Attacks

What we want (almost)

- **Confidentiality**
  - Ensuring that information is only accessible to those who are authorized to view it

- **Integrity**
  - Ensuring that data remains accurate, consistent and unaltered except by authorized entities

That's trivial to achieve!

- **Confidentiality**
  - Ensuring that information is only accessible to those who are authorized to view it

- **Integrity**
  - Ensuring that data remains accurate, consistent and unaltered except by authorized entities

- Just switch everything off

CIA Triad (what we want)

- **Confidentiality**
  - Ensuring that information is only accessible to those who are authorized to view it
- **Integrity**
  - Ensuring that data remains accurate, consistent and unaltered except by authorized entities
- **Availability**
  - Ensuring that systems, networks and data are accessible when needed by authorized users

What adversaries want

- **Violate** one or more of:
  - **Confidentiality**
  - **Integrity**
  - **Availability**

Why?

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)

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

Ransom

- Encrypt data and ask ransom for decrypting it (**ransomware**)
- Steal data and ask ransom for not making it public (**double extortion**)
- **Huge** societal problem

Attack cost	relatively low
Potential ROI (Return on Investment)	huge

⇒ **Lot** of potential attackers

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

⇒ **Every** organization is a potential target

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"

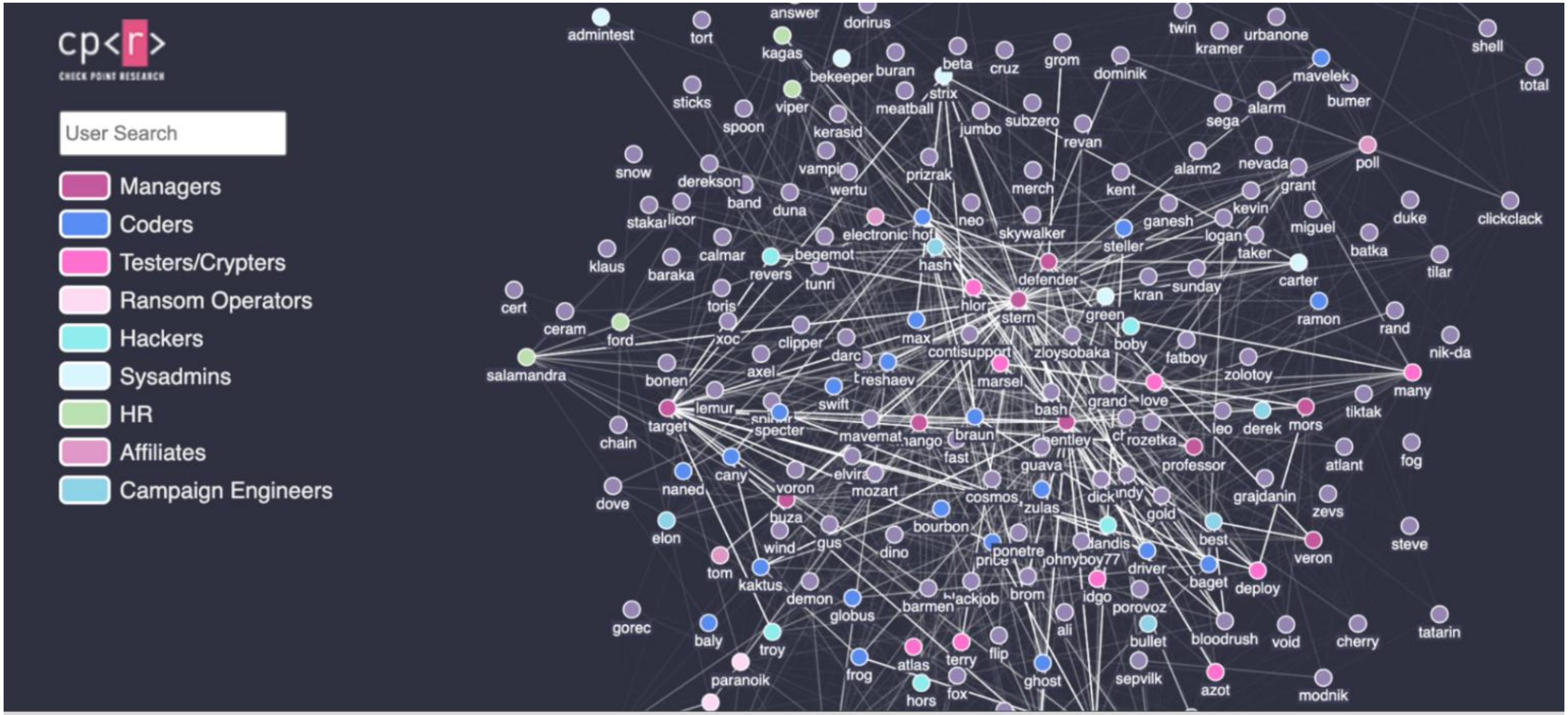


Immagine da research.checkpoint.com

Motivations vs CIA Triad

Money	C	I	A
Stealing of information	C		
Disruption of operation		I	A

Attacks (REMIND)

- ❑ Motivations
- ❑ Target categories
- ❑ Attacking each target category

Target Categories (I)

1. **Organizations**
   - ❑ Private companies
   - ❑ Public administrations
   - ❑ ...
   - ❑ "Any large entity with lots of computers and networks that operate on **files**"

2. **Single** individuals

3. **...**

Computers: IT vs OT

- **Information** Technology ≈
  Computers that operate on **"files"**

- **Operational** Technology ≈
  Computers that operate on the **"physical world"**
  - Devices and systems
    - Cars, Ships, Aircrafts (engine, brakes, helm,...)
    - Healthcare : (insulin pump, electrocardiograph,...)
    - ...
  - **Industrial processes**

OT: Industrial Processes

- Manufacturing (production lines, quality control,...)
- Transportation systems (traffic lights, railway signaling,...)
- Drinking Water & Wastewater
- Energy generation & distribution
- Chemical processes (materials, reactions, ...)
- ...

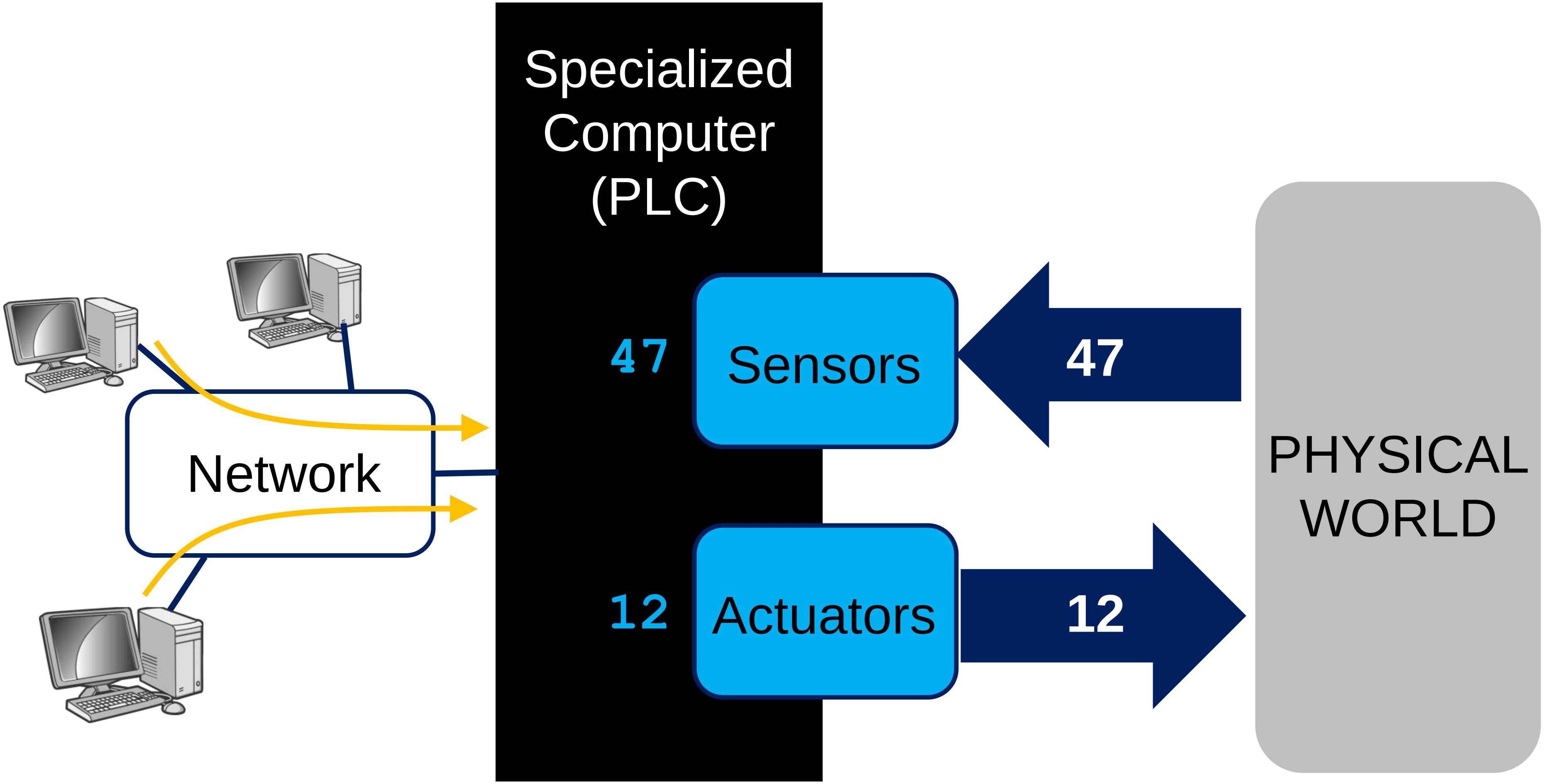
- **Everywhere**
- **Essential component of our life**

OT: Key functions?

- **Monitor: Read** information from the physical world
  - **Sensors**
    - Temperature, Pressure, Motion, Concentration, ...

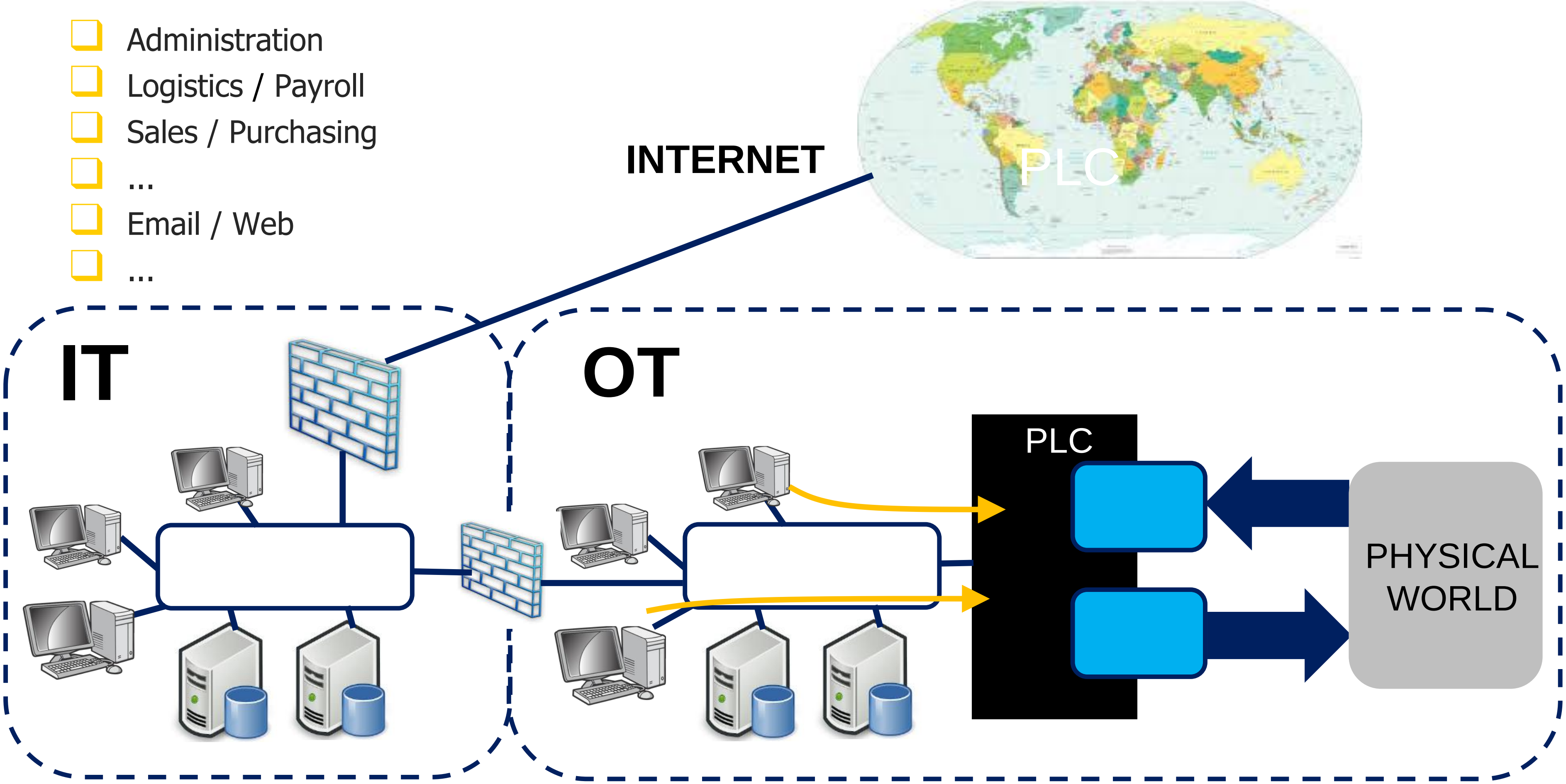
- **Control: Write** information on the physical world
  - **Actuators**
    - Motors, Valves, ...

OT: PLC


Specialized Computer (PLC)
47
Sensors
47
12
Actuators
12
Network
PHYSICAL WORLD

ICS:
Industrial Control Systems

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



Target Categories (II)

1. **Organizations**
   - □ Information Technology

2. **Single** individuals

3. Industrial Control Systems (**ICS**)
   - □ Information Technology

     +
   - □ Operational Technology

Our next steps

- Attacks against **Organizations**

- A few words about:
  - **Single individuals**
  - **ICS**

Attacking an Organization

Attacking an Organization

- It may take from **minutes** to **months**
- Several **phases**
- Each phase:
  - Done for a reason (**tactical** objective) **WHY**
  - Can be executed with several **techniques** **HOW**

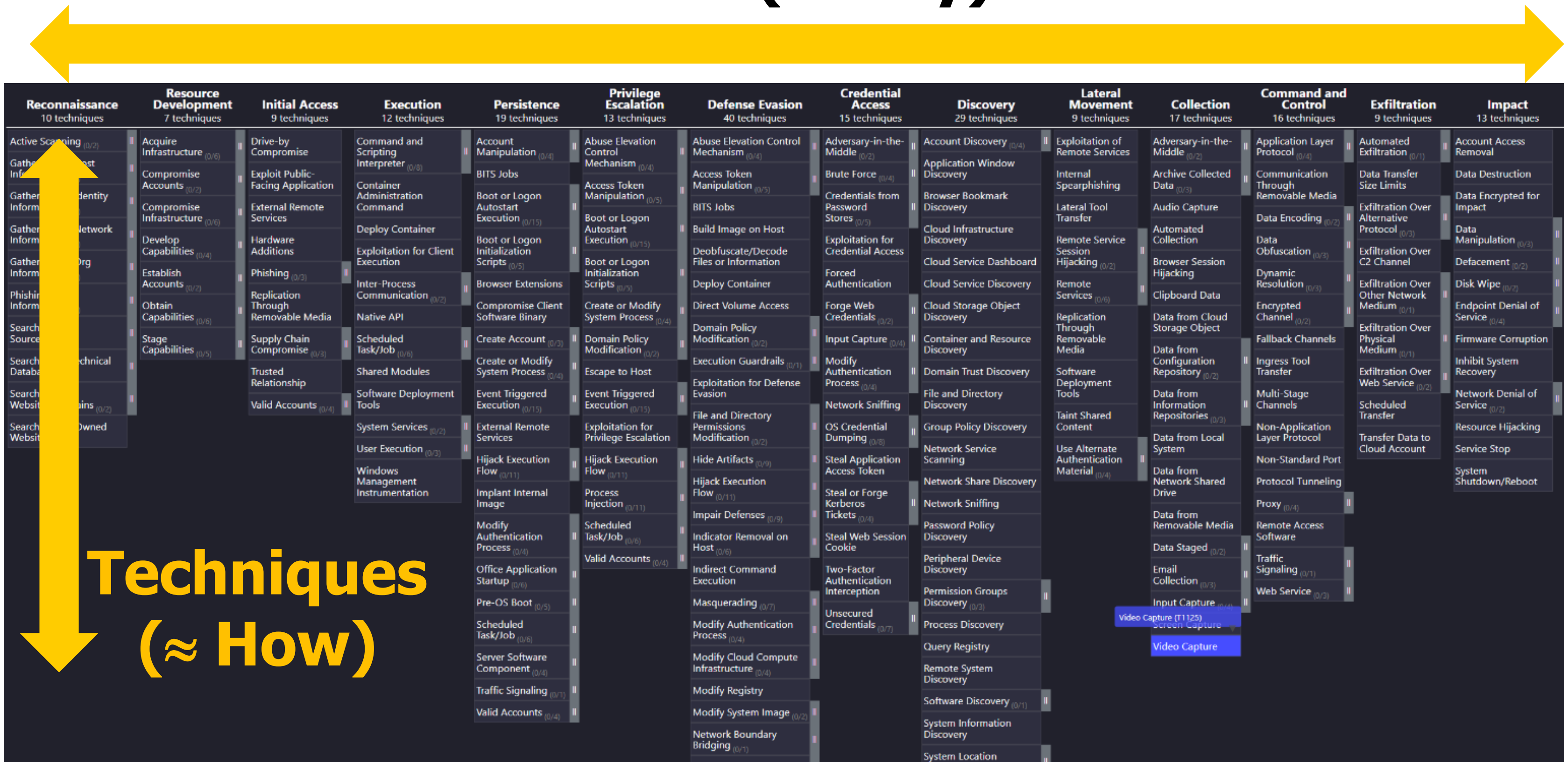
- Models for reasoning about the overall attack:
  - Kill chain (first widely used)
  - ...
  - **MITRE ATT&CK** ("the" model today)

MITRE ATT&CK (I)

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

MITRE ATT&CK Matrix

Tactics (≈ Why)



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
Gathe ost Inf	Compromise 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 dentity Inform	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 Network Inform	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 Org Inform	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)
Phishin Inform	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 Source	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 echnical Databa		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 Websit ins (0/2)		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 Owned Websit			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					

Video Capture (T1125)

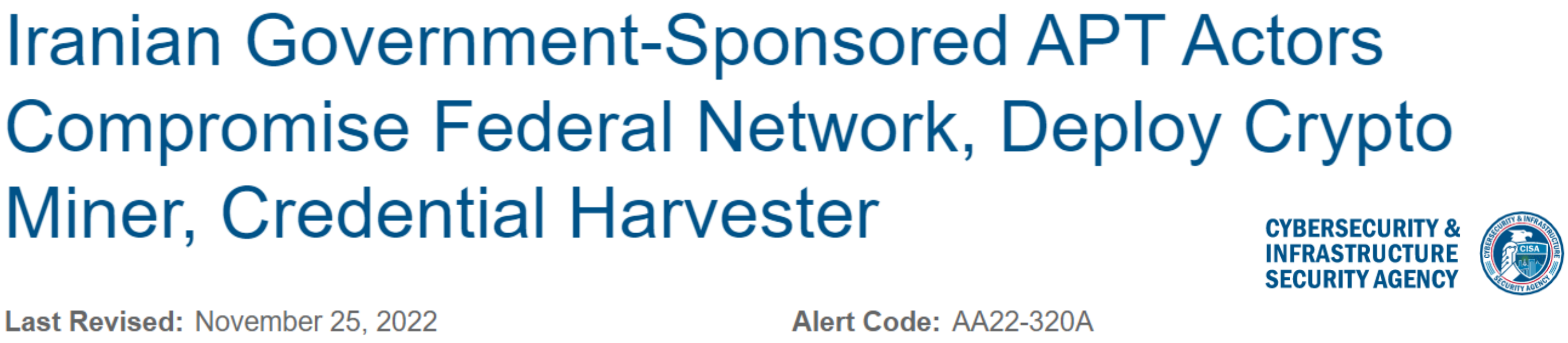
Techniques (≈ How)

MITRE ATT&CK (II)

- Periodically **updated** to reflect more recent/accurate knowledge
  - `search "MITRE ATT&CK version history"`

- 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

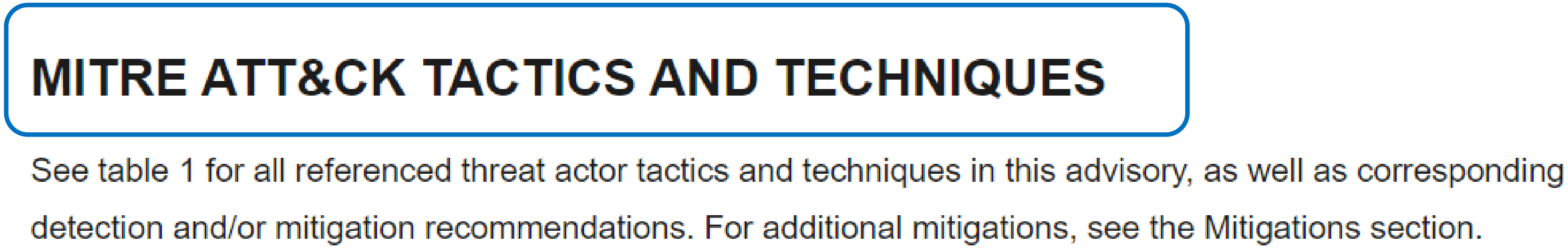


Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Last Revised: November 25, 2022

Alert Code: AA22-320A

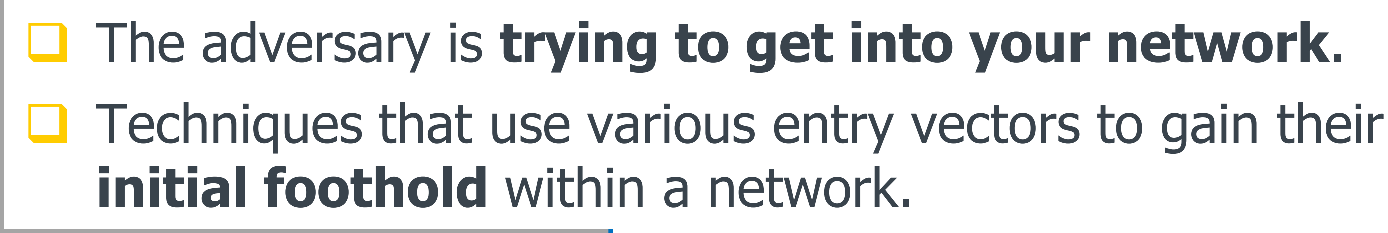


MITRE ATT&CK TACTICS AND TECHNIQUES

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)

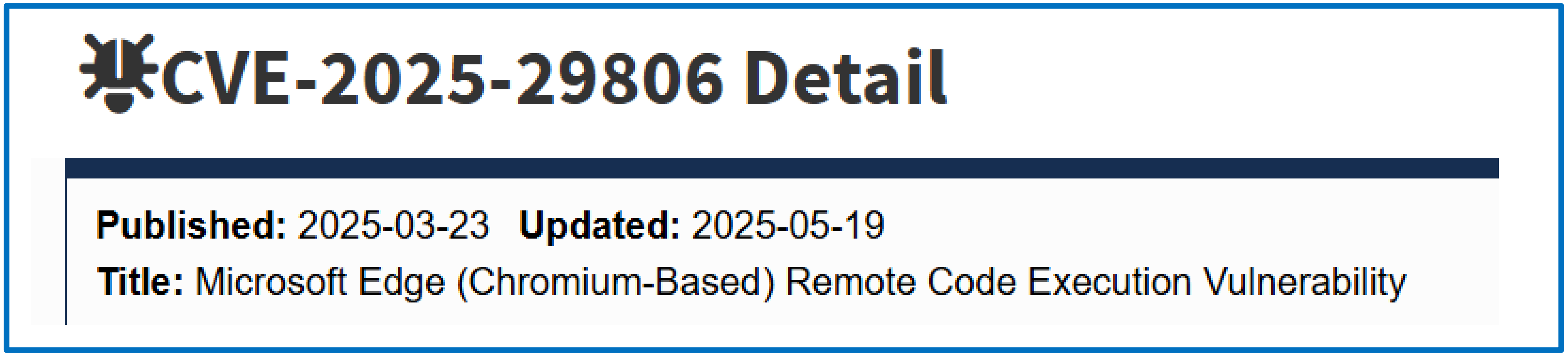
- Initial Access
  - **Phishing**. Malicious attachments or links in emails
  - **Valid Accounts**. Abuse of compromised credentials

(+5 Techniques) MITRE ATT&CK

Vulnerability

- A **mistake** in **software** that can be directly used to **gain access** to a system or network

Example: Vulnerability in Browser



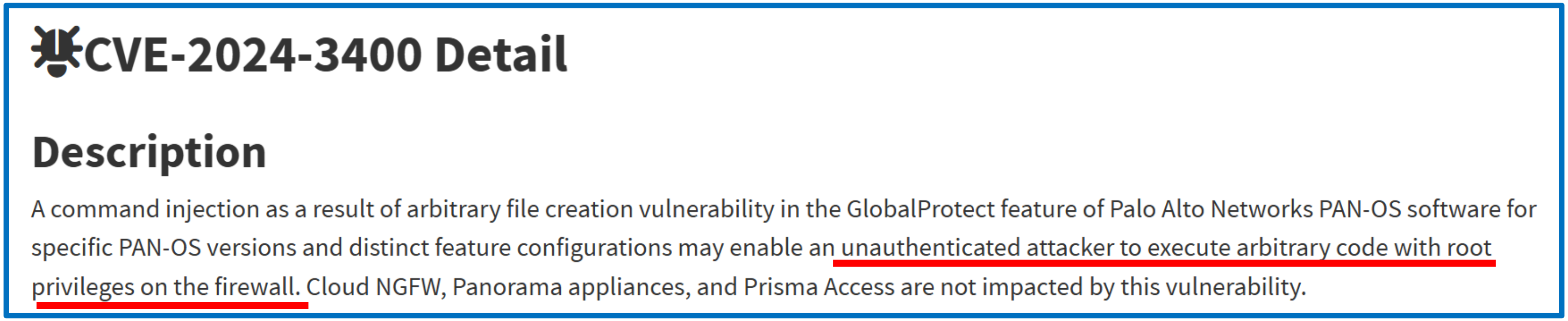
CVE-2025-29806 Detail

Published: 2025-03-23 **Updated:** 2025-05-19

Title: Microsoft Edge (Chromium-Based) Remote Code Execution Vulnerability

1. You fetch a web resource from an Attacker-controlled URL
2. An **attacker-chosen code** is executed with **your** identity on **your** machine (in the Browser process)

Example: Vulnerability in Server SW



CVE-2024-3400 Detail

Description

A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.

1. You have a vulnerable firewall reachable from the Internet
2. **Anyone** can execute an **arbitrary command** on the firewall with **root** identity

"Gain foothold" (I-c)

- 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

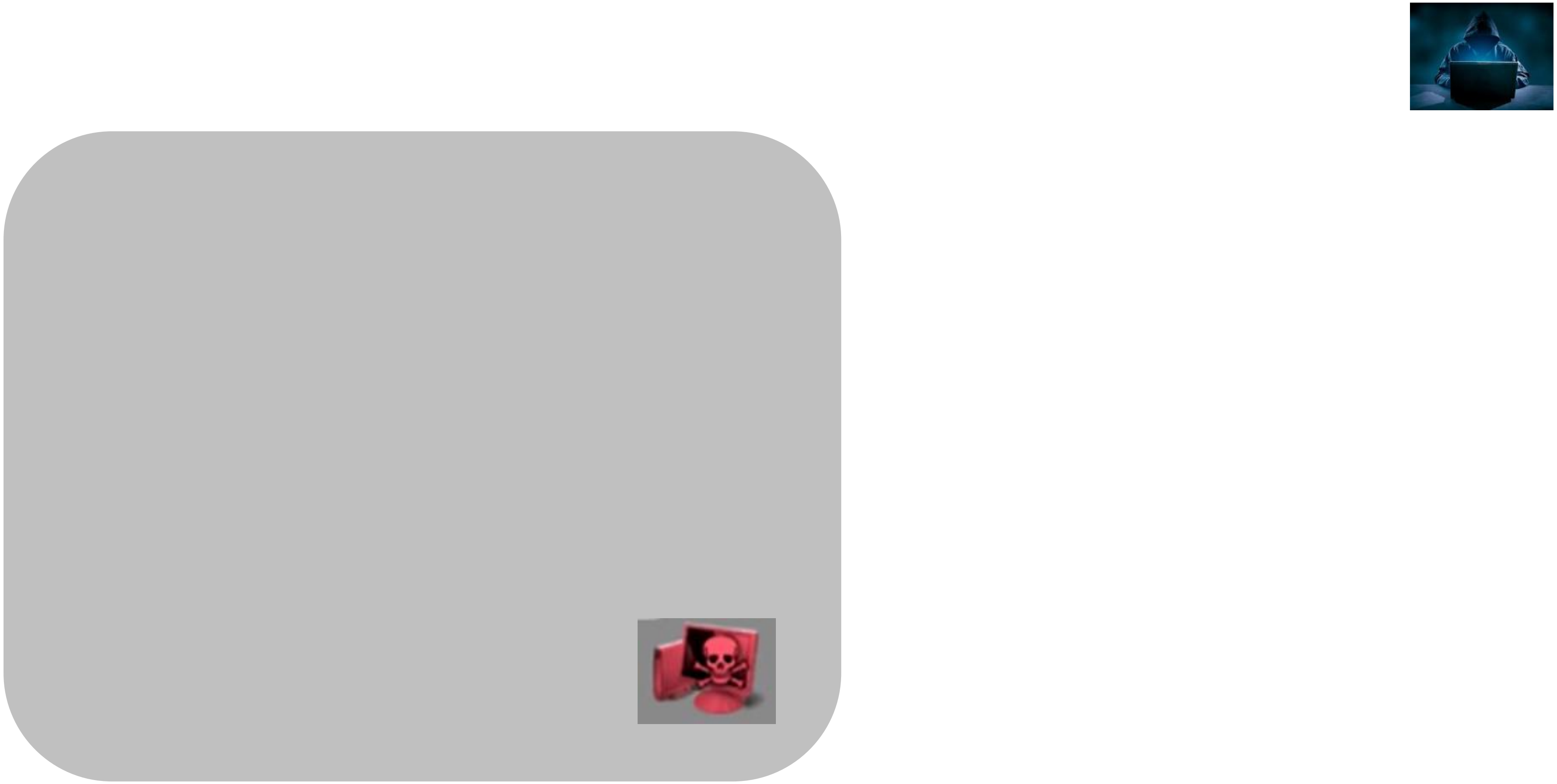
"Gain foothold" (II)

- 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

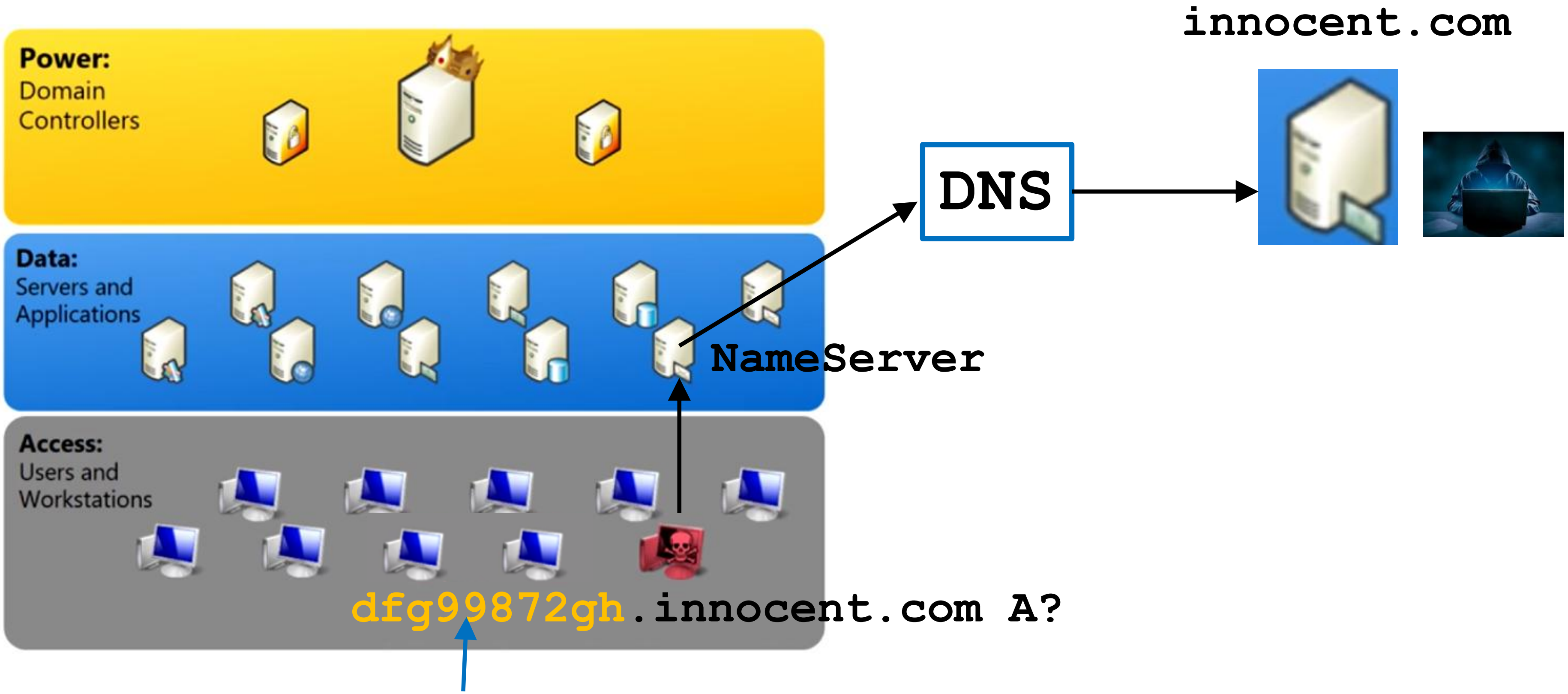


Command & Control (C&C)

- 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

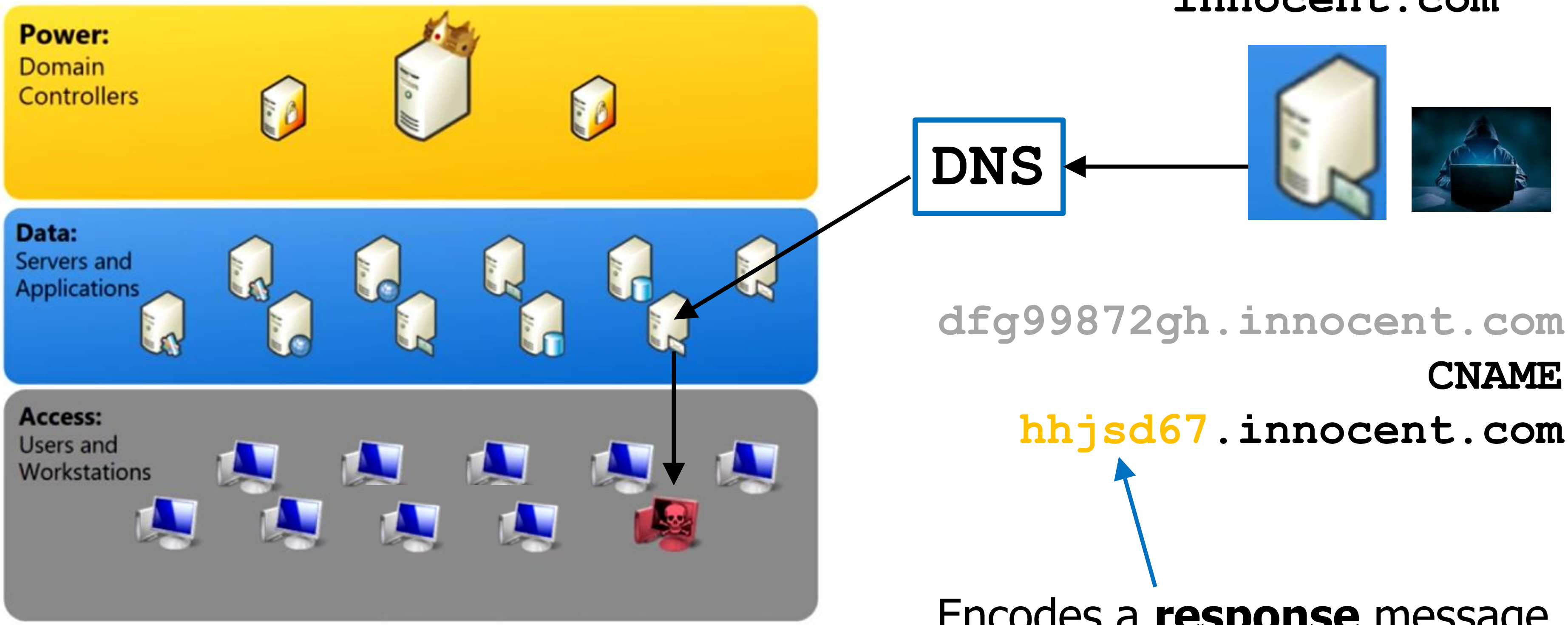
DNS

NameServer

dfg99872gh.innocent.com A?

Encodes a **request** message to attacker

Example (outline): DNS Tunneling (II)



innocent.com

DNS

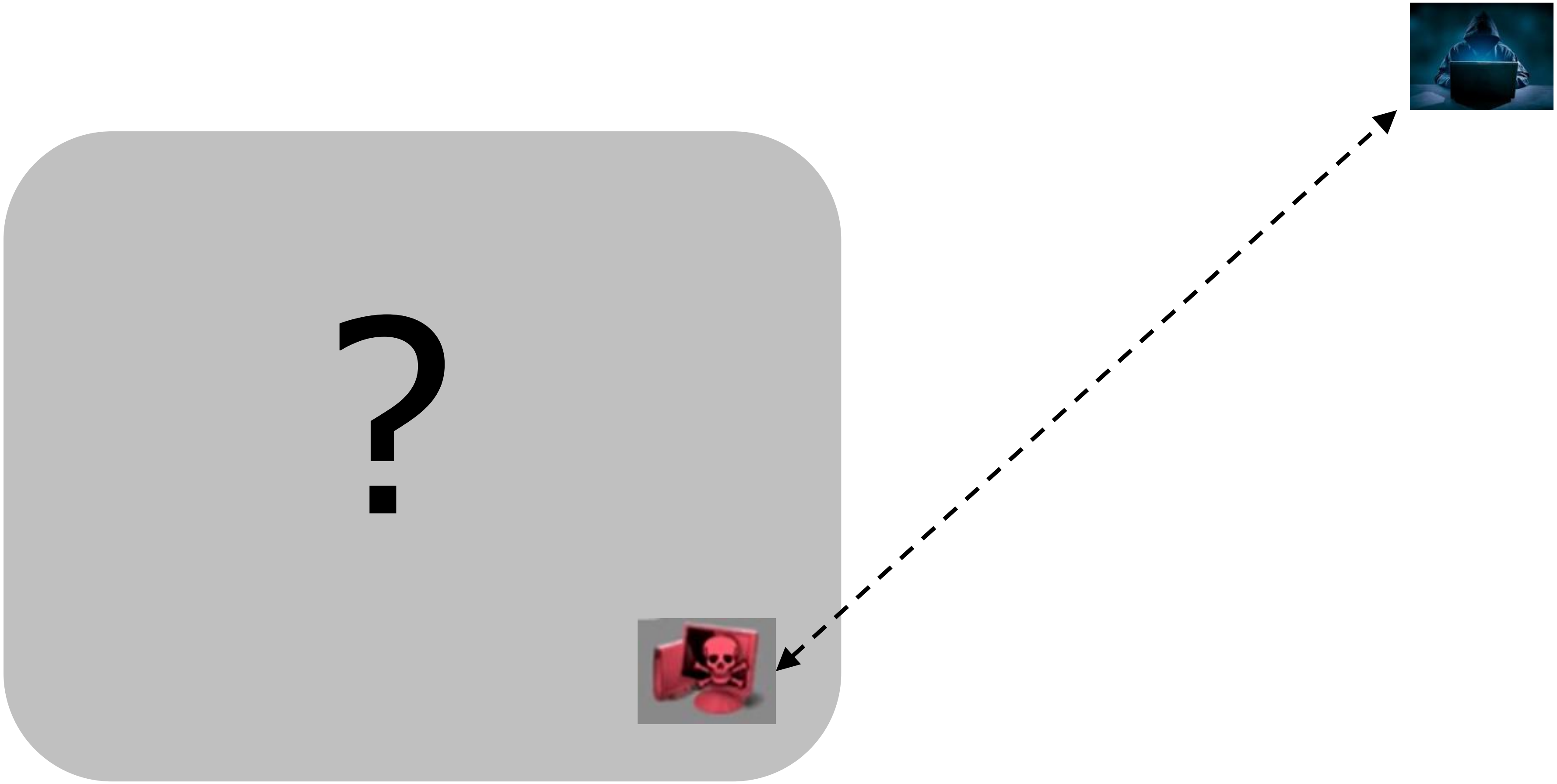
dfg99872gh.innocent.com

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...

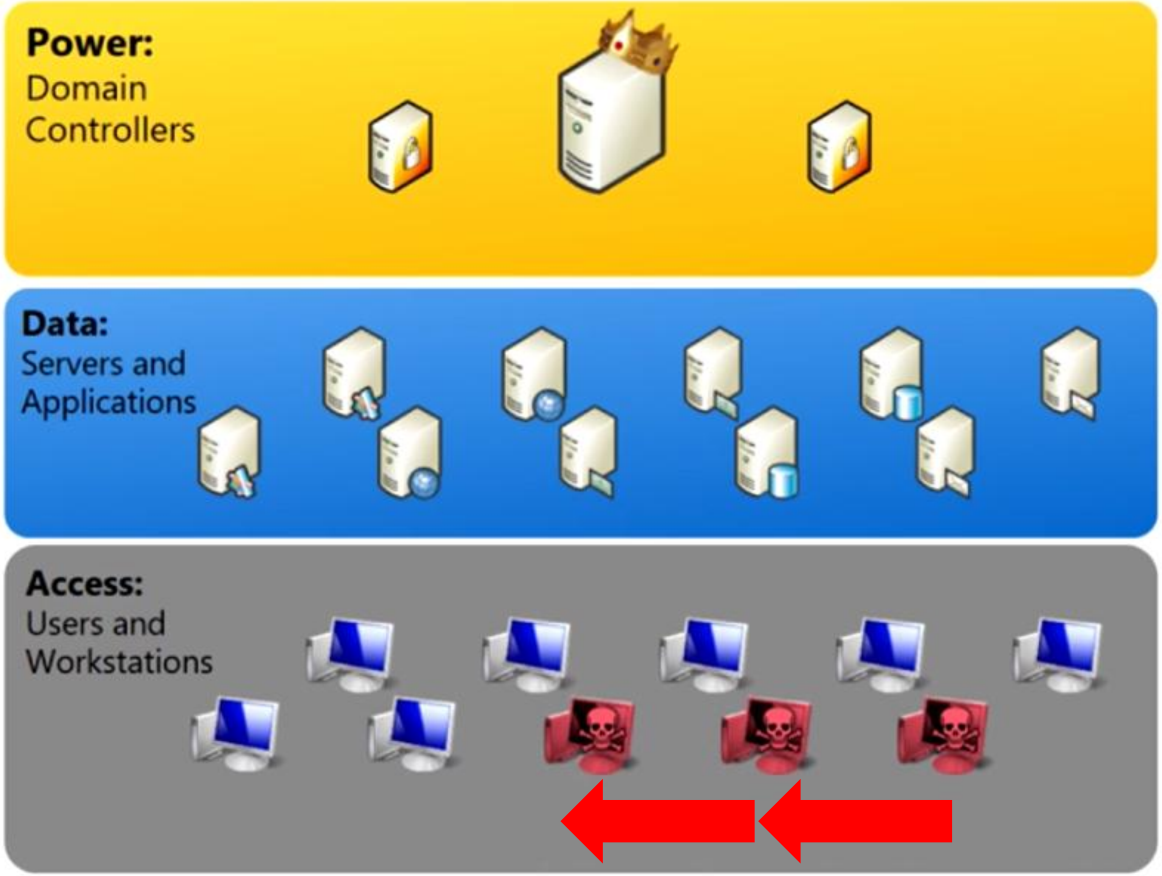
"Walk around"

- 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.
- **...**

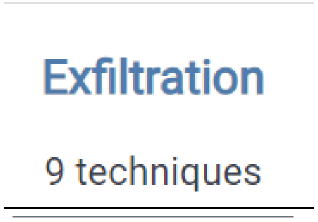
(+10 more techniques)

No damage yet

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

Damage: CIA Triad violations

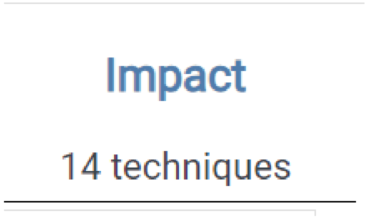
- Confidentiality
  - Ensuring that information is only accessible to those who are authorized to view it



Exfiltration

9 techniques

- Integrity
  - Ensuring that data remains accurate, consistent and unaltered except by authorized entities
- Availability
  - Ensuring that systems, networks and data are accessible when needed by authorized users



Impact

14 techniques

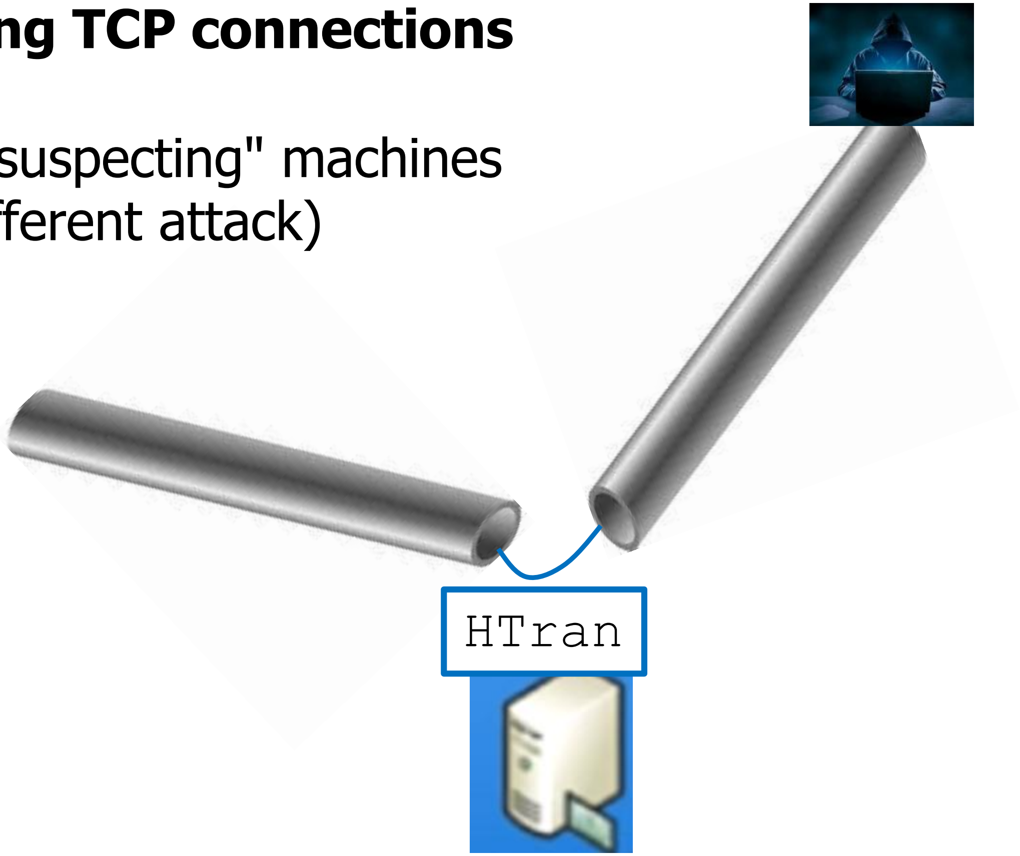
Exfiltration

- …
- **Exfiltration**
  - The adversary is trying to **steal** data.
  - Once they’ve collected data, adversaries often package it to avoid detection (**compression** and **encryption**).
  - Techniques for getting data out of a target network typically include transferring it over their **C&C channel** or **an alternate channel** and may also include putting size limits on the transmission.

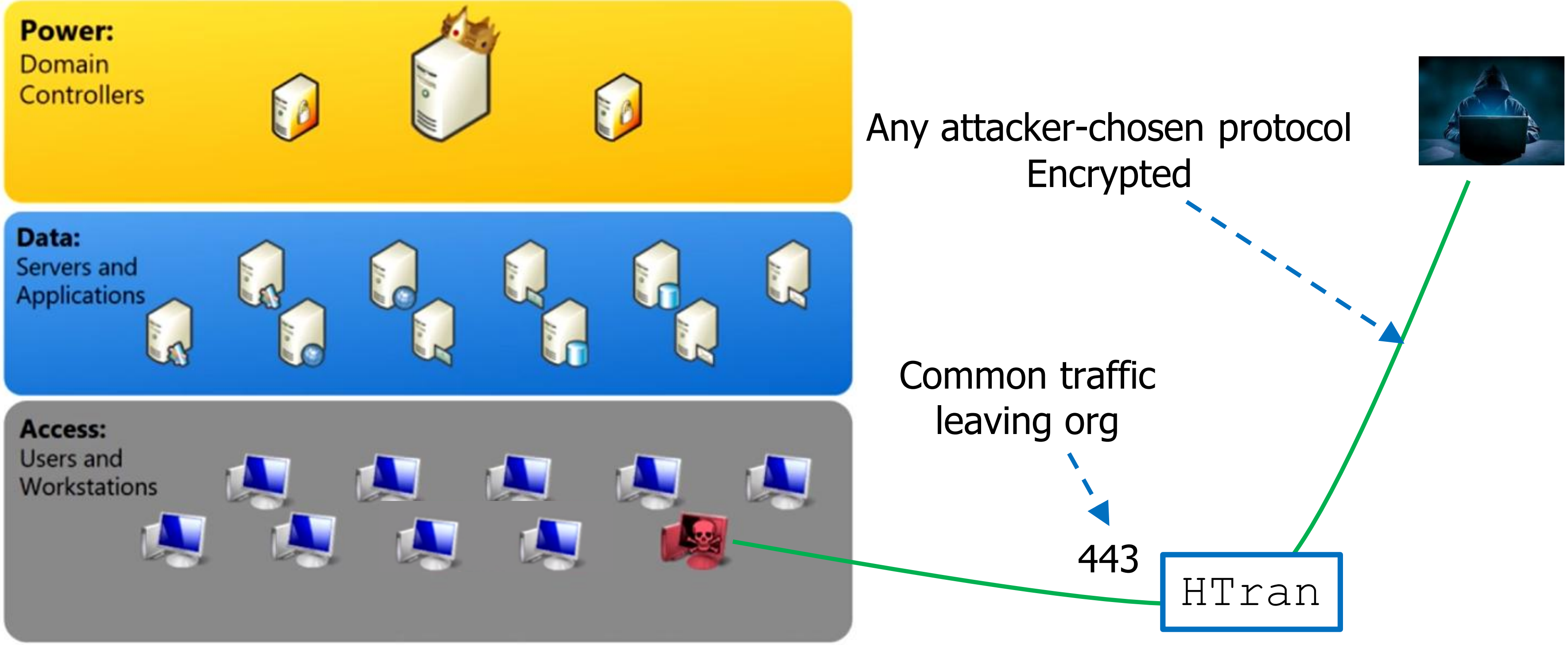
    (9 Techniques)

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

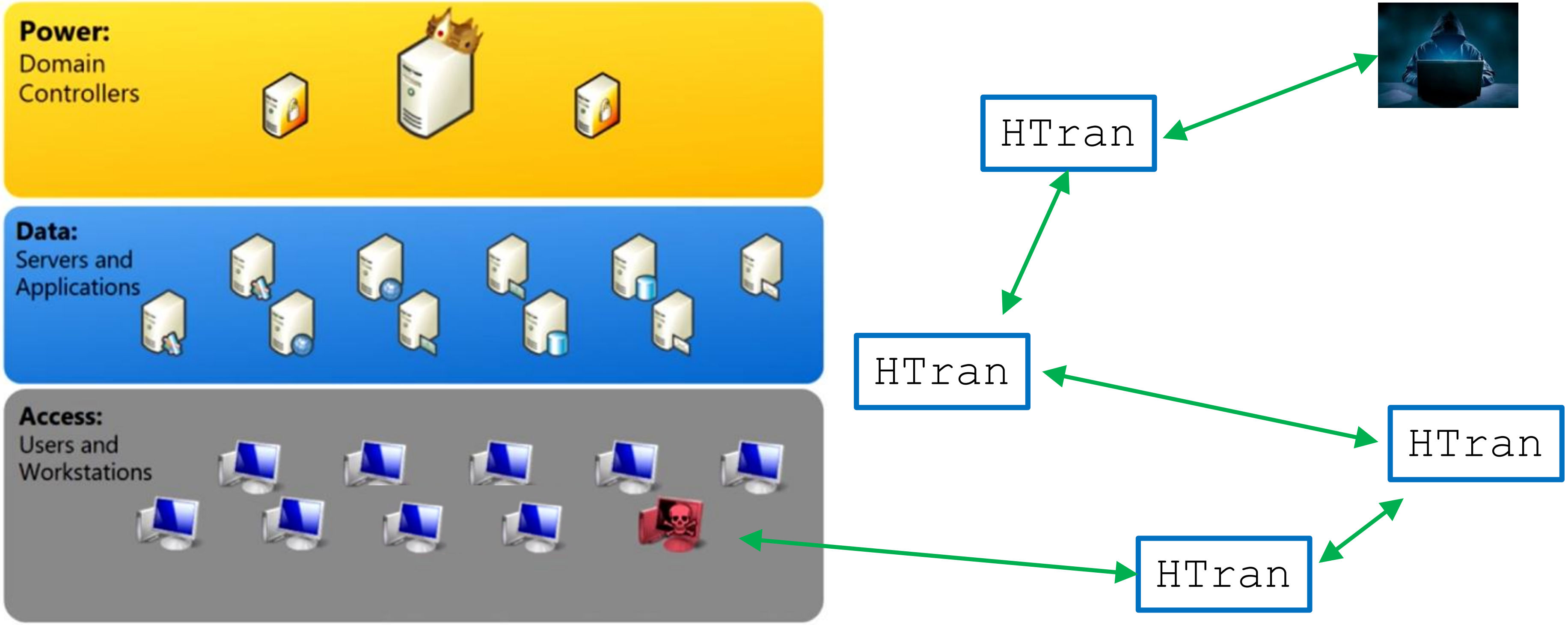
Common traffic
leaving org

443

`HTran`

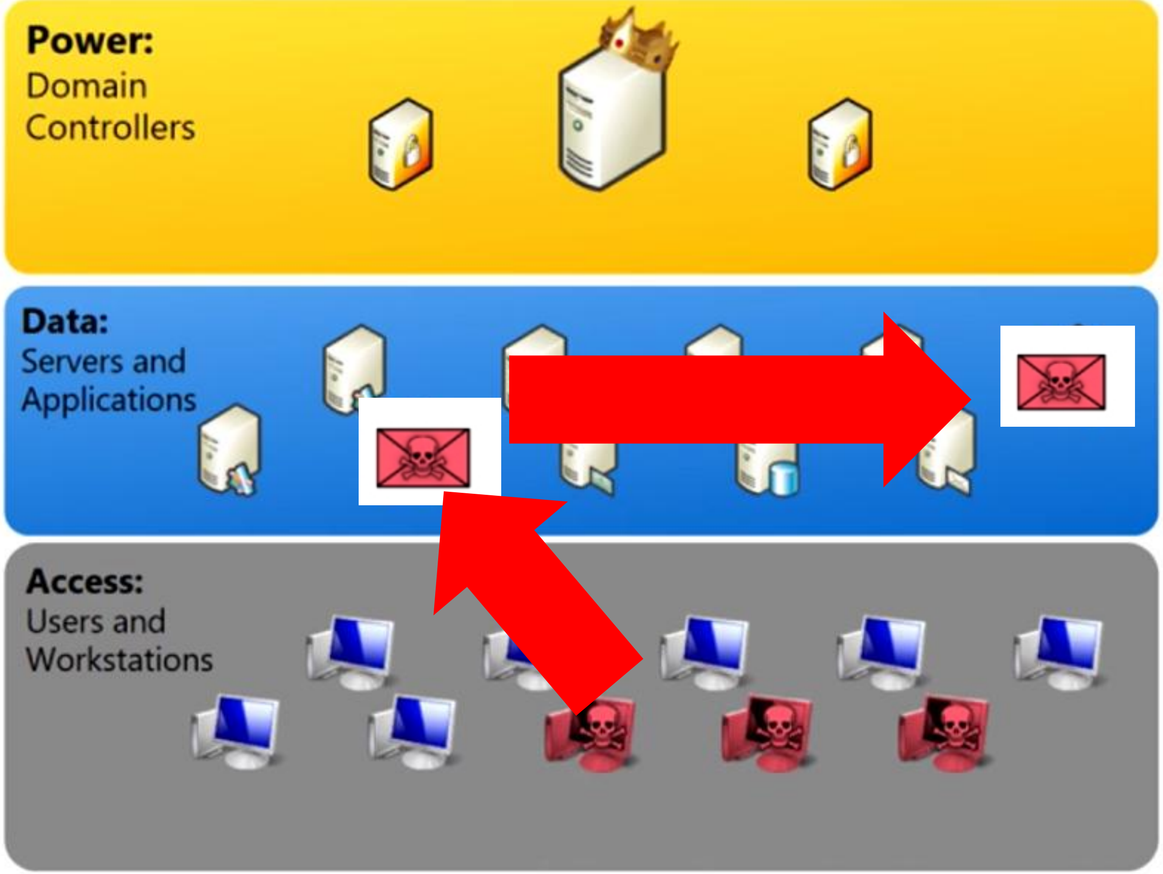
- "By using HTran in this way, the threat actor... **several months** without being detected."

Example: HTran (II-b)



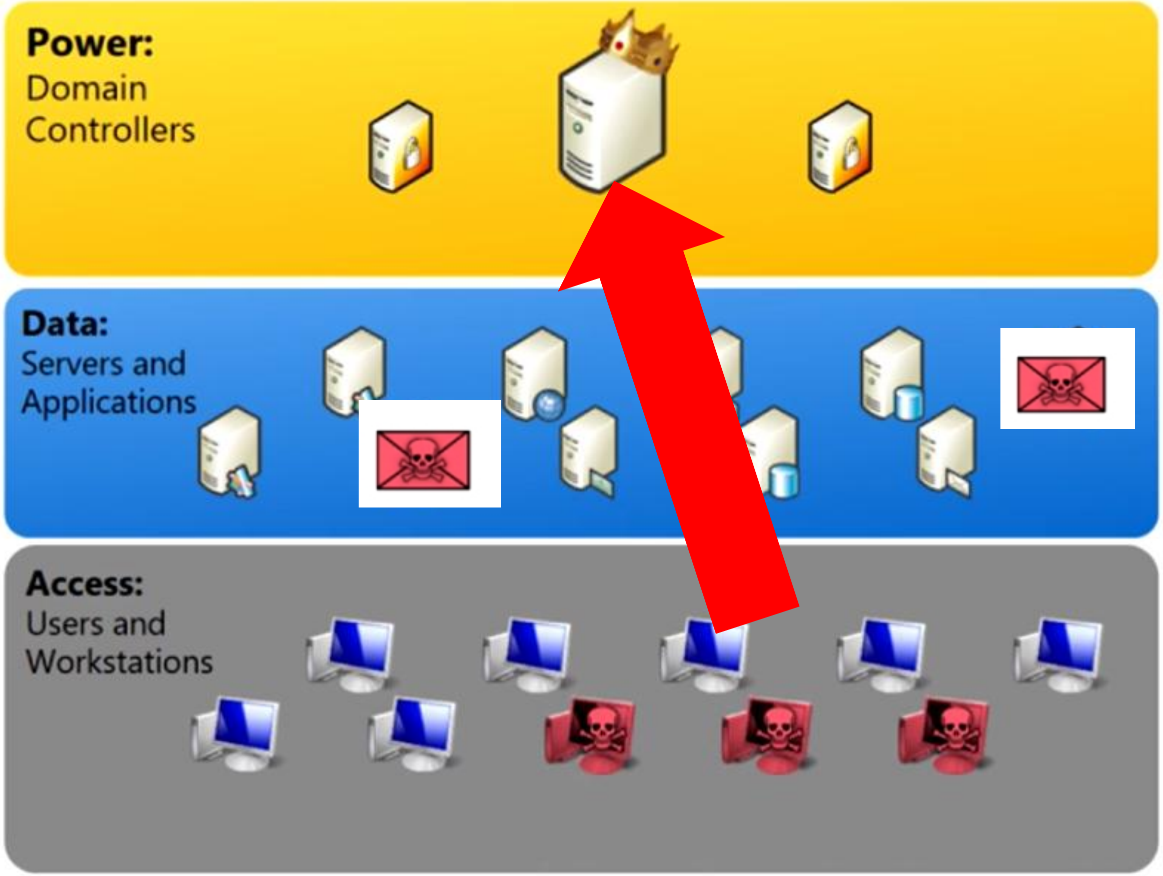
- "By using HTran in this way, the threat actor... **several months** without being detected."

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)



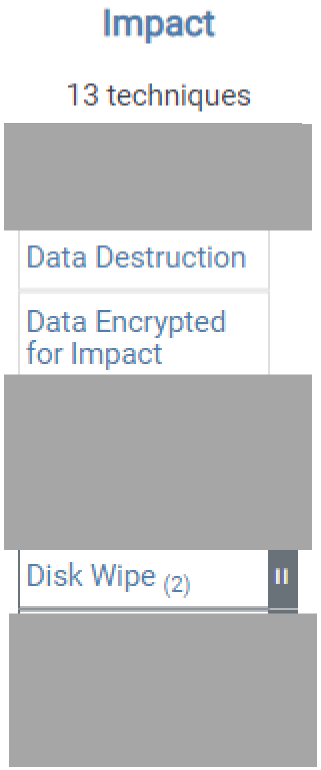
Total Catastrophe

Impact

- …
- **Impact**
  - The adversary is trying to **manipulate**, **interrupt**, or **destroy** your systems and data.
  - Techniques that adversaries use to disrupt **availability** or compromise **integrity** by manipulating business and operational processes.
    - In some cases, business processes **can look fine**, but may have been altered to benefit the adversaries' goals.
    - These techniques might be used by adversaries to follow through on their end goal or **to provide cover** for a confidentiality breach.

(14 Techniques)

Availability: Ransomware / Sabotage



Impact

13 techniques

[redacted]

Data Destruction

Data Encrypted for Impact

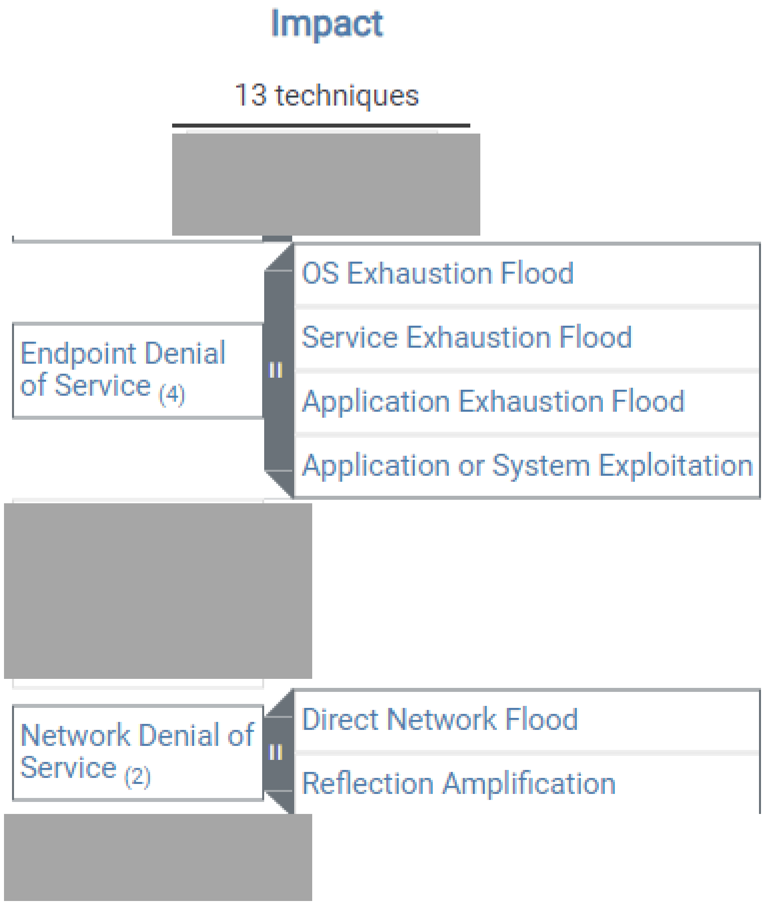
[redacted]

Disk Wipe (2)

[redacted]

- Adversaries may **encrypt data** on target systems or on large numbers of systems in a network to **compromise availability**.
- This may be done in order to **extract monetary compensation** from a victim in exchange for decryption or a decryption key (**ransomware**) or to render data **permanently inaccessible** in cases where the key is not saved or transmitted.
- To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to **propagate** across a network

Availability: Denial of Service (DoS)



Impact

13 techniques

Endpoint Denial of Service (4)

- OS Exhaustion Flood
- Service Exhaustion Flood
- Application Exhaustion Flood
- Application or System Exploitation

Network Denial of Service (2)

- Direct Network Flood
- Reflection Amplification

- Adversaries may perform **Endpoint DoS** attacks to degrade or block the **availability** of **services** to users.
- This can be performed by **exhausting** the system resources those services are hosted on or exploiting the system to cause a **persistent crash** condition.
- Example services include websites, email services, DNS, and web-based applications.

- **Network DoS** can be performed by exhausting the **network bandwidth** services rely on.

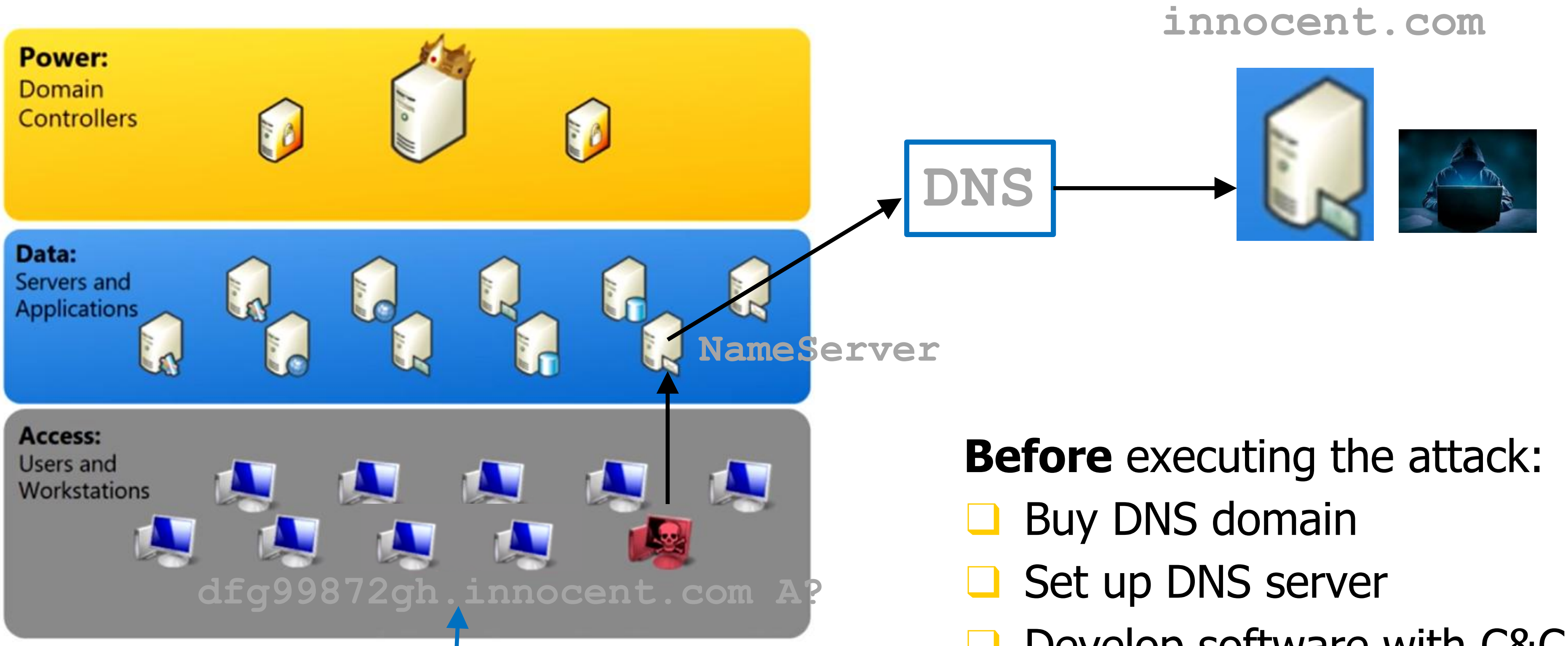
Damage done

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

Integrity
Availability

Confidentiality

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

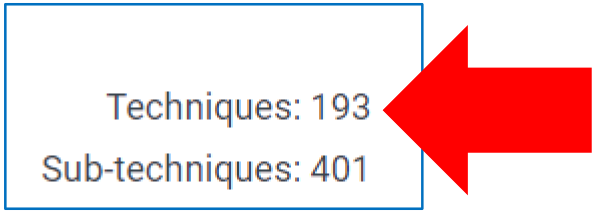
⬇

- 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**

A few words on other target categories

Attacking Single Individuals

1. Organizations
2. Single individuals
3. ICS

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

Economic view (I)

- Expected Gain >> Attack Cost
- Expected Gain from Single Individual "**small**"

How can it be cost-effective?

Economic view (II)

- Expected Gain >> Attack Cost
- Expected Gain from Single Individual "small"

- **Automation** is essential: **One** tool and **Many** targets
  - Attack Cost ≈ Independent of #targets
  - Expected Gain grows with #targets

  - More details near the end of the course

Attacking ICS

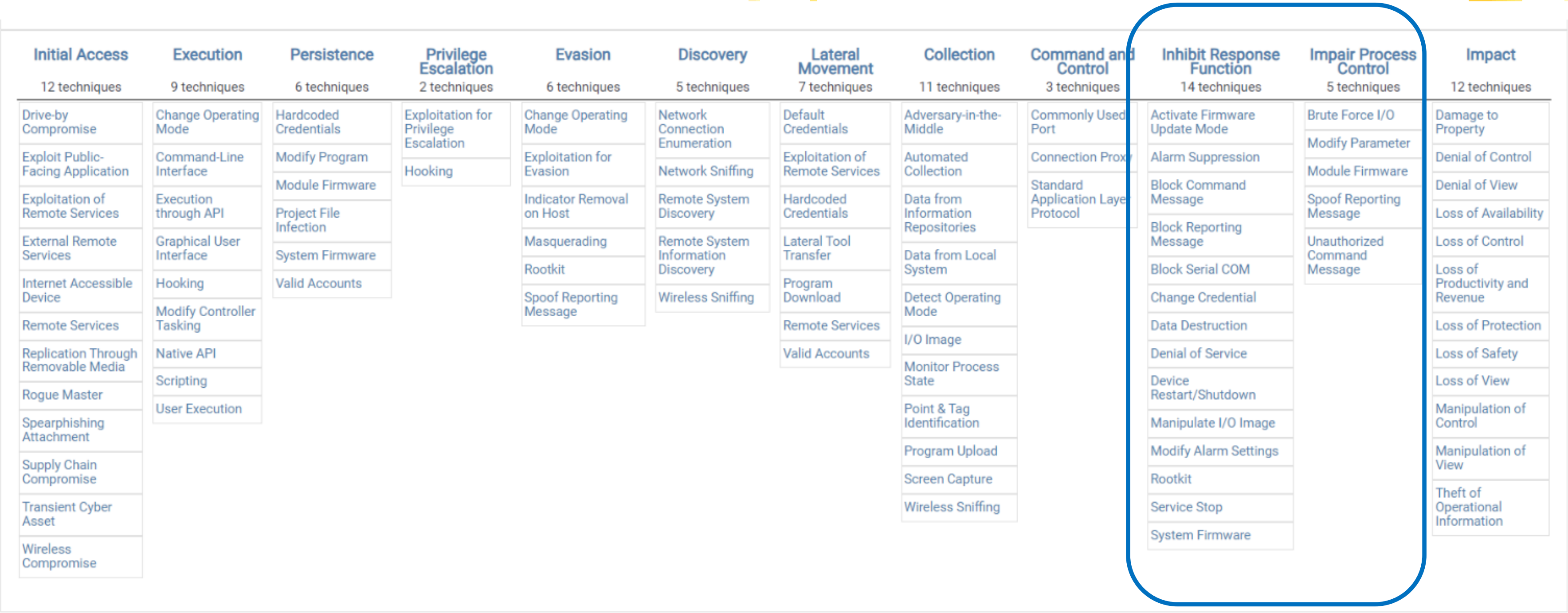
1. **Organizations**
   - □ Information Technology

2. **Single** individuals

3. Industrial Control Systems (**ICS**)
   - □ Information Technology

     +
   - □ Operational Technology

MITRE ATT&CK Matrix

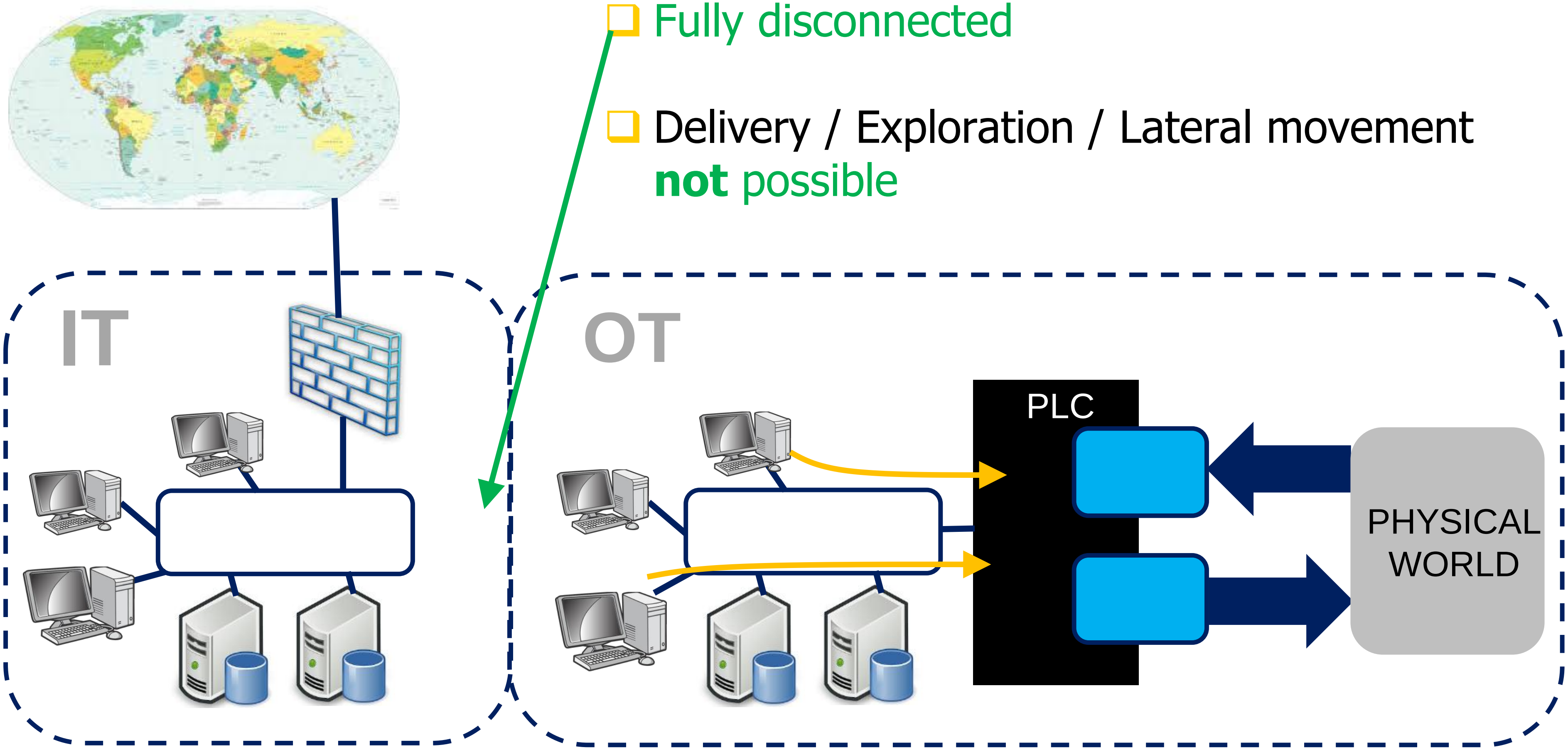


Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 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

Air Gap: Theory

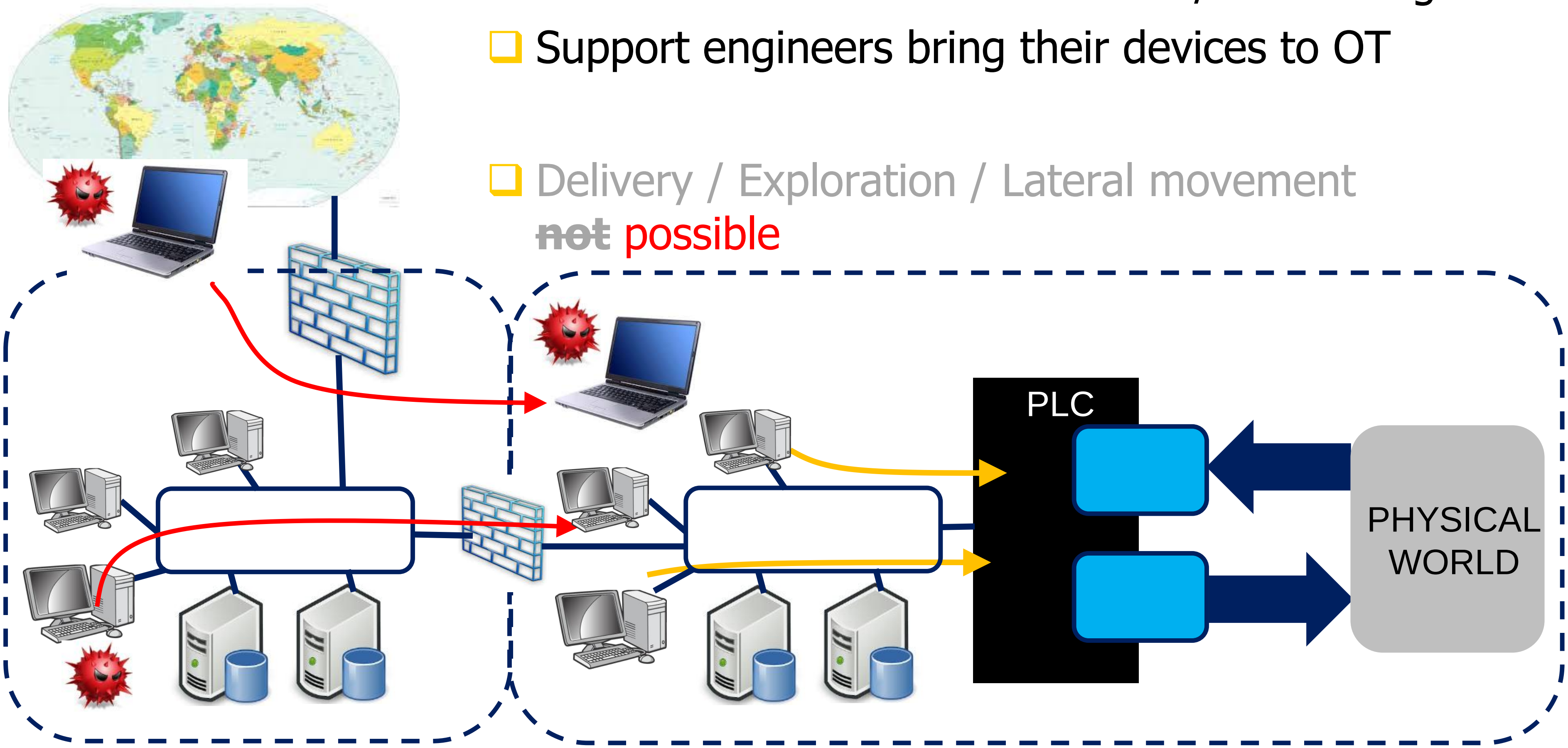
- ❑ Fully disconnected
- ❑ Delivery / Exploration / Lateral movement **not** possible



Air Gap: Practice

- ❑ OT accessible from IT for control / monitoring
- ❑ Support engineers bring their devices to OT

- ❑ Delivery / Exploration / Lateral movement ~~not~~ possible



Target Category: Organization

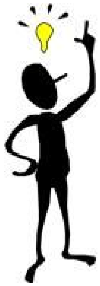
- Many **similarities** between Organizations
- A **given set** of skills, tools and knowledge
  is highly effective on **many different** organizations
- Standard, highly effective procedures for obtaining **money**

Target Category: ICS

- **Very few similarities** between OT in different ICSs
- A **given set** of skills, tools and knowledge is highly effective on **very specific** OT systems
- 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

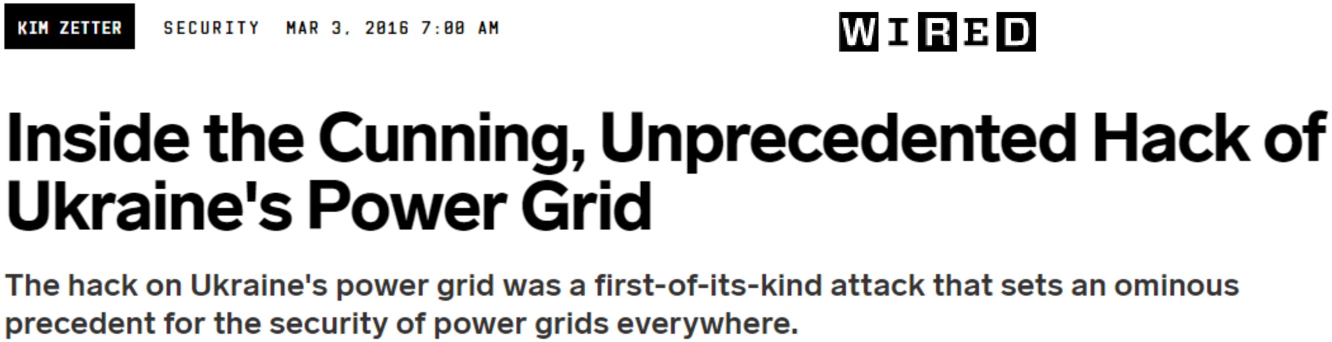


Important Remark 1

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

- ❑ Attacks on ICS may have strategic / intelligence motivations
- ❑ Objective is 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

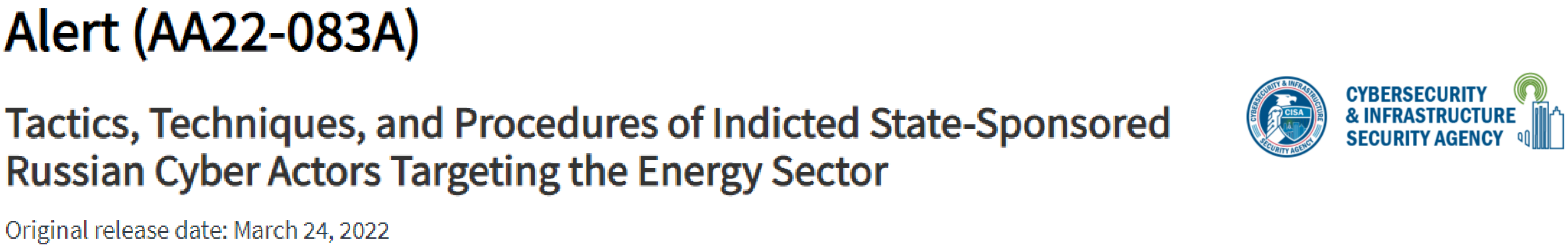
Bundesamt
für Sicherheit in der
Informationstechnik

- 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`

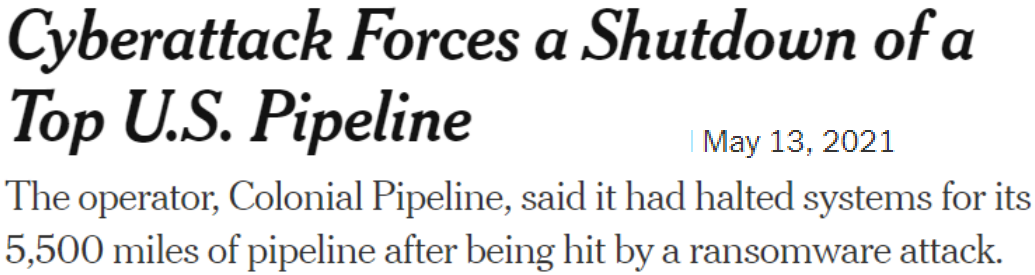
Important Remark 2

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

- Attacks on ICS may have strategic / intelligence motivations
- Objective is Stealing / Disruption
  (**not** Money)

- You do **not** need to attack the OT part to **disrupt** industrial operations.

Example 1



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

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.

The New York Times

- 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

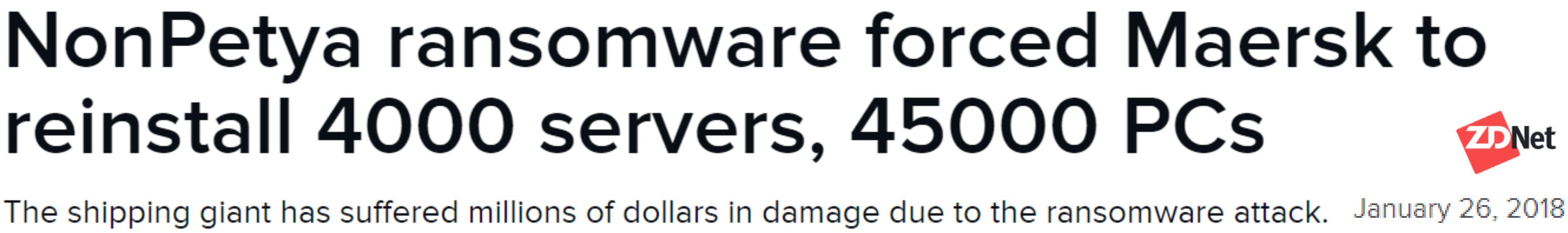
Toyota halts operations at all Japan plants due to cyberattack

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"