A Study on the Application of MITRE ATT&CK Framework to Nuclear Field

Taejin Kim [a*], JunYoung Son [a], Young-Jun Lee [a], In Jung Yoon [b]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea*
[b]*CINAMON, 86, Tongil-ro, Jung-gu, Seoul, Republic of Korea*

Keywords : MITRE ATT&CK, industrial control system, cyberattack, cyber threat

1. Introduction

With advances in cyber threats, there have been several cyberattacks in the nuclear field, such as stuxnet attack on the nuclear facility in Iran [1], information leak in the nuclear power plant in Japan [2], cyber terrorism to Korea Hydro & Nuclear Power (KHNP) in South Korea [3], etc. However, frequent cases arise where cyberattacks are not effectively countered due to a lack of information about attacker's tactics and techniques.

In order to ensure the visibility of cybersecurity for industrial control systems (ICSs), systematic analysis is essential to cope with cyberattacks by utilizing a security threat knowledge database. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a repository of up-to-date attack technique information used by attackers, visualizing the relationship between an attacker's tactics and techniques through the observation of real attack cases [4]. Furthermore, MITRE ATT&CK for ICS has been introduced for enabling analysis of tactics and techniques from the perspective of control systems. In this paper, the concept and characteristics of MITRE ATT&CK for ICS are explained. Additionally, an analysis of incidents which related to the nuclear fields is conducted using MITRE ATT&CK for ICS.

2. MITRE ATT&CK for ICS

MITRE ATT&CK provides information about tactics and techniques specialized for each industry, including Enterprise, Mobile, and ICS. In this section, an investigation of MITRE ATT&CK for ICS was conducted to align with the characteristics of the nuclear industry.

2.1 Tactics and Techniques

Tactics mean the actions taken by attackers based on their attack objectives. There are a total of 12 tactics for ICS, and the 12 tactics and its meaning are represented in Table I [4]. Techniques illustrate the methods attackers use to achieve these tactics. There are a total of 81 techniques for ICS, including Activate Firmware Update Mode, Automated Collection, and more, and they are categorized for each respective tactic.

Table I: ICS Tactics for MITRE ATT&CK [4]

Tactics	Meaning
Initial Access	The adversary is trying to get into your ICS environment.
Execution	The adversary is trying to run code or manipulate system functions, parameters, and data in an unauthorized way.
Persistence	The adversary is trying to maintain their foothold in your ICS environment.
Privilege Escalation	The adversary is trying to gain higher-level permissions.
Evasion	The adversary is trying to avoid security defenses.
Discovery	The adversary is locating information to assess and identify their targets in your environment.
Lateral Movement	The adversary is trying to move through your ICS environment.
Collection	The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.
Command and Control	The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.
Inhibit Response Function	The adversary is trying to prevent your safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
Impair Process Control	The adversary is trying to manipulate, disable, or damage physical control processes.
Impact	The adversary is trying to manipulate, interrupt, or destroy your ICS systems, data, and their surrounding environment.

2.2 Data Sources

Data Sources refer to various entities that can be collected from sensors and logs [4]. For Data Sources of ICS, we have identified 17 types as follows: a) Application Log, b) Asset, c) Command, d) Drive, e) File, f) Firmware, g) Logon Session, h) Module, i) Network Share, j) Network Traffic, k) Operational

Databases, l) Process, m) Scheduled Job, n) Script, o) Service, p) User Account, q) Windows Registry [4].

2.3 Mitigations

Mitigations provide techniques to prevent cyberattacks carried out by attackers. A total of 52 mitigations for ICS have been identified, including Access Management, Account Use Policies, Antivirus/Antimalware, and more [4].

2.4 Groups and Software

Groups list identified hacking groups and categorize their attack techniques [4]. Therefore, based on this information, when a hacking group is identified during a cyberattack, it can be utilized for cyberattack response. Additionally, after a cyberattack, it is possible to speculate about which hacking group might be responsible based on the tactics and techniques used during the attack.

Software categorizes tools available for defenders and malware used by attackers [4]. The techniques employed by each malware such as Stuxnet, Dtrack, etc. have been documented, and this information can be used for cyberattack response based on the techniques employed during cyberattacks.

3. Application of MITRE ATT&CK

In this section, MITRE ATT&CK for ICS are utilized to analyze tactics and techniques in perspective of the software which is Stuxnet and in perspective of the group which is Lazarus Group.

3.1 Stuxnet attack on Nuclear Facility in Iran

In June 2010, there was an incident involving the destruction of centrifuges at Iran's uranium enrichment facility due to the Stuxnet attack. Stuxnet was a malicious code designed to target large-scale industrial facilities operating in closed networks, causing malfunctions in the control systems and resulting in severe damage. The attack process of Stuxnet can be summarized as follows [5]: a) Propagation of Stuxnet to the Main PC controlling the PLC via USB, b) Transmission of infected system information from the Main PC to the Command & Control (C&C) server, c) Attack on other systems within the internal network for malware distribution, d) Sharing of attack commands between the infected Main PC and additionally compromised internal systems, e) Generation of malicious code by the attacker and transmission to the C&C server, f) Manipulation of PLC control commands using the malicious code, g) Occurrence of PLC control failures.

With knowledge of the malware information, MITRE ATT&CK for ICS allows for the identification of tactics and techniques utilized for the specific attack and enables a swift response. As an example, tactics and techniques, analyzed by MITRE ATT&CK for ICS, are illustrated in Table II when there is a Stuxnet attack [6].

Table II: Stuxnet analyzed by MITRE ATT&CK [6]

Tactics	**Techniques**
Initial Access	Exploitation of Remote Services, Remote Services, Replication Through Removable Media
Execution	Command-Line Interface, Hooking, Modify Controller Tasking, Native API, User Execution
Persistence	Hardcoded Credentials, Modify Program, Project File Infection
Privilege Escalation	Hooking
Evasion	Masquerading, Rootkit
Discovery	Network Sniffing, Remote System Information Discovery
Lateral Movement	Exploitation of Remote Services, Hardcoded Credentials, Lateral Tool Transfer, Program Download, Remote Services
Collection	I/O Image, Monitor Process State
Command and Control	Commonly Used Port, Standard Application Layer Protocol
Inhibit Response Function	Manipulate I/O Image, Rootkit
Impair Process Control	Modify Parameter
Impact	Manipulation of Control, Manipulation of View

3.2 ICS attack by Lazarus Group

The Lazarus Group is a cybercrime organization operated by the North Korean government [7]. In the nuclear field, in September 2019, the Lazarus Group attacked India's Kudankulam Nuclear Power Plant using spyware called Dtrack, but this attack, occurred in the Enterprise Domain, only infects administrative PCs of the nuclear power plant but not infiltrating the ICS [8]. Utilizing MITRE ATT&CK for Enterprise allows for the identification of tactics and techniques used by the Lazarus Group [9], and it makes attack analysis highly convenient.

Looking into cases where the Lazarus Group targeted the ICS domain, there is an instance where they were associated with a gang named Covellite, and the Lazarus Group spear-phished a U.S. electric grid company [10]. Based on the event, only one technique which is Spear-phishing in the target category of Initial Access is existed in the matrix of the Lazarus Group within MITRE ATT&CK for ICS [11].

4. Conclusion

As cyberattacks become more sophisticated, it is crucial to establish strategies for effectively countering cyber threats in the nuclear field. This paper examines MITRE ATT&CK, which provides a systematic security threat knowledge database for industrial control systems. Furthermore, it analyzes tactics and techniques in perspective of the software which is Stuxnet and in perspective of the group which is Lazarus Group. By leveraging MITRE ATT&CK, when armed with knowledge of the attacking group or malware, it becomes possible to enable effective response by identifying the tactics and techniques employed based on past incidents.

ACKNOWLEDGEMENTS

This work was supported by a grant from the Ministry of Trade, Industry and Energy in Korea (No. 20224B10100140) and the Nuclear Research & Development Program of the National Research Foundation of Korea, funded by the Korean government, Ministry of Science and ICT (grant number 2020M2D5A1078133)

REFERENCES

[1] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[2] https://securityaffairs.com/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html
[3] https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack
[4] https://attack.mitre.org/
[5] https://www.ahnlab.com/kr/site/securityinfo/secunews/%20secuNewsView.do?menu%20dist=2&seq=%2016852
[6] https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0603%2FS0603-ics-layer.json
[7] https://en.wikipedia.org/wiki/Lazarus_Group
[8] Threat landscape for industrial automation systems, Kaspersky ICS CERT, H2 2019
[9] https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org% 2Fgroups%2FG0032%2FG0032-enterprise-layer.json
[10] https://www.securityweek.com/five-threat-groups-target-industrial-systems-dragos/
[11] https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0032 %2FG0032-ics-layer.json