# Comprehensive scrutiny of threat vectors leading to attacks in ICS

Mufaddal Masalawala[a], Simran Sankhala[b] and Gayatri Laxman Nayak[c]

[ab]*Associate Security Consultant, SecurView, Inc.*
[c]*Associate Security Consultant, Aujas Cybersecurity Private Ltd.*

**Abstract**

Industrial Control System such as SCADA and DCS are exclusive designed to monitor and control critical infrastructures such as power generations and distribution plants, gas and oil refineries, nuclear plants etc. Recently, huge spike in ICS attacks have been observed on the internet reachable ICS devices which lack appropriate security measures. The objective of this paper is to study and deduce the most recurrent threat vectors of the past ICS attacks. This study is expected to be a useful reference to implement best practices and policies by the industries to prevent future attacks.

**Keywords 1**

Industrial Control System, SCADA, ICS attacks, ICS threat vectors, ICS attacks prevention strategies.

## 1. Introduction

Industrial control systems (ICS) are a collection of devices, systems, networks, and controls used to operate and automate the industrial process. ICS are functional in different industrial sectors and critical infrastructures such as the transportation, manufacturing, and water treatment industries. The two prominently used ICS are Distributed control systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. The local operations are remotely controlled using Field Devices that receive supervisory commands.

ICS systems have faced multiple threats with varying units of potential loss. From noncompliance to disruption of operations, which may result in potential loss of a user and destruction of property. Examples of ICS related threats include Advanced Persistent Threats (APT), hacktivist attacks, insider sabotage, catastrophic human error, coordinated physical & cyberattack, supply chain disruption or compromise, unintended spillover of corporate network compromises disruption of voice & network data services, distributed denial of service.

ICS security researchers are anxious about the systemic lack of authentication in designing, operations, and unsecure deployment of current ICS systems. A compromised system that monitors an HMI/ inventory represents a different risk than monitoring or managing interface of a temperature control system. Some of the issues include infrequent rules for patching and updating control systems, out-of-date firmware, hardware, and operating systems. ICS devices make it easy for hackers to set up persistent bridgeheads into target networks for information filtering, command injection, protocol exploitation, and other technical attacks [1].

The goal of the CIA triad is to ensure confidentiality, integrity, and availability which are considered pillars of information security. Information security prevents valuable information from

WCES-2021: Workshop on Control and Embedded Systems, May 01, 2021, Chennai, India.
EMAIL: gayatrinayak1456@gmail.com (Gayatri Laxman Nayak)
ORCID: 0000-0002-3679-8793 (Gayatri Laxman Nayak)

unauthorized access, modification, and distribution by following the CIA Triad. However, ICS security prioritizes the availability of industrial processes because downtime of ICS can impact the productivity of industries resulting in financial loss, data loss and potential risk to human lives. Thus, Confidentiality has a lower priority in the industrial control system as they mainly focus on Availability.

The rest of the paper is structured as follows. First, section 2 provides an overview of miscellaneous threat vectors in industrial control system. Next, Section 3 describes the analysis of distinct ICS attacks, including details on the impact, methodology, and threat vectors exploited in the ICS attack. Subsequently, section 4 presents evaluation of results and an analysis of recurrent threat vectors in ICS. Finally, section 5 gives summarized conclusion of the study.

## 2. Miscellaneous threat vectors in Industrial Control System

According to our research, the ICS infrastructure is exposed to various cyberattacks which cause damaged equipment, operational shutdowns, intellectual property theft, financial loss, and substantial health and safety risks. The attackers gain access to an industrial network by exploiting various threat vectors in the IT infrastructure to disrupt the ICS operations. They mainly take advantage of known vulnerabilities to exploit the target. Hence, it is important to know about existing vulnerabilities [2][3] in ICS components to take appropriate protective measures and risk assessment.

This section outlines most prominent threat vectors observed in the ICS systems.

## 2.1. Security Misconfiguration

### 2.1.1. Data transmission in plain text

Some ICS devices provide a web interface that supports both HTTP (plain-text, not secure) and HTTPS (encrypted) for remote connections. Majorly, the ICS server uses HTTP, which allows any attacker to capture credentials in plain text who has access to the connection between client and server. Tools like Wireshark are publicly available to perform network sniffing that could be used to exploit this vulnerability. An attacker with this information can easily build a database of admin credentials linked to the company that owns the device. Hence, the network channel communication should always be encrypted, and HTTPS supported [2].

### 2.1.2. ICS protocol uses weak integrity checks.

If an attacker has reverse-engineered ICS network communication protocols and has access to ICS communication paths, then it is possible to manipulate data flowing between system components. This data includes alarms, and command messages sent to an operator screens and control field equipment. This could out-turn trick the operator into performing unusual actions or hiding malicious actions. The checksum in a protocol act as the initial layer of security to check for data integrity. To mitigate this, data integrity checks should be implemented in ICS protocol communications. Monitoring the network using an Intrusion Detection System (IDS) can help detect man in the middle (MitM) attacks. It is also recommended to add a checksum to the protocol and switch to a more secure alternative protocol or to use an encrypted channel to transfer the data [2].

### 2.1.3. Lack of host configuration procedure

ICS hosts are not properly configured which exposes them to various vulnerabilities that are exploited and leveraged by an attacker. This is due to a lack of proper configuration documentation which details step by step installation, patching, and configuration of OSs, applications, libraries, and services. A documented procedure must be created for ICS components [3].

### 2.1.4. Lack of rate limiting

Rate Limiting is required to maintain the incoming and outgoing traffic by a network interface. It allows an individual to limit the request attempts in a set time frame. Rate limiting is important to increase the efficiency and decrease the end to end latency over ICS systems. An attacker can pass all possible combinations of credentials to guess usernames and passwords. Lack of rate limiting could make a network unresponsive or unavailable for some time. Client side and server side rate limiting is implemented to allow the data flow in a balanced way to reduce the possibility of a DOS attack [2].

### 2.1.5. Lack of system hardening

Initially, attacker's recon as much information they can by enumerating services, intercepting requests, etc. Use of default configurations, login information hardcoded into the script, displaying verbose errors, lack of hardening for e.g. null sessions left enabled/ DEBUG mode set to true, etc. all results in security misconfiguration. This will further facilitate the attacker to carry out severe attacks by directly exploiting specific features. To mitigate this, any unused features should be removed, and services should be hardened to the best security possible [2].

### 2.1.6. Lack of access control list restriction

An ACL allows you to control the flow of packets for multiple IP addresses or various protocols, such as TCP, UDP, ICMP. ACL contains a list of rules that categorize packets and help you understand when to allow or deny any network traffic. The rules are applied on the interface to filter incoming and outgoing packets. It allows you to infiltrate the source and destination IP addresses, N/W layer protocol type, source and destination port, and other parameters. If the restriction on IP address has not been implemented, it may result in access to the other files and folders for which the user does not have permissions using find, browse, restore, and delete data operations. It is possible to restrict end-user access to common resources by enabling access control on the client-side data [2].

### 2.1.7. Lack of network segmentation

Network segmentation creates security zones that restrict an attacker to take full control of the systems which could otherwise lead to high-level consequences. Lack of secure network design could result in findings like corporate LANs directly accessing control-related systems, lack of internal segmentation of production network, lack of firewall rules. This could impact network DOS, unnecessary exposure, and unprotected attack paths. A firewall should segregate different ICS networks and a DMZ should be implemented to provide only limited data to any network if required. Network administrators should invest in a secure ICS network architecture diagram to know all connections to subnets, DMZs, and other internal and external networks [2].

### 2.1.8. Lack of proper authentication

Many ICS systems do not support features like encryption and password protection. Improper use of IT security practices in ICS may often hamper availability and timing disruptions. Authentication policies are required to define when authentication mechanisms like, systems might not have appropriate authentication controls, lack of passwords policy implementation, making unauthorized access to ICS systems more likely. There may not be computing resources available to modify these systems with current security capabilities. For example, in TFTP, no login is required at all and for FTP the login password is not encrypted. Taking advantage of no password, an attacker can log into the system and access all the information and system controls and could gain access to user accounts. Enforce secure authentication for all users attempting to gain access to the ICS system or network [2].

### 2.1.9. Sensitive data exposure

OSINT for critical infrastructure like ICS systems are used by groups who are interested in disrupting critical systems for monetary gain. Data which can be gathered during reconnaissance can reveal sensitive information about ICS systems such as ports, IP address, hostname, technology, and geolocation. Shodan provides information about internet-connected devices. Shodan could be used by adversaries to find configurations, vulnerable elements, and exploit tools to attack and gain access to industrial control systems. Attacks can be minimized by auditing the ICS devices by the asset owners, using isolated networks, active monitoring of network and infrastructure, maintenance of detailed inventory, and MFA [2] [3].

### 2.1.10. Unauthorized directory traversal allowed

Directory traversal vulnerability exists in all types of applications. In ICS system directory traversal may allow access to system configuration files and gain knowledge of system internal file structure. The recommendation to prevent directory traversal is to perform input validation on URL. Input should be decoded and converted into the system's internal representation before being validated [2][3].

### 2.1.11. Unauthenticated access to a web server

Attackers most commonly gain access to the web servers by exploiting vulnerabilities in ICS web services. Access control mechanisms are also not enforced correctly on every page at the server side for web applications. Authentication mechanisms are not enforced correctly on web servers. All such misconfiguration leads to unauthenticated access to a web server. Web applications should be completely tested for input validations and also make use of well-known, secured third-party web servers [2].

### 2.1.12. Use of vulnerable open network shares

The design of ICS requires open network shares on ICS hosts which results in the storage of ICS artifacts on a shared file system. An attacker can assess various findings by exploiting this feature like publicly available network shares on ICS hosts, information leakage through shared directories, source code of ICS, etc. The recommendation to prevent this vulnerability is the use of firewall rules that block access to file sharing ports, network segmentation and restricted read-write permissions to a minimum number of users [2].

### 2.1.13. Use of vulnerable components

Many modern architects/ developers use components such as frameworks or libraries readily available on the Internet which reduces their work and instantly provides intended functionality. The same applies to unpatched operating systems, services, applications in ICS hosts. This could then result in unauthorized access to ICS components which leads to code execution, DOS, or data loss. ICS systems should only include well-known and security tested components and update it timely [3].

### 2.1.14. Use of vulnerable remote display protocols

Most ICS protocols do not implement encryption. Thus, an intruder who has access to the network would be able to inspect and manipulate traffic. For this reason, the use of secure shell (SSH), hypertext transfer protocol secure (HTTPS), VNC, and simple network management protocol

(SNMP) v3 is strongly recommended for authentication and access to devices like HMI composing it. The implementation of secure protocols makes it difficult to detect the devices behind firewalls and control system networks. Providing them isolation from the sensitive network could lessen the chances of exploitation [3].

#### 2.1.15. Unencrypted non-proprietary ICS protocol communication

Use of advanced IT infrastructure and non-proprietary protocols have been implemented to centralize the control of field devices over the internet which exposes the present architecture, leading to exploitation of the entire network communication. Based on the current scenario, the security solutions (using cryptography implementations) have been proposed to protect the protocol (DNP3 /MODBUS/MQTT) communication. Prevention can be done by encrypting the communication and logically isolating network segments using virtual private network (VPN) and virtual local area network (VLAN) technologies [2].

#### 2.1.16. Weak encryption used in standard IT protocol

It is considered a security risk to allow unsecured protocols like HTTP, FTP, etc. as they are prone to traffic sniffing and modification. An authentication protocol like Kerberos, RADIUS, TACACS+ communicates information or data between the system performing authentication and the authentication server. Remote connections over the Internet should use an encrypted protocol, such as application server, VPN, Proxy servers, (SFTP) or HTTPS access, and authenticate using MFA to access the corporate network. Post connection, they should be re-authenticated at the control network firewall using a strong mechanism to gain access to the control network [2].

#### 2.1.17. Weak firewall rules

A firewall is used to segregate the ICS network to protect it against external attacks. Certain misconfigurations like direct connections of cables to ICS LAN, corporate, and ICS LANs bridged through the SSH server facilitates firewall bypassing for an attacker. A firewall should be properly configured to restrict access to all LAN segments except for necessary communications. A firewall should segregate the corporate and ICS network, and a DMZ should be implemented to provide only limited data to the corporate network. Firewall rules should be properly inspected to eliminate any weak rules which can be easily bypassed [2][3].

### 2.2. Authentication and authorization related threats

#### 2.2.1. Improper privilege management

This class of attack occurs when a user gets access to more resources or functionality than they are normally privileged to access. Attackers can perform malicious actions with more privileges than those intended by the administrator. Access to modules or functions should be properly defined for every user to avoid such unauthorized access [2] [3].

#### 2.2.2. Improper file permissions

Each file and directory belong to a selected user ID and group ID and features a set of permissions related to it. If the permissions are not set properly, an attacker could read or modify files or directories, execute any unauthorized code or commands, and crash or restart critical programs or files, which could potentially cause a Denial of Service. Some flaws in current ICS systems include allowing the hosts to read or overwrite files on other hosts, with no logging. Arbitrary file download, upload on ICS hosts, allowing the remote client to gain access and launch any process. ICS vendors should use the principles of least privilege and implement security measures like authentication and data integrity checks to prevent manipulation of firmware files and unauthorized physical access [2].

### 2.2.3. Lack of server side authentication

The application which authenticates users locally is an easy target to a skilled hacker who may modify values before being submitted to the server and bypass authentication. The ICS system becomes vulnerable to such attacks due to only client side validation of the HMI application credentials. Poor programming of the controller and client side validation of username and password for remote configuration makes the ICS system prone to these attacks. It is recommended. to perform duplicate checks if client side security checks are performed. Implementation of robust authentication by server or component which grant access to the application is preferred [2] [3].

### 2.2.4. Poor authentication in vulnerable web services

Vulnerabilities in web services used in ICS are often exploited to gain unauthorized access to the systems. Some common vulnerabilities related to authentication are poor or no login required to ICS HMI, login information saved client side, Kerberos authentication always succeeds, etc. ICS applications should use secure and well-known web servers. Web applications should be properly assessed for authentication bypass attacks [2].

### 2.2.5. Services running with unnecessary privileges

After some ICS installation, services are automatically started with the root privileges. The exploitation of any such service could allow an attacker to intrude in the ICS network and perform a privilege escalation to obtain full access to the exploited host. The recommended practice is to run a service with minimal privilege required. This can be done during the ICS design and implementation phase to reduce the window of exposure [2] [3].

### 2.2.6. Use of default credentials

Factory default software configurations often consist of simple, publicly documented passwords of ICS devices and appliances. Default credentials are used for the initial phase of testing, installation part, configuring various modules and operations. An attacker can easily gather passwords available in product documentation, compiled lists available on the internet and read me text file. An attacker with a basic understanding of the password and network access to a system can easily log in, usually with administrative or root privileges. It is essential to change default provided passwords and change the credentials along with restricting network access to critical systems [2] [3].

## 2.3. Physical security related threats

### 2.3.1. Lack of physical access control

Piggybacking and tailgating are the most common threat to the physical security of an ICS system. This scenario is observed when an intruder tries to bypass a security perimeter by following another person with or without his knowledge. The security measures at the entrance and exit, form the first line of defense against physical intrusion. Apart from the traditional implementation of access control devices, organizations can educate their employees to prevent piggybacking and tailgating [2].

### 2.3.2. Lack of port security

Oftentimes security is not properly configured on the network equipment that limits accessibility after an unauthorized physical access is obtained. An attacker could plug into the network which is behind the firewall and perform unauthorized actions while they have physical access to an unsecure port. Port security should be implemented, limiting the MAC address to fixed interfaces, disable unused interfaces are few recommendations to follow [2].

## 2.4. SSDLC related threats

### 2.4.1. Injections

Injection attacks occur when untrusted data is injected to a code interpreter through a form or data input to an interface. This could result in data loss, data manipulation, or security bypass through SQL injection, Code injection, etc. HMI and Data historians are most prone to such attacks. Validating/ sanitizing user-submitted data, the use of secure libraries/ frameworks, and assigning proper access rights are some common practices to prevent this issue [2].

### 2.4.2. Lack of input validation

Applications usually assume that the input received from the user is secure and hence does not perform proper validation. This results in a buffer overflow attack wherein the attacker enters large, or negative values into an array that passes this 'extra' data into its adjacent memory which results in abnormal operation of the ICS service. The impact could be as severe as crashed ICS communication service or crashed fault-tolerant network equipment protocol. These are usually found in custom server applications which process ICS network traffic and other ICS protocol messages. To prevent this, secure coding guidelines should be followed, and all input data should be validated by the application code [3].

### 2.4.3. Poor programming and code quality

Lack of secure coding and adequate testing leads to bugs which not only make the ICS system vulnerable but also fragile to attacks and unstable. The use of potentially dangerous functions or lack of input validation leads to vulnerabilities like remote code execution etc. “Strcpy” in C is the most exploited function leading to buffer overflow vulnerabilities. Developers should follow secure programming standards and guidelines to mitigate this issue at the initial stage. Also automated and manual secure code analysis should be performed using various tools [2] [3].

### 2.4.4. Session related vulnerabilities

Session Hijacking allows a malicious actor to create an interactive session and access the command line interface and send commands to execute buffer overflow. This enables an attacker to redirect the victim to a malicious webpage, steal session tokens, and perform reconnaissance to later inject a backdoor. Lack of secure authentication and resources for session initiation and message authentication could lead to giving an attacker access for initiating the sessions or alter established sessions with ease.ICS developers should use vetted frameworks and libraries that provide functions for implementing CSRF solutions. The system should automatically terminate the session after the time reaches an organization's defined period of inactivity [3].

### 2.4.5. Use of insecure protocols for remote management

Network devices in ICS are mostly configured to allow remote management over insecure clear-text protocols. Any disgruntled employee or actor who is into the network can easily sniff sensitive data like management credentials over insecure protocols like FTP, SNMP, Telnet, HTTP. Network architects should look for and avoid using any unnecessary protocols and replace them with their succeeding secured ones. ICS protocol uses weak authentication in the network [3].

## 2.5. Miscellaneous Threats

### 2.5.1. DOS

DOS aims to downgrade the quality of service of a system or a network to the extent of making it inoperable or inaccessible. Saturation of the available resources and catastrophic error is usually observed in critical processes causing the entire system to cease to work. As communication is disrupted, the higher level of networks like process control networks and corporate networks will also be affected. DOS can be prevented by integrating Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS). It is further recommended to use filters, honeypots, strong anti-spyware and anti-virus software on all systems with internet connectivity [2].

### 2.5.2. Lack of protection against steganographic attacks

Steganography is a process of embedding secret data within a file, image, or any other non-secret data to avoid detection. The malware attacks on ICS used steganography with encryption to increase covertness. Though it is difficult to completely prevent steganographic attacks, software delivery and distribution mechanism should be tightened to protect against the insider threat. Network segmentation and monitoring outbound traffic help in identifying the presence of steganographic actors [34].

### 2.5.3. Phishing

Phishing is a method of sending potential users multiple requests that appears to be legitimate but is intended to lure a victim into providing some personal information for evil purposes, including identity and other details. The phishing can be performed using email, text, or web page. These attacks are aimed at a target's email address, which is usually present on a company's IT network. ICS systems typically segregate them from their IT networks with an “air gap”. That air gap insulates the ICS systems from the kinds of infections perpetrated by spear-phishing attacks. Phishing campaigns have always been popular among attackers leveraging several attempts. So, it is necessary to be aware of the phishing trends and to keep your system and internet browsers updated with the latest antivirus and security patches available [2][3].

## 3. Analysis of distinct ICS attacks

The ICS system is increasingly targeted by sophisticated cyber-attacks resulting in undesirable consequences. Thus, swift identification, control, and prevention against the threats are recommended to secure ICS.

Each attack in the list below indicates the impact, methodology, and threat vectors exploited in the attack.

**Table 1:** Table indicates attacks occurred in Industrial Control system, their year of occurrence and threat vectors exploited by the attacks

| Attack Name | Y<br>ear | Threat Vectors |
|---|---|---|
| Zotob Worm | 2 | 1. Use of vulnerable components |

| | | |
|---|---|---|
| | 005 | 2. Lack of port security<br>3. Use of vulnerable Open network shares |
| Stuxnet | 2010 | 1. Lack of port security<br>2. Use of vulnerable Open network shares<br>3. Services running with unnecessary privileges<br>4. ICS protocol uses weak integrity checks |
| Night Dragon | 2010 | 1. Injections<br>2. Phishing<br>3. Use of vulnerable components<br>4. Sensitive data exposure |
| Duqu/ Flame/ Gauss | 2011 | 1. Phishing<br>2. Lack of port Security<br>3. Services running with unnecessary privileges<br>4. Unauthorized Directory traversal allowed |
| Weak password attack | 2011 | 1. Use of Default Credentials<br>2. Sensitive data exposure<br>3. Lack of server side Authentication |
| Shamoon | 2012 | 1. Use of vulnerable Open network shares<br>2. Services running with unnecessary privileges<br>3. Improper file permissions |
| Target Stores attack | 2013 | 1. Phishing<br>2. Injections<br>3. Improper privilege management |
| New York Dam Attack | 2013 | 1. Sensitive data exposure<br>2. Lack of system hardening<br>3. Unauthenticated access to a web server |
| Havex | 2014 | 1. Sensitive Data Exposure<br>2. Phishing<br>3. Use of vulnerable Open network shares |
| German Steel Mill Attack | 2014 | 1. Sensitive Data Exposure<br>2. Phishing<br>3. Lack of network segmentation |
| Black Energy | 2014 | 1. Phishing<br>2. Use of vulnerable Open network shares<br>3. Use of Vulnerable Remote Display Protocols<br>4. Improper File Permissions<br>5. Improper privilege management |
| Ukraine Power Grid Attack | 2015 | 1. Phishing<br>2. Sensitive Data Exposure<br>3. Use of Vulnerable Remote Display Protocols<br>4. Services running with unnecessary privileges |

| | | |
|---|---|---|
| | | 5. DOS |
| Kemuri water company Attack | 2016 | 1. Sensitive Data Exposure<br>2. Phishing<br>3. Injection<br>4. Use of vulnerable components<br>5. Lack of proper authentication<br>6. Lack of network segmentation |
| Shamoon 2 | 2016 | 1. Use of Vulnerable open network shares<br>2. Services running with unnecessary privileges<br>3. Improper file permissions |
| CrashOverride | 2016 | 1. Sensitive Data Exposure<br>2. DOS<br>3. Use of vulnerable Open network shares<br>4. Services running with unnecessary privileges |
| TRITON/Trisis/HatMan | 2017 | 1. Phishing<br>2. Data transmission in plain text<br>3. Unencrypted non-proprietary ICS protocol communication<br>4. Services running with unnecessary privileges<br>5. Improper File Permissions<br>6. ICS protocol uses weak integrity checks |
| SamSam | 2018 | 1. Use of vulnerable components<br>2. Lack of rate limiting<br>3. Lack of proper authentication<br>4. Improper privilege management<br>5. Lack of network segmentation<br>6. Use of Vulnerable Remote Display Protocols |
| GreyEnergy malware | 2018 | 1. Phishing<br>2. Use of vulnerable components<br>3. Poor Authentication in vulnerable web services |
| LockerGoga ransomware | 2019 | 1. Phishing<br>2. Lack of rate limiting<br>3. Improper privilege management |
| MegaCortex | 2019 | 1. Lack of network segmentation |
| Wildpressure APT | 2019 | 1. Improper privilege management<br>2. Lack of rate limiting<br>3. Lack of proper authentication<br>4. Use of Vulnerable Remote Display Protocols |
| Nation-State APT | 2019 | 1. Phishing<br>2. Improper file permissions |

| | | |
|---|---|---|
| | | 3. Running services with unnecessary privileges |
| New Sandworm attack | 2019 | 1. Weak firewall rules<br>2. Use of vulnerable components<br>3. Phishing<br>4. Sensitive Data Exposure<br>5. Improper privilege management<br>6. Services running with unnecessary privileges |
| EKANS (Snake backward) ransomware | 2020 | 1. Phishing<br>2. Improper file permissions<br>3. Use of Vulnerable Remote Display Protocols<br>4. Lack of network segmentation |
| Ransomware Event at U.S. Pipeline Operator | 2020 | 1. Phishing<br>2. Lack of network segmentation<br>3. Use of Vulnerable Remote Display Protocols<br>4. Use of vulnerable components |
| PoetRAT Trojan | 2020 | 1. Phishing<br>2. Weak Encryption used in standard IT protocol |
| Kwampirs malware | 2020 | 1. Lack of network segmentation<br>2. Use of default credentials<br>3. Services running with unnecessary privileges<br>4. Sensitive data exposure<br>5. Use of vulnerable Open network shares |
| Steganography attack in ICS | 2020 | 1. Phishing<br>2. Services running with unnecessary privileges<br>3. Lack of protection against steganographic attacks |

## 3.1. 2005 - Zotob Worm

In 2005, 13 units of DaimlerChrysler U.S car manufacturing plant were affected by Zotob worm which led them to downtime of nearly an hour costing the company a loss of thousands of dollars [4]. The worm propagates itself by exploiting a critical vulnerability of Microsoft Windows Plug and Play Service (MS05-039) on port TCP/ 445. A command shell is then initiated which sends a script through FTP to download and execute the worm on port 8888 on the victim's system. The worm downloaded is saved as 'haha.exe'. The victim system listens on port 33333 to receive commands from their master and infect other hosts.

The attack takes advantage of threat vectors like use of vulnerable components, lack of port security and use of vulnerable open network shares which aids the propagation of worms.

## 3.2. 2010 - Stuxnet

In 2010, Stuxnet was among the most sophisticated attacks which destroyed numerous centrifuges in Iran's nuclear facilities [5]. Stuxnet targeted windows operating systems and networks which compromised Iranian PLC and caused fast-spinning centrifuges to tear themselves apart. Stuxnet worm enters a network through a USB stick and infects all the systems running windows evading automated detection systems. It then searches for ICS machines made by Siemens deployed in Iran and updates itself from the Internet. The worm exploits zero-day vulnerabilities in the target's logic controllers, subsequently, it initiates information gathering which helps to take control of the system burning them to failure. Meanwhile, it also deviates HMI by sending false information.

The attack takes advantage of threat vectors like lack of port security, use of vulnerable open network shares, services running with unnecessary privileges, and ICS protocol uses weak integrity checks.

## 3.3. 2010 - Night Dragon

McAfee's Night Dragon attack targeted most of the global energy, oil, and petrochemical companies in 2009 [6]. Night Dragon performed Industrial espionage by gathering legal and financial information, information on deals by having undetected access to the company's network for more than a year. The attackers tried to compromise extranet servers through SQL Injection resulting in remote code execution. They further gained access to internal desktop and servers by uploading hacker's tools available on the Internet. Additional usernames and passwords are gathered using password cracking tools providing them authenticated access to sensitive internal resources. RATs and malware were installed on targeted systems to steal email archives and other sensitive documents of executives.

The attack takes advantage of threat vectors like injections, phishing, use of vulnerable components, and sensitive data exposure.

## 3.4. 2011 - Duqu/ Flame/ Gauss

Duqu, Flame, and Gauss are malware that belongs to the same family as Stuxnet. They intend to perform cyber-espionage on ICS in the middle east. Duqu exploits a zero-day vulnerability of windows kernel, installs a backdoor to capture keystrokes and information that could be used to attack ICS. The flame spreads in the network using print spooler exploit (MS10-061) and LNK exploit (MS10-046) [7]. Flame tricks the target computer into a proxy of Windows update through which other systems in the network try to update and get infected [8]. Gauss architecture is closely related to Duqu and Flame whereas Gauss targets at stealing online banking access credentials and system configurations [9].

The attack takes advantage of threat vectors like phishing, lack of port security, services running with unnecessary privileges, and unauthorized directory traversal allowed.

## 3.5. 2011 - Weak password attack

In 2011, a disgruntled employee who used to handle water and sewage infrastructure for south Houston, Texas compromised Siemens HMI software which was easily accessible over the Internet [10]. The attacker compromised the HMI remotely by simply using a 3 character password presumably default and hardcoded into the system.

The attack takes advantage of threat vectors like use of default credentials, sensitive data exposure, and lack of server side authentication.

## 3.6. 2012 - Shamoon

In 2012, the largest Energy Company named Saudi Aramco was hit by destructive malware which replaced data of over 30,000 computers with an image of an American burning flag [11][12].

Shamoon renders a compromised system unusable by corrupting partition tables, Master Boot Record (MBR), and most of the files with random data. The malware consists of 3 components: Dropper, Wiper, and Reporter. The main source of infection is dropper which drops other components into the system, network shares, and automatically starts a service on windows boot. A wiper is a destructive module that compiles a list of files, sends information about them to the attacker, and erases them, obstructing the recovery process. The reporter module sends information to the attacker about the domain, some files that were overwritten, the IP address, and the state of the compromised computer.

The attack takes advantage of threat vectors like use of vulnerable open network shares, services running with unnecessary privileges, and improper file permissions.

## 3.7. 2013 - Target Stores attack

The Target Stores were attacked in 2013, where hackers gained access to the network and stole sensitive financial data costing them a loss of $309M. The hackers used phishing to lure the victim into installing a trojan that helped attackers to get legitimate credentials for initial entry in HVAC ICS. Further, they escalated privileges by exploiting an unknown flaw and stole sensitive information like credit and debit card details, their CVV, and the expiration date of seventy million users.

The attack takes advantage of threat vectors like phishing, injection, and improper privilege management.

## 3.8. 2013 - New York Dam attack

In 2013, an Iranian hacker attacked a dam in New York to gain unauthorized access via a cellular modem to its SCADA system facing the Internet [14]. This allowed intruder to gain information about operating status like temperature, water levels, and sluice gate controls. The critical infrastructure and control system become easy to target due to vulnerable internet connections and lack of security controls.

The attack takes advantage of threat vectors like sensitive data exposure, Lack of system hardening and unauthenticated access to a webserver.

## 3.9. 2014 - Havex

ICS tailored malware called Havex is a RAT (remote access trojan) employed by the Russian group, Energetic Bear, and DragonFly [15]. The malware can upload computer details such as name, its version, list of files, and user details to the command and control servers (C&C). The malware may also execute component files which gathers information about computer and shared resources. The attackers used a waterhole technique to infiltrate their target and gained access to the system by planting phishing emails containing the trojan.

The attack takes advantage of threat vectors like sensitive data exposure, phishing, and use of vulnerable open network shares.

## 3.10. 2014 - German Steel Mill attack

In 2014, the sophisticated attackers caused physical damage to the German steel plant by taking control of ICS components which resulted in an unregulated furnace [16]. Attackers used social engineering techniques to intrude in the German mill's office network. From this network, they navigated to the production network and caused network outages by taking control of various components. This caused in significant loss to the plant because the outage prevented appropriate shutting down of a blast furnace.

The attack takes advantage of threat vectors like sensitive data exposure, phishing, and lack of network segmentation.

## 3.11. 2014 - Black Energy

Black energy is a highly modular malware that first appeared in 2007 as a DDOS tool but later performed cyber espionage against the ICS network [17]. This malware infected the Energy companies via spear phishing and exploited Microsoft documents. They further gained access to the network by compromising internet connected HMI devices. The attackers then exploited Dropbear SSH vulnerability to create a backdoor and collect information about the ICS environment.

The attack takes advantage of threat vectors like phishing, use of vulnerable open network shares, use of vulnerable remote display protocols, improper file permissions, and improper privilege management.

## 3.12. 2015 - Ukraine Power Grid Attack

Ukrainian Power Grid outage was caused by a cyber-attack in 2015 which affected 30 substations and left 230,000 people without electricity [18]. A similar attack was observed later in December 2016 where a power outage occurred for a duration of 3 hours. The attacker used spear phishing techniques to gain access to the organization’s internal network, where the attackers performed keylogging for stealing credentials. Later the attackers entered the ICS network using VPN and took remote access of an HMI device by issuing commands from a remote station. Once they gained control over the ICS network, they performed Telephonic DOS along with firmware modification of communication devices to disconnect the uninterrupted power supply. The key variant amid the 2 attacks is the former was remote controlled to manually trip down breakers whereas later attacks used sophisticated malware "CRASHOVERRIDE" to automate the process.

The attack takes advantage of threat vectors like phishing, sensitive data exposure, use of vulnerable remote display protocols, services running with unnecessary privileges, and DOS.

## 3.13. 2016 - Kemuri water company attack

In 2016, as per the reports of Verizon, the Kemuri water company (KWC) was targeted by a Syrian group of hacktivists [19]. They were able to gain approximately 2.5 million customer records and alter SCADA controls. Attackers used SQL injection and phishing techniques to exploit the KWC customer portal and gain access to the webserver, where credentials of internal AS400 servers were stored in plain text. Thereby, able to gain information about KWC's internal network and manipulate SCADA controls.

The attack takes advantage of threat vectors like sensitive data exposure, phishing, injection, use of vulnerable components, lack of proper authentication, and lack of network segmentation.

## 3.14. 2016 - Shamoon 2

The second wave of Shamoon was observed in 2016 which overwrote master boot record partitions and file with random data. Although Shamoon 2 had more sophisticated components, the attack vector was similar to its predecessor [20].

The attack takes advantage of threat vectors like the use of vulnerable open network shares, services running with unnecessary privileges, and improper file permissions.

## 3.15. 2016 - CrashOverride

CrashOverride is the first malware to target the electric grid specifically which caused an outage in Ukraine. It implies modular framework consisting of a backdoor, a launcher, and various payload modules. The backdoor can perform several actions like creation, modification, execution of process, files, and services. The payload module is launched to manipulate ICS and cause destruction using the Wiper function. The malware can create a denial of visibility conditions, executing amplification attacks, forcing an islanding effect, causing power outages, and hampering protective relays [21].

The attack takes advantage of threat vectors like sensitive data Exposure, DOS, use of vulnerable open network shares, and services running with unnecessary privileges.

## 3.16. 2017 - TRITON/Trisis/Hatman

Triton/Trisis/Hatman is a malware that attacks the Safety Instrumented System (SIS) of Triconex Safety Controller mainly used in Nuclear, Oil and Gas refineries, chemical plants, etc. The malware was designed to perform malicious functionalities like reading, manipulating memory contents, and executing custom codes. The attackers gained access to the main network probably via spear phishing and moved on to the ICS Network for analysis of tri-station communication protocol used by SIS controllers. The triton framework is an executable Python script that masquerades as a Triconex trilogy application. The python file contains various libraries and injectors to implant the backdoor and gains control of Triconex products [22].

The attack takes advantage of threat vectors like phishing, data transmission in plain text, unencrypted non-proprietary ICS protocol communication, services running with unnecessary privileges, improper file permissions, and ICS protocol uses weak integrity checks.

## 3.17. 2018 - SamSam

In 2018, Samsam ransomware targeted multiple critical industries that need to be highly available and hence are likely to pay larger ransom [23]. The attacker penetrated the network by exploiting the JBoss application on the Windows server and infected all reachable host. The cyber actors used brute force for stealing credentials of RDP to gain persistent access over the network. Further, the Samsam actors escalate to administrator privileges, drop malware on the server, and run an executable file without victims' actions.

The attacks take advantage of threat vectors like use of vulnerable components, lack of rate limiting, lack of proper authentication, improper privilege management, lack of network segmentation, and use of vulnerable remote display protocols.

## 3.18. 2018 - GreyEnergy malware

GreyEnergy malware targeted industrial networks in Ukraine and other eastern European countries to take control of SCADA servers for monitoring and data collection [24]. The attackers sent phishing emails containing malicious word documents to targeted organizations. The macro once downloaded executes a packer which consists of a key required to perform decryption of encrypted data and loads a dropper into the memory. The dropper drops the malware and sets a persistent backdoor upon execution.

The attack takes advantage of threat vectors like phishing, use of vulnerable components, and poor authentication in vulnerable web services.

## 3.19. 2019 - LockerGoga ransomware

In 2019, LockerGoga ransomware targeted aluminum production to disrupt its operations by causing an outage and forced some factories to halt production [25]. Initially, attackers compromised the network using spear phishing and brute force the credentials of the active directory to conduct lateral movement. Once LockerGoga ransomware is installed, it modifies the user's password and encrypts files stored on the infected system. After the encryption process, it will attempt to disconnect the system from any outside connection.

The attacks take advantage of threat vectors like phishing, lack of rate limiting, and improper privilege management.

## 3.20. 2019 - MegaCortex

Megacortex is a new ransomware that propagates to devices on victim's LAN affecting several customers in Italy, U.S., Canada, and other countries [26]. The attackers used stolen credentials to compromise the domain controller and run a cobalt strike script to open a meterpreter reverse shell which connects to a remote C2 server. The attacker used a reverse shell to issue commands and inject malware into devices within the domain controller through Windows Management Instrumentation (WMI). Once malware is injected, a batch file executes a list of commands to terminate or disable running services; the last command in the list executes Megacortex which performs encryption of files.

The attack takes advantage of vulnerability like lack of network segmentation.

## 3.21. 2019 - Wildpressure APT

Wildpressure APT group targets the industrial sector in the Middle east to spread Milum RAT and take control of the infected system [27]. Once the RAT is installed in the machine it uses a base64 encoded JSON beacon to communicate with the C2 server. Milum can execute a wide range of commands from the attacker like upgrading to a new version, collecting, and sending information to the C&C server, or deleting itself.

Though the exact vulnerabilities are not yet known it has been assumed that attackers use threat vectors like improper privilege management, lack of rate limiting, Lack of proper Authentication, and use of vulnerable remote display protocols.

## 3.22. 2019 – Nation State APT

Lookback malware targeted more than a dozen US utilities that can perform actions like having access to resources such as system, process, file data, reboot machines, take screenshots and delete itself [28]. The attacker gains access to the utility network using spear phishing. The phishing email contains a Microsoft document which is originally a macro that drops three files. The dropped files then mirrors the name of common tools for establishing C2 connections. Once executed lookback malware can take control of the system and perform various malicious activities.

The attack takes advantage of threat vectors like phishing, improper file permissions, and running services with unnecessary privileges.

## 3.23. 2019 - New Sandworm attack

Russian military intelligence group also known as "Sandworm" attacked email servers having Exim Mail Transfer Agent (MTA) connected to ICS and SCADA systems [29]. The attacker sent specially crafted email to the organizations with unpatched public facing Exim software. Once the shell script is executed from a sandworm-controlled domain, hackers can perform privilege escalation, modify network security settings, and configure SSH to enable further remote access to accelerate the exploitation process.

The attack takes advantage of threat vectors like weak firewall rules, use of vulnerable components, phishing, sensitive data exposure, improper privilege management, and services running with unnecessary privileges.

## 3.24. 2020 - EKANS (Snake backward) ransomware

Ekans ransomware was observed in the US and Europe affecting various industries including energy, healthcare, transportation, architecture, and manufacturing [30]. Ekans ransomware consists of a static kill list to stop various software's targeting the antivirus, ICS processes, and services, then it proceeds to disable restoration capability by deleting the shadow file. After encrypting files Ekans modify the extension which aids to evade instant detection, the primary behavior of Ekans ransomware is to display a ransom note at the end of encryption.

The attack takes advantage of threat vectors like phishing, improper file permissions, use of vulnerable remote display protocols, and lack of network segmentation.

## 3.25. 2020 - Ransomware Event at U.S. Pipeline Operator

The US CISA reported a ransomware event impacting both IT and ICS resources which resulted in causing two days of downtime due to the loss of control [31]. The attackers use spear phishing as an initial vector to gain access to the victims' network. Then the attacker compromised the active directory to deploy ransomware and perform encryption on infected windows machines. This resulted in the loss of availability on OT networks including HMI data historians and polling servers which caused operation disruptions.

The attack takes advantage of threat vectors like phishing, lack of network segmentation, use of vulnerable remote display protocols, and use of vulnerable components.

## 3.26. 2020 - PoetRAT Trojan

PoetRAT used Covid-19 lure to target public and private companies including the SCADA sector and performed a phishing campaign of Azerbaijan government infrastructure [32]. The attackers gained an initial foothold by sending malicious word document to deploy python based remote access trojan. After opening the document, a macro file is executed leading to extract and run the malware, thus providing complete access of the compromised system. An operator tool monitors the hard disk and exfiltrates data automatically using FTP. The malware also includes keyloggers, password stealers, and camera control applications.

The attack takes advantage of threat vectors like phishing and weak encryption used in standard IT protocol.

## 3.27. 2020 - Kwampirs malware

The Kwampirs malware of the Orangeworm group targeted ICS assets in global health care entities to perform cyber espionage [33]. Kwampirs starts with establishing a backdoor on the targeted network and based on the target the modules are released. The imaging vendors having domain access are targeted to enter the victim's network. During mergers and acquisition, malware spreads through lateral movement using shared and internet connected resources of software development processes.

The attack takes advantage of threat vectors like lack of network segmentation, use of default credentials, services running with unnecessary privileges, sensitive data exposure, and use of vulnerable open network shares.

## 3.28. 2020 - Steganography attack in ICS

Recently steganography attacks have been observed in various Industrial computers of Europe and Japan [34]. Initially, the attackers send a phishing email containing an urgent request to open a malicious attachment. The PowerShell script is triggered when the victim enables the active content of an excel spreadsheet, which allows the malicious macro to execute. The PowerShell script randomly selects a URL from a list and downloads an image from image hosting servers. Steganographic technique is used to hide the data in the image which triggers a second PowerShell script responsible for extracting the data and executing the malware.

The attack takes advantage of threat vectors like phishing, services running with unnecessary privileges, and lack of protection against steganographic attacks.

# 4. Results

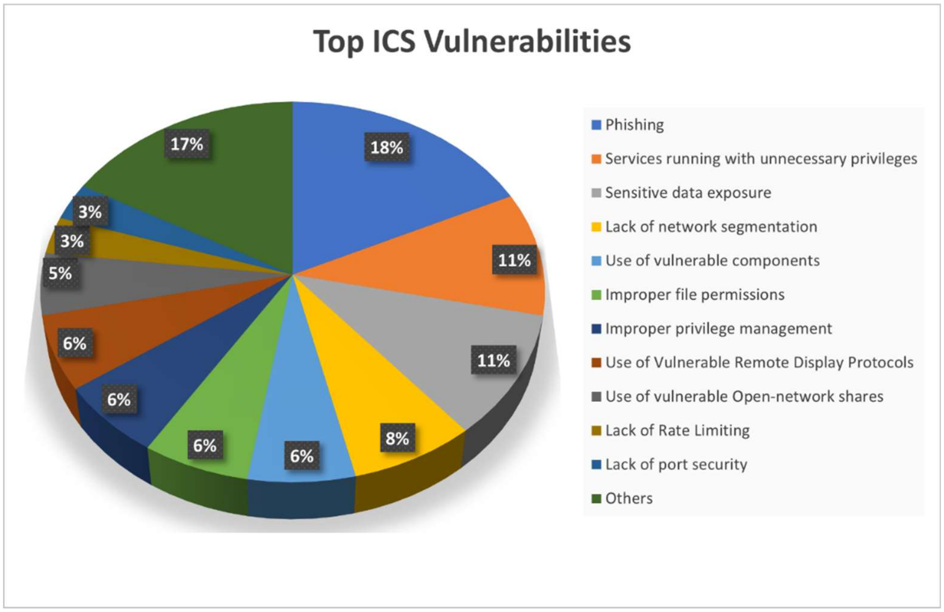

**Figure 1:** The chart describes frequently exploited threat vectors in ICS attacks that have happened since 2005 till date. The observation is based on the recurrence of threat vectors exploited in ICS attacks.

On observation of attacks that occurred between 2005 to 2020, it was apparent that most of the attacks exploited few common threat vectors; among which phishing was the most common initial vector used by the attackers to penetrate the industrial network. Phishing comprises 18% of frequently exploited ICS threat vectors which are used to deploy sophisticated malware on ICS remotely. The next frequently exploited threat vectors are services running with unnecessary privileges and sensitive data exposure which comprises 11% individually. Services running with unnecessary privileges allow an attacker to intrude the ICS network and gain full access to exploited hosts through privilege escalation whereas sensitive data exposure reveals crucial details about ICS which are exploited by attackers to disrupt critical services. Lack of network segmentation makes ICS networks vulnerable to DOS which correspond to 8% of frequently exploited threat vectors. The use of vulnerable components, improper file permissions, improper privilege management, and Use of vulnerable remote display protocols independently signify 6% of frequently exploited threat vectors. The use of vulnerable components provides information about ICS architecture which easily leads to unauthorized access. Improper file permissions allow unauthorized manipulation of files and directories affecting data integrity. Improper privilege management allows the attacker to perform unauthorized malicious actions while the use of vulnerable remote display rules allows an intruder to inspect and manipulate traffic of ICS networks. The use of vulnerable open network shares which sums up to 5%, allows an attacker to access various publicly available files on an ICS host. Lack of rate limiting, and lack of port security contains 3% individually. The former allows an attacker to brute force the credentials whereas the latter allows an intruder to access an unsecured port of ICS. The other threat vectors consist of DOS, use of default credentials, unauthorized directory traversal, etc. which adds up to 17% of the common threat vectors.

The industries and organizations can use this research to create a checklist for implementing best practices and policies by referring to the most frequently exploited threat vectors to prevent further exploitation.

## 5. Conclusion

The study of this research concludes that ICS emphasizes availability rather than the confidentiality in the CIA triad. ICS devices are exposed to the public internet without proper security measures, thus resulting in undesirable consequences. We have described 34 threat vectors observed on internet facing ICS components and suggested the recommendations to protect the ICS system. Based on the extensive study we listed 28 attacks along with their impact, identified their methodology, and mentioned threat vectors exploited by them. After comparing various attacks, we made a comprehensive list of threat vectors that were exploited by most attacks.

Lastly, we conclude this study helps industries to create best practices and policies by referring to the listed threat vectors and take corrective actions to prevent further exploitation.

## 6. References

[1] Keith Stouffer, Joe Falco, Karen Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 (September 2008)

[2] Trent Nelson, May Chaffin, Common Cybersecurity Vulnerabilities in Industrial Control Systems, Homeland Security (May 2011)

[3] May Chaffin, Kathleen Lee, NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses, Idaho National Laboratory/EXT-10-18381 (May 2010)

[4] F-secure, Zotob. A. https://www.f-secure.com/v-descs/zotob_a.shtml(accessed 11 July 2020)

[5] ScienceDirect, Stuxnet. https://www.sciencedirect.com/topics/computer-science/stuxnet (accessed 11 July 2020)

[6] Global Energy Cyberattacks: "Night Dragon", McAfee Foundstone Professional Services and McAfee Labs (2011)

[7] Boldizsár Bencsáth, Gábor Pék, Levente Buttyan, The Cousins of Stuxnet: Duqu, Flame, and Gauss, Future Internet (2012), 4(4), 971-1003 https://doi.org/10.3390/fi4040971

[8] ComputerWorld, Gauss malware: Nation-state cyber-espionage banking Trojan related to Flame, Stuxnet.https://www.computerworld.com/article/2597456/gauss-malware--nation-state-cyber-espionage-banking-trojan-related-to-flame--stuxnet.html (accessed 12 July 2020)

[9] Threatpost, New Gauss Malware, Descended From Flame and Stuxnet, Found On Thousands of PCs in Middle East. https://threatpost.com/new-gauss-malware-descended-flame-and-stuxnet-found-thousands-pcs-middle-east-080912/76892/ (accessed 12 July 2020)

[10] Threatpost. Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System. https://threatpost.com/hacker-says-texas-town-used-three-character-password-secure-internet-facing-scada-system-11201/75914/ (accessed 13 July 2020)

[11] Baker J, Bronk C, Tikk-Ringas E, Hack or Attack? Shamoon and the Evolution of Cyber Conflict, Issue of Survival, Global Politics and Strategy (2013)

[12] Belden, Shamoon: Malicious Malware Harms 30,000+ Computers. https://www.belden.com/blog/industrial-security/shamoon-malicious-malware-harms-30-000-computers (accessed 13 July 2020)

[13] Hemsley, Kevin E. E. Fisher, Dr. Ronald, History of Industrial Control System Cyber Incidents, OSTI INL/CON-18-44411-Rev002 (2018)

[14] TrendMicro, Seven Iranian Hackers Indicted over Alleged Cyber Attacks Targeting US Banks and NY Dam. 14. https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/seven-iranian-hackers-indicted-over-attacks-on-banks-ny-dam (accessed 14 July 2020)

[15] F-Secure Labs, Havex Hunts For ICS/SCADA Systems.https://archive.f-secure.com/weblog/archives/00002718.html (accessed 14 July 2020)

[16] TrendMicro, German Steel Plant Suffers Significant Damage from Targeted Attack. https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/german-steel-plant-suffers-significant-damage-from-targeted-attack (accessed 15 July 2020)

[17] NJCCIC Threat Profile, BlackEnergy. https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/blackenergy (accessed 15 July 2020)

[18] Robert M. Lee, SANS Michael J. Assante, SANS Tim Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid Defense Use Case, SANS (2016)

[19] The Kemuri Water Company Hack, Vericlave

[20] ENISA, Shamoon Campaigns with Disttrack. https://www.enisa.europa.eu/publications/info-notes/shamoon-campaigns-with-disttrack (accessed 16 July 2020)

[21] Crashoverride Analysis of the Threat to Electric Grid Operations, Dragos Inc. (2017)

[22] Fireeye, Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html (accessed 16 July 2020)

[23] SamSam: the (almost) six million dollar ransomware, Sophos Ltd. (2018)

[24] Kaspersky ICS CERT, Threat landscape for industrial automation systems. H2 2018 https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/#_Toc4416094 (accessed 16 July 2020)

[25] TrendMicro, What You Need to Know About the LockerGoga Ransomware. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware (accessed 17 July 2020)

[26] Christopher Kim, MegaCortex Ransomware, Infoblox (2019)

[27] SecureList, WildPressure targets industrial-related entities in the Middle East https://securelist.com/wildpressure-targets-industrial-in-the-middle-east/96360/ (accessed 17 July 2020)

[28] Proofpoint, LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards. https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks (accessed 18 July 2020)

[29] ZDNET, NSA warns of new Sandworm attacks on email servers. https://www.zdnet.com/article/nsa-warns-of-new-sandworm-attacks-on-email-servers/ (accessed 18 July 2020)

[30] Paloalto networks, Threat Assessment: EKANS Ransomware. https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/ (accessed 19 July 2020)

[31] Smart Energy International, Assessment of ransomware event at US pipeline operator. https://www.smart-energy.com/industry-sectors/cybersecurity/assessment-of-ransomware-event-at-us-pipeline-operator/ (accessed 19 July 2020)

[32] Talos, PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors. https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html (accessed 20 July 2020)

[33] Helpnet Security, Kwampirs threat actor continues to breach transnational healthcare orgs. https://www.helpnetsecurity.com/2020/03/31/kwampirs/ (accessed 20 July 2020)

[34] Kaspersky ICS CERT, Steganography in attacks on industrial enterprises (updated). https://ics-cert.kaspersky.com/reports/2020/06/17/steganography-in-attacks-on-industrial-enterprises/#:~:text=Attack%20victims%20include%20suppliers%20of,to%20detect%20and%20analyze%20malware (accessed 21 July 2020)

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.