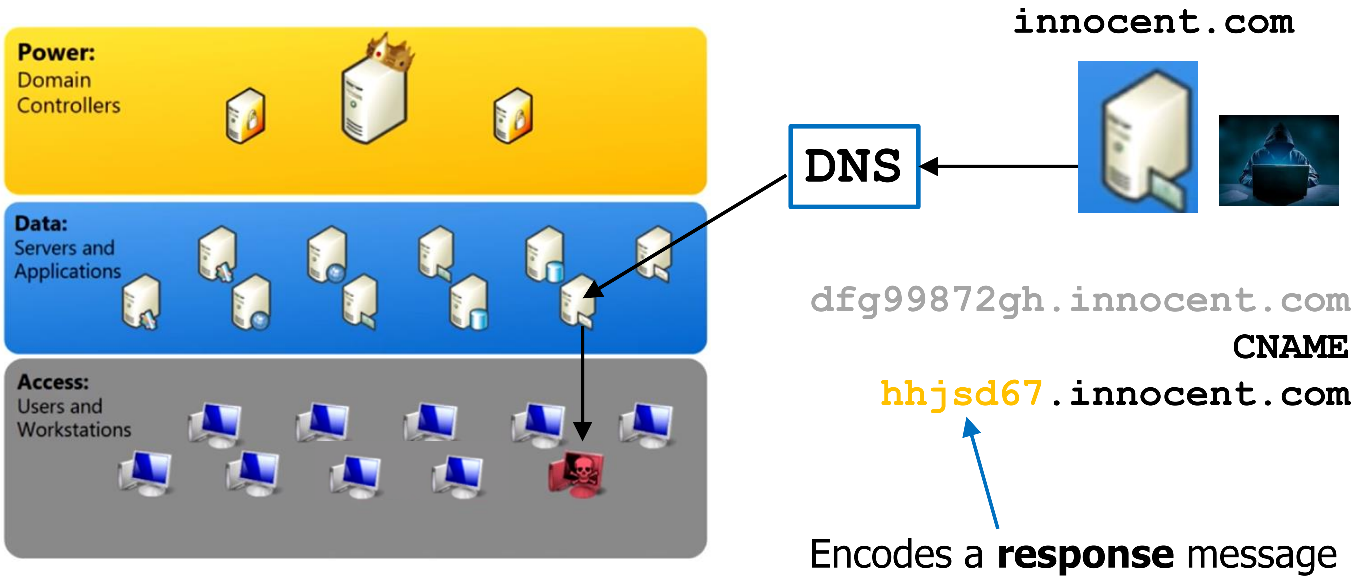
DNS

NameServer

dfg99872gh.innocent.com A?

Encodes a **request** message to attacker

Example (outline): DNS Tunneling (II)



innocent.com

DNS

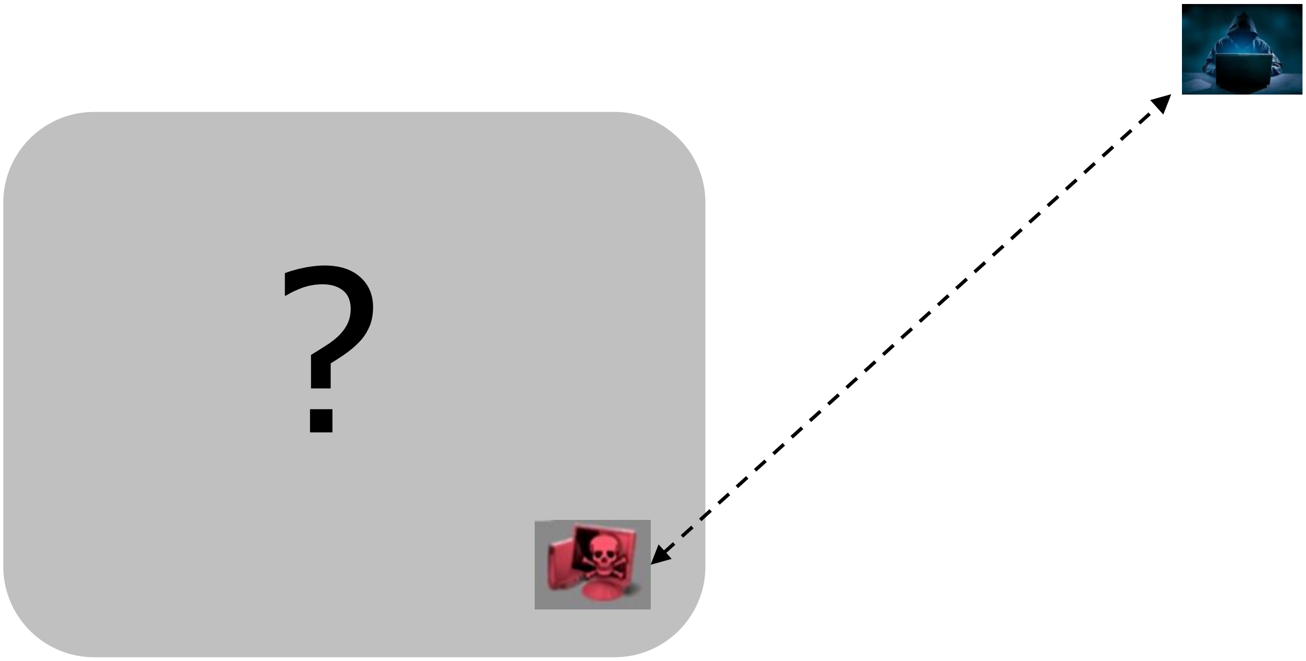
dfg99872gh.innocent.com

CNAME

hhjsd67.innocent.com

Encodes a **response** message from attacker

Scenario so far



"Look around"

- Initial Access
- Execution
- Persistence
- C&C (Command & Control)
- Discovery

Techniques to **gain knowledge** about the internal environment and decide how to act

- Networks, Hosts, Devices
- Applications
- Users, Groups, Access Rights
  (29 Techniques)

Example: nmap

- Nmap ("Network Mapper") is an open source tool for **network exploration** and **security auditing**.
- It was designed to rapidly scan large networks, although it works fine against single hosts.
- Nmap uses raw IP packets in novel ways to determine
  - what **hosts** are available on the network,
  - what **services** (application name and version) those hosts are offering,
  - what **operating systems** (and OS **versions**) they are running,
  - what type of **packet filters/firewalls** are in use,
  - and dozens of other characteristics.
- Usually quite noisy...

"Walk around"

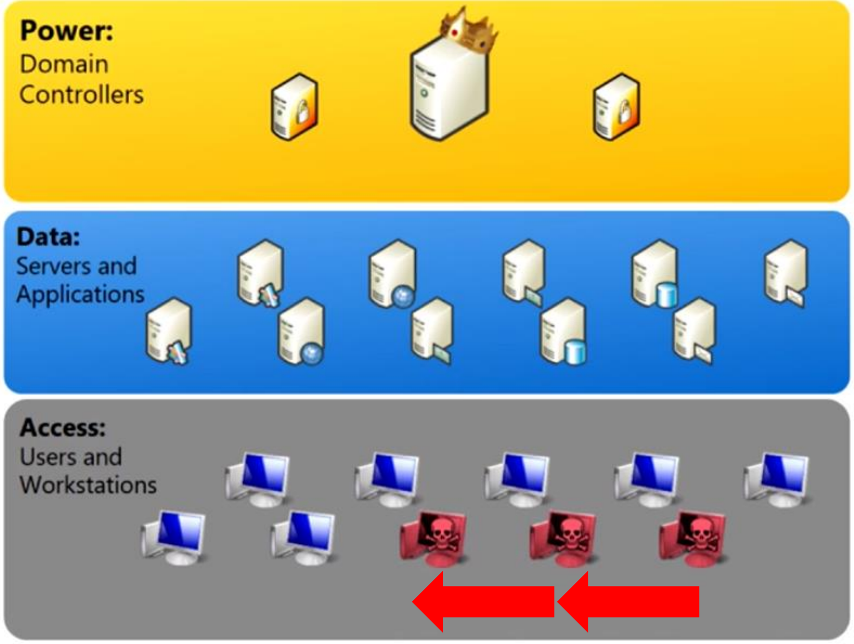
- Initial Access
- Execution
- Persistence
- C&C (Command & Control)
- Discovery
- Lateral movement

Techniques to **enter** and **control** remote systems

(9 Techniques)

We will discuss this phase later

Lateral Movement



Privilege Escalation (I)

- Initial Access
- Execution
- Persistence
- C&C (Command & Control)
- Discovery
- Lateral movement
- Privilege escalation

Techniques for **gaining higher-level permissions** on a system or network

(13 Techniques)

Privilege Escalation (II-a)

Privilege Escalation

13 techniques

- **Exploitation for privilege escalation**
  Adversaries may exploit software **vulnerabilities** in an attempt to elevate privileges.

- **Valid Accounts**
  Adversaries may obtain and abuse **credentials of existing accounts**. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence.

Privilege Escalation (II-b)

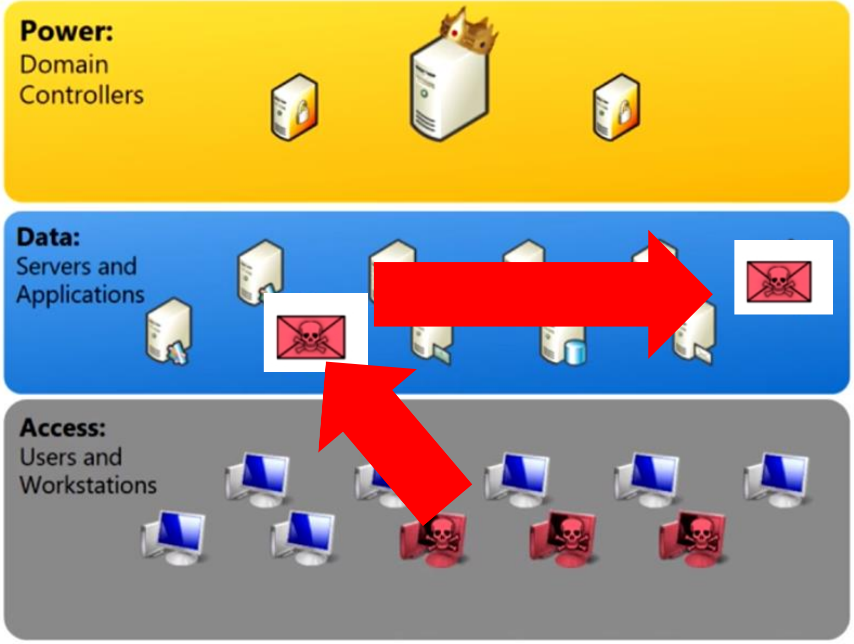
Privilege Escalation

13 techniques

- **Domain policy modification**
  Adversaries may **modify the configuration** settings of a domain to escalate privileges in domain environments... Since domain configuration settings control many of the interactions within the Active Directory (AD) environment, there are a great number of potential attacks that can stem from this abuse.
- **...**

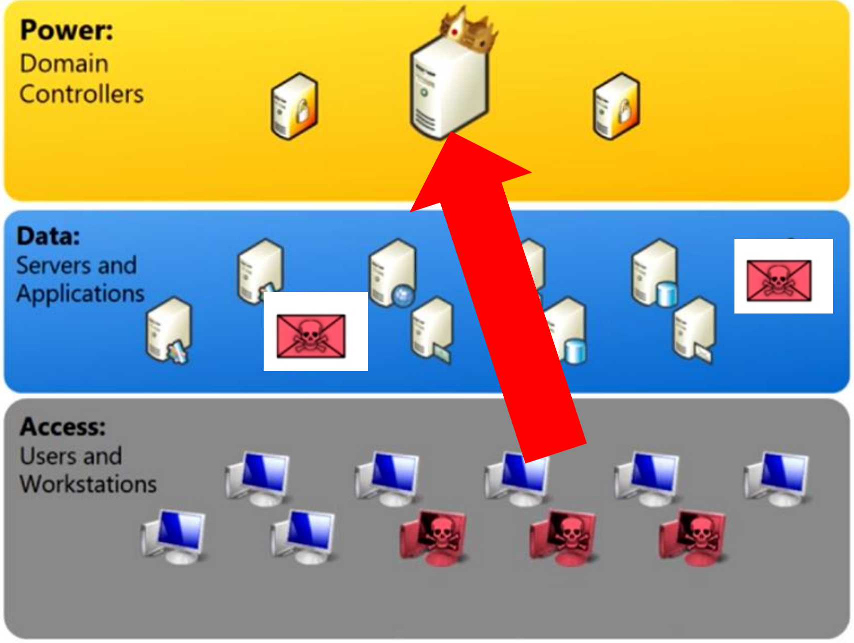
(+10 more techniques)

Lateral Movement after Privilege Escalation (I)



- Attacker can access "data"
- Which data and which access rights will depend on the available credentials

Lateral Movement after Privilege Escalation (II)



Total Catastrophe

Exfiltrate

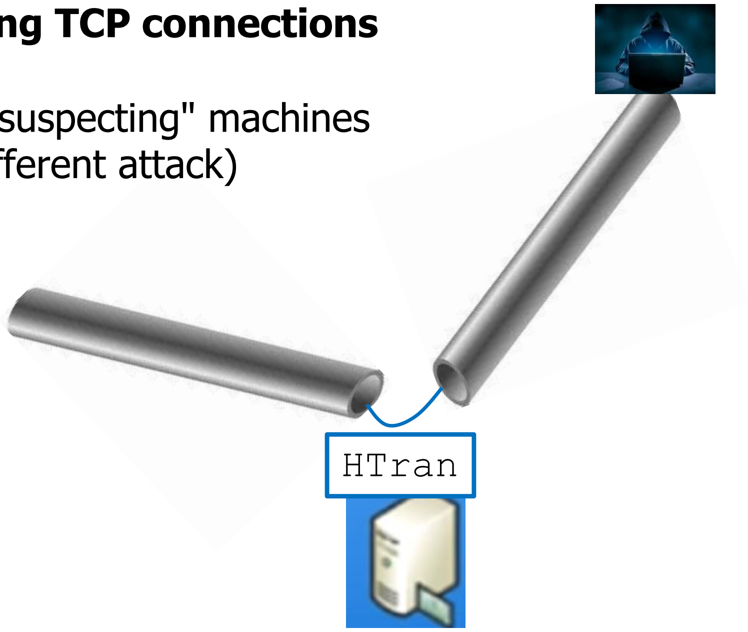
- Initial Access
- Execution
- Persistence
- C&C (Command & Control)
- Discovery
- Lateral movement
- Privilege escalation
- Exfiltration

- **Steal data**
- Transferring it over their C&C channel or an alternate channel
- Compression, Encryption, Size limits

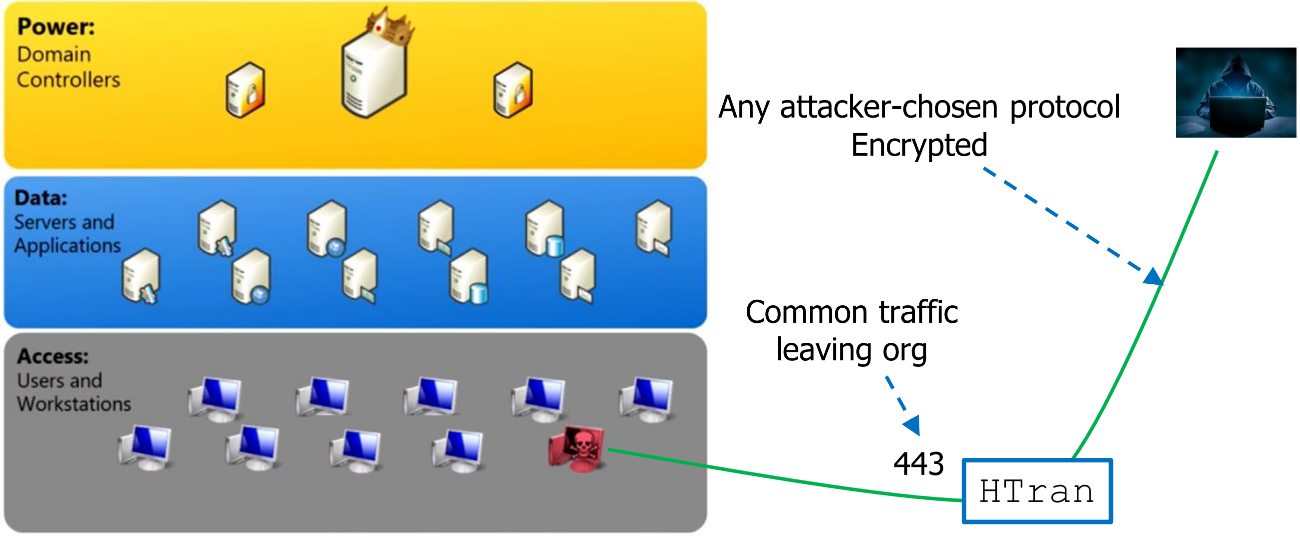
(9 Techniques)

Example: HTran (I)

- Tool for **proxying TCP connections**
- Installed on "unsuspecting" machines (with a prior, different attack)



Example: `HTran` (II-a)



Any attacker-chosen protocol
Encrypted

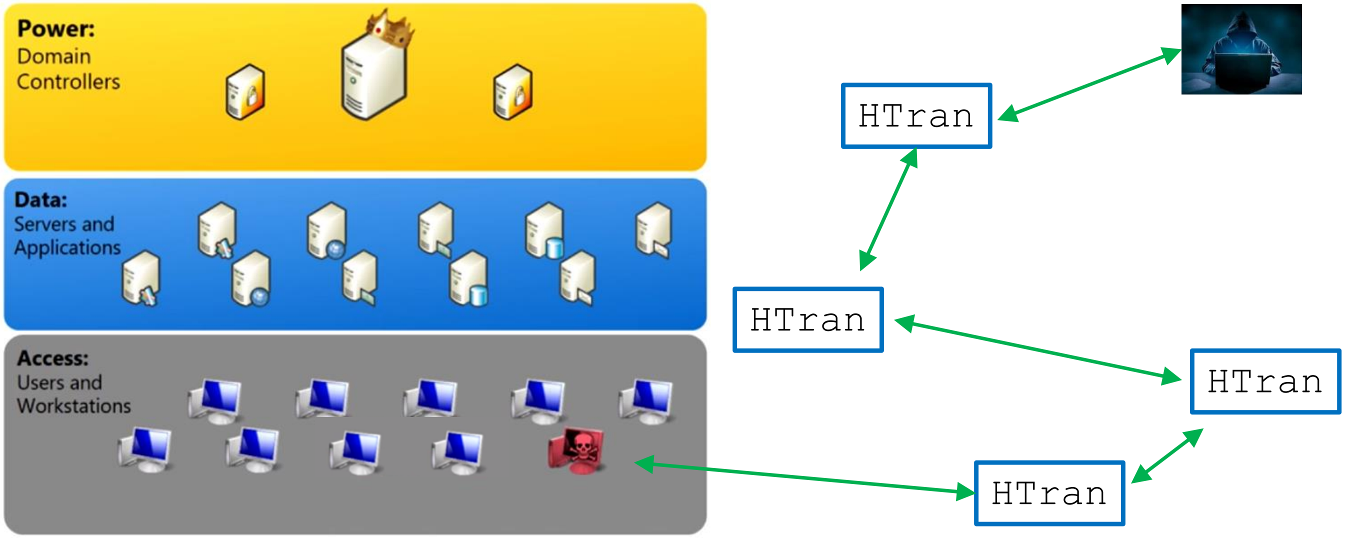
Common traffic
leaving org

443

`HTran`

- "By using HTran in this way, the threat actor... **several months** without being detected."

Example: `HTran` (II-b)



`HTran`

`HTran`

`HTran`

`HTran`

- "By using HTran in this way, the threat actor... **several months** without being detected."

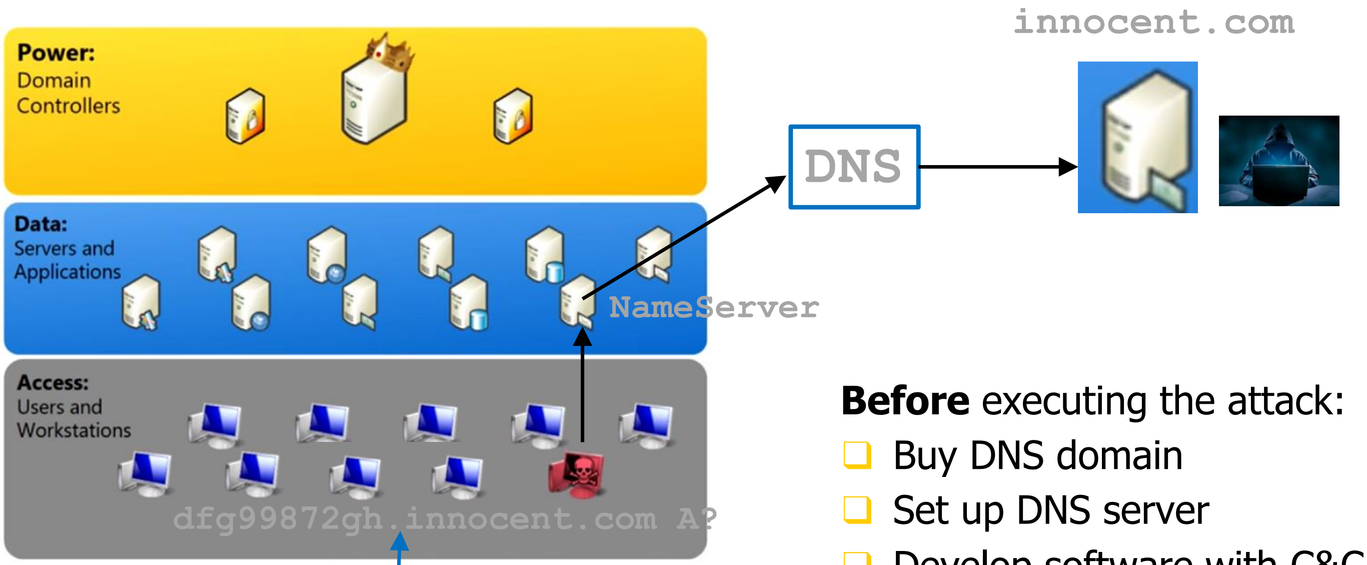
One sequence does not fit all

- …
- ~~Exfiltration~~ Impact

- **Impact** Manipulate, interrupt, or destroy your systems and data (≈~~secrecy~~, availability, integrity)
- Examples: **ransomware**, web defacement, disk wiping, ...

(13 techniques)

REMIND



Encodes a **request** message to attacker

Before executing the attack:

- Buy DNS domain
- Set up DNS server
- Develop software with C&C protocol

Before Initial Access

- **Resource Development** Establish resources for supporting future operations
- Create, purchase, steal resources (software, infrastructure, accounts, capabilities) (7 techniques)

- Initial Access
- Execution
- Persistence
- C&C
- Discovery
- Lateral movement
- Exfiltration

Even before...

- **Reconnaissance** Gather information for planning future operations (10 techniques)

- **Resource Development** Establish resources for supporting future operations
- Create, purchase, steal resources (software, infrastructure, accounts, capabilities) (7 techniques)

- Initial Access
- Execution
- Persistence
- C&C
- Discovery
- Lateral movement
- Exfiltration

Defense:
A Few Key Remarks

Defense:
A Few Key Remarks (I)

- Insisting on **complete prevention of Initial Access** is usually **meaningless** (perimeter just too large)
- Attacks **never** consist of **one** single step

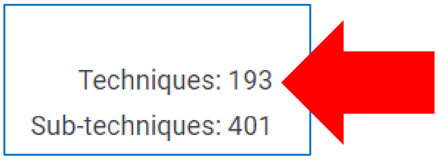
↓

- Defensive budget should be distributed across **all** attack phases
- A strong defense on a **few techniques** may suffice to **disrupt the attack** ("kill chain")

Defense:
A Few Key Remarks (II)

- Defensive budget should be distributed across **all** attack phases
- Defense must consist of:
  - **Mitigation**
    - "Prevent a technique from being successfully executed" = make attacks more difficult
  - **Detection**
  - **Remediation**
    - Backups

Defense:
A Few Key Remarks (III)



Techniques: 193

Sub-techniques: 401

- **Our job is very difficult**
  - **Real** complexity (not an ATT&CK artifact)
  - It is unlikely that we really understand all the techniques

- We need **systematic methods** for:
  - **Understanding** the **scope** of defensive mechanisms
  - **Prioritizing** techniques
  - Understanding the (potential) scope of **data sources**

Understanding MITRE ATT&CK

Attack vs MITRE ATT&CK ?

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

- Given a specific attack
- How is it mapped on Tactics and Techniques?

Attack vs MITRE ATT&CK (I)

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

- **NO**:
  - Touching **all** the Tactics

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

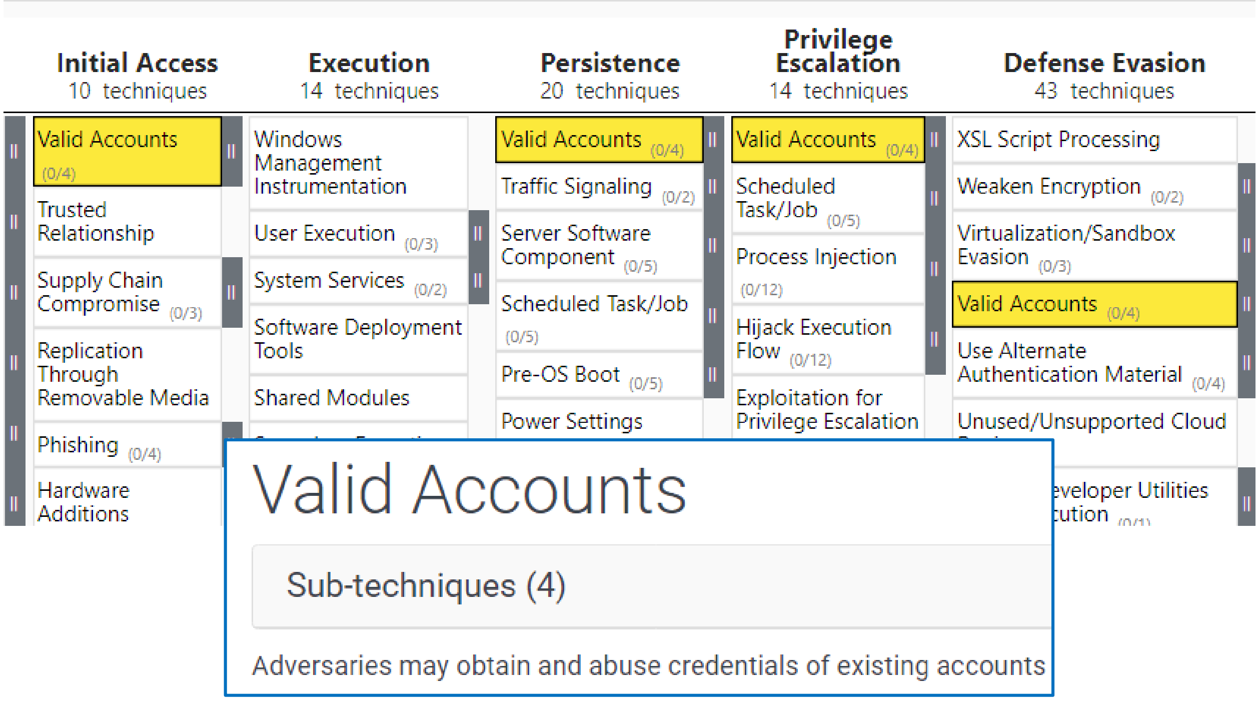
Attack vs MITRE ATT&CK (II)

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

- **NO**:
  - Each Technique is used for a specific 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
				eveloper Utilities cution (0/1)

Valid Accounts

Sub-techniques (4)

Adversaries may obtain and abuse credentials of existing accounts

Attack vs MITRE ATT&CK (III)

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

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

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

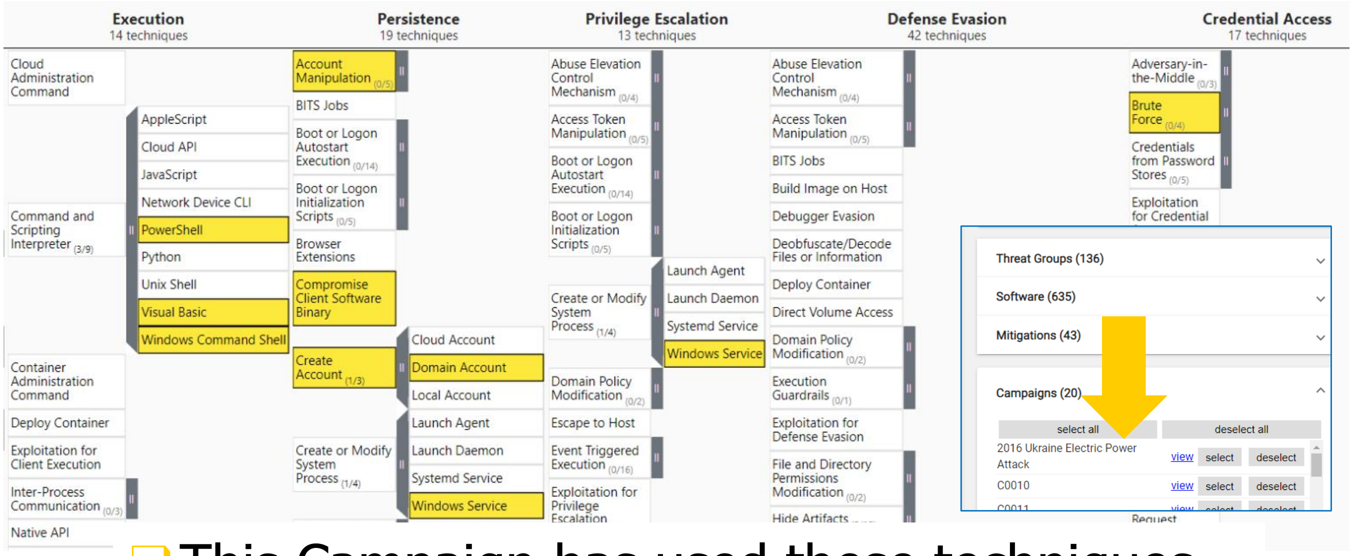
Example (I)

- …
- 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)



Execution
14 techniques

Cloud Administration Command
Command and Scripting Interpreter (3/9)
AppleScript
Cloud API
JavaScript
Network Device CLI
PowerShell
Python
Unix Shell
Visual Basic
Windows Command Shell
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API

Persistence
19 techniques

Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (1/3)
Cloud Account
Domain Account
Local Account
Create or Modify System Process (1/4)
Launch Agent
Launch Daemon
Systemd Service
Windows Service

Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (1/4)
Launch Agent
Launch Daemon
Systemd Service
Windows Service
Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for Privilege Escalation

Defense Evasion
42 techniques

Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts

Credential Access
17 techniques

Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Request

Threat Groups (136)
Software (635)
Mitigations (43)
Campaigns (20)

2016 Ukraine Electric Power Attack

C0010

C0011

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

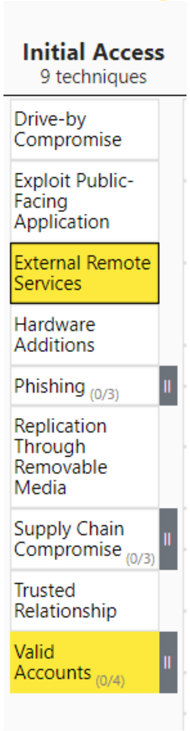
Attack vs MITRE ATT&CK (IV)

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

- **NO**:
  - Every attack step clearly corresponds to **one** specific Technique

- **YES**:
  - Every attack step may correspond to one or **more** Techniques (even in **different Tactics)**

Example



Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

- Campaign that used multiple techniques for Initial Access

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

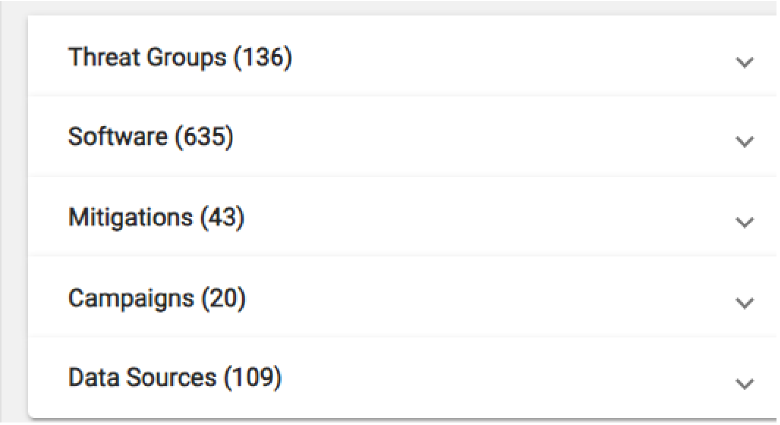
- There are statistics
- But in cybersecurity we **never** know their **coverage**
  - How many incidents missing from the statistics?
- ...nor their **bias**
  - Is the sample really relevant for "our" environment?

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:



Threat Groups (136)

Software (635)

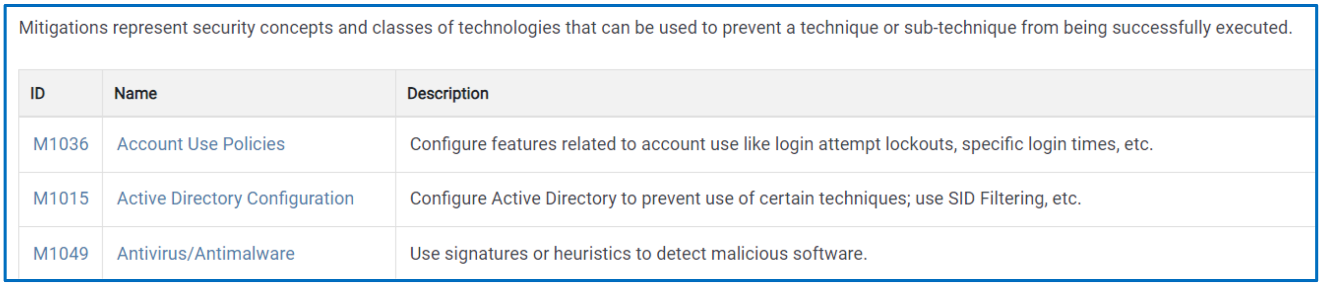
Mitigations (43)

Campaigns (20)

Data Sources (109)

- Coverage obviously incomplete

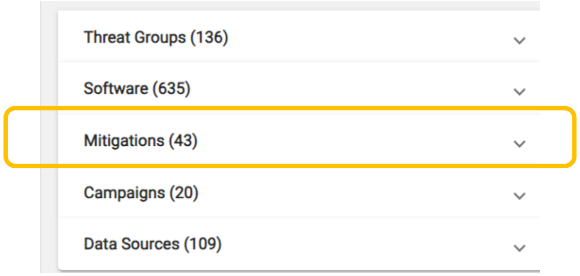
Example: Mitigations



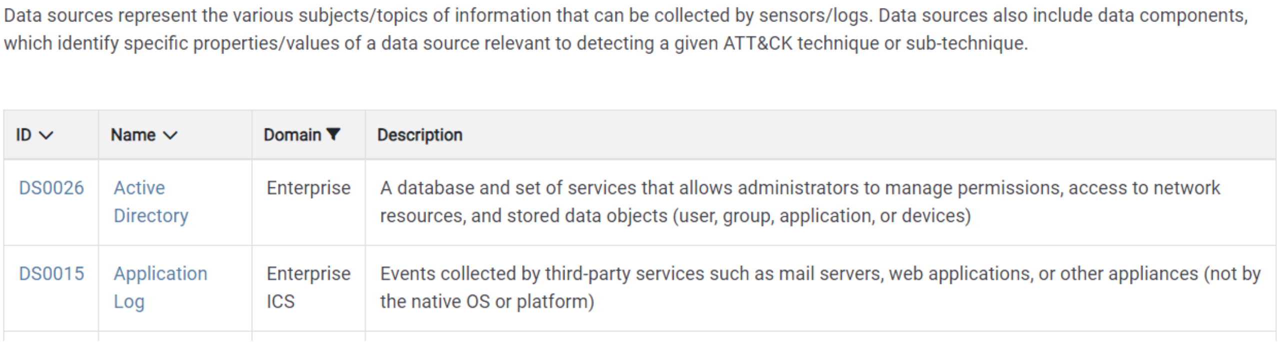
Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed.

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**?



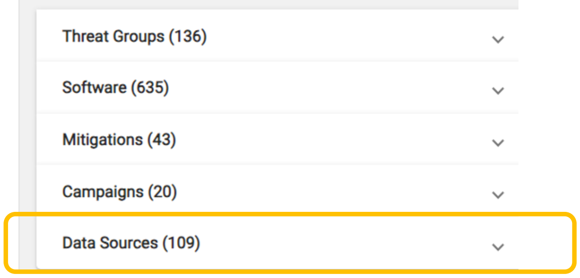
Example: Data Sources (≈"log")



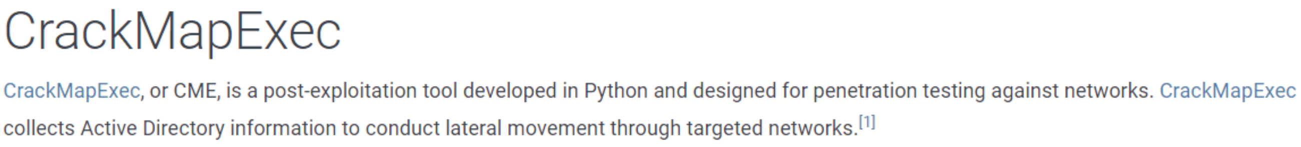
Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.

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**?



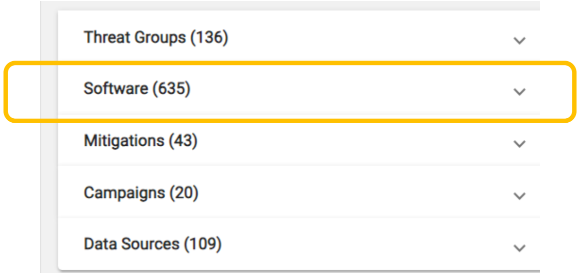
Example: Software (I)



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

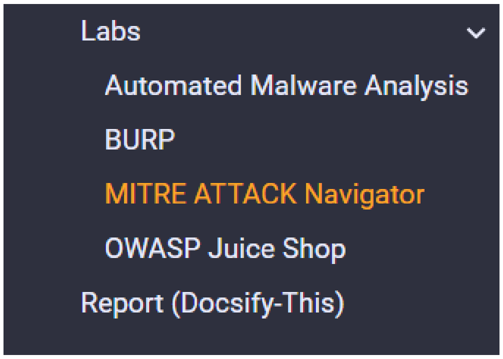
- **Extract password hashes** from all machines where local admin

```
cme smb IP-range   -u username -p password
                   -M mimikatz
```

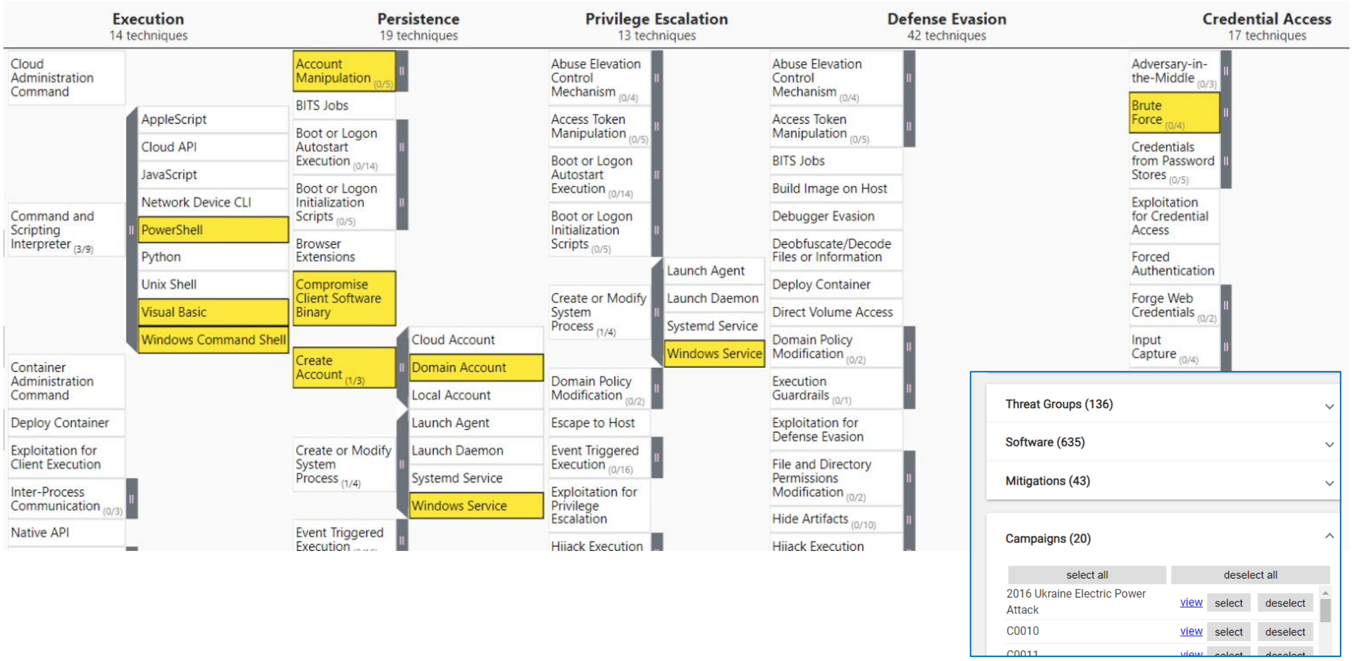
Credential Access

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



Execution
14 techniques

Cloud Administration Command
Command and Scripting Interpreter (3/9)
- AppleScript
- Cloud API
- JavaScript
- Network Device CLI
- PowerShell
- Python
- Unix Shell
- Visual Basic
- Windows Command Shell

Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (0/3)
Native API

Persistence
19 techniques

Account Manipulation (0/5)
BITS Jobs
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Browser Extensions
Compromise Client Software Binary
Create Account (1/3)
- Cloud Account
- Domain Account
- Local Account

Create or Modify System Process (1/4)
- Launch Agent
- Launch Daemon
- Systemd Service
- Windows Service

Event Triggered Execution

Privilege Escalation
13 techniques

Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
Boot or Logon Autostart Execution (0/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (1/4)
- Launch Agent
- Launch Daemon
- Systemd Service
- Windows Service

Domain Policy Modification (0/2)
Escape to Host
Event Triggered Execution (0/16)
Exploitation for Privilege Escalation
Hijack Execution

Defense Evasion
42 techniques

Abuse Elevation Control Mechanism (0/4)
Access Token Manipulation (0/5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (0/2)
Execution Guardrails (0/1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (0/10)
Hijack Execution

Credential Access
17 techniques

Adversary-in-the-Middle (0/3)
Brute Force (0/4)
Credentials from Password Stores (0/5)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (0/2)
Input Capture (0/4)

Threat Groups (136)
Software (635)
Mitigations (43)
Campaigns (20)
select all
deselect all
2016 Ukraine Electric Power Attack view select deselect
C0010 view select deselect
C0011 view select deselect

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
  - **Reasoning** about attacks and attack campaigns

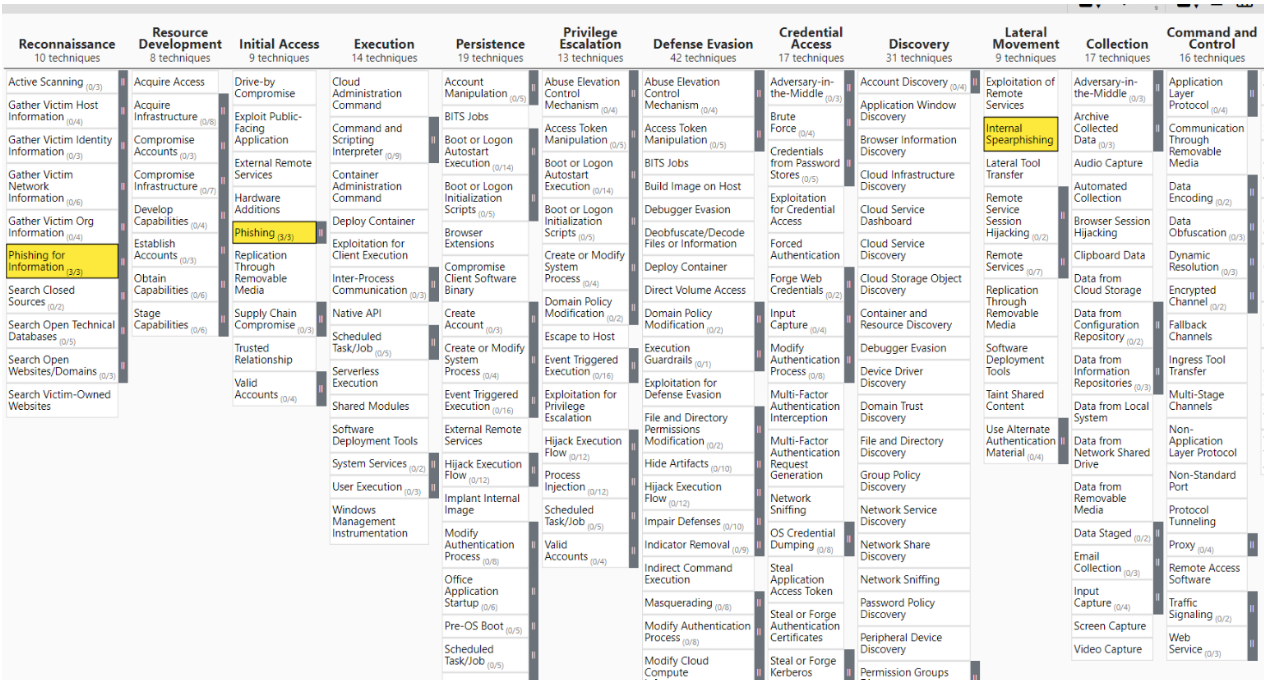
- **Very powerful (conceptual) tool**

My suggestions

- For each topic covered in the course, **always try** to understand which **Tactic** (≈phase) it relates to

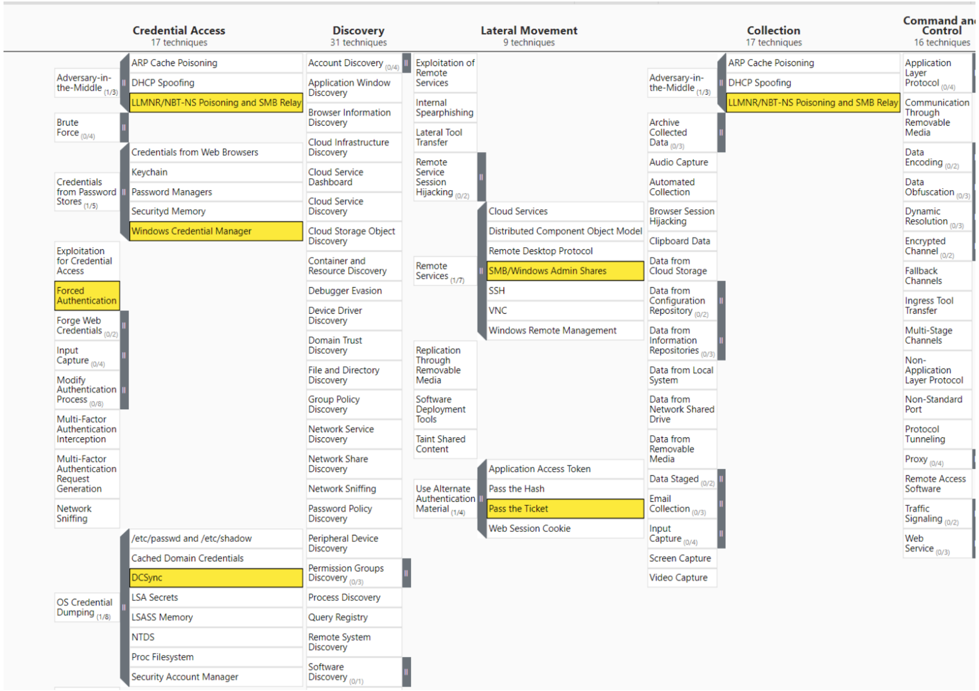
- Keep in mind that such a mapping may be **complex** and **not intuitive**
  - One topic may relate to multiple **Techniques** in different **Tactics**

Example: "phishing"



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques
Active Scanning (0/3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Exploit Public-Facing Application	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Phishing (3/3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/7)	Browser Session Hijacking	Dynamic Resolution (0/3)
Phishing for Information (3/3)	Establish Accounts (0/3)	Replication Through Removable Media	Inter-Process Communication (0/3)	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Supply Chain Compromise (0/3)	Native API	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Trusted Relationship	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Serverless Execution	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol
			Software Deployment Tools	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port
			System Services (0/2)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery		Data from Removable Media	Protocol Tunneling
			User Execution (0/3)	Modify Authentication Process (0/8)	Valid Accounts (0/4)	Hide Artifacts (0/10)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Proxy (0/4)
			Windows Management Instrumentation	Office Application Startup (0/6)		Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Network Service Discovery		Email Collection (0/3)	Remote Access Software
				Pre-OS Boot (0/5)		Impair Defenses (0/10)	Steal or Forge Kerberos	Network Share Discovery		Input Capture (0/4)	Traffic Signaling (0/2)
				Scheduled Task/Job (0/5)		Indicator Removal (0/9)		Network Sniffing		Screen Capture	Web Service (0/3)
						Indirect Command Execution		Password Policy Discovery		Video Capture	
						Masquerading (0/8)		Peripheral Device Discovery			
						Modify Authentication Process (0/8)		Permission Groups			
						Modify Cloud Compute					

Example: "ntlm"



Credential Access 17 techniques
- Adversary-in-the-Middle (1/3)
  - ARP Cache Poisoning
  - DHCP Spoofing
  - LLMNR/NBT-NS Poisoning and SMB Relay
- Brute Force (0/4)
- Credentials from Password Stores (1/5)
  - Credentials from Web Browsers
  - Keychain
  - Password Managers
  - Securityd Memory
  - Windows Credential Manager
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (1/8)
  - /etc/passwd and /etc/shadow
  - Cached Domain Credentials
  - DCSync
  - LSA Secrets
  - LSASS Memory
  - NTDS
  - Proc Filesystem
  - Security Account Manager

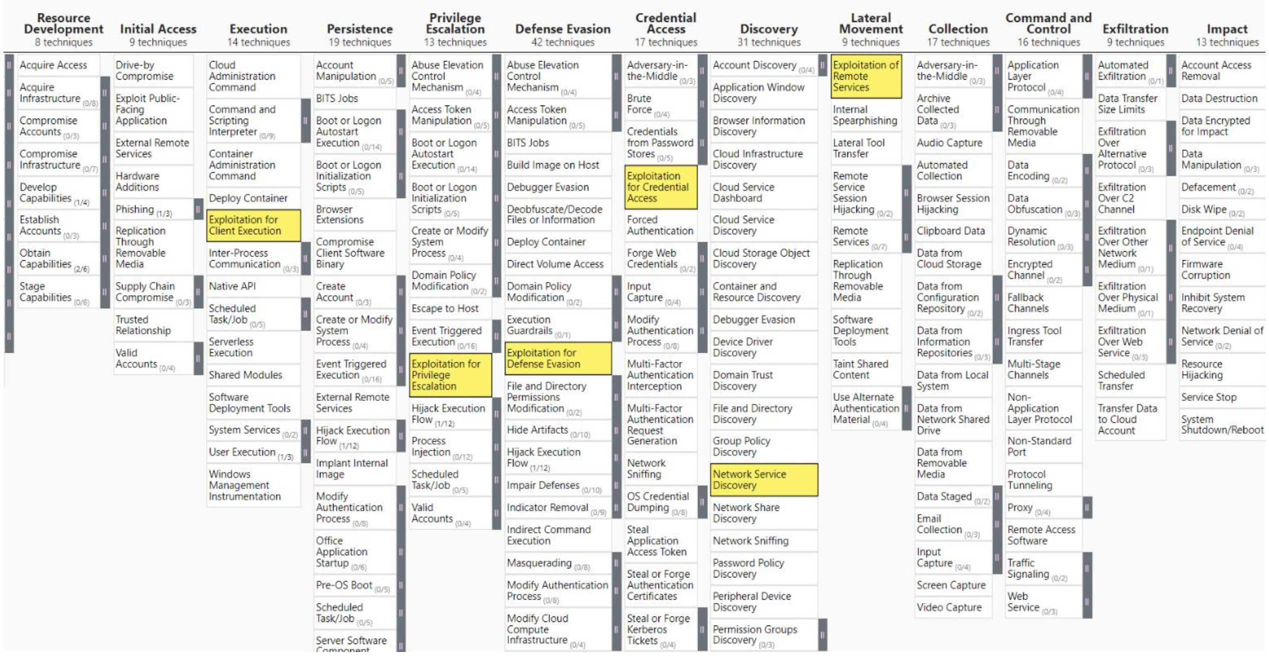
Discovery 31 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery (0/1)

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (1/7)
  - Cloud Services
  - Distributed Component Object Model
  - Remote Desktop Protocol
  - SMB/Windows Admin Shares
  - SSH
  - VNC
  - Windows Remote Management
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (1/4)
  - Application Access Token
  - Pass the Hash
  - Pass the Ticket
  - Web Session Cookie

Collection 17 techniques
- Adversary-in-the-Middle (1/3)
  - ARP Cache Poisoning
  - DHCP Spoofing
  - LLMNR/NBT-NS Poisoning and SMB Relay
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

Example: "vulnerability"



Resource Development 8 techniques
- Acquire Access
- Acquire Infrastructure (0/8)
- Compromise Accounts (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (1/4)
- Establish Accounts (0/3)
- Obtain Capabilities (2/6)
- Stage Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (0/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3)
- Windows Management Instrumentation

Persistence 19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (1/12)
- Implant Internal Image
- Modify Authentication Process (0/8)
- Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- Scheduled Task/Job (0/5)
- Server Software Component

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

Defense Evasion 42 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (1/12)
- Impair Defenses (0/10)
- Indicator Removal (0/9)
- Indirect Command Execution
- Masquerading (0/8)
- Modify Authentication Process (0/8)
- Modify Cloud Compute Infrastructure (0/4)

Credential Access 17 techniques
- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets (0/4)

Discovery 31 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery (0/3)

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection 17 techniques
- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection (0/3)
- Input Capture (0/4)
- Screen Capture
- Video Capture

Command and Control 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access Software
- Traffic Signaling (0/2)
- Web Service (0/3)

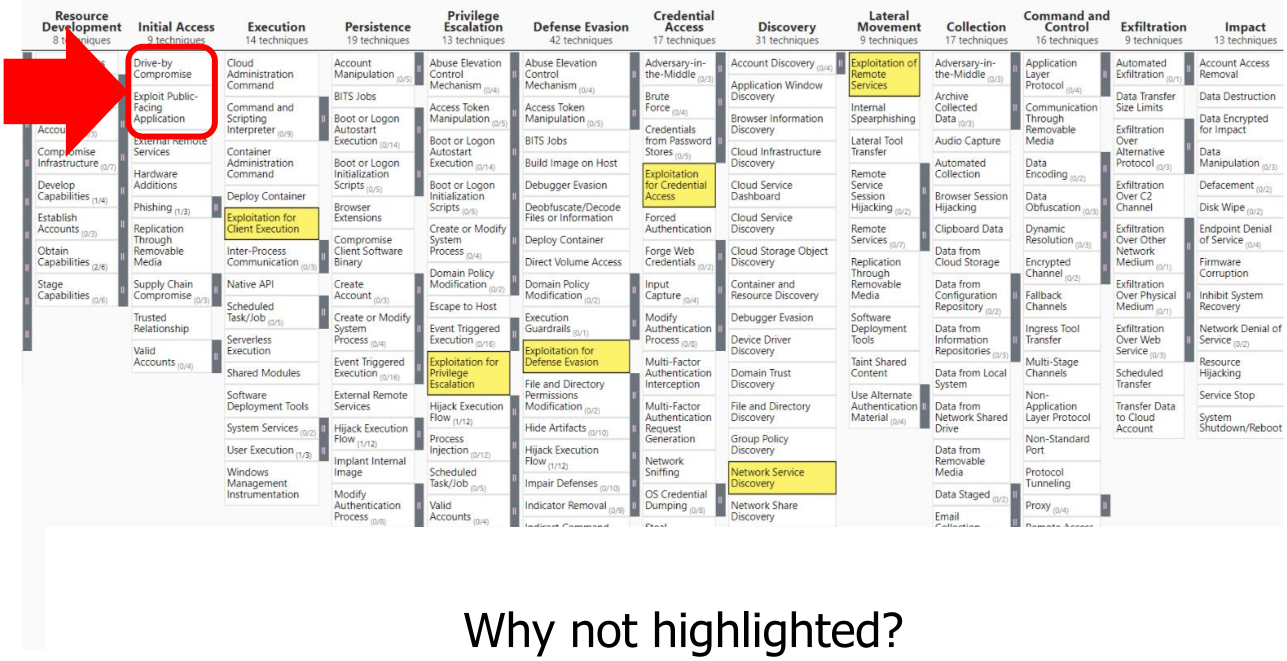
Exfiltration 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/3)
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Warning

- Keep in mind that such a mapping may be **complex** and **not intuitive**
  - One topic may relate to multiple **Techniques** in different **Tactics**
  - Relation topic-might **not** be encoded in ATT&CK
  - ...or it may follow criteria different from ours
    - Personal assessment often necessary

Example: Vulnerability



Resource Development 8 techniques
- Accou (0/3)
- Compromise Infrastructure (0/7)
- Develop Capabilities (1/4)
- Establish Accounts (0/3)
- Obtain Capabilities (2/6)
- Stage Capabilities (0/6)

Initial Access 9 techniques
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/3)
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/4)

Execution 14 techniques
- Cloud Administration Command
- Command and Scripting Interpreter (0/9)
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/Job (0/5)
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services (0/2)
- User Execution (1/3)
- Windows Management Instrumentation

Persistence 19 techniques
- Account Manipulation (0/5)
- BITS Jobs
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Client Software Binary
- Create Account (0/3)
- Create or Modify System Process (0/4)
- Event Triggered Execution (0/16)
- External Remote Services
- Hijack Execution Flow (1/12)
- Implant Internal Image
- Modify Authentication Process (0/8)

Privilege Escalation 13 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- Boot or Logon Autostart Execution (0/14)
- Boot or Logon Initialization Scripts (0/5)
- Create or Modify System Process (0/4)
- Domain Policy Modification (0/2)
- Escape to Host
- Event Triggered Execution (0/16)
- Exploitation for Privilege Escalation
- Hijack Execution Flow (1/12)
- Process Injection (0/12)
- Scheduled Task/Job (0/5)
- Valid Accounts (0/4)

Defense Evasion 42 techniques
- Abuse Elevation Control Mechanism (0/4)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/10)
- Hijack Execution Flow (1/12)
- Impair Defenses (0/10)
- Indicator Removal (0/9)
- Indirect Command

Credential Access 17 techniques
- Adversary-in-the-Middle (0/3)
- Brute Force (0/4)
- Credentials from Password Stores (0/5)
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- Input Capture (0/4)
- Modify Authentication Process (0/8)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping (0/8)
- Steal

Discovery 31 techniques
- Account Discovery (0/4)
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- Network Share Discovery

Lateral Movement 9 techniques
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- Remote Services (0/7)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material (0/4)

Collection 17 techniques
- Adversary-in-the-Middle (0/3)
- Archive Collected Data (0/3)
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged (0/2)
- Email Collection

Command and Control 16 techniques
- Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- Dynamic Resolution (0/3)
- Encrypted Channel (0/2)
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy (0/4)
- Remote Access

Exfiltration 9 techniques
- Automated Exfiltration (0/1)
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/3)
- Scheduled Transfer
- Transfer Data to Cloud Account

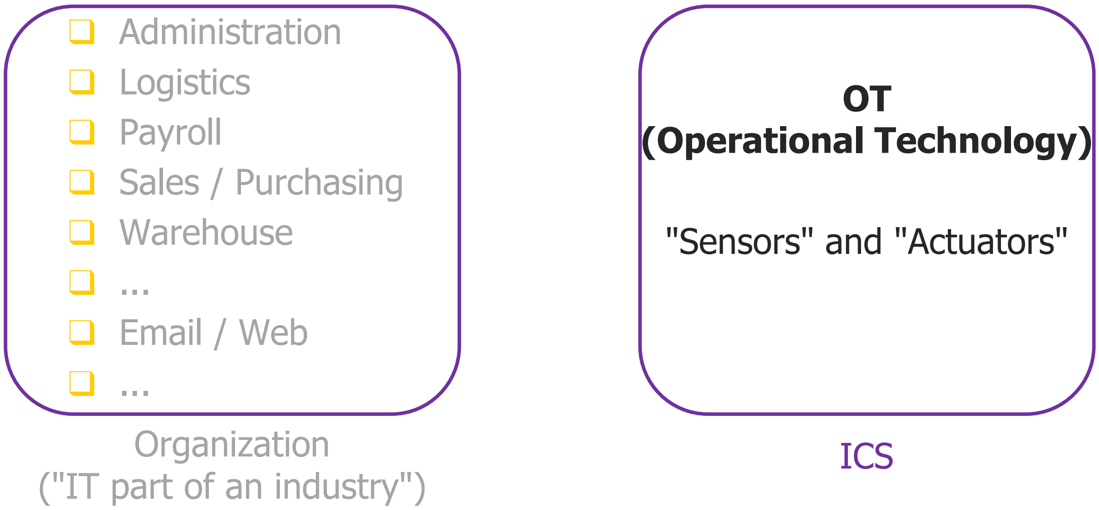
Impact 13 techniques
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- Endpoint Denial of Service (0/4)
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service (0/2)
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Why not highlighted?

Attacking an ICS

Target Categories: ICS

1. Organizations
2. Industrial Control Systems (ICS)
3. Single individuals



- ❑ Administration
- ❑ Logistics
- ❑ Payroll
- ❑ Sales / Purchasing
- ❑ Warehouse
- ❑ ...
- ❑ Email / Web
- ❑ ...

Organization
("IT part of an industry")

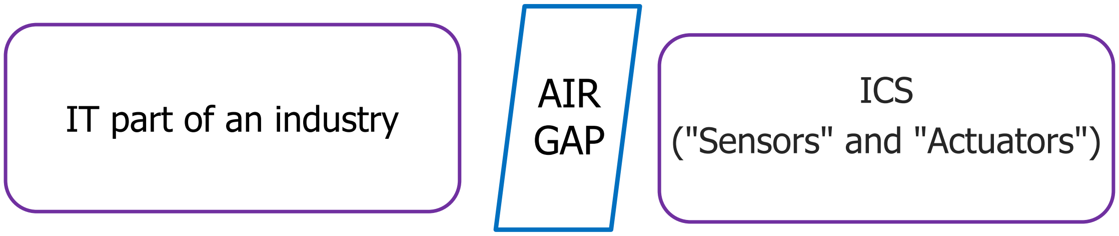
OT
(Operational Technology)

"Sensors" and "Actuators"

ICS

Air Gap: Theory

- IT part connected to the Internet
- ICS part **fully disconnected** from the IT part and from the Internet



IT part of an industry

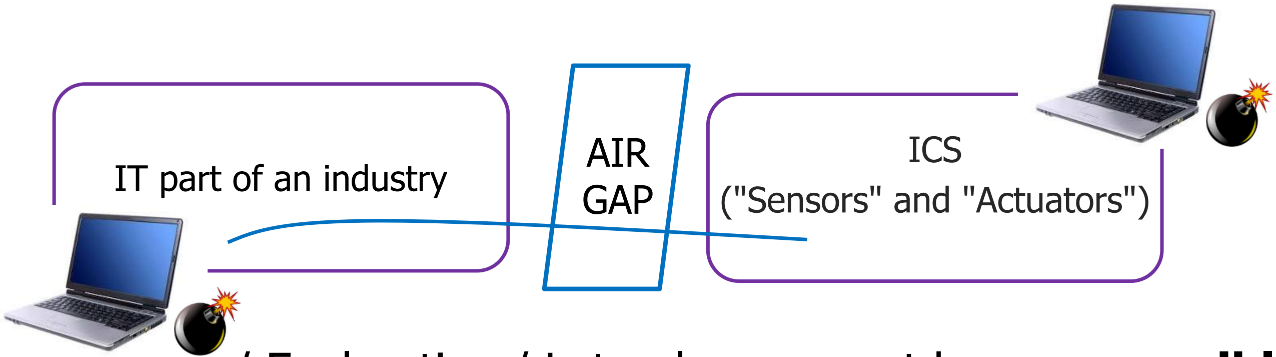
AIR GAP

ICS ("Sensors" and "Actuators")

- Delivery / Exploration / Lateral movement **not** possible

Air Gap: Practice

- Support engineers occasionaly connect their notebooks on the ICS
- ICS permanently accessible from (selected locations of) IT part for remote control / monitoring
  - ...sometimes even from the Internet



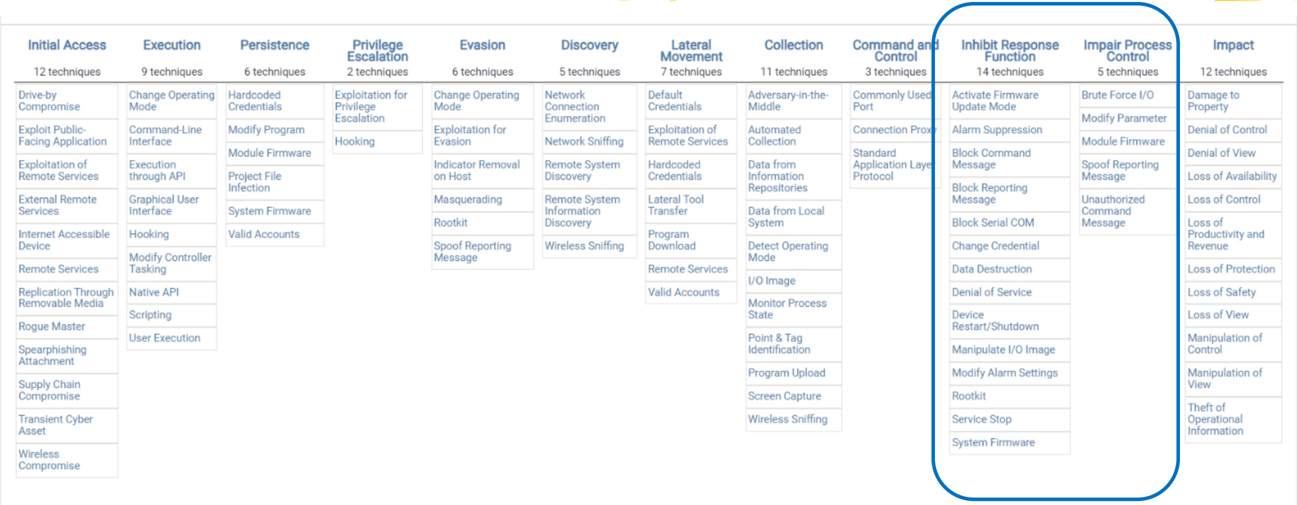
IT part of an industry

AIR GAP

ICS ("Sensors" and "Actuators")

- Delivery / Exploration / Lateral movement become **possible**

MITRE ATT&CK Matrix



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Prox	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Laye Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

- In a nutshell:
  - "General" tactics more or less the same
  - Two more tactics: Inhibit Response, Impair Process Control
  - Much less techniques

Target Category: Organization

- Many **similarities** between Organizations

- A **given set** of skills, tools and knowledge
  is highly effective on **many different** organizations

- Standard, highly effective procedures for obtaining **money**

Target Category: ICS

- **Very few similarities** between ICSs
- A **given set** of skills, tools and knowledge is highly effective on **very few** ICSs
- You need to **invent** some **highly specific** way for obtaining **money**

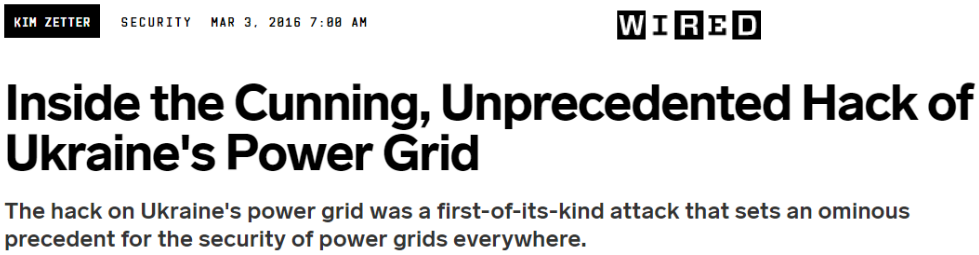
- Attacks to ICS are **much less frequent** than attacks to Organizations:
  - Much more costly
  - Much more difficult to get money

Important Remark 1

- Attacks to ICS are much less frequent than attacks to organizations
  - Much more costly
  - Much more difficult to get money

- Attacks on ICS may have strategic / intelligence motivations
  - High budget
  - Objective is Data stealing / Disruption (not Money)

Example 1



KIM ZETTER SECURITY MAR 3, 2016 7:00 AM

WIRED

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

- ...about 30 substations offline...two other power distribution centers at the same time...leaving more than 230,000 residents in the dark.
- They also disabled backup power supplies...leaving operators themselves stumbling in the dark.

- Spear phishing then **many months** of extensive **reconnaissance**...
- Each company used a different distribution management system for its grid, and during the reconnaissance phase, the attackers studied each of them carefully.

Example 2

Die Lage der IT-Sicherheit in Deutschland 2014

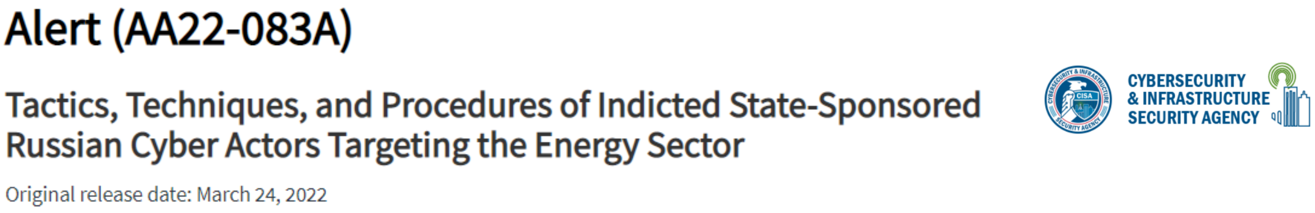
Bundesamt
für Sicherheit in der
Informationstechnik

- Targeted attack on a **steel mill** in Germany (pg. 31)

- There were frequent failures of individual control components or entire systems.
- ...a **blast furnace was not regulated**, it could be shut down and get in an undefined state...

- As a consequence there was **massive damage** to the facility.

Example 3



Alert (AA22-083A)

Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector

Original release date: March 24, 2022

- Multiple intrusion campaigns conducted by **state-sponsored Russian cyber actors from 2011 to 2018** and targeted U.S. and international **Energy** Sector

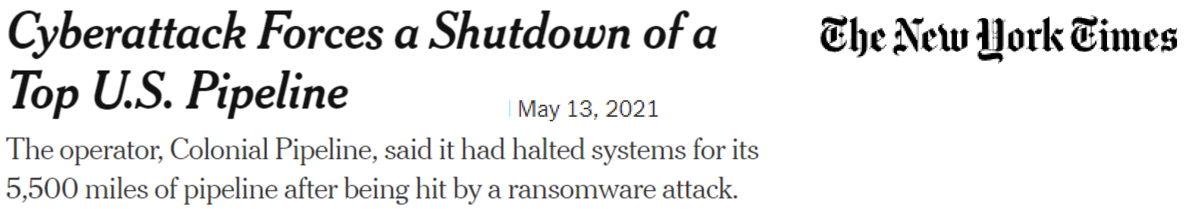
- Description with MITRE ATT&CK framework
  `https://bartoli-alberto.blogspot.com/search?q=guerra`

Important Remark 2

- Attacks to ICS are much less frequent than attacks to organizations
  - Much more costly
  - Much more difficult to get money

- An attack on the **"IT part"** may **disrupt** industrial operations

Example 1



Cyberattack Forces a Shutdown of a Top U.S. Pipeline

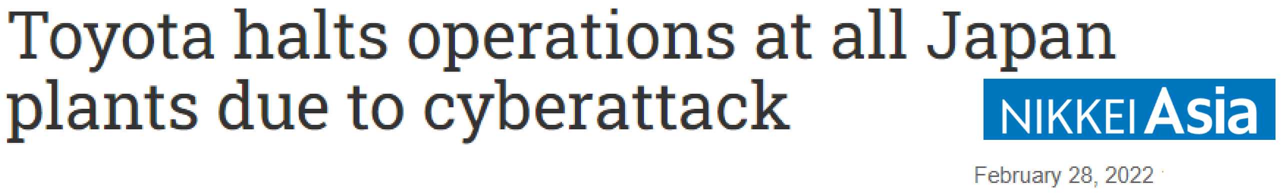
The New York Times

May 13, 2021

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

- One of the nation’s largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware...
- Colonial Pipeline...had shut down its 5,500 miles of pipeline, which it says carries 45 percent of the East Coast’s fuel supplies, in an effort to contain the breach.

Example 2



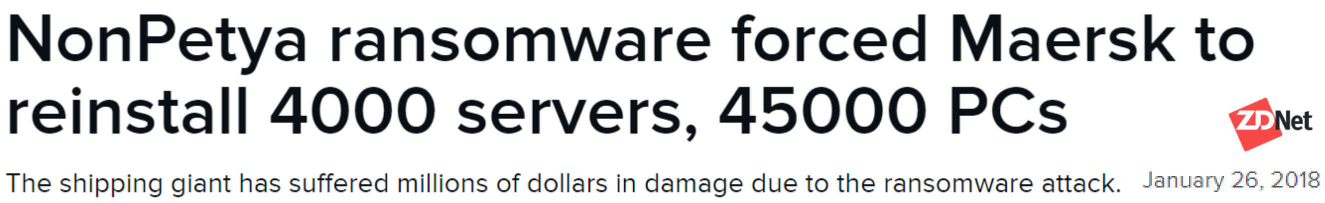
Toyota halts operations at all Japan plants due to cyberattack

NIKKEI Asia

February 28, 2022

- Toyota Motor on Tuesday halted operations at all of its plants in Japan after a major supplier was hit by a cyberattack, disrupting the automaker's parts supply management system.

Example 3



NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.

January 26, 2018

- Maersk has revealed that a devastating ransomware attack which struck businesses across Europe in 2017 required close to a "complete infrastructure" overhaul and the reinstallation of thousands of machines.
- The firm, with offices in 130 countries and a workforce of close to 90,000,
- "Imagine a company where a ship with 10 to 20 thousand containers is entering a port every 15 minutes, and for 10 days, you have no IT," Hagemann commented. "It's almost impossible to even imagine."

Key remarks

- Computer attacks no longer affect only "**data**"
- They may affect the "**physical world**"
- They may **disrupt** "**non IT** orgs"

Attacking Single Individuals

Target Categories: Single Individuals

1. Organizations
2. Industrial systems (ICS)
3. Single individuals

- ❑ Initial Access
- ❑ Execution
- ❑ Persistence
- ❑ C&C
- ~~❑ Discovery~~
- ~~❑ Lateral movement~~
- ❑ Impact

Motivations

1. Money
2. Stealing of information
3. Disruption of operations

- Money is by far the **most frequent** motivation

- Look at "How to obtain money"

Key Remark

- Human operators execute **all the steps**

- Actions can be **tailored** to the **specific** environment
- Costly

- Automated tool executes **all the steps**

- Actions **cannot** be **tailored** to the **specific** environment
- Investment can be amortized over many targets

- **Automation is much more frequent**
  - Can be made **very effective**
    (unlike attacks to organizations)
  - Only way for justifying **small gain** per successful target
    (attacks to organization have large gain per successful target)