A Diamond Model Approach to Analyzing GhostSec's Intrusion Paths

Cheng-Ying He
M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Nai-Yu Chen
M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

Jung-Shian Li
Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

I-Hsien Liu
Department of Electrical Engineering, National Cheng Kung University
No.1, University Rd., East Dist., Tainan City 701401, Taiwan

*E- mail: cyhe@cans.ee.ncku.edu.tw, nychen@ cans.ee.ncku.edu.tw, jsli@cans.ee.ncku.edu.tw, ihliu@cans.ee.ncku.edu.tw**

Abstract

The convergence of Operational Technology (OT) and Information Technology (IT) has heightened risks for critical infrastructure (CI) and industrial control systems (ICS), leading to a surge in diverse and sophisticated OT attacks with severe consequences. Thus, this study combines the Diamond Model with the Cyber Kill Chain to analyze potential attack paths and methods in the GhostSec case, where attackers compromised a Berghof PLC to demonstrate their access capabilities. Understanding these attack paths offers valuable insights into adversary strategies, aiding in the development of defense measures to prevent similar attacks.

Keywords: Industrial Control Systems, Diamond Model, ICS Cyber Kill Chain, Cyber threat intelligence

1. Introduction

The convergence of Operational Technology (OT) and Information Technology (IT) has significantly reshaped the security landscape of critical infrastructure (CI) and industrial control systems (ICS). While traditionally isolated ICS systems were not designed with robust security measures, increasing internet connectivity has exposed them to vulnerabilities [1] [2]. Tools like Shodan further exacerbate these risks by identifying internet-facing ICS devices, creating opportunities for remote exploitation [3].

The increasing frequency and sophistication of OT-targeted attacks underscore the urgent need for tailored cybersecurity measures [4]. For example, during the 2021 Oldsmar water treatment attack [5], attackers attempted to alter the water's chemical levels to hazardous concentrations. Similarly, in the 2023 Pennsylvania booster station attack, the attacker targeted Israeli-made Unitronics V570 PLCs. Following the incident, Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory highlighting vulnerabilities that allowed attackers to exploit default administrative passwords and gain control [6]. These incidents underline the evolving capabilities of adversaries and the critical need for proactive defense strategies. This study leverages the Diamond Model [7], enhanced with the Activity Thread Graph, to analyze adversary behaviors in the GhostSec case. Here, attackers compromised a Berghof Programmable Logic Controller (PLC) to demonstrate OT vulnerabilities [8]. By mapping attack paths and tactics, this research emphasizes adversary Tactics, Techniques, and Procedures (TTPs), offering actionable insights through Cyber Threat Intelligence (CTI), enabling the development of proactive defense strategies to enhance the resilience of critical infrastructure. The primary contributions of this work are:

- Application of the Diamond Model and Activity Thread Graph to systematically analyze adversary behaviors and attack sequences in OT environments;
- A detailed analysis of the GhostSec case, focusing on adversary strategies and attack vectors;
- Practical recommendations for enhancing cybersecurity in critical infrastructure environments.

2. Methodology

2.1. Diamond Model

The Diamond Model [7], shown in Fig. 1, is a cyber threat analysis framework with four core elements: Adversary, Capability, Infrastructure, and Victim. These elements form a diamond-shaped structure emphasizing

their interdependencies. Additionally, the model includes optional meta-features for deeper analysis. In this study, the Diamond Model is used to pinpoint adversary objectives, identify tactics, track behaviors, and uncover defensive opportunities.

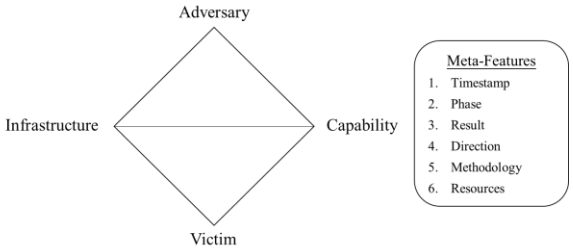

Fig. 1. Diamond Model

2.2. Cyber Kill Chain

The Cyber Kill Chain [9], shown in Fig. 2 and developed by Lockheed Martin, outlines seven stages of a cyber attack: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives. Each stage represents a critical step in the attacker's workflow. This study applies the Cyber Kill Chain to classify actions, map Diamond Model events, and identify intervention points, enabling proactive defense measures.

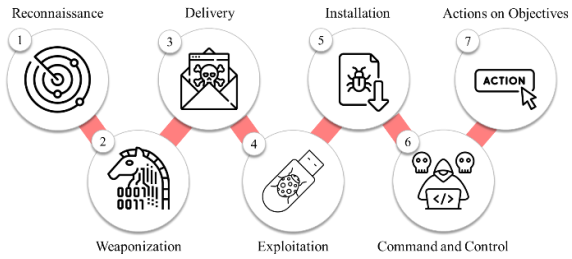

Fig. 2. Cyber Kill Chain.

2.3. Activity Thread Graph

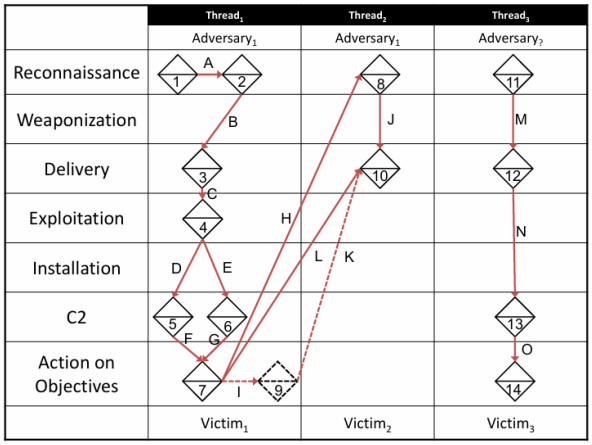

Fig. 3. An example visualization of Activity Thread Graph.

The Activity Thread Graph, detailed in Section 8 of [7] and shown in Fig. 3, provides a timeline-based visualization of attack sequences by connecting events into a coherent flow. In Fig. 4, diamonds denote events, while arcs indicate causal relationships. This study utilizes the Activity Thread Graph to reconstruct and analyze attack paths, offering a clearer understanding of the sequence and structure of adversary activities.

1	The solid line diamond defines the actual event.
2	The dotted line diamond defines the hypothesis event.
A	The solid line arc defines the causal relationship between the event is the actual attack paths.
B	The dotted line arc defines the causal relationship between the event is the hypothesis possible attack paths.
1	The number inside the diamond defines the ID of the event.
A	The number below the arc defines the ID of the causal relationship between the event.

Fig. 4. Definition of the Activity Thread Graph.

3. Case Analysis

3.1. Case description

On September 4, 2022, the hacker group GhostSec claimed responsibility for hacking 55 Berghof Programmable Logic Controllers (PLCs) made in Israel, showcasing their ability to control PLC management interfaces. The group released videos and screenshots of logged-in PLC interfaces as evidence of unauthorized access [8]. Motivated by anti-Israel sentiment, GhostSec targeted PLCs manufactured in Israel. They exploited internet-exposed PLCs, leveraging weak passwords to gain access and possibly undisclosed vulnerabilities for further control. The attack highlighted the critical risks of poor cybersecurity hygiene in industrial systems and the need for stronger access controls and regular security assessments. Such incidents expose vulnerabilities in critical infrastructure, raising concerns about broader implications for national security.

3.2. Activity Thread Graph of Diamond model

As shown in Fig. 5, the Activity Thread Graph depicts two distinct threads representing the GhostSec attack on Berghof PLCs. The events are mapped in Table 1, with their corresponding causal relationships illustrated in Table 2, and the adversary-victim pair of each thread detailed in Fig. 6. In Thread 1, Events 01–05 describe how the attacker leveraged OSINT, Shodan scanning, and weak password exploitation to gain access to the target PLC. Events 06–08 highlight the installation of persistence mechanisms and the establishment of a

Command & Control (C2) channel. Finally, Events 09–11 reveal the attack's objectives, including data exfiltration, public disclosure, and complete operational control of the PLC. Thread 2 focuses on lateral movement and further exploitation. Events 12–13 detail reconnaissance efforts to identify other devices in the network, while Events 14–15 illustrate the attacker gaining administrative privileges through default credentials. Events 16–17 conclude with the disruption of industrial processes and potential data manipulation. This analysis demonstrates the multi-staged, coordinated attack strategy and emphasizes the need for proactive defenses to secure critical infrastructure systems against similar threats.

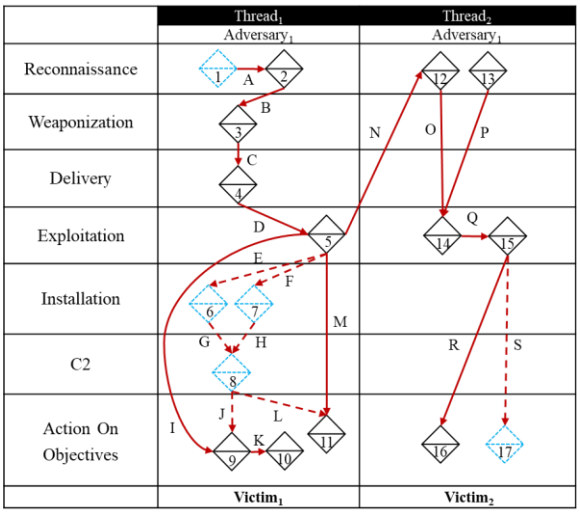

Fig. 5. Diamond model activity thread graph.

Table 1. Activity thread event descriptions for Figure 5.

Event	Hypothesis/Actual	Description
01	Hypothesis	Gather public information on the target using OSINT.
02	Actual	Use Shodan to scan internet-exposed Berghof PLCs.
03	Actual	Create scripts to guess default or weak passwords for target PLCs.
04	Actual	Execute scripts to attempt login on the target PLC.
05	Actual	Successfully log in to the PLC interface, accessing system status, settings, and logs.
06	Hypothesis	Install a backdoor for persistent access to the PLC.
07	Hypothesis	Modify PLC configurations to maintain access.
08	Hypothesis	Establish a Command and Control (C2) channel for continuous device control.
09	Actual	Export HMI screenshots and sensitive system data from the PLC.
10	Actual	Publicly share exported screenshots and backup files on social media.
11	Actual	Halt operations, download system files, reset settings, and delete applications via the PLC interface.
12	Actual	Use exported data to identify IP addresses of other devices.
13	Actual	Scan network for additional devices and gather IP information.
14	Actual	Attempt unauthorized logins using default passwords.
15	Actual	Gain admin access to other PLCs using default credentials.
16	Actual	Control PLCs via the interface, disrupting industrial processes or causing faults.
17	Hypothesis	Modify HMI data display via Modbus commands.

Table 2. Activity thread arc descriptions for Figure5

Arc	Confidence	And / Or	Hypothesis / Actual
A	High	And	Actual
B	High	And	Actual
C	High	And	Actual
D	High	And	Actual
E	Low	Or	Hypothesis
F	Low	Or	Hypothesis
G	Low	And	Hypothesis
H	Low	And	Hypothesis
I	High	Or	Actual
J	Low	Or	Hypothesis
K	High	And	Actual
L	Low	Or	Hypothesis
M	High	Or	Actual
N	Medium	And	Actual
O	High	And	Actual
P	High	And	Actual
Q	High	And	Actual
R	High	Or	Actual
S	Low	Or	Hypothesis

Thread1
Adversary1: Iran, GhostSec Victim1: • Partner Communications Company Ltd. • Berghof PLC DC2004W Q TS 0.8S 1131NTL – 270010700 • Firmware Version:1.21.0 • Codesys RTS version: 3.5.13.30 • IP:192.168.1.3 • Mac:00:E0:BA:95:50:1E
Thread2
Adversary2: Iran, GhostSec Victim2: • Partner Communications Company Ltd. • Others PLC

Fig. 6. Adversary-Victim pair of each thread

4. Conclusion

This study highlights the vulnerabilities of industrial control systems exposed to cyber threats, demonstrated by the GhostSec attack on Berghof PLCs. Applying the Diamond Model and Activity Thread Graph provided valuable insights into adversary tactics and attack sequences, emphasizing the need for proactive defense strategies. To enhance the cybersecurity of critical infrastructure, this research suggests the following recommendations:

- Strengthening Access Controls: Enforcing multi-factor authentication, updating default credentials, and applying strong password policies.
- Network Security Management: Disconnect PLCs from the open internet. If remote access is needed, enforce VPNs, firewalls, and secure remote protocols to limit exposure and lateral movement.
- Continuous Monitoring and Threat Intelligence: Deploying advanced threat detection systems and leveraging Cyber Threat Intelligence (CTI) to identify and respond to emerging threats in real time.

Acknowledgment

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 113-2634-F-006-001-MBK, and by the Water Resources Agency (WRA) under the Ministry of Economic Affairs (MOEA) in Taiwan under contract number MOEAWRA1130243.

References

1. Yassine Mekdad, Giuseppe Bernieri, Mauro Conti, Abdeslam El Fergougui, “A threat model method for ICS malware: the TRISIS case,” the 18th ACM International Conference on Computing Frontiers, Virtual, Italy, 11-13 May, 2021.
2. M. Cook, A. Marnerides, C. Johnson and D. Pezaros, “A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions,” IEEE Communications Surveys & Tutorials, vol. 25, no. 3, pp. 1705-1747, 2023.
3. Shodan, “Unitronics Search Query,” [Online]. Available: https://www.shodan.io/search?query=unitronics.
4. R. Davis, O. F. Keskin, “Cyber Threat Modeling for Water and Wastewater Systems: Contextualizing STRIDE and DREAD with the Current Cyber Threat Landscape,” in 2024 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, USA, 3 May, 2024.
5. I-H. Liu, J.-S. Chen, K.-M. Su, J.-S. Li, “Dam Control System’s Cybersecurity Testbed”, IIH-MSP 2022, Kitakyushu, Japan, Dec. 16-18, 2022.
6. CISA, “IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities,” 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf
7. S. Caltagirone, A. Pendergast, C. Betz, “The Diamond Model of Intrusion Analysis,” Defense Technical Information Center, 2013.
8. Otorio, “Pro-Palestinian Hacking Group Compromises Berghof PLCs in Israel,” Jul 2024. [Online]. Available: https://www.otorio.com/blog/pro-palestinian-hacking-group-compromises-berghof-plcs-in-israel/.
9. Hutchins, Eric M.; Cloppert, Michael J.; Amin, Rohan M., “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Lockheed Martin Corporation, 2011.

Authors Introduction

Ms. Cheng-Ying He

He is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. He received his B.B.A. degree from the Bachelor of Information Management, National Taiwan University of Science and Technology, Taiwan in 2022. His interests include ICS Security, Cyber Threat Analysis and Intrusion Detection.

Ms. Nai-Yu Chen

She is a postgraduate of M.S. Degree Program on Cyber-Security Intelligence, National Cheng Kung University in Taiwan. She received her B.B.A. degree from the Bachelor of BioBusiness Management, National Chiayi University, Taiwan in 2021. Her interests include ICS Security and Network-Based Intrusion Detection.

Dr. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests include Cyber-Security, OT Security, and Wired & Wireless Communication. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.