CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

ORCA – Online Research @ Cardiff

This is an Open Access document downloaded from ORCA, Cardiff University's institutional repository:https://orca.cardiff.ac.uk/id/eprint/177987/

This is the author's version of a work that was submitted to / accepted for publication.

Citation for final published version:

Kurt, Fatih, Saxena, Neetesh , Kumar, Vijay and Theodorakopoulos, george 2025. POSTER: Automating ICS Malware Analysis with MITRE ATT&CK. Presented at: ACM AsiaCCS, Hanoi, Vietnam, 25-29 August 2025.

Publishers page:

Please note:
Changes made as a result of publishing processes such as copy-editing, formatting and page numbers may not be reflected in this version. For the definitive version of this publication, please refer to the published source. You are advised to consult the publisher's version if you wish to cite this paper.

This version is being made available in accordance with publisher policies. See http://orca.cf.ac.uk/policies.html for usage policies. Copyright and moral rights for publications made available in ORCA are retained by the copyright holders.

POSTER: Automating ICS Malware Analysis with MITRE ATT&CK

Fatih Kurt, Neetesh Saxena, Vijay Kumar, and George Theodorakopoulos*
School of Computer Science and Informatics, Cardiff University
Cardiff, United Kingdom

Abstract

The increasing interconnections and rapid changes in the nature of cyber threats targeting the Industrial Control Systems (ICS), it is crucial to understand how the malware patterns and behavior have evolved over the years. Gaining the understanding allows us to assess the effectiveness of current detection and defense mechanisms. Insights from this work will help feeding to build effective defenses to counter such sophisticated behavior. Traditional threat analysis methods rely on text heavy representations, making it difficult to identify attack trends efficiently. This work improves the usability of the MITRE ATT&CK framework by automating the extraction, comparison, and visualization of malware attack techniques. By analyzing five ICS targeting malware families BlackEnergy, Industroyer, Industroyer2, Pipedream, and Triton, our developed tool identifies recurring adversary tactics and provides structured heatmaps and network graphs for improved threat intelligence. This approach enables analysts to compare malware behaviors more effectively, prioritize security strategies, and strengthen ICS cybersecurity resilience.

Keywords

ICS, Malware Analysis, MITRE ATT&CK, Automated Threat Correlation, Attack Mapping

ACM Reference Format:

Fatih Kurt, Neetesh Saxena, Vijay Kumar, and George Theodorakopoulos. 2018. POSTER: Automating ICS Malware Analysis with MITRE ATT&CK. In *Proceedings of August 25–29, 2025 (Conference acronym 'ACM ASIACCS).* ACM, New York, NY, USA, 3 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

Managing critical infrastructure, such as power grids, water treatment facilities, and manufacturing plants, is paramount in the era of cyber warfare and international conflicts. This is clearly evident in Russia-Ukraine conflict [7]. Due to growing demands for real-time data access, cost efficiency, and IT/OT convergence, ICS networks are now increasingly interconnected with corporate IT environments. While the integration enhances automation and operational decision making, it also expands attack surface, exposing industrial systems to sophisticated cyber threats. In recent years, ICS focused malware has been a major driver of cyber-attacks against industrial environments [3]. The growing complexity and adaptability of these threats highlight the importance of understanding adversary tactics to strengthen ICS cybersecurity.

1.1 Motivation

Understanding ICS malware behavior is crucial for enhancing existing defense mechanisms and developing effective security strategies. Classifying attacker's Tactics, Techniques, and Procedures (TTPs) is an essential step in improving cyber threat intelligence and detection systems. Previous studies demonstrate that structured threat frameworks improve detection accuracy and feature selection for anomaly-based security models as shown in [2]. Furthermore, the traditional intrusion detection system are not effective against APT-based attacks [1], leaving the current security defenses ineffective. Pirca et al. [6] indicates that both experts and non experts find MITRE ATT&CK challenging to navigate due to its text heavy format, lack of visualization, and the manual effort required to analyze multi domain threats. The MITRE ATT&CK Navigator is a web-based tool for interacting with and exploring ATT&CK matrices. Despite its structured nature, it has several limitations that hinder its practical application. Additionally, users must first select a domain (Enterprise or ICS) and create separate layers for both IT and OT environments. For malware analysis, a new layer is required for each sample, and another custom layer must be created for comparisons. This makes the process less efficient and requiring users to configure certain settings manually.

To address these challenges, this work focuses on automating the extraction, comparison, and visualization of ICS malware tactics and techniques using MITRE ATT&CK matrices. Currently, it analyzes five well-known ICS malware strains to identify commonalities and differences in their attack patterns. The goal is to improve threat intelligence and cybersecurity response by providing a more structured, automated, and visual approach to build effective cyber defenses against such malware families.

1.2 Contributions

The current work introduces a script-based approach and a tool to improve the identification of overlapping techniques for better detection. (i) The tool derives the most frequently used tactics and techniques across five ICS malware strains, and provide insights that allowing SOC analysts and security teams to prioritize common techniques instead of broadly scanning for anomalies. (ii) It further enhances automated threat correlation. MITRE ATT&CK Navigator requires manual effort to compare different malware campaigns. Our tool automates malware-to-malware correlation, reducing analyst workload and quickening threat analysis. (iii) Visualizing malware attack patterns is also addressed. The text heavy format of MITRE ATT&CK makes it difficult to identify trends. Our tool addresses this by providing heatmaps and network graphs that visually represent malware behaviors, enabling analysts to quickly detect common attack patterns and individual techniques across different threats.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
Conference acronym 'ACM ASIACCS,
© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/XXXXXXX.XXXXXXX

2 Related Work

Existing research on ICS cybersecurity has mainly focused on APT actors, individual malware analysis, or different frameworks including ICS Cyber Kill Chain.

Some studies analyzed APT groups rather than individual malware strains, such as Bahrami et al[1]. Similarly, [5] examines Trojan.Naid, Trojan.Hydraq, Stuxnet, Duqu, Shamoon, Mimikatz, WannaCry, and Gh0st RAT. However, while some including Stuxnet are ICS targeted malware, they are primarily cyber warfare tools rather than dedicated ICS malware. Other studies focused on single ICS malware strains, as in [4], which exclusively analyze TRISIS. While these works provide detailed insights into specific malware families, their scope is limited to individual cases rather than comparative analysis. Additionally, Mekdad et al[3] examined multiple ICS targeting malware using ICS Cyber Kill Chain as framework. However, they focused on older malware such as Stuxnet and Havex, overlooking recent threats. In contrast, our work prioritizes newer ICS focused malware including Industroyer2 and Pipedream.

Unlike these prior studies, our research introduces an automated, structured, and visualized approach to multi malware correlation using MITRE ATT&CK, allowing for better threat intelligence, cross malware comparisons, and security strategy development.

3 Methodology

The current work analyzes five ICS targeting malware families BlackEnergy, Industroyer, Industroyer2, Pipedream, and Triton—by mapping their TTPs using MITRE framework. We extract malware techniques directly from MITRE ATT&CK's software catalog, ensuring accuracy in mapping each malware's attacking methods. Since the MITRE ATT&CK separates ICS and Enterprise techniques, we analyze these domains independently, generating two separate heatmaps. This approach prevents the loss of domain specific insights while still allowing a comparative analysis. In addition to heatmaps, we generate network graphs that illustrate which techniques are shared across multiple malware families. A structured approach helps identify common attack trends and outlying behaviors, providing useful insights for future security monitoring.

Our findings provide actionable insights for improving anomaly detection systems. By identifying which techniques are frequently used across malware strains, security teams and ML-based detection models can: (i) prioritize high risk techniques when training models, and (ii) develop targeted anomaly detection rules based on real-world adversary behaviors. It improves defensive strategies by focusing on techniques with high occurrence rates across all considered attacks.

Our methodology improves upon MITRE ATT&CK Navigator, which requires manual correlation and lacks visual analytics by automating the extraction, comparison, and visualization of attack techniques. This structured mapping can be adapted into SIEM systems and ML-based security tools, strengthening proactive cyber defense mechanisms.

4 Results and Discussion

Our analysis highlights recurring tactics and techniques across ICS focused malwares. By analyzing BlackEnergy, Industroyer, Industroyer2, Pipedream, and Triton, we identified patterns in how malware families operate, which can help improve detection, prioritize defenses, and support ML-based security solutions. Table 1, presents the top three most frequently observed tactics for each malware family and it highlights key trends. Beyond what is listed in the table, in the ICS ATT&CK domain, Discovery, Collection, and Command & Control (C2) were the most frequently observed tactics, appearing in four, out of five malware families. Execution, Persistence, Inhibit Response Function, and Impact Process Control were each used in at least three malware families, showing that adversaries rely on reconnaissance and remote control before launching disruptive actions.

Table 1: Top 3 Enterprise and ICS Tactics by Malware

Malware	Top 3 Enterprise	Top 3 ICS
BlackEnergy	Discovery (7), Credential Access (3), Persistence (3)	Initial Access (1), Persistence (1), C2 (1)
Industroyer	Discovery (6), C2 (4), Impact (3)	Inhibit RF (8), Impact (7), Discovery (3)
Industroyer2	Discovery (1)	Impair PC (3), Collection (2), Discovery (1)
Pipedream	None	Discovery (3), Collection (2), C2 (2)
Triton	None	Execution (6), Evasion (3), C2 (2)

For the Enterprise ATT&CK domain, Discovery was present in every malware leveraging Enterprise techniques, confirming its role as a critical first step before transitioning into ICS attacks. This was followed by Persistence, Defense Evasion, C2, and Impact, demonstrating that adversaries establish a foothold in IT environments before targeting ICS. The heatmaps in Figure 1 and Figure 2 show the tactics that each malware family used. The number in each box indicates how many techniques were used under that tactic.

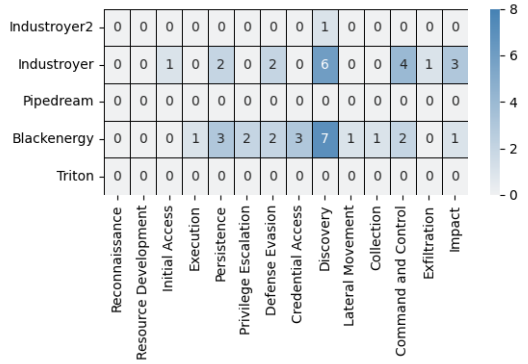

Figure 1: Enterprise ATT&CK Heatmap

A closer look at shared techniques across malware families reveals that attackers frequently use Remote System Discovery (T0888), Standard Application Layer Protocol (T0869), Unauthorized Command Message (T0855), and Remote System Information Discovery (T0846). These techniques provide adversaries with critical capabilities such as reconnaissance, lateral movement, and unauthorized control of ICS devices, making them high-priority for detection. Observed patterns reveal that all malware, except Industroyer2, share an average of 8 common tactics, indicating strong overlaps in attack methodologies. Figure 3 illustrates the

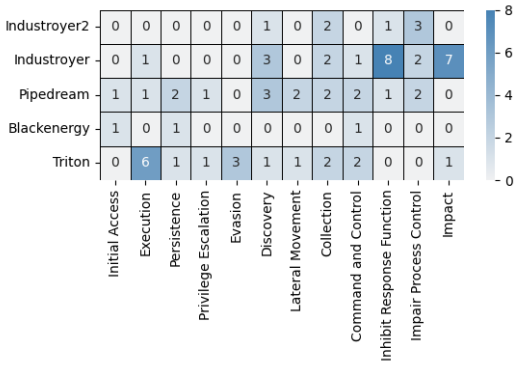

Figure 2: ICS ATT&CK Heatmap

relationship between malware families (red nodes) and the attack techniques they use. The technique nodes get darker (light gray → light blue → blue) as more malware share them. Smaller, light gray nodes represent techniques used by only one malware. Remote System Discovery (T0888) was used by Industroyer, Industroyer2, and Pipedream to map out ICS networks and identify connected devices before launching an attack. Since this technique allows adversaries to understand network topology and locate high value targets, security teams must prioritize monitoring for unauthorized scanning activities within ICS environments. Implementing network segmentation and restricting asset enumeration can limit an attacker's ability to gather intelligence before executing an attack.

Standard Application Layer Protocol (T0869) was commonly exploited in Triton, Pipedream, and BlackEnerg, where attackers abused legitimate ICS protocols like Modbus and DNP3 to maintain stealthy C2 operations. Since these protocols are widely used in industrial networks, traditional security tools struggle to differentiate between legitimate and malicious traffic. Defenders should implement anomaly detection on ICS protocol traffic and enforce strict communication baselines to identify and block suspicious protocol abuse. Unauthorized Command Message (T0855) was observed in Industroyer, Industroyer 2 and Pipedream, allowing attackers to send malicious commands directly to ICS devices. Since many ICS lack authentication mechanisms for commands, adversaries can exploit this weakness to override normal operations or cause physical damage. Security teams should enforce command whitelisting and

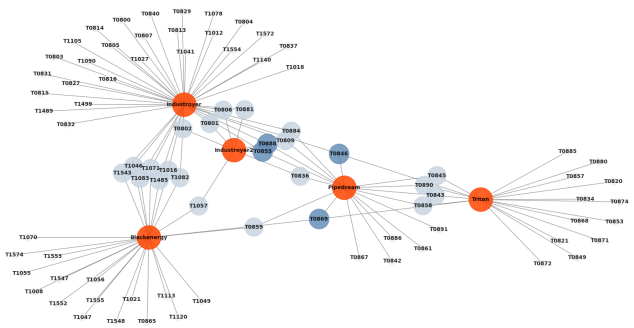

Figure 3: Network graph of malware families and their mapped techniques.

implement behavioral monitoring to detect and block unauthorized control messages. Remote System Information Discovery (T0846) was widely used in Industroyer, Triton and Pipedream, enabling attackers to collect system details such as software configurations, running processes, and network settings. The reconnaissance phase helps adversaries customize their attack for maximum impact. Defenders should monitor system information requests and flag unexpected queries from unauthorized sources, as this may indicate an early stage attack.

By visualizing these attack strategies through heatmaps and network graphs we automated the process of correlating attack techniques, reducing manual efforts for analysts. A structured approach allows security teams to focus on the most exploited techniques and prioritize defenses; in this way, our tool can help integrate new malware samples and enhance overall ICS security.

5 Conclusion and Future Works

Our work enhances the usability of MITRE ATT&CK by making malware analysis more structured, visual, and efficient. Instead of relying solely on text-based analysis, we use visualization techniques like heatmaps and network graphs to help analysts quickly recognize attack patterns and connections between malware families. Additionally, our tool automates the mapping of malware techniques, eliminating the need for manual sorting between the Enterprise and ICS domains, ensuring that software is categorized based on tactics first and then techniques rather than predefined domains which saves time and makes threat analysis more accessible and actionable.

Currently our system utilizes MITRE's software catalog as its database source. In future work, we plan to extend its functionality by incorporating dynamic malware execution platforms like any.run. This integration will enable users to analyze unknown malware samples in real-time and automatically extract associated attack techniques. By leveraging an API-driven approach, the tool will process live malware behaviors, correlate them with known ICS threats, and generate automated reports. Our advancement will create a more adaptive and efficient system for identifying emerging malware threats and enhancing cybersecurity defenses.

References

[1] Pooneh Nikkhah Bahrami, Ali Dehghantanha, Tooska Dargahi, Reza M. Parizi, Kim-Kwang Raymond Choo, and Hamid H. S. Javadi. 2019. Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures. *Journal of Information Processing Systems* 15, 4 (2019), 865–889.

[2] Woohyun Choi, Suman Pandey, and Jongwon Kim. 2024. Detecting Cybersecurity Threats for Industrial Control Systems Using Machine Learning. *IEEE Access* 12 (2024), 153550–153563.

[3] Yassine Mekdad, Giuseppe Bernieri, Mauro Conti, and Abdeslam El Fergougui. 2022. The Rise of ICS Malware: A Comparative Analysis. In *ESORICS International Workshops Computer Security*. Springer International Publishing, 496–511.

[4] Yassine Mekdad, Giuseppe Bernieri, Mauro Conti, and Abdeslam El Fergougui. 2021. A threat model method for ICS malware: the TRISIS case. In *Proceedings of the 18th ACM International Conference on Computing Frontiers* (Virtual Event, Italy). 221–228.

[5] Seongmin Park, Myeongsu Lee, Sarang Na, and Joonhyung Lim. 2024. Destructive Malwares on MITRE ATT&CK Tactics for Cyber Warfare: A Brief Survey and Analysis. In *Mobile Internet Security*. 260–270.

[6] Ana Maria Pirca and Harjinder Singh Lallie. 2023. An empirical evaluation of the effectiveness of attack graphs and MITRE ATTCK matrices in aiding cyber attack perception amongst decision-makers. *Computers Security* 130 (2023), 103254.

[7] RFE/RL's Ukrainian Service and RFE/RL's Russian Service. [n. d.]. Ukraine, Russia Target Energy Facilities With Drones, Missiles. https://www.rferl.org/a/ukraine-strikes-energy-infrastructure/33000408.html. 2025-06-20.