Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.
Digital Object Identifier XX.XXXX/YYY.20XX.ZZZZZZZ

Enhancing Industrial Cyber security: Insights from Analyzing Threat Groups and Strategies in Operational Technology Environments

MUKUND BHOLE[1], WOLFGANG KASTNER[2] (Senior Member, IEEE) and THILO SAUTER[3] (Fellow, IEEE)
[1]TU Wien, Vienna, Austria (e-mail: mukund.bhole@tuwien.ac.at)
[2]TU Wien, Vienna, Austria (e-mail: wolfgang.kastner@tuwien.ac.at)
[3]TU Wien, Vienna, Austria (e-mail: thilo.sauter@tuwien.ac.at)

Corresponding author: MUKUND BHOLE (e-mail: mukund.bhole@tuwien.ac.at)

This work was supported by TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry, a research cooperation between TU Wien and TÜV AUSTRIA.

ABSTRACT In recent years, IT concepts and components have made their way into the shop floor, today better known as Operational Technology (OT). The increasing interconnection and convergence of IT and OT have exposed industrial infrastructures to cyber attacks. In addition, they have become vulnerable to Advanced Persistent Threats (APTs). This article examines real-world incidents, looking at the complex landscape of threat groups targeting OT environments and the Tactic, Technique, and Procedures (TTPs) employed by these threat groups. Consequently, it highlights the need for heightened vigilance in protecting OT environments, which can be done by leveraging a variety of open-source threat intelligence platforms and databases, including ThaiCERT, Malpedia, MITRE ATT&CK, and ICS-CERT. We aim to furnish stakeholders, including Chief Information Security Officers (CISOs), with insights into emerging threat groups, attack victims and their locations, the origins of attacks, the tools and types of tools used, and the motivations behind these attacks. This understanding is crucial for enhancing defensive strategies and safeguarding OT environments against evolving cyber threats.

INDEX TERMS Operational Technology, Security, Threat Group Analysis

I. INTRODUCTION

Operational Technology (OT) environments encompass complex systems and technologies meticulously designed to oversee and regulate physical processes across diverse industrial sectors. Unlike its counterpart, Information Technology (IT), which centers around data manipulation and communication on an enterprise level, OT is dedicated explicitly to automating and monitoring industrial machinery, processes, and equipment. OT has emerged as the cornerstone of modern industrial advancement in manufacturing, energy, oil and gas, industrial, petrochemical, and critical infrastructure domains.

In an era marked by the swift convergence of IT and OT, blending digital technologies with industrial infrastructure, the security of OT environments has emerged as a significant concern [1]. Security on the field level of the automation pyramid is not a completely new topic and has been looked at for more than two decades [2]. However, the rapid spread of IT concepts and components in the OT domain and the resulting tight interconnection resulting from this convergence have severely aggravated the problem. It has made OT increasingly vulnerable to threats that we used to know only from the IT world. Consequently, this has enabled and emboldened cyber adversaries to target and disrupt also OT systems. Among these adversaries are also threat groups such as *APT41* and *Dragonfly* that now have the possibility to pivot and infiltrate a wide range of industrial infrastructure, exploiting the blurred boundaries between IT and OT security.

State-sponsored threat groups or Advanced Persistent Threats (APTs) benefit from substantial resources and excel in stealthy infiltrations of OT infrastructures, targeting sectors crucial to national interests by developing specialized malware for OT environments [3], [4]. Collaboration among threat groups in underground forums amplifies attacks on OT environments, facilitating synchronized efforts [5]. Threat groups are also leveraging Artificial Intelligence (AI) and Machine Learning (ML) techniques to elevate attack sophistication, posing an escalating threat to OT security [6]–[8]. Furthermore, they are keen on merging cyber capabilities

with physical attacks on OT infrastructure, sparking concerns about destructive cyber-physical assaults [9], [10].

Several notable incidents underscore the potentially catastrophic outcomes of cyber attacks on OT environments:

- The BlackEnergy malware was used in several high-profile attacks on OT environments by threat group Sandworm, including the 2015 cyber attack on the Ukrainian power grid. BlackEnergy is a modular malware that can steal data, disrupt operations, and cause physical damage [11].
- The Industroyer malware was used in a cyber attack by the threat group Dragonfly on a Ukrainian electricity distribution company in 2016. Industroyer is sophisticated malware that can target both IT and OT systems, causing physical damage by disrupting the operation of critical infrastructures [12].
- The VPNFilter malware was discovered in 2018 and targets Virtual Private Network (VPN) devices that connect OT networks to the Internet used by the threat group Sofacy (APT28). VPNFilter can steal data, disrupt operations, and deny access to critical systems [13].
- The Triton malware was discovered in 2020 and is sophisticated malware used by the threat group TEMP.Veles targeting Industrial Control Systems (ICS), capable of causing physical damage by disrupting the essential operation of infrastructure [14].
- The EKANS ransomware, discovered in December 2019 and more prevalent in early 2020, targets explicitly ICS and OT networks used by the threat group Turla. It encrypts files crucial to industrial processes, such as files used in Supervisory Control and Data Acquisition (SCADA) systems, Human Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs), demanding ransom payments for decryption keys [15].
- The Colonial Pipeline ransomware attack, discovered in May 2021, targeted the major fuel pipeline operator in the US by the threat group Carbanak (Anunak). Using DarkSide ransomware, it encrypted crucial OT systems responsible for managing pipeline operations [16].
- The Pipedream malware was discovered in early 2022 and reported by Dragos to have been created by the Chernovite threat group. Although there have been no reported attacks using Pipedream, it explicitly targets ICS and OT components, including PLCs, SCADA systems, and the Codesys software platform used to program PLCs. Pipedream is capable of disrupting or manipulating industrial processes, stealing data, and causing physical damage [17].

A common denominator in all such attacks is that it starts with infiltration of IT systems before proceeding to the actual OT level. Defenders must, therefore, implement robust cybersecurity measures to mitigate these evolving threats. The particular challenge is that many OT environments heavily rely on legacy systems, often with unpatched vulnerabilities, which facilitates attacks [9]. Before creating a defense strategy, stakeholders should carefully study the Tactic, Technique, and Procedure TTPs used by the threat actors. This *modus operandi* of threat groups has been well studied in the IT domain [18]–[21]. However, little attention has been given so far to specific OT aspects.

This article aims to comprehensively analyze the complex landscape of APTs that have OT environments as their ultimate target. It explores different risk and vulnerability aspects while examining the TTPs used by the adversaries. The article is organized as follows: Section II provides related work on threat groups or APTs, Section III offers a comprehensive analysis of threat groups in OT environments, Section IV presents the phases of the ICS cyber-kill chain procedure followed by threat groups and their impact on OT environments, while Section V discusses the interpretation of statistical analysis of threat groups. Section VI provides strategies for defending against threat groups and malware. Finally, we offer some concluding remarks in Section VII.

II. RELATED WORK

APT or threat group attribution is a complex challenge requiring a holistic approach, combining definitions, characteristics, and attack execution across both IT and OT environments.

Hussain et al. [22] overview APTs and their communication mechanisms, detailing how compromised hosts interact with Command and Control (C2) servers for command issuance and data exfiltration via persistent malware. However, the study focuses on IT environment detection frameworks and omits OT environment attack methodologies and preventive measures. Manar et al. [23] studied potential solutions for detecting APT beaconing, emphasizing communication channel-based techniques to detect C2 malware and beaconing activities. However, defense requires a layered approach beyond identifying communication channels; the study does not identify specific sectors targeted by APTs or the layers of architecture affected. Alshamrani et al. [21] examined the APT lifecycle, scrutinizing existing detection tools for identifying different stages of APT attacks and exploring machine learning approaches to enhance threat detection systems. While the objective of their study aligns with ours, it neither addresses sector-specific issues in OT environments nor provides data-backed argumentation. Lemay et al. [18] surveyed open-source literature on APT actors and their activities up to 2017, emphasizing APT operations over defense or detection approaches. While this aligns with our goal of identifying research gaps in APTs, it neither cover sector-specific nor OT-specific threat groups.

Kotenko et al. [24], Huang et al. [25], and Muhammed et al. [26] examined cybercrime services and tools from a value chain perspective, identifying 24 key activities and their interrelations. While their analysis highlights the specialization and collaboration in cyber attacks, it neither addresses country-specific nor sector-specific attacks in OT environments. Bahrami et al. [19] provided a comprehensive overview of TTPs for APT, analyzing 22 APT groups

and their 40 attacks. Their study outlined seven phases of the cyber kill chain: reconnaissance, weaponization, delivery, exploitation, installation, C2, and Action on Objectives (AOO). However, their overview lacks OT-specific and sector-specific attacks, whereas our study analyzes 120 threat groups across the ICS/OT sector. Singh et al. [20] examine APT modeling and behavioral patterns, including various APT types and zero-day exploits. Their research focuses on clustering, learning, and extraction techniques. Models such as the Kill Chain [27], Attack Tree [21], Attack Pyramid [28], Attack Graph [29], Markov model [30], Network Evolution [31], Diamond Model [32], Q Model [33], and Enterprise Commercial Model [34] outline APT attack attribution. Although aligned with our goals, the study still lacks coverage of sector-specific ICS/OT attacks.

Sundaram et al. [35] proposed an active defense mechanism for OT that involves introducing noise into the OT network to detect unauthorized manipulations by APTs and insider threats. However, their study does not address how TTPs might evolve in response to the implemented defense mechanisms. Krasznay et al. [36] developed a framework for sharing information on the TTPs of threat actors targeting the OT/ICS environment in the energy sector, utilizing a honeypot. While their study provides valuable insights into threat intelligence, it lacks detailed information on specific TTPs and is limited to a single sector. Jadidi et al. [37] proposed a three-phase threat hunting framework for ICS/OT networks that integrates the Diamond Model [32] and MITRE ATT&CK. This framework aims to identify TTPs and visualize attack routes toward targets. However, it does not offer a comprehensive overview of the TTPs and APTs across the broader OT/ICS environment.

The novelty of our work, compared to the studies mentioned, lies in its focus on the OT environment. This area still has significant research gaps, particularly regarding the current landscape of APT/ threat groups exploiting OT systems. By investigating data-backed arguments on sector-specific analyses, emerging threat groups in OT environments, their TTPs, and identifying the countries responsible for or affected by these attacks, we aim to provide new directions for future research.

III. ANALYSIS OF THREAT GROUPS

There are several open-source threat intelligence platforms and databases that provide information about known threat groups, their activities, tactics, and techniques. Notable sources, with data available until June 2023, include Threat Group Cards by ThaiCERT [38], Malpedia by Fraunhofer FKIE [39], MITRE ATT&CK [40], and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [41]. The data sources used also periodically encompass reports published by various OT security service providers, for instance, Dragos, Darktrace, FireEye, Nozomi Networks, Claroty, Forescout, Kaspersky.

In datasheet [42], we gathered data from these notable sources and made the collected information publicly available, including news articles and threat reports, based on categories such as victim sector (targeted industries), threat actor group (responsible for the attack), number of publicly reported attacks until June 2023, year of threat group discovery, infrastructure target component (ISA-95 model level targeted by attackers), source country of the threat, victim countries of the threat, motivation behind the attack, tools used for the attack, and tool type employed in the attack.

From these sources, we compiled information on approximately **443** threat groups, with **120** of them targeting OT/ICS environments in industrial sectors such as manufacturing, energy, oil & gas, industrial, petrochemical, and critical infrastructure. These platforms and databases may not cover all threat groups, but they do offer valuable insights into the latest threats and trends in the OT cyber security landscape. Cybersecurity professionals often use a combination of open-source intelligence, commercial threat intelligence feeds, and proprietary research to develop a comprehensive understanding of threat groups and their activities. Security researchers frequently study TTPs to create "threat profiles" that assist in identifying the origin, intent, and capabilities of a threat group. This information is crucial for comprehending the threat landscape, devising effective defenses, and responding to incidents.

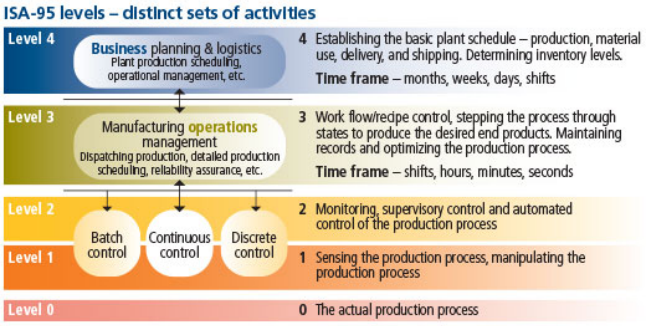

FIGURE 1: The ISA-95 standard addresses the adoption of a level for each activity [43]

A. THREAT ACTOR GROUP

Numerous threat actors pose significant risks to industries in the realm of OT. These threat actors encompass diverse entities, each with distinct motivations and capabilities. Figure 2a presents the statistical analysis of threat groups that conducted attacks up until June 2023. The data reveals that the *Lazarus Group (also known as Hidden Cobra, Labyrinth Chollima)* accounted for the highest percentage of approximately 10% of overall attacks, followed closely by the *Lockbit gang and Sofacy (also known as APT 28, Fancy Bear, Sednit)*, both contributing to approximately 8.5% of attacks on OT environments and so forth.

B. VICTIM SECTOR

Attacks on OT environments in different sectors can result in significant operational disruptions. Manufacturing produc-

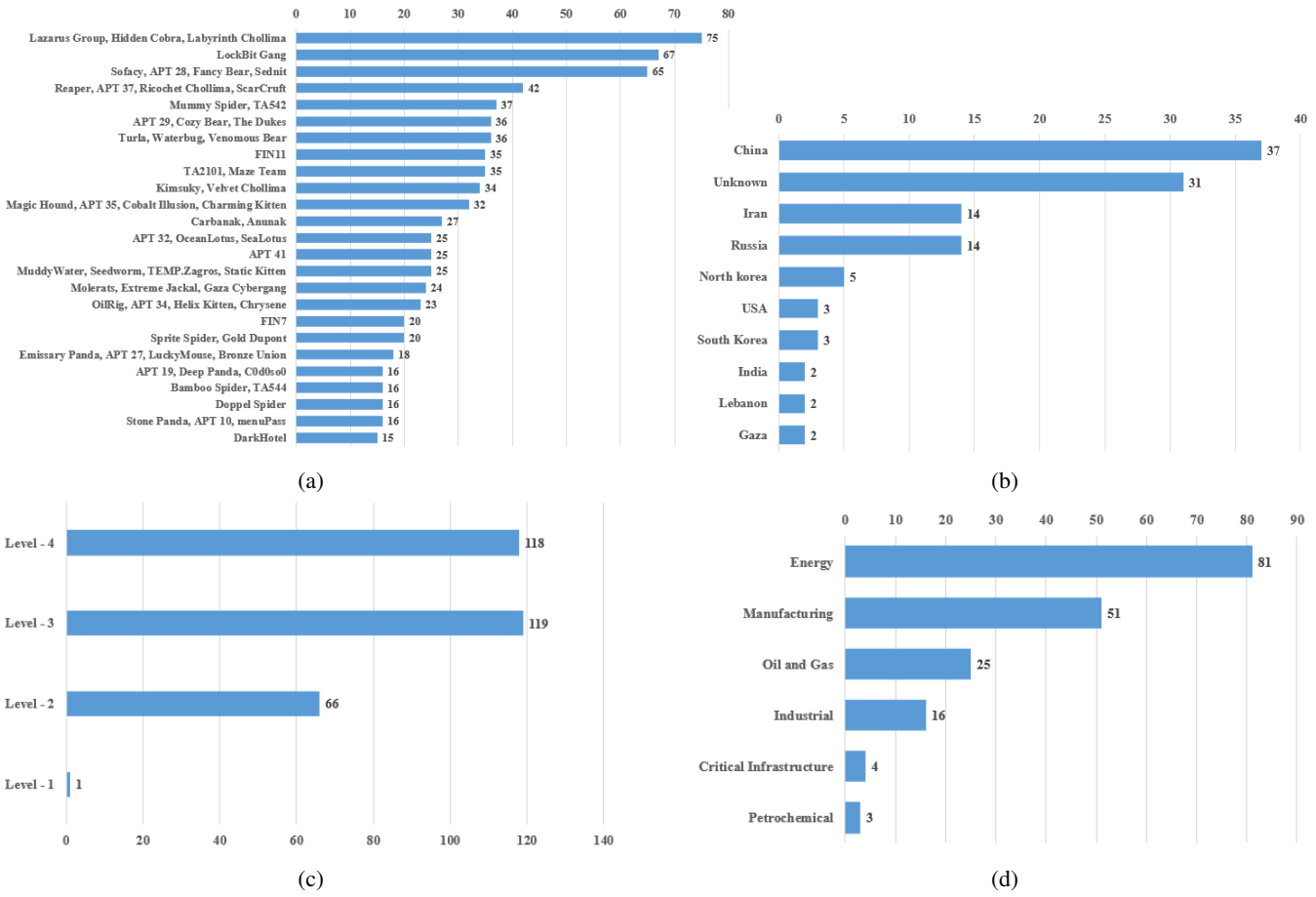

FIGURE 2: (a) Top 25 Threat Groups (with alias), (b) Top 10 Threat Source Countries, (c) ISA-95 Level-Based Attacks by Threat Groups, (d) Threat Groups Victim Sector

tion lines may come to a halt, causing delays in product delivery. Energy, oil, and gas facilities might experience shutdowns or disruptions in the supply chain, leading to energy shortages and price fluctuations. Petrochemical plants could suffer from equipment malfunctions, affecting their output. A high-profile attack on an OT environment can tarnish the reputation of the impacted organization or industry. Customers, partners, and investors might lose trust in the organization's capacity to safeguard critical infrastructure, potentially losing business and brand value. Figure 2d presents a statistical analysis of the affected victim sectors, along with the number of threat groups targeting each respective sector. The *energy sector* emerges as the most frequently attacked, contributed by 67.5% of the threat groups, followed by *manufacturing* with 42.5%, and *oil and gas* with 20.8%.

C. OT INFRASTRUCTURE TARGET LEVEL

In industrial automation, the convergence of two domains within ICS, namely IT and OT, has emerged as the driving force behind Industry 4.0 (I4.0). Adopting cutting-edge software technologies, business intelligence, and analytics propels this evolution. Referring to the ISA-95 automation pyramid [43] (see Figure 1 for a depiction of the related activities at each level), IT is positioned at Level 4 according to the standard. It governs business planning and logistics, encompassing data distribution software, data centers, corporate networks, and enterprise systems for data processing. Furthermore, OT occupies a position from Level 0, extending up through Level 2, and at times even encompassing Level 3. Its purview encompasses oversight of manufacturing operations and controls, including data acquisition systems, process plants, field equipment, human interfaces, and control networks. Figure 2c illustrates a statistical analysis of the most targeted levels based on ISA-95. It reveals that *Level 3* is the most frequently attacked, targeted by 99% of threat groups, followed by *Level 4* with 98%, *Level 2* with 55%, and *Level 1* with approximately 1%.

D. SOURCE COUNTRY OF THREAT GROUP

Attributing cyber threat groups to specific source countries can present challenges and complexities due to using various techniques, such as proxy servers, VPNs, and false flag operations. These techniques allow attackers to conceal their actual locations and identities. Moreover, certain threat actors intentionally obfuscate their origins to avoid detection and attribution.

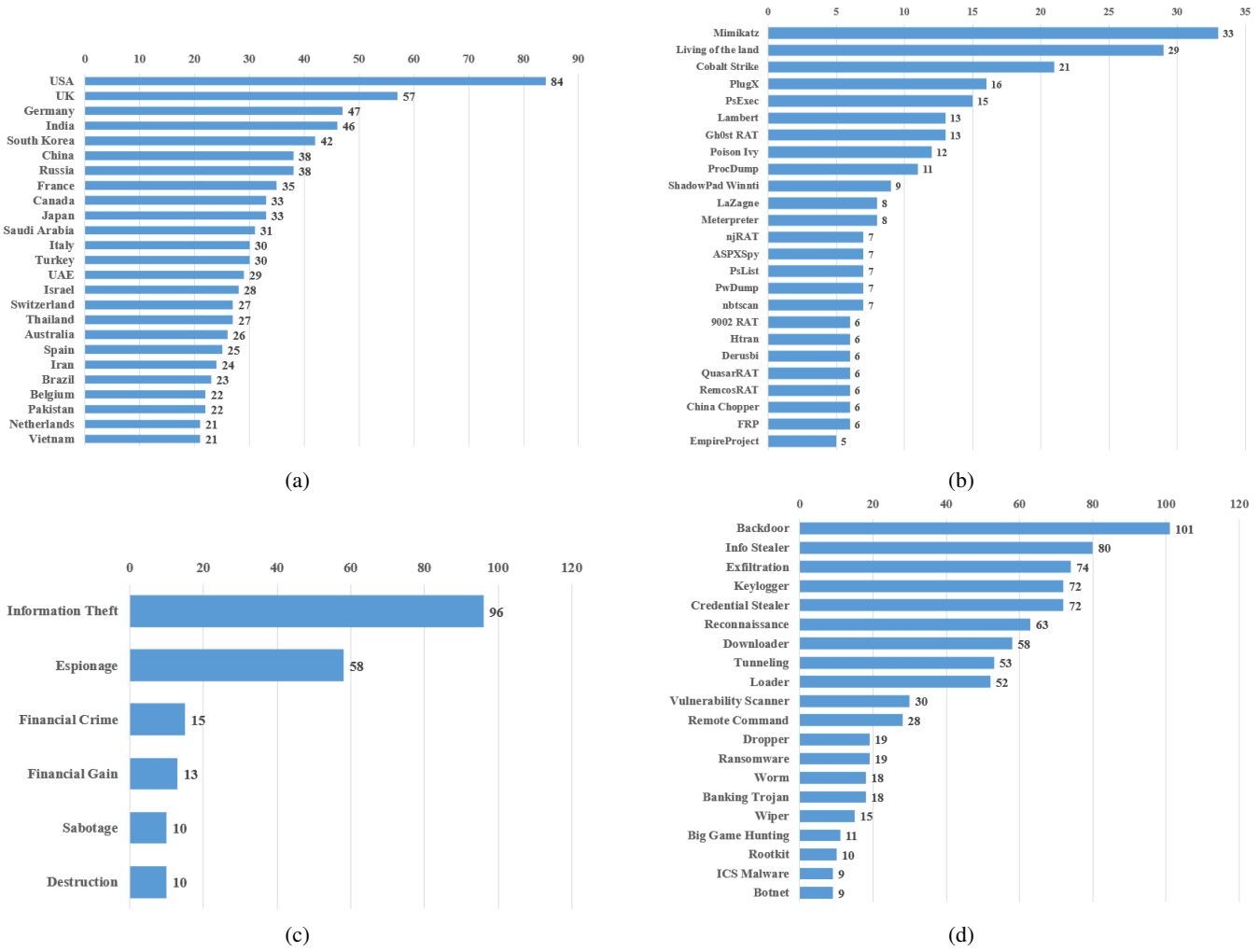

FIGURE 3: (a) Top 25 Victim Countries, (b) Top 25 Tools used by Threat Group, (c) Threat Group Attack Motivation, (d) Top 20 Type of Tool Used

However, cyber security researchers and experts often analyze diverse indicators and TTPs employed in cyber attacks to formulate informed assessments about the likely origin of threat groups. Despite these challenges, continuous research and collaboration within the cybersecurity community enhance the accuracy of attribution and deepen the comprehension of the global threat landscape.

Figure 2b displays a statistical analysis of the threat landscape, indicating the countries of origin for the threat groups. *China* emerges as the primary source, accounting for 30.8% of the threat groups, followed by *unidentified countries* at 25.8%, *Iran* and *Russia* at 11.6%, and others.

E. VICTIM COUNTRY OF ATTACK

The specific attribution of attacks to victim countries can be intricate and subject to change over time; certain countries are known to be more frequently targeted. Recognizing that these attacks can impact multiple countries is essential, and the roster may shift as new threats and campaigns emerge. Cyber attacks have the potential to affect numerous countries and organizations worldwide. While it is possible to report and analyze specific incidents and attacks, it is crucial to avoid making generalizations by assuming that threat groups exclusively focus on particular countries. Cyber attacks represent a global phenomenon; victims can be identified in diverse countries and industries.

Figure 3a illustrates a statistical analysis of countries frequently targeted due to their essential industrial infrastructure, which is critical for the operation of their economies. For instance, the *United States* has emerged as the primary target, being targeted by 70% of threat groups, hosting numerous major manufacturing plants, oil and gas pipelines, and power plants. These facilities are potential targets for threat groups aiming to disrupt or harm critical infrastructure. Following the *United States* are the *United Kingdom* at 47.5%, *Germany* at 39%, and other countries.

F. MOTIVATION OF ATTACK

As mentioned in the introduction, the motivation of threat groups varies depending on the specific goals they aim to achieve. Based on the analyzed data, we have observed that among the **120** threat groups, the outcomes of their motivations are illustrated in Figure 3c. Approximately 80% of the threat groups are motivated by *information theft*, while approximately 48% of them focus on *espionage*, and so forth.

G. TOOLS USED IN ATTACK

Considerable research has been undertaken to study the selection of tools utilized by threat groups when targeting specific entities. Threat actors often follow discernible patterns in their attacks on these entities, and devising a strategy to counteract these tools could prove highly effective. The functionalities of all the tools are detailed in Table 1. Figure 3b illustrates the various tools employed by the analyzed threat groups, with the *Mimikatz* tool being used by these threat groups approximately 28% of the time, followed by *Living off the Land* tools at 24.1%, *Cobalt Strike* at 17.5%, and others.

H. TYPE OF TOOLS USED IN ATTACK

The different types of malware cover a variety of malicious software; most malware is designed to exploit systems for the benefit of cybercriminals. Understanding the various types of malware is crucial in protecting your devices and systems from cyber-attacks. Comprehending the different types of tools is essential in safeguarding yourself from potential compromises. Figure 3d displays the percentage usage of tool types by the threat groups, with *Backdoors* being used the most, accounting for 84% of the time, followed by *Info Stealers* at 66%, *Exfiltration tools* at 61%, and others.

IV. ICS CYBER-KILL CHAIN PROCEDURE

Here, we use the SANS ICS cyber kill chain [44], [45], a framework for dissecting complex attacks into nonexclusive stages. This two-stage model outlines an attacker's steps to target and compromise an ICS. Understanding these stages allows defenders to implement security measures to disrupt the attack process and mitigate risks. The stages of the ICS cyber kill chain are:

Stage 1: Reconnaissance - The attacker gathers information about the target ICS/OT environment, such as scanning for vulnerabilities, identifying devices and systems, and understanding the overall architecture.

Stage 2: Weaponization - The attacker uses the gathered information to develop and test tools or exploits to attack the ICS/OT. This may involve creating custom malware or modifying existing tools to target specific ICS vulnerabilities. Figure 4 illustrates the ICS Cyber-Kill Chain procedure along with the attack source country, attack motivation, reported victim countries, and reported victim sectors, OT infrastructure level affected in relation to the threat group analysis (cf. Section III) for two distinct attacks: the SolarWinds and TRITON attacks.

TABLE 1: Functionalities of tools used by threat groups

Tool	Functionality
Mimikatz	Credential theft tool, primarily used for extracting plaintext passwords, hashes, and tickets from memory.
Living off the Land	Refers to the use of legitimate system tools and functionalities by attackers for malicious purposes, making detection more challenging.
Cobalt Strike	Framework for adversary simulation and red team operations, facilitating post-exploitation activities, command and control, and lateral movement.
PlugX	Remote Access Trojan (RAT) is designed for targeted attacks, allowing attackers to control compromised systems.
PsExec	Microsoft Sysinternals tool used for executing processes on remote systems, often employed for lateral movement in network exploitation.
Lambert	Part of the Equation Group's toolset, associated with sophisticated cyber espionage activities.
Gh0st RAT	Remote access Trojan used for unauthorized access and control of compromised systems.
Poison Ivy	Remote access Trojan with features for surveillance, data theft, and control of infected systems.
ProcDump	Sysinternals tool for creating process dumps is often used for analyzing and troubleshooting software.
ShadowPad Winnti	Backdoor is associated with the Winnti Group, known for targeted attacks against the gaming industry and other sectors.
LaZagne	Credential recovery tool, similar to Mimikatz, focuses on retrieving passwords from various applications.
Meterpreter	A payload within the Metasploit framework, providing a wide range of post-exploitation capabilities on compromised systems.
njRAT	RAT are used for remote control, surveillance, and data theft.
ASPXSpy	Webshell are used for unauthorized access and control of web servers.
PsList	Sysinternals tool for listing detailed information about processes.
PwDump	Tool for extracting password hashes from Windows systems.
nbtscan	Network tool for discovering and enumerating NetBIOS shares.
9002 RAT	Remote access Trojan known for evading detection and maintaining persistence on compromised systems.
Htran	Covert communication tool for creating hidden communication channels.
Derusbi	Backdoor are associated with various cyber threat groups, including APT17.
QuasarRAT	Remote access Trojan with features for keylogging, screenshot capture, and more.
RemcosRAT	Remote access Trojan with capabilities for remote control and surveillance.
China Chopper	Webshell often used by Chinese threat actors for unauthorized access to web servers.
FRP	Network tunneling tool for bypassing firewalls and accessing restricted networks.
EmpireProject	Post-exploitation framework for offensive security operations, similar to Cobalt Strike.

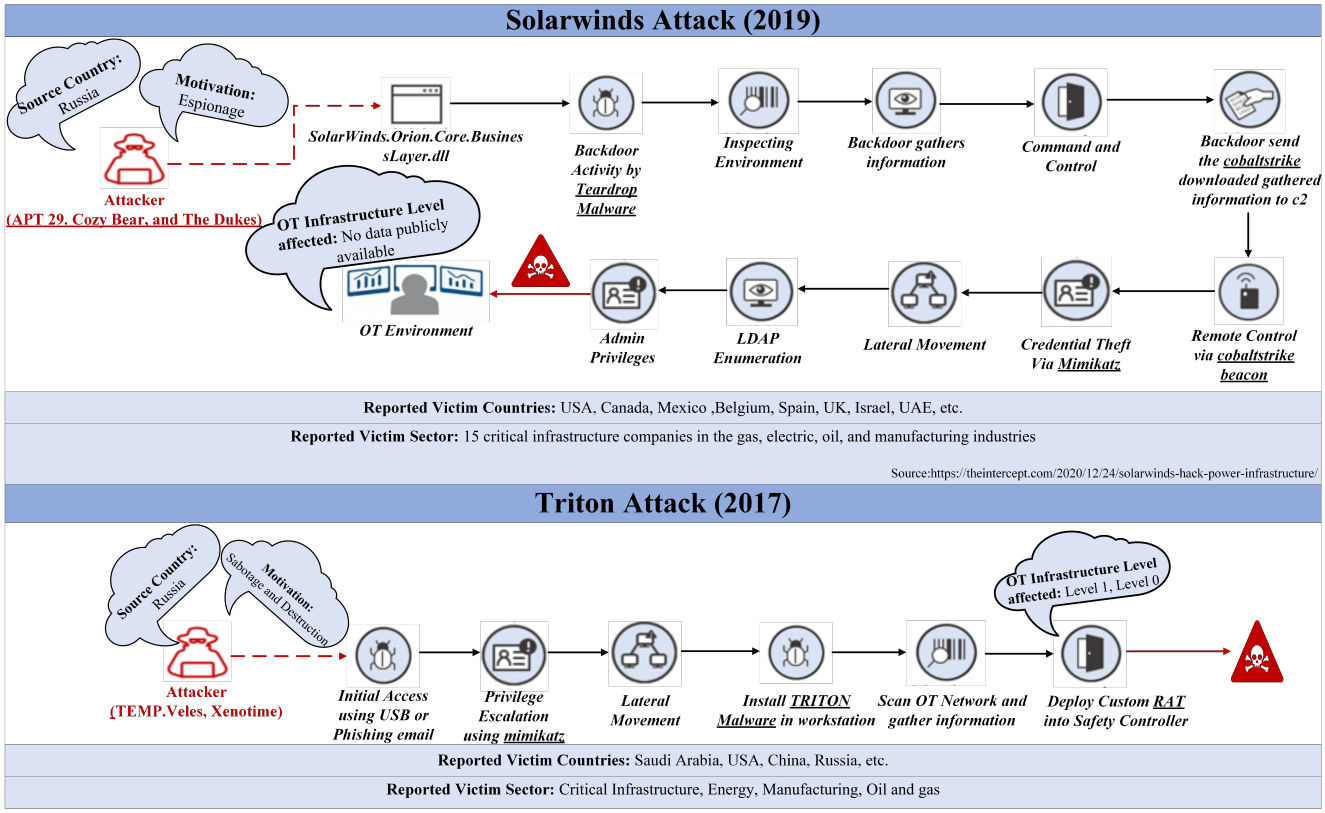

FIGURE 4: ICS Cyber-kill chain procedure phases and impact of Solarwinds and TRITON attack on OT environment

The SolarWinds attack [46], attributed to the Russian APT group Cozy Bear (APT29), was a supply chain breach that infiltrated both SolarWinds' servers and customer networks. **During the reconnaissance phase**, attackers likely gathered information from public sources, industry reports, or even social media to plan how to exploit SolarWinds' software as an initial access vector. SolarWinds' software, designed for network monitoring, extends to OT levels, including SNMP networks and devices used in industrial and building automation. In the weaponization phase, the Teardrop malware was injected into SolarWinds' update servers to exploit vulnerabilities in SolarWinds Orion and provide remote access. The attack implanted a malicious payload within SolarWinds' Orion platform software, specifically in *SolarWinds.Orion.Core.BusinessLayer.dll*. Subsequently, teardrop malware was deployed, creating a backdoor for collecting network information and establishing connections with a C2 server. Through Cobalt Strike, the attacker gained remote access, facilitating credential theft and privilege escalation. Mimikatz was employed for credential theft, enabling lateral movement within the network, LDAP enumeration, and obtaining admin privileges. With admin access, the attacker could have compromised the OT environment with ease.

According to the Schneider Electric analysis and disclosure [47], the Triton attack was executed through a phishing campaign and attributed to the Russian APT group TEMP.Veles (also known as Xenotime). In the Triton attack [48], it appears that the attackers attempted to implant a Remote Access Trojan (RAT) within the Triconex Safety Instrumented System (SIS). **During the reconnaissance phase**, the attackers likely gathered information from industry publications, ICS vendor documentation, or even by exploiting zero-day vulnerabilities. They studied ICS protocols, identified vulnerabilities in Triconex SIS, and developed customized malware later named Triton (or Trisis). **In the weaponization phase**, initial access was possibly gained through phishing emails, insecure remote access, or USB infiltration. After gaining access, the attackers moved laterally within the compromised system and achieved privilege escalation using Mimikatz. Once inside the workstations, the attackers installed the Triton malware. Triton then scanned the OT network to gather information on PLCs and safety controllers, subsequently deploying a custom RAT to reprogram them. This action led to a safety incident, resulting in production downtime.

V. DISCUSSION

Analyzing **threat groups** enhances situational awareness in OT environments, enabling organizations to monitor emerging threats, adapt to evolving tactics, and implement proactive security measures.

Analyzing **victim sectors** facilitates the development of tailored defense strategies that address each sector's specific

challenges and risks. Despite the unique characteristics of each sector, common threat patterns and attack vectors often transcend across multiple sectors. By scrutinizing victim sectors, shared vulnerabilities and tactics can be identified, fostering the development of cross-sector threat intelligence and collaborative defense measures. This analysis is instrumental in assisting organizations to ensure compliance with sector-specific cybersecurity regulations and guidelines. As illustrated in Figure 2d, the number of attacks on sectors such as energy, manufacturing, and oil & gas underscores their heavy reliance on OT systems.

Analyzing the **target level** assists in evaluating the criticality and potential impact of cyber-attacks on specific OT infrastructure components. This evaluation guides risk management efforts, enabling organizations to allocate resources and prioritize mitigation strategies for high-value targets. As illustrated in Figure 2c, understanding the target level reveals that most attacks target ISA-95 levels 3 and 4, underscoring their critical importance. These levels typically contain vital production data, such as schedules, specifications, and quality control information. Breaching these layers can grant threat actors access to sensitive intellectual property and proprietary data, posing significant competitiveness and business continuity risks.

Analyzing the **source country** can provide insights into the potential motivations behind the attacks, assisting organizations in gaining a deeper understanding of the intent of the threat group. If the source country is identified, organizations can engage diplomatic channels for reporting cyber incidents and seeking cooperation in investigations, mitigation efforts, sanctions, or retaliatory measures. On the other hand, as illustrated in Figure 2b, it demonstrates the OT exploitation capabilities of countries such as China, Iran, and Russia.

Analyzing the **victim country** assists in evaluating the potential impact of cyber attacks on OT systems within that nation. This analysis establishes a foundation for assessing the severity of the threat and its ramifications for national security and public safety. Moreover, scrutinizing the victim country offers a broader perspective on the global cyber threat landscape, enabling organizations to remain informed about international cyber incidents and adapt their defenses accordingly. As illustrated in Figure 3a, it interprets the higher adoption of OT in countries such as the USA, UK, Germany, and many more.

The **motivation behind an attack** can serve as a guide for prioritizing vulnerabilities to be patched or mitigated. Vulnerabilities that align with the attackers' motivations are more likely to be actively exploited and demand immediate attention. High-impact motivations might necessitate heightened investment in defensive measures and incident response capabilities. As illustrated in Figure 3c, attacks motivated by information theft, espionage, and financial gain in OT environments can disrupt supply chains, compromise critical infrastructure, threaten national security, and harm the economy.

Analyzing these **tools** helps organizations understand that certain tools may be associated with specific threat groups or campaigns. This analysis assists in attributing attacks to known threat actors or identifying patterns that can be utilized for future signature detection. Additionally, analyzing tools aids organizations in developing tailored defensive countermeasures. Security measures, including Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and firewalls, can be configured to identify and block the usage of specific tools. As illustrated in Figure 3b, it suggests that the number of attacks using tools like Mimikatz, Living off the Land, and Cobaltstrike may be directly proportional to the inability of security measures to detect them.

Knowing **tool types** facilitates proactive threat-hunting activities. Security teams can then search for Indicator of Compromises (IoCs) associated with the identified tool types, enabling early detection of potential threats.

VI. STRATEGIES TO DEFEND AGAINST ADVERSARIES

The literatures [49]–[58] offers a range of common strategies for defending against adversary threat groups:

- **Use Updated Antivirus and Antimalware Software:** Install reputable antivirus and antimalware software on all devices and servers. Keep these applications updated to ensure they can detect and remove the latest malware threats.
- **Regular Software Updates and Patching:** Keep your operating systems, applications, and software up-to-date with the latest security patches. Many malware attacks exploit known vulnerabilities in outdated software.
- **Implement Strong Password Policies:** Enforce strong password policies across your network to prevent unauthorized access. Use complex passwords, multi-factor authentication (MFA), and regularly update passwords.
- **Educate Users:** Train your employees and users about the risks of malware, phishing, and other social engineering techniques. Teach them to recognize suspicious emails, links, and attachments.
- **Restrict User Privileges:** Limit user privileges to the minimum necessary for their job function. Users should only have access to the resources they require to perform their duties.
- **Network Segmentation:** Segment your network into smaller, isolated subnetworks. This helps contain malware and prevents it from spreading throughout the entire network.
- **Regular Data Backups:** Maintain regular backups of critical data and store them in a secure location, preferably offline or in the cloud. In case of a malware infection, you can restore your data without paying ransom or losing important information.
- **Web Filtering and Firewalls:** Employ web filtering and firewalls to block access to malicious websites and unauthorized network traffic. Firewalls act as a barrier between your internal network and the internet, reducing the risk of malware infiltration.

- **Email Protection:** Implement advanced email security measures, such as anti-spam filters, email authentication (Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC)), and email encryption to prevent phishing attacks and malicious email attachments.
- **Monitoring and Incident Response:** Continuously monitor your network for signs of malware activity and establish an incident response plan. This plan should outline how to handle and contain security incidents promptly and effectively.
- **Secure Remote Access:** If your organization allows remote access to its network, ensure that remote connections are secured using VPNs and other encryption technologies.
- **Application Whitelisting and Blacklisting:** Consider using application whitelisting to allow only approved applications to run on your systems, and use blacklisting to block known malicious software.
- **Disable Autorun:** Disable autorun and autoplay features on your devices to prevent malware from spreading through removable media.
- **Secure Mobile Devices:** Extend your security measures to mobile devices (e.g., smartphones, tablets) that connect to your network. Implement mobile device management (MDM) solutions to enforce security policies on these devices.
- **Regular Security Audits:** Conduct periodic security audits and penetration tests to identify vulnerabilities and address them proactively.

Many industries employ these common strategies to defend OT environment against adversary threat groups, and they often align their control systems with various popular frameworks, including ISA/IEC 62443, NIST 800-53, NIST 800-82, the ISO 27000 Series, CIS Critical Security Controls, NERC CIP, the NIS Directives, MITRE ATT&CK ICS Framework, NISTIR 8374, Cybersecurity Maturity Model Certification, The Qatar ICS Security Standard, TSA Pipeline-2021-02D (SD-02D), and the NCA Essential Cybersecurity Controls (ECC).

VII. CONCLUSION

This paper undertakes an in-depth analysis of threat groups operating in OT environments, offering valuable insights into the dynamic landscape of cyber threats. By examining motives, tactics, and tools employed by adversaries targeting industrial infrastructure, this comprehensive study aims to deepen the understanding of potential risks. The examination explores victim sectors, target levels, associated countries, attack motivations, and tools. Figure 5 visually represents the interconnectedness of these critical factors and outlines the process of escalation attacks. The genesis of any high-profile attack is often rooted in the actions of threat actor groups, which, notably, lack inherent affiliation with any specific source country due to the global distribution of their members.

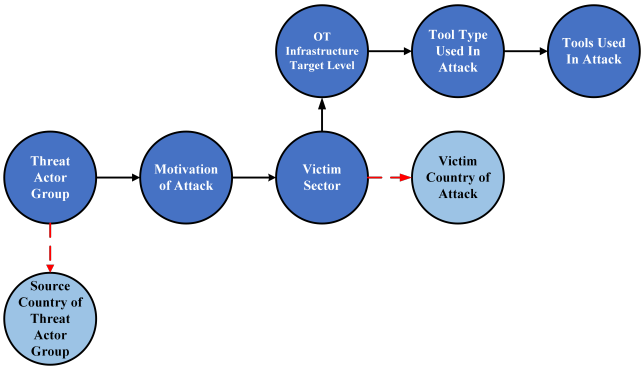

FIGURE 5: Escalation of attacks in OT environment

Each threat actor is motivated by specific factors, influencing their choice of target sectors. Notably, the location of the victim sector may not be specific to any particular country. Subsequently, the threat group strategically determines the OT infrastructure level they intend to target, employing specific tool types based on this level. The selection of tools is critical for gaining access to the targeted infrastructure.

Understanding the motivations behind attacks empowers organizations to mitigate vulnerabilities proactively. An in-depth analysis of tools enhances threat detection capabilities and facilitates the implementation of tailored countermeasures against those tools. Insights into targeted sectors, levels, and countries foster collaborative defense strategies.

Although in recent years, recognition of cybersecurity's importance in industry is growing, prompting increased investment in security measures and collaboration among industry, government, research, and private sectors shows the strengthening responses to OT security challenges, exemplified by initiatives such as the ETHOS open-source platform for sharing anonymous early warning threat information [59]. Growing innovations in anomaly detection tools based AI and ML are enhancing threat detection capabilities in industrial settings.

However, gaps persist in cybersecurity standards and regulations for ICS as standardization does not guarantee a fully secure environment. Although, research into threat modeling and vulnerability assessments is one way to deepen understanding of OT security risks. However, challenges remain, including reliance on outdated legacy technology, a shortage of cybersecurity professionals in OT environments, and resistance to change. This essential factor is hampering cybersecurity adoption and progress in securing the industry.

To overcome these obstacles, research should take a holistic approach, considering technical, organizational, and human factors by prioritizing high-risk areas and developing adaptive security measures vital for resilient industrial cybersecurity. The insights and strategies presented in this paper might provide a foundation for navigating the intricate realm of OT cybersecurity.

ACKNOWLEDGMENT

This paper was supported by TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry, a research cooperation between TU Wien and TÜV AUSTRIA.

REFERENCES

[1] S. Santos, P. Costa, and A. Rocha, "IT/OT Convergence in Industry 4.0 : Risks and Analysis of the Problems," in 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1–6, 2023.

[2] T. Sauter and C. Schwaiger, "Achievement of secure internet access to fieldbus systems," Microprocessors and Microsystems, vol. 26, no. 7, pp. 331–339, 2002.

[3] J. Ford and H. S. Berry, "Leveling Up Survey of How Nation States Leverage Cyber Operations to Even the Playing Field," in 2023 11th International Symposium on Digital Forensics and Security (ISDFS), pp. 1–5, 2023.

[4] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," Internet of Things and Cyber-Physical Systems, vol. 4, pp. 186–202, 2024.

[5] B. Bracken, "ICS Ransomware Danger Rages Despite Fewer Attacks," https://www.darkreading.com/ics-ot-security/ics-ransomware-rages-fewer-attacks, [Accessed 24-04-2024].

[6] Deloitte, "Mitigate Healthcare Cyber Threats with AI-powered Intelligence," https://www2.deloitte.com/us/en/pages/risk/solutions/elevating-healthcare-security-proactive-defense-with-ai-threat-intelligence.html, [Accessed 24-04-2024].

[7] A. Bécue, I. Praça, and J. Gama, "Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities," Artificial Intelligence Review, vol. 54, no. 5, pp. 3849–3886, Jun. 2021.

[8] N. Kaloudi and J. Li, "The AI-Based Cyber Threat Landscape: A Survey," ACM Comput. Surv., vol. 53, no. 1, Feb. 2020.

[9] J. Sengupta, S. Ruj, and S. Das Bit, "A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT," Journal of Network and Computer Applications, vol. 149, p. 102481, 2020.

[10] L. Papadopoulos, K. Demestichas, E. Muñoz-Navarro, J. J. Hernández-Montesinos, S. Paul, N. Museux, S. König, S. Schauer, A. C. Alarcón, I. P. Llopis, T. Stelkens-Kobsch, T. Hadjina, and J. Levak, "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach," International Journal of Critical Infrastructure Protection, vol. 44, p. 100657, 2024.

[11] K. Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. (2016). [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[12] Industroyer' virus could bring down power networks, researchers warn. (2017). [Online]. Available: https://tinyurl.com/r7p56vye

[13] T. Spring. Vpnfilter malware infects 500k routers including linksys, mikrotik, netgear. (2018). [Online]. Available: https://threatpost.com/vpnfilter-malware-infects-500k-routers-including-linksys-mikrotik-netgear/132212/

[14] M. Giles. Triton is the world's most murderous malware, and it's spreading. (2019). [Online]. Available: https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[15] B. Hunter and F. Gutierrez. Ekans ransomware: A malware targeting ot ics systems. (2020). [Online]. Available: https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

[16] T. W. House. Colonial pipeline cyber incident. (2021). [Online]. Available: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

[17] S. Hanson. Deep dive into pipedream's opc ua module, mousehole. (2023). [Online]. Available: https://www.dragos.com/blog/pipedream-mousehole-opcua-module/

[18] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," Computers Security, vol. 72, pp. 26–59, 2018.

[19] Bahrami, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," J. Inf. Process. Syst., vol. 15, no. 4, pp. 865–889, Aug. 2019.

[20] S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, "A comprehensive study on apt attacks and countermeasures for future networks and communications: challenges and solutions," J. Supercomput., vol. 75, no. 8, p. 4543–4574, Aug. 2019.

[21] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019.

[22] S. Hussain, M. B. Ahmad, and S. S. Uddin Ghouri, "Advance Persistent Threat—A systematic review of literature and meta-analysis of threat vectors," in Advances in Computer, Communication and Computational Sciences, pp. 161–178. Singapore: Springer Singapore, 2021.

[23] M. Abu Talib, Q. Nasir, A. Bou Nassif, T. Mokhamed, N. Ahmed, and B. Mahfood, "APT beaconing detection: A systematic review," Computers Security, vol. 122, p. 102875, 2022.

[24] I. Kotenko, D. Gaifulina, and I. Zelichenok, "Systematic literature review of security event correlation methods," IEEE Access, vol. 10, pp. 43 387–43 420, 2022.

[25] K. Huang, M. Siegel, and S. Madnick, "Systematically understanding the cyber attack business: A survey," ACM Comput. Surv., vol. 51, no. 4, Jul. 2018.

[26] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, p. 107094, 2020.

[27] P. Bhatt, E. T. Yano, and P. Gustavsson, "Towards a framework to detect multi-stage advanced persistent threats attacks," in 2014 IEEE 8th International Symposium on Service Oriented System Engineering, pp. 390–395, 2014.

[28] P. Giura and W. Wang, "A context-based detection framework for advanced persistent threats," in 2012 International Conference on Cyber Security, pp. 69–74, 2012.

[29] J. R. Johnson and E. A. Hogan, "A graph analytic metric for mitigating advanced persistent threat," in 2013 IEEE International Conference on Intelligence and Security Informatics, pp. 129–133, 2013.

[30] G. Ioannou, P. Louvieris, N. Clewley, and G. Powell, "A markov multi-phase transferable belief model: An application for predicting data exfiltration apts," in Proceedings of the 16th International Conference on Information Fusion, pp. 842–849, 2013.

[31] W. NIU, X. ZHANG, G. YANG, R. CHEN, and D. WANG, "Modeling attack process of advanced persistent threat using network evolution," IEICE Transactions on Information and Systems, vol. E100.D, no. 10, pp. 2275–2286, 2017.

[32] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," pp. 62–80.

[33] T. Rid and B. Buchanan, "Attributing cyber attacks," Journal of Strategic Studies, vol. 38, no. 1-2, pp. 4–37, 2015.

[34] Y. Mei, W. Han, S. Li, X. Wu, K. Lin, and Y. Qi, "A review of attribution technical for apt attacks," in 2022 7th IEEE International Conference on Data Science in Cyberspace (DSC), pp. 512–518, 2022.

[35] A. Sundaram, H. S. Abdel-Khalik, and O. Ashy, "A data analytical approach for assessing the efficacy of operational technology active defenses against insider threats," Progress in Nuclear Energy, vol. 124, p. 103339, 2020.

[36] C. Krasznay and G. Gyebnár, "Possibilities and limitations of cyber threat intelligence in energy systems," in 2021 13th International Conference on Cyber Conflict (CyCon), pp. 171–188, 2021.

[37] Z. Jadidi and Y. Lu, "A threat hunting framework for industrial control systems," IEEE Access, vol. 9, pp. 164 118–164 130, 2021.

[38] "All groups - Threat Group Cards: A Threat Actor Encyclopedia," https://apt.etda.or.th/cgi-bin/listgroups.cgi, [Accessed 26-07-2023].

[39] F. FKIE, "Malpedia (Fraunhofer FKIE)," https://malpedia.caad.fkie.fraunhofer.de/, [Accessed 26-07-2023].

[40] "Groups | MITRE ATT&CK," https://attack.mitre.org/groups/, [Accessed 26-07-2023].

[41] "Cybersecurity Alerts & Advisories | CISA," https://www.cisa.gov/news-events/cybersecurity-advisories, [Accessed 26-07-2023].

[42] M. P. Bhole, "Data analysis and results of threat groups in ot environment," https://researchdata.tuwien.at/records/ewmb8-3ad52, Nov. 2023.

[43] "Enterprise-control system integration – part 1: Models and terminology," International Society of Automation, 2010.

[44] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in Security in Computing and Communications, J. H. Abawajy, S. Mukherjea, S. M. Thampi, and A. Ruiz-Martínez, Eds., pp. 438–452. Cham: Springer International Publishing, 2015.

[45] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:213190869

[46] R. Lakshmanan. Here's how solarwinds hackers stayed undetected for long enough. (2021). [Online]. Available: https://thehackernews.com/2021/01/heres-how-solarwinds-hackers-stayed.html
[47] A. Kling and P. Forney. Triton - schneider electric analysis and disclosure. Youtube. [Online]. Available: https://www.youtube.com/watch?v=f09E75bWvkk
[48] B. Johnson, D. Caban, M. Krotofil, D. Scali, N. Brubaker, and C. Glyer. Attackers deploy new ics attack framework "triton" and cause operational disruption to critical infrastructure. (2017). [Online]. Available: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton
[49] "Bundesamt für Sicherheit in der Informationstechnik - Recommendations," https://tinyurl.com/BSIRecommendations, (Accessed on 08/08/2023).
[50] K. Scarfone, "NIST Special Publication (SP) 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops," https://csrc.nist.gov/pubs/sp/800/83/r1/final, [Accessed 04-08-2023].
[51] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf, (Accessed on 08/08/2023).
[52] D. Walkowski, "What Is the Principle of Least Privilege and Why is it Important?" https://www.f5.com/labs/learning-center/what-is-the-principle-of-least-privilege-and-why-is-it-important, [Accessed 04-08-2023].
[53] Praveen, "Six Best Practices for Secure Network Firewall Configuration," https://www.eccouncil.org/cybersecurity-exchange/network-security/six-network-firewall-configuration-best-practices/, [Accessed 04-08-2023].
[54] "How DMARC Advances Email Security," https://www.cisecurity.org/insights/blog/how-dmarc-advances-email-security, [Accessed 04-08-2023].
[55] K. Scarfone, "NIST Special Publication (SP) 800-61 Rev. 2, Computer Security Incident Handling Guide," https://csrc.nist.gov/pubs/sp/800/61/r2/final, [Accessed 04-08-2023].
[56] S. Karen, "NIST Special Publication (SP) 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," https://csrc.nist.gov/pubs/sp/800/46/r2/final, [Accessed 04-08-2023].
[57] "What Is Endpoint Security? How It Works & Its Importance," https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html#:~:text=EPPs%20secure%20endpoints%20through%20application,which%20helps%20prevent%20data%20loss., [Accessed 04-08-2023].
[58] "Using Caution with USB Drives | CISA," https://www.cisa.gov/news-events/news/using-caution-usb-drives, [Accessed 04-08-2023].
[59] "ETHOS | Emerging Threat Open Sharing — ethos-org.io," https://www.ethos-org.io/, [Accessed 23-07-2024].

MUKUND BHOLE earned a B.Tech degree in Information Technology from Shivaji University, Kolhapur, India, in 2019, and later completed his M.Tech degree in Information Security from COEP Technological University, Pune, India, in 2021. Currently, he is pursuing a Ph.D. degree at TU Wien, with a research focus on safety and security in operational technology environments. Additionally, he also serves as a project assistant at #SafeSecLab. His research interests span Information Security, Penetration Testing, Intrusion Detection, and Vulnerability Assessment.

WOLFGANG KASTNER (M'06) (Senior Member, IEEE) is currently a Full Professor of the Industrial Internet of Things with the Faculty of Informatics, Technische Universität Wien (TU Wien). His research addresses distributed automation and (industrial) communication systems in various application domains, such as factory automation, building automation, and smart grids. His research topics tackle the safe while secure IT/OT convergence and approaches for the Industrial Internet based on information modeling and knowledge representation.

THILO SAUTER (M'93, SM'09, F'14) holds a Ph.D. degree in electrical engineering and is professor for automation technology at TU Wien, Vienna, Austria, as well as senior scientist at the University of Continuing Education Krems, Wiener Neustadt, Austria. From 2004 to 2013, he also was the Founding Director of the Institute for Integrated Sensor Systems at the Austrian Academy of Sciences. His expertise and research interests include embedded systems and integrated circuit design, smart sensors, and automation and sensor networks with a focus on real-time, security, interconnection, and integration issues relevant to cyber-physical systems and the Internet of Things in various application domains such as industrial and building automation, smart manufacturing, or smart grids. Dr. Sauter is member of the Board of the Austrian Electrotechnical Association and Senior AdCom Member of the IEEE Industrial Electronics Society (IES). Moreover, he has been involved in the standardization of industrial communication systems for more than 25 years.