Sri Lanka Institute of Information Technology

APT Attacks on Industrial Control Systems

Individual Assignment

IE2020 – Introduction to Cyber Security

Submitted by: D.O.J. Silva

Student Number: IT23440418

Table of Contents

Abstract

The Industrial Control Systems (ICS) market is experiencing growth driven by the increasing demand for automation and a rising emphasis on operational efficiency. Industries are adopting ICS solutions to automate processes, leading to enhanced productivity and reduced costs. Since then, now they have resulted a major impact on information security due to misuse of these resources as a media to mediate crimes. Out of the attacks carried out by cyber-criminals, APT attacks have become an emerging topic. And it's important to study on involvement of Industrial control systems in APT attacks.

The main goal of this report is to explain how APT attacks operate against industrial control systems. APT attacks have become a significant focus within cybersecurity due to their widespread nature and the extensive impact they can have on targeted systems and infrastructures. So, under this context the architecture of APT attacks on Industrial Control System, evolution of APT attacks, risk factors, applicable security controls and future development areas regarding the topic will be discussed in details.

1. Introduction

Modern technology is significantly evolving day by day due to constant development in fields such as machine learning, artificial intelligence, cyber security in most of the domains including telecommunication, health, industrial, agriculture. As a result, the current landscape increasingly gravitates towards technologies such as Industrial Control Systems (ICS), driven by evolving concepts such as smart manufacturing, automation in industrial processes, and integrated operational technologies. Although new technologies are being introduces, many Industrial Control Systems (ICS) often lack security measures. This vulnerability, along with less user awareness and the increasing usability of these systems, has led to a notable rise in the number of users counting on ICS for critical operations. As a result, the need for strong security protocols and knowledge in safe practices become crucial. The industrial Control Systems market size is estimated at USD 185.28 billion in 2024, and is expected to reach USD 283.77 billion by 2029 [2]. So best practice is to study more on ICS technology and think of strategies which can take in order to improve the security around this technology.

1.1 What is ICS?

ICS (Industrial Control System) are integrated systems designed to monitor, control and automate industrial processes and critical infrastructure operations [3][4]. ICS are following information and communication technologies for predictive maintenance, data analytics and IP based services, while leaving behind analogue devices, isolated operations and propritary hardware/software [5].

The first ICS, including the Modular Programmed Controller(MPC) from the 1960s and emerging SCADA systems for remote monitoring, primarily in the electric power industry, laid the groundwork for the advanced ICS we have today [6].ICS systems mainly feature of Supervisory Control and Data Acquisition(SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC) components. SCADA performs the functions of automatic data collection, control and monitoring of industrial systems.DCS comprises systems designed to manage large industry processes, utilizing devices that are operated from a central room [3].

1.2 ICS Architecture

The general architecture of an ICS is shown in Fig. 1.

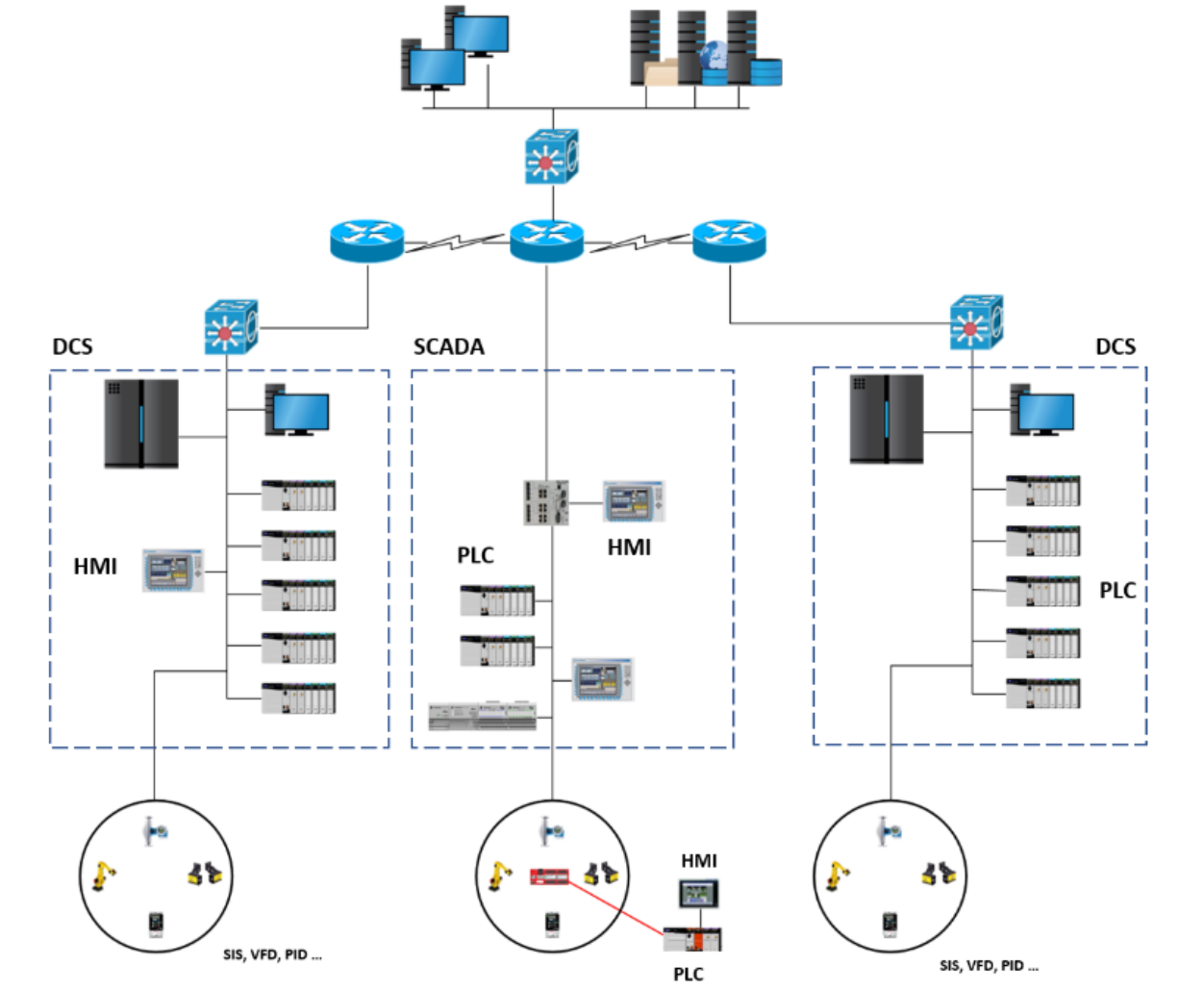

Figure 1.1 Basic architecture of an Industrial Control System [15]

The main components of an ICS include:

Programmable Logic Controller (PLC): A PLC is an industrial computer control system that continuously monitors the state of input devices and makes decisions based upon a custom program to control the state of output devices [10]. PLCs operate in harsh environmental conditions, such as excessive vibration and high noise [11]. With this kind of control system, almost any production line, machine function, or process can be greatly improved. However, the biggest benefit in using a PLC is to make changes and replicate the operation or process while collecting and communicating vital information.

Distributed Control System (DCS): acts as the central brain of the industrial operation. It coordinates and controls, in real time, the process subsystems that are located in an industrial operation [12]. Distributed control systems control complex processes and are able to coordinate processes in large manufacturing plants while offering top-down control [12].

Supervisory Control and Data Acquisition (SCADA): SCADA is a system of software and hardware elements that allows organizations to control and monitor industrial processes by directly interfacing with plant-floor machinery and viewing real-time data[13]. These systems are vital to industrial organizations as they help sustain efficiency, process data for wiser decisions, and communicate system issues to reduce downtime.

1.3 What are APT attacks?

An Advanced Persistent Threat (APT) is a sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time [7].

And APT attack is strategically devised and designed to gain access a specific organization, avoid existing security measures and fly under the radar remain inside for a period of time, with potentially destructive consequences. Techniques and tools to maintain access and navigate within network include compromising employees through phishing, social engineering, utilizing malware, rootkits and trojans [8].

1.4 Reasons for Using APTs to Attack Industrial Control Systems

- ICS networks often segregated from conventional computer systems, making them harder to breach. APTs are resource-intensive and can involve multi-stage campaigns, including spear-phishing, supply chain attacks, or exploiting trusted insider access, which are well-suited to breaching complex ICS environments.

- APTs are designed to stay hidden within network for long periods. Since ICS environments prioritized uptime and stability over frequent updates and monitoring are vulnerable to this. Attackers can remain undetected, and observe and understand the system in depth for conducting full-scale attacks.

- Attackers often establish long term access through backdoors. This gives attacker capability to control system over time.

- ICS networks often use older operating systems, proprietary protocols, devices that aren't frequently updated, making them ideal targets.

- ICS environments use security tools and protocols designed for conventional IT environments that may not fully provide security to industrial environments.

1.5 APT Life-Cycle

According to Kaspersky, an evolving advanced persistent attack life cycle has been analyzed in 5 stages [9].

1. Gain Access
2. Establish a Foothold
3. Deepen Access
4. Move laterally
5. Look, Learn, and Remain

Gain Access Stage:

This stage involves attackers breaching the target network, usually by exploiting vulnerabilities across a number of fronts: older software, social engineering, or insecure configurations to delivering malicious software. The goal here is often to compromise

the system using malware, such as remote access trojans (RATs), or to utilize application vulnerabilities to gain an initial entry point. Techniques like spear-phishing or leveraging zero-day vulnerabilities are common in this phase.

Establish a Foothold Stage:

Once access is gained, the attacker works to set up persistent control. This is through establishing malware or malicious scripts that are designed to operate in the system environment without the owners of the system or security protocols detecting their existence. Some attackers install backdoors, network tunnels, or command-and-control servers in order to maintain access to the system. Advanced and well-developed malware is even capable of rewriting its code according to the environment, cloaking its presence, or hiding in legitimate system processes that allow the attacker to stay undetected longer. The intention here is one of persistence: even though the breach is detected by the authorized parties, the attackers have gained access through other entry points.

Deepen Access Stage:

In this stage, the attacker targets gaining a higher level of privilege, often targeting administrator information and credentials to control critical parts of the system and restricted parts of the system to normal users. They might employ password cracking strategies, further exploration of vulnerabilities, or the use of privilege escalation methods to increase their control and user level. The attacker will be able to bypass many of the security measures that are in place with the aid of administration-level permissions and expand access throughout the network. In this administrative access, an attacker is allowed to monitor activity, manipulate data, or disable established security features of a system in preparation for further exploitation.

Move Laterally Stage:

After deepened their access, attackers start moving laterally across the network, accessing other servers, databases, or areas of the network that are segregated or more secure. By moving laterally, attackers have access to valuable data that wasn't available in previous stages. Using stolen credentials or other compromised systems, they spread malware, researching for additional vulnerabilities and invade other high-value areas of the network, including confidential and sensitive databases and financial systems.

Look, Learn, and Remain Stage:

In the last stage, the attackers are already fully knowledgeable about the ICS environment and can execute their objectives in a manner likely to be effective through data exfiltration and manipulation of critical areas of the systems. Long-term attacks are normally constituted where attackers access confidential and sensitive information, intellectual property, or internal on-going information over time. The attackers may also leave backdoors so as to return at later stages when it may be difficult for the organization that is authorized to eliminate the threat fully. Sometimes, attackers can also keep their presence for several months or years, continuing to harvest data while appearing dormant or inactive.

In order to minimize the damage which is caused by the APT attacks, parallel security measures are taken along with the progressive attack evolution tactics applied against the Industrial Control Systems. The classifications and advancements in detection mechanisms will be further touched in the evolution of this topic.

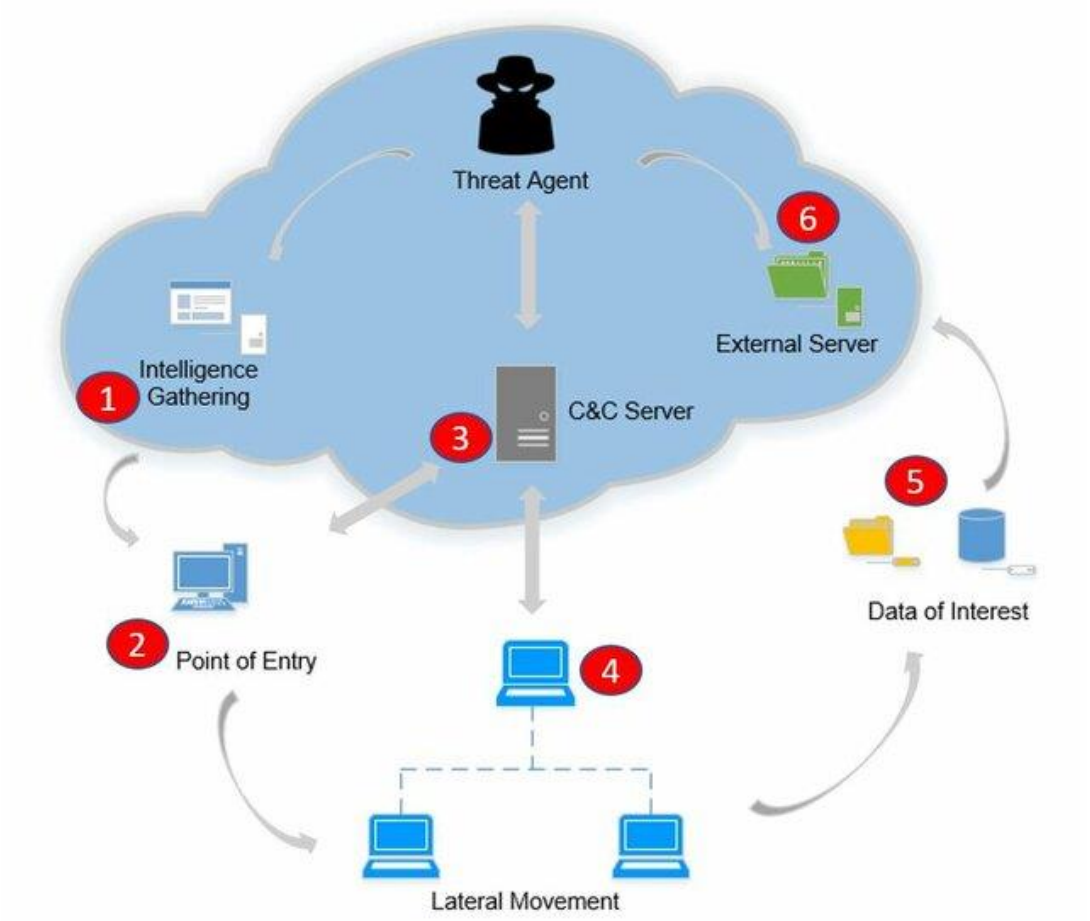

Figure 1.2 Typical stages of APT attack [16]

2 Evolution of the topic

2.1 History and evolution of APT attacks

The term Advanced Persistent Threat was not created to be a generic label for all cyber threats but was, in fact, developed to identify certain state-sponsored groups operating in the Asia-Pacific region in targeted attacks under the direction of the U.S. government. The term "Advanced Persistent Threat" was coined by the USAF in 2006 for naming these sophisticated cyber threats with a common language to communicate to counterparts in the unclassified public domain. Over time, the term has morphed and today is loosely used by marketers and media as a general term to describe almost everything related to cyber threats and has thus lost its original specificity and context [14].

With the first generation of cyber threats, only a few systems were compromised, since the number of devices using the Internet was still at a low count. Even then, however, governments were also conducting cyber espionage by targeting each other with these up-and-coming online capabilities.

The first of these cases to be documented publicly is described in Clifford Stoll's book, The **Cuckoo's Egg**. The story tells the tale of a West German hacker, Markus Hess, who, in 1986, broke into a computer at the Lawrence Berkeley National Laboratory while working for the Soviet KGB. Stoll's story not only illustrated just how vulnerable those times were but also foreshadowed complexities and implications of state-sponsored cyber activities that would evolve over the next decades [14].

At the turn of the century, it was discovered that there was a whole series of coordinated attempts to hack into U.S. government websites, all part of an attack codenamed **Moonlight Maze**. These attacks, which had been running undetected for almost two years, included systems at such high-profile institutions as the Pentagon, NASA, and the U.S. Department of Energy, plus several universities and research laboratories working on military-related projects. Events that actually took place are considered by some experts to be one of the first major examples of an APT, although the term itself was not in common usage then.

These Moonlight Maze attacks stole tens of thousands of files containing sensitive information with details like maps of military installations, troop configurations, and designs of military hardware. The financial losses from these intrusions were estimated to run into millions of dollars. Investigators were able to trace these attacks to a mainframe computer in the former Soviet Union, but the Russian government maintained it had nothing to do with these activities. Speculation has remained that this stolen information could then have been sold to the highest bidder, showing the possibility of major geopolitical consequences emanating from cyber espionage [14].

Starting around 2006 but until recently rediscovered, an Advanced Persistent Threat manipulated the breach in the collection and stealing of sensitive secrets and intellectual property, including critical information regarding design, finance, manufacturing, and strategic planning [14]. **Sykipot** attacks often use spear-phishing methods, laced emails with malicious attachments or links to compromised websites combined with zero-day exploits to compromise targeted systems. The Sykipot attacks have been quite broad-the malware has been used to compromise several companies throughout the United States and the United Kingdom within the computer, telecommunications, energy, chemicals, and government sectors, among others. In 2011, research by AlienVault Labs demonstrated that many of the command-and-control servers were based in China. Furthermore, considering the nature of the specific targets and the type of information gathered, the likely beneficiary was an intelligence agency [14].

2.2 Different types of APT attacks on ICS over time

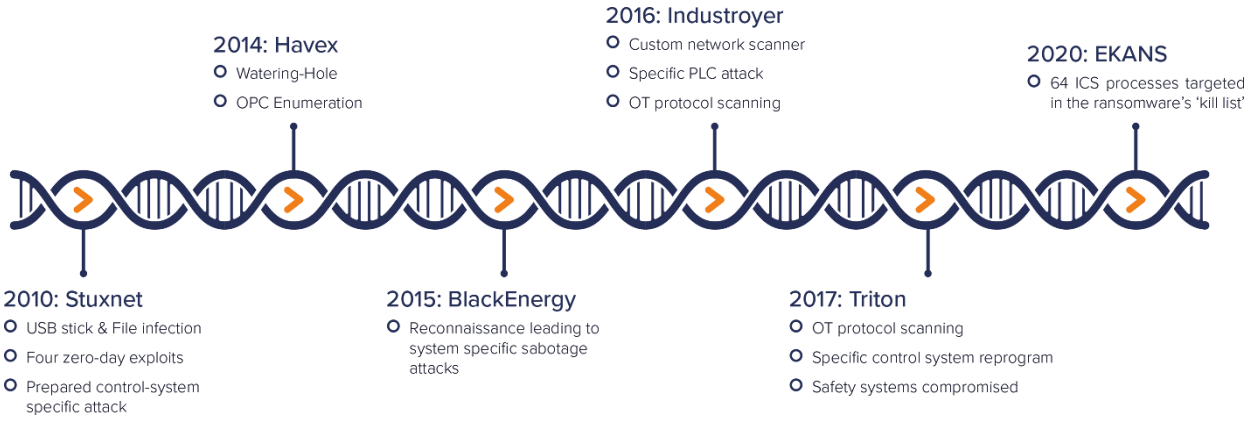

Figure 2.2 An overview of distinctive methods used in attacks against industrial environments [17].

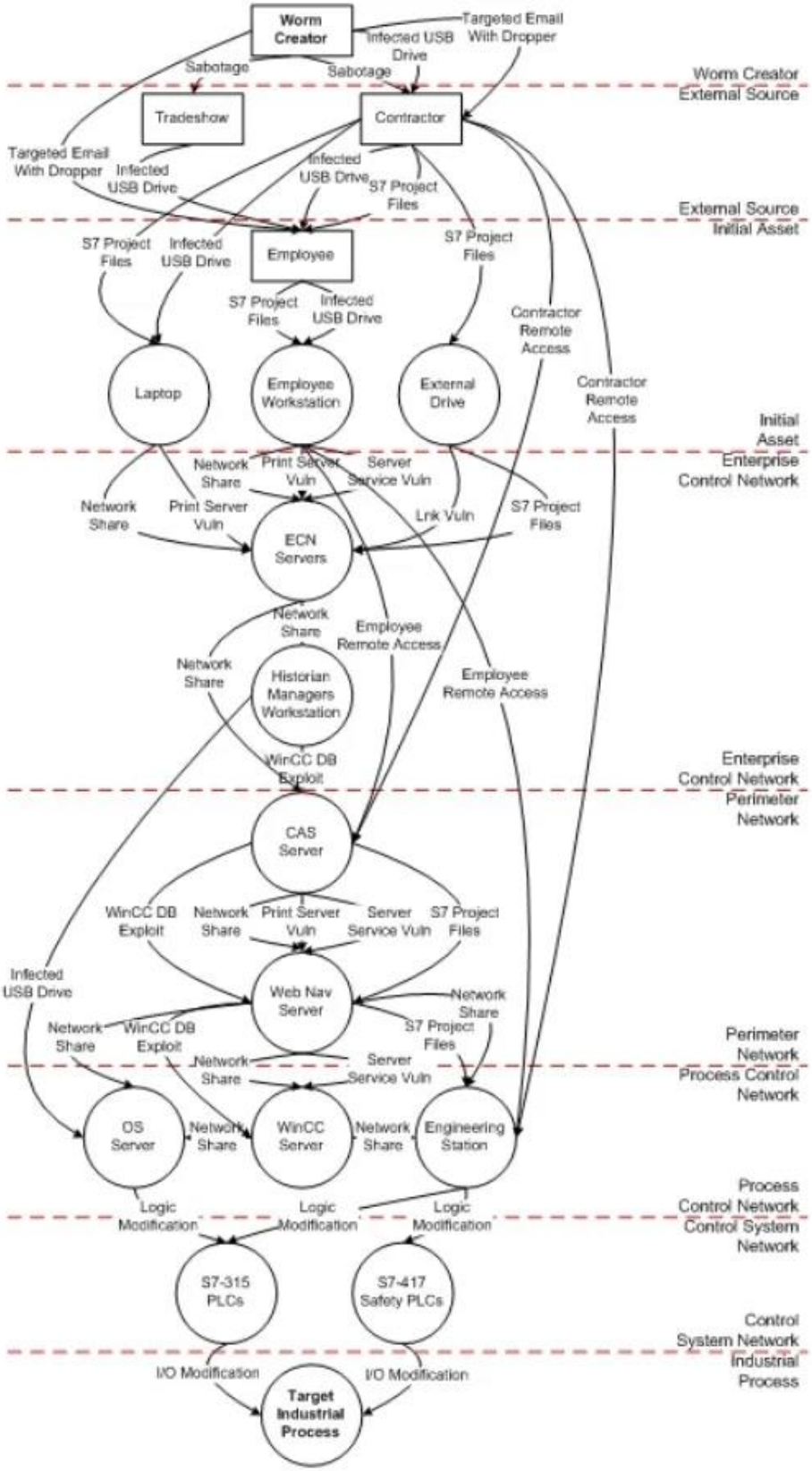

Figure 2.3 Stuxnet attack graph [18].

2010 - the International Atomic Energy Agency's inspectors who were present at the Iranian Natanz uranium enrichment facility reported that the centrifuges which were in use to enrich uranium gas were breaking down at an astonishing level [19]. The reason was a total enigma - seemingly to the Iranian engineers fixing the broken centrifuges as much as the inspectors watching them. Five months down the line, another even took place that appeared to be entirely unrelated. A Belarus computer security company had to be recalled to assist in resolving an issue of series of computers in Iran which were misbehaving and crashing numerous times [20]. Once more, the source of the problem was also a mystery. Which was the case until when a couple of malicious files were discovered on one of the systems and the first cybernetic weapon was uncovered. **Stuxnet**, as it came to be known, was different from any other computer virus or worm that had been developed before [20]. Most computer viruses and worms would merely use targeted terminals, or try to extract some amount of data with the help of those terminals. It, however, was able to leave the confines of the cyber world and cause actual damage to the hardware that the targeted computers controlled.

2014 -**Havex** Advanced Persistent Threat (APT) attack has maliciously penetrated industrial control systems (ICS) primarily in the energy, defense and manufacturing sectors. The group 'Dragonfly' or 'Energetic Bear' has been linked to the Havex attacks, which are suspected to be state-sponsored with ties to Russian nationals. The attackers deployed spear-phishing, watering hole and trojanized updates to propagate across the networks [21].

Once breached, the hack commanded the release of Havex malignant software to siphon off Information from ICS and SCADA systems that are meant to regulate industrial activities. One of the defining features of Havex was its ability to perform reconnaissance on target ICS devices within a network and provide the necessary information to the user in order to compromise them.

2015 -The **BlackEnergy** group, which has been associated with cyber assaults against the energy sector of Ukraine, is one of the cases that have been chronicled of disruptive cyber activities leading to massive power blackouts [22]. The viruses were contained in spear-phishing messages which gave the attackers initiation into the industrial control systems (ICS) for the purpose of stealing data and disrupting operations. BlackEnergy's modular architecture enabled attackers to use different types of payloads for information gathering, destruction of equipment, or general surveillance. The 2015 Ukraine power grid attack, which affected power for hundreds of thousands, demonstrated the hands of several advanced persistent threats which target country's critical infrastructure, and also attacked information control systems [23].

2016 -**Industroyer** APT, managed to create a power outage in Kyiv, Ukraine to a great extent. State-sponsored actors most likely from Russia are said to be behind Industroyer, which was purposefully created to go after industrial control systems (ICS) or SCADA systems found in places such as power grids. Its most unique component was that it could talk to industrial based protocols, namely IEC 60870-5-101 and IEC 61850, and the likes in order to give out commands to obstruct business processes [24]. Consequently, the malicious tool was able to induce blackouts, vandalize hardware, and eliminate evidences by utilizing inkcap features, which made any attempts for reinstatement almost impossible. Industroyer indicated how cyberattacks became even more threatening for the vital systems, and articulated the necessity for improving av protection as the threats were becoming more advanced.

2017 -**Triton** APT, which has appeared under the both the labels "Triton" and "Trisis," has its main targets set on safety instrumented systems (SIS) used within industrial settings. It is connected with a cyber onslaught against the Saudi petrochemical plant, whose primary weapon was the malware that attempted to sabotage the plant's protective measures, thus directly endangering human life and the plant's operations. Triton attacks weaknesses found in Triconex systems that are designed for the execution of safety-critical operations [25].

2020 - **Ekans** APT is a specific form of a ransomware targeting industrial control systems (ICS) only. It is thought in the industry that it is a product of the team connected to the Russian speaking hacker's community. Many aspects of Conti are present in the way that Ekans not just performs file encryption attacks, but it also exterminates the processes running several ICS and SCADA systems which could paralyze the operations of critical sectors such as manufacturing and power supply [26]. The malware is usually disseminated via phishing campaigns, and exploits flaws in the network security. Attacking industrial systems, Ekans represents the emerging wave of ransomware targeting rehabilitation of critical services and draws serious attention towards the importance of safety in such services for the economy, as well as for the operational performance.

2.3 Challenges in APT Detection and Mitigation in Industrial Control Systems

The detection and mitigation of Advanced Persistent Threats poses a challenge that is distinct from others mostly because of the complexities that are associated with these threats. This is a problem because such threats use complex methods of operation to avoid exposure and thus it becomes impossible for the companies affected to detect and take action against their threats.

1. Stealth Techniques: APTs are very sophisticated and therefore very hard to detect using the standard security layers due to their tactics of advanced evasion.
2. Persistence: The long-term nature of APTs means that it is not easy to completely wipe out even when spotted.
3. Adaptive Behavior: Tactics of APT actors change as the defenses improve.
4. Resource Intensity: Considerable expenditure of resources in technology and skilled manpower is required to effectively contain an APT.
5. Supply Chain Vulnerabilities: As seen from attacks such as the SolarWinds attack, APTs are able to abuse the trust to defend against attacks, using legitimate software and software updates and avoiding many security measures.

Understanding these challenges is crucial for developing and implementing effective detection techniques and mitigation strategies, which are discussed in the next sections [27].

2.4 APT detection techniques in ICS environments

While it continues to rapidly evolve, industrial control systems have become the preferred targets of APTs from very sophisticated attackers. Minimizing these risks requires the focus of prevention through early identification of vulnerabilities and effective security measures that impede APTs from taking their toll.

A. **Network- based Detection Methods –** Network-based detection mechanisms trace all network traffic to help look out for certain anomalies or suspicious patterns. Their target includes behaviors that are out of the norm, such as when there is an external server being contacted while this was not the case, or when data is transferred in bigger amounts to those on the outside, which is usually dangerous and may be a hint at an APT. This therefore enables the organization to work with threats as they appear and get filtered through the entire network of the organization.

1. **Traffic Analysis and Anomaly Detection**

This approach is the process of effecting standards of normal network activity and deviation from the normal baseline to try and flag APT activity.

2. **Deep Packet Inspection (DPI)**

DPI goes deeper than network header information and looks for known threats embedded within network packets or any suspicious behavior.

3. **NetFlow Analysis**

NetFlow analyzed data gives an overall view of a network with traffic that comes in and out of the network and helps figure out the usual communication behavior inside the network.

B. **Host-based Detection Methods –** Host-based detection techniques, on the other hand, work on single endpoints and estimate the attributes of the system in order to detect system misuse. These approaches are able to monitor any access to files, creation of processes and actions by users to expose where even the slightest change has occurred or malware is present. This helps in ascertaining the possible reach of APT activities toward endpoints ensuring better measures are in place.

1. **Endpoint Detection and Response (EDR)**

   EDR systems record and treat information with regard to what routine the endpoint performs in order to find and remove the threat.

2. **User and Entity Behavior Analytics (UEBA)**

   UEBA systems establish baselines of user behavior with the help of normal patterns of user behavior and other metrics; deviations from these patterns indicate a possible breach.

3. **File Integrity Monitoring**

   This strategy focuses on ensuring that critical program files and configurations are not altered without permission

C. **Log-based Detection Methods –** Log-based detection techniques use the assessment of certain windows and/or application logs to find the cause of any aberrant or suspicious behavior. Following particular motifs, associations and outliers of the recorded data can also bring certain APT activities to light. This allows a more nuanced view of the assaults for crime investigations as well as improving crime fighting techniques.

1. **Security Information and Event Management (SIEM)**

   SIEMs detect security incidents by aggregating and correlating security incident logs from various sources.

2. **Log Correlation and Analysis**

   This includes a review of the set of logs captured from different sources in order to establish a series of events related to APT activities or any other malicious activity.

D. **Machine Learning and AI-based Detection** - Zone systems offer detection based on machine learning and AI, which aims to examine large data volumes in search of APT patterns. Because of the historical data, the systems are also able to detect advanced threats and small-scale anomalies that span for a long period of time. This is important as it partially resolves the issue of enhancement of detection and response times in dealing with sophisticated attacks such as an APT.

1. **Supervised Learning Approaches**

These approaches train systems to recognize known APT tactics and activities, using labeled datasets.

2. Deep Learning Models for APT Detection

Techniques such as recurrent neural networks (RNNs) and convolutional neural networks (CNNs), which fall under the category of deep learning, have been utilized for the detection of APT attacks in the recent years, and particularly for the tasks that involve time-series data, like network traffic.

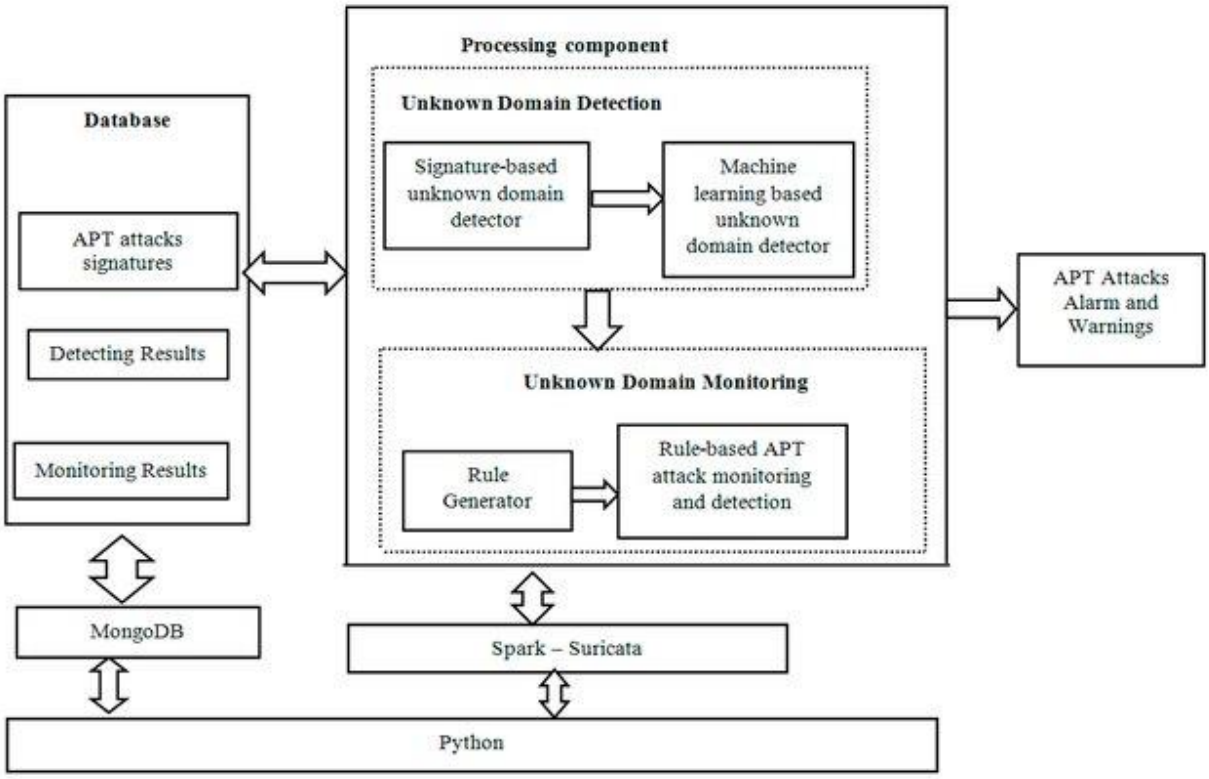

Figure 2.4 Solution architecture of APT attack detecting and monitoring component.

2.5 APT Mitigation Strategies in ICS Environments

Successful mitigation of Advanced Persistent Threats (APTs) demands a multilayered approach: prevention, detection, and response. This section looks at the consideration of key strategies in defeating the APTs and emphasizes how an integrated approach to these tactics formulates a sound security strategy.

Strong Authentication Mechanisms

Creating and implementing effective authentication strategies can prevent any unwanted access and safeguard accounts from being compromised. Multi-factor authentication (MFA) should be used, privileged access management (PAM) should be carried out, and regular password audits should be conducted to reinforce the security levels.

Regular Patching and Vulnerability Management

Update the information systems and application software to remediate the known exploits that advanced persistent threats (APTs) may utilize. Implement regular support patching procedures; employ patch management tools to discover and make corrections to sequenced levels of threat exposure within the system.

Continuous Monitoring and Threat Hunting

Actively looking for the threat indicators (IoCs) and abnormal behavior can help in APT spotting early enough before they cause a lot of damage. Implement security information and event management (SIEM) systems; recruit a specialized threat hunting group.

Deception Technologies

Deploying honeypots, honeyfiles, and other deception techniques can lure and detect APT actors. Set up decoy systems and fake data that mimic production environments [27].

Incident Response Planning and Automation

The importance of an incident response strategy that is definitive and frequently rehearsed is even more pronounced where APT threats are concerned. Create and modify as necessary

incident response strategy documents; incorporate the use of Security Orchestration, Automation and Response (SOAR) technologies.

Security Awareness Training

Systematic training sessions enhance the ability of the personnel to detect and escalate possible APT attempts. Regularly practice social engineering tactics; place and train specific individuals in different departments on security issues.

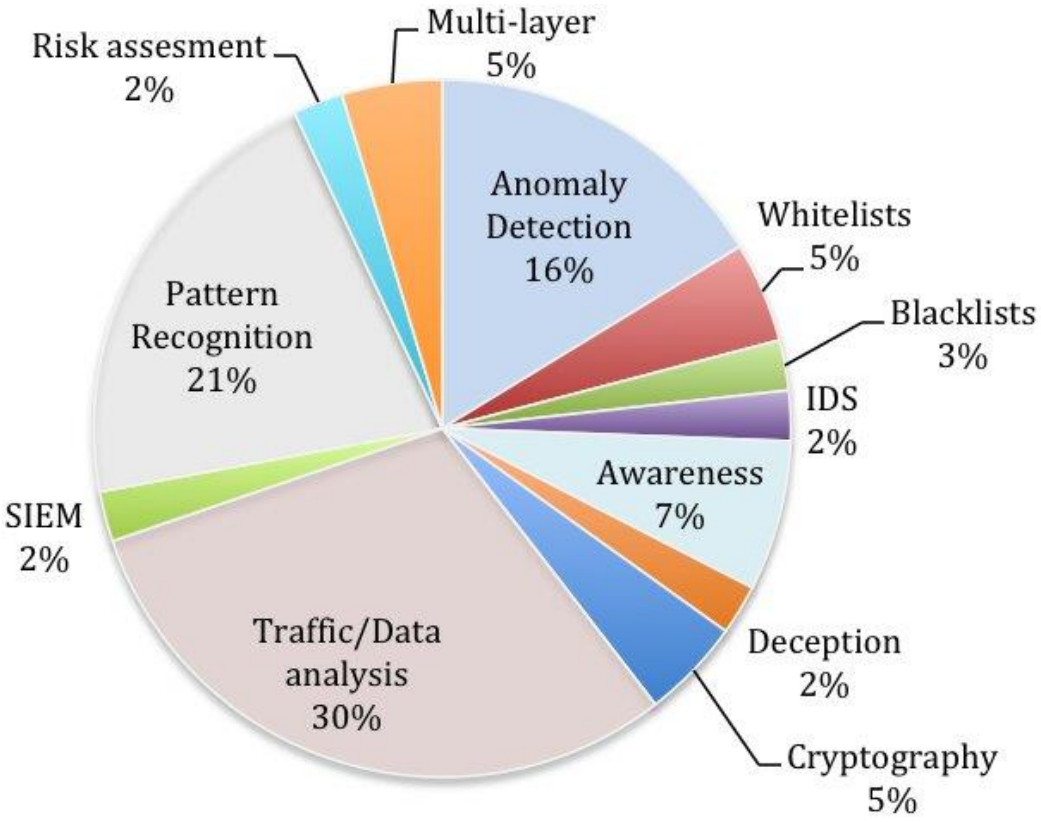

Figure 2.5 Pie chart showing Mitigation Techniques Used against APT by 25 researchers [28]

3 Future Developments in the area

Future APT attacks against ICS installations are going to be bleak, with cyber criminals adapting to growing digitization and interoperability in industrial environments. As sectors like manufacturing and transportation continue to adapt to newer technologies, they are widening their attack surfaces and becoming more proximate to the doorsteps of the APTs.

Experts predict a further rise in APT activities that will affect targeting of industries such as agriculture, logistics, pharmaceuticals, and high-tech sectors. The trend has broadened to include not only traditional targets-such as infrastructures serving military and government institutions-but also the more recent ones [29]. This development in using cloud services because of operational efficiency is considered the necessary evolution in ICS, yet with new vulnerabilities [30]. The reliance on third-party cloud solutions opens up an organization to risks if such services are using inadequate security measures.

Recent developments bring out several key trends that shape the future of APT threats:

Quantum Computing Threats and Countermeasures - Quantum computing could even break current cryptographic protocols, thus providing new challenges to ICS. Researchers are working on the development of quantum-resistant encryption methods that would help keep critical infrastructure safe from APTs, should they leverage quantum computational power for the decryption process or network infiltration [31].

Use of AI and Generative Technologies – APT attack groups are using generative AI to further enhance phishing campaigns. Such tools enable the automatic generation of highly convincing spear-phishing emails, whereby adversaries can conduct initial network access by deceiving a person so much more easily. The more an organization uses AI technologies themselves, the more they may be creating new vectors through which APT actors will attack them [32].

Focus on Managed File Transfer (MFT) Systems - Due to this critical role of transferring sensitive data, there has been an increasing trend in the targeting of APT actors at the systems of Managed File Transfer [32]. Their complex architectures contain a lot of vulnerabilities that, upon exploitation, result in data breaches. Although MFT solution adoption is being

carried out for securing data transfers among organizations, it is time for the implementation of robust security controls over these systems to save them from APT attacks.

Enhanced Espionage Tactics - The APT actors keep evolving their tactics to create automations for cyber-espionage activities. In keeping with the core of intelligence gathering, this would also include monitoring online presence through social media and public platforms for such victims to facilitate more targeted attacks [32].

Emerging Threats from New Technologies – The integration of new technologies, such as IoT devices, are being brought into the environment of ICS, further increasing the attack surface that APT groups can leverage. Many of these devices have limited security features, thus becoming a very attractive target for attackers who would like to infiltrate critical infrastructure [33].

In addition, future developments in APT defense for ICS will focus on AI-driven threat detection, Zero Trust architectures, and the reinforcement of cybersecurity policy in order to improve resilience against sophisticated attacks.

4 Conclusion

With the tremendous growth of industrial technology towards concepts of smart manufacturing, the application of Industrial Control Systems or ICS has also expanded manifold. Correspondingly, the effects of their growth attract the attentions of cybercriminals also, which led to higher risks of Advanced Persistent Threats or APT. Advanced Persistent Threats are a kind of sophisticated and persistent cyber-attack specifically designed to infiltrate critical infrastructure that remain mostly undetected for a longer period of time.

The ICS environment is especially vulnerable due to antiquated systems, lack of ongoing security patches, and prioritization of operational efficiency over cybersecurity. This in turn gives the cybercriminal opportunities to exploit whatever exposed weakness they can, resulting in the eventual execution of damaging attacks, which could be anything from espionage and data theft right through to physical equipment destruction.

Various aspects have been discussed throughout this report, from the entrance vectors taken by the attackers to the lifecycle of APTs and threat detection and mitigation challenges of APTs against ICS. To be more precise, network-based techniques are found to be very effective in anomaly tracking, while host-based techniques are helpful in the detection of malicious activities at the endpoint level.

The report further emphasizes that active measures of constant monitoring, patch management, and detection systems would keep away such threats. Further ahead, integrations of AI-driven threat detection systems, Zero Trust architectures, and robust security policies will empower the development in APT defense to safeguard critical infrastructure against those evolved attacks.

According to my point of view, the following are some security recommendations that might be fundamental in hardening the security of ICS:

- Improve multi-factor authentication and privileged access management.
- Apply security patching and updates to reduce the vulnerability of ICS devices and systems.
- Enforce the concept of least privilege using zero-trust architectures while securing sensitive systems.
- Regular security awareness training for the staff enables better threat identification, such as phishing attempts or social engineering.

Finally, we have to concern more focus on evolving long-term prevention strategies to stay ahead of rapidly changing APT tactics and improving the overall resilience of ICS environments against future attacks.

Note: Here 5033 words have been covered regardless of references. While 5611 words were covered including references (Decided to ignore words of references).

5 References

[1] Suraj Gujar, “Industrial Control Systems (ICS) Market Size, COVID-19 Impact Analysis, Regional Outlook, Application Development Potential, Price Trend, Competitive Market Share & Forecast, 2024 – 2032,” Global Market Insights Inc., Apr. 15, 2024. https://www.gminsights.com/industry-analysis/industrial-control-systems-market

[2] “Industrial Control Systems Market Analysis - Industry Report - Trends, Size & Share,” www.mordorintelligence.com. https://www.mordorintelligence.com/industry-reports/industrial-control-systems-market-industry

[3] Ayça Gül, “Industrial Control Systems Attack and Security Measures,” Medium, Jun. 23, 2024. https://medium.com/@aycagl/industrial-control-systems-attack-and-security-measures-4275796c300d .

[4] “What Is ICS (Industrial Control System) Security?,” Fortinet. https://www.fortinet.com/resources/cyberglossary/ics-security

[5] R. Kumar, R. Kela, S. Singh, and R. Trujillo-Rasua, “APT attacks on industrial control systems: A tale of three incidents,” International Journal of Critical Infrastructure Protection, vol. 37, p. 100521, Jul. 2022, doi: https://doi.org/10.1016/j.ijcip.2022.100521.

[6]T. M. McGowan, "The Evolution of Industrial Control Systems: A Historical Perspective," IEEE Industrial Electronics Magazine, vol. 5, no. 1, pp. 18-27, Mar. 2011. doi: 10.1109/MIE.2011.941835.

[7]B. Lenaerts-Bergmans, “Advanced Persistent Threats (APTs) | Definition & Examples,” crowdstrike.com, Jun. 15, 2022. https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/

[8]J. Ledesma, “What is an APT?: Advanced Persistent Threat Overview | Varonis,” Varonis.com, Dec. 08, 2021. https://www.varonis.com/blog/what-is-apt#works .

[9]Kaspersky, “What Is an Advanced Persistent Threat (APT)?,” Kaspersky.com, 2024. https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[10]Amci, “AMCI : Advanced Micro Controls Inc :: What is a PLC?,” Amci.com, 2017. https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/

[11]“What is a programmable logic controller (plc)?,” [On-line]: http://www.wisegeek.org/what-is-a-programmable-logic-controller.htm.

[12]T. Frost, “What is a DCS?,” Schneider Electric Blog, Jan. 30, 2024. https://blog.se.com/industry/2024/01/30/what-is-a-dcs/

[13]P. Loshin, “What is SCADA (supervisory control and data acquisition)?,” WhatIs.com, Dec. 2021. https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition

[14]“CyberSecurity: Origins of the Advanced Persistent Threat (APT),” Dr.Shem, Oct. 08, 2015. https://drshem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/

[15]Packt-cdn.com, 2024. https://static.packt-cdn.com/products/9781788395151/graphics/8c3628fb-c3b4-48a9-8404-911d362c3004.png (accessed Oct. 05, 2024).

[16]M. A. R. A. Amin, S. Shetty, L. Njilla, D. K. Tosh, and C. Kamhoua, “Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement,” IEEE Access, vol. 9, pp. 49662–49682, 2021, doi: https://doi.org/10.1109/access.2021.3069105.

[17]“How Cyber-Attacks Take Down Critical Infrastructure | Darktrace,” Darktrace.com, Jul. 07, 2021. https://darktrace.com/es/blog/how-cyber-attacks-take-down-critical-infrastructure .

[18]gHale, “Stuxnet Report V: Security Culture Needs Work - ISSSource,” ISSSource, Mar. 24, 2011. https://www.isssource.com/stuxnet-report-v-security-culture-needs-work/ .

[19]Kaspersky, “Stuxnet explained: What it is, who created it and how it works,” www.kaspersky.com, Apr. 19, 2023. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

[20]K. Zetter, “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon,” Wired, Nov. 03, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[21]Loubna IZIKA, “Understanding Havex Malware: A Threat to Industrial Control Systems,” Medium, Jan. 03, 2024. https://medium.com/@loubnaizika/understanding-havex-malware-a-threat-to-industrial-control-systems-2f2bcf092cc2 (accessed Oct. 11, 2024).

[22]“What is BlackEnergy Malware? | Security Encyclopedia,” www.hypr.com. https://www.hypr.com/security-encyclopedia/blackenergy

[23]“BlackEnergy, Software S0089 | MITRE ATT&CK®,” attack.mitre.org. https://attack.mitre.org/software/S0089/

[24]ESET Research, “Industroyer2: Industroyer reloaded,” WeLiveSecurity, Apr. 12, 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

[25]“Trellix,” Trellix.com, 2022. https://www.trellix.com/blogs/research/triton-malware-spearheads-latest-generation-of-attacks-on-industrial-systems1/

[26]“Ekans ransomware: features and operation | INCIBE-CERT | INCIBE,” Incibe.es, 2020. https://www.incibe.es/en/incibe-cert/blog/ekans-ransomware-features-and-operation (accessed Oct. 11, 2024).

[27]V. Malik, A. Khanna, N. Sharma, and Suryaprakash nalluri, “Advanced Persistent Threats (APTs): Detection Techniques and Mitigation Strategies,” Aug. 2024, doi: https://doi.org/10.21428/e90189c8.91e89a3e.

[28]Adelaiye, Oluwasegun & Ajibola, Aminat & Silas, Faki. (2019). Evaluating Advanced Persistent Threats Mitigation Effects: A Review.

[29]S. Williams, “Kaspersky predicts shifts in threat landscape to industrial control systems in 2023,” SecurityBrief Australia, Nov. 24, 2022. https://securitybrief.com.au/story/kaspersky-predicts-shifts-in-threat-landscape-to-industrial-control-systems-in-2023 (accessed Oct. 12, 2024).

[30]R. Machtemes, “New Report: Cyber Security Threats in Manufacturing Industry,” Waterfall Security Solutions, Jul. 2024. https://waterfall-security.com/ot-insights-center/manufacturing/2024-threat-report-manufacturing-takeaways/

[31]P. K. V, “Why is Chinese threat actor APT 41 in a tearing hurry?,” Security Boulevard, Sep. 30, 2024. https://securityboulevard.com/2024/09/why-is-chinese-threat-actor-apt-41-in-a-tearing-hurry/ (accessed Oct. 12, 2024).

[32]C. Pernet, “Kaspersky’s Advanced Persistent Threats Predictions for 2024,” TechRepublic, Nov. 20, 2023. https://www.techrepublic.com/article/kaspersky-advanced-threat-predictions-2024/

[33]GReAT, “APT trends report Q2 2024,” Securelist.com, Aug. 13, 2024. https://securelist.com/apt-trends-report-q2-2024/113275/ (accessed Oct. 12, 2024).