Types of Cyber Attacks on Critical Infrastructure

Subjects: Engineering, Electrical & Electronic

Contributor: Hugo Riggs , Shahid Tufail , Imtiaz Parvez , Mohd Tariq , Mohammed Aquib Khan , Asham Amir , Kedari Vineetha Vuda , Arif I. Sarwat

Several critical infrastructures are integrating information technology into their operations, and as a result, the cyber attack surface extends over a broad range of these infrastructures. Cyber attacks have been a serious problem for industries since the early 2000s, causing significant interruptions to their ability to produce goods or offer services to their clients. The thriving cybercrime economy encompasses money laundering, black markets, and attacks on cyber-physical systems that result in service disruptions. Furthermore, extensive data breaches have compromised the personally identifiable information of millions of people.

computer networks cyber attack signal detection machine learning smart grid

1. Introduction

The projection shown in **Figure 1** was conducted from the data collected by the Center for Strategic and International Studies (CSIS) in Washington, D.C. The CSIS provides a significant cyber attack list [1]. The CSIS defines a significant cyber attack as one that results in at least USD 1 million in damage. Significant cyber attacks are defined as cyber attacks on government agencies, defense, and high-tech companies, or attacks on other CIs that cause losses of more than USD 1 million **Figure 1** shows the total number of significant cyber attacks measured and includes a projection of expected attacks through 2025. The projection, using polynomial regression, shows that there will be more significant cyber attacks in the next five years than the combined significant cyber attacks since 2005. The list from CSIS was further analyzed based on a keyword search to relate the cyber attack to a specific critical infrastructure. For example, if the cyber attack targeted a military base, it was attributed to the military CI, and if an attack contained the words financial or banking, it was included in the financial CI. The significant attacks per-CI are shown in **Figure 2**. The following sections expand on the discussion of the disruptive cybercrime economy. The sections also enumerates the various top-level cyber attack types with some of their sub-variants.

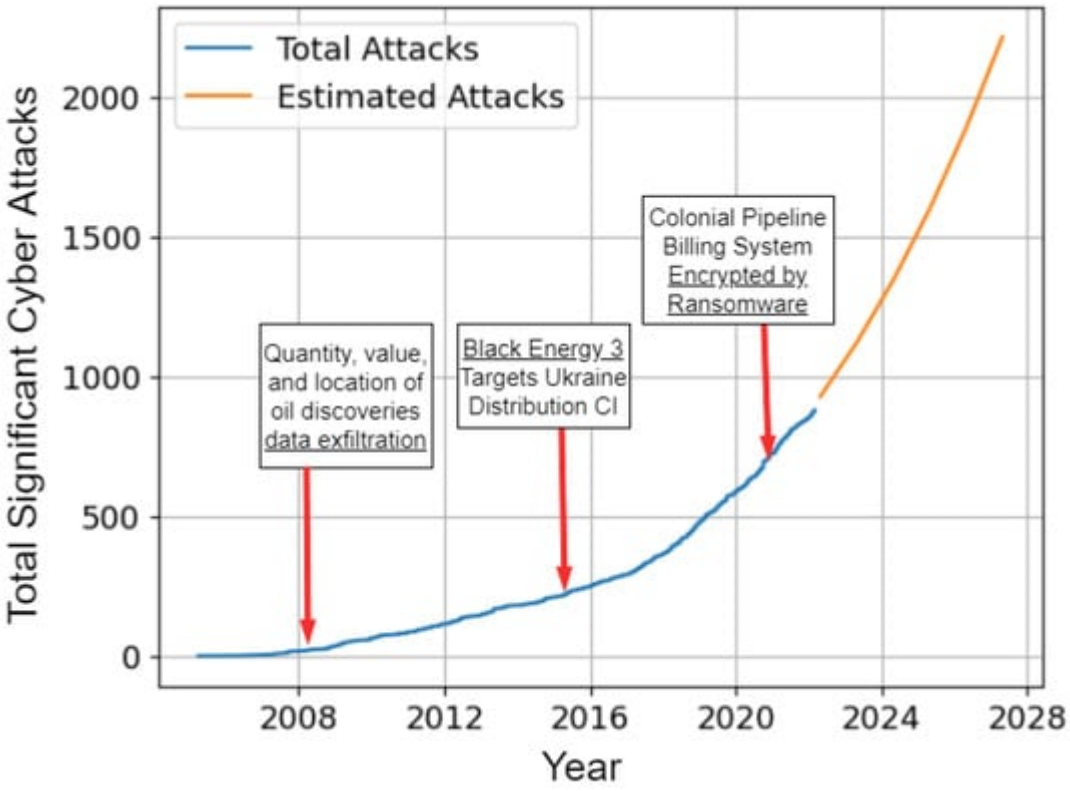

Figure 1. Estimate: cyber attacks will increase exponentially.

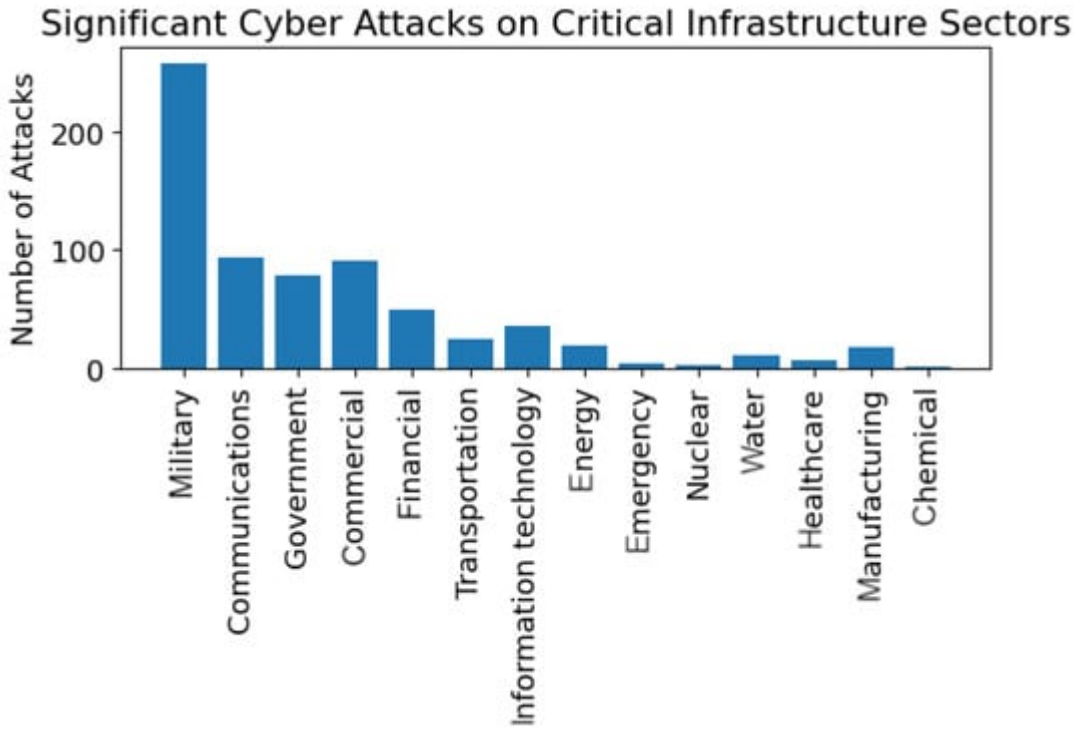

Figure 2. Significant cyber attacks by the CI sector since 2006, analyzed from the CSIS incidents list.

2. Cybercrime Economy

The cybercriminal economy has emerged worldwide, enabling many types of cyber attack functions as a service. However, while the focus is on cyber attacks in these sections, the cybercrime economy enables many other types of criminal activity. In [2], a literature review yields an extensive and consistent survey of the services used by the cybercrime business, organized using the value chain perspective, to understand cyber attacks systematically. Further, an understanding of the specialization, commercialization, and cooperation in coordinating a cyber attack is developed. They identify 24 value-added activities and their relations in the cybercrime market. These can be offered “as a service” for use in a cyber attack. The framework in [2] of cyber attacks “as a service” helps us understand the modern cybercriminal ecosystem and hacking innovations. Some services that facilitate cyber attacks include training and recruiting, development of exploitative software, scanning networks, denying service, phishing, target ranking, and money laundering. These services are provided as subscriptions, licenses, pay-per-records, or commission-based services [2][3]. The prominent concern for CIs is APTs. APTs are groups that are supported by their host nations and perform long-term targeting of the victim’s CI. The general goal of APTs is to steal data from the victim. However, they also target the control management systems and components [3] of CI. The critical importance of the power infrastructure to the socioeconomic stability and the effect of blackouts make the smart grid a primary target [4]. APTs represent a subset of the cybercrime economy, and an APT is often a benefit to the host nation’s economy, as they are compensated for their actions. This is due to the subterfuge of critical infrastructures slowing the economies of competitors to the host nation. An emergent factor for the electrical infrastructure is electricity theft, which is a major contributor to nontechnical losses in the distribution systems of the smart grid [5].

Money Laundering, Theft, Black Markets, and Ransom

One role of the cybercrime economy is in money laundering. This activity is evident in the use of cryptocurrencies for financial exchange from the victims to the attacker. A cryptocurrency transaction occurs, such as a ransom payment, and it is exchanged into another currency by the attacker. Cryptocurrencies lend themselves to this practice as they are functional currencies for communication networks that operate outside of traditional banks [6]. Trojan malware can facilitate information theft. If an enterprise system is compromised and the database is accessed to steal personally identifiable information, this information can be sold online. Online black markets exist, and they are frequently pursued by law enforcement and shut down. However, popular and well-known digital black markets commonly re-emerge at a new location, as moving software frameworks throughout different IT infrastructures is easily facilitated [7][8][9]. Another example of the function of the cybercriminal economy involves the ransom of critical computer systems. These ransomware-based attacks are targeted against critical services, such as utilities and hospitals [10]. The reasons for targeting these services are clear. They are critical for the public, and victims are willing to pay significant amounts of money to free their computer systems from ransomware. This is simply because it is less expensive for them to pay the ransom and recover their systems than remain out of operation [11].

3. The Ransomware Cyber Attack

A ransomware's malicious action is to either encrypt, lock, or exfiltrate data, and the ransomware will be specialized for the target platform. The variety of operating systems means that system-specific libraries and functions will be used by the ransomware to perform malicious actions. Mostly, they will target PC/workstations with a Windows operating system [12]. Within the cybercrime economy, some groups operate as Ransomware-as-a-Corporation (RAAC). Attackers operating as RAAC frequently issue press releases and use corporate language in their communications. If the ransom is not paid, then the victims' operational systems will remain inaccessible, and any critical personal information that has been exfiltrated will be posted on a dark web leak site to damage the company's reputation and business processes [7].

Although current ransomware campaigns do not target CPS, the installation of more intelligent electronic devices in the field by CI makes the CI and its CPS a more likely target for ransomware. As smart technologies continue to expand and integrate into homes, transportation, buildings, and throughout cities, they will become a growing target in the future development of ransomware that targets this new environment. Thus, ransomware that targets industrial CPS intelligent electronic devices will become more prevalent [12][13][14][15].

Most commonly, e-mails are the delivery method of ransomware. Malicious e-mails carry ransomware as an attachment, which contains the malware. These messages are often sent as spam broadcast to as many e-mail addresses as possible or can be directed and tailored to specific individuals or organizations. The attachment can provide a link or file that initiates the installation of ransomware [12].

Encryption ransomware prevents victims from accessing their files by encrypting them with a secret key. The key and decryption software are then used for ransom. With advances in ransomware design, more targeted algorithms are used in encryption to specifically target file types of higher value to the victim. This reduces the time needed to perform the malicious encryption action after infecting the victim's computer. Locking ransomware has a similar goal to encryption-based malware, but it targets locking mechanisms designed to lock a system, such as a master boot record lock, screen lock, or computer desktop lock. The malware uses built-in security systems to lock the victim out of their computer system [16]. Finally, an information theft ransomware exfiltrates personally identifiable information (PII) from a victim's computer. The stolen PII is advertised to the victim as blackmail, and ransom is paid to prevent the publishing of the PII.

Supply Chain Ransomware

This type of ransomware is distributed through a trusted software distribution mechanism, particularly through a software updater provided by an IT service company. The attack was worldwide and affected businesses such as pharmacies, railways, and storefronts. The attack exploited a vulnerability in the IT service company's software updating system, which compromised the businesses that relied on it for updates [17].

4. Denial of Service

In the DoS attack the attacker prevents the intended user from accessing a resource. The attacker can reduce the intended user's access to the server by flooding the network i.e., increasing the traffic to disrupt access to a service. The attacker also attempts to break the connectivity between two systems [18]. Flooding services make the system receive too much traffic for the servers to handle. Flooding a system slows the system down and can ultimately halt the system.

The implication of DoS-based electricity theft against the energy CI is shown in the experimental results. The growing installation of intelligent electronic devices in CPS and the Internet of Things (IoT) domestic devices, such as connected homes and smart appliances, also increases the potential damage to CI from DoS attacks. The proliferation of more internet-connected grid technologies creates an increased vulnerability to such attacks [19].

4.1. Flooding in Mesh Networks

A utility can implement advanced meter infrastructure (AMI) using large wireless mesh networks. However, delays in wireless sensor networks can be caused by network flooding attacks. A malicious node in a wireless mesh network can tamper with messages that are sensitive to flooding attacks, resulting in a saturation of the AMI network. The DoS attack will come from a malicious node or nodes in the mesh network, sending excessive unnecessary data packets throughout the network and issuing excessive requests for communication. This traffic congests the mesh network and forms the basis of the flooding attack, which is identified as a DoS and impacts the network by increasing the latency of the communications [20][21].

IEC 62351 assigns digital signatures as a requirement for low-latency critical communication in ICS. However, digitally signed messages in wireless mesh networks are vulnerable to flooding DoS attacks, as demonstrated in [22], in which a model of phasor measurement data collection and transmission was subjected to flooding DoS. The flooding blocked the phasor measurement unit from transmitting data to the load flow control center. This type of interruption can affect the decision-making processes of the control center and generation control centers. In [19], an experiment with a consumer meter was performed, in which the meter was subjected to a flooding cyber attack. The flooding attack caused the meter to under-report the average watt-hour consumed at a rate of 1.77% less reported power consumption after four days. Other intelligent electronic devices may also be targeted. In [23], experimental signal jamming is performed on wireless networks against IEC 62351-based technologies. The GOOSE substation protocol is evaluated on a WiFi-based wireless power network, and the reactive jamming resulted in an 88% degraded throughput. Time-critical messaging is affected, resulting in latency overshooting the maximum message delay constraints.

4.2. Incidents of Denial of Service Attack

In 2000, a DoS attack on Yahoo rendered the site non-operational for more than 3 h. The attack was based on a Smurf attack and a Tribe Flood Network Technique. Through this attack, Yahoo received data requests of around or greater than one gigabyte per second [18]. Another DoS attack on the electric grid operations of Los Angeles County in California and Salt Lake County in Utah interrupted the electrical system operations for more than 10 h. It

affected the computer systems used within the electrical utilities responsible for running the office functions. The attack had little impact on power delivery, but it raises concerns about the future if proper steps are not taken to mitigate such attacks [24].

5. Man-in-the-Middle

This Man-in-the-Middle (MITM) cyber attack is a kind of cyber attack where an outsider enters between two communication nodes and tries to remain undetected. The MITM can change the routed information before the information reaches the other node. This cyber attack accesses, reads, changes, or modifies the secret information without the victim's detecting manipulation. One capability involves injecting new messages and another involves the capacity to intercept all messages. Despite cryptography, a successful MITM attacker compromises exchanges between two systems. The MITM is either a passive listener or imitates one of the parties and manipulates the data sent. There may be many objectives for an attack either using the data overheard for a subsequent action or changing the data before it reaches the other party. The attacker extracts information to be used in many ways: fraud, unapproved support exchanges, blackmail, credential theft, and spying [25].

A MITM attack intercepts the victim's activity through the attacker's system before it is routed to its intended destination. The attacker gains access to an unsecured network, often targeting networks in public areas such as Wi-Fi access points [25]. This provides the attacker with an avenue to deploy tools that intercept information between the victims, often targeting personal computers where their connection to websites is monitored. This can result in credentials, financial details, and personally identifiable information being captured [25]. There are several types of MITM attacks, and the man-in-the-browser variant injects malicious software into the victim's computer or mobile device through phishing. Upon clicking on a phishing e-mail link or opening the attachment, the user loads the malware, and the malware installs itself on the browser without the user's knowledge. The malware enables the attacker to capture the information between the victim and specific websites. Exploits that are used to enter a MITM include internet protocol (IP) spoofing, address resolution protocol (ARP) spoofing, global navigation satellite system (GNSS) spoofing, and domain name system (DNS) spoofing [26].

5.1. IP Spoofing

In IP spoofing, the attacker modifies the source address in the IP packet header to make the receiver believe that the packet was received from a trusted site. From the victim's side, the packets will be received as though they were sent from a trusted source. However, the IP source reported in the packet is modified and does not represent the actual source [27].

5.2. ARP Spoofing

ARP spoofing involves sending a false ARP reply message to the default network gateway, claiming to associate the MAC address with the target's IP address. This ARP protocol translates IP addresses to MAC addresses. MITM ARP packets transmit over LAN by sending malicious ARP packets to a default gateway on the local area network

[28]. The re-association request from the attacker can enable them to appear as the default gateway for traffic; thus, all other hosts in the network will transmit their data through the MITM.

5.3. DNS Spoofing

In DNS spoofing, the IP address in a DNS record is replaced by an IP address in the control of the attacker. This redirects internet traffic to fraudulent websites that resemble intended destinations [29][30][31].

5.4. HTTPS/SSL Hijacking

Stolen data can be decrypted using several methods, including HTTPS spoofing, SSL hijacking, SSL stripping, and others. In HTTPS spoofing, the attacker uses a domain that appears identical to the target website's domain. In SSL hijacking, the attacker passes the produced authentication keys to both the client and application during a TCP handshake [32]. This seems, by all accounts, to be a safe association when the MITM controls the whole session. In SSL stripping, the attacker sends a decoded form of the application's site to the client by maintaining the anchored session with the application. Meanwhile, the client's whole session is noticeable to the attacker.

6. Phishing and Remote Execution

Phishing and remote attacks rely on social engineering methods designed to have the victim reveal sensitive information or use malicious software. Phishing is highly prevalent in cyber attacks on CIs and it is identified in many of the significant cyber attacks in **Table 1**. Attackers send fraudulent communication to coerce a victim into sharing classified credentials or other information. Credentials obtained can be used to perform other attacks, such as the installation of malware, remote access, or the theft of information. Attackers may ransom credentials through the threat of publication [33][34][35].

Table 1. Abridged list of significant cyber attacks in recent years.

Adversary Technique	Types of Cyber Attacks Used	CI	Impact on CI Operations
Initial Access, Execution, Lateral Movement, Impact	Phishing, Remote Desktop, BlackEnergy3 (FDIA)	Energy (2015–2016)	Opened breakers in substations in Ukraine, causing 230,000 customers to lose power.
Initial Access, Execution, Impact	Ransomware	Energy (2021)	Fuel shortages for Southeast US with gas prices rising (9–16 cents per gallon) and 10,600 stations without gas. The Colonial Pipeline billing system shutdown for six days.
Initial Access, Execution, Impact	Stuxnet Worm, Zero-day Vulnerabilities	IT (2009–2011)	Shutdown of uranium enrichment facilities in Natanz, Iran.

Adversary Technique	Types of Cyber Attacks Used	CI	Impact on CI Operations
Initial Access, Execution, Persistence, Collection	Trojan Laziok, reconnaissance malware	Energy (2014)	Gathered information from devices on the network that has vulnerabilities.
Initial Access, Execution, Collection, Impact	Ransomware	Food (2021)	Data of customers, suppliers, and employees were stolen. Productivity was reduced, access to some systems was blocked. A USD 11 million ransom was paid. Operation servers were shutdown and operations halted.
Initial Access, Execution, Impact	Ransomware	Healthcare (2021)	All Hospital appointments and radiology services were impacted, the ransomware affected Windows operating systems. The failure was experienced across national networks.
Initial Access, Execution, Impact	Phishing and Ransomware (Roobinhood)	Financial (2019)	Trading services of exchange halted and maintained offline, as computer systems were maliciously encrypted.
Initial Access, Execution, Collection	Phishing	Financial (Disclosed 2017)	The Equifax data breach resulted in the theft of personal data belonging to 140 million Americans and caused the company's share price to drop by 13%.
Initial Access, Execution, Persistence, Collection	Trojan Malware	Financial (2016)	The malware recorded debit cards and their pins from compromised ATM machines. Approximately USD 194,000 was stolen.
Initial Access, Execution, Collection, Impact	WannaCry Ransomware Cryptoworm	Energy (2017)	Worldwide Microsoft Windows operating systems were ransomed using an older Windows systems vulnerability EternalBlue.
Initial Access, Execution, Collection	Phishing, Ransomware	IT (2021)	The Accellion data breach and ransomware attack led to the theft of data in the Accellion data management service.
Initial Access, Execution, Lateral Movement, Impair Process Control	Supply Chain Ransomware	IT (2021)	Over 1500 businesses and organizations halted operations. A software updater released by an IT company, operating as a managed service provider
Initial Access, Execution, Inhibit Response Function, Impact	Ransomware	Municipal Services (2018)	Required over 5000 government computers to be shut down for 5 days to resolve the attack. Affected servers that were used to issue police warrants and employ new hiring processes, as

e [36]. The 2020 Federal Bureau of Information's Internet Crime Report lists phishing as the most common cyber attack performed against US citizens by a wide margin, likely due to the increasingly sophisticated methods that

Adversary Technique	Types of Cyber Attacks Used	CI	Impact on CI Operations
			well as official city complaints could not be submitted. [37]

crime was

the lead-up to Christmas in 2015, attackers took full control of remote terminal units in the Ukrainian power distribution grid and used them to change the set points on breakers. This action triggered the opening of critical breakers, de-energizing around 225,000 customers for an extended duration [38]. Phishing was the initial means by which attackers gained access to perform remote connection sabotage. Furthermore, in December 2016, attackers disabled energy delivery from a Kiev transmission station by using phishing to initiate remote sabotage, which caused a one-hour outage [39]. The flow of the phishing and remote execution cyber attack against the energy distribution system CI is shown in **Figure 3**. The attack sequence is framed as a separation of the cyber and physical planes, highlighting the sequential process of the attack by the APT. The process starts with reconnaissance, followed by a phishing campaign, gaining access, tunneling into OT, installing malware in OT, and finally using human-machine interfaces to sabotage physical systems in the field. The flow is captured in **Figure 3**.

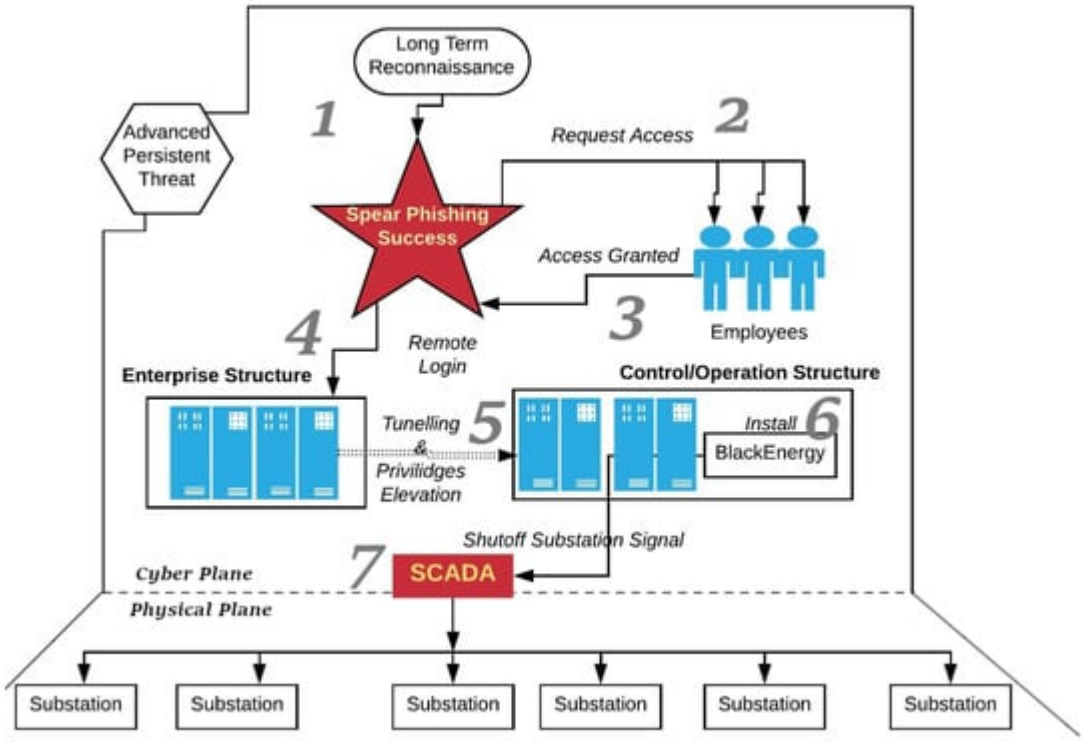

Figure 3. Targeting employees with socially engineered phishing campaigns, leading to remote sabotage.

6.1. Bulk Phishing

The most common form of phishing (bulk phishing) involves broadcasting messages through emails that are not personalized or targeted towards a specific individual or company. Attackers typically impersonate banking services, email/cloud providers, and streaming services to obtain credentials from potential victims.

6.2. Spear Phishing

In contrast to bulk phishing, ‘spear phishing’ includes methods of attack intended to target a specific organization or person with tailored communication. To increase the chances of deceit, attackers gather and use personal information about their target. Spear phishing targeted Hilary Clinton’s 2016 presidential campaign by Threat Group-4127 [40].

6.3. CEO Phishing and Whaling

Whaling and chief executive officer (CEO) fraud represent two specific types of spear phishing tactics. Whaling involves phishing targeting CEOs or senior executives. CEO fraud is a reciprocal tactic in which the phishing attempt is made to impersonate the CEO [41].

6.4. Clone Phishing

Clone phishing is another phishing attack; in this tactic, attackers manipulate the link/attachment files included in an otherwise legitimate email. Using a previously delivered email, attackers will attempt to clone an email and include malicious attachments in place of original files and links. This form of phishing typically requires that one of the parties, either the sender or the recipient of the email, has previously had their account compromised [33].

6.5. Additional Phishing Tactics

Phishing is practiced in attacks outside of email communication, as well. Voice phishing involves attackers spoofing a phone number to resemble a trusted institution. Attackers will dial large quantities of phone numbers and play automated recordings that try to coerce sensitive information to help resolve an issue on the victim’s account [42]. Finally, page hijacking is another form of phishing in which attackers will compromise or mimic legitimate web pages and redirect users to malware or an exploit kit utilizing cross-site scripting [43].

7. False Data Attack (Parameter/Command Injection)

False data injection is an attack that attempts to corrupt the control data. FDIA is presented in three types [44]:

- Targeted constrained FDIA: In this type of attack, data are injected after clear analysis, with a known amount of data inserted to appear realistic.
- Targeted unconstrained FDIA: In this type of attack, the attacker attempts to corrupt the values of some variables, and those variables in turn corrupt the remaining dependent variables.
- Random FDIA: In this type of attack, data packets are randomly distributed without consideration of the real values.

7.1. Protocols without Encryption in the CI

Digitization and ubiquitous computing have found their way into areas once solely operated by electromechanical controls. False data injection in CI control systems of the energy sector can damage the power electronics hardware. Protocol-level challenges in securing cyber-physical systems within the energy distribution grid are apparent in Distributed Network Protocol 3 (DNP3), GOOSE, and Modbus, as these protocols transmit data without encryption [45]. These systems should operate on physically isolated networks. An additional method to enhance their security is through the use of *bump in the wire*, an encryption hardware that encrypts the transmitted data before they travel the wider network. A methodology for layer-by-layer analysis of protocols to identify vulnerabilities is provided in [45]. Understanding protocol-level weaknesses is key to a secure network. Cyber-physical systems that utilize data generated from sensors in their processing and interact with information are prime targets for FDIA attacks. The cyber-physical system uses sensor data to implement the network and control adjustments of power electronics. In certain cases, these systems also require low latency in communication, which can make encryption of communications impossible, such as in the IEC 61850 GOOSE standard. If voltage is incorrectly controlled, it can cause damage to the power electronics.

7.2. Automatic Generator Control

FDIA on automatic generator control is a vulnerability that enables the manipulation of data in closed-loop control of generator control signals. This type of attack can cause significant damage to the generation and transmission equipment of the power grid, potentially leading to blackouts. This control system—if attacked by FDIA—will lead to overloading transmission lines by excessive power generation [46].

7.3. Parameter Modification in Inverters

As the power grid becomes increasingly dependent on renewable energy sources, new grid services will emerge based on smart inverters (SI) connected to these sources. The settings of these smart inverters are critical for these grid services to operate optimally. The settings of these inverters represent a point where FDIA can be particularly damaging to the smart grid [47]. A SI attack can affect the SI functions for volt–var, volt–watt, and a constant power factor. Such attacks potentially impact voltage profiles, system losses, and the operation of voltage control legacy devices. In such cases of FDIA, the severity depends on the prevailing SI functions [47].

8. Worm and Trojan Malware

A computer worm is a computer virus that is characterized as a self-replicating malware that spreads across networks executing disruptive payloads [48]. A worm targets hosts by following these scan types:

- An active selective random scan or sequential scan, in which the worm scans for vulnerable hosts.
- A hit-list scan, where the worm creates a target list and then searches for susceptible hosts.

- A routable scan, which utilizes information about a network to select and scan the IP address space [48].

Using a routable IP address allows the worm to propagate quickly and effectively, avoiding some detection methods. Another characteristic of a worm is the target space or medium through which it propagates. This includes the internet, email, P2P, USB local, and more. The worm propagates either as self-carried or through a second channel. In the second channel method, the main malware payload is remotely downloaded by the base installer. The activation of a worm on a system uses a vulnerability in the host, and the worm may protect itself by modifying its binary code with encryption [49].

The Stuxnet Worm

Stuxnet is a computer worm that was initially found in Iran but has since spread worldwide. This worm targets the control systems of a nation's critical infrastructure, and a successful attack by Stuxnet can result in the manipulation of the control system, causing disruption and damage to critical infrastructure and posing a threat to modern society. In 2010, Iran identified over 30,000 infected industrial computer systems, with Stuxnet specifically targeting nuclear power plant operational technology (OT) computers. The initial infections were at reactor core sites with flash memory used to introduce the worm locally. The worm targets an industrial control system that runs on Windows from Siemens [50].

9. Trojan

A Trojan can be installed on a computer through phishing or a local device. The purposes of a Trojan can vary, but often this malware hides its files under well-known directories, such as the user's documents, under the name of a trusted program, such as a web browser. Trojans are commonly used as a backdoor device to collect information from the infected computer. A keylogger is a type of data collection Trojan that can operate over a network or locally through a universal serial bus (USB) as an insider threat attack vector [51][52][53].

Additionally, hardware Trojan attacks refer to malicious modifications of electronic hardware at various stages of its operation. These attacks are a serious security concern for the electronics industry as they can lead to control interference and the leaking of secret data. The growing global demand for electronics makes it a larger point of vulnerability. It requires the adversary to have physical access to the integrated circuits [54][55].

References

1. Significant Cyber Incidents. Center for Strategic & International Studies. Available online: https://www.csis.org/ (accessed on 4 December 2022).
2. Huang, K.; Siegel, M.; Madnick, S. Systematically Understanding the Cyber Attack Business: A Survey. ACM Comput. Surv. 2018, 51, 70.

3. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 2020, 169, 107094.
4. Tufail, S.; Parvez, I.; Batool, S.; Sarwat, A. A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid. Energies 2021, 14, 5894.
5. Wei, L.; Sundararajan, A.; Sarwat, A.I.; Biswas, S.; Ibrahim, E. A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game. In Proceedings of the 2017 Resilience Week (RWS), Wilmington, DE, USA, 18–22 September 2017; pp. 5–11.
6. Worlds Largest Meat Processing Company Hit by Cyber Attack (JBS). BBC. 2 June 2021. Available online: https://www.bbc.com/news/world-us-canada-57318965 (accessed on 7 July 2021).
7. Ransomware on the Rise in Critical Infrastructure Sector. JD Supra. 13 May 2021. Available online: https://www.jdsupra.com/legalnews/ransomware-on-the-rise-in-critical-1687319/ (accessed on 4 December 2022).
8. The Curious Case of the Baltimore Ransomware Attack: What You Need to Know. Heimdal Security Blog. 8 September 2020. Available online: https://heimdalsecurity.com/blog/baltimore-ransomware (accessed on 14 November 2022).
9. WannaCry Ransomware Attack Summary. Data Protection Report. 17 May 2017. Available online: https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ (accessed on 5 December 2022).
10. Chokshi, N. Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. The New York Times. 22 May 2019. Available online: https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html (accessed on 5 December 2022).
11. 'Number of Days' before Systems back Working—HSE 2021. Section: News. ProteusCyber. 17 May 2021. Available online: https://proteuscyber.com/it/privacy-database/news/4482-number-of-days-before-systems-back-working-hse (accessed on 22 July 2022).
12. Oz, H.; Aris, A.; Levi, A.; Uluagac, A.S. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ACM Comput. Surv. 2022, 54, 238.
13. Hanna, Y.; Cebe, M.; Mercan, S.; Akkaya, K. Efficient Group-Key Management for Low-bandwidth Smart Grid Networks. In Proceedings of the 2021 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Aachen, Germany, 25–28 October 2021; pp. 188–193.
14. Zhi, Y.; Fu, Z.; Sun, X.; Yu, J. Security and privacy issues of UAV: A survey. Mob. Netw. Appl. 2020, 25, 95–101.

15. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Trans. Comput. Healthc. 2021, 2, 1–44.
16. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Comput. Secur. 2018, 74, 144–166.
17. Menn, J. Kaseya ransomware attack sets off race to hack service providers -researchers. Reuters, 4 August 2021.
18. Lau, F.; Rubin, S.; Smith, M.; Trajkovic, L. Distributed denial of service attacks. In Proceedings of the 2000 IEEE International Conference on Systems, Man and Cybernetics, Nashville, TN, USA, 8–11 October 2000; Volume 3, pp. 2275–2280.
19. Kumar, S.; Kumar, H.; Gunnam, G.R. Security Integrity of Data Collection from Smart Electric Meter under a Cyber Attack. In Proceedings of the 2019 2nd International Conference on Data Intelligence and Security (ICDIS), Island, TX, USA, 28–30 June 2019; pp. 9–13.
20. Parvez, I.; Islam, A.; Kaleem, F. A key management-based two-level encryption method for AMI. In Proceedings of the 2014 IEEE PES General Meeting|Conference & Exposition, National Harbor, MD, USA, 27–31 July 2014; pp. 1–5.
21. Thomas, M.S.; Ali, I.; Gupta, N. A secure way of exchanging the secret keys in advanced metering infrastructure. In Proceedings of the 2012 IEEE International Conference on Power System Technology (POWERCON), Auckland, New Zealand, 30 October–2 November 2012; pp. 1–7.
22. Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 449–454.
23. Lu, Z.; Wang, W.; Wang, C. Modeling, evaluation and detection of jamming attacks in time-critical wireless applications. IEEE Trans. Mob. Comput. 2013, 13, 1746–1759.
24. DiChristopher; Tom, K.F. An Alarmingly Simple Cyberattack Hit Electrical Systems Serving LA and Salt Lake, but Power Never Went Down. 2019. Section: Cybersecurity. Available online: https://finance.yahoo.com/news/alarmingly-simple-cyberattack-hit-electrical-193034191.html (accessed on 4 December 2022).
25. Mallik, A.; Ahsan, A.; Shahadat, M.M.Z.; Tsou, J.C. Understanding Man-in-the-middle-attack through Survey of Literature. Indones. J. Comput. Eng. Des. 2019, 1, 44–56.
26. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. Proc. IEEE 2016, 104, 1258–1270.
27. Schuckers, S.A. Spoofing and anti-spoofing measures. Inf. Secur. Tech. Rep. 2002, 7, 56–62.
28. ARP Poisoning. Available online: https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/ (accessed on 17 November 2021).

29. Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051.
30. Callegati, F.; Cerroni, W.; Ramilli, M. Man-in-the-Middle Attack to the HTTPS Protocol. IEEE Secur. Priv. 2009, 7, 78–81.
31. Cheng, K.; Gao, M.; Guo, R. Analysis and research on HTTPS hijacking attacks. In Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Austin, TX, USA, 24–25 April 2010; Volume 2, pp. 223–226.
32. What Is HTTPS Spoofing MitM? Secret Double Octopus. Available online: https://doubleoctopus.com/security-wiki/threats-and-tools/https-spoofing/ (accessed on 17 November 2021).
33. Verizon Data Breach Investigations Report. Verizon. 2019. Available online: https://www.verizon.com/business/resources/reports/dbir/ (accessed on 17 November 2021).
34. Josh Fruhlinger. CSO Online. Equifax Data Breach: What Happened, Who Was Affected, What Was the Impact? Available online: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed on 7 May 2022).
35. Four Members of China's Military Indicted over Massive Equifax Breach. Wall Street Journal. 11 February 2020. Available online: https://www.wsj.com/articles/four-members-of-china-s-military-indicted-for-massive-equifax-breach-11581346824 (accessed on 7 May 2022).
36. Stavroulakis, P.; Stamp, M. Handbook of Information and Communication Security; Springer Science & Business Media: Berlin/Heidelberg, Germany, 2010.
37. IC3. Cyber Crime Report; Federal Bureau of Investigation, Internet Crime Complaint Center: Washington, DC, USA, 2020.
38. Robert, M.; Lee, M.J.; Assante, T.C. Analysis of the Cyber Attack on the Ukrainian Power Grid. Available online: https://www.eisac.com/s/ (accessed on 2 February 2022).
39. Lanna Deamer. The DDoS Threat for Energy and Utility Companies. ElectronicSpecifier. 19 January 2018. Available online: https://www.electronicspecifier.com/products/cyber-security/the-ddos-threat-for-energy-and-utility-companies (accessed on 17 November 2021).
40. Spearphishing via Service, Technique T1194—Enterprise|MITRE ATT&CK®. Available online: https://attack.mitre.org/techniques/T1566/003/ (accessed on 14 July 2022).
41. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Front. Comput. Sci. 2021, 3, 563060.
42. Vishing. In Proceedings of the 5th Annual Conference on Information Security Curriculum Development, Kennesaw, GA, USA, 26–27 September 2008.

43. Static detection of cross-site scripting vulnerabilities. In Proceedings of the 2008 ACM/IEEE 30th International Conference on Software Engineering, Leipzig, Germany, 10–18 May 2008.
44. Tufail, S.; Batool, S.; Sarwat, A.I. False data injection impact analysis in ai-based smart grid. In Proceedings of the SoutheastCon 2021, Atlanta, GA, USA, 10–13 March 2021; pp. 1–7.
45. Sundararajan, A.; Chavan, A.; Saleem, D.; Sarwat, A.I. A Survey of Protocol-Level Challenges and Solutions for Distributed Energy Resource Cyber-Physical Security. Energies 2018, 11, 2360.
46. Ameli, A.; Hooshyar, A.; El-Saadany, E.F.; Youssef, A.M. Attack detection and identification for automatic generation control systems. IEEE Trans. Power Syst. 2018, 33, 4760–4774.
47. Olowu, T.O.; Dharmasena, S.; Jafari, H.; Sarwat, A. Investigation of False Data Injection Attacks on Smart Inverter Settings. In Proceedings of the 2020 IEEE CyberPELS (CyberPELS), Miami, FL, USA, 13 October 2020; pp. 1–6.
48. Pratama, A.; Rafrastara, F.A. Computer worm classification. Int. J. Comput. Sci. Inf. Secur. 2012, 10, 21.
49. Nissim, N.; Moskovitch, R.; Rokach, L.; Elovici, Y. Detecting unknown computer worm activity via support vector machines and active learning. Pattern Anal. Appl. 2012, 15, 459–475.
50. Kerr, P.K.; Rollins, J.; Theohary, C.A. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability; Congressional Research Service: Washington, DC, USA, 2010.
51. Chandel, S.; Yu, S.; Yitian, T.; Zhili, Z.; Yusheng, H. Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat. In Proceedings of the 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (Cyberc), Guilin, China, 17–19 October 2019; pp. 81–89.
52. Clark, J.; Leblanc, S.; Knight, S. Risks associated with USB hardware trojan devices used by insiders. In Proceedings of the 2011 IEEE International Systems Conference, Montreal, QC, Canada, 4–7 April 2011; pp. 201–208.
53. Kaspersky, J. BlackEnergy APT Attacks in Ukraine; Kaspersky Co.: Moscow, Russia, 2015.
54. Bhunia, S.; Hsiao, M.S.; Banga, M.; Narasimhan, S. Hardware Trojan attacks: Threat analysis and countermeasures. Proc. IEEE 2014, 102, 1229–1247.
55. Konstantinou, C.; Keliris, A.; Maniatakos, M. Taxonomy of firmware trojans in smart grid devices. In Proceedings of the 2016 IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 17–21 July 2016; pp. 1–5.