Internet of Things and Cyber-Physical Systems 4 (2024) 186–202

Contents lists available at ScienceDirect

Internet of Things and Cyber-Physical Systems

journal homepage: www.keaipublishing.com/en/journals/internet-of-things-and-cyber-physical-systems

Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges

Mourad Benmalek

Computer Engineering Department, College of Engineering and Architecture, Al Yamamah University, Riyadh, Saudi Arabia

ARTICLE INFO

Keywords:
Cyber-physical systems
Industrial control systems
Security
Ransomware
Challenges

ABSTRACT

Ransomware attacks have emerged as one of the most significant cyberthreats faced by organizations worldwide. In recent years, ransomware has also started to target critical infrastructure and Cyber-Physical Systems (CPS) such as industrial control systems, smart grids, and healthcare networks. The unique attack surface and safety-critical nature of CPS introduce new challenges in defending against ransomware. This paper provides a comprehensive overview of ransomware threats to CPS. We propose a dual taxonomy to classify ransomware attacks on CPS based on infection vectors, targets, objectives, and technical attributes. Through an analysis of 10 real-world incidents, we highlight attack patterns, vulnerabilities, and impacts of ransomware campaigns against critical systems and facilities. Based on the insights gained, we identify open research problems and future directions to improve ransomware resilience in CPS environments.

1. Introduction

Cyber-Physical Systems (CPS) are smart interconnected systems that integrate computation, communication, and control with physical assets to manage infrastructure, processes and environments [1]. CPS encompass Industrial Control Systems (ICS), embedded devices, Internet of Things (IoT), robotics, and smart connected equipment. By fusing the cyber and physical worlds, CPS provide capabilities like automated control, situational awareness, operational visibility, remote supervision and intelligent decision support for industrial facilities, power grids, manufacturing plants, smart healthcare, and other critical infrastructure [2–6].

However, the blurring of boundaries between Information Technology (IT) and Operational Technology (OT) also expands the attack surface for cyberthreats [7]. Legacy ICS environments were traditionally air-gapped or used proprietary protocols assuming obscurity provided security. But increasing connectivity to leverage IoT data and IT software in OT has exposed once-isolated CPS to external risks. Adversaries are rapidly honing techniques to target the cyber-physical core of smart infrastructure [8,9].

A prime threat in this context is ransomware, which has emerged as one of the most lucrative cybercrimes targeting enterprises and organizations globally [10]. Unlike traditional malware focused on data theft or service disruption, the goal of ransomware is extortion by denying access to systems and data. Ransomware encrypts files or devices and demands ransom payments from victims in return for decryption keys and restoring availability [11].

With the rise of cryptocurrencies like Bitcoin [12] providing anonymous payment channels, ransomware attackers have successfully extracted huge payouts from private firms and public infrastructure worldwide [13]. The global damages from ransomware may exceed $20 trillion annually by 2031 according to cyber risk predictions [13].

In recent years, ransomware has started aggressively targeting CPS and ICS that operate critical infrastructure in sectors like energy, water treatment, manufacturing, transportation, and healthcare [14]. The OT managed by CPS has unique vulnerabilities unlike conventional IT systems. Legacy platforms, proprietary architectures and lack of security by design increase the attack surface. The real-time responsiveness and availability requirements also restrict downtimes for patching. Furthermore, the convergence of IT and OT has introduced new risks, as compromising enterprise systems provides pathways to traverse into CPS networks [15–17].

Successful ransomware attacks on CPS can have severe financial, operational, reputational and human safety impacts. The 2017 NotPetya compaign [18] and 2020 Ryuk ransomware [19] incidents highlighted massive business and infrastructure disruptions from ransomware. With increasing reliance on interconnected smart systems to manage essential processes and services, ransomware has become an apex threat for organizations owing CPS assets [20].

In this paper, we present a comprehensive study of ransomware

E-mail address: m_benmalek@yu.edu.sa.

https://doi.org/10.1016/j.iotcps.2023.12.001
Received 4 September 2023; Received in revised form 27 October 2023; Accepted 15 December 2023
Available online 6 January 2024

threats targeting CPS. The key contributions are:

- We provide an examination of recent survey papers tackling ransomware threats, defenses, and research directions in order to position our study in the literature.
- We propose a dual taxonomy to classify ransomware attacks on CPS: one based on infection vectors, targets and objectives, and another based on technical attributes and behaviors.
- We compile an up-to-date catalog of 10 major real-world ransomware incidents that have impacted critical infrastructure organizations across industry verticals.
- We derive pivotal lessons regarding ransomware tactics and innovations and vulnerable architectures.
- We discuss the key open challenges and future research directions for improving ransomware resilience in CPS.

The rest of the paper is organized as follows: Section II provides an examination of recent survey papers tackling ransomware threats, defenses, and research directions. Section III provides background details on ransomware threats and the unique security challenges faced by CPS. Section IV introduces our proposed dual taxonomy for categorizing ransomware attacks on CPS infrastructure. Section V describes major real-world CPS ransomware incidents compiled from public reports and disclosures. Section VI derives key lessons learned from these attacks and highlights priority areas needing focus to address open challenges. Finally, Section VII concludes the paper. In the end, Table 1 tells about the list of abbreviations used in this work.

Table 1
List of abbrevitions used.

Short forms	List of Abbreviations
AES	Advanced Encryption Standard
CI	Critical Infrastructure
CI/CD	Continuous Integration/Continuous Delivery
CPS	Cyber-Physical Systems
CT	Computed Tomography
DL	Deep Learning
DNN	Deep Neural Networks
DT	Decision Tree
ECU	Electronic Control Units
EEPROM	Electrically Erasable Programmable Read-Only Memory
ERP	Enterprise Resource Planning
FPGA	Field Programmable Gate Array
GPT	GUID Partition Table
HMI	Human-Machine Interface
HMM	Hidden Markov Model
I/O	Input/Output
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IED	Industrial Emissions Directive
IoT	Internet of Things
IT	Information Technology
KNN	K-Nearest Neighbours
MBR	Master Boot Record
ML	Machine Learning
MPS	Managed Service Provider
MRI	Magnetic Resonance Imaging
OEM	Original Equipment Manufacturer
OT	Operational Technology
PC	Personal Computer
PLC	Programmable Logic Controller
RaaS	Ransomware-*as*-a-Service
RDP	Remote Desktop Protocol
RSA	Rivest-Shamir-Adleman
RTU	Remote Terminal Unit
SaaS	Service-*as*-a-Service
SG	Smart Grid
SMB	Server Message Block
USB	Universal Serial Bus
VPN	Virtual Private Network

2. Related surveys

In recent years, ransomware attacks have rapidly proliferated, prompting greater research focus on analyzing this threat. Several survey papers have conducted literature reviews centered on ransomware analysis, detection, taxonomy, and real-world impacts. This section summarizes related ransomware surveys and highlights how our proposed study differs in its CPS focus. Table 2 provides an overview comparison of our survey paper against the other related works in terms of focus, taxonomy, and analyzed incidents.

The survey proposed by Al-rimy et al. [21] provides a comprehensive literature review of ransomware analysis, detection, prevention, and prediction techniques. It proposes a ransomware taxonomy based on severity, platform, and victim type. Through examples like WannaCry, it highlights real-world impacts and factors enabling ransomware growth. Authors examine structural and behavioral detection approaches using techniques like machine learning and event monitoring. They also cover prevention methods like access control, backups, and patching.

The survey by Tandon and Nayyar [22] provides a comprehensive overview of ransomware threats, including the history, attack methods, and prevention strategies. It explains the ransomware attack framework in detail covering installation, contacting command-and-control servers, key exchange, encryption, extortion, and payment. The paper analyzes the WannaCry ransomware specifically. It also summarizes prevention measures like user awareness, backups, access controls, disabling services, securing networks, and payment tracking. The survey aims to provide insights into ransomware operations to help organizations defend against this threat.

Maigida et al. [23] propose a taxonomy to classify ransomware attacks based on techniques to crypto-based techniques and locker-based techniques. They compile and tabulate sources of ransomware datasets to facilitate future research. The paper examines the metrics used to evaluate ransomware detection methods like CPU utilization, signature matching, content monitoring etc. The survey identifies unresolved challenges like lack of predictive models, need for ensemble classification, ransomware evolution handling, and anonymized payment tracking.

Fernando et al. [24] provide a comprehensive review of ML and Deep Learning (DL) techniques for ransomware detection. They analyze prominent research studies showcasing various algorithms like logistic regression, gradient boosting, SVM, decision trees, neural networks, etc. for detecting ransomware based on features like API calls, network traffic, file entropy etc. The authors evaluate detection rates, limitations and potential improvements of the approaches. They also assess the longevity of the models by testing them on newer ransomware variants to simulate concept drift. The paper highlights open issues like lack of emphasis on ransomware evolution, limited diversity in datasets, and need for proactive techniques. It also discusses directions for future ransomware detection research.

In [25], Humayun et al. provide a comprehensive overview of ransomware threats in the context of IoT. The proposed paper covers the security challenges introduced by IoT that make it vulnerable to ransomware attacks. It analyzes different types of ransomware such as crypto and locker ransomware and reviews the major ransomware attacks from 2005 to 2019, linking the evolution of ransomware to the growth of IoT. It discusses the infrastructure beyond just malware code that is needed to deploy ransomware campaigns. The paper also analyzes whether victims should pay ransom demands, provides statistics on ransomware attacks covering top target countries, infection volumes and propagation methods, identifies key ransomware challenges for IoT environments, and reviews prevention techniques.

Sharma et al. [26] focus specifically on ransomware threats targeting Android devices. They examine static, dynamic, and hybrid analysis techniques used for Android ransomware feature extraction. The proposed paper surveys machine learning algorithms like Hidden Markov Model (HMM), K-Nearest Neighbours (KNN), Decision Trees (DTs), Deep

Table 2
Comparison of related surveys.

Publication	Year	Focus	Taxonomy	Real-World Incidents
[21]	2018	Comprehensive literature review of ransomware analysis, detection, prevention and prediction techniques	Classifies ransomware based on severity, platform, and victim type	Examples like WannaCry demonstrating real-world impacts
[22]	2019	Comprehensive overview of ransomware operations, attack framework, and prevention strategies	No taxonomy proposed	Analysis of WannaCry ransomware specifically
[23]	2019	Comprehensive review of ransomware attacks and defense mechanisms	Classifies ransomware attacks into two categories: crypto-based and locker-based techniques	No real-world incidents analyzed
[24]	2020	Comprehensive review of ML and DL techniques for ransomware detection	No taxonomy proposed	No specific incidents analyzed
[25]	2021	Comprehensive overview focused on ransomware threats in the context of IoT	No taxonomy proposed	Review of major ransomware incidents from 2005 to 2019 and attack statistics
[26]	2021	Focuses specifically on Android ransomware feature extraction and detection	No taxonomy proposed	Timeline of major Android ransomware families
[27]	2021	Systematic review of ransomware detection mechanisms for Windows platforms	Categorizes ransomware attacks into four stages: (1) Delivery, (2) Deployment, (3) Destruction, and (4) Dealing	Analysis of detection techniques tested on various ransomware families
[28]	2021	Recent advances in ransomware detection and prevention	No taxonomy proposed	Analysis of a few popular ransomware samples and a simple ransomware created by the authors
[29]	2022	Broad overview of ransomware threats to traditional IT systems	Categorizes ransomware based on encryption strategy, distribution vector, and payload delivery	Examples like WannaCry and NotPetya highlighting impacts on regular IT systems
[30]	2023	Comprehensive overview of ransomware evolution, taxonomy and research directions	Classifies ransomware types based on characteristics and behavior	Examination of key ransomware events and absence of analysis regarding specific incidents
[31]	2023	Specific focus on detecting encryption activities in ransomware attacks	Proposes ransomware cyber kill chain model with four phases: (1) Initial Compromise, (2) Establishing Foothold, (3) Encryption, and (4) Extortion	Examination of encryption detection methods and the absence of analysis regarding real-world incidents
This survey	2023	Specific focus on ransomware threats to CPS	Dual taxonomy tailored for CPS environments analyzing infection vectors, targets, objectives, and technical attributes	Analysis of major incidents affecting OT and industrial control processes in CPS

Neural Networks (DNNs), and ensemble methods employed for detection. It provides a timeline of major Android ransomware families and highlights analysis on manifest files, DEX code, native libraries, dynamic behavior, and network traffic. The survey concludes by outlining challenges around datasets, detection methods, feature engineering, and hybrid analysis techniques.

The survey by Moussaileb et al. [27] provides a systematic review of ransomware detection and prevention mechanisms for Windows platforms. It categorizes ransomware attacks into four stages: (1) Delivery, (2) Deployment, (3) Destruction, and (4) Dealing. For each stage, it summarizes the available countermeasures in the literature including awareness campaigns, data backups, access controls, signature-based detection, API call monitoring, network traffic analysis, system honeypots, hardware performance counters, and bitcoin payment tracking. The paper clusters related techniques and highlights tested prototypes. It also discusses limitations of current approaches and provides a research roadmap identifying gaps to address polymorphic ransomware and evasion techniques.

The survey by Beaman et al. [28] provides a comprehensive review of recent advances in ransomware detection and prevention approaches. The authors categorize existing studies into prevention techniques like access control, data backup, key management, and user awareness, and detection techniques like file analysis, network traffic analysis, and machine learning models. Through experiments with known ransomware samples and a custom ransomware called AESthetic, they highlight limitations of current antivirus products against novel threats. They also analyze major challenges like user unawareness and inadequate detection rates, and suggest future research directions in areas like fog computing, blockchain countermeasures, and resilient architectures.

Oz et al. [29] provide a broad overview of ransomware threats, analyzing key features like encryption techniques, distribution methods, payment mechanisms, and defense strategies. It proposes a taxonomy to categorize ransomware based on encryption strategy, distribution vector, and payload delivery. Through examples like WannaCry and NotPetya, it highlights real-world ransomware impacts on regular IT systems.

Razaulla et al. [30] trace the origins of ransomware since 1989 and categorize different types based on characteristics and behavior. They review many recent contributions across various goals including detection, classification, prevention, mitigation, and prediction of ransomware. The paper finds that most research has focused on Machine Learning (ML)-based ransomware detection, with a lack of emphasis on prediction techniques. It also highlights under-explored areas like adversarial ML and concept drift in ML models. The authors suggest future directions in real-time protection, zero-day ransomware identification, reverse engineering of recent strains, and resilient architectures.

Begovic et al. [31] provide a comprehensive survey focused specifically on the detection of encryption activities in ransomware attacks. The authors propose a ransomware cyber kill chain model with four phases: (1) Initial Compromise, (2) Establishing Foothold, (3) Encryption, and (4) Extortion. The survey focuses on the Encryption phase which is the key differentiating characteristic of cryptographic ransomware. The authors identify three main encryption detection approaches: API and system call monitoring, I/O monitoring, and filesystem monitoring. The survey examines recent research contributions in each of these areas, analyzing the pros and cons of techniques like ML models for API call sequences, power consumption monitoring, deception files, and file entropy analysis. The study highlights gaps between academic research and commercial products, and challenges like custom encryption and evolving adversary tactics. It emphasizes the importance of multi-layered detection focused on pre-encryption behaviors.

While the aforementioned surveys provide useful insights, our study makes unique contributions by comprehensively examining ransomware risks specifically for CPS. We propose taxonomies tailored to CPS environments analyzing vectors, targets, objectives, and ransomware attributes. Through the analysis of 10 major incidents affecting industrial facilities, we uncover pivotal lessons regarding vulnerable architectures, adversary innovations, and impactful safeguards directly relevant for CPS. Our focus on OT systems differentiates this survey from IT-centered studies. The insights gained on infection pathways, ransomware behaviors, safety impacts, and detection gaps aim to help CPS operators make informed investments to improve ransomware resilience. As ransomware rapidly evolves to target essential CPS, our analysis fills an important

knowledge gap regarding contemporary risks and priorities to secure smart infrastructures.

3. Background

CPS are IT systems that find application in the physical world. These systems come equipped with embedded sensors and actuators. Advances in Information and Communications Technology (ICT) have led to enhanced communication between the digital and physical realms, thereby amplifying the interaction among various physical processes [1].

3.1. CPS in real world

CPS represent the next generation of embedded control systems designed for monitoring and managing the physical environment. Numerous sectors including energy, transportation, and healthcare are progressively reliant on CPS technology. The specific nature of CPS examples can be quite diverse; for instance, the Supervisory Control and Data Acquisition system (SCADA) stands out as a notable CPS in the realm of Critical Infrastructures (CIs), such as Smart Grids (SG) and ICS [32–36]. Additionally, wearable and Implantable Medical Devices (IMDs) serve as significant CPS instances within the medical field [37, 38]. Enumerating all the variations of CPS is not the main objective of this work, yet we will spotlight four representative CPS applications and provide concise insights into those specific cases:

3.1.1. Industrial control systems

ICS, also referred to as SCADA or distributed control systems, function as control systems that optimize production and control processes across various industries such as nuclear plants, water and sewage systems, and irrigation systems. Within the realm of ICS, diverse controllers like the Programmable Logic Controller (PLC) play a crucial role. This device boasts a range of capabilities that can collaborate to achieve specific outcomes. To interface this device with the physical world, sensors and actuators are employed. The system is designed with both wireless and wired communication capabilities, adaptable to the specific environmental context. Additionally, it facilitates centralized monitoring and operational control through connection to PC systems [32,34,35].

3.1.2. Smart grid

Despite the long-standing use of power grids, the SG represents the subsequent evolution in electricity generation, equipped with advanced features. This next-generation grid offers economic and environmental viability on a local scale, empowering consumers with improved energy usage management. On a broader national scale, it augments control over emissions, global load distribution, and contributes to energy conservation [39–41].

3.1.3. Medical devices

Cyber and physical capabilities have been incorporated to improvise medical devices with an aim to deliver better health care services. These medical devices are designed to serve the patients by being implanted inside the patient's body or worn by them in the form of wearable devices. Such devices are smart and they have wireless capabilities to communicate with other devices. This communication is being provided by programmer, require for updating and reconfiguring the devices. Wearable device is more helpful in tracking minor activities of patients [37,38].

3.1.4. Smart vehicles

Intelligent vehicles embody a greener, more fuel-efficient, and safer driving experience, coupled with enhanced user-friendliness and convenience. These advancements have been realized by relying on a network of 50–70 interconnected computers known as Electronic Control Units (ECU). These ECUs are tasked with supervising and managing diverse functions, including engine emission control, brake systems, in-car entertainment (such as radios and multimedia players), and comfort features (like cruise control and window operation). These technological breakthroughs are of paramount importance in the present-day context, aiming to address challenges like traffic congestion and accidents in our roadways and regions [42–44].

3.2. CPS security challenges

While connectivity and integration can provide efficiency and functionality gains, security considerations for the expanded CPS attack surface remain a work in progress. Legacy ICS systems lacked native security capabilities during design, assuming air-gapped environments or proprietary protocols provided sufficient protection. But external connectivity has invalidated these assumptions, allowing external threats ingress into previously isolated environments.

Several unique attributes of OT infrastructure also hamper traditional security approaches [45–51]:

- Stateful continuity requirements typical of IT stateless server transaction models are not feasible given the need for continuous monitoring and control. Shutting down processes like power grids and manufacturing for patching and upgrades is difficult.
- The use of custom or proprietary software, operating systems and hardware with limited vendor support hampers patch availability and asset management. Lack of visibility into all connected assets also complicates inventory management.
- Real-time performance constraints prevent security techniques like encryption, which delay data flows unacceptable in high-speed process environments. Signature-based malware detection can also disrupt tightly scheduled processes when compute resources are diverted.
- Legacy devices and unencrypted communications necessary to interface across decades of existing installations prevent wholesale security upgrades without environment disruption.
- Functional safety requirements necessitate physical fail-safe mechanisms to automatically deal with failures, over-rides and forced shutdowns. But cybersecurity protections for safety systems remain inadequate.
- Physical accessibility of remote field infrastructure introduces physical tampering and firmware-level threats. Lack of visibility into all interconnected third-party vendor systems also obscures risks.
- Additionally, the different risk management culture between IT and OT hampers security integration. IT systems require constant updates and patching to address newly discovered threats. But OT systems prioritize high reliability, uptime and operational consistency given the physical process risks.

This complex security posture has made CPS prime targets for emerging cyberthreats like ransomware that can paralyze operations by targeting both IT and OT layers. While initially focused on conventional data theft and encryption for extortion, ransomware is increasingly incorporating OT-specific features for greater physical damage potential [52,53].

3.3. Ransomware threat landscape

Ransomware, which denies access to systems until ransom payments are received, has rapidly emerged as one of the most lucrative cybercrimes targeting enterprises, government agencies and critical infrastructure worldwide [14].

Unlike traditional malware focused on data theft or service disruption, ransomware's unique economic model is centered around denying access to data and systems until payment is received. As shown in Fig. 1, typical ransomware encrypts files, drives or computers using robust encryption algorithms, while posting ransom payment instructions on how victims can purchase decryption tools and keys to regain system

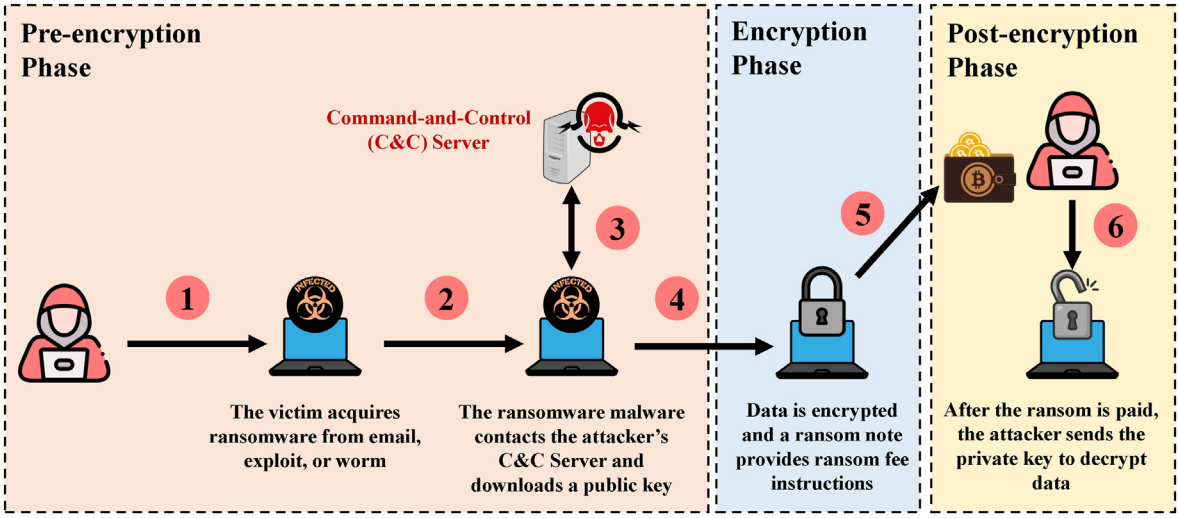

Fig. 1. General workflow for most types of ransomware.

availability [54].

With the rise of cryptocurrencies like Bitcoin [12], ransomware attackers found ways to anonymously collect payments at scale while hindering authorities from tracking financial flows. Some ransomware operations run on a Ransomware-*as*-a-Service (RaaS) model similar to legitimate Service-*as*-a-Service (SaaS) businesses, with platform developers, affiliates conducting campaigns, support infrastructure, and revenue sharing agreements [55,56]. This professionalization has fueled ransomware industrialization and exponential growth.

While traditionally focused on typical IT systems, ransomware attackers have expanded capabilities for ICS environments over the past decade. The proliferation of RaaS has also lowered skill barriers to paralyze critical infrastructure like water, manufacturing and healthcare delivery. However, most ransomware affecting industrial facilities still relies on conventional propagation approaches after an initial compromise, lacking custom OT capabilities. Nonetheless, the expanding attack surface due to IT/OT convergence provides greater opportunities for ransomware penetration into mission-critical systems. Once inside ICS environments, even traditional ransomware can inflict severe availability and safety impacts [57].

3.3.1. *Ransomware components*

Ransomware incorporates several key components that enable deployment, encryption, extortion and payment collection [58–60]:

- **Installer:** Initial code that placement ransomware onto victim systems via distribution vectors like phishing, exploits, physical media. Often includes deception tactics.
- **Reconnaissance Modules:** Components that fingerprint victim environment to map assets, pathways and high-value targets to maximize damage.
- **Propagation Agents:** Functions that allow lateral movement between systems to expand infection blast radius using remote execution, credential theft, fileless scripts.
- **Evasion Modules:** Routines for disabling security tools, antivirus, reporting mechanisms and backups that could block ransomware operation.
- **Encryption Engine:** Robust symmetric (like Advanced Encryption Standard - AES) and asymmetric (like Rivest-Shamir-Adleman - RSA) encryption algorithms for scrambling files, disks and systems to deny access.
- **Ransom Graphical Interface:** Visual ransom notes with payment instructions, threats and decryption procedures for victims. Created in formats like HTML, RTF, PNG.
- **Command and Control:** Communication protocols allowing ransomware to contact attacker infrastructure for key management, configuration, updates.
- **Cryptocurrency Modules:** Components for generation of payment addresses, wallets and transaction tracking to handle ransom transfer logistics.
- **Decryption Framework:** Decryption software provided to victims making payments, to restore locked systems. May be single-use or universal.
- **Wiping Modules:** In destructive strains, routines that destroy data irrecoverably after encryption or system manipulation.

Ransomware often blends these components for tailored campaigns targeting specific sectors, geographies or organizations. The diversity of technical innovations shows sophistication exceeding traditional malware, necessitating dedicated defenses for CPS.

3.3.2. *Attack vectors*

Ransomware groups employ a range of tactics to gain initial access into target networks, providing a beachhead for deploying encryption payloads across wider environments [61]:

- Phishing is a prevalent infiltration tactic. Adversaries send socially engineered emails impersonating trusted entities to trick recipients into enabling malware installation through malicious documents or links [62,63].
- Exploiting internet-facing systems like RDP and VPNs using brute force credential attacks or vulnerabilities provides another ransomware penetration method [64]. Remote access services often lack latest security patches or use default passwords.
- Compromising third-party vendors and managed service providers furnishes soft intermediary targets for traversing into customer networks using stolen credentials [65]. Vendor access channels provide opportunities for adversaries.

3.3.3. *Extortion tactics*

Beyond basic data encryption for ransom demands, adversaries employ various tactics to pressure victims into paying:

- **Data Theft and Leakage:** Stealing sensitive files before encryption and threatening to publish them online compels victims to meet extortion demands [66].

- **DDoS Attacks:** Some ransomware groups hit victims with distributed denial of service attacks while systems are down to hamper recovery efforts [67].
- **Company Impersonation:** Adversaries fake communication posing as the victim company to spread misinformation and reputational damage [61].
- **Physical Sabotage:** Rare but some cases involve hackers manipulating operating parameters of physical equipment to force ransom payment [68].
- **Custom Ransom Amounts:** Certain ransomware gangs research victims' finances to tailor non-negotiable ransom figures to what organizations can pay [69].

3.3.4. Targeting CPS

CPSs like industrial control systems, utilities, smart factories, and healthcare networks are high-value targets for ransomware groups due to their role managing physical world infrastructure. Specific factors make CPS environments lucrative targets:

- **OT Legacy Systems:** CPS often rely on outdated OT equipment and proprietary protocols that lack modern security capabilities. These legacy assets contain vulnerabilities ransomware can exploit [70].
- **Real-Time Availability Requirements:** CPS continuously monitor and control physical processes where any downtime or disruption risks human harm, asset damage, and supply chain chaos [1]. This pressures victims into paying ransoms to restore operations faster.
- **Difficulty Patching and Upgrading:** The real-time responsiveness needs of CPS restrict opportunities for patching vulnerabilities. Ransomware takes advantage before defenses are updated [71].
- **Interconnected IT/OT Convergence:** Blending enterprise IT systems with OT for data analytics and visibility bridges air gaps and expands the CPS attack surface ransomware can penetrate [72].
- **Safety System Impacts:** Encrypting or manipulating cyber-physical safety systems, protective relays, and fail-safes can result in physical damage beyond data loss, raising extortion stakes [71].
- **Lack of Resilience Planning:** Most CPS operators historically assumed air gaps and siloed networks ensured availability. Ransomware response plans are still maturing [20].

4. Dual taxonomy for classifying ransomware threats to CPS

To systematically analyze the risk posed by ransomware attacks on CPS, we require a structured taxonomies to categorize and characterize various attributes of ransomware campaigns targeting these critical systems. We propose a dual taxonomy model encompassing:

- An attack lifecycle taxonomy based on infection vectors, targets, and objectives.
- A technical taxonomy centered on ransomware architecture, capabilities and effects on physical process operations.

Each taxonomy provides vital perspectives into adversary tactics, ransomware capabilities, targeting priorities and attack severity against industrial facilities and CPS.

4.1. Lifecycle-based ransomware taxonomy

As shown in Table 3, the lifecycle taxonomy focuses on ransomware attack progression from initial compromise to final disruptive impact based on three dimensions: (1) infection vectors, (2) targets, and (3) objectives. This provides a framework to understand how ransomware attacks penetrate CPS environments, what mission-critical components they impact, and the motivations behind such attacks. Fig. 2 provides a concise summary of the various types of ransomwares, categorized according to the proposed taxonomy.

Table 3
Key elements of lifecycle-based ransomware taxonomy.

Taxonomy Dimension	Description
Infection Vectors	How ransomware infiltrates the initial foothold such as phishing emails or compromised vendor accounts.
Targets	What systems are ultimately encrypted or disrupted including IT, OT, safety mechanisms.
Objectives	Adversary motivations such as financial extortion, operational disruption, industrial espionage.

4.1.1. Infection vectors

The initial infection vectors through which ransomware enters a target CPS network provide insights into adversary tactics and vulnerabilities being exploited. The common vectors include:

- **Phishing Campaigns:** Highly-crafted phishing emails containing infectious malware documents or links remain a prevalent tactic for adversaries to socially engineer end users and plant ransomware in CPS. Adversaries research target organizations extensively to fabricate emails impersonating trusted contacts and entities that convince victims to enable malware installation [73]. Employing psychologically manipulative techniques, adversaries trick users into disabling security to infect endpoints [59].
- **Remote Access Exploits:** Unpatched internet-facing management interfaces like Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) gateways provide ransomware penetration pathways for adversaries. Identifying vulnerabilities in outdated remote access services allows adversaries to remotely exploit and gain access into CPS industrial networks [74].
- **Third-party Compromise:** Trusted third-parties like vendors, contractors, and Managed Service Providers (MSPs) serve as soft intermediary targets for leapfrogging into tightly controlled CPS environments. Their compromised networks and stolen credentials allow adversaries to bypass conventional cybersecurity boundaries [75].
- **Insider Threats:** Disgruntled employees or malicious contractors can intentionally infect CPS networks by exploiting their privileged access and trust. Personnel risk mitigation via strict access controls, behavioral monitoring, prompt off-boarding and insider threat programs are imperative alongside technical protections [76].
- **Physical Infections:** Infected USB drives, SD cards and devices intentionally seeded into facilities provide an air-gap bridging vector for malware like Stuxnet [77]. This allows adversaries to traverse from unsecured external environments into secured CPS networks physically disconnected from untrusted networks [11].
- **ICS Protocol Attacks:** Adversaries probe proprietary industrial protocols and equipment interfaces to identify vulnerabilities for tailored ICS attacks. By reverse engineering protocols like Modbus[1] [78], DNP3[2] [79] or IEC61850[3] [80], attackers can craft malicious packets to penetrate or traverse across OT network boundaries and zones [15].

4.1.2. Targets

The specific systems, processes and data within the CPS infrastructure targeted by ransomware also reveal adversary goals and priorities:

- **Industrial Controllers:** Encrypting PLCs, Remote Terminal Units (RTUs), Industrial Emissions Directives (IEDs) and ICS equipment directly halts CPS physical processes and damages assets from unsafe states [81].

[1] https://www.modbus.org.
[2] https://www.dnp.org.
[3] https://iec61850.dvl.iec.ch.

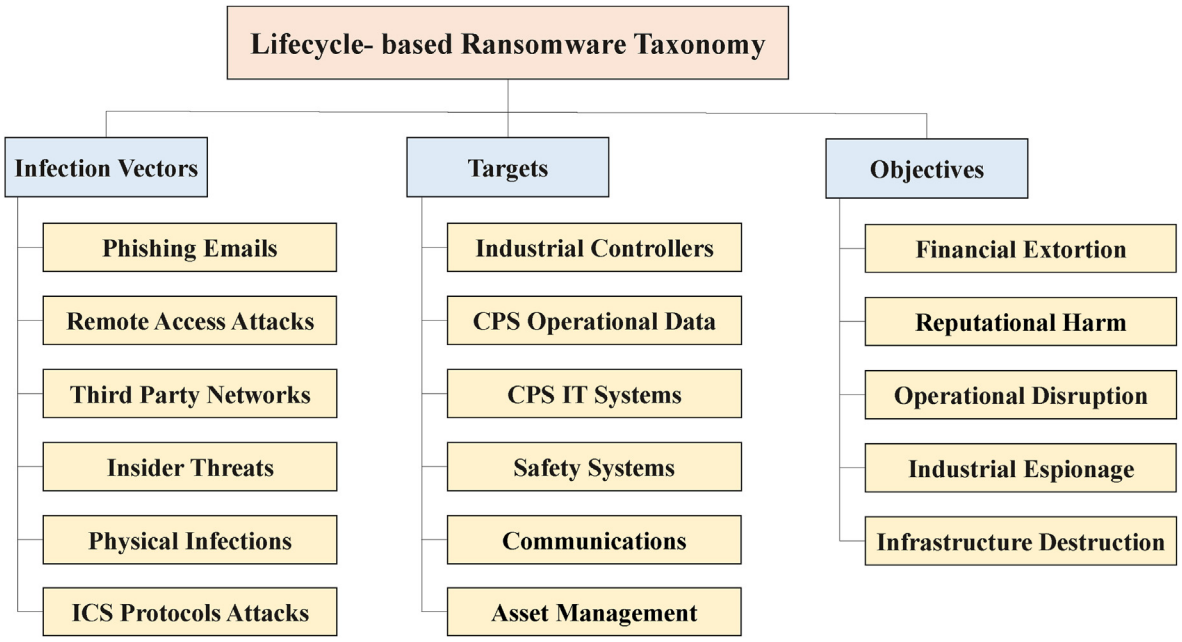

Fig. 2. Lifecycle-based ransomware taxonomy for CPS.

- **CPS Operational Data:** Historians, HMI/SCADA databases, batch recipes represent high value targets for maximum persistence of operational disruption. Unique operational technology data is hard to recreate [82].
- **CPS IT Systems:** Servers like active directories, file shares provide essential services to OT systems. Their disruption provides leverage [53].
- **Safety Systems:** Programmable safety controllers, physical safety mechanisms and failsafes are targets for adversaries aiming at human harm rather than mere data extortion [83].
- **Communications:** Disrupting the CPS protocols and networks connecting operators, engineers, controllers and sensors paralyzes visibility into processes [53].
- **Asset Management:** Workstations, engineering servers, configuration repositories help adversaries analyze the CPS environment and maximize damage [53].

4.1.3. *Objectives*

Ransomware attacks on CPS aim to achieve a range of adversarial objectives. The motives behind ransomware attacks determine the end goals [84]:

- **Financial Extortion:** Adversaries encrypting CPS for ransom payments account for most incidents. Downtime sensitivity coerces victims into paying.
- **Reputational Harm:** Public visibility into operational disruption and safety risks from ransomware coercers providers of critical infrastructure services like power and water to pay ransoms.
- **Operational Disruption:** Certain ransomware aims to severely disrupt essential CPS services like fuel, water, power and healthcare rather than just extort finances.
- **Industrial Espionage:** Some campaigns also involve stealing intellectual property before encryption with monetary demands being secondary objectives.
- **Infrastructure Destruction:** Rare but rising ransomware risks exist from manipulating physical safety systems and forcing unsafe equipment states deliberately rather than just encrypting data.

4.2. *Technical Behavior-based ransomware taxonomy*

As shown in Table 4, this taxonomy categorizes ransomware threats targeting CPS environments based on internal structure, capabilities, behaviors and effects on physical process operations. We propose four major ransomware architecture classes encompassing associated subtypes (Fig. 3):

4.2.1. *Network-propagating ransomwares*

Self-propagating ransomware features worm-like behaviors enabling rapid peer-to-peer infection between networked systems after an initial beachhead. Network-spreading ransomware aims to achieve enterprise-wide compromise by traversing across domains, servers and endpoints leveraging stolen credentials and host vulnerabilities.

- **Lateral Movement Ransomware:** focuses on utilizing stolen credentials, Windows admin tools and network shares for traversal across segmented domains and subnets to expand infection. Techniques include: (1) Using Mimikatz and credential dumping tools to harvest passwords, tokens and hashes to impersonate legitimate users and assets. (2) Scanning network shares and guessing weak passwords via brute force to gain access to additional systems. (3) Disabling security systems and logging mechanisms to mask detection by terminating processes for antivirus, reporting and analytics [85].
- **Self-Replicating Ransomware:** Incorporates worm-like functionality to infect entire CPS rapidly. Aggressive peer-to-peer replication allows exponential growth. Techniques include: (1) Using network scanning tools to identify live hosts based on open ports, platform types and known vulnerabilities. (2) Propagating laterally via file-

Table 4
Ransomware categories based on technical behavior.

Taxonomy Category	Description
Network-Propagating	Self-spreading ransomware using exploits and stolen credentials.
Destroying Wipers	Ransomware that irreversibly corrupts systems.
Ransomware-*as*-a-Service	Ransomware kits, builders and infrastructure sold to affiliates.
CPS-Aware Ransomware	Ransomware tailored to ICS protocols, devices, safety logic.

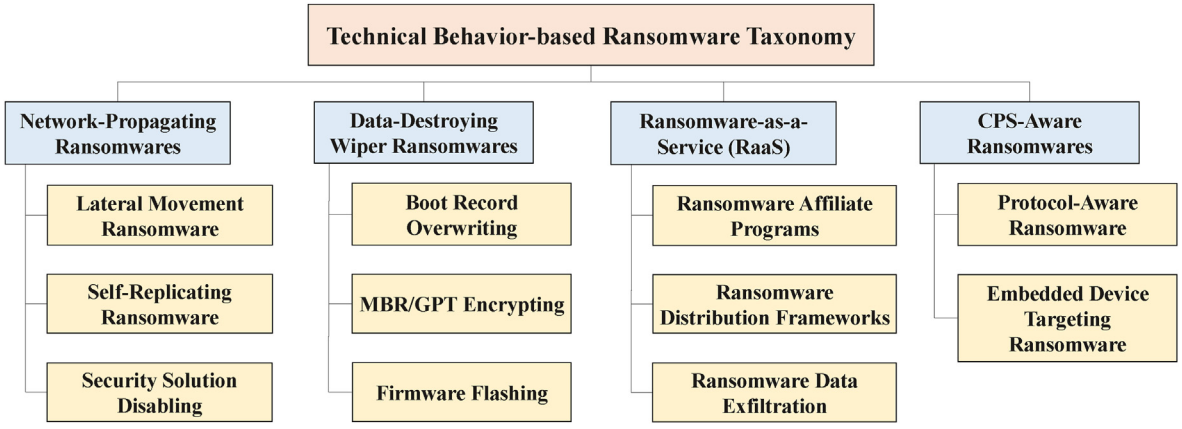

Fig. 3. Technical behavior-based ransomware taxonomy for CPS.

sharing protocols like Server Message Block (SMB) by guessing weak credentials. (3) Targeting commonly multi-homed assets like remote desktop servers and file shares to maximize lateral reach [86].

- **Security Solution Disabling:** Certain ransomware bloodlines exhibit behaviors focused on disabling and circumventing installed security solutions, monitoring tools and defenses to enable unimpeded operation [87]. Tactics include: (1) Removing security solution hooks from critical CPS components like kernel drivers, process injections and user-land monitoring interfaces. (2) Blocking and blackholing domain names and infrastructure IP addresses used for command and control by defenses. (3) Encrypting anti-malware definition signature databases or overwriting with random data to blind solutions.

4.2.2. *Data-destroying wiper ransomwares*

Destructive wiper malware poses as ransomware but with the actual objective of inflicting maximum damage through irrecoverable corruption of critical files, data stores, backup repositories and system settings [88]:

- **Boot Record Overwriting:** Permanently destroying boot configuration records needed for system startup represents a highly disruptive corruption vector. Tactics include: (1) Directly overwriting the Master Boot Record (MBR) or GUID Partition Table (GPT) with destructive code sequences to damage partition data structures and prevent OS loading. (2) Locking users out of boot order configuration screens via firmware flaws or stolen admin passwords to prevent circumventing corrupted MBR/GPT records. (3) Rendering boot media like USB drives used for system recovery inoperable by manipulating firmware settings and corrupting controller logic [88,89].
- **MBR/GPT Encrypting:** Ransomware can irrecoverably encrypt partition tables and boot records necessary for system startup while retaining traditional file encryption payloads. Tactics include: (1) Generating asymmetric key pairs to use for encrypting MBR, GPT or partition tables separately from file contents, without retaining private keys for recovery. (2) Employing cryptographically-secure pseudo-random number generators and stream ciphers for irreversible random corruption of boot records, rather than structured public key encryption. (3) Combining MBR/GPT encryption with full disk encryption and individual file encryption for layered damage [88,89].
- **Firmware Flashing:** Corrupting embedded device firmware and logic governing hardware appliance operations represents permanent damage vectors [90]. Tactics encompass: (1) Manipulating non-volatile memory containing device logic on integrated circuits like FPGAs (Field Programmable Gate Arrays) used in CPS gear. (2) Overwriting EEPROM (Electrically Erasable Programmable Read-Only Memory) and flash storage used for persistent code and configuration storage on networked equipment.

4.2.3. *Ransomware-as-a-service (RaaS)*

As shown in Fig. 4 Ransomware-*as*-a-Service lowers barriers for less sophisticated threat actors by offering convenient ransomware development, deployment and extortion frameworks via a subscription model. RaaS allows adversaries to customize, deliver and manage campaigns with turnkey infrastructure:

- **Ransomware Affiliate Programs:** RaaS affiliate programs coordinate large scale, geographically distributed ransomware execution by collaborating threat groups. Models include: (1) Central RaaS operators develop ransomware toolkits and manage backend payment and money laundering operations. (2) RaaS dashboards allow tracking infections, ransom status and payments across affiliate operations. (3) Cryptocurrencies enable ransom collection across global regions with money laundering also offered as a service [91].
- **Ransomware Distribution Frameworks:** RaaS offerings provide turnkey installation, deployment and management capabilities to affiliates through distribution frameworks: (1) Initial compromise vectors like exploit kits, phishing campaigns, vulnerability scanners provided as a service. (2) Network reconnaissance tools fingerprint environments and identify high value targets automatically post-intrusion. (3) Propagation frameworks automate lateral movement using credential theft, fileless scripts, remote execution. (4) Command and control capabilities for managing payloads across compromised devices and continuing control after deployment [92].
- **Ransomware Data Exfiltration:** Certain RaaS offerings integrate data theft prior to encryption for additional extortion leverage through public leakage threats. Tactics include: (1) Stealthy data aggregation and compression split over multiple stages before detection. (2) Exfiltrating IP, credentials, emails, source code and databases for proprietary data. (3) Manipulating stolen data integrity to maximize controversy and reputation losses if leaked [92,93].

4.2.4. *CPS-aware ransomwares*

They incorporate proprietary OT asset knowledge and industrial protocol behaviors to traverse, map, and manipulate operations within critical infrastructure environments:

- **Protocol-Aware Ransomware:** Reverse engineering industrial protocols allows ransomware to blend in or disrupt critical CPS communications [34,81]. Tactics include: (1) Passively parsing protocol exchanges between operators, sensors, drives and controllers to map asset roles. (2) Mimicking valid protocol conversational flows and data types to propagate between assets. (3) Manipulating protocol fields and payload contents to deliver malicious code and configuration changes. (4) Introducing protocol-level viruses that

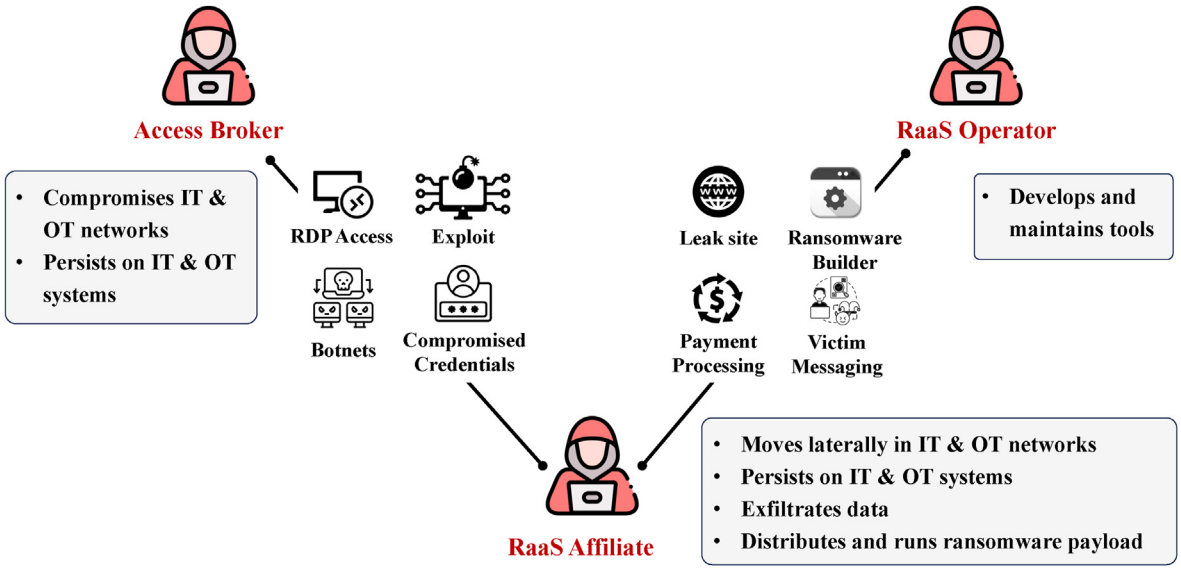

Fig. 4. Ransomware-*as*-a-Service (RaaS).

self-replicate through valid protocol message exchanges like client-server interactions.

- **Embedded Device Targeting Ransomware:** Increasing integration of embedded devices into CPS infrastructure creates specialized ransomware targets. Tactics include: (1) Compromising integrated microcontroller-based sensors, drives, instruments by abusing open debugging ports, unvalidated firmware updates and hardcoded credentials. (2) Analyzing embedded web and management interfaces through automated scanners to find vulnerabilities. (3) Bridging air gaps by first compromising integrated IoT and edge devices with backend connectivity [34,81].

5. Analysis of real-world ransomware threats to CPS

By thoroughly examining major real-world ransomware incidents through the lens of the proposed taxonomy models, we can gain vital insights into the progression stages, internal technical capabilities, industrial targeting priorities and impacts of contemporary ransomware threats to availability and safety of CPS. In the following, we present detailed analysis of the most recent ransomware attacks on CPS. Table 5 summarizes the key characteristics of the major ransomware incidents analyzed.

The methodology for investigating and analyzing the ransomware incidents involved:

- Identifying major publicly reported attacks targeting industrial and critical infrastructure organizations using sources like cybersecurity disclosures and Kaspersky ICS-CERT advisories.
- Prioritizing incidents with confirmed OT impacts beyond conventional IT systems.
- Selecting 10 high-profile cases across sectors like energy, manufacturing, and transportation for technical analysis.
- Extracting key details on infection vectors, internal propagation, systems affected, objectives, duration, demands, and impacts.
- Structured examination of diverse real-world cases to discern patterns related to adversary tactics, vulnerabilities, resilience factors, and safety/financial/operational effects.
- Leveraging empirical evidence and contextual insights to inform ransomware preparedness investments for CPS entities.

5.1. NotPetya campaign (2017)

The NotPetya campaign [94–96] represents one of the most damaging real-world examples of ransomware's potential to incur physical disruption and damages across multiple industrial sectors. Blending ransomware capabilities with destructive data wiping, NotPetya disabled hundreds of enterprises globally within hours in 2017, exemplifying risks from self-propagating network worms hitting legacy and unpatched OT systems.

As shown in Fig. 5, NotPetya exploited the ubiquitous EternalBlue vulnerability[4] in outdated Windows environments [97] to enable rapid lateral movement across internal networks of organizations without requiring extensive adversary customization or target-specific knowledge. Once inside victims' perimeter defenses, NotPetya aggressively sought to encrypt files on all systems while also irreversibly overwriting MBRs, rendering infected computers permanently inoperable even if ransom payments were initiated [98].

Unlike financially motivated ransomware, NotPetya integrated data wiping functionality that destroyed systems rather than merely encrypting recoverable data [99]. With propensity to spread between interconnected networks via unpatched hosts and no possibility of restoring encrypted systems, NotPetya inflicted indiscriminate damage across private sector firms and public infrastructure entities globally. Major multinationals like shipping giant Maersk[5] and pharmaceutical manufacturers Merck[6] and FedEx[7] experienced severe disruptions across global operations, requiring months to rebuild crippled IT and OT systems [100].

While NotPetya masqueraded as typical ransomware, forensic analyses revealed its core objectives as destructive rather than financially motivated. By combining ransomware penetration techniques like phishing with wiper payloads without recovery options, NotPetya highlighted evolution of threat actors focused on disruption of national critical infrastructure for ideological, terror or strategic objectives rather than mere criminal financial gain.

[4] EternalBlue is the name for an exploit of a vulnerability in the Windows implementation of the SMB protocol (CVE-2017-0144). The vulnerability was the result of a flaw which allowed a remote attacker to execute arbitrary code on a targeted computer sending it specially crafted data packets.

[5] https://www.maersk.com.

[6] https://www.merck.com.

[7] https://www.fedex.com/.

Table 5
Summary of major ransomware attacks on CPS.

Ransomware	Industry Vertical	Target Organization	Infection Vector	Systems Affected	Objectives	Attack Innovations	Security Gaps	Physical Impacts
NotPetya (2017)	Critical Infrastructure	Maersk, Merck, FedEx, Telecom Operators, Power Companies	EternalBlue Exploit	IT & OT Systems	Data Destruction	Exploiting common vulnerability to enable worm-like propagation	Unpatched systems, lack of segmentation	Shut down port operations, suspended drug production, halted package delivery
SamSam (2018)	Healthcare	Hancock Health	RDP Brute Force	IT & OT Systems	Financial Extortion, Operational Disruption	Traversing from admin systems into medical OT networks	Inadequate network segmentation between IT and OT	Suspended surgeries, diverted ambulances, cancelled medical procedures
LockerGoga (2019)	Manufacturing	Norsk Hydro	Phishing Email	IT & OT Systems	Financial Extortion	Targeting Active Directory for credential theft and lateral movement	Overly permissive trust between IT and OT networks	Suspended aluminum production lines
Ryuk (2020)	Automotive	Honda	Phishing Email	IT & OT Systems	Operational Disruption, Financial Extortion	Abusing BITSAdmin for malware distribution, pivoting from IT to OT	Flat trust between corporate and plant networks	Shut down vehicle assembly plants
Sodinokibi (2020)	Automotive	Gedia	Phishing Email	IT & OT Systems	Operational Disruption, Financial Extortion	Traversing from phished admin credentials into production networks	Unpatched systems, lack of privileged access controls	Suspended automotive parts plants
CLOP (2020)	Pharmaceutical	ExecuPharm	Vulnerability Exploit	IT & OT Systems	Operational Disruption, Financial Extortion	Traversing from exposed VPN gateway into OT systems	Unpatched public-facing systems, lack of segmentation	Disrupted drug packaging lines
RansomEXX (2020)	Technology	Konica Minolta	MSP Compromise	IT & OT Systems	Operational Disruption, Financial Extortion	Exploiting MSP access into customer OT networks	Overly permissive third-party access, lack of monitoring	Suspended printer manufacturing lines
BlackMatter (2021)	Agriculture	NEW Cooperative	Vulnerability Exploit	IT & OT Systems	Operational Disruption, Financial Extortion	Targeting grain storage OT networks	Poor perimeter security, inadequate OT system patching	Halted grain handling and feed milling systems
DarkSide (2021)	Energy	Colonial Pipeline	Vulnerability Exploit	IT & OT Systems	Operational Disruption, Financial Extortion	Traversing from VPN compromise to pipeline OT systems	Unpatched perimeter systems, lack of segmentation	Disrupted fuel logistics and pipeline operations
Hive (2022)	Retail	MediaMarkt	Vulnerability Exploit	IT Systems	Operational Disruption, Financial Extortion	Exploiting public eCommerce platform as initial access vector	Insecure web-facing systems, flat enterprise trust	Suspended retail stores and distribution centers

5.2. SamSam ransomware attack on Hancock Health (2018)

Hancock Regional Hospital,[8] a regional hospital system in Indiana, was significantly impacted by a ransomware attack in 2018 that used the SamSam strain of ransomware [101].

The attackers gained initial access by exploiting a vulnerable internet-facing server through an RDP brute force attack to achieve network penetration. After compromising an administrative server, SamSam utilized stolen Windows credentials extracted with Mimikatz[9] to traverse widely across Hancock's internal Windows infrastructure [102].

In addition to encrypting IT assets like file shares and email servers, the ransomware spread into medical care zones housing Magnetic Resonance Imaging (MRI) machines, Computed Tomography (CT) scanners and other medical devices due to lack of segmentation between administrative and healthcare networks. Monitoring workstations, imaging servers and OT terminals running critical diagnostics equipment were eventually infected and encrypted.

With core medical imaging and diagnostics lines disabled by the ransomware, Hancock had to divert ambulances and cancel surgeries across multiple facilities. SamSam demanded ransom payments in Bitcoin to decrypt both IT and OT systems across Hancock's business and healthcare environments [103].

The attack severely disrupted operations at Hancock's three hospitals, forcing staff to cancel surgeries, divert ambulances, and rely on paper records. Without access to diagnostic reports and digital medical charts, care was significantly impacted. The ransomware prevented access to over 1400 servers, workstations, and laptops.

Hancock chose not to pay the ransom after consulting with cybersecurity experts who determined the encrypted files could be restored from backups. Their IT staff worked continuously over several days to restore systems and recover files.

In total, the SamSam attack cost Hancock Health an estimated $55,000 in recovery efforts and lost revenue [102]. The attack highlighted vulnerabilities in legacy systems as well as the crippling impact ransomware can have on healthcare networks. Hancock has since invested heavily in security upgrades and employee education to prevent future attacks.

[8] https://www.hancockregionalhospital.org.

[9] Mimikatz is an open-source tool that uses admin rights on Windows to display passwords of currently logged in users in plaintext.

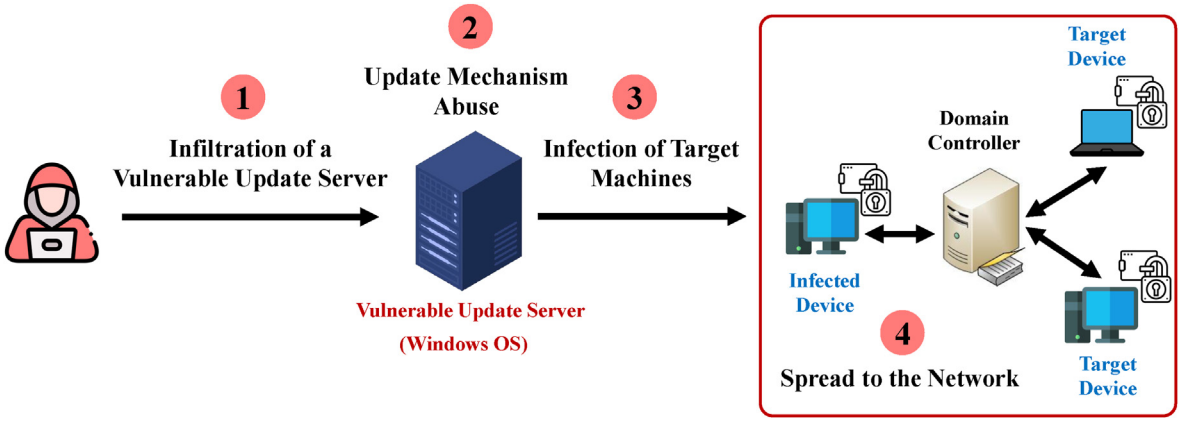

Fig. 5. The NotPetya ransomware process.

5.3. LockerGoga ransomware attack on Norsk Hydro (2019)

Norwegian aluminum manufacturing giant Norsk Hydro[10] was significantly impacted by the LockerGoga ransomware attack in March 2019 which encrypted systems across 170 sites in 40 countries, forcing multiple extrusion and production plants offline [104].

LockerGoga initially compromised Norsk Hydro's systems through phishing emails sent to administrative personnel which activated trojanized Microsoft Office documents to activate the malware. With a beachhead established on office workstations, LockerGoga utilized leaked Windows credentials extracted with Mimikatz to traverse widely across Hydro's global Windows infrastructure [105].

In addition to encrypting IT assets like file shares and email servers, the ransomware spread into manufacturing zones housing extrusion lines, smelters and electrolysis cells due to lack of segmentation between plant and office systems. PLCs, industrial controllers and OT terminals running production lines were eventually infected and encrypted.

With core aluminum manufacturing lines disabled by the ransomware, Hydro had to suspend multiple plants responsible for producing parts used across automotive, aerospace and construction industries. LockerGoga demanded ransom payments in Bitcoin to decrypt both IT and OT systems across Hydro's business and production environments [106].

LockerGoga illustrated risks from flat IT trust models allowing ransomware compromising business systems to freely traverse into manufacturing networks. Successful segmentation between Hydro's enterprise and plant floor environments could have contained the blast radius and allowed partial manufacturing operations despite the IT breach [107].

5.4. Ryuk ransomware outbreak at honda (2020)

Japanese automotive giant Honda[11] suffered major disruption in 2020 from the Ryuk ransomware encrypting and disabling enterprise IT systems and production lines across its North American manufacturing facilities [108,109]. As shown in Fig. 6 Ryuk gained initial access by compromising Active Directory credentials after sending phishing emails to Honda business personnel.

With network access obtained, Ryuk spread laterally using the Mimikatz tool to steal additional account credentials from compromised systems. The Windows BITSAdmin utility[12] was abused to download additional malware payloads and tools enabling lateral traversal across Honda's corporate servers.

Once sufficiently embedded within the IT network, Ryuk pivoted to breach Honda's manufacturing zones housing assembly line operational technology. The malware encrypted Windows systems managing robotic assembly machinery and quality assurance systems, eventually propagating to PLCs coordinating Honda's just-in-time production lines.

With core automation equipment encrypted, Honda suspended operations across multiple North American plants responsible for producing popular models like the Civic and Accord. Ryuk demanded a multi-million dollar ransom in return for decrypting computers across finance, supply chain, manufacturing and design departments victimized by the attack. Honda ultimately chose not to pay, undertaking a prolonged restoration by rebuilding crippled systems [108,109].

The Ryuk incident illustrated risks from flat enterprise IT trust models allowing ransomware compromising conventional information systems to traverse into production line OT environments. Lack of privileged access controls and network segmentation between IT and manufacturing systems enabled extensive plant disruption.

5.5. Sodinokibi ransomware attack against automotive supplier gedia (2020)

Sodinokibi ransomware severely impacted automotive parts manufacturer Gedia[13] in 2020 by encrypting international IT and production networks across Europe and USA, forcing plant shutdowns [110]. Gedia supplies chassis and drivetrain components to major automakers including Volkswagen and Daimler.

The Sodinokibi (REvil) gang gained initial access by compromising Active Directory credentials after sending phishing emails to manufacturing personnel. After expanding across file shares and internal servers, Sodinokibi pivoted to OT equipment controlling robotic stamping presses and machining tools on Gedia's automotive component production lines [111].

In addition to business systems like email and ERP (Enterprise Resource Planning) software, the ransomware encrypted PLCs, industrial controllers and HMIs governing manufacturing stations across multiple plants supplying automakers [110]. With production lines disabled, Gedia halted component shipments while recovering encrypted controllers and negotiating ransom terms.

The attack showcased Sodinokibi's capability to traverse from conventional IT systems into industrial control processes after gaining initial network access. Production shutdowns increased pressure on Gedia to pay ransom to decrypt manufacturing assets vital for just-in-time automotive supply chains.

[10] https://www.hydro.com.
[11] https://www.honda.com.
[12] BITSAdmin is a command-line tool used to create, download or upload jobs, and to monitor their progress.
[13] https://www.gedia.com/.

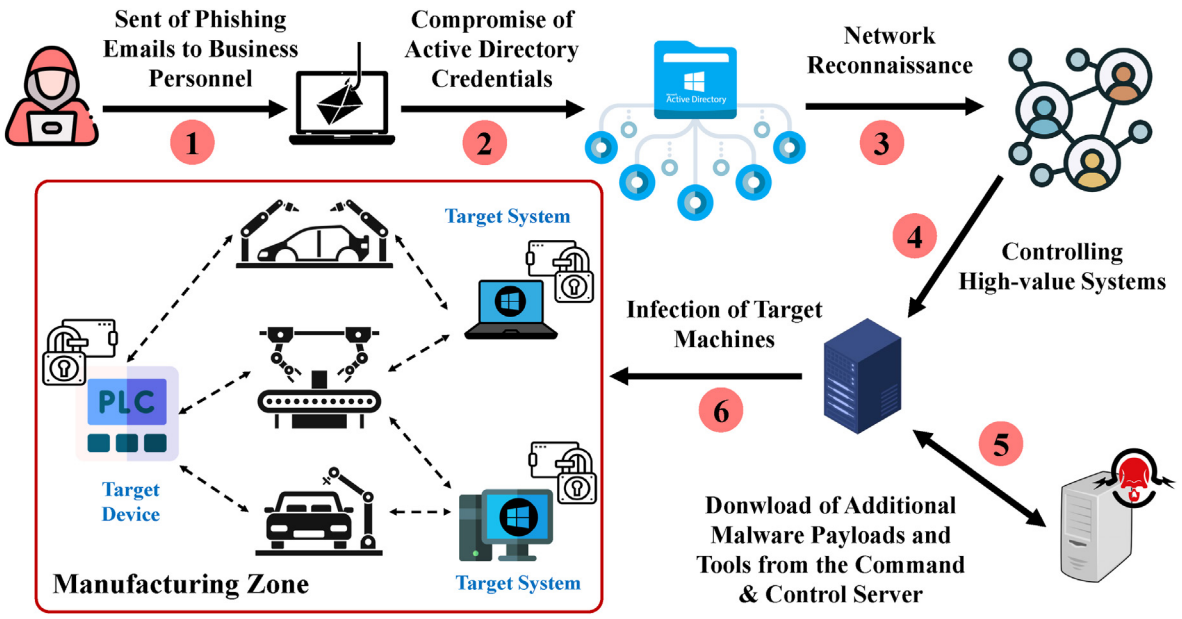

Fig. 6. The ryuk ransomware process.

5.6. CLOP ransomware attack on ExecuPharm (2020)

Global pharmaceutical services provider ExecuPharm faced major disruption in 2020 from a CLOP ransomware attack that encrypted systems across its offices and production facilities in the US and Canada [112].

CLOP infiltrated ExecuPharm's network by exploiting an unpatched VPN gateway vulnerability to achieve initial system access. After compromising file servers and internal infrastructure, CLOP deployed ransomware payloads across connected endpoints.

In addition to encrypting thousands of computers and servers on corporate IT systems, CLOP also impacted OT equipment at ExecuPharm's drug packaging facilities including labeling printers, conveyors, and monitoring systems used in medication bottle assembly lines.

With core pharmaceutical packaging processes disrupted, ExecuPharm suspended production at multiple facilities during remediation, resulting in shipment delays for drug manufacturer clients. CLOP demanded ransom payment in Bitcoin to decrypt scrambled systems across global business units and production networks [113].

While ExecuPharm ultimately restored from backups, CLOP illustrated the risks of inadequate segmentation between IT and plant floor environments, allowing traversal from enterprise into production OT. The attack emphasized needs for strict identity and access controls between IT and industrial systems.

5.7. RansomEXX ransomware attack on Konica Minolta (2020)

Global technology company Konica Minolta[14] suffered major disruption in 2020 from a RansomEXX ransomware attack that encrypted systems across its offices, production facilities, and managed IT networks worldwide [114].

RansomEXX infiltrated Konica Minolta's network by compromising an MSP used by the company, exploiting stolen administrator credentials to achieve initial access. After expanding across file servers and internal infrastructure, RansomEXX deployed ransomware payloads onto managed systems across Konica Minolta's clients.

In addition to encrypting thousands of endpoints across corporate IT systems, RansomEXX also impacted OT networks at Konica Minolta production plants. Industrial controllers, robotics, and automation servers governing digital printer manufacturing lines were disabled [114].

With core production equipment encrypted or disrupted, Konica Minolta had to halt operations at multiple printer and copier factories resulting in shipment delays. RansomEXX demanded a sizable ransom payment in Bitcoin to decrypt scrambled systems across global business units and production networks.

While Konica Minolta restored most capabilities using backups, RansomEXX illustrated risks from third-party MSP compromises traversing into OT systems. The attack emphasized needs for rigorous identity management, network segmentation, and access controls between IT and manufacturing environments.

5.8. BlackMatter ransomware attack on NEW cooperative (2021)

Major US agricultural supplier NEW Cooperative[15] suffered significant disruption in 2021 from the BlackMatter ransomware which encrypted systems for managing grain storage, logistics and food production [115].

The initial intrusion occurred by compromising an internet-facing corporate server using exploits against unpatched vulnerabilities to gain entry. After expanding across Active Directory systems, BlackMatter eventually accessed and infected OT networks monitoring grain storage bins and feed milling automation.

In addition to administrative systems, BlackMatter encrypted industrial controls governing grain handling equipment and feed production machinery across multiple cooperative sites. NEW halted plant operations for over a week during remediation to avoid safety risks from operating production lines blind [116].

The disruptions inflicted during critical agriculture harvest windows increased pressure for NEW to pay the demanded ransom in order to restore encrypted systems and promptly accept crop deliveries from farm suppliers again. The incident illustrated ransomware's leverage against industrial producers supporting vital agriculture value chains.

[14] www.konicaminolta.com.

[15] https://www.newcoop.com.

5.9. DarkSide ransomware attack on Colonial Pipeline (2021)

Colonial Pipeline,[16] the major US fuel transport and logistics company, suffered a devastating ransomware attack in 2021 attributed to the DarkSide ransomware group which disrupted pipeline operations and fuel delivery across the southern and eastern United States [117].

DarkSide infiltrated Colonial's business network after compromising a legacy VPN account through password spraying. Once inside the corporate environment, the ransomware began propagating using Mimikatz for credential theft and other tools to traverse widely across Colonial's enterprise Active Directory infrastructure.

In addition to encrypting IT systems like billing, scheduling, payroll and communications platforms, DarkSide also eventually accessed the OT network monitoring and managing Colonial's vast oil and gas pipeline infrastructure. Pipeline control stations, leak monitoring systems, and other operational equipment had supervision and control capabilities impacted by encryption [118].

With core energy management and logistics systems disabled by the ransomware, Colonial Pipeline proactively shut down approximately 5500 miles of pipeline responsible for nearly half of all fuel transported on the East Coast. This caused severe gasoline shortages and price spikes for millions of consumers dependent on Colonial's delivery infrastructure.

DarkSide demanded a 75 Bitcoin ransom worth nearly $5 million at the time to provide decryption tools to recover scrambled systems [119]. While Colonial ultimately paid the ransom, the disruptions highlighted ransomware's potential for inflicting physical supply chain havoc and energy delivery outages at national scale by traversing unrestrained across IT/OT infrastructure.

5.10. Hive ransomware attack on MediaMarkt (2022)

European consumer electronics retailer MediaMarkt[17] experienced significant disruption in early 2022 from a Hive ransomware attack that encrypted systems across its stores, offices, and distribution centers throughout Europe.

The Hive ransomware operation was behind the attack and infiltrated MediaMarkt's network by exploiting vulnerabilities in its public-facing eCommerce platform to gain initial access. After compromising domain admin credentials, Hive deployed ransomware payloads across thousands of endpoints on corporate systems using tools like Cobalt Strike [120].

In addition to encrypting business data, Hive eventually impacted OT systems and industrial controls supporting logistics automation and inventory management in MediaMarkt's warehouses. This disrupted distribution operations and in-store inventory availability.

With core retail IT and warehouse OT systems encrypted, MediaMarkt had to temporarily close hundreds of stores across Europe during remediation. Hive demanded an unrealistic $240 million ransom payment in cryptocurrency in exchange for decrypting scrambled infrastructure [121].

While most capabilities were restored from backups, Hive demonstrated the extensive impacts possible from ransomware attacks that penetrate across enterprise-retail convergence environments compromising both IT and OT assets.

6. Key lessons and open challenges

By examining major real-world ransomware incidents across CPS environments spanning manufacturing, energy, transportation, healthcare and other sectors, we can derive pivotal lessons regarding adversary tactics, malware innovations, vulnerable architectures and impactful countermeasures. These learnings allow CPS owners to make informed resiliency investments tailored for ransomware protection. We outline key lessons learned followed by priority areas needing focus to address open challenges.

6.1. Lessons learned from ransomware attacks on CPS

6.1.1. Segmenting IT and OT environments restricts ransomware spread

A consistent and hugely impactful theme across numerous major attacks has been ransomware initially compromising conventional IT systems, followed by unconstrained traversal into adjacent cyber-physical process control networks due to flat trust models lacking segmentation between enterprise IT and OT environments.

This highly interconnected architecture with minimal network segregation between office productivity systems and industrial control processes enabled ransomware like LockerGoga and Ryuk to exponentially expand damage by encrypting HMIs, PLCs, safety controllers and other devices governing real-world manufacturing lines, power generation equipment, patient treatments and physical infrastructure operations.

In multiple incidents, compromised enterprise credentials were enough for attackers to easily pivot from encrypting office data to paralzying OT systems monitoring and controlling core physical world operations. The lack of zoning segmentation, network access controls and identity management separating IT from OT allowed adversaries to drastically amplify impact by chaining ransomware expansion from generic office systems into mission-critical ICS assets managing electric grids, water plants, food production lines and medical technology.

In contrast, organizations that proactively invested in robust network segmentation, identity access management and monitoring between conventional IT and industrial control environments proved far more successful in containing ransomware to corporate systems during initial response. While business functions were disrupted by encrypting servers, file shares and productivity tools, proper IT/OT boundaries prevented significant outage of core physical operations during remediation and recovery phases.

As digital transformation and connectivity initiatives further dissolve the traditional demarcation between information and operational technologies, conscious architecture strategies centered on zero trust, least privilege access and network microsegmentation become imperative to limit ransomware blast radius from cascading unconstrained across cyber-physical environments.

6.1.2. Third-party vectors are high-value ransomware targets

Another prominent and progressively more impactful infection vector has been ransomware penetration through third-party vectors like contractors, Managed Service Providers (MSPs) and supply chain partners who often have extraordinarily high levels of trusted access into tightly controlled operational technology environments.

Numerous incidents across water plants, food processors, semiconductor foundries and automotive OEMs (Original Equipment Manufacturers) highlight how adversary compromise of vendor tools, support portals and update mechanisms allowed devastating traversal of ransomware across IT/OT boundaries into customer production networks. By infiltrating MSP monitoring tools, contractor accounts and vendor credential stores, attackers were able to deploy encryption payloads simultaneously across numerous downstream industrial control system networks.

This effectively amplified the scale and impact of campaigns by exploiting shared trust models granting extensive permissions to third-party tools and support mechanisms implanted across industrial customers for configuration, telemetry and troubleshooting purposes. With vast installed bases of legacy systems and remote management portals, these vendor access pathways provide soft underbelly opportunities for adversaries.

Strengthening third-party access governance, implementing least

[16] https://www.colpipe.com.
[17] https://www.mediamarkt.be.

privilege architectures, expanding vendor risk management, and continuously monitoring authentication patterns remain imperative for securing this high-value ransomware attack vector. As connectivity between vendors and industrial operators continues expanding due to efficiency demands, more creative solutions like ephemeral credentials, smart access scoping and proactive session monitoring are necessitated to avoid vendor channels becoming trojan horses invaded by adversaries for mass ransomware deployment.

6.1.3. Targeting enterprise IT to disrupt CPS operations

Historically ransonware campaigns have often been stereotyped as financially motivated cybercrime focused on stealing and encrypting office documents, emails and databases for extortion. But contemporary major attacks have proven targeted encryption or disruption of essential enterprise IT systems supporting cyber-physical system monitoring, engineering, control and coordination can yield huge leverage over victims dependent on continuous smart infrastructure operations.

In numerous incidents across manufacturing plants, power utilities and healthcare networks, ransomware paralyzing file servers, Active Directory servers, manufacturing execution system, alarm notification platforms and internal portals created strong pressures for paying sizable ransoms simply to regain minimal workflow coordination, situational awareness and production scheduling needed to safely manage processes tied to the physical world.

By freezing interactive historian mirrors, model repositories, configuration management databases and version control systems used by engineers, operators could no longer maintain up-to-date situational awareness or safely modify control parameters for infrastructure. Availability of such supporting IT systems is a hidden requirement for reliable CPS operations.

This highlights the need to architect deliberate redundancy for enterprise IT systems providing vital visualization, analytics, simulation, development and authentication capabilities to sustain smart industrial processes and grids. Data historian mirrors with real-time sync, diversified HMI visualization options, replicated version control repositories, and alternative authentication stores represent examples of measures needed to prevent ransomware targeting “non-critical” enterprise systems from cascading into physical operations outage.

6.1.4. Evolving ransomware objectives beyond encryption

The ransomware landscape continues to evolve beyond conventional data encryption for financial extortion to include deliberate process disruption, industrial sabotage, and direct manipulation of physical safety system parameters and settings. Numerous documented campaigns have exhibited adversary willingness to corrupt control logic, force equipment like turbines and motors into physically hazardous states outside safe envelopes, and disable in-built fail-safes and human alerts designed to detect and automatically mitigate unsafe conditions.

Safety instrumented systems, protective relays, emergency shutdown valves and other cyber-physical safety mechanisms continue to be probed and targeted to understand response and assess capability for inflicting real-world damage. Attackers have also demonstrated interest in manipulating physical flows and storage tanks levels for chemicals, oil, gas and water to evaluate potential as environmental attack vectors. These techniques go beyond conventional information encryption to purposefully create industrial accidents and damage scenarios.

Protecting smart infrastructure from such threats requires thinking beyond pure information security to measures focused on true physics-aware system safety assurance spanning cyber, electrical and mechanical layers. Examples include resilient fail-safe designs, air-gapped hardwired safety mechanisms, continuous passive monitoring to detect unexpected protocol manipulation attempts, regular validation of automated safety logic, and robust configuration management for embedded device firmware underpinning last-line physical protections.

As ransomware motivations expand beyond data theft into operational disruption and infrastructure damage, integrating disciplines like reliability engineering, safety assessment and resilience management with cybersecurity becomes imperative for smart CPS protection.

6.2. High priority open challenges

With ransomware adversaries rapidly honing techniques tailored for industrial control system disruption and extortion, securing critical infrastructure requires addressing blindspots in today's defenses. Some high priority areas needing focus include:

6.2.1. Threat modeling frameworks for interconnected CPS

More consistent methodologies based on control theory, graph analytics and adversarial ML are imperative for scientifically modeling ransomware risks across diverse CPS topologies, third-party connections and industrial verticals [122–126]. Physics-aware metrics that can quantitatively assess vulnerability risks and operational impact are needed to prioritize patching and zoning investments.

Automated ransomware propagation simulators need to reflect unique CPS behaviors and responses across ICS, IoT gateways, robotics assets and embedded devices. Models incorporating survivability analysis under ransomware need to account for cascading failures, graceful degradation and infrastructure interdependencies.

6.2.2. High-fidelity cyber-physical digital twin simulation environments

High-fidelity digital twin environments simulating ransomware trajectories across virtualized power plants, manufacturing lines, transportation systems and smart infrastructure would provide predictive intelligence on sequence of events, cascading impacts, infrastructure resilience and recovery insights [127,128].

Simulation-based what-if analysis to identify optimal detection placements, adversary containment strategies, and resilient architecture choices would provide OT cybersecurity teams actionable intelligence for hardening and threat hunting tailored to their environments [129]. Detailed digital twins allow evaluating ransomware response prior to actual attacks.

6.2.3. Adversarial trend analysis focused on CPS

More proactive insights into adversary tactics, techniques and procedures require continued malware reverse engineering and intelligence sharing between public and private organizations. CPS vendors and critical infrastructure sectors tend to examine attacks in isolation rather than collectively identifying cross-vertical ransomware innovations [130,131].

In-depth collaborative analysis of CPS-targeted ransomware code evolution, attack infrastructure, adversarial telemetries and victim profiling is essential for anticipating - and getting ahead of - emerging techniques that could inflict large-scale smart infrastructure outages. Identifying early indicators of adversaries developing CPS domain expertise provides warning to preemptively harden defenses.

6.2.4. Resilient-by-design CPS reference architectures

While zero trust and microsegmentation concepts provide strong foundations, detailed guidance is lacking on ransomware-resilient system architectures specifically spanning IT/OT integration models, CI/CD (Continuous Integration/Continuous Delivery) integration, controller communications, and secure-by-default embedded devices.

CPS-tailored server, network, container, endpoint and field device hardening templates focused on lateral traversal prevention and blast radius containment would help organizations accelerate implementation. Extensible architecture patterns that also address patching orchestration, asset management and rotational diversity could have big impact [132].

6.2.5. Physics-aware risk quantification and metrics

Lack of consistent metrics based on reliability and safety impact for evaluating CPS ransomware preparedness makes risk-driven decision making and investment justification difficult [20]. Most assessments

remain subjective or generic.

Reference frameworks quantifying intrinsic CPS infrastructure resilience based on factors like redundancy, diversity, compartmentalization and designed-in failure containment would enable more scientific risk evaluations and cyber insurance underwriting. Adaptable metrics that align cyber-physical threats to operational goals like availability, safety and responsiveness are needed.

6.2.6. *Threat intelligence sharing frameworks and benchmarks*

Anonymous operational data sharing of ransomware techniques, adversary trends and measured impacts between critical infrastructure operators remains limited but essential to accelerate awareness of what protections are working [133].

Secure telemetry frameworks that allow centralized aggregation and selective querying of key attack characteristics, indicators and defensive successes could dramatically accelerate protection. Interest is expanding in voluntary resilience benchmarking that allows blinded assessments of preparedness across peers.

6.2.7. *Cyber insurance models for OT environments*

Inadequate actuarial data on ransomware impacts spanning costs, recovery timeframes and risk reduction efficiencies for OT hinders insurance models tailored for industrial availability and safety risks.

Anonymous data contribution covering areas like outage durations, replacement part lead times, workaround effectiveness and institute resilience could help differentiate premiums based on intrinsic CPS infrastructure architectures. This allows cost-optimized cyber insurance to incentivize embedding security early across operational environments rather than transferring full risk via premiums [134,135].

6.2.8. *Public-private technology partnerships for resilience*

The asymmetric nature of cyber threats necessitates collaboration between CPS vendors, OT operators and government agencies - spanning areas from resilience R&D to threat intelligence sharing and collective deterrence mechanisms tailored for CPS ransomware threats.

Joint technology initiatives, information exchange platforms, financial support and resources from the public sector combined with rigorous solution R&D and real-world deployment experience from CPS vendors and end-users in the private sector are key to sustainable security against cyber-extortion threats currently outpacing defenses.

But communicating both the acute threats and affordable solutions is essential to motivating resilient-by-design systems that are critical for economic functioning. The imperative lies in preemptive cyber-physical security rather than reactive response.

Addressing these open challenges requires cross-disciplinary efforts combining cybersecurity, reliability engineering and risk economics tailored for the unique risks ransomware poses to cyber-physical system safety and essential service availability. But communicating both the acute threats and affordable solutions is essential to motivating resilient-by-design systems critical for economic functioning.

7. Conclusion

In conclusion, this paper conducted a comprehensive study of ransomware threats targeting cyber-physical systems across multiple industry verticals including manufacturing, energy, transportation, and healthcare. We proposed a dual taxonomy to categorize ransomware attacks based on infection vectors, targets, objectives and technical attributes. Through the analysis of 10 major real-world ransomware incidents on CPS infrastructure, we highlighted key lessons regarding adversary tactics, malware innovations, vulnerable architectures, and impactful countermeasures.

Our analysis revealed several high-priority challenges that need to be addressed to enhance ransomware resilience for CPS environments. These include developing better threat modeling frameworks, creating high-fidelity digital twin simulations, improving adversarial trend analysis, defining resilient-by-design system architectures, quantifying physics-aware risk metrics, increasing threat intelligence sharing, and building effective public-private partnerships.

As ransomware groups continue to refine techniques tailored for industrial control system disruption, organizations need to take a proactive resilient-by-design approach. This requires combining cybersecurity, reliability engineering and risk management disciplines in a cross-disciplinary fashion to safeguard critical infrastructure. Ransomware mitigation for CPS necessitates going beyond pure information security to true physics-aware system safety assurance. We hope this paper provides useful insights to help secure vital CPS infrastructure against one of the most significant cyberthreats faced today.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A.K. Tyagi, N. Sreenath, "Cyber physical systems: analyses, challenges and possible solutions,", Internet of Things and Cyber-Physical Systems 1 (2021) 22–33.
[2] M.A. Aguida, S. Ouchani, M. Benmalek, "A review on cyber-physical systems: models and architectures,", in: 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, 2020, pp. 275–278.
[3] J.P.A. Yaacoub, M. Noura, H.N. Noura, O. Salman, E. Yaacoub, R. Couturier, A. Chehab, "Securing internet of medical things systems: limitations, issues and recommendations,", Future Generat. Comput. Syst. 105 (2020) 581–606.
[4] M.H. Cintuglu, O.A. Mohammed, K. Akkaya, A.S. Uluagac, "A survey on smart grid cyber-physical system testbeds,", IEEE Communications Surveys & Tutorials 19 (1) (2017) 446–464.
[5] J. Lee, B. Bagheri, H.A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems,", Manufacturing Letters 3 (2015) 18–23.
[6] C.V. Lozano, K.K. Vijayan, "Literature review on cyber physical systems design,", Procedia Manuf. 45 (2020) 295–300.
[7] A. Humayed, J. Lin, F. Li, B. Luo, "Cyber-Physical systems security - a survey,", IEEE Internet Things J. 4 (6) (Dec. 2017) 1802–1831.
[8] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, "Cyber-physical systems and their security issues,", Comput. Ind. 100 (2018) 212–223.
[9] Y. Ashibani, Q.H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions,", Comput. Secur. 68 (2017) 81–97.
[10] H. Habibzadeh, B.H. Nussbaum, F. Anjomshoa, B. Kantarci, T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities,", Sustain. Cities Soc. 50 (2019) 101660.
[11] W. Duo, M. Zhou, A. Abusorrah, "A survey of cyber attacks on cyber physical systems: recent advances and challenges,", IEEE/CAA Journal of Automatica Sinica 9 (5) (May 2022) 784–800.
[12] L.P. Nian, D.L.K. Chuen, "Chapter 1 - introduction to bitcoin,", in: D.L.K. Chuen (Ed.), Handbook of Digital Currency, Academic Press, 2015, pp. 5–30, 9780128021170.
[13] S. Faltermaier, K. Strunk, M. Obermeier, M. Fiedler, "Managing organizational cyber security - the distinct role of internalized responsibility,", in: Proceedings of the 56th Hawaii International Conference on System Sciences, 2023, pp. 6098–6106.
[14] S. Rani, A. Kataria, M. Chauhan, P. Rattan, R. Kumar, A.K. Sivaraman, "Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: state-of-art work,", Mater. Today: Proc. 62 (7) (2022) 4671–4676.
[15] R. Paes, D.C. Mazur, B.K. Venne, J. Ostrzenski, "A guide to securing industrial control networks: integrating IT and OT systems,", IEEE Ind. Appl. Mag. 26 (2) (March-April 2020) 47–53.
[16] G. Murray, M.N. Johnstone, C. Valli, "The convergence of IT and OT in critical infrastructure,", in: Proceedings of 15th Australian Information Security Management Conference, Dec. 2017, pp. 149–155.
[17] S.Z. Kamal, S.M. Al Mubarak, B.D. Scodova, P. Naik, P. Flichy, G. Coffin, "IT and OT convergence - opportunities and challenges,", in: The SPE Intelligent Energy International Conference and Exhibition, Aberdeen, Scotland, UK, 2016.
[18] M. McQuade, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 2018.
[19] N.A. Hassan, "Ransomware families,", in: Ransomware Revealed, Apress, Berkeley, CA, 2019.
[20] J.P.A. Yaacoub, O. Salman, H.N. Noura, N. Kaaniche, A. Chehab, M. Malli, "Cyber-physical systems security: limitations, issues and future trends,", Microprocess. Microsyst. 77 (2020) 103201.
[21] B.A.S. Al-rimy, M.A. Maarof, S.Z.M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions,", Comput. Secur. 74 (2018) 144–166.

[22] A. Tandon, A. Nayyar, "A comprehensive survey on ransomware attack: a growing havoc cyberthreat,", in Data Management, Analytics and Innovation: Proceedings of ICDMAI 2018 2 (2019) 403–420.
[23] A.M. Maigida, et al., "Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms,", Journal of Reliable Intelligent Environments 5 (2019) 67–89.
[24] D.W. Fernando, N. Komninos, T. Chen, "A study on the evolution of ransomware detection using machine learning and deep learning techniques,", IoT 1 (2) (2020) 551–604.
[25] M. Humayun, N.Z. Jhanjhi, A. Alsayat, V. Ponnusamy, "Internet of things and ransomware: evolution, mitigation and prevention,", Egyptian Informatics Journal 22 (1) (2021) 105–117.
[26] S. Sharma, R. Kumar, C. Rama Krishna, "A survey on analysis and detection of Android ransomware,", Concurrency Comput. Pract. Ex. 33 (16) (2021) e6272.
[27] R. Moussaileb, N. Cuppens, J.L. Lanet, H.L. Bouder, "A survey on windows-based ransomware taxonomy and detection mechanisms,", ACM Comput. Surv. 54 (6) (2021) 1–36.
[28] C. Beaman, A. Barkworth, T.D. Akande, S. Hakak, M.K. Khan, "Ransomware: recent advances, analysis, challenges and future research directions,", Comput. Secur. 111 (2021) 102490.
[29] H. Oz, A. Aris, A. Levi, A.S. Uluagac, "A survey on ransomware: evolution, taxonomy, and defense solutions,", ACM Comput. Surv. 54 (11s) (2022) 1–37.
[30] S. Razaulla, et al., "The age of ransomware: a survey on the evolution, taxonomy, and research directions,", IEEE Access 11 (2023) 40698–40723.
[31] K. Begovic, A. Al-Ali, Q. Malluhi, Cryptographic Ransomware Encryption Detection: Survey, Computers & Security, 2023 103349.
[32] A. Daneels, W. Salter, "What is SCADA?", International Conference on Accelerator and Large Experimental Physics Control Systems (1999) 339–343.
[33] M. Benmalek, K. Harkat, K.D. Haouam, Z. Gheid, "SE-CDR: enhancing security and efficiency of key management in internet of energy consumer demand-response communications,", 4, in: International Journal of Safety and Security Engineering 13, 2023, pp. 611–623.
[34] S. Ali, T. Al Balushi, Z. Nadir, O.K. Hussain, "ICS/SCADA system security for CPS,", in: Cyber Security for Cyber Physical Systems. Studies in Computational Intelligence vol. 768, Springer, 2018.
[35] B. Galloway, G.P. Hancke, "Introduction to industrial control networks,", IEEE Communications Surveys & Tutorials 15 (2) (2013) 860–880.
[36] M. Benmalek, Y. Challal, A. Derhab, "Authentication for smart grid AMI systems: threat models, solutions, and challenges,", in: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, 2019, pp. 208–213.
[37] A. Gatouillat, Y. Badr, B. Massot, E. Sejdić, "Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine,", IEEE Internet Things J. 5 (5) (Oct. 2018) 3810–3822.
[38] I. Lee, O. Sokolsky, "Medical cyber physical systems,", in: Proceedings of 47th Design Automation Conference, NY, USA, 2010, pp. 743–748.
[39] A.V. Jha, B. Appasani, A.N. Ghazali, P. Pattanayak, D.S. Gurjar, E. Kabalci, D.K. Mohanta, "Smart grid cyber-physical systems: communication technologies, standards and challenges,", Wireless Network 27 (2021) 2595–2613.
[40] S.K. Khaitan, J.D. McCalley, C.C. Liu, Cyber Physical Systems Approach to Smart Electric Power Grid, Springer, 2015, 9783662459270.
[41] K.R. Davis, C.M. Davis, S.A. Zonouz, R.B. Bobba, R. Berthier, L. Garcia, et al., "A cyber-physical modeling and assessment framework for power grid infrastructures,", IEEE Trans. Smart Grid 6 (5) (2015) 2464–2475.
[42] A.A. Alshdadi, "Cyber-physical system with IoT-based smart vehicles,", Soft Comput. 25 (2021) 12261–12273.
[43] A. Pundir, S. Singh, M. Kumar, A. Bafila, G.J. Saxena, "Cyber-Physical systems enabled transport networks in smart cities: challenges and enabling technologies of the new mobility era,", IEEE Access 10 (2022) 16350–16364.
[44] S.P. Mohanty, "Advances in transportation cyber-physical system (T-CPS),", 4, in: IEEE Consumer Electronics Magazine 9, 2020, pp. 4–6.
[45] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin, "Cybersecurity for industrial control systems: a survey,", Comput. Secur. 89 (2020) 101677.
[46] W. Knowles, D. Prince, D. Hutchison, J.F.P. Disso, K. Jones, "A survey of cyber security management in industrial control systems,", in: International Journal of Critical Infrastructure Protection 9, 2015, pp. 52–80.
[47] M.A. Aguida, S. Ouchani, M. Benmalek, "An IoT-based framework for an optimal monitoring and control of cyber-physical systems: application on biogas production system,", in: Proceedings of the 11th International Conference on the Internet of Things, 2021, pp. 143–149.
[48] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, Y. Halgand, A Survey of Approaches Combining Safety and Security for Industrial Control Systems, vol. 139, Reliability Engineering & System Safety, 2015, pp. 156–178.
[49] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.R. Sadeghi, M. Maniatakos, R. Karri, "The cybersecurity landscape in industrial control systems,", Proc. IEEE 104 (5) (May 2016) 1039–1057.
[50] Z. Drias, A. Serhrouchni, O. Vogel, "Analysis of cyber security for industrial control systems,", in: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC), Shanghai, China, 2015, pp. 1–8.
[51] M.N. Al-Mhiqani, R. Ahmad, W. Yassin, A. Hassan, Z.Z. Abidin, N.S. Ali, K.H. Abdulkareem, "Cyber-Security incidents: a review cases in cyber-physical systems,", Int. J. Adv. Comput. Sci. Appl. 9 (1) (2018) 499–508.
[52] A.H. El-Kady, S. Halim, M.M. El-Halwagi, F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems,", Process Saf. Environ. Protect. 173 (2023) 384–413.
[53] H. Kayan, M. Nunes, O. Rana, P. Burnap, C. Perera, "Cybersecurity of Industrial Cyber-Physical Systems: A Review" in ACM Computing Surveys 54 (11s) (2022) 1–35.
[54] B.A.S. Al-rimy, M.A. Maarof, S.Z.M. Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: a survey and research directions,", Comput. Secur. 74 (2018) 144–166.
[55] P.H. Meland, Y.F.F. Bayoumy, G. Sindre, "The Ransomware-as-a-Service economy within the darknet,", Comput. Secur. 92 (2020) 101762.
[56] R. Davidson, "The fight against malware as a service,", Netw. Secur. 2021 (8) (2021) 7–11.
[57] P. O'Kane, S. Sezer, D. Carlin, "Evolution of ransomware,", IET Netw. 7 (5) (2018) 321–327.
[58] K.P. Subedi, D.R. Budhathoki, D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis,", in: 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2018, pp. 180–185.
[59] P.L. Gallegos-Segovia, J.F. Bravo-Torres, V.M. Larios-Rosillo, P.E. Vintimilla-Tapia, I.F. Yuquilima-Albarado, J.D. Jara-Saltos, "Social engineering as an attack vector for ransomware,", in: 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), Pucon, Chile, 2017, pp. 1–6.
[60] V.K. Anand, K. Bamanjogi, A.R. Shaw, M. Faheem, "Comparative study of ransomwares,", in: 2022 7th International Conference on Computing, Communication and Security (ICCCS), Seoul, Korea, Republic of, 2022, pp. 1–9.
[61] A.H. Mohammad, "Ransomware evolution, growth and recommendation for detection,", Mod. Appl. Sci. 14 (3) (2020) 68.
[62] M.A. Mos, M.M. Chowdhury, "The growing influence of ransomware,", in: 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 2020, pp. 643–647.
[63] S. Poudyal, D. Dasgupta, "AI-Powered ransomware detection framework,", in: 2020 IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, ACT, Australia, 2020, pp. 1154–1161.
[64] P. Bajpai, R. Enbody, "Dissecting. net ransomware: key generation, encryption and operation,", Netw. Secur. 2020 (2) (2020) 8–14.
[65] S. Saeed, N.Z. Jhanjhi, M. Naqvi, M. Humayun, S. Ahmed, "Ransomware: a framework for security challenges in internet of things,", in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Saudi Arabia, Sakaka, 2020, pp. 1–6.
[66] A. Bello, A. Maurushat, "Technical and behavioural training and awareness solutions for mitigating ransomware attacks,", in: Applied Informatics and Cybernetics in Intelligent Systems, 2020, pp. 164–176.
[67] S. Sharmeen, Y.A. Ahmed, S. Huda, B.Ş. Koçer, M.M. Hassan, "Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches,", IEEE Access 8 (2020) 24522–24534.
[68] S.Y. Yu, A.V. Malawade, S.R. Chhetri, M.A. Al Faruque, "Sabotage attack detection for additive manufacturing systems,", IEEE Access 8 (2020) 27218–27231.
[69] J. Hernandez-Castro, A. Cartwright, E. Cartwright, "An economic analysis of ransomware and its welfare consequences,", R. Soc. Open Sci. 7 (3) (2020) 190023.
[70] O. Givehchi, K. Landsdorf, P. Simoens, A.W. Colombo, "Interoperability for industrial cyber-physical systems: an approach for legacy systems,", IEEE Trans. Ind. Inf. 13 (6) (Dec. 2017) 3370–3378.
[71] S. Tan, J.M. Guerrero, P. Xie, R. Han, J.C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems,", IEEE Syst. J. 14 (4) (Dec. 2020) 5329–5339.
[72] D.G. Pivoto, et al., "Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: a literature review,", J. Manuf. Syst. 58 (2021) 176–192.
[73] H. Riggs, S. Tufail, I. Parvez, M. Tariq, M.A. Khan, A. Amir, K.V. Vuda, Sarwat, "Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure,", Sensors 23 (8) (2023) 4060.
[74] O. Ude, B. Swar, "Securing remote access networks using malware detection tools for industrial control systems,", in: 2021 4th IEEE International Conference on Industrial Cyber-Physical Systems (ICPS), Victoria, BC, Canada, 2021, pp. 166–171.
[75] N. Daswani, M.M. Elbayadi, "Technology defenses to fight the root causes of breach: Part One,", in: Big Breaches, Apress, Berkeley, CA, 2021.
[76] M. Burmester, E. Magkos, V. Chrissikopoulos, "Modeling security in cyber-physical systems,", 3–4, in: International Journal of Critical Infrastructure Protection 5, 2012, pp. 118–126.
[77] J.P. Farwell, R. Rohozinski, "Stuxnet and the future of cyber war,", Survival 53 (1) (2011) 23–40.
[78] P. Huitsing, R. Chandia, M. Papa, S. Shenoi, "Attack taxonomies for the Modbus protocols,", in: International Journal of Critical Infrastructure Protection 1, 2008, pp. 37–44.
[79] S. East, J. Butts, M. Papa, S. Shenoi, "A taxonomy of attacks on the DNP3 protocol,", ICCIP 2009: Critical Infrastructure Protection III 311 (2009) 67–81.
[80] A. Elgargouri, M. Elmusrati, "Analysis of cyber-attacks on IEC 61850 networks,", in: 2017 IEEE 11th International Conference on Application of Information and Communication Technologies, AICT), Moscow, Russia, 2017, pp. 1–4.
[81] J. Ibarra, U. Javed Butt, A. Do, H. Jahankhani, A. Jamal, "Ransomware impact to SCADA systems and its scope to critical infrastructure,", in: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability, ICGS3), London, UK, 2019, pp. 1–12.
[82] S.M. Khalil, H. Bahsi, H.O. Dola, T. Korotko, K. McLaughlin, V. Kotkas, "Threat modeling of cyber-physical systems - a case study of a microgrid system,", Comput. Secur. 124 (2023) 102950.

[83] A. Zimba, Z. Wang, H. Chen, "Multi-stage crypto ransomware attacks: a new emerging cyber threat to critical infrastructure and industrial control systems,", ICT Express 4 (1) (2018) 14–18.
[84] H. Oz, A. Aris, A. Levi, A.S. Uluagac, "A survey on ransomware: evolution, taxonomy, and defense solutions,", ACM Comput. Surv. 54 (11s) (2022) 37.
[85] G.V. Santangelo, V.G. Colacino, M. Marchetti, Analysis, Prevention and Detection of Ransomware Attacks on Industrial Control Systems, IEEE 20th International Symposium on Network Computing and Applications (NCA), Boston, MA, USA, 2021, pp. 1–5.
[86] G. Falco, R. Thummala, A. Kubadia, "WannaFly: an approach to satellite ransomware,", in: 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT), Pasadena, CA, USA, 2023, pp. 84–93.
[87] M. Gazzan, F.T. Sheldon, "Opportunities for early detection and prediction of ransomware attacks against industrial control systems,", Future Internet 15 (4) (2023) 144.
[88] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, "Cutting the gordian knot: a look under the hood of ransomware attacks,", in: DIMVA 2015: Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3–24.
[89] T. Alladi, V. Chamola, S. Zeadally, "Industrial control systems: cyberattack trends and countermeasures,", Comput. Commun. 155 (2020) 1–8.
[90] P. Sindhwad, F. Kazi, "Exploiting control device vulnerabilities: attacking cyber-physical water system,", in: 2022 32nd Conference of Open Innovations Association (FRUCT), Finland, Tampere, 2022, pp. 270–279.
[91] A. Dalvi, S. Salve, G. Zape, F. Kazi, S.G. Bhirud, "Security of cyber-physical systems through the lenses of the dark web,", in: 2021 International Conference on Intelligent Cyber-Physical Systems, ICPS), Singapore, 2021, pp. 39–50.
[92] M. Al-Hawawreh, F.d. Hartog, E. Sitnikova, "Targeted ransomware: a new cyber threat to edge system of brownfield industrial internet of things,", IEEE Internet Things J. 6 (4) (2019) 7137–7151.
[93] N. Kshetri, J. Voas, "Ransomware as a business (RaaB),", IT Professional 24 (2) (2022) 83–87.
[94] S.Y.A. Fayi, "What petya/NotPetya ransomware is and what its remidiations are,", in: Information Technology - New Generations, 2018, pp. 93–100.
[95] R.A. Lika, D. Murugiah, S.N. Brohi, D. Ramasamy, "NotPetya: cyber attack prevention through awareness via gamification,", in: 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, 2018, pp. 1–6.
[96] S.Y.A. Fayi, "What Petya/NotPetya ransomware is and what its remidiations are,", in: Information Technology-New Generations: 15th International Conference on Information Technology, 2018, pp. 93–100.
[97] Z. Liu, C. Chen, L.Y. Zhang, S. Gao, "Working mechanism of eternalblue and its application in ransomworm,", in: CSS 2022: Cyberspace Safety and Security, 2022, pp. 178–191.
[98] S. Furnell, D. Emm, "The ABC of ransomware protection,", Comput. Fraud Secur. 2017 (10) (2017) 5–11.
[99] R. Chaudhary, G.S. Aujla, N. Kumar, S. Zeadally, "Lattice-Based public key cryptosystem for internet of things environment: challenges and solutions,", IEEE Internet Things J. 6 (3) (Jun. 2019) 4897–4909.
[100] S. Mansfield-Devine, "Ransomware: the most popular form of attack,", Comput. Fraud Secur. 2017 (10) (2017) 15–20.
[101] A. Wirth, "The times they are a-changin': Part One,", Biomed. Instrum. Technol. 52 (2) (2018) 148–152.
[102] A. Kumar, A. Singh, A. Sengupta, "Securing cyber-resilience in healthcare sector,", in: Cyber Security in Intelligent Computing and Communications, 2022, pp. 211–226.
[103] A. Zimba, M. Chishimba, "Understanding the evolution of ransomware: paradigm shifts in attack structures,", Int. J. Comput. Netw. Inf. Secur. 11 (1) (2019) 26.
[104] S. Leppanen, S. Ahmed, R. Granqvist, "Cyber security incident report—norsk Hydro,", in: Procedia Economics and Finance, 11 pages, 2019.
[105] P. Nakhonthai, K. Chimmanee, "Digital forensic analysis of ransomware attacks on industrial control systems: a case study in factories,", in: 2022 6th International Conference on Information Technology (InCIT), Nonthaburi, Thailand, 2022, pp. 416–421.
[106] I.A. Chesti, M. Humayun, N.U. Sama, N. Jhanjhi, "Evolution, mitigation, and prevention of ransomware,", in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Saudi Arabia, Sakaka, 2020, pp. 1–6.
[107] M. Lehto, "Cyber-Attacks against critical infrastructure," in *cyber security*, Computational Methods in Applied Sciences 56 (2022) 3–42.
[108] P. O'Connor, "2020 security review: a year that shook IT,", Itnow 62 (4) (2020) 40–41.
[109] H.Y. Kwon, T. Kim, M.K. Lee, "Advanced intrusion detection combining signature-based and behavior-based detection methods,", Electronics 11 (6) (2022) 867.
[110] S.R. Davies, R. Macfarlane, W.J. Buchanan, "Differential area analysis for ransomware attack detection within mixed file datasets,", Comput. Secur. 108 (2021) 102377.
[111] A.C. S, R. Shanker, "Zero trust resilience strategy for linux crypto ransomware obviation and recuperation,", in: 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 2023, pp. 1–7.
[112] A. Adler, J. Beal, M. Lancaster, D. Wyschogrod, "Cyberbiosecurity and public health in the age of COVID-19,", in: Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues, 2021, pp. 103–115.
[113] K. Coffey, Standing up to Hackers: Article III Standing for Victims of Data Breaches, vol. 77, University of Miami Law Review, 2022, p. 295.
[114] M.A. Vander–Pallen, P. Addai, S. Isteefanos, T.K. Mohd, "Survey on types of cyber attacks on operating system vulnerabilities since 2018 onwards,", in: 2022 IEEE World AI IoT Congress (AIIoT), 2022, pp. 1–7.
[115] M. Hazrati, R. Dara, J. Kaur, "On-farm data security: practical recommendations for securing farm data,", Front. Sustain. Food Syst. 6 (2022) 884187.
[116] S. Santos, P. Costa, A. Rocha, "IT/OT convergence in industry 4.0 : risks and analisy of the problems,", in: 2023 18th Iberian Conference on Information Systems and Technologies (CISTI), Aveiro, Portugal, 2023, pp. 1–6.
[117] J. Beerman, D. Berent, Z. Falter, S. Bhunia, "A review of colonial pipeline ransomware attack,", in: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW), Bangalore, India, 2023, pp. 8–15.
[118] J.W. Goodell, S. Corbet, "Commodity market exposure to energy-firm distress: evidence from the Colonial Pipeline ransomware attack,", Finance Res. Lett. 51 (2023) 103329.
[119] N. Kshetri, J. Voas, "Ransomware: pay to play?,", Computer 55 (3) (2022) 11–13.
[120] G. Kim, S. Kim, S. Kang, J. Kim, "A method for decrypting data infected with hive ransomware,", J. Inf. Secur. Appl. 71 (2022) 103387.
[121] L. Abrams, MediaMarkt Hit by Hive Ransomware, Initial $240 Million Ransom, BleepingComputer, 2021. https://www.bleepingcomputer.com/news/security/mediamarkt-hit-by-hive-ransomware-initial-240-million-ransom/.
[122] A.M. Jamil, L. Ben Othmane, A. Valani, "Threat modeling of cyber-physical systems in practice,", in: Proceedings of the International Conference on Risks and Security of Internet and Systems, 2021, pp. 3–19.
[123] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, "STRIDE-based threat modeling for cyber-physical systems,", in: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Turin, Italy, 2017, pp. 1–6.
[124] S.M. Khalil, H. Bahsi, H. Ochieng'Dola, T. Korõtko, K. McLaughlin, V. Kotkas, "Threat modeling of cyber-physical systems-A case study of a microgrid system,", Comput. Secur. 124 (2023) 102950.
[125] I. Zografopoulos, J. Ospina, X. Liu, C. Konstantinou, "Cyber-Physical energy systems security: threat modeling, risk assessment, resources, metrics, and case studies,", IEEE Access 9 (2021) 29775–29818.
[126] H. Almohri, L. Cheng, D. Yao, H. Alemzadeh, On threat modeling and mitigation of medical cyber-physical systems,", in: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies, CHASE), Philadelphia, PA, USA, 2017, pp. 114–119.
[127] W.D. Lin, "An integrated digital twin simulation and scheduling system under cyber-physical digital twin environment,", in: 2022 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Kuala Lumpur, Malaysia, 2022, pp. 231–235.
[128] G. Caiza, R. Sanz, "Digital twin to control and monitor an industrial cyber-physical environment supported by augmented reality,", Appl. Sci. 13 (13) (2023) 7503.
[129] C. Qian, X. Liu, C. Ripley, M. Qian, F. Liang, W. Yu, "Digital twin—cyber replica of physical things: architecture, applications and future research directions,", Future Internet 14 (2) (2022) 64.
[130] J. Li, Y. Liu, T. Chen, Z. Xiao, Z. Li, J. Wang, "Adversarial attacks and defenses on cyber–physical systems: a survey,", IEEE Internet Things J. 7 (6) (2020) 5103–5115.
[131] F.O. Olowononi, D.B. Rawat, C. Liu, "Resilient machine learning for networked cyber physical systems: a survey for machine learning security to securing machine learning for CPS,", IEEE Communications Surveys & Tutorials 23 (1) (2021) 524–552.
[132] A.S. Jin, et al., "Resilience of cyber-physical systems: role of AI, digital twins, and edge computing,", IEEE Eng. Manag. Rev. 50 (2) (2022) 195–203.
[133] N. Mtukushe, A.K. Onaolapo, A. Aluko, D.G. Dorrell, "Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems,", Energies 16 (13) (2023) 5206.
[134] S. Amin, G.A. Schwartz, A. Hussain, "In quest of benchmarking security risks to cyber-physical systems,", IEEE Network 27 (1) (2013) 19–24.
[135] A.A. Malik, D.K. Tosh, "Quantitative risk modeling and analysis for large-scale cyber-physical systems,", in: 2020 29th International Conference on Computer Communications and Networks, ICCCN), Honolulu, HI, USA, 2020, pp. 1–6.