MITRE ATT&CK® for Industrial Control Systems

CYBERSECURITY M

Project report

Student: Gian Marco De Cola
0000977684

SOMMARIO

1 INTRODUCTION

1.1 WHAT IS AN INDUSTRIAL CONTROL SYSTEM?

Industrial Control System (ICS) is a general term that includes several types of control systems in an industrial setting [1]. It is also often associated with a variety of physical/logical assets, networks and instrumentations used in Operational Technology (OT) processes and generally in industrial process control.
Depending on the specific industry or industrial sector these ICSs can differentiate in several types:

- **Discrete controllers**: the most basic form of ICS, based upon small discrete controllers in a single loop, typically with an integrated operator interface.
- **Distributed Control Systems (DCSs)**: digital processor control system for a process or a plant where the controllers and the actuators/sensors are distributed throughout the system.
- **Supervisory Control And Data Acquisition (SCADA)**: computer based system that receives information and operational state from the controllers, presents the status in a graphical form to the operator, from which it takes commands to forward to the controller. Typically used in Distribution Management Systems (DMS) as a DMS Server.

1.1.1 ICS assets

For convenience, a list of the ICS technological domain assets [1] used in this document is hereby presented, dividing it in the following asset categories[1][2]:

- **Data Historian**: a centralized database, accessed by external corporate users, in which system data are logged for archival and analysis use.
- **Engineering Workstation (EWS)**: very reliable computing platform designed for configuration, maintenance and diagnostics of the control system applications and equipment.
- **Field Controller (RTU/PLC)**: computerized control units typically racked, or panel mounted, with modular processing and interface cards. They communicate with physical sensors/actuators using a various range of serial or specialized network protocols to provide the users with information and let them pass commands to the devices.
- **Human-Machine Interface (HMI)**: graphical, textual, and auditory information presented by the controllers to the operator and control sequences the operator employs to control the system. Nowadays these interfaces are usually deployed on traditional workstations through GUIs and/or web-based interfaces.
- **Input/Output Server**: provides the interface between the control system LAN and the field equipment, converting the control system application data into packets transmitted over to the field devices using proprietary protocols or to the HMIs using TCP/IP protocols.

[1] https://www.cisa.gov/uscert/ics/Secure-Architecture-Design-Definitions
[2] https://collaborate.mitre.org/attackics/index.php/All_Assets

- **Safety Instrumented System (SIS)**: takes automatic actions to keep an ICS in a safe state or to put it in a safe state, when anomalies happen (e.g. emergency shutdowns/cooling, etc.)

1.1.2 The Purdue Model

It is custom to refer to an ICS architecture in terms of the Purdue Model [2], a reference architecture for a general enterprise, widely used in literature and industry. The adaptation of the model to ICS architecture security usually divides it in 5-6 functional tiers: each tier both defines a functional layer and is formed by various assets. The tiers, their description and assets are included in *Figure 1.1*.

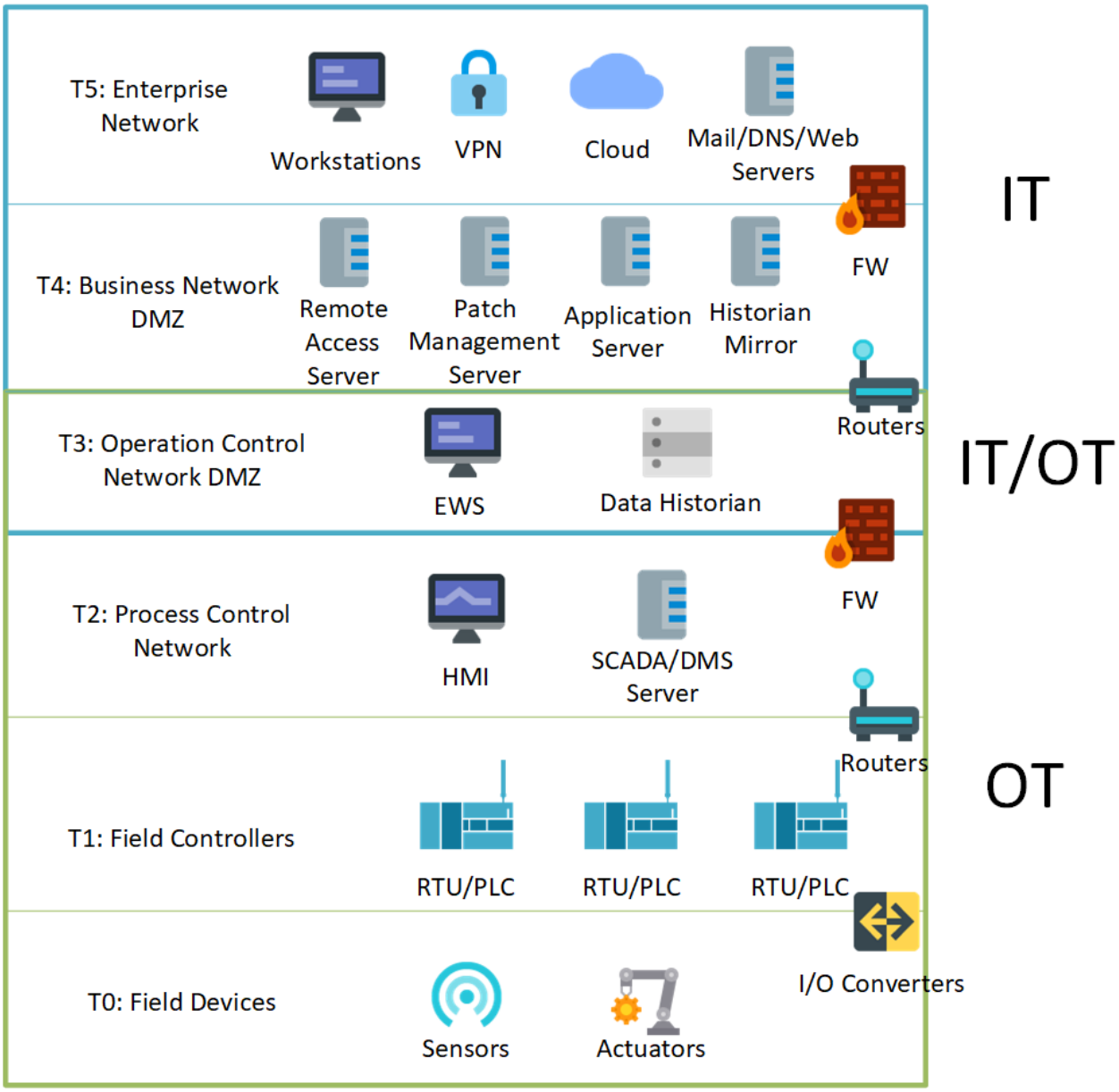

Figure 1.1-The Purdue Model for Industrial Control Systems

1.2 What is MITRE ATT&CK?

ATT&CK is a free knowledge base and model of cyber adversary behavior by the MITRE Corporation [3]; it is globally accessible, and community fed, so that every cyber security community member

can actually participate to the growth of the knowledge base itself. As a matter of fact, ATT&CK is based on real-world observations, by gathering OSINT on the most important attacks so far and categorizing them to fit the ATT&CK knowledge base (investigated in *Section 1.2.1*). It is a living and ongoing project, so the knowledge base is constantly being updated with the most recent information about attacks as soon as advisories, disclosures and research are available for the project maintainers to integrate.

The project was born in 2013 and leaned towards the world of enterprise IT attacks, by considering an "assume breach" mentality and focusing on "post compromise" behavior; in 2017, a complementary model, the PRE-ATT&CK matrix, was integrated, also considering "left of exploit" phases of the cyber kill chain[3]. Since then, it has reached wide consensus in the cyber security community and the MITRE researchers began the process of creating new versions of ATT&CK, also orienting the scope towards the Mobile world, the Cloud world and, most recently, the ICS world.

1.2.1 The knowledge base

Each of the aforementioned worlds have its own ATT&CK Matrix. An ATT&CK matrix is a set of Tactics, Techniques and Procedures (TTPs), used by threat actors to perform a cyber-attack. For this reason, an ATT&CK matrix is organized as such [3] [4]:

- **Tactics**: a column of the matrix. They represent the "why" of a technique: the adversary tactical goal that they hope to achieve by performing a specific technique.
- **Techniques**: a box under a tactic column. They represent "how" an adversary expects to achieve a tactical goal. There are multiple techniques under a tactic column, as there are multiple ways to achieve a specific goal.
- **Procedures**: represent a specific implementation of a technique (e.g. Sandworm Team's Unauthorized Command Message in the Ukrainian 2015 incident).

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

Figure 1.2-The ATT&CK for ICS Matrix

[3] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

The Matrices are accessible on the MITRE ATT&CK website[4]: clicking on a tactic or technique will open a window that contains descriptions, OSINT sources, possible mitigations, and detection/prevention ideas; in case of a technique, multiple known procedures of as many threat groups as available in the sources are presented. Another useful way to use the matrices, is the ATT&CK Navigator[5]: a very powerful tool that allows to customize a specific matrix to your needs and to export your modifications in report-friendly formats (example of use will be provided in *sections 2.1* and *2.2*).

1.3 MOTIVATIONS FOR ATT&CK FOR ICS

The advent of Industry 4.0, 5G networks, edge computing and IIoT has led to the adoption of more and more interconnected devices, even in the critical infrastructure/industrial world[6]. The consequences of this are a double bladed knife: on the one hand it enables quicker notification of anomalies, optimized control and management of field devices/controllers, etc., on the other hand this widens the cyber-attack surface, by introducing new threats and vulnerabilities in the already much insecure ICS world. In fact, ICSs suffer from the fact that many instrumentations, devices, and controllers are very much outdated and, most importantly, difficult to update or substitute without unaffordable disruption of service. This scenario was already critical 10 years ago, as the Stuxnet[7] case made us realize, but now that the "air gap" has been filled, such a situation cannot be overseen.

The lack of numerous and organized reporting on ICS cyber security incidents has led the MITRE Corporation to start a dedicated ATT&CK project on this topic, in 2017. The new initiative is also justified by the fact that adversary goals and techniques, as well as technology and defenses are somewhat different from an IT enterprise case. It has to be noted (*Figure 1.3*) that a certain degree of overlapping is present between the ATT&CK for Enterprise and for ICS knowledge bases, and this is mirrored by the fact that, more often than not, the initial compromise of an ICS/OT network comes from the exploiting of the IT network, that combined with a scarce segmentation of the networks, serves as the initial foothold for a larger ICS compromise.
The main differences between IT and OT/ICS attacks are:

- **Adversary goals**: an ICS/OT attacker aims at impairing process control by the operators, inhibiting the response functions of a SIS and/or causing a physical impact to the systems, as well as reducing its safety, going as far as creating danger for human lives (e.g. terrorist attacks). These goals are not chasable by an IT enterprise attacker. This results in an addition of new tactics in the ATT&CK for ICS matrix in respect to the Enterprise one [4].
- **Technology differences**: proprietary/domain specific communication protocols, embedded platforms, specialized applications and process automation protocols which are different from or lacking in Enterprise IT networks. This results in an addition of new techniques in the ATT&CK for ICS matrix in respect to the Enterprise one [4].

[4] [4] https://attack.mitre.org/matrices/
[5] https://mitre-attack.github.io/attack-navigator/
[6] https://ics.kaspersky.com/media/Kaspersky_ARC_ICS-2020-Trend-Report.pdf
[7] https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

- **Different defenses**: there are unique concerns about mitigations in the ICS world. To test the mitigation effectiveness is not trivial, neither is their deployment or application.

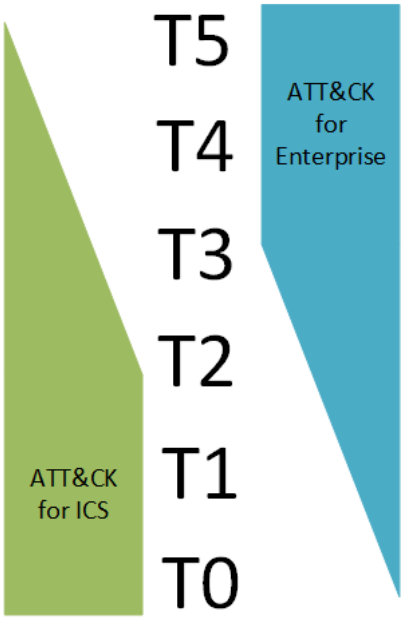

Figure 1.3-ATT&CK for Enterprise/ICS mapping to the Purdue Model

2 APPLYING ATT&CK FOR ICS

The philosophy and the process that created ATT&CK is one of the biggest efforts so far to advert a transition from an Indicator of Compromise (IoC) and reactive based approach to cyber security to a threat based one, by proposing a methodology that encompasses Cyber Threat Intelligence and proactive approaches [3], [4]. To do this, as already pointed out in *Section 1.2.1*, the framework offers a profile of threat actors, by categorizing the TTPs used by them in previous attacks: by doing so, the model focuses on adversary behavior, rather than their tools, assets, IP addresses or malicious file hashes. This is also advised in David Bianco's "Pyramid of pain"[8] (*Figure 2.1*), a conceptual model which explains *«the relationship between the types of indicators you might use to detect an adversary's activities and how much pain it will cause them when you are able to deny those indicators to them*».

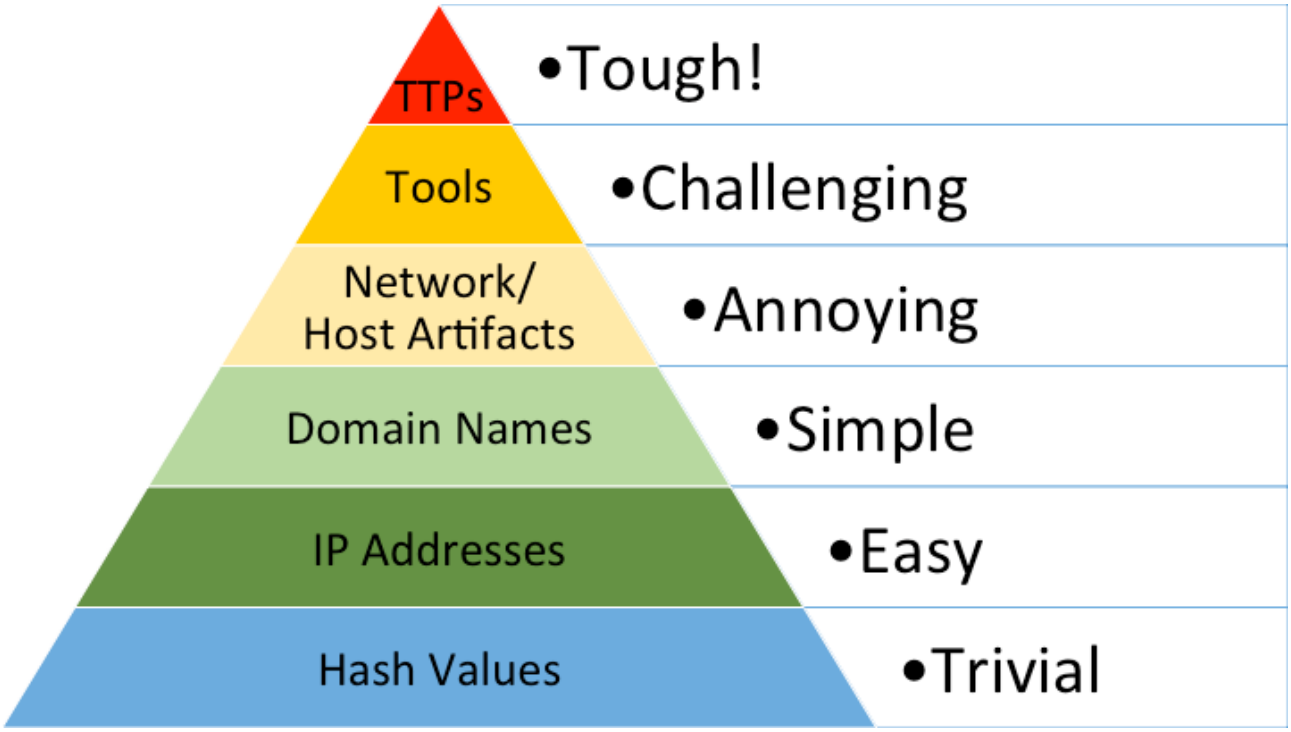

Figure 2.1-David Bianco's Pyramid of Pain[8]

Possible use cases of the framework span from red teaming and Adversary emulation [5] to SOC maturity assessments and defensive gap assessments [3]. Of course, given the nature of the framework, it can be also used to enrich the Cyber Threat Intelligence process and as a "common tongue" for more comprehensible and unambiguous reports. It can also be very useful in risk assessments to delineate your company defensive posture and prioritize in which category to put your defensive efforts. In the case of the ICS framework, Failure Scenario Development is also an option for the framework usage [4], useful to understand what can go wrong if a specific device of the architecture fails during operations.

[8] http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

2.1 SIMULATING A DEFENSE GAP ASSESSMENT

«A defensive gap assessment allows an organization to determine what parts of its enterprise lack defenses and/or visibility» [3]; this can be leveraged to define a priority scale for investments in defensive solutions and to assess the general effectiveness of existing defenses. Hereafter, a simulation of a defense gap assessment will be presented. The work has been conducted by envisioning a company in charge of an energy center; a rough network distribution of the center and interested devices is available at *Figure 2.2*. The simulation has been carried out imagining four different phases[9]:

- A **white team** is appointed of assessing the defensive posture of the company. To do so, it leverages the MITRE ATT&CK for ICS model, mapping what TTPs the existent defense policies and technologies can actually prevent, detect or respond to (*Figure 2.3*). In the current example, these policies and technologies are used:
    - **Strong password policy**: enforces the use of safe passwords for logging in and the changing of default passwords in assets to prevent trivial brute force/dictionary attacks.
    - **Account identification**: to ensure accountability.
    - **Manual intervention to change operative modes of controllers**: to prevent remote changing of critical controllers' state by non-authorized personnel.
    - **SIM**: to enable centralized logging of actions and events on the network for later response/recovery. Logs are inspected on a 6 month basis.
    - **AV**: to detect any malicious file being downloaded onto hosts using a signature-based approach.
    - **Firewall**: packet filtering to let only the SCADA servers access the historian for network segmentation between tier 3 and lower tiers of the Purdue Model.
- A **red team** is appointed to develop an attack scenario by exploiting TTPs utilized by APTs in known attacks to similar targets (*Figure 2.4*). This is also performed with the help of the ATT&CK for ICS framework and the ATT&CK navigator, which also let you search TTPs by filtering them by specific APT or threat group adoption. The developed attack scenario goes as follows (leveraged TTPs in bold):
    - The **initial access** in the system is gained by leveraging a previous attack to the lithium-ion batteries vendor and leveraging asset information and credentials discovered in such attack. The cellular modem used to enter the network is an **internet accessible device**, with a **public-facing application**, needed by the lithium-ion battery vendor to monitor and maintain the state of the devices.
    - A **CLI** exposed by the modem GUI will be leveraged to actuate a **Remote Systems Discovery** and **gain information** about them by pinging devices on the network and contacting their commonly used ports.

[9] Please note that the simulation is a clear understatement of the work actually needed for performing such an assessment, but the simplification is needed to give an example and convey the purpose of the assessment with the limited time and resources available. The scenario was loosely based on the 2012 Telvent attack (https://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/)

    - **Lateral Movement** and connection **persistence** is ensured by the fact that adversaries will be using **valid accounts** and credentials. Also leveraging valid accounts, **Lateral Tool Transfer** of any tool needed to perpetuate the attack will be attempted, as it is often difficult to only "live off the land". The tools will be carefully **masqueraded** as expected vendor executables and configuration files, for detection **evasion**
    - **Privilege escalation** is attempted to allow access to the Turbine HMI by pivoting through the data historian, using Remote Desktop Protocol. Here **Screen Capture** will be performed to stealthily **collect** further data about the PLCs state and parameters without the operator knowing or being kicked off the HMI
    - These data will be used to **modify PLC parameters** through the HMI, sending commands to the SCADA master to **Impair Process Control** and cause **Manipulation of control**. The modified PLC parameters will allow **Loss of Availability** of the turbines, as they will be shut down indirectly by the parameters injected in the PLC
- At this point, an adversary emulation of the developed attack scenario can be carried out by the red team. A **blue team** could also be appointed to try to detect/respond to the attacks in real time. Given that this is out of scope (and resources) for this project, this phase is skipped.
- The white team assesses the results of the performed attack scenario, integrating the gathered data with the precedent defense posture assessment and using it to generate a list of possible defenses/countermeasures. This results in a scored ATT&CK matrix (*Figure 2.5*), which highlights the main issues after the attack. This can be leveraged to invest in the filling of higher priority defensive gaps.

2.1.1 Conclusions

From the assessment, the white team can detect a difficulty in the response phase in case of impact, which should be seriously considered by the company managers. As expected, the most critical gap is found in the "Initial access" phase, as the proposed attack leveraged valid credentials. In this case, though, the breach of the vendor (if timely disclosed) should have been considered carefully, and a policy for credentials revocation could have been put in place for the compromised accounts. Next, the command line interface of the cellular modem, should be hardened against misuses, enforcing a whitelist of legitimate, permitted commands. Moreover, it has to be noted that although the network is segmented, it is not correctly segregated, as it should not be possible to access another machine from the data historian (only data packets should be allowed in the outgoing direction).

On the technological standpoint, the company could integrate the AV with a HIDS/NIDS, to also detect suspicious files on all the assets and network activity such as lateral movement and lateral tool passing. Finally, a SIEM is advised to fully implement an active detection phase (maybe also based on machine learning), to promptly prevent or mitigate suspicious actions, instead of just logging them and assessing them later. To assess the segregation problem, upgrading the packet filtering firewall to an application-level gateway could be one solution (to also monitor application payload, as performance is not so critical in this point).

As a sidenote, the adoption of a Zero Trust Architecture (ZTA), could have avoided the whole incident as lateral movement is prevented by-design and the compromised vendor credentials would not have permitted access, if the ZTA was correctly configured to dynamically evaluate Authentication and Authorization for every session.

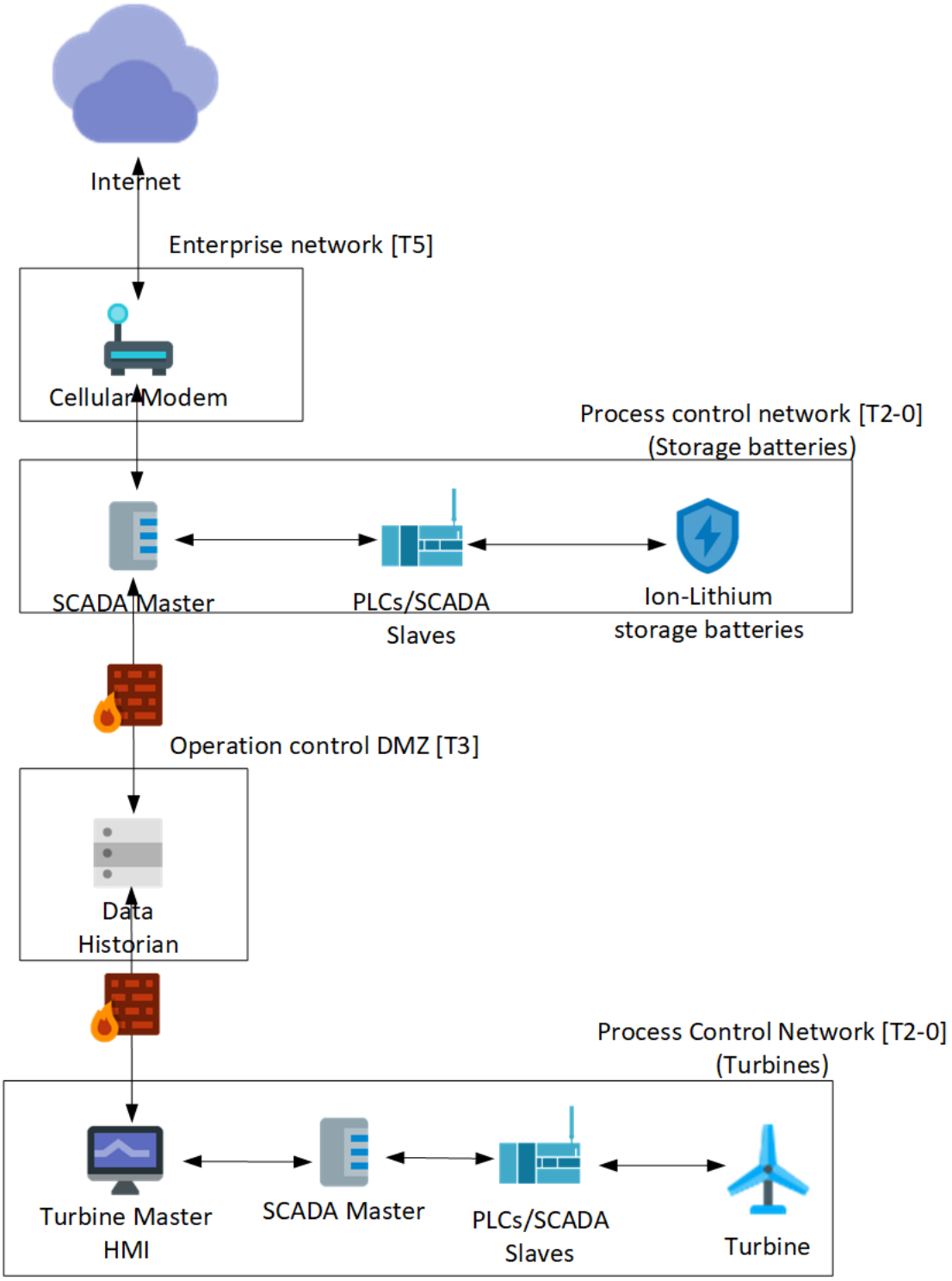

Figure 2.2-Energy center network model (Purdue model tiers in squared brackets

Figure 2.3-Defensive posture of the assessed company, using ATT&CK for ICS

Figure 2.4-Attack Scenario mapped on the ATT&CK for ICS matrix

Figure 2.5-Defensive gaps resulted by the emulation of the attack scenario. The higher the score, the worst the gap.

2.2 MAPPING THE 2015 UKRAINIAN POWER GRID ATTACK

Mapping an attack by a famous APT (SandWorm Team in this case), can be useful for Threat Intelligence and proactive defense purposes, as the adversary behavior can then be more easily emulated by a company Red Team or can be methodically investigated and confronted with the company defensive posture. It could be also leveraged using a reactive approach, embracing an "assume breach" mentality, to carefully and selectively look at the most probably exploited parts of the system to speed up the breach detection. Hereafter an attempt to map the 2015 Ukrainian power grid attack [6] [7] to the ATT&CK (Enterprise+ICS) framework is made. A very thoroughly made report is available at [7], but here its dissection of the attack is revised to better map it to the ATT&CK framework (tactics are underlined. Stages 1 to 8 are relative to the Enterprise matrix only, the other stages begin to mix Enterprise and ICS techniques, so technique belonging will be specified. A diagram of the attack is presented at *Figure 2.6* to follow along with the following description, while Enterprise and ICS matrixes mappings are available at *Figure 2.7* and *Figure 2.8* respectively):

- ***Stage 1***: Reconnaissance and Intelligence Gathering (techniques listed under the Reconnaissance tactic in the Enterprise matrix)
- ***Stage 2***: obtaining and modifying the BlackEnergy3 RAT and weaponizing Word/Excel documents (techniques listed under the Resource Development tactic)
- ***Stage 3***: deliver BlackEnergy 3 (BE3) (attached to Spearphishing emails, Initial Access tactic)
- ***Stage 4***: BE 3 is installed by the users, enabling macros on MS Office files attached to the phishing email (techniques listed under the Execution tactic and Office Application Startup technique under the Persistence tactic)
- ***Stage 5***: Command and Control connection establishment
    - ***Stage 5.1***: BE3 modifies MS Windows registry security settings to allow outgoing connections to CC servers (Modify Registry technique under the Defense Evasion tactic)
    - ***Stage 5.2***: installed malware opens HTTPS connection to the CC servers (Application Layer Protocol under the Command and Control tactic)
- ***Stage 6:*** BE3 acts as a receiver of malware plugins through the CC connection (Ingress Tool Transfer technique under the Command and Control tactic)
- **Stage 7**: credentials and accounts takeover
    - **Stage 7.1**: a BE3 plugin logs keystrokes and harvests stored credentials (techniques are listed under the Credential Access and Collection tactics)
    - **Stage 7.2**: harvested credentials are exfiltrated through the CC channel (Exfiltration Over C2 Channel technique under the Exfiltration tactic)
    - ***Stage 7.3***: harvested admin credentials are used to access the domain controller to steal further credentials and create new high privileged users (Create Account under the Persistence tactic)

    - ***Stage 7.4***: newly created accounts or stolen admin credentials are used to blend into regular network traffic (Valid Accounts techniques under the Defense Evasion tactic)
- **Stage 8**: enterprise network systems access
    - **Stage 8.1**: vulnerable systems enumeration within the corporate network (techniques are listed under the Discovery tactic)
    - **Stage 8.2**: MS PsExec is exploited to gain access to remote workstations and servers (Windows Remote Management technique under the Lateral Movement tactic)
- **Stage 9**: ICS network foothold (**ICS matrix**)
    - **Stage 9.1**: stolen credentials are used to access the ICS network through VPN access to the DMS server and through Remote Desktop Protocol from the Enterprise workstations to the HMI workstations (respectively External Remote Services and Remote Services techniques under the Initial Access tactic)
    - **Stage 9.2**: information gathering on the ICS network (techniques listed under the Discover tactic)
- **Stage 10**: obtaining the KillDisk (KD) malware and modifying Serial-to-Ethernet converters' firmware (techniques listed under the Resource Development tactic of the **Enterprise matrix**)
- **Stage 11**: final attack staging (**Enterprise Matrix**)
    - **Stage 11.1**: deliver KD to the network share (Ingress Tool Transfer technique under the Command and Control tactic)
    - **Stage 11.2**: set up policies on the Domain Control Server to retrieve the KD malware from Network Shares and execute it at systems' reboot (Create or Modify System Process technique under the Persistence tactic)
- **Stage 12**: schedule UPS disruptions for telephone servers and data center servers (Create or Modify System Process technique under the Persistence tactic of the **Enterprise Matrix**)
- **Stage 13**: access the DMS server and HMI workstation to issue unauthorized command messages to toggle the breakers (Unauthorized Command Message technique under the Impair Process Control tactic and Loss of Availability and Productivity and Revenue techniques under the Impact tactic of the **ICS Matrix**)
- **Stage 14**: PLC Serial-to-Ethernet converter modules firmware compromise (**ICS Matrix**)
    - **Stage 14.1**: malicious firmware and KD malware delivered and installed to the converters (System Firmware technique under the Persistence tactic)
    - **Stage 14.2**: malicious firmware renders the converters inoperable, manual access to the breakers is needed to switch them on again (Denial of Control technique under the Impact tactic and Block Command Message technique under the Impair Process Control tactic)
- **Stage 15**: TDoS attack to the telephone server to prevent customers to reach the customer service and notify the distruption (Endpoint Denial of Service technique under the Impact tactic of the **Enterprise Matrix**)

- **Stage 16**: scheduled suspension of UPS takes place, enterprise workstations and RTUs/PLCs shut down because of the power outage and UPS suspension (System Shutdown/Reboot technique under the Impact tactic of the **Enterprise/ICS Matrix**)
- **Stage 17**: Once the power returns, KD malware executes, wiping the MBR enterprise systems disks (Data Destruction and Disk Wipe techniques under the Impact tactic of the **Enterprise Matrix**) and RTUs/PLCs firmware (Loss of Availability and of Productivity and Revenue techniques under the Impact tactic of the **ICS Matrix**)

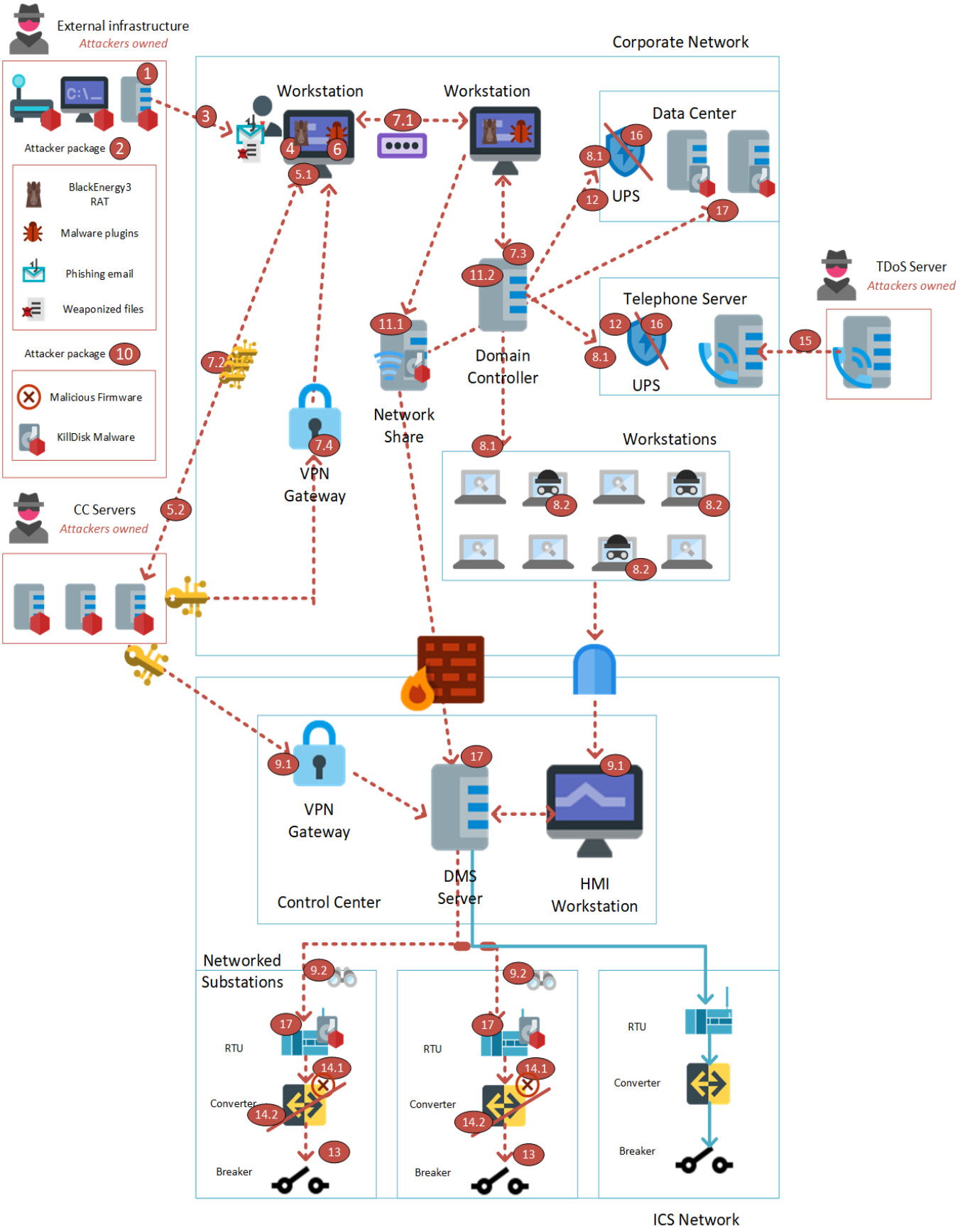

Figure 2.6-Stages of the 2015 Ukrainian power grid attack (adapted from [6])

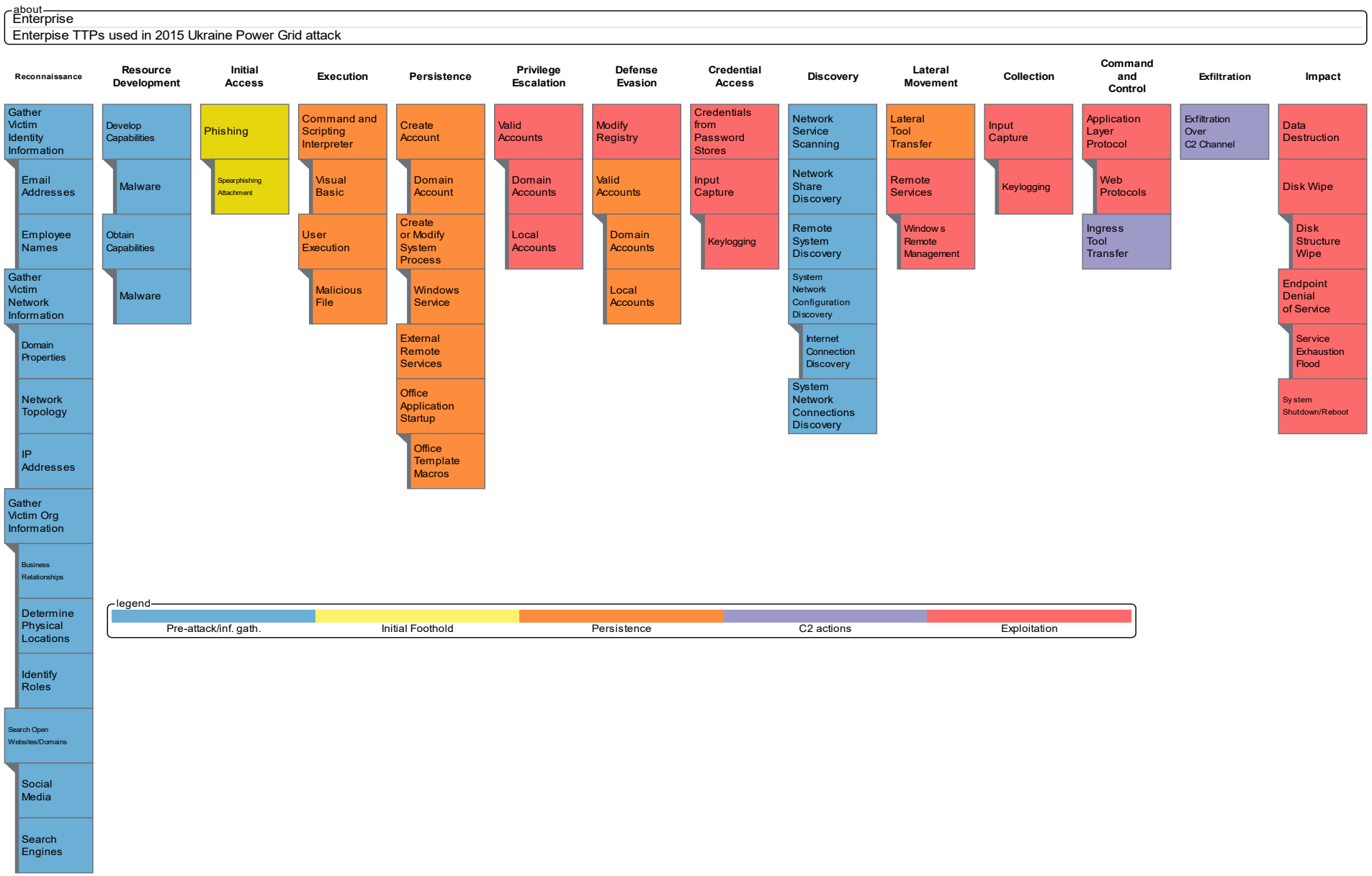

Figure 2.7-IT attacks mapped on the ATT&CK for Enterprise matrix (techniques that have not been used in the attack are omitted for graphical purposes)

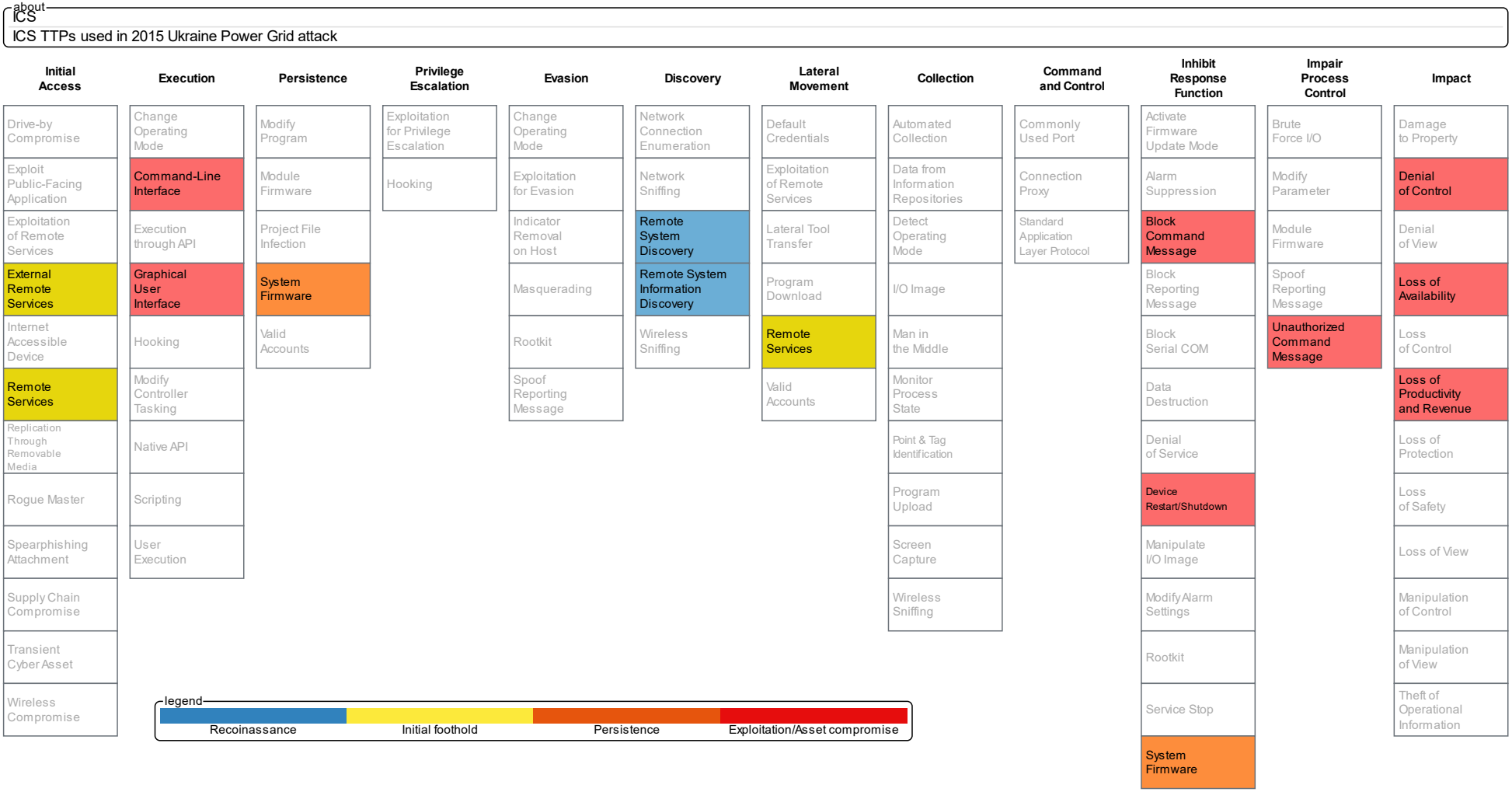

Figure 2.8-OT attacks mapped on the ATT&CK for ICS matrix

REFERENCES

[1] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security [NIST Special Pubblication 800-82]," May 2015. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[2] T. Williams, "The Purdue Enterprise Reference Architecture (PERA)," *12th Triennal Wold Congress of the International Federation of Automatic control ,* 1993.

[3] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. P. Pennington and C. B. Thomas, "MITRE ATT&CK®: Design and Philosophy [White Paper]," The MITRE Corporation, July 2018. [Online]. Available: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[4] R. M. Lee, M. J. Assante and T. Conway, "TLP:White Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case," E-ISAC, SANS, 18 March 2016. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf.

[5] J. Styczynski and N. Beach-Westmoreland, "When the lights went out - A comprehensive review of the 2015 attacks on Ucranian critical infrastructure," Booz Allen Hamilton Inc., November 2016. [Online]. Available: http://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf.

[6] O. Alexander, M. Belisle and J. Steele, "MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy [White Paper]," The MITRE Corporation, March 2020. [Online]. Available: https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT%26CK_for_ICS_-_Philosophy_Paper.pdf.

[7] B. E. Strom, J. A. Battaglia, M. S. Kemmerer, W. Kupersanin, D. P. Miller, C. Wampler, S. M. Whitley and R. D. Wolf, "Finding Cyber Threats with ATT&CK™-Based Analytics [Technical Report]," The MITRE Corporation, June 2017. [Online].