INL/EXT-22-xxxxx
Revision 001

Ransomware Entry Points for Control Systems

An analysis of control system ransomware and common injection vectors

October 2022

Idaho National Laboratory
Chris Spirito

Temple University
Dr. Aunshul Rege
Rachel Bleiman
Parker Naugle

INL is a U.S. Department of Energy National Laboratory
operated by Batelle Energy Alliance, LLC

INL/
Revision 001

Ransomware Entry Points for Control Systems

Idaho National Laboratory
Chris Spirito

Temple University
Dr. Aunshul Rege
Rachel Bleiman
Parker Naugle

October 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Engineering
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

SUMMARY

This report provides background information on the state of ransomware use against critical infrastructure. The report analyzes ransomware attacks specifically against the energy and nuclear sectors. Case studies are presented and utilized to create attack scenarios, enumerate points of entry during the initial access stage of an attack, and describe attack impact based upon analyzed events.

This literature review and close analysis of specific events has broadened our understanding of the most common points of entry seen in ransomware attacks, along with the common impacts experienced by victims of these attacks. It has also shifted our knowledge of ransomware as a unique cyberattack, with differences compared to general cyber-attacks. This report has identified the need for increased transparency when institutions are impacted by cyber-attacks and ransomware attacks so that researchers and industry professionals can better understand and defend against these attacks.

Page intentionally left blank

CONTENTS

TABLES

FIGURES

Page intentionally left blank

ACRONYMS

CI	Critical Infrastructure
ICS	Industrial Control System
PoE	Point of Entry

Page intentionally left blank

Ransomware Entry Points for Control Systems

1. Introduction

Ransomware attacks against critical infrastructure are a growing threat against society, as Critical Infrastructure (CI) consists of businesses and organizations that are relied on and needed for society's day-to-day functions. Due to the Ukraine-Russia War and the inter-dependencies between Russia and EU nations, Energy Security and more broadly Critical Infrastructure Security has garnered much attention. Thus, Russian application of ransomware to EU and Ukraine energy solutions remains a driving force. Ransomware attacks against CI and energy systems in particular have the potential to include more catastrophic physical effects. This elevates the concern of ransomware attacks against energy systems, especially compared to targets with fewer dependencies. For example, the attack against Colonial Pipeline (discussed in more detail later in the report) showed that freezing a specific business function via ransomware allowed for the subversion of dependent functions with a broad impact to associated organizations and people.

1.1 Ransomware and CI Overview

The research team at Temple University collected and analyzed disclosed ransomware incidents against critical infrastructure. Table 1 contains a summary of the most frequently used ransomware strains from an aggregated set of 1,293 publicly disclosed ransomware incidents against critical infrastructure, with incidents dating from November 2013 up through the end of August 2022. While some of these strains were certainly prolific during their peak, such as WannaCry who had a global attack against hundreds of organizations (although many were undisclosed), many of these strains are no longer observed in use, including WannaCry, REvil, and Maze, although variant forms have been observed. The right side of Table 1 provides a windowed view of the most common ransomware strains in publicly disclosed attacks from over the last 6 months (March 2022-August 2022). Note: other strains are in existence and pose as threats but have not been identified or credited in any publicly disclosed incidents against critical infrastructure.

Table 1: Top 10 Most Common Ransomware Strains (Rege, 2022)

All-time		**Within past 6-months**	
Strain	**Frequency**	**Strain**	**Frequency**
Maze	60	Lockbit	14
REvil	58	Hive	9
Ryuk	48	Conti	9
Conti	42	BlackCat	8
WannaCry	33	ViceSociety	3
NetWalker	26	Quantum	2
DoppelPaymer	24	Black Basta	2
LockBit	22	Yanluowang	2
RansomExx	15	LV Ransomware	2
Hive	14	Clop [a]	1
Total	**342**	**Total**	**52**

[a] Several strains had a single occurrence, including the following: RansomHouse, Lapsus$, Stormous, AvosLocker, RansomExx, Pandora, ROADSWEEP, PLAY, Daixin Team, BitLocker, and Ragnar Locker

Table 2 provides an overview of the attack frequency against each critical infrastructure sector, sorted by frequency of attacks highest to lowest, split between overall and last 6 months. These frequencies represent *publicly disclosed* attacks and may not represent the actual state of attacks against each sector. Organizations often decline to disclose ransomware attacks, especially in sectors such as energy and so these numbers must be used with a bit of caution.

Note on Table 2: some attacks against organizations overlap sectors with a maximum overlap of 1 (e.g., an IT company that primarily services the healthcare industry would overlap both sectors).

Note on : Education facilities are treated as a subsector apart from its parent sector, Government Facilities, due to the large number of publicly disclosed incidents specific to education. Thus, the government facilities sector frequency does not include any attacks against education facilities specifically.

Table 2: Attacks Across Critical Infrastructure Sectors (Rege, 2022)

All-time		**Within last 6 months**	
CI Sector	**Freq.**	**CI Sector**	**Freq.**
Government Facilities	299	Government Facilities	26
Healthcare and Public Health	247	Healthcare and Public Health	22
Education Facilities Subsector	197	Education Facilities Subsector	16
Critical Manufacturing	106	Critical Manufacturing	15
Information Technology	105	Communications	8
Transportation Systems	82	Energy	8
Emergency Services	73	Information Technology	7
Communications	64	Transportation Systems	6
Commercial Facilities	62	Food and Agriculture	6
Financial Services	54	Commercial Facilities	5
Energy	47	Financial Services	4
Food and Agriculture	44	Water and Wastewater Systems	3
Chemical	17	Defense Industrial Base	2
Water & Wastewater Systems	13	Emergency Services	1
Defense Industrial Base	7	Chemical	0
Nuclear Reactors, Materials, & Waste	1	Nuclear Reactors, Materials, & Waste	0
Total	**1,418**	**Total**	**129**

Next, Figure 1 presents the yearly trend of *publicly disclosed* ransomware attacks against any critical infrastructure, with the total frequency of attacks per year from 2013 through the end of August 2022. While the figure asserts that 2020 had the most publicly disclosed ransomware attacks, the frequency of non-disclosed attacks is most likely significantly higher. There are several reasons as to why the frequency of non-disclosed attacks is higher. As noted in the limitations in section 2.4, some reasons include the threat to the organization's reputation, advertising their vulnerabilities in a way that may lead to revictimization, liability issues, or even to prevent legal ramifications, as the US government has taken a stand against paying ransomware demands. In fact, a victimized organization that chose to pay the ransom demand may face financial sanctions from the US Treasury due to recently passed bills, such as the Ransomware and Financial Stability Act.

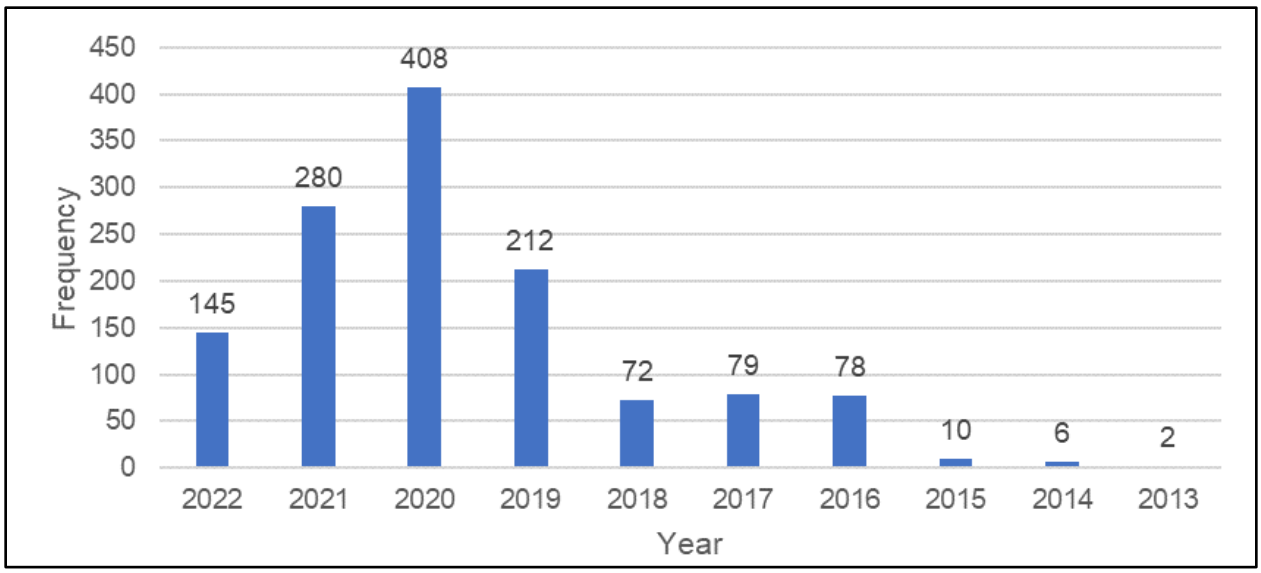

Figure 1: Frequency of Attacks per Year (Rege, 2022)

Next, Table 3 presents a categorization of ransom amounts demanded in ransomware attacks against critical infrastructure organizations and the frequency of each ransom demand, sorted from highest frequency to lowest. The categories of ransom demands were created via natural breaks in the raw data. Because this data is gathered solely from publicly available sources, the ransom demand amount is not known for all cases. Table 3 makes it clear that higher ransom demands are more common now than they have been in the past. While the demands in Table 3 are noted in USD, nearly all ransomware demands are demanded and paid in cryptocurrency, typically Bitcoin. The value of cryptocurrency fluctuates, so the conversion of USD to bitcoin is its price on October 16, 2022.

Table 3: Ransom Amounts Demanded (Rege, 2022)

All-time			**Within past 6-months**		
Ransom Amount (USD)	**BTC**	**Freq.**	**Ransom Amount (USD)**	**BTC**	**Freq.**
$50,000 or less	<2.61	74	$5,000,000 or less	<261.19	6
$1,000 or less	<0.052	54	More than $5,000,000	>261.19	3
More than $5,000,000	>261.19	48	$1,000,000 or less	<52.24	2
$1,000,000 or less	<52.24	45	$100,000 or less	<5.22	1
$5,000,000 or less	<261.19	30	$50,000 or less	<2.61	1
$100,000 or less	<5.22	21	$1,000 or less	<0.052	0
Total		**272**	**Total**		**13**

1.2 Ransomware and Electric Grids

For details on all publicly disclosed ransomware incidents specifically impacting the energy sector, see Endnotes. Below are descriptions of specific case studies impacting electric grids, ranging from broad energy to specifically impacting the nuclear sector. More information on these incidents, including attack playbooks, points of entries, and impacts will be discussed in further detail in a later section.

1.2.1 Colonial Pipeline

The Colonial Pipeline cyber-attack in the Spring of 2021 is one of the most publicized cases in recent years due to the scale of the attack and the effect it had on public perception of cyber-attacks on the energy sector. The ransomware group DarkSide was responsible for the Colonial Pipeline attack along with attacks in more than a dozen countries such as Ukraine, Belgium, Italy, Turkey, Canada, and the United States. Their targets mostly included the finance and manufacturing industries, where they targeted more than 90 companies, and stole tens of millions of dollars.

According to a profile on DarkSide by Mandiant (Nuce et al., 2021), DarkSide lends out their software for a portion of the third party's ransom but conducts "big game hunting" on their own. This is where the group goes after large organizations who are more likely to have the means to pay a larger ransom, like the Colonial Pipeline. The DarkSide group first appeared on dark web message boards in the Summer of 2020 commencing attacks on victims shortly thereafter. From August to October of 2020, the group established a website and posted receipts for donations to children's charities and clean water projects. Then, from December of 2020 to May of 2021, the group conducted cyber operations against Brenntag, CompuCom, and Toshiba along with many other companies across the globe. These attacks finally culminated with the Colonial Pipeline attack in early May 2021.

The Colonial Pipeline attack was DarkSide's most publicized attack which led to the shutdown of one of the largest oil pipelines in the United States that provides 45% of the oil for the eastern coast. This attack forced the pipeline operators to shut down the pipeline for five days, causing panic buying of fuel for consumers and issues for airlines trying to source jet fuel for commercial flights. The group extorted roughly $5 million worth of Bitcoin from the organization of partners that own the pipeline. The FBI confirmed that DarkSide was responsible for the attack and provided resources to the incident response team at Colonial Pipeline to assist in investigation of the attack. The FBI assisted them in retrieving a portion of the ransom that was paid to DarkSide.

See section 3.2.1 for information on DarkSide's attack playbook, Points of Entry (PoE), and Impacts in their attack against the Colonial Access Pipeline.

1.2.2 Black Energy

Another specific case study of interest is the Black Energy ransomware. Attributed to Russian nation-state cyber actors in the Sandworm group, Black Energy TTPs have evolved since 2007, continuing to cause disruptions to critical infrastructures across the globe. Their targets have included Ukrainian entities, especially those in the energy sector, government, and media, along with ICS/SCADA and energy companies worldwide (NJCCIC, 2017).

While BlackEnergy was originally designed to create botnets for use in conducting DDoS attacks, it now includes a modular plug-in architecture, including SCADA and ICS plugins. The modular architecture, in which different components serve different functions, allows for only essential functions and features to be delivered onto the target (NJCCIC, 2017). One of the initial instances of Black Energy in 2007 was used as a DDoS tool and deployed in the Russia-Georgia 2008 confrontation. In 2010, Sandworm used the tool to conduct espionage on ICS networks. Then in 2014, a variant, BlackEnergy2 started incorporating SCADA plugins and was used to infect critical infrastructure in the United States. BlackEnergy3 was then used in a 2015 attack against Ukrainian power companies to collect information about the ICS environment and compromise user credentials of network operators (MITRE, 2022a).

One scenario of its use is during a 2015 attack against the Ukrainian energy grid. Sandstorm used Black Energy to target the Prykarpattya Oblenergo power facility and other electricity distribution companies in

Ukraine, which resulted in a massive six-hour blackout across the country (Trend Micro, 2016). However, there are reports that while the BlackEnergy3 was present in the 2015 Ukrainian power system, there is no confirmation of a causal link between the malware and the power outage (CISA, 2014).

While BlackEnergy is characterized as a malware, and not specifically ransomware, its associated impacts are like those that could occur as a result of a ransomware incident against ICS, so understanding how this attack played out and its impacts is useful for understanding ransomware attacks against ICS. See section 3.2.2 for information on BlackEnergy's attack playbook, PoE, and Impacts in their attack against the Ukrainian power grid.

1.2.3 Sol Oriens

Sol Oriens is a consulting firm that works with the Department of Energy and the National Nuclear Safety Administration as a contractor. The veteran-owned firm works on concepts and technologies "with a strong potential for space and military applications," according to their website. In May 2021, the firm became aware of a cyber-attack on their systems and notified law enforcement. The company said that an unauthorized user gained access to documents from their systems, but that none of the documents were classified. Some of the documents later surfaced on forums on the dark web that showed descriptions of research and projects that are being worked on by other Department of Energy contractors, along with payment documents that included the full names and social security numbers of employees.

The Gold Southfield ransomware group, which operates the REvil ransomware strain, has been implicated as the perpetrator of this attack, as they later added Sol Oriens to their website and listed them as one of their victims. This group has been active and financially motivated since at least 2019 and is responsible for many high-profile attacks like their 2021 attack on JBS foods, the largest meat supplier in the United States.

See Section 3.2.3 Sol Oriens for information on REvil's attack playbook, PoE, and attack impacts.

1.2.4 Eletrobras

Another example of ransomware targeting electric grids is the attack against Eletrobras (Seals, 2021), in which their specific nuclear unit was targeted. In early February 2021, the administrative network of Eletrobras's Eletronuclear subsidiary was hit in the attack. The network runs two nuclear power plants, Angra1 and Angra2. Although details regarding point of entry and initial access were not made public, more details were given on the impacts associated with the attack. Because of the attack, the company suspended "some of its systems to protect the integrity of data." The company released a statement in which they confirmed that the operational technology (OT) systems are not connected to the administrative network that was targeted in the attack. Because the OT system that runs the nuclear power plants was isolated from the administrative network, the impacts were minimal, with no threat to the safety or operation of the power station.

2. Methodology

2.1 Literature Review

The literature review culminated in a set of 46 references (see Endnotes) that were cited or consulted while reviewing the literature that focused on ransomware attacks against ICS, including those on specific malware groups or attacks, as well as general information about ICS security and impacts. These articles were identified through keyword searches on Google and Google Scholar, using keywords 'ransomware,' 'ICS,' 'nuclear,' 'energy,' and 'ICS impacts.' Once specific attack cases were identified, further searches were conducted to gather more information on these attacks or specific adversary groups. References ranged from academic articles, news reports from both security firms and media, governmental alerts or recommendations, and legal documents. For each relevant document, the researchers identified attack points of entries and any further attack details. Additionally, the researchers mapped each attack onto the ATT&CK ICS Impact framework.

The literature review revealed details on several ransomware incidents impacting the energy sectors, including the 2021 attack against Colonial Pipeline, the BlackEnergy malware and its use against Ukrainian power grid, a 2021 attack on Eletrobras' nuclear sector, and an attack on nuclear contractor Sol Oriens. Through the literature review, the researchers were also able to identify several popular PoEs and common impacts that ICS face as a result of an attack. Furthermore, the literature review revealed information to help better understand the adversarial mindset in executing ransomware attacks against ICS.

2.2 Point of Entry (PoE)

Point of Entry is a term used to describe the various ways that an adversary gains initial access into a system. Often, the point of entry is either unknown or undisclosed. Nevertheless, the following are various points of entries identified in the literature review: phishing, spear phishing, baiting via USB devices, insecure remote desktop protocols, and exposed passwords.

Phishing, spear phishing, and baiting are all forms of social engineering, or psychological manipulation to influence someone to do or reveal something that they otherwise would not. Phishing, and in its more targeted form, spear phishing, are social engineering tactics in which adversaries attempt to trick their target into clicking on a malicious link or downloading malicious files onto a system. Adversaries may conduct a "phishing campaign" that targets an employee base as a whole, in order to get one of them to click a malicious link or download a malicious file that was included in the phishing email. A Spear Phishing attack is similar to a regular phishing attack in the sense that both involve the use of social engineering through a fake email, but spear phishing is the practice of crafting a fake email that is tailored towards the specific target inside of an organization.

Baiting also often results in a user unknowingly bringing malware onto their device, and they are 'baited' into doing so, sometimes with a lost USB stick that a user plugs into their device, curious to see the content within the device or to whom it belongs. Within nuclear and critical infrastructure facilities, the baiting issue is related to the Insider Threat and more specifically, the unwitting insider that conducts an action on behalf of an agent to deliver an effect into the target environment.

Insecure remote desktop protocol is when a user downloads a '.rdp' file, usually from a phishing email or unsafe site. When a user opens and/or runs a '.rdp' file, they allow someone else full access to their computer remotely. This allows the other person to do anything they would be able to do if they were sitting at the computer, such as export files, data, and manipulate systems and networks to which they are connected. This would be a variation on a malware remote access tool (RAT) that offers similar features but in a malicious delivery package rather than one that resides on the target system.

Exposed passwords, often through password reuse, are another point of entry. Exposed passwords from data leaks and data breeches are a common form of a point of entry for adversaries looking to gain access to computers and networks with sensitive information. One concern is the use of duplicate passwords by site staff such that if the account password is compromised externally, it can be utilized for account access attempts internally when a user of both systems is identified.

Of the various points of entry methods used in cyberattacks, exposed passwords and spear phishing are commonly used as points of entry for ransomware attacks. These methods allow adversaries to gain access to a system and network and observe operations on the network to better understand their target environment and identify mechanisms for exfiltrating data and conducting the ransomware attack. Due to the segmentation of nuclear energy architectures, initial POEs that target system administrators and privileged users yield more useful results. The employee at the point of entry needs to be targeted so that adversaries can assure they are gaining access to the necessary system to execute maximum damage to the extent that the targeted organization pays. If various systems are isolated, targeting the HR system will not result in as great of a payout as targeting the nuclear reactor system.

2.3 Impact

There are several impacts that can result from attacks against energy grids. These range from momentary disruptions to services to complete long-term shutdowns. Impacts can cause harm to both employees and consumers in various levels of severity. An example of an extreme potential impact is an attack scenario developed in 2015 in which the Eastern Interconnection is targeted (Senate Republican Policy Committee, 2021). The Eastern Interconnection is the provider of power to about half of the US. This scenario detailed an attack that would cause a blackout across 15 states in addition to Washington D.C. and could result in 93 million people losing power. For the success of such an attack, it is reported that only 10% of the provider's generators need to be taken offline. While this is an example of a severe impact, there are any number of impacts that can occur, ranging in severity. These impacts can be described and mapped along MITRE's ATT&CK ICS Impact Framework.

The researchers used the MITRE ATT&CK ICS Framework to identify ICS impacts from ransomware attacks (MITRE, 2022b). The framework includes adversarial techniques that are used against or that impact ICS environments. They may include techniques with immediate impacts or techniques in which the impact is long-term. Using each article from the literature review, several impacts were identified. Impact techniques and their associated ATT&CK technique IDs found in the literature review include the following: damage to property (T0879); denial of control (T0813); loss of availability (T0826); loss of productivity and revenue (T0828); loss of view (T0829); and theft of operational information (T0882). Described briefly in Table 4, Section 3 demonstrates examples of these impacts in the context of specific ransomware case studies.

Table 4: ICS Impacts and Descriptions

Impact	Description	Ransomware Application
Damage to Property (T0879)	Adversaries may cause damage and destruction of property to infrastructure, equipment, and the surrounding environment when attacking control systems.	In a ransomware attack against an energy grid, this may appear as damage to the surrounding outside environment, because of experiencing another impact, such as loss of power.
Denial of Control (T0813)	Adversaries may cause a denial of control to temporarily prevent operators and engineers from interacting with process controls.	In a ransomware attack, this may appear as nuclear facility operators being unable to interact with their controls.

Loss of Availability (T0216)	Adversaries may attempt to disrupt essential components or systems to prevent operators from delivering products or services.	In a ransomware attack, this may appear as the necessary shutdown of systems.
Loss of Productivity and Revenue (T0828)	Adversaries may cause loss of productivity and revenue through disruption and even damage to the availability and integrity of control system operations, devices, and related processes. Loss of productivity may eventually present an impact for the consumers of products and services including supply shortages and increased prices.	In a ransomware attack on an energy provider this could manifest as a widespread blackout of billing and service management after a prolonged period of non-operation due to a ransomware attack.
Loss of View (T0829)	Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention, for instance, a restart or manual operation.	In a ransomware attack, this may appear as operators being unable to view system processes and requiring manual operation.
Theft of Operational Information (T0882)	Adversaries may steal operational information on a production environment as a direct mission outcome for personal gain or to inform future operations.	As a result of a ransomware attack, adversaries may gain access to and steal sensitive information related to an institution's technical operations, such as security measures or normal operational guidelines. This stolen information may be used as further means for ransom or to be sold to an interested party.

2.4 Limitations

The primary limitation in generating this literature review was the lack of open-source information available on ransomware attacks against the energy or nuclear sector. Many incidents are not disclosed due to the possibility that disclosure of ransomware incidents may harm the infrastructures' reputation and publicize their vulnerabilities, possibly subjecting them to future ransomware (or other) attacks. Oftentimes, even when the occurrence of a specific incident is disclosed, the ICS impacts and details of specific cases are not provided. There are a few possible ways to bridge this gap to increase disclosure, which is important, as the knowledge gained from previous victims can be used to better defend and protect future targets. Because many organizations have valid reasons for choosing not to disclose when they have been attacked, there could be an anonymous attack disclosure service available to improve overall crossway for organizations to disclose their attack and the details of their attack. Whether it is anonymized only to the public and disclosed to researchers, government, or industry experts, it would be beneficial to have this information shared, even if it is without a company name attached.

3. Findings

3.1 Adversarial mindset, Contextual PoEs and Impacts

In the majority of ransomware attacks, it is thought that adversaries' motivations are financial, where they are looking to maximize profit. During a typical attack, profit is calculated as follows:

$$Profit = Population * Value - Cost$$

where *Population* refers to the number of potential targets, *Value* refers to data value (to the target or to leak and sell), and *Cost* refers to attack execution expenses (Formby, Durbha, and Beyah, 2017).

In ransomware attacks against traditional (non-ICS) targets, the population (# of potential targets) is high and the value of encrypted data is low. However, in ICS Ransomware attacks, the number of targets is often constrained. For instance, the number of disclosed, victimized targets in the energy or nuclear sectors is only 48 (Endnotes), as compared to the number of disclosed victimized targets across all sectors is nearly 1,300. Instead of the number of targets being high, the value of the data is high. However, the value is not in the data itself, rather the value is focused on function impact such as system downtime, equipment health, and safety to personnel. So, while there are fewer targets (population) in ICS Ransomware attacks, there is perceivably more at stake (value), allowing ransomware groups to demand higher ransoms and thus generate greater profits (Formby, Durbha, and Beyah, 2017). As the impact from ransomware attacks against ICS can have severe consequences, it is important for us to understand defensive options that include an enumeration of initial access points. These are discussed in the following sections within the context of specific attacks against energy and nuclear companies.

One finding the literature review revealed was that common points of entry for adversaries to execute ransomware attacks include exposed passwords, phishing and spear phishing, unsecure remote desktop protocol, and malicious USB sticks. To understand how these PoEs are vulnerable to adversaries, the following case studies contextually demonstrate their use as an initial access point.

Additionally, while there are several potential ICS impacts, the literature review revealed the most common impacts to be the following: Loss of Productivity and Revenue (T0828), Theft of Operational Information (T0882), Loss of Availability (T0826), demonstrated contextually in the case studies below.

3.2 Case Studies

Across each case study, it is important to keep in mind what is known about the adversarial mindset, as it may change in each stage of an attack. While the adversary's exact knowledge during each stage of the attacks is often unclear or muddled, criminological theory can help explain decision making processes. The Rational Choice Theory (Becker, 1968; Clarke, 1992) asserts that people are rational and hedonistic beings, and with each decision they make, they are conducting a cost-benefit analysis of the risks and rewards. Therefore, while their knowledge during each stage of the attack is unknown, it can be assumed that they believed that the risks did not outweigh the rewards. In the initial access stage, risks or costs include potential criminal sanctions and even the time it would take to execute an attack on a certain target. This time measure can be exacerbated by particularly good technical defense measures or by adept employees that are hard to social engineer. Throughout any stage of an attack, elevating any risks associated with adversaries executing an attack would tip the risk-reward balance to potentially deter adversaries from moving forward with their attack.

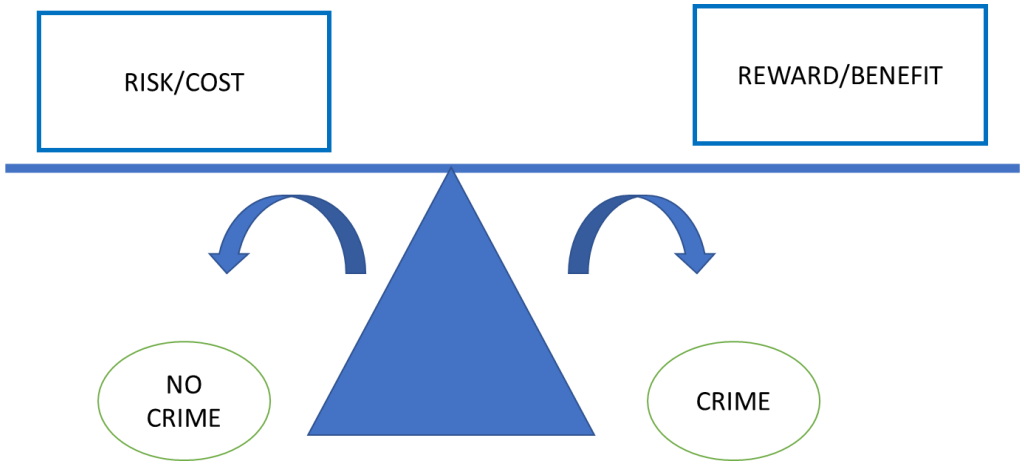

Figure 2: Rational Choice Theory

As adversaries gain initial entry into a system or network, they have the choice of waiting and observing normal operations on the network, or immediately initiating their attack. *[Spirito] This isn't quite correct as an adversary that immediately delivers an effect upon arriving on the target system either needs knowledge of the system prior to arrival or a willingness to risk the effect delivery outcome being compromised due to a lack of target system situational awareness.* Adversaries may see less of a reward after they've made entry and may decide the attack doesn't warrant the risk they would be undertaking. For example, if adversaries were looking for a specific piece of high-value information when attacking a victim, they would be less likely to initiate their attack if the information could not be found or exfiltrated in a manner that would not alert the victim of their access.

3.2.1. Colonial Pipeline

According to a timeline analysis by TechTarget (Kerner, 2022), on May 6th, 2021, the ransomware group DarkSide made entry into computers on the Colonel Access Pipeline's network which is responsible for business operations, communication, administrative work, and company records, not pipeline operations. The group then exfiltrated data from company computers connected to the infiltrated network. On May 7th, 2021, the ransomware attack was initiated, and the pipeline became aware of the breach due to the widespread encryption on their network and connected computers. The pipeline is then taken offline to avoid any further damage, and the ransom of $4.4 million was paid. On May 12th, 2021, the pipeline was restarted and fully operational, and the U.S. government would later assist the pipeline in recouping nearly half of the ransom.

Figure 3: Colonial Pipeline Order of Events

According to a timeline analysis by TechTarget (Kerner, 2022), on May 6th, 2021, the ransomware group DarkSide made entry into computers on the Colonel Access Pipeline's network which is responsible for business operations, communication, administrative work, and company records, not pipeline operations. The group then exfiltrated data from company computers connected to the infiltrated network. On May 7th, 2021, the ransomware attack was initiated, and the pipeline became aware of the breach due to the widespread encryption on their network and connected computers. The pipeline is then taken offline to avoid any further damage, and the ransom of $4.4 million was paid. On May 12th, 2021, the pipeline was restarted and fully operational, and the U.S. government would later assist the pipeline in recouping nearly half of the ransom.

The Colonial Pipeline attack was initiated by an employee's third-party VPN account password being compromised in a data breach. The employee's password for their VPN was the same password they used to protect their work account(s) and/or computer(s), the specific entry point is unknown. The adversaries,

the DarkSide group, used this duplicate compromised password to access the Colonial Pipeline network and lock devices and networks associated with the pipeline. The heads of the pipeline decided to take the pipeline and the remaining unaffected systems offline to prevent the spread of the malware onto any further systems and networks. While the systems and networks were locked by the ransomware, the adversary group encrypted and exfiltrated over 100 GBs worth of data. Now that the data was in the hands of the adversaries, they threatened to leak the data to the dark web unless the multi-million-dollar ransom was paid. The attack left several impacts including Loss of Productivity and Revenue (T0828), Loss of Availability (T0826), and Theft of Operational Information (T0882). The pipeline was non-operational from May 7th, 2021, to May 12th, 2021, which led to the Loss of Productivity and Revenue (T0828) and Loss of Availability (T0826). The stolen data that the adversaries exfiltrated and threatened to leak also constituted Theft of Operational Information (T0882).

Points of Entry:
The adversaries used an exposed password for a VPN that was compromised during a data breach within the VPN company. This password was a duplicate and was used on other accounts which gave the adversaries access to the employee's work computer or accounts that were protected with that same password.

Impact:
The impacts of the Colonial pipeline attack included a Loss of Productivity and Revenue (T0828) and Loss of Availability (T0826) due to the pipeline being offline from May 7th, 2021, to May 12th, 2021. The data that was stolen and was threatened to be leaked triggered the Theft of Operational Information (T0882).

3.2.2 Black Energy

The following playbook demonstrates how adversaries using the BlackEnergy malware were able to gain initial access in their attack against the Ukrainian power grid. As noted in the figure below, adversaries sent spear phishing emails containing malicious attachments, disguised as seemingly benign Microsoft Word, Excel, or PowerPoint documents (Brook, 2016). An employee downloaded and opened the attachment. Importantly, these documents contained macros. Enabling the macros in the document triggered the malware script to run (Trend Micro, 2016). Once the malware script was activated, it wiped out parts of computers' hard drives and prevented systems from rebooting. There were also varying reports of an associated DDoS attack against the customer call center. These actions culminated in several impacts, including Loss of Availability (T0826), Damage to Property (T0879), Loss of View (T0829), and Denial of Control (T0813). In the context of the attack and its impacts, (T0826) Loss of Availability and (T0879) Damage to Property were associated with the power outages that affected nearly 225,000 people. Loss of View (T0829) and Denial of Control (T0813) were associated with the impact that onsite operators had to switch the dispatch control center to manual mode. With the reports of the DDoS attack against the customer call center, people were unable to call in the center to report power outages, exacerbating the time to recovery.

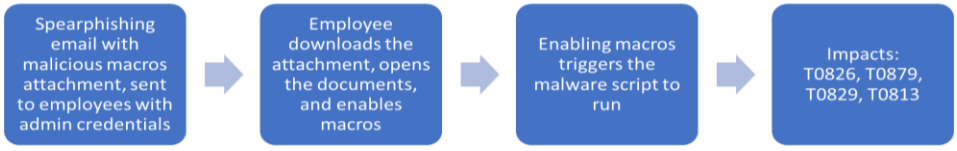

Figure 4: Black Energy Order of Events

3.2.3 Sol Oriens

While the exact point of entry for the Sol Oriens cyber-attack is unknown, it was likely one of two possibilities. It was likely either an exposed password that allowed access to the company's systems that stored important information, or there was a system with a vulnerable remote access protocol, which can allow people remote access and control of the system, as well as the network it operates on. After making initial entry into the compromised system, the adversaries may have laid in wait to monitor normal operations, or they could have immediately conducted their operation which locked infected computers and led to the exfiltration of company documents, employee records, and other publicly unknown information (Din, 2021). The impacts of this attack included Data Encrypted for Impact (T1486), Theft of Operational Information (T0882), and Loss of Productivity and Revenue (T0828). The full extent of the attack and impacts were not made public. Most notably, the ransom amount remains unknown to the public.

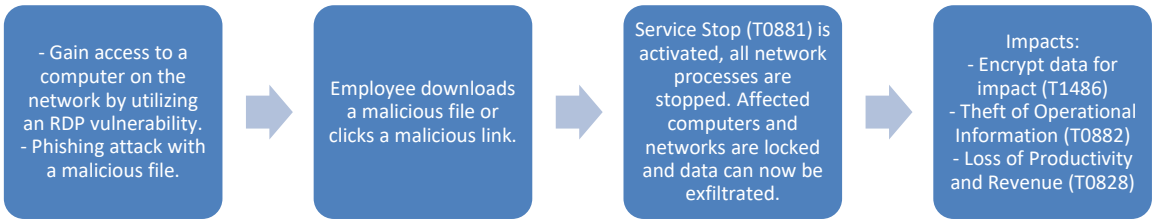

Figure 5: Sol Oriens Order of Events

Points of Entry:
The exact point of entry for the Sol Oriens case is unknown to the public but the adversaries likely utilized a vulnerable remote desktop protocol or a phishing campaign that allowed them access to a company computer or system. If the adversaries utilized a phishing campaign, they would have either sent a malicious email en masse hoping to catch someone off guard, or they could have conducted a targeted phishing attack (spear phishing) and tailored their malicious email to the exact person they were going after. If the adversaries decided to gain entry by gaining access to a vulnerable remote desktop protocol, they could have complete control of the computer that was vulnerable, and then the network that the computer is operating on is likely vulnerable too.

Impact:
The adversaries encrypted and stole data pertaining to the research, contracts, and employees of the organization which is Theft of Operational Information (T0882) and Encrypt Data for Impact (T1486). The Organization also experienced a Loss of Productivity and revenue (T0828) due to the attack.

4. Conclusion

[Research Team] This report provided an overview of ransomware attacks against critical infrastructure, with a focus on attacks against the energy and nuclear sectors. The details and lessons learned from the attacks against Colonial Pipeline, Sol Oriens, Eletrobras, and those executed by BlackEnergy can provide insight on ways to better prepare and defend against future attacks, particularly when examined in the context of the Rational Choice Theory. By making the potential risks outweigh the potential rewards, the rational, logical, adversaries will be less likely to continue their execution of an attack. As such, it is recommended to incorporate any technical additions that create a greater risk to adversaries in terms of their time and effort to execute an attack, chances of being identified, or uncertainty in finding what they are looking for within a system. As seen within the case studies, keeping systems isolated from each other created a risk to adversaries as it increased the amount of time and effort to continue their attack, especially when they were already exposed. In addition to any such technical measures, greater sanctions on adversaries would increase the risk associated with attempting to target an organization. Furthermore, as

the case studies showed that points of entry often rely on human error, a final recommendation is to continue putting emphasis on social engineering training, so that employees do not unintentionally facilitate adversaries in gaining initial access into systems.

The main limitation of this literature review was the reliance on open-source data. However, future work should seek to understand the process by which adversaries conduct their open-source intelligence in their initial selection of their targets. While it would be difficult to gain connections to an existing or former ransomware group to understand this process, a simulated version could also provide insight into the behaviors of adversaries.

[Spirito] The research team took on a challenging assignment to assess control system ransomware, identify or predict the points of entry, and theorize on the motivations of the ransomware group or developer. This paper was the result of a 3-month summer collection and analysis project by a group that is outside of what I would call the hacker collective and thus the analysis exists at a higher level than we generally produce. The open question is whether to take this work and extend it further into the realm of social psychology such that we may be able to more tightly correlate attacker mentality with both points of entry choices and effect delivery options. To be continued…

Page intentionally left blank

Endnotes

Abrams, L. (2021, June 7). *US recovers most of Colonial Pipeline's $4.4M ransomware payment*. https://www.bleepingcomputer.com/news/security/us-recovers-most-of-colonial-pipelines-44m-ransomware-payment/amp/

Barrera, A. (2019, November 12). Ransomware attack at Mexico's Pemex halts work, threatens to cripple computers. Reuters. https://www.reuters.com/article/us-mexico-pemex/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041

Becker, G. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy, 76(2), p.169.

Blackgof (2022). The State of Ransomware in 2022. Blackfog.com. https://www.blackfog.com/the-state-of-ransomware-in-2022/

Borenius, S., Gopalakrishnan, P., Lina, B. T., & Kantola, R. (2022). Expert-Guided Security Risk Assessment of Evolving Power Grids. Energies, 15(9), 3237. https://doi.org/10.3390/en15093237

Brook, C. (2016). BlackEnergy APT Group Spreading Malware via Tainted Word Docs. threatpost. https://threatpost.com/blackenergy-apt-group-spreading-malware-via-tainted-word-docs/116043/

Butrimas, V. (2022). Defending critical infrastructure: The challenge of securing industrial control systems. Hybrid CoE Working Paper (18). https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascds%3AUS%3Aaa3ae3ae-2a9c-334b-abd7-2d04fbc96a34&viewer%21megaVerb=group-discover

Carpenter, T. (2022, March 25). U.S. prosecutors unseal indictments tied to computer hack at Kansas nuclear plant. Kansas Reflector. https://kansasreflector.com/2022/03/25/u-s-prosecutors-unseal-indictments-tied-to-computer-hack-at-kansas-nuclear-plant/

CISA (2014). ICS Alert (ICS-ALERT-14-281-01E) Ongoing Sophisticated Malware Campaign Compromising ICS (Update E). https://www.cisa.gov/uscert/ics/alerts/ICS-ALERT-14-281-01B

CISA (2020, October, 24). Ransomware Impacting Pipeline Operations. cisa.gov https://www.cisa.gov/uscert/ncas/alerts/aa20-049a

Clarke, R. (1992). Situational crime prevention. New York: Harrow and Heston Publishers.

CloudSEK. (2022, May 25). *Cyber Attacks on Energy Sector: Targeting US, Middle East, & South America*. https://cloudsek.com/threatintelligence/cyber-attacks-on-energy-sector-targeting-us-middle-east-south-america/

Cohen, G. (2022). Ransomware Attack Trends: Critical Infrastructure In The Crosshairs. Forbes Technology Council. https://www.forbes.com/sites/forbestechcouncil/2022/03/08/ransomware-attack-trends-critical-infrastructure-in-the-crosshairs/?sh=3082623a5d4c

Din, A. (2021, June 17). *Nuclear Contractor Sol Oriens Hit by REvil Ransomware Attack*. Heimdal Security Blog. https://heimdalsecurity.com/blog/nuclear-contractor-sol-oriens-hit-by-revil-ransomware-attack/

Dragos Inc (2022). Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems. Dragos, Inc. Whitepaper. https://acrobat.adobe.com/link/track?uri=urn:aaid:scds:US:786f712d-1a33-373a-a6b6-e38888272d43#pageNum=1

Gatlan, S. (2022). US Senate: Govt's ransomware fight hindered by limited reporting. Bleeping Computer. https://www.bleepingcomputer.com/news/security/us-senate-govt-s-ransomware-fight-hindered-by-limited-reporting/

Graham, R. (2022, February 13). Germany's Mabanaft Says First Test After Hack Wasn't Successful. Bloomberg.com. https://www.bloomberg.com/news/articles/2022-02-13/germany-s-mabanaft-says-first-test-after-hack-wasn-t-successful

Hunter, B (2022). 'Til the Next Zero-Day Comes, Safety-Critical Systems eJournal. 1(1).

Ibarra, J., Javed Butt, U., Do, A., Jahankhani, H., and Jamal, A. (2019). "Ransomware Impact to SCADA Systems and its Scope to Critical Infrastructure," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 1-12, doi: 10.1109/ICGS3.2019.8688299.

Ilascu, I. (2020, June 11). Power company Enel Group suffers Snake Ransomware attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

Jordan Nuce, Jeremy Kennelly, Kimberly Goody, Andrew Moore, Alyssa Rahman, Matt Williams, Brenden Mckeague, & Jared Wilson. (2021, May 11). Shining a Light on DARKSIDE

Justice.gov (2022, July 13). *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*. justice.gov. https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical

Kaspersky (n.d). BlackEnergy APT Attacks in Ukraine. https://usa.kaspersky.com/resource-center/threats/blackenergy

Kerner, S. M. (2022, April 26). *Colonial Pipeline hack explained: Everything you need to know*. WhatIs.com. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Kovacs, E. (2022, April 12). Energy Provider in Ukraine Targeted With Industroyer2 ICS Malware | SecurityWeek.Com. SecurityWeek. https://www.securityweek.com/energy-provider-ukraine-targeted-industroyer2-ics-malware

Kshetri, N and Voas, J. (2017). Hacking Power Grids: A Current Problem. Computer, 50(12), pp. 91-95, doi: 10.1109/MC.2017.4451203.

Lookingglasscyber (2022, March 31). DOJ Indicts Russian Gov Employees Targeting Power Sector. Lookingglasscyber.com. https://lookingglasscyber.com/blog/news/doj-indicts-russian-govt-employees-over-targeting-power-sector/

MITRE (2022a). BlackEnergy. MITRE ATT&CK. https://attack.mitre.org/software/S0089/

MITRE (2022b). ICS Impact. MITRE ATT&CK. https://attack.mitre.org/tactics/TA0105/

Nicol, D.M. (2021). The Ransomware Threat to Energy-Delivery Systems. IEEE Security & Privacy, 19(3), pp. 24-32, doi: 10.1109/MSEC.2021.3063678.

NJCCIC (2017). BlackEnergy Threat Profile. https://www.cyber.nj.gov/threat-center/threat-profiles/ics-malware-variants/blackenergy

Paganini, P. (2021, June 15). REvil ransomware gang hit US nuclear weapons contractor Sol Oriens. Security Affairs. https://securityaffairs.co/wordpress/118968/security/revil-ransomware-sol-oriens.html

Portugal's EDP hit with costly ransomware attack. (2020, April 17). hydroreview.com. https://www.hydroreview.com/business-finance/portugals-edp-hit-with-costly-ransomware-attack/#gref

Ransomware attack hits K-Electric, disrupts billing, online services. (2020, 10). Energy Update, 5 http://libproxy.temple.edu/login?url=https://www.proquest.com/magazines/ransomware-attack-hits-k-electric-disrupts/docview/2450167668/se-2

Ransomware Operations. Mandiant. https://www.mandiant.com/resources/blog/shining-a-light-on-darkside-ransomware-operations

Rege, A. (2022). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset". Version 12.3. Temple University. Online at https://sites.temple.edu/care/cira/. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

Reshmi, T.R. (2021). Information security breaches due to ransomware attacks - a systematic literature review, International Journal of Information Management Data Insights, 1(2). https://doi.org/10.1016/j.jjimei.2021.100013.

Slowik, J. (2019). Crashoverride: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos, Inc. https://acrobat.adobe.com/link/track?uri=urn:aaid:scds:US:3a14c302-4d6d-3415-b0a2-6b66c4f23d9b#pageNum=1

Soares, B. (2021, February 2). *BR: State-owned energy utility, COPEL, suffers cyberattack*. databreaches.net. https://www.databreaches.net/br-state-owned-energy-utility-copel-suffers-cyberattack/

Staden-Coats, R., & Gupte, E. (2022, February 3). S&P Global Commodity Insights. spglobal.com. https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/020322-cyberattack-causes-chaos-at-key-european-oil-terminals

Stupp, C. (2021, May 11). Energy Tech Firm Hit in Ransomware Attack. WSJ. Retrieved October 16, 2022, from https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034

Thakur, K, Ali, M.L., Jiang, N., and Qiu, M. (2016). Impact of Cyber-Attacks on Critical Infrastructure. Proceedings of the 2016 IEEE 2.nd International Conference on Big Data Security on Cloud. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.22

Trend Micro (2016). Frequently Asked Questions: Black Energy. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/faq-blackenergy

TrendMicro (2016, April 27). Malware Discovered in German Nuclear Power Plant. trendmicro.com. https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant

Trend Micro Research (2022). Ransomware Spotlight AvosLocker. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker

Waldman, A (2022). FBI: Ransomware hit 649 critical infrastructure entities in 2021, techtarget.com. https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021

Walton, R. (2021, December 6). *A month after "malicious" cyberattack, a small Colorado utility still doesn't have all systems back online*. Utility Dive. https://www.utilitydive.com/news/a-month-after-malicious-cyberattack-a-small-colorado-utility-still-doesn/610983/

Warner, T. (2022, February 2). Cyberattack causing problems at ARA storage terminals. Argus Media. https://www.argusmedia.com/en/news/2297896-cyberattack-causing-problems-at-ara-storage-terminals

Zimba, A., Wang, Z., Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems, ICT Express, 4(1), pp 14-18, ISSN 2405-9595, https://doi.org/10.1016/j.icte.2017.12.007.