Uncovering Threats from the Surface Web and Darknet: A Qualitative Analysis of Content Relating to Cybersecurity and Critical Infrastructure

by

Yuxuan (Cicilia) Zhang

B.A., Simon Fraser University, 2019

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Criminology
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY
Summer 2022

Declaration of Committee

Name:	**Yuxuan (Cicilia) Zhang**
Degree:	**Master of Arts**
Title:	**Uncovering threats from the Surface Web and Darknet: A Qualitative Analysis of Content Relating to Cybersecurity and Critical Infrastructure**
Committee:	**Chair: Evan McCuish** Assistant Professor, Criminology
	Richard Frank Supervisor Associate Professor, Criminology
	Bryan Kinney Committee Member Associate Professor, Criminology
	Aunshul Rege Examiner Associate Professor, Criminal Justice Temple University

Abstract

The increasing connectivity of critical infrastructure (CI) is now exposing facilities and institutions to malicious actors who aim to cause significant damage. During the process of a cyber-attack, open-source data could be used by hackers to gather information, knowledge, and plan attacks against targeted CI sectors. The purpose of the current study is to explore and identify the types of data useful for malicious individuals intending to conduct cyber-attacks against the CI industry. Applying and searching keyword queries in four open-source surface web platforms and one darknet forum, search results were reviewed and qualitatively analyzed to categorize information that could be useful to hackers. The thematic results from this study reveal an increasing amount of open-source information useful for malicious attackers against industrial devices, as well as the necessity to implement policies and preventative strategies to counter the increasing threat against critical infrastructure brought by accessible open-source information.

Keywords: Open-source intelligence; critical infrastructure; cybersecurity; thematic analysis; surface web; darknet forums

Acknowledgements

This thesis would not have been possible without the support of many people. I would like to express my deepest appreciation to my supervisor, Dr. Richard Frank, for your guidance and continued support throughout my degree. I would not have discovered my interest in analyzing OSINT and cybersecurity threats against CI without your advice, insight, and encouragement during my research progress. It was a pleasure working with you and I look forward to continuing this collaboration throughout the progress of my PhD studies.

Words cannot express my gratitude to Dr. Bryan Kinney for being a member of my committee and providing invaluable editorial suggestions to my thesis. To my external examiner, Dr. Aunshul Rege, thank you for agreeing to become part of the committee with such short notice in the summertime. I would also like to express my appreciation to Dr. Evan McCuish for chairing my thesis defense.

Lastly, I want to thank my family and friends for supporting (and listening to me complaining about pretty much everything but my supervisor) throughout my degree. I cherish the words of encouragement and the faith you all have in me; I would not been able to complete this thesis without your support. Thank you!

Table of Contents

List of Tables

List of Figures

List of Acronyms

APT	Advanced Persistent Threat
CI	Critical Infrastructure
CIP	Common Industrial Protocol
DNP3	Distributed Network Protocol
DoS	Denial of Service
ICS	Industrial Control System
IoT	Internet of Things
IP	Internet Protocol
MTU	Master Terminal Unit
SCADA	Supervisory Control and Data Acquisition
OPSEC	Operational Security
OSINT	Open-source Intelligence
PGP	Pretty Good Privacy
PLC	Programmable Logic Controller
PoC	Proof of Concept
RTU	Remote Terminal Unit
TCP	Transmission Control Protocol
US	United States

Chapter 1. Introduction

Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems and other smaller systems or controllers, are commonly used in industrial production or critical infrastructure sectors. Essential service sectors such as oil and gas processing facilities, pipeline companies, water treatment plants, as well as power grids are all dependent on ICS and SCADA systems for monitoring and controlling the production and transmission processes (Techslang, n.d.). Over the past decade, the development of automated decision-making and remote accessing and controlling of industrial devices has benefitted service vendors and providers in various aspects. These remote-control systems have reduced manual labour and increased the overall efficiency of production (Coffey et al., 2018; Ghafir et al., 2018; Rodofile et al., 2019; Samtani et al., 2018). Valuing convenience brought by technology, countries like Canada are now connecting every major industry including critical infrastructure to the cyber-world (Public Safety Canada, 2009; Quigley & Roy, 2012). It is no longer rare to find critical infrastructure such as power grids and industrial facilities in service and manufacturing sectors transitioning their Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems from an air-gapped network environment to an externally connected one with internet networks, yielding more opportunities for malicious attacks and cyber warfare (Chen, 2014; Miller & Rowe, 2012; National Institute of Standards and Technology, 2015).

Part of what makes the CI devices at higher risk of security breaches is the availability of open-source intelligence (OSINT) to gather information relevant to CI systems and plan out attacks. The use of OSINT during data gathering by both hackers and security professionals typically involves the use of publicly available sources such as online articles, search engines, websites, social networking platforms, video recordings, open-access databases, as well as personal blogs (Mittal et al., 2016). Both automatic and manual collection methods using different OSINT data gathering tools may be adopted by individuals during the researching process (Ben-Chitrit, 2021). With widely available information related, but not restricted to, cybersecurity and critical infrastructure, such data disclosure could provide hackers opportunities to gather and learn from these online data and pinpoint desirable targets and strategies for successful cyber-attacks (Kranenbarg et al., 2021; Pastor-Galindo et al., 2020). Although previous

literature has pointed out some areas of concern with regards to the danger of OSINT data collection and cybersecurity of industrial systems in the CI sector, studies about the types of CI-related information one can gather from open-source surface web and darknet discussion platforms have rarely attracted researchers' attention. Serving as main platforms for social media sites and information sharing, surface web websites may contain fruitful resources, tools, and data useful for malicious hackers conducting cyber-physical attacks. In addition to surface web OSINT research, the existence of darknet discussion forums may also serve as locations for malicious actors to search, collect, and exchange information relevant to CI facilities and vulnerabilities.

This thesis aims to explore the major types and potential use of data obtainable by malicious individuals targeting the CI industry from the openly accessible surface web and darknet. Using publicly available OSINT resources such as step-by-step tutorials, technical analysis of zero-day exploits[1], or information and discussions about vulnerable devices, exploits, and open-source tools, this study provides rich information about cyber-attacks against critical infrastructure systems. The findings of the current study may provide insight on the potential threat surface web and darknet forum contents could pose to CI facilities, as well as aid in the development of more rigorous mitigation strategies, policies implications, and recommendations to CI vendors to prevent from future cyber-attacks.

1.1. Critical Infrastructure, Cybersecurity, and Related Threats

According to Public Safety Canada (2021), critical infrastructure (CI) includes both independent or interconnected "systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government" (para.1). Throughout the years, the sectors considered as essential CI service has changed (Boyle & Speed, 2018). Although the types of essential services represented in different CI sectors were briefly described by Public Safety Canada as part of its response to the recent COVID-19 pandemic, the classification of CI in Canada still remained unclear (Public Safety

[1] Zero-day exploits are vulnerabilities or system flaws discovered by cybercriminals but were unknown to program developers (Stouffer, 2021).

Canada, 2021). Within Canada, critical infrastructure is categorized into ten different sectors: Energy and utilities, information and communication, finance, health, water, food, transportation, safety, government, and manufacturing (Public Safety Canada, 2016). Each of the above sectors is governed by designated sector-specific federal agencies.

It has been recognized by both Canadian and international governments that recent digital transformation and increased hyper-connectivity between CI facilities and the internet have opened more vulnerabilities and weak points for malicious actors to research, target, and exploit (Ablon et al., 2014; Public Safety Canada, 2021). Unlike expensive and resource intensive traditional physical attacks on CI facilities, the interconnected nature of industrial devices makes cyber-attacks against CI sectors inexpensive (Public Safety Canada, 2016). Further, malicious actors are also experiencing lower levels of risk during the planning and launching stages of these large-scale attacks. The rise of cybersecurity incidents indicated that cyber vulnerabilities would become a persistent issue, and threat actors such as hacktivists, for-profit criminals, advanced persistent threats (APTs)[2], and insider threats will continue to be hazardous against Canadian CI (Public Safety Canada, 2016; Zajko, 2015).

When discussing the danger of cyber-attacks against CI in Canada, there is an increasing concern that these attacks against common Industrial Control Systems (ICS), including the Supervisory Control and Data Acquisition (SCADA) systems, may result in serious damage and dysfunction of CI facilities (Nicholson et al., 2012; Public Safety Canada, 2016). Within the current industrial system, multiple devices, including but not limited to the programmable logic controllers (PLCs), remote terminal units (RTUs), master terminal units (MTUs), three-term controllers (PID controllers), and SCADA servers, all require internet to complete the automation process (Rodofile et al., 2019; Samtani et al., 2018). Specific communication protocols for industrial production are also coded, such as the Modbus protocol, Transmission Control Protocol/Internet Protocol (TCP/IP), Distributed Network Protocol (DNP3), and Common Industrial Protocol (CIP) (Tariq et al., 2019). Functioning interdependently in the system, a successful intrusion in any of these devices or protocols would compromise the entire system and ultimately

[2] Advanced persistent threats (APTs) are intruders or groups of cybercriminals conducting long-term, sophisticated hacking techniques to continuously monitor and mine sensitive information from their targets (Kaspersky, 2022d).

result in cascading failure of multiple interconnected SCADA systems in the industrial sector. As systems start to fail after successful attacks, broad-scale impacts may arise, including financial and physical damage to the facilities, loss of lives, and damage to the reputation and market share of the companies (Goebel et al., 2019; Nicholson et al., 2012).

The physical and financial consequences discussed in previous literature are beyond sheer imagination; prior cyber-attack incidents against CI facilities have demonstrated the severe damage residents and countries may experience. For example, in 2015, a group of Russian hackers deployed a malware attack targeting electrical utilities functioning in Ukrainian power grids causing a blackout affecting almost a quarter-million residents in the Western region of Ukraine (Zetter, 2016). Soon after the first-ever successful cyber-physical attack against Ukrainian power grid, the same group of hackers conducted a second attack in 2016, causing widespread power outages in the city of Kyiv (Greenberg, 2017). The blackout, which happened in the winter, caused Ukrainian residents unable to access electricity and heating for hours. Five years after these two incidents, the same group was discovered conducting a third cyber-attack against Ukrainian power systems (Greenberg, 2022). Consisted of functions from the old Industroyer[3] malware, the modified malware named Industroyer2 was deployed against high-voltage electrical facilities. Fortunately, the malware was detected on time and no damage was caused to any power stations (Greenberg, 2022).

In the United States (US), a recent hack against a water treatment plant in Oldsmar, Florida alerted the world again to the potential damage cyber-physical attacks can cause to citizens and public services (Bergal, 2021). In February 2021, the water plant was cyber-targeted and the operating system controlling water-treating chemicals was infiltrated and remotely controlled, resulting in the release of toxic levels of sodium hydroxide to the water supply of the facility. Noticing the intrusion, an employee was able to quickly fix the level of chemical dispersed in the water and prevented residents in the town from water poisoning. Had this attack not been noticed by the operator, water

[3] Industroyer (also referred as Crashoverride) is a malware designed and deployed by a group of Russian hackers to attack the Ukrainian power grids in 2016. The malware was specifically programmed to target Industrial Control Systems (ICS) within the infrastructure sectors (Mitre, 2022).

released into the town's supply system would have caused severe health and physical damages to its users (Bergal, 2021).

These incidents and system breaches in Ukraine and the United States displayed the dangers of cyber-physical attacks against often vulnerable critical infrastructure sectors. Although such large-scale incidents have not yet been reported in Canada, it does not mean that Canadian CI facilities are out of malicious actors' reach. According to Parent and Beatty's (2021) report, companies and infrastructure systems are now under the risk of newer types of cyber threats and attack tactics. In fact, in December 2020, Metro Vancouver's major transportation network TransLink was targeted, and sensitive personal information were remotely accessed by a malicious hacking group named Egregor (Judd & Little, 2020; TransLink, 2022). Despite no incidents were yet discovered to misuse information obtained from the TransLink cyber-attack, the case warned of the damaging attacks that may occur to Canada's CI sectors. It is thus important to understand the dangers and threats malicious actors may pose against critical infrastructure.

1.2. The Cyber-attack Kill-Chain

Extensive research has been carried out to understand the process and purpose of various cyber-attacks (Coffey et al., 2018; Ghafir et al., 2018; Hahn et al., 2015; Hutchins et al., 2010). Building upon the increasing interest in cybersecurity and cyber-attacks, Hutchins et al. (2010) proposed a kill-chain model with seven end-to-end stages of a cyber-attack, informing a starting point for research layering out what and how hackers need to do prior to a successful cyber-attack. Upon preparation of a cyber-attack, hackers will often follow this path: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally to act on an objective (Hutchins et al., 2010).

The first stage in the kill-chain, reconnaissance, refers to the phase when hackers gather information about the target to plan out the attack (Coffey et al., 2018; Ghafir et al., 2018; Hahn et al., 2015). Reconnaissance data are vital to a successful attack: Attackers are required to obtain information related to communication configurations, ports and exploitable vulnerabilities, as well as ideal devices granting access to the system in order to proceed to later attack stages (Coffey et al., 2018).

Using data gathered in the research stage, hackers then develop custom malware against the desirable target and seek suitable means to distribute the exploit in the weaponization (stage 2) and delivery (stage 3) phase (Hutchins et al., 2010). The successful delivery of the exploit would then trigger the exploitation stage (stage 4) where malicious codes start running and infecting the host system, followed by the installation of malware (stage 5) granting access to the hackers (Hutchins et al., 2010). The intrusion of malware into the host provides hackers with full command and control (stage 6) over the target system, allowing them to take actions to achieve their goals. In attacks targeting critical infrastructure and cyber-physical systems such as power grids and industrial manufacturing plants, hackers often intend to achieve physical objectives (stage 7) such as disruption of service and/or destruction of the facility by commanding and controlling the devices (Hahn et al., 2015).

1.3. Open-source Data Gathering

Advances in the Internet of Things (IoT) and exposure of industrial devices to the internet is now putting systems in the CI sectors at higher levels of risk. The term IoT refers to the collection of smart devices connected to the internet for easier controlling and accessibility (Trend Micro, 2021). While IoT can bring advantages in terms of productivity, these connected devices were often targeted by cybercriminals due to their lack of security. In comparison to other connected networks or systems, IoT devices were manufactured without standardized guidelines or security measures in place (Kaspersky, 2022b). Further, users of IoT devices, such as industries and ICS vendors, often did not implement strong security solutions, therefore exposing CI devices to various security issues (Kaspersky, 2022b; Trend Micro, 2021).

The cybersecurity risks became particularly problematic when an increasing amount of ICS-related open-source information and tools are available to the public. Hackers with low or advanced hacking skills, including script kiddies[4], could conduct OSINT search with the purpose of identifying and exploiting vulnerable targets (Stannard, 2021; Verton, 2001). Platforms including surface web search engines, as well

[4] Script kiddies are low-skilled cybercriminals who use pre-existing malware or programs for their cyber-attacks (Lutkevich, n.d.). They often do not understand the functions of these programs, nor can they write or develop malware on their own.

as darknet discussion forums, are commonly used by cybercriminals to conduct research and reconnaissance prior to cyber-attacks (Bermudez Villalva et al., 2018). Researchers have begun to see that data gathered through public domain could help both cybersecurity professionals and malicious hackers significantly in the reconnaissance stage (Hayes & Cappa, 2018; Samtani et al., 2017). To demonstrate, Samtani et al. (2017) conducted a study focusing on gathering hacking-related data from hacker communities. The findings suggested vast amounts of information related to hacking and cyber-attacks obtainable by malicious individuals from online sources (Samtani et al., 2017). The availability of new generation data gathering tools and platforms, therefore, provided hackers opportunities to identify vulnerable targets, settle efficient exfiltration methods, as well as to evolve their hacking tactics (Papastergiou et al., 2020).

1.3.1. Surface and Darknet Platforms

The world wide web holds rich sources of information relevant to hacking and CI facilities, but data gathering through these different layers of the internet sometimes require different techniques and applications. Currently, the internet has been commonly divided into three layers: the surface web, the deep web, and the darknet (Kaur & Randhawa, 2020). The surface web is the visible section of the internet; it contains all visible, indexed content accessible to the public using regular search engines (e.g., Google). Making up over 90% of the web content, on the other side, the deep web contains a variety of hidden content unidentifiable by standard search engines, including academic journals behind paywalls, databases requiring authorization, or darknet contents (Kaspersky, 2022a). Lastly, being part of the deep web, the darknet consists of unindexed contents accessible only through specialized web browsers (Guccione, 2021; Kaspersky, 2022a; Kaur & Randhawa, 2020).

The three layers of the internet are constantly accessed by hackers during their data gathering process. Publicly accessible information, including results returned from search engines and open discussion forums, were confirmed to help hackers to collect data, share knowledge, and establish virtual peer connections (Meland et al., 2020). Through using OSINT techniques in the surface web, information about CI facilities and personnel working in CI sectors may be gathered and analyzed (Mittal et al., 2016). Further, surface web social networking platforms may also contribute to the resilience of

illicit information exchange in the darknet (Kwon & Shao, 2021). In Kwon and Shao's (2021) study on content discussed in Reddit, they suggested that Reddit and other social media platforms may serve as gateways of knowledge and could direct individuals to darknet websites and exchange illicit contents in the hidden web.

Despite providing rich open-source intelligence on CI facilities and cybersecurity, it is rare for surface web platforms to directly display illicit hacking information on their sites. The monitoring infrastructure and legislative boundaries often prevented any incriminating and controversial contents to be shared in the surface web (Google Search Help, 2021; Reddit, 2021; YouTube Help, 2021). Consequently, malicious actors may attempt to access additional hacking information through darknet platforms such as discussion forums and hacker communities. The Tor browser is often preferred by individuals to access hidden contents within the darknet (Kaspersky, 2022a). Originally established by the US Navy, the browser's ability to anonymously browse hidden contents in the internet was quickly recognized and abused by malicious actors to share and access illicit contents in the darknet (Kaur & Randhawa, 2020; Tor, 2021). The issue has been brought up by several researchers; all of them have suggested that the development of Tor browser has led to the rapid growth of illegal and controversial contents in the darknet (Guccione, 2021; Kaur & Randhawa, 2020).

As suggested by Hurlburt (2017), the illicit content within the darknet may be responsible for many cybersecurity threats. Darknet chat rooms and discussion forums, in particular, provided members a place where they can share their knowledge and experience on controversial issues (Buxton & Bingham, 2015). According to some studies, the availability of discussion forums offered hackers locations to communicate with each other regarding specific hacking practices and network intrusion techniques (Deb et al., 2018; Jordan & Taylor, 1998). In both Deb et al. (2018) and Jordan and Taylor's (1998) research, skilled members in the forum were observed to aid in the resource sharing processes through means of publishing their malware codes, or posting tutorials or personal experiences useful for acquiring hacking skills. The findings, therefore, suggested that malicious actors wishing to conduct cyber-attacks against computer systems can develop their technical abilities through accessing these hacking forums as a resource (Jordan & Taylor, 1998; Leukfeldt et al., 2017). This view was supported by Shakarian et al. (2016) which argued that publicly accessible forums allowed less sophisticated hackers or aspiring hackers to gain hacking-related

knowledge and status through learning and practicing hacking against vulnerable targets. Furthermore, cybercriminals may also establish their social networks online through accessing various discussion forums (Leukfeldt et al., 2017). Leukfeldt et al. (2017) analyzed hacker networks and argued that the existence of cybercriminal forums is important in the establishment of social networks and bonds among malicious attackers. The study research indicated the ability for forum members to not only acquire knowledge necessary for carrying out cyber-attacks, but also to participate in different hacking organizations and peer networks (Leukfeldt et al., 2017).

1.3.2. Network Scanners

Open-source data gathering research focused on the impact of OSINT tools such as network scanners on cybersecurity have also been studied extensively (Bodenheim et al., 2014; Chen et al., 2020; Samtani et al., 2018). Publicly available network scanners, with their ability to search for internet-connected industrial devices, for example, can be exploited by malicious attackers (Bodenheim et al., 2014). According to Bodeheim et al. (2014), in fact, Shodan search engine was able to collect information on ICS devices through establishing communications with open service ports. Upon successful communication between the Shodan signal and the service port, the search engine would record information including the device's location, IP address, as well as detailed data such as open ports, services, and protocols exploitable by hackers (Bodenheim et al., 2014; Shodan, n.d.). This rendered Shodan as one of the most useful network scanning search engines available to the public, identifying all of the four PLC[5] devices and the static IP addresses assigned to each of the controller, demonstrating the search engine's ability to discover internet-connected industrial devices (Bodenheim et al., 2014).

Recent studies of Shodan have further confirmed Bodeheim et al.'s (2014) result (Chen et al., 2020; Samtani et al., 2018). In 2018, researchers found that more than 500,000 internet-connected SCADA devices are discoverable through Shodan; numerous devices were detected to have existing exploitable features such as the use of default credentials and unpatched system vulnerabilities (Samtani et al., 2018). Another

[5] A Programmable Logic Controller (PLC) is a device monitoring and controlling the functions and manufacturing process of industrial production line (AMCI, n.d.).

study conducted by Chen et al. (2020) discovered Shodan's capability of identifying and indexing all six honeypots[6] they released to the public, demonstrating the exploitable scanning abilities and functions featured in OSINT tools during the reconnaissance stage of a cyber kill-chain.

1.3.3. Social Engineering

Apart from focusing on the data-gathering process using OSINT tools, previous research has focused on social engineering based cyber-attacks and human-centric factors affecting ICS as well (Green et al., 2015; Jagatic et al., 2007). Social engineering is referred to as a "form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity" (Jagatic et al., 2007, p.94). For malicious attackers, employees with access and control over internal networks and CI facilities are often targets to gather information and perform attacks on. Through leveraging different OSINT tools, social networking information and techniques, malicious offenders can target vulnerable employees working in the CI sectors and exploit their trust and personal information for cyber-attacks (Green et al., 2015; Huber et al., 2009; Mansfield-Devine, 2018). In some scenarios, malicious attackers would conduct social engineering through forms of coercion, manipulation, intimidation, or blackmailing the targets using the information they obtained online (Ghafir et al., 2018).

The selection of ideal targets among the list of employees working in the CI sector is not random; only employees with select features or characteristics are considered as ideal targets (Edwards et al., 2017; Hayes & Cappa, 2018; Huber et al., 2009; Mansfield-Devine, 2018). Particularly, hackers would look for the ranking or position of the employee within the company. Key employees working in target industrial companies would attract most of the attackers' attention as they often possess confidential information and administrator usernames and passwords that would grant privileged access to control systems (Hayes & Cappa, 2018).

[6] Honeypots are functioning computer systems set up as vulnerable targets attracting cybercriminals into attacking them (Kaspersky, 2022c). Hackers' behaviors and attack patterns can be traced and studied after honeypot systems are attacked.

Other demographic characteristics such as gender, cyber awareness and skills, or frequency and amount of personal information employees shared online are also important features to consider (Edwards et al., 2017; Huber et al., 2009; Mansfield-Devine, 2018). For example, Jagatic et al. (2007) conducted an experiment sending out phishing emails to a group of targeted participants; the findings suggested female employees and individuals who do not have technology backgrounds are more likely to become victims of social engineering. Through manual or automated data gathering methods, attackers could easily identify employees with desirable traits which could signal their low resistance against social engineering and therefore deploy phishing emails to gain trust from these victims (Huber et al., 2009). The information gathered from the public domain containing organization's contact information, identification of an individual as an affiliate or employee in the company, as well as social media connections between different colleagues are also rich sources of information for malicious attackers, allowing them to curate scenarios less likely to be detected by targeted victims as fraudulent (Edwards et al., 2017).

1.4. Operational Security and Anonymity

As defined by Computer Security Resource Center (n.d.), operational security (OPSEC) is referred to the implemented methods ensuring the security and privacy of any sensitive information. While the concept was invented and used more by government and military sectors, the same OPSEC process was widely discussed and adopted by individuals valuing their privacy and system security (Computer Security Resource Center, n.d.; Zhang, 2020). Currently, the standard OPSEC process is divided into five major steps: Critical data identification, threat analysis, vulnerability examination, risk assessment, and countermeasure implementation (Security Studio, 2021).

Although privacy-oriented browsers such as Tor employ multiple layers of encryption and use random routing to ensure the anonymity of their users, many hackers preferred applying additional OPSEC methods prior to accessing or engaging in illicit darknet activities (Kaur & Randhawa, 2020). For malicious hackers, privacy-focused operating systems and software may be installed to further enhance their anonymity. For example, encryption techniques such as the Pretty Good Privacy (PGP) encryption system, is commonly adopted by darknet users when communicating online (Petters,

2020). Bermudez Villalva et al. (2018) discovered from their study that when accessing leaked Gmail honey accounts, experienced attackers with higher levels of skills and awareness are more likely to use privacy-oriented systems such as Linux. Similarly, articles by Diaz (2021) and Watson (2017) showed that most of the preferred operating systems recommended by cybersecurity professionals are Linux-based systems. As noted by the authors, systems such as virtual machines, Tails, or Whonix operating systems can add extra layers of privacy-oriented protection, ensuring individual's personal information and online activities difficult to trace by governments and/or hackers (Diaz, 2021; Watson, 2017).

Empirical research on hacking forums and darknet marketplaces have highlighted the importance of anonymity and operational security to users when accessing illicit content. As Barratt (2011) suggested, pseudonymous in online environments may encourage members to contribute and engage in forum discussions on controversial and illegal topics. Supporting Barratt's (2011) suggestion, Shakarian et al.'s (2016) study on hacker forums reported the characteristics and contents shared between cybercriminals; the authors concluded that good OPSEC is prioritized and discussed across various sub-forums. Within hacker communities, malicious actors often stressed the separation of their real and online identity, and that personally identifiable information should never be discussed within the forums. Similarly, Kwon and Shao (2021) also found that within hacking forums, threads on the topic of establishing and maintaining good OPSEC is often discussed and recommended by community members. Particularly, the maintenance of good personal OPSEC has been recognized by some individuals as the preferred method to evade possible criminal prosecution after their engagement in illicit hacking activities (Shakarian et al., 2016).

1.5. This thesis

This thesis helps to resolve the lack of research in the types of open-source data related to critical infrastructure searchable from the surface web and darknet. Previous literature related to the use of OSINT data have principally focused on developing and testing data mining or deep learning models used to detect and track communications and motivations shared by criminals online (Pastor-Galindo et al., 2020). Although studies concerning OSINT data-gathering for the purpose of malicious cyber-attacks are on the rise, most research has concentrated on exploring personal profiles useful for

social engineering attacks, or general illicit materials circulated in the darknet (Kalpakis et al., 2016; Pastor-Galindo et al., 2020).

To my knowledge, there has been a lack of research focusing on OSINT data related to the cybersecurity of CI facilities circulating in the surface web and darknet platforms. While studies have discussed OSINT data, techniques, and the benefit of them in areas of risk assessment or cyber-forensic analyses, the majority of tools and information were examined and applied in platforms including (but not limited to) Twitter, Facebook, or Shodan (Bodenheim et al., 2014; Chen et al., 2020; Kalpakis et al., 2016; Pastor-Galindo et al., 2020). Further, research related to darknet forums tend to focus more on illicit underground drug markets, whereas hacker communities or discussions focusing on hacking remain under-researched (Kalpakis et al., 2016). Indeed, current OSINT-related research rarely paid attention to the types of CI-related data offered in both surface web search engines and darknet discussion forums that could greatly benefit ill-intended hackers. As there has been a substantive increase in the quantity and frequency of cyber-attacks as well as hacking against organizations and businesses, the types of exploitable OSINT data retrieved from different web platforms may pose serious security threat on CI or other industrial devices. As such, I aimed to answer the following research questions:

RQ1. What types of CI-related data can be found from the surface web and the darknet?

RQ2. How can these data be useful for malicious cyber-attackers?

Chapter 2. Surface Web Platform Analysis

The following sub-chapters detailed out data sources and methods used in analyzing OSINT information available in the surface web platforms. As stated in the earlier chapter, prior studies have discussed the danger of OSINT techniques and data gathering processes. The literature, however, did not discuss in detail the types and uses of open-source data relevant to CI facilities. Therefore, websites and information from publicly accessible surface web platforms were collected and analyzed for this study.

2.1. Methodology

2.1.1. Data Sources

The dataset for this research was collected based on results returned from keyword queries in four open-source search engines and websites including Google, Reddit, YouTube, and Shodan on the surface web. These four platforms were specifically selected for the study as they are all widely known public search platforms accessible for internet users to find information and have their questions answered. The platforms are also bounded by content posting policies where sensitive information will be monitored and removed (Google Search Help, 2021; Reddit, 2021; YouTube Help, 2021). Open-source data from privacy-oriented programs such as DuckDuckGo were not investigated or included in the current study as more effort and knowledge related to the search engine are required, and the search extension is not commonly used by users (DuckDuckGo, 2021). Thus, those types of websites and search engines were excluded.

2.1.2. Data Collection

A purposive sampling technique was employed; a list of keyword queries relating to industrial control systems and critical infrastructure was composed deductively and searched in the four selected open-source search engines. The set of keywords contained parts and devices commonly installed in CI facilities, including model names and product series manufactured by specific commercial brands (e.g., Schneider,

Honeywell, Eaton, etc.). Further, a list of malware used to attack CI facilities were also included in the keyword queries. *Table 2.1* presents all the keywords bulk-searched from the targeted open-source websites in the current study. The default search setting was applied to all websites (e.g., Google, YouTube, Reddit); no filters or advance search settings were applied. All posts were by relevance. The keyword search yielded over 4,000 results aggregated across either of the Google[7], YouTube, and Reddit searches (*Figure 2.1*).

Table 2.1. List of keyword queries searched in surface web platforms

Keyword Set #1		Keyword Set #2
(SCADA OR supervisory control and data acquisition)		
(programmable logic controller OR programmable logic controllers OR PLC)		
(PID OR PID controller OR three-term controller)		
(RTU OR remote terminal unit)		
(Modbus OR DNP3)		
(Modicon OR Unitronics)		
(Eaton OR Eaton industrial OR Honeywell OR Midas gas detector)		
(CirCarLife OR Advantech OR Laquis)		
(SINEMA Siemens OR industrial OR server)		
(PROFIBUS OR Honeywell HART OR Simatic OR Schneider OR Cisco)		
(infrastructure OR chemical OR dam OR emergency OR nuclear OR transportation OR water OR plant OR energy OR blackout OR electricity OR power OR gas OR industrial OR manufacturing cascading failure)	**AND**	(exploit OR vulnerability OR hack OR malware OR attack OR zero-day OR 0day OR access OR intrude)
(industrial control system OR ICS OR critical infrastructure)		
(PCS OR process control system OR advanced process control OR distributed control system OR distributed control systems OR DCS)		
(GE Automation OR OMRON industrial controller OR OMRON PLC OR Mitsubishi electric PLC)		
(very small aperture terminal OR VSAT OR power grid OR smart grid)		
(Dragonfly OR Havex OR Industroyer OR Crashoverride OR Stuxnet OR Duqu OR BlackEnergy OR Triton OR Trisis OR EKANS OR MegaCortex)		
		Total keywords (*N*) = 81

[7] Only a certain number of most relevant results were displayed by Google keyword search, with majority of the repetitive and non-relevant webpages were omitted.

The initial plan was to unify the data collection method and evaluate the keyword search results returned from all of the publicly available search engines including Shodan. Due to the device-scanning nature of Shodan, the search engine would only return information on internet-connected critical infrastructure devices, protocols, or product series. Therefore, a modified list of keywords containing the devices' names and model series (e.g., Siemens S7, PLC, Modbus, SINEMA, etc.) was searched in Shodan. Instead of counting the number of vulnerable or scannable devices, the number of threats were counted and included in the sample. For example, a total count of 396 publicly searchable Modbus devices across the world would be considered as one single Modbus-related cybersecurity threat in the dataset. The modified keyword search and count yielded 28 unique CI-related cyber threats identified by Shodan search engine.

2.1.3. Data analysis

All relevant results displayed by search engines (Google and Shodan) were analyzed during the analysis phase (n=3,530). As the sum of search results returned from YouTube and Reddit searches were not displayed, a random selection of 70 YouTube videos, as well as 400 posts from Reddit were reviewed until saturation was reached.

From among those collected data, criterion sampling was employed to identify information-rich webpages and to filter out irrelevant contents that were not of interest for this study (Palinkas et al., 2015). Through implementing the purposeful criterion sampling method, a maximum number of results relevant to the current study could be captured and analyzed by researchers. A five-year range starting from 2015 to 2020 was selected for data collection to ensure the information obtained online was up-to-date. Therefore, only content published between January 1st, 2015 to July 15th, 2020[8] were recorded for analysis. To be included, results also had to provide enough information for a malicious hacker about CI systems and information related to hacking these systems. For example, content reporting occurrences of cyber-attacks will be excluded as it does not contain much information related to hacking techniques. On the

[8] This is the last day of data collection for the surface web platform analysis.

other hand, websites that may have contained information about exploitable CI facilities, or technical analysis and in-depth discussion relating to CI mechanisms or security will be included for further analysis. Lastly, to be included in the study, data was limited to English language content.

Contents remained after applying criterion sampling will be kept in the same Excel spreadsheet for qualitative analysis. Enghoff and Aldridge (2019) have emphasized on the value of naturally occurring unsolicited online data for research projects. Further, collection and analysis of digital data such as OSINT information may provide insight for researchers in understanding the thoughts, characteristics, and cybercrime patterns (Décary-Hétu & Aldridge, 2015). Thus, a qualitative thematic content analysis approach is best suited for answering the research questions proposed in my study and to uncover the common types and use of information obtainable from OSINT sources by malicious attackers (Braun & Clarke, 2006; Kamphausen & Werse, 2019; Palys & Atchison, 2013).

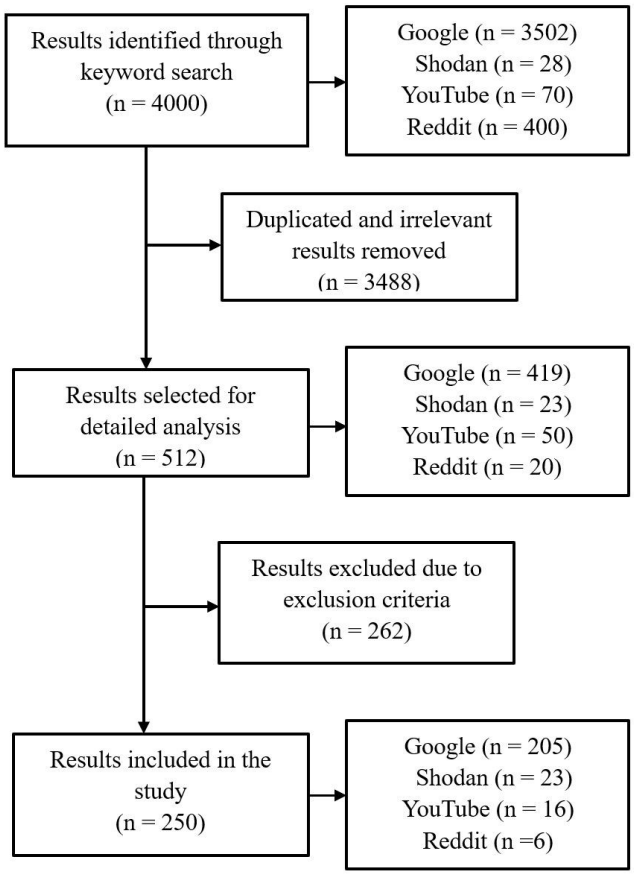


Figure 2.1. Surface web results selection process

Four rounds of inductive coding were conducted to allow the development of descriptive codes. The results and the themes that emerged from the thematic analysis were presented. First, I conducted a title review; data that met the inclusion criteria at this stage were recorded in a spreadsheet for further analysis. Then, a first round of coding was conducted and any results that did not meet inclusion criteria were excluded. Coding and analysis of all results that emerged from the keyword queries were completed by the author. The final sample included in this consisted of 205 webpages discoverable from Google, 23 results retrieved from Shodan, 16 videos from YouTube, as well as one relevant Subreddit[9] community and five threads (*Figure 2.1*). The codes and themes were developed during the progress. All the contents listed in the final sample were analyzed and coded individually in the same spreadsheet, with the authors' names replaced with letters (e.g., *Author A*, *Author B*, *Website C*, etc.). A total of six codes emerged from the dataset and were later collapsed into three main themes.

2.2. Results

In this section, I detail the types of data malicious attackers could retrieve from open-source web searches. A total of three main themes were identified after three rounds of coding: "Indirect reconnaissance data," "Proof-of-concept codes," and "Educational materials." Within the themes, three sub-themes were identified in "Indirect reconnaissance data," and two sub-themes were categorized under the theme "Educational materials." A complete list of the themes, sub-themes, and the frequency count emerged from the current dataset can be found in *Table 2.2* below. The findings were consistent with results discussed in previous literature (Albataineh & Alsmadi, 2019; Cartagena et al., 2020; Coffey et al., 2018; Hahn et al., 2015; Hayes & Cappa, 2018; Positive Technologies, 2018; Samtani et al., 2018). Although most of the information from open-source websites were intended for cyber-security personnel or ethical hackers with benign purposes, the same set of data, such as threat-related information, hacking trainings, as well as published proof-of-concept exploits, could be abused by malicious hackers against critical infrastructures and vendors.

[9] Subreddit is referred to an online community residing within Reddit.

Table 2.2. Surface web platforms results: themes, sub-themes, and frequencies

Theme	Sub-themes	Frequency (%)
Indirect reconnaissance data	Threat-related information	132 (52.8%)
	Hacking and reconnaissance tools	32 (12.8%)
	Demonstration videos	12 (4.8%)
Proof-of-concept codes		40 (16.0%)
Educational materials	"How to" tutorials	26 (10.4%)
	Training courses	8 (3.2%)
		250 (100%)

2.2.1. Indirect Reconnaissance Data

The majority of the information (70.4%) I discovered through OSINT search of keywords were data helping hackers indirectly during the research stage of cyber-attack kill-chain (n=176). The availability of such knowledge allows attackers to determine the appropriate hacking strategy, methods to avoid detection, the malware of choice, as well as ideal targets prior to the attack. Three forms of data were identified in the open web: (1) threat-related information; (2) hacking and reconnaissance tools; and (3) demonstration videos.

Threat-related Information

General information about critical infrastructure, vulnerable industrial devices and potentially useful malware was the most prominent type of data one can look up in the public domain. Online communities such as Reddit allowed their users to share hacking-related information potentially related to critical infrastructure. In one of the posts, *User A*[10] shared a book with an updated version of programming code for members interested in learning coding and understanding cybersecurity. *User A* suggested in his post, that "some of the contents of the book cover how to program port scanners, reverse shells, your own botnet command and control center, extract EXIF information from image files, instantiate an anonymous browser in Python and more." The content shared by users like *A* suggested that individuals could gather useful cybersecurity information from social networking communities.

[10] Identities and usernames of posters and content creators were replaced with random letters.

Although Reddit allowed its members to ask questions with regards to existing bugs and exploitation techniques with each other, certain rules had to be followed and were enforced by volunteer moderators. The public nature of social media often required various platforms to strictly obey the rules and regulations enforced by the government. One subreddit was particularly concerned about the contents posted in the community and stated:

> "Avoid self-incriminating posts. Sometimes you might do some research that is ethically (and legally) questionable. Soliciting others to incriminate falls under this umbrella, as you would become co-conspirators. This is Reddit, and this is public. Use your brain. … No "Please hack X" posts. Save that shit for hack forums." (Subreddit R1)

Information released in governmental websites or academic journals or conference publications could provide insight for malicious attackers as well. For example, *advisory*[11] *B* provided both descriptions of the vulnerability and its affected device models and software versions:

> "A Heap-based Buffer Overflow was found in Emerson OpenEnterprise SCADA Server 2.83 (if Modbus or ROC Interfaces have been installed and are use) and all versions of OpenEnterprise 3.1 through 3.3.3, where a specially crafted script could execute code on the OpenEnterprise Server."

Most of these sources would be beneficial to hackers in the planning phase when easy-to-target models and services, potential attack strategies, and available vulnerability for malware-development need to be decided.

Similar to the information posted in public advisories and articles, technical analysis reports could also provide hackers with vague instructions on how certain strategies and cyber-attacks were employed on industrial devices. For instance, *report C* analyzed the malware CrashOverride and discussed the features and registers of the backdoor module found in the exploit's artifact,

> "… reviewing memory during execution and analysis of other modules in the malware indicates that \Sessions\1\Windows\ appears multiple times, indicating that a check may be performed. The backdoor writes a file to either C:\Users\Public\ or C:\Users\<Executing User>."

[11] Advisories are announcements and alerts identifying and describing cybersecurity vulnerabilities discovered in computer systems and/or software.

This type of analysis was common in reports produced by technical analysts since security personnel were required to understand zero-day exploits prior to the development of patches and mitigation strategies for these vulnerabilities. Oftentimes, academic researchers were also interested in publishing journals or blogs about exploitable industrial devices:

> "Another diagnostic command attacker can use is Read Device Identification as an attempt to gather information on Modbus device: A MODBUS request packed with function code 43 Read Device Identification will cause a MODBUS server to return the vendor name, product name, and version number. Additional information may also be provided in optional fields. An attacker sends the MODBUS request packet with function code 43 to all systems in the network and gathers intelligence that may be helpful in future attacks." (Researcher D)

As described by *researcher D*, a hacker could obtain detailed information of a target device by injecting certain command toward the Modbus system. Although the information was meant to alert service providers about the cybersecurity threat and to encourage the implementation of mitigation strategies, malicious attackers could gather and abuse this information during the reconnaissance stage and plan cyber-attacks accordingly.

Some public sources were able to give directions to hackers on social engineering techniques toward employees working in the target industrial company. Providing instructions on what pirates should do prior to hacking into SCADA systems in the cargo ships, *presenter E* said:

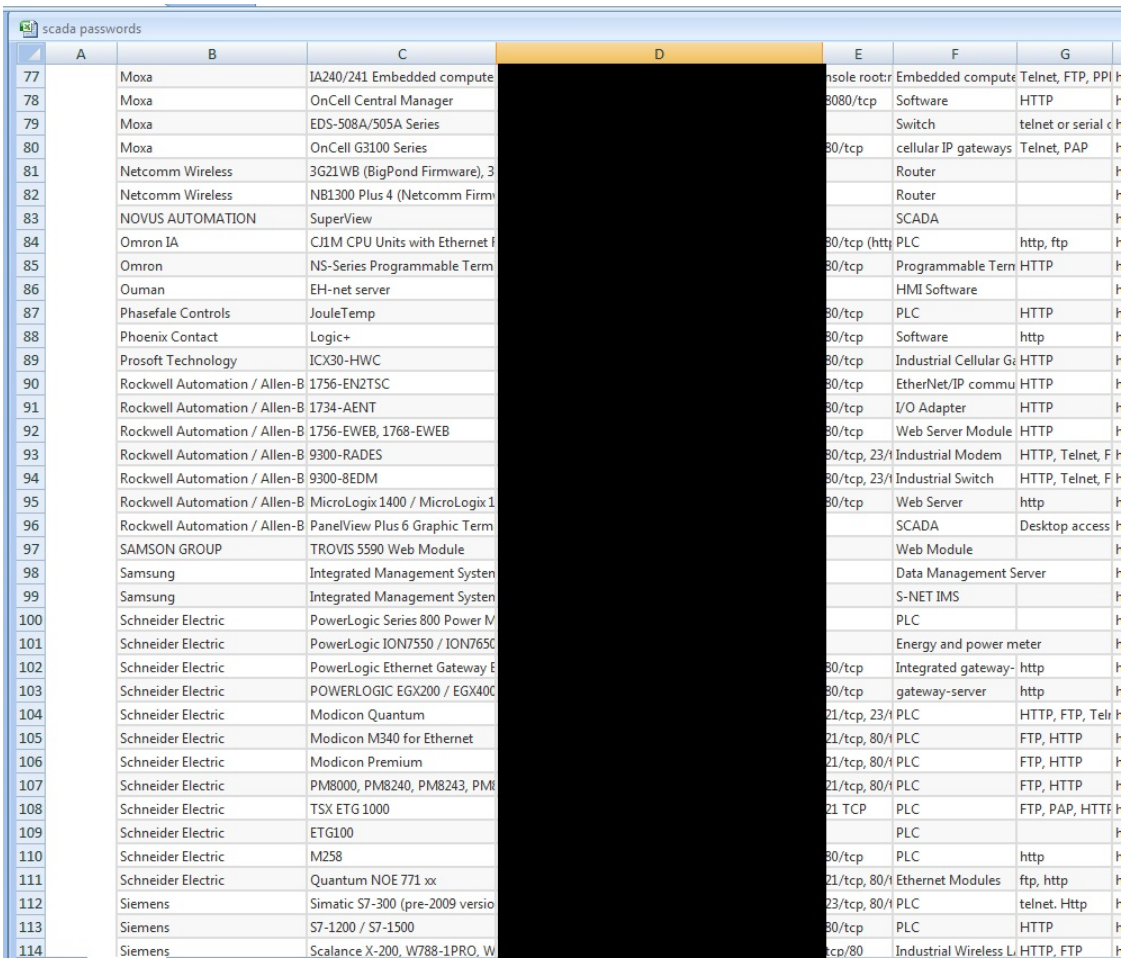
> "…we are gonna pivot from the ship tracker sites into myship.com. … You can go in, look up any ship you want, find out who the crew are, find out who their ship mates are, and then social engineer the hell out of it. … And then pivot from there with whatever it is you do …"

This kind of social engineering method was typically used in cyber-physical attacks; attackers could either gain the trust of the target employee and obtain their credentials to access the industrial system, or they could gather the victims' private information and coerce the employee to become an insider and conspire the cyber-attack together.

Other hackers could attempt to gain access to the industrial systems by using default credentials retrieved online. Default usernames and passwords were primarily found in publicly accessible user manuals of industrial devices: "After installation, log in

with the user name ‘admin’ and the password ‘admin’” (User manual F). Compiled list of default credentials of industrial devices, such as the spreadsheet shared by *User G* in *Figure 2.2*, can also be found. This information can pose risk to institutions still using default usernames and passwords for commanding and controlling their ICSs.

.


scada passwords

	A	B	C	D	E	F	G
77		Moxa	IA240/241 Embedded compute	[redacted]	nsole root:r	Embedded compute	Telnet, FTP, PPI
78		Moxa	OnCell Central Manager		8080/tcp	Software	HTTP
79		Moxa	EDS-508A/505A Series			Switch	telnet or serial c
80		Moxa	OnCell G3100 Series		80/tcp	cellular IP gateways	Telnet, PAP
81		Netcomm Wireless	3G21WB (BigPond Firmware), 3			Router	
82		Netcomm Wireless	NB1300 Plus 4 (Netcomm Firm			Router	
83		NOVUS AUTOMATION	SuperView			SCADA	
84		Omron IA	CJ1M CPU Units with Ethernet I		80/tcp (htt	PLC	http, ftp
85		Omron	NS-Series Programmable Term		80/tcp	Programmable Tern	HTTP
86		Ouman	EH-net server			HMI Software	
87		Phasefale Controls	JouleTemp		80/tcp	PLC	HTTP
88		Phoenix Contact	Logic+		80/tcp	Software	http
89		Prosoft Technology	ICX30-HWC		80/tcp	Industrial Cellular Ga	HTTP
90		Rockwell Automation / Allen-B	1756-EN2TSC		80/tcp	EtherNet/IP commu	HTTP
91		Rockwell Automation / Allen-B	1734-AENT		80/tcp	I/O Adapter	HTTP
92		Rockwell Automation / Allen-B	1756-EWEB, 1768-EWEB		80/tcp	Web Server Module	HTTP
93		Rockwell Automation / Allen-B	9300-RADES		80/tcp, 23/t	Industrial Modem	HTTP, Telnet, F
94		Rockwell Automation / Allen-B	9300-8EDM		80/tcp, 23/t	Industrial Switch	HTTP, Telnet, F
95		Rockwell Automation / Allen-B	MicroLogix 1400 / MicroLogix 1		80/tcp	Web Server	http
96		Rockwell Automation / Allen-B	PanelView Plus 6 Graphic Term			SCADA	Desktop access
97		SAMSON GROUP	TROVIS 5590 Web Module			Web Module	
98		Samsung	Integrated Management Systen			Data Management Server	
99		Samsung	Integrated Management Systen			S-NET IMS	
100		Schneider Electric	PowerLogic Series 800 Power M			PLC	
101		Schneider Electric	PowerLogic ION7550 / ION765(			Energy and power meter	
102		Schneider Electric	PowerLogic Ethernet Gateway E		80/tcp	Integrated gateway-	http
103		Schneider Electric	POWERLOGIC EGX200 / EGX40(		80/tcp	gateway-server	http
104		Schneider Electric	Modicon Quantum		21/tcp, 23/t	PLC	HTTP, FTP, Tel
105		Schneider Electric	Modicon M340 for Ethernet		21/tcp, 80/t	PLC	FTP, HTTP
106		Schneider Electric	Modicon Premium		21/tcp, 80/t	PLC	FTP, HTTP
107		Schneider Electric	PM8000, PM8240, PM8243, PM		21/tcp, 80/t	PLC	FTP, HTTP
108		Schneider Electric	TSX ETG 1000		21 TCP	PLC	FTP, PAP, HTTP
109		Schneider Electric	ETG100			PLC	
110		Schneider Electric	M258		80/tcp	PLC	http
111		Schneider Electric	Quantum NOE 771 xx		21/tcp, 80/t	Ethernet Modules	ftp, http
112		Siemens	Simatic S7-300 (pre-2009 versio		23/tcp, 80/t	PLC	telnet. Http
113		Siemens	S7-1200 / S7-1500		80/tcp	PLC	HTTP
114		Siemens	Scalance X-200, W788-1PRO, W		cp/80	Industrial Wireless L	HTTP, FTP

Figure 2.2. Partial list of default credentials shared by User G from personal Blog

Hacking and Reconnaissance Tools

Not surprisingly, educational tools and software programs designed for ethical hackers were commonly shared on open-source websites. Some platforms and websites may post disclaimers and terms of use to ensure the legitimate use of these hacking and reconnaissance tools. For example, *platform H* in its terms of use stated that:

> "… [y]our use of the Website and Service must not violate any applicable laws, including … sanction laws, or other laws in your jurisdiction. You are responsible for making sure that your use of the service is in compliance with laws and any applicable regulations."

Despite providing safeguards for resources designed for ethnical hacking, platforms and website owners often depend on the users to abide these policies and guidelines.

Simulation software of industrial devices were able to provide individuals opportunities to understand the algorithms and operational commands ensuring the functioning of the systems. *Website I* highlighted the educational version of a ladder logic[12] programming software used to operate industrial systems:

> "… [a] complete (not crippled version) software package for learning about PLC programming and for users to evaluate the power of Ladder Logic or Ladder+BASIC software programming. … The program files you created using the Educational version are identical to that of the Production version so you can write and test your entire program to make sure that it can do what you want …"

According to this description, the PLC programs written in this free software are identical and applicable to PLC systems in the real world.

Other tools such as OSINT reconnaissance programs or penetration testing software provided to professional cybersecurity researchers could be downloaded by malicious attackers. *User J* shared a list of useful resources professional hackers could use when conducting vulnerability assessments, including tools capable of "bruteforce the password used by S7[13] instances from a PCAP using a dictionary."

Research on the open-source scanner Shodan was able to provide reconnaissance information of internet-connected industrial devices. Results from Shodan could give general information such as the quantity of industrial devices and controllers identified on the internet, the locations of the devices, as well as top service manufacturers of the device. *Figure 2.3* displays the search result for Allen-Bradley devices discovered by Shodan. Manufactured and sold by one of the largest industrial automation providers, Allen-Bradley branded devices can be commonly found in various

[12] Ladder logic refers to the programming language commonly used to program and control Programmable Logic Controllers (PLCs). For more information, see Rehg & Sartori (2010).

[13] S7 is referred to the Siemens S7 PLC product series.

CI facilities across the world (Plant Automation Technology, 2022; Rockwell Automation, 2022).

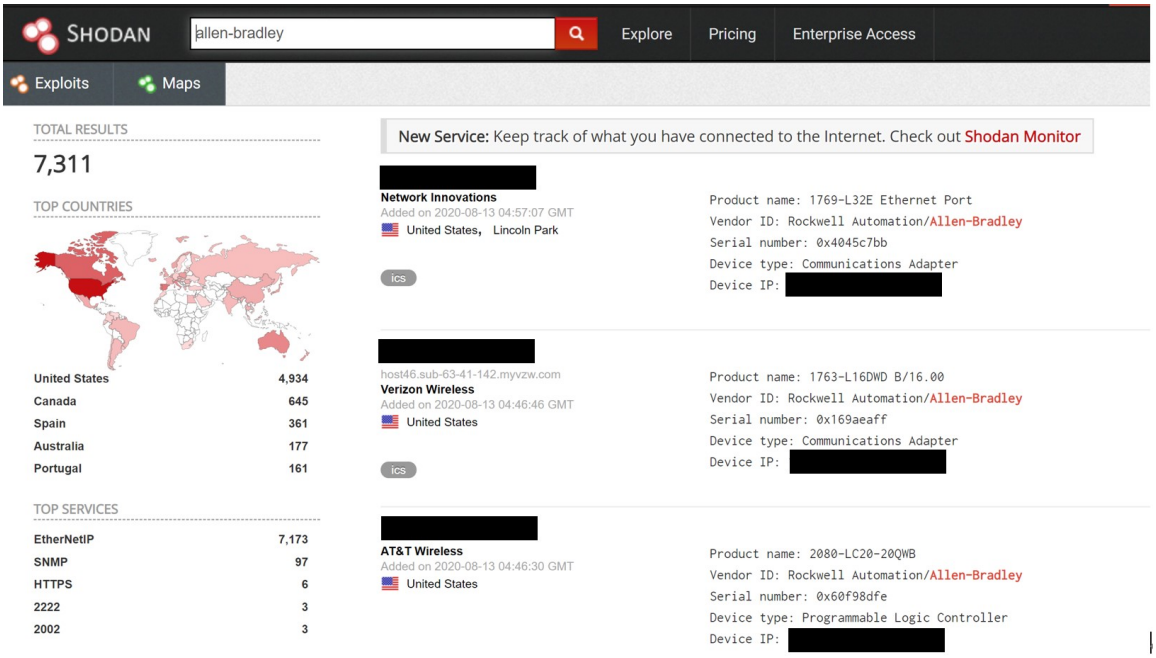


Figure 2.3. Shodan search result for Allen-Bradley devices

Detailed data on these devices are available for further inspection on Shodan. *Figure 2.4* illustrates Shodan's ability to identify specific industrial devices connected to the internet. These types of information are helpful for both professional researchers and cyberterrorists in the early stages of attack to determine the ideal target and attack strategies.

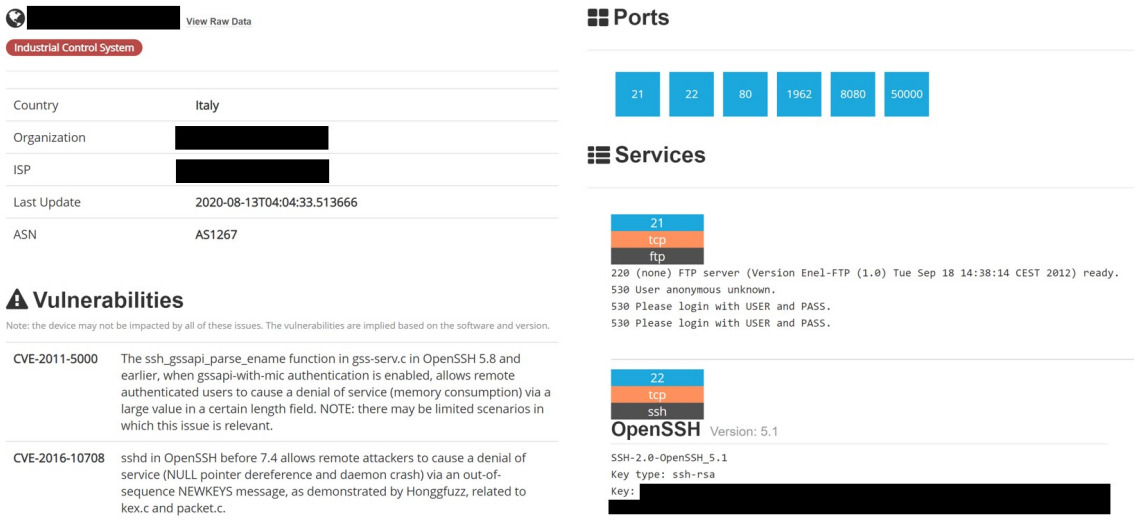


Figure 2.4. Detailed information of an industrial PLC device in Italy

The textual details of this specific logic controller displayed in *Figure 2.4* provided information about the IP address and the organization owning the device, open ports on the device, as well as services operating on each of the ports. Shodan also compiled a list of reported vulnerabilities one could potentially exploit against the device if the issues were unpatched by its vendor.

Demonstration Videos

Videos demonstrating successful intrusion into industrial systems are uploaded by cybersecurity companies or individuals interested in hacking and computer programming. Among all of the uploaded videos, users often did not provide any verbal explanations to either the hacking process or the exploit; rather, these videos were mostly silent with snippets of the coding inputs and outputs presented throughout. Although brief descriptions of the content and types of the attack against industrial devices were provided, most of the users did not provide further information with regards to where and how to obtain a copy of the zero-day exploit or source codes of the

malware. As shown in *Figure 2.5*, *User K* demonstrated a successful Denial of Service (DoS)[14] attack against a virtual PLC model using Python[15].

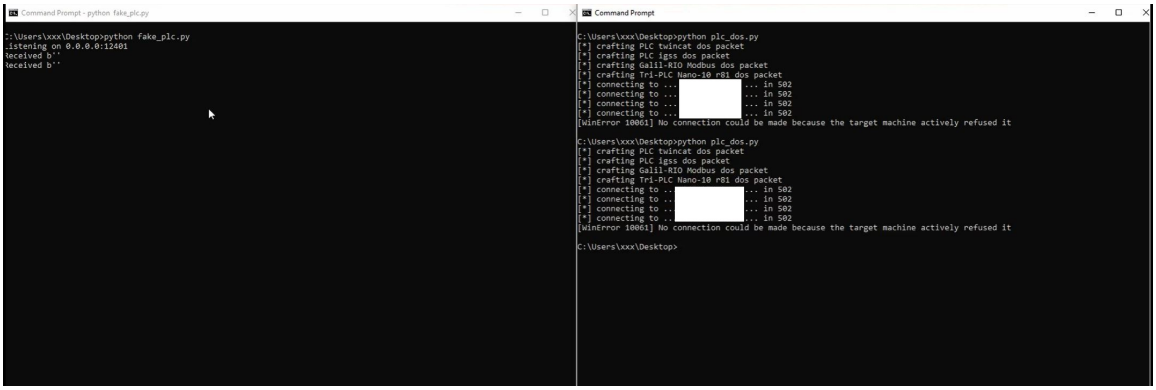


Figure 2.5. DoS attack toward virtual PLC (User K)

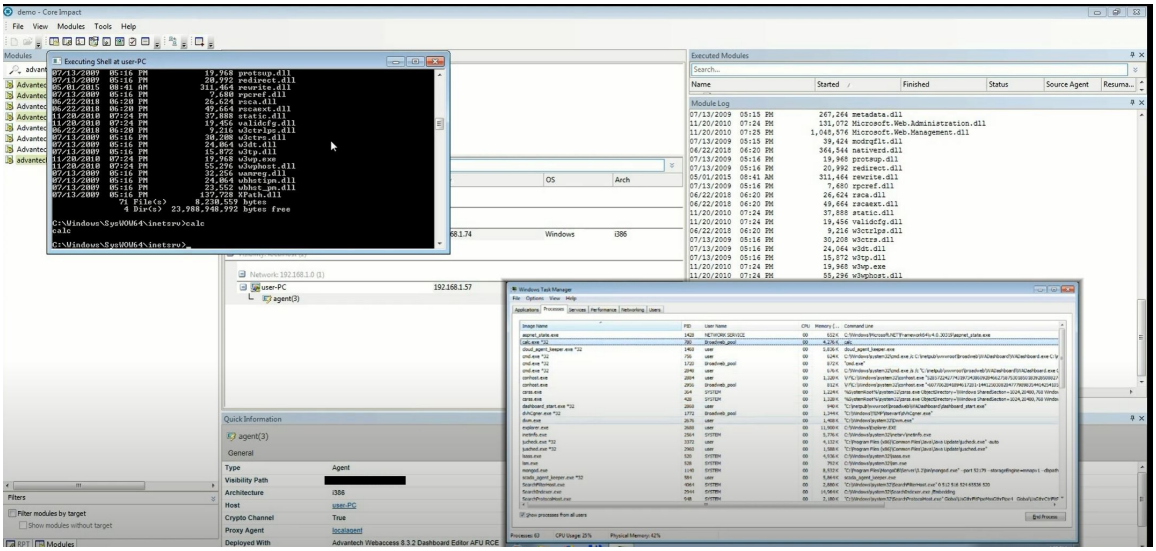


Figure 2.6. Remote code execution on Advantech WebAccess (Lab L)

Cyber-attacks targeting specific industrial devices or software were also performed and uploaded on YouTube or Vimeo by security labs as proof of vulnerability

[14] Denial of Service (DoS) attack is a type of cyber-attack which networks or systems are flooded with traffic and requests, resulting in network disruptions and systems inaccessible to their intended users (Trend Micro, 2022).

[15] Python is a programming language commonly used by programmers (Python, 2022).

assessment results for their clients or cohorts. To illustrate, *Lab L* uploaded a YouTube video demonstrating how Advantech WebAccess[16] Version 8.3.2 can be hacked and remotely controlled by hackers (*Figure 2.6*).

2.2.2. Proof-of-Concept Codes

The second major type of data retrievable from surface web platforms are proof-of-concept (PoC) codes. The idea of sharing these PoC codes can be traced back to some early projects proposed by cybersecurity personnel in the past decade. Most significantly, Project Basecamp, presented in a cybersecurity conference in 2012 has proposed the idea of sharing proof-of-concept codes so the industry would become aware of the potential vulnerabilities of in-the-field devices (Peterson, 2012). In the presentation, the event lead Peterson explained the team's motive for sharing the PoC codes:

> "… Eric Butler a few years later came up with this Firefox plugin called Firesheep now made it possible for anyone sitting in a coffee shop who could use a browser to hijack a session and guess what, it got people's attention. Even though everyone knew before, now that everyone could do it. Things change very quickly and those vendors that had done nothing about it very quickly added the capability to … solve this problem. … maybe we need a firesheep moment in PLC security." (S4 Events, 2016)

The initial goal for sharing PoC codes was to allow security researchers to perform and understand the exploits and eventually develop and enforce better mitigation strategies to protect industrial devices. With this intention, the proof-of-concept exploits can often be discovered on websites such as Exploit Database (EDB), GitHub, or attached within official advisories published by security companies or government websites.

For example, *User M* released a version of buffer overflow[17] exploit on Exploit Database, noting that the successful launch of the code would crash the Modbus server programmable logic controllers. The details of the affected software, the tested version of the device, as well as the operating system used to perform the exploit were provided.

---

[16] The Advantech WebAccess software allows industrial companies to connect the devices with internet and provides remote access to the ICS (Advantech, 2022).

[17] A buffer overflow occurs when the volume of data overflows or exceeds the storage capacity of the memory in the software, forcing the software to overwrite the excess data to its adjacent storage locations and ultimately changing the execution and functioning of the program (Imperva, 2021).

User M also included a brief instruction on the steps required to run and reproduce the exploit. An excerpt of the PoC exploit is shown in *Figure 2.7*.

```
# msfvenom -p generic/tight_loop --platform windows_86 -f perl -e x86/shikata_ga_nai
# print /x &loop
# $1 = 0x555555558030

open(code, ">exploit.msw");
binmode(code);
$loop =
"\xbb\x3c\x56\x3b\x1e\xd9\xc4\xd9\x74\x24\xf4\x58\x2b\xc9" .
"\xb1\x01\x31\x58\x14\x83\xc0\x04\x03\x58\x10\xde\xa3\xd0" .
"\xe0";

print code $loop;
close(code);
```

Figure 2.7. Partial PoC code of Modbus buffer overflow (User M)

Critical exploits of devices commonly installed in the industry could also be discovered in vulnerability reports. *Figure 2.8* below illustrates a partial PoC exploit capable of inducing a DoS attack on Schneider Electric's Modicon PLCs[18].

```
    res = getPLCInfo(s)

    # first write system bits and blocks
    mbtcp_fnc = "\x5a"
    session   = "\x00"
    umas_fnc  = "\x23"
    crc = struct.unpack("<I", res[14:18])[0]
    shifted_crc = crc << 1
    crc = struct.pack("<I", shifted_crc)
    data = "01011000800000000c080f3a0a70000200000".decode('he
x')
    umas = "%s%s%s%s%s" % (mbtcp_fnc, session, umas_fnc, crc,
data)
    send_message(s, umas=umas)

    # get plc info
    getPLCInfo(s)

    # second write system bits and blocks
```

Figure 2.8. PoC exploit against Schneider Modicon PLC (Report N)

[18] These devices are programmable logic controllers (PLCs) manufactured by Schneider Electric in their Modicon product series. See Schneider Electric (2022).

Different from the contents posted by personal blogs or programmers, reports published by cyber threat analysts sometimes included detailed analysis of unique features and processes of the exploit. *Report N* stated that the malware operated in a process which "[i]n the non-recoverable fault state, the CPU has entered an error mode where all remote communications have been stopped, process logic stops execution, and the device requires a physical power cycle to regain functionality." Accompanying the PoC exploits, detailed analysis discussed in security reports could provide further information to both professional researchers and hackers.

2.2.3. Educational Materials

This theme involved different kinds of open-access resources that were able to directly teach people hacking-related knowledge. Although the frequency of materials related to the theme (13.6%) was relatively lower than the other two main themes identified in the current study, these educational resources provided attackers important insight on how to perform cyber-attacks against computer systems and CI facilities. Two types of materials were identified from the current sample: (1) "how to" tutorials, and (2) training courses.

"How to" Tutorials

The overwhelming majority of the data in this category were found in personal blogs or YouTube videos teaching viewers the steps needed to hack into SCADA systems and to develop exploits. This result suggested that attackers were able to find materials providing detailed information with regards to cyber-attacks against critical infrastructures in the open domain.

A small number of blogs detailed the steps a person would need to recreate a malware or improvise an existing exploit for a cyber-attack. For instance, *researcher O* posted a blog discussing what hackers should do to create an exploit similar to the Stuxnet exploit and deploy it to Schneider Modicon PLCs:

> "… Our breakpoint on MyAsmArmStream is reached, and if we follow the arguments in the stack, we can see that the first argument contains a pointer to our ASM source code. Now we will execute the function MyAsmArmStream and see what happens. … So, we disassemble the byte code at the offset of the label DebugLabel2 (offset bytecode+0X90) to ensure that we retrieve the ASM source code. We have recovered our

> original ASM source code, so MyAsmArmStream is in charge of the compiled processing. Therefore if we hook into this function, we will be able to inject our own "malicious" code…"

While tutorial blogs tend to include both textual and visual explanations to help readers understand the hacking processes, some of the steps were still omitted and not described in these instructional blogs. Slightly different from these tutorials, *User P* taught others how to write buffer overflow exploits with shellcode by uploading videos on YouTube:

> "…When you use CAT without parameters, it simply redirects its standard input to the standard output. See like here, you type something in, and it gets reflected out. Now you can chain programs together on one line, for example with semicolon, so we can first print the output of the exploit, and afterwards CAT is executed, so we can enter new input, and if we group that now with some brackets, and redirect their combined output into the stack level, the exploit will first run and execute a shell, and then CAT will take over and we can simply relay input via the CAT to the shell. … It works! We have an ugly shell, and we can verify our identity with "whoami", or id. So now we escalated privileges to root…"

In their tutorial, *User P* discussed how individuals could use non-functioning source codes and modify them to a root shell[19] and obtain root access[20] to a target system. In addition to the instructions provided by *User P*, extra source codes and links to programs were also shared in the description section, allowing viewers to obtain copies of the code and practice writing exploits on their own.

Training Courses

Advertisements for courses teaching individuals coding and ethical hacking were offered on open-source websites. Typically, people would need to provide some personal information in order to register for the courses. The majority of courses only required individuals to provide their full name and a valid email address to subscribe to the course packages. Some of the ethical hacking training courses required more information, including the applicant's company names, valid work or university emails, and home addresses to ensure the training was done for legitimate purposes.

---

[19] Root shell is the user interface for accessing into an operating system (e.g., a Linux system) using the top-level administrative privilege (IBM, 2022a; TechTerms, 2017).

[20] Root access would grant one unlimited access into an operating system with administrative privilege (IBM 2022b; TechTerms, 2017).

For both online training and in-person training courses, many of them are offered only for a limited period of time. These courses would take an individual approximately a week to complete, depending on the schedule and the objectives of the course. For example, one course offered by *security researcher Q* was designed to be a four-day training course held during a virtual Black Hat event. Within this four-day training schedule, *Q* stated that the course was planned to:

> "…teach hands-on penetration testing techniques … [that] will apply directly to systems such as the Smart Grid, PLCs, RTUs, smart meters, building manufacturing, …, SCADA, …, and even IoT. … The course exercises will be performed on a mixture of real world and simulated devices to give students the most realistic experience as possible in a portable classroom setting…"

In some cases, some of the courses not only taught individuals how to conduct penetration testing against industrial systems, but also offered an ethical hacker certification exam upon completion of the course package. *Website R* stated in its course webpage that,

> "… once you've completed … [the course] and practiced your skills in the labs, you're ready to take the certification exam. … the OSCP exam has a 24-hour time limit and consists of a hands-on penetration test in our isolated VPN network. … A passing exam grade will declare you an Offensive Security Certified Professional (OSCP) … [that] is well-known, respected, and required for many top cybersecurity positions…"

These courses indicated that the training sessions were mainly designed for technology professionals or individuals planning to obtain an ethical hacker certification in order to apply for jobs in the cybersecurity field. Upon learning the skills and techniques required for performing penetration testing on different systems, motivated hackers may seek additional resources to learn, differentially associate, and imitate advanced hacking techniques performed by malicious actors. Individuals may then attempt to illicitly apply these skills and exploit devices used in critical infrastructure.

Chapter 3. Darknet Forum Analysis

In the following sections and sub-sections, darknet forum data were collected and analyzed to address the proposed research questions. While previous studies have discussed cybercriminals' use of hacker forums and the darknet for data gathering and social interaction purposes, it is yet unclear how information circulated in the darknet forum could aid malicious actors motivated to attack CI facilities. Thus, darknet discussion forum data was collected and analyzed in this part of the analysis.

3.1. Methodology

3.1.1. Data Sources

The dataset compiled for this section of the research was gathered from keyword queries returned from one darknet discussion forum named Dread. Being referred as the darknet version of Reddit, Dread forum is the largest open-source English discussion platform containing rich conversational threads related to a variety of subjects including cybersecurity and hacking (Admin, 2021; dnstats, n.d.; Darknetlive, n.d.). Further, Dread is also a forum located only in the hidden network, requiring individuals to install Tor browsers to establish connection to the platform (Admin, 2021). When accessing the forum using Tor, the browser will route internet traffic through three nodes[21], ensuring user identities remained hidden during the transmission of internet requests and messages (Australian Cyber Security Centre, 2021; Electronic Frontier Foundation, n.d.). These three nodes provided additional layers of protection, as law enforcement agencies or internet service providers cannot perform traffic analysis to determine the origins of the messages sent by their users (Tor, n.d.). For greater security, the browser will regularly select routing paths with three random nodes every 10 minutes. The application of these security measures rendered privacy-oriented platforms and darknet contents difficult to monitor by governmental institutions or platform staff, thus providing more opportunities for malicious individuals to openly share illegal hacking contents (Tor, 2021).

[21] A node is referred to as a router, website, or server used as a connection point inside a network capable of relaying and transmitting data (IBM Cloud Education, 2021).

Other search engines operable in the darknet, including DuckDuckGo, were not included in the current study to ensure that only darknet discussion results were collected. When applying keyword searches to these search engines, only indexed open-source information can be returned and displayed (Kaspersky, 2022a). Further, these standardized search engines are unable to capture or categorize unindexed and hidden contents shared on *.onion* websites within the darknet (Leon, 2020). As this part of the study is to discover the types of critical infrastructure and cybersecurity related data shared and discussed specifically in the darknet, Dread would be considered as the most appropriate data source for my analysis.

3.1.2. Data Collection

A purposive sampling technique was employed for this portion of the study. The initial plan was to apply the same keyword queries relevant to industrial control systems and critical infrastructure facilities searched within the surface web platforms (see *Table 2.1*) to the darknet forums. However, as the search function in Dread was designed to only allow simple searches including words (e.g., infrastructure) and short phrases (e.g., “critical infrastructure”), the list of keywords were modified. In order to narrow down search results, general terms and keywords (e.g., chemical) were modified and more specific phrases relevant to the objectives of the current study (e.g., chemical sector) were created for the search. An additional keyword commonly brought up by Dread users, OSINT, was also deductively discovered and added into the list of keywords in the data collection phase. *Table A.1* in *Appendix A* presents the entire list of keywords and keyword phrases searched in the Dread forum. When using the search tool, the default search setting was applied; posts with titles and comments containing keywords and phrases were extracted for analysis. A total of 2,879 threads and 33,914 comments were returned and collected from Dread.

3.1.3. Data Analysis

Upon obtaining the list of search results, criterion sampling was applied to exclude any posts and comments that were outside the scope of the current study. As Dread was developed and launched in 2018 and all information within the forum were considered recent and up-to-date, threads published since the launching of the forum were included for analysis (dnstats, n.d.). The date of published content ranged between

February 15th, 2018[22] to May 11th, 2022 (last day of data collection). In order to be included in the study, search results must provide readers with sufficient information or knowledge on the topic of critical infrastructure or hacking. To demonstrate, posts sharing brief reports on the occurrences of cybersecurity breaches were excluded. Other contents, such as posts and comments containing discussions or communications about hacking strategies and tools, or conversations sharing opinions on technical functioning of malware or computer and industrial facilities, were included for further analysis. Lastly, only contents written in English were included in the sample data.

All relevant results meeting the inclusion criteria were selected and copied into a Microsoft Excel spreadsheet document and then analyzed by the author. A title and general content review were conducted to record down threads matching the current research aim for further analysis. A final list of results (n=888), including 170 posts and 718 comments, were recorded for detailed coding and analysis (*Figure 3.1*). The data collected were analyzed using thematic content analysis. This was an appropriate method for the current study as the goal was to identify and report the types and common topics discussed by users within the darknet (Braun & Clarke, 2006).

[22] This date was identified by Darknetlive (n.d.) as the day when Dread was first launched.

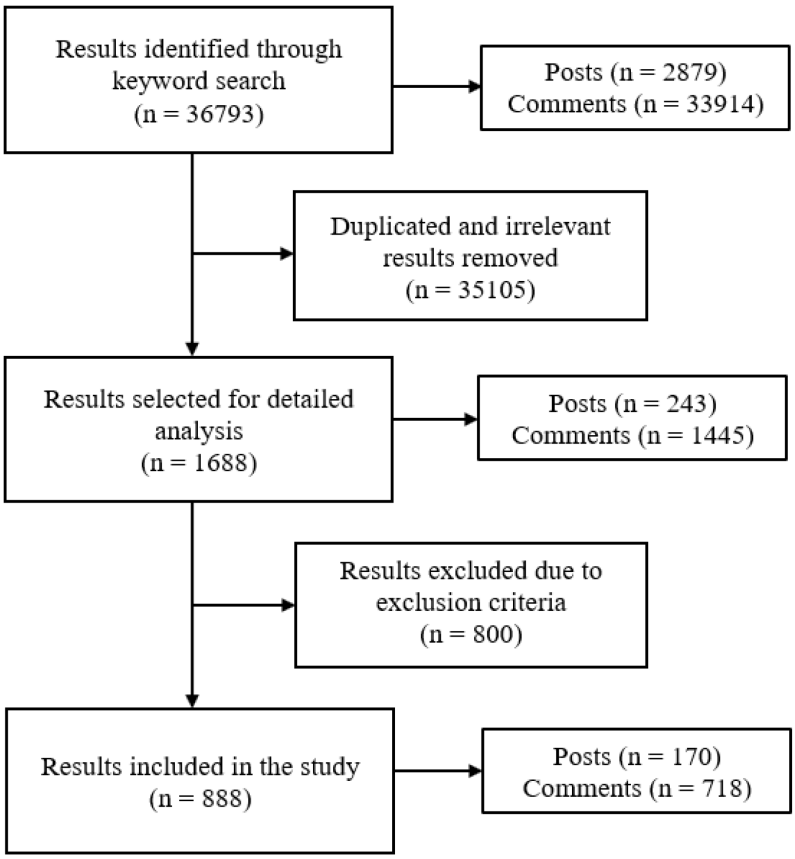


Figure 3.1. Darknet forum results selection process

Four rounds of inductive coding were conducted to allow collective exploration and generation of descriptive themes. The contents were manually read through in detail during the first two rounds of coding to filter out threads not meeting the criterion and to establish familiarization with the data. During the last two rounds of coding, detailed codes were devised and organized into themes by the author based on their patterns (Braun & Clarke, 2006). The established themes and sub-themes were then reviewed and refined in a final round of coding. All threads and comments included in the final sample were analyzed and coded within the same spreadsheet, with individuals' usernames removed to ensure confidentiality. A total of nine codes emerged from the final sample and were later organized into four major themes.

3.2. Results

The results from the data are described and discussed in this section. Four overarching themes were constructed after multiple rounds of coding: "Indirect

reconnaissance data," "Question inquiries," "Hacking-as-a-service," and "Educational materials." Within the primary theme, "Indirect reconnaissance data," three sub-themes were identified. Another three sub-themes were also categorized under the theme "Hacking-as-a-service", while two sub-themes were reflected in the theme related to "Educational materials." *Table 3.2* below demonstrates the breakdown of themes, sub-themes, and frequency counts emerged from the darknet forum dataset. Analysis of the data in this part of the study demonstrated rich resources darknet discussion forums can provide to malicious individuals, aiding them to learn and discuss topics of hacking and cybersecurity relevant to critical infrastructure sectors (Basheer & Alkhatib, 2021; Holt et al., 2012; Leukfeldt et al., 2017; Shakarian et al., 2016). The findings and illustrative quotes are described below.

Table 3.1. Darknet platforms results: themes, sub-themes, and frequencies

Theme	Sub-themes	Frequency		Total (%)
		Posts	Comments	
Indirect reconnaissance data	Operational Security	24	392	416 (46.8%)
	Hacking tools and advice	13	104	117 (13.2%)
	Threat-related information	19	88	107 (12.0%)
Question inquiries		62	41	103 (11.6%)
Hacking-as-a-service	Potential interest	2	47	49 (5.5%)
	Freelancers for hire	19	13	32 (3.6%)
	Recruitment	17	5	22 (2.5%)
Educational materials	"How to" tutorials	13	19	32 (3.6%)
	Training courses	1	9	10 (1.1%)
		170	718	888 (100%)

3.2.1. Indirect Reconnaissance Data

The majority of the content (72.0%) discovered within the final sample composed of information indirectly helping hackers to prepare and plan malicious cyber-attacks (n=640). While the information found are indirect and general in their nature, accessibility of this information could prepare cybercriminals to determine optimal hacking plans, find ideal tools, as well as to remain untraceable and anonymous during the hacking process. Three types of data were commonly discussed within the darknet community: (1) Operational Security; (2) hacking tools and advice; and (3) threat-related information.

Operational Security

When sharing information about cybersecurity and hacking, posts and comments in the forum often discussed the importance of anonymity through proper Operational Security (OPSEC) process and computer set ups. OPSEC was a big topic circulating between darknet users, and relevant subdreads[23] were set up to discuss the subject. In one of the subdreads, the moderators encouraged any discussions focusing on "this community's OpSec … around Dark Net (DN) activity, [and] all members of this sub are encouraged to think about, discuss, and share ideas relating to OpSec that extend beyond the bounds of the DN" (Subdread A). Originally applied by industrial, military, and critical infrastructure sectors, the same data protection process to manage sensitive information was also adopted by darknet users to ensure the protection of their privacy and online activities (Computer Security Resource Center, n.d.; Zhang, 2020).

For darknet users, the necessity of high levels of OPSEC was largely in the context of concerns about their illegal online behavior identifiable by law enforcement agencies. Users are often alerted by the possibility of governmental institutions collecting incriminating evidence against their involvement in illicit activities.

> "If the FBI secretly gained control of your attack infrastructure in a bid to try to locate and arrest you for hacking into multiple banks and donating stolen money to charities, what's the base OPSEC requirements you would have needed to have a pretty good chance of not going to prison?" (User 1)

> "… To be fair I personally think that the governments have enough resources to decrypt anything they want if they like. I think they are infiltrating markets as we speak and waiting for the right moment to engage their attacks. That's just my bet. And if you wanna be even more safe then …" (User 2)

As can be inferred from the posts above, it is crucial for members to adopt methods capable of hiding their identities and evade government surveillance. Safe OPSEC set ups are considered essential for users to continue browsing legal materials and engaging in illicit behavior in the darknet. The strong need to stay anonymous online also led to the creation of posts and comments proposing OPSEC set ups and instructions to other users about ways to stay anonymous. For example, one *User 3*

[23] Subdread is a type of small community residing within the Dread forum where a specific subject or a scope of subjects will be discussed and categorized under the subdread.

recommended some steps to ensure the disconnection between one's online and physical identities:

> "…All devices which are not tied to you're real identity and all devices used for illegal activity must be completely clean. The best method is to just buy laptops, cell phones and prepaid plans online using prepaid gift cards or even crypto (on some sites) and have the phones shipped to a clean residence. Of course use solid digital opsec. … NEVER ACCESS ANYTHING WHICH CAN BE CONNECTED TO YOUR REAL IDENTITY FROM A CLEAN DEVICE. … Don't use [social media]. If you do, don't put up any pictures of yourself or refer to yourself using you're real name. I've seen too many people get busted for shit because LE was able to use social media for some investigative purpose or another…"

In addition to providing recommendations on OPSEC methods to stay anonymous, posters would share their thoughts about the best operating systems and software for hacking and maintaining anonymity as well. After personally using or experiencing certain software, users may provide feedbacks on the effectiveness of these tools and systems. *User 4*, in one of their posts, recommended a series of operating systems useful for both hacking and keeping good OPSEC:

> "Pentesting/hacking [:] Kali Linux or Parrot security OS. Why: They come pre-loaded with lots of hacking tools, No-bullshit setup process (mostly) … Daily Driver (Medium/advanced) [:] Arch Linux. Why: Not-too-complicated setup if you're used to Linux. Pacman is great … Staying Anonymous [:] Tails. Why: All internet traffic routed through TOR, Automatically spoofs your MAC address, Internet killswitch for if TOR disconnects. High Security…"

Differed from contents posted by *User 4*, some posters may share information about unsecured software and operating systems. For instance, *User 5* discussed how the Ubuntu[24] systems should be avoided if one wants to stay undetected: "If you are concerned with privacy, you should not use Ubuntu as it has partnered up with Amazon and is financed by it." Certain programs funded by business corporations may be avoided by darknet users due to concerns about their identities being compromised. Software and systems where funding companies had a history of cooperation with law enforcement organizations, in particular, would not be recommended by members as the

[24] Ubuntu is an open-source operating system commonly used by program developers. The system claimed to provide more privacy, security, and tools useful for both IT professionals and beginners (TechTarget Contributor, 2009; Ubuntu, 2022).

likelihood of their personal information being provided to government agencies increases.

In addition to the effort individuals take to heighten their OPSEC levels prior to any hacking activities, useful anti-forensics strategies and tools were also found in the forum. As stated by many users, the installation of anti-forensic software was to prevent the gathering and analyzing of any self-incriminating digital evidence stored on the computers. Methods such as full-disk encryptions were often preferred by posters. For instance, *User 6* in their thread explained how disk encryptions could securely hide and lock all data stored in the computers, therefore affecting law enforcement's investigation processes:

> "Strong full disk encryption with a strong password cannot be broken as far as we know. So, never leave your computer on when you aren't in front of it, and when you are in front of it, all you need to do is hit the power button (or in Tails, pull the USB stick out if you need to be really fast). … That being said, always using encryption is far better because it works, with minimal effort."

Hacking Tools and Advice

The Dread forum and subdreads were observed as useful platforms for posters to exchange hacking tools and share thoughts on basic hacking skills. Experienced users often provided suggestions to script kiddies or aspiring hackers on the types of programs or skillsets necessary for cyber-attacks. These recommendations or guidelines were created based off of users' own hacking experiences:

> "…Learn how to program. A good one to start with, if you are a total n00b is Python. It's syntax is easy to learn, and it's somewhat easy to debug. The goal is really to get a firm grip on programming logic, which will help you in the vast majority of other programming languages. … Once you are confortable with those, then move to a language that's lower level, perhaps C or C++ (personal preference for C here, but to each his own) … SQL/MySQL is almost a must. Many things these days are database driven. These are to of the most popular languages to interact with databases, and understanding how they work will help you gain access to areas you aren't supposed to. Particularly for hacking websites." (User 7)

As described by *User 7*, it is important for low-skilled hackers to understand programming languages such as Python, C++, or SQL/MySQL if they want to start hacking.

Differing from users providing guidelines about skillsets necessary for individuals to learn prior to conducting cyber-attacks, some members shared programming and ethical hacking resources to other members. Posters such as *User 8* offered lists and copies of programming and hacking-related books:

> "… Hacking Exposed Linux Security Secrets And Solutions, 3rd Edition.pdf … Cisco Routers For The Desperate 2nd Edition Book.pdf … Optimized C++.pdf … MYSQL in a Nutshell (In a Nutshell (O'Reilly).pdf … The Python Book The ultimate guide to coding with Python.pdf … Cisco IOS Cookbook, 2nd Edition (Cookbooks (O'Reilly).pdf … Pen_Testing_and_Ethical_Hacking_Study_Guide.pdf …"

These textbooks and tools may be shared between hackers to aid in their understanding of computer networks, system vulnerabilities, as well as functions of different hacking tools. Operational manuals and guides on industrial devices commonly used in critical infrastructure devices, including Cisco operating systems named IOS (Cisco 2022a), were also available in darknet forums. While these books and resources may not provide direct information about cyber-attacks against CI, they may still be useful for hackers to acquire knowledge needed for conducting future attacks.

Comments endorsing hacking tools were also frequently found in the forum. For instance, *User 9* shared a list of hacking and penetration testing tools, including "Flutter/Dark reverse engineering tool' and tools for 'quickly gathering information from Shodan.io." In cases where users attached links for others to access the tools, the majority of the links were from open-source surface websites such as GitHub.

Threat-related Information

Information about exploits and vulnerabilities discoverable on industrial devices were identified in darknet forums. Noticeably, some surface web content and cybersecurity analysis were shared by members in the darknet forums, such as the post shared by *User 10*:

> "Cisco has released software updates to address four security vulnerabilities in its software that could be weaponized by malicious actors to take control of affected systems. ... An attacker could exploit this vulnerability by sending a crafted HTTP POST request to the NX-API of an affected device, successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system…"

Extracting information from the descriptions and analyses in these reports, hackers might identify exploitable targets and plan cyber-attacks.

Among the plethora of posts providing threat-related information, potential executable attack strategies were commonly disclosed and discussed between users. When discussing effective strategies to obtain access into critical infrastructure facilities or organizations, methods such as social engineering or phishing were mentioned:

> "go spear phishing for a specific employee at the company/government you want and send them a malicious Exel and if they click it and turn macro's on you have privilege escalation and possibly full access.. do what you want after." (User 11)

> "i'm more into PLCs and industrial networks + modbus. you could probably spearphish officials, take over their account and spearphish from their accounts to eventually get to people on washington." (User 12)

While described in varying levels of detail, similar cyber-attack ideas shared between users might be useful for malicious actors in the reconnaissance stage of the cyber kill-chain to plan and conduct cyber-attacks accordingly.

Occasionally, some posters may sell OSINT packages to motivated hackers in the forums. Personal information, such as data collected and sold by *User 13*, could also aid hackers during the reconnaissance stage of the cyber kill-chain:

> "…personal social media etc, publication creds, personal info, family/friends/contacts, phone number w/pins, article history, cross reports regarding leaks and employer). … Similar projects re: corporations available but currently in use. Will be offered when available to share. Also small unstable nation states."

Although data may not directly relate to industrial devices or CI facilities, collections of staff information remained valuable for hackers to identify vulnerable employees working in the desired target institutions. By planning and applying appropriate social engineering methods to these selected victims, malicious actors may obtain access to CI facilities and to proceed to later stages of the cyber kill-chain.

3.2.2. Question Inquiries

This theme demonstrates how discussion forums in the darknet provided users, including malicious attackers, opportunities to actively seek advice relevant to cyber-

attacks, hacking, and OPSEC. In the forum, posters frequently asked questions or inquired about information helpful for planning or learning cyber-attack skills against government or infrastructure facilities. Malicious individuals with little to no skills, such as *User 14*, would seek general advice on sabotaging governmental facilities:

> "I had a question on where I should start if I wanted to hack a government agency especially (israel). Like how they did against Iran with the nuclear sabotage. Do you need lots of money and resources to complete a task like that?"

Some beginner hackers used the forums to ask questions about effective malware or exfiltration methods to compromise computer networks. *User 15*, for example, was looking for "… the best RAT[25] to get hold off and play around with for beginners … [to] nick some social logins or generally browse around someones PC to see what useful things i can find." On the other hand, *User 16* wondered "how it would be possible to move lateral in the environment and be able to compromise all the machines." On occasions where posters were unable to obtain malware codes from surface web platforms, they may ask members within the community: "if anyone was able to get the proof of concept for the new Microsoft Exchange Server attack before it was pulled from GitHub" (User 17).

Another frequently inquired category of questions was on the topic of OPSEC and computer settings. Users with little knowledge on OPSEC often asked questions about "which OS is the most secure? And what's the best setup" (User 18). Other posters may attempt to set up their OPSEC settings but were unsure about the plausibility of the set up:

> "… I feel like there are way too many moving parts, and ultimately causes more chances of leaks... would SSL/SSH will be enough protection for this set-up. … I have literally tried to spread out my data as much as possible while preventing physical and virtual leaks - is there anything that I am missing? …" (User 19)

Topics such as these illustrated the importance of anonymity among cybercriminals. As many posters are concerned about their OPSEC settings, questions relevant to privacy

[25] Remote Access Trojan (RAT) is a type of malware allowing malicious attackers to remotely obtain administrative control over a target's computer. A RAT will often run invisibly without victims' notice (Proofpoint, 2022).

and computer set ups were more likely to attract members to actively participate in the discussions.

3.2.3. Hacking-as-a-service

Threads offering hacking as a service were the third most frequently discussed topic, with 38 posts and 65 comments included. Posters spoke about and offered hacking-related service with three different roles: Individuals expressing *potential interest*, *freelancers for hire*, and people looking for *recruitment*. Users in the darknet recognized that discussion forums and subforums could serve as a platform for them to describe their needs or abilities in exchange of hacking services or money.

Potential Interest

In the comment sections of many job offering or job searching posts, darknet users often communicated on behalf of themselves to express their interest toward the original poster's contents. These contents of interest could be a certain type of service posters are offering or some projects or ideas that may have prompted the users to join. Posters may get motivated by certain hacking incidents and would express a desire to initiate cyber-attacks and seek hacking companions. One *User 20* was motivated by cyber-attacks against government facilities and stated:

> "…since "Gary" and those security firms were already hacked, we now must go after the ultimate prize: the pigs themselves. I am sure their secu[rity] sucks. I mean, even Kevin Mitnick hacked the FBI so he would know when they were closing in on him. Let's do it again!"

Despite expressing the strong inclination to find other users to engage and plan potential cyber-attacks against policing organizations together, *User 20* was unclear and did not provide additional details in the thread.

Additionally, users were also vague about their decisions to purchase services or to participate in cyber-attacks; the majority of the posts and comments only contained general information such as "I can definitely help you with this... please consult me soon" (User 21) or "interest[ed in] your service. check inbox" (User 22). Once shown potential interest on certain services or hacking projects in the comments section, most users preferred establishing private connections by reaching out to the original posters' messaging accounts.

Freelancers for Hire

In a considerable number of posts, individuals expressed a wish to obtain job offers from other users. In doing so, posters would list out their skills, the types of jobs they felt convenient or capable of working, as well as contact information for detailed inquiries or discussions about the services. One user stated in their post:

> "…I'm looking for a job that has anything to do with cybersecurity or some other related jobs. I'm an unemployed cybersecurity engineer with 12 years of experience on the field… The fields in which I feel more comfortable and fluent working are network security and information gathering (searching for people, obtaining sensitive information about someone, network infrastructure analysis and reporting... you name it...) …" (User 23)

To some extent, several job-searching subdreads addressed some basic rules for posts searching or offering for-profit services. Specifically, some subdreads required their members to provide details in their offers which "[a]ll offers must be made as clear as possible in order to avoid any conflict", and "[h]acker for hire services are not allowed" (Subdread C). Individuals whose posts violated the rules set out by the moderators would result in a removal of their posts, or a ban of their accounts.

Despite prohibiting posts offering "hackers for hire", posters continued to promote their hacking services. Wording and descriptions of some posts were carefully curated so that hacking services were discretely advertised. One poster who identified themselves as a Blackhat hacker, described themselves available for a range of work, including:

> "… freelance work, DB dumps, OSINT investigation, DDOS, spear fishing ect, message me with what you you need. … What I can do - Get you the DB/access of small sites with low budgets like colleges, local gov sites, blogs/news, scam sites, ect. …" (User 24)

Despite not directly mentioning the availability of hacking services, the poster's identified Blackhat status, as well as descriptions of their work to access and get into websites or databases, implied to members that hacking services may be offered upon client request.

Moreover, many subdreads were leniently regulated and posts promoting hacking or hacking-related services were often ignored by the moderators. For instance, several members openly stated in their posts that they were "on call for OSINT, hacking,

and programing tasks" (User 25), or they could "try to access your chosen site by means of hacking, cracking, social engineering, anythings that will gain us access to the target infrastructure" (User 26). The increasing tolerance moderators had on advertisements relevant to hacking services increased opportunities for users to promote and offer hacking to malicious actors.

In response to the pricing of the services, many posters considered the rate negotiable and tended not to list out the estimates they charged for their work. However, several users would include the amount of money they charged for certain types of services. In one of the posts, *User 27* offered investigation service "using OSINT techniques and methods. … [with] Rates $50 BTC for 5 hours. $100 BTC for 10 hours." Any users interested in collecting personal information for malicious purposes, including social engineering victims working in certain target critical infrastructure facilities, can hire people to conduct research for them.

Recruitment

Other common threads found in darknet forums were recruitment posts in which posters were looking for experienced hackers to partake in cyber-attacks or hacking organizations. The recruitment was achieved by publishing posts listing the nature of the job, the positions available, skills required, and methods of contact.

> "…We are looking for these kind of people listed below. 1- Penetration Testers/Hacker: Those on the front lines battling against corporate security teams to steal data and plant ransomware. 2- Coder: Programmers to write malicious code, integrate disparate technologies. … 5- Reverse Engineers - disassemble computer code, study it, find vulnerabilities or weakness…" (User 28)

Aside from posts looking for expert hackers, some hacking projects might also look for individuals with little to no hacking skills. For instance, *User 29* was looking for someone who can become an insider and embed malware into the company's network:

> "…This is something anyone with a desk job can do, we are looking for individuals who will be paid a small amount, to install malware on networks and even devices such as a Raspberry Pi. … Even if you know nothing about computers you could be useful to us. … We can pay somewhere between $50 and $500USD for your work as an insider.…"

Despite not acquiring programming or hacking skills, recruitment of employees working inside target companies or CI facilities could effectively cause damage toward the target's network and devices.

While a limited number of recruiters may specify budget or pay for the jobs, the majority of the job offers were not provided with standardized pay and the rates were often "negotiable" (User 30). The level of a project's complexity and one's involvement in the projects would also affect the pays. As one hiring manager from a hacking team commented under their recruitment message, the amount of money receivable "[d]epends on position, operation, and tasks given (all are included). … [assuring] you, we are transparent and split all profits fairly" (User 31).

3.2.4. Educational Materials

The last common theme that emerged from the sample data pertained to materials educating individuals knowledge related to hacking, programming, and OPSEC configurations. Two types of materials were found within the theme: *"How to" tutorials*, and *training courses*.

"How to" Tutorials

Many posters shared step-by-step guides teaching forum members how to hack into computers and systems, including industrial systems or devices commonly used in critical infrastructure. One hacker (*User 32*) shared in their thread:

> "…PLCs run on port 502. You can find open port 502s by searching port:502 on Shodan or Zoomeye. Even better is scanning port 502 with zmap on a CIDR block like zmap -p 502 166.169.0.0/16 or masscan across a large IP range such as masscan -p 502 166.141.0.0-166.141.255.255. You can also use nmap's modbus-discover, tools like plcscan, etc. Use mbtget to see the values on the PLC and throw the IP in the search browser to see if it's connected to an HMI (human machine interface). … ./mbtget -w6 40000 -a 0 -n 100 <IP address> —to change address 0's value to 40000. Changing the values on a PLC can result in severe damage to the industrial, physical process…."

This excerpt demonstrated several methods hackers could employ to obtain access and cause damages to industrial controls, including SCADA systems, Modbus systems, and Programmable Logic Controllers (PLCs).

In addition to hacking tutorials, some users would share guides about software or hardware configurations strengthening their systems' operational security. For instance, *User 33* wrote a post teaching other members how to install and configure an anti-forensics program named USBkill:

> "to install usbkill you can just copy and paste the source code from here below, into a text editor and name it usbkill.sh … you can run this script by making it executable by typing chmod 775 usbkill.sh. [A]fter hitting the enter key into the terminal for that you will type sudo sh usbkill.sh … The source code to copy and paste is as follows …"

According to *User 33*, the program would be able to detect any foreign device plug-ins, forcefully shut down the computer, and wipe all memories stored in the device after installation. While posts like these did not provide direct information related to hacking CI facilities, they may be useful for malicious actors in concealing their online identities and destroying incriminating evidence relevant to the cyber-attacks.

Training Courses

Making up only 1.1% of the sample, some forum threads (n=10) offered training materials teaching individuals basics on information technology (IT) and cybersecurity. It was observed that many courses in the darknet forum are certified training sessions available from the surface web. For example, one user shared a list of digital CCNP[26] certification sessions and online hacking courses for free:

> "…216+ GB INE Cisco courses collection [external link] AND FOR OTHER COURSE AND CERTS TO STUDY, HERE. I GOT PLENTY. HOPE IT WILL CATCH YOUR INTEREST AND HAPPY LEARNING! … CCNP Security 300-71x5 SISE CIsco Learning Network Video [external link] CCNP Security 300-735 SAUTO CIsco Learning Network Video [external link] … Advanced Python Course [external link] …" (User 34)

In contrast, some posters may offer similar training courses for a small fee. Posters would also accept requests from clients about specific training course topics. In

[26] Offered by Cisco, CCNP security certification and training courses are available for IT professionals and experts to obtain training in cybersecurity (Cisco, 2022b).

one of the threads, the poster agreed to search and download INE CCNA-CCIE[27] training videos for another user, available after receiving payments:

> "… we've got the ICND1 & ICND2 for CCNA (which you may or may not need anymore), CCNA Collaboration 210-060 (CICD) & 210-065 (CIVND2), CCNA-Data Center DCICN 200-150, CCNA-Data Center 200-155, INE CCNA DATA Center (640-911 & 640-916). All told, it's just under 11GB of data. If you don't need the ICND1 & 2, that leaves exam prep for 6 Cisco exams and all of the data is recent (within the past 9-10 months). Say $5/exam for a total of $30?" (User 35)

Training courses available in the darknet were often offered for cheaper prices relative to prices invoiced from official course websites. For users looking into INE CCNA-CCIE training, the price offered by individuals such as *User 35* was much cheaper compared to the surface web platforms where a minimum charge of $39 a month was required (INE, 2022). Individuals obtaining training materials from the darknet would also protect their personal-identifiable information from the surface web platforms, ensuring their privacy and anonymity.

Although these training sessions were mainly designed for IT professionals and were not directly relevant to hacking, malicious actors would still find these courses useful in acquiring knowledge relevant to cybersecurity and networking of digital systems and devices. Understanding the functioning and settings employed by CI businesses may make it easier for malicious attackers in the reconnaissance and planning stages in order to conduct their attacks more efficiently. In addition, completion of these courses may also provide opportunities for low-skilled cybercriminals to understand basic programming and computer security in order to learn advanced illicit hacking techniques.

[27] The INE CCNA-CCIE training courses are sets of expert learning content offered by INE; the courses focused on teaching people contents related to networking, cybersecurity, and could learning (INE, 2022).

Chapter 4. Discussion

Open-source information may become a threat toward critical infrastructure as various OSINT techniques and data could inspire attackers on planning and conducting cyber-attacks or to acquire hacking skills against targeted providers. The themes uncovered in the current study provided a general overview of the types of useful information discoverable by malicious attackers in both surface web and darknet domains. Further, the findings in this study supported results from previous literature, suggesting the security risks associated with open-source data from the surface web and darknet platforms on critical infrastructure should be addressed (Albataineh & Alsmadi, 2019; Ghafir et al., 2018; Kaspersky ICS CERT, 2020; Papastergiou et al., 2020; Wang et al., 2019).

4.1. Research Questions

My first research question aimed to examine the types of CI-related data available from various web platforms. Through collecting and analyzing surface web data from Google, YouTube, Reddit, and Shodan, three major categories of information were found: (1) CI-related reconnaissance data and information-gathering tools; (2) malware proof-of-concept codes; and (3) educational materials relevant to hacker skills training. In the thematic content analysis conducted in the darknet forum named Dread, four main themes were identified: (1) questions and inquiries related to hacking; (2) information helpful for preparation and identification of CI threats and vulnerabilities; (3) hacker skills training materials; as well as (4) posts providing hacking services. Similar types of CI-related information, including reconnaissance data and educational materials, were found in both surface web and darknet forum datasets.

Reconnaissance data related to CI security and threats, hacking and information-gathering tools, as well as demonstration videos of hacking process against CI devices are often shared in various surface web and darknet platforms. For offenders, training tutorials and educational courses on hacking and exploit development were also retrievable through personal blogs, video channels, training sites, or darknet discussion forums. Malicious individuals looking for malware or vulnerabilities' proof-of-concept codes could retrieve data from surface web platforms such as Exploit Database, GitHub,

or official government or cybersecurity reports. In situations where hackers were unable to find desirable hacking tools or have questions regarding cyber-attacks against CI facilities, they could post questions and potentially receive answers or suggestions from darknet forums. Lastly, hacking services were also available upon individuals' request from the darknet.

To further understand the value of the data, my second research question explored the potential use of these information in the hands of malicious cyber-attackers. The findings from both surface web and darknet suggest the plausibility of ill-intended hackers using the identified types of data for the purposes of reconnaissance information-gathering, operational security set-up and attack preparation, repurposing and improvisation of malware against CI devices, or to learn hacking skills. Using data collected through different open-source platforms, offenders may thoroughly research their target, learn adequate hacking skills, apply OPSEC methods to cover their tracks, and potentially plan and select the desirable strategy to achieve their objectives. The availability of PoC codes, on the other hand, may provide hackers resources to reverse engineer pre-existing malware against industrial devices, improve the programs, and potentially deploy them against CI facilities. In addition, hacking services available in the darknet also increased the opportunities for individuals to consider planning and conducting large-scale cyber-attacks; the bars and skill requirements for individuals to conduct cyber-attacks are lowered, thus allowing malicious actors with little to no skills to hire others and conduct attacks for them (Ablon et al., 2014; Shakarian et al., 2016). My findings illustrate how reconnaissance and weaponization stages (stages 1 and 2) within the cyber-attack kill-chain were the predominant phases where malicious attackers may gather and make use of CI-related OSINT data (Coffey et al., 2018; Ghafir et al., 2018; Hahn et al., 2015; Hutchins et al., 2010).

4.2. CI-Related Data Collection and Attack Preparation

Information gathered by hackers during the reconnaissance stage of a cyber-attack were found to be the most prominent type of data among both surface web and darknet datasets. Though not all information are about CI facilities, the presence of these data is evidence suggesting that information circulating in surface websites and darknet forums could pose dangers against CI. The importance of this information has been especially clear in studies related to cybersecurity. The success rate of cyber-

attacks on ICS systems relies on whether malicious individuals gained sufficient knowledge on the functioning and interactions between cyber, control, and physical layers of systems (Hahn et al., 2015). Particularly, information gathering during the research phase of the cyber-attack was vital and necessary for both planning and later stages of cyber-attacks (Hunt, 2021; Ranum, 2014; Rodofile et al., 2019; Yadav & Rao, 2015).

As observed from the current research, reconnaissance data related to CI facilities on websites and forums can be retrieved by applying keyword searches. Close examination of the open-source data revealed that the majority of the materials could provide indirect forms of information with regards to exploitable devices, vulnerabilities, as well as programming algorithms may be useful in future attacks. Utilizing darknet forums such as Dread, curious cybercriminals would be able to exchange information and knowledge on topics of CI facilities or cyber-attack strategies (Basheer & Alkhatib, 2021). In addition, the relatively lower level of skills required to obtain such OSINT data suggest the possibility for novice hackers to take part in complex cyber-attacks against CI through the means of data-gathering. Script kiddies, if not the only hackers involved in planned cyber-attacks, could become a threat to CI facilities by recklessly researching and providing useful reconnaissance and OSINT data necessary for a successful cyber-attack (Verton, 2001).

My findings corresponded with previous research and demonstrated the potential negative effect of open-source information exposure relevant to industrial infrastructures (Holt et al., 2012; Leukfeldt et al., 2017; Samtani et al., 2018; Wang et al., 2019). If malicious attackers are indeed searching for vulnerabilities of industrial devices and methods to break into CI facilities, information related to attack strategies such as buffer overflow, man-in-the-middle attacks, denial of service (DoS) attacks, as well as default credentials may be accessible through open-source domains (Albataineh & Alsmadi, 2019; Kaspersky ICS CERT, 2020; Samtani et al., 2018). For example, Albataineh and Alsmadi's (2019) research recently showed that 18,539 out of the 80,611 active devices returned from Shodan queries were found to use default credentials. Kaspersky ICS CERT (2020) also published a report identifying the most popular types of exploits used by hackers, where data relevant to the malware and attack strategies can be easily gathered through OSINT. Within darknet forums, rich information on hacking and vulnerabilities may be discussed and exchanged between members; participation in the

forums may provide opportunities for malicious attackers to complete their reconnaissance goals more effectively. In fact, the primary reason for people to participate in online discussion forums was to gather information that may aid in their goal achievement (Ridings & Gefen, 2004). According to Ridings and Gefen (2004), participation in online communities would not only provide tremendous opportunities for users to exchange useful information, but also provide social support toward each other.

The processes and effort needed to look for relevant data, as shown in both my findings and previous literature, are not technically difficult for offenders. In the findings section, information related to common exploits, such as default usernames and passwords and potential attack strategies, were searchable from different internet platforms, potentially helping hackers to identify CI vulnerabilities and plan out effective cyber-attack strategies. Further, discussions and circulation of information on subjects of cybersecurity threats may generate an increasing number of cyber-attacks against companies and facilities, as well as to inspire users engaging in illicit hacking (Jordan & Taylor, 1998; Mirea et al., 2018). These results may be contextualized in the broader research relevant to data gathering and CI security: Researching, discussing, and using CI-related data where relevant information can be easily obtained through OSINT may make the planning of attacks easier, and possibly result in more cyber-attacks in the future.

Data from websites were not the only sources of information related to cyber-vulnerability and the identification of such exploits. Results in my current study demonstrated how different types of OSINT tools such as Shodan and information-gathering software continued to prove their abilities in providing information to hackers regarding CI facilities. As many ICS companies are unaware of the security of their devices and considered additional security measures unnecessary, countless CI devices are discoverable by OSINT tools and network scanners (Andreeva et al., 2016; Powers et al., 2015). Industrial devices searchable by network scanners are at higher risk of being hacked or exploited by malicious individuals, since sniffing tools and search engines such as Shodan, Nmap, and Nessus can gather details about industrial devices and network communications (Coffey et al., 2018). For example, Samtani et al.'s (2018) assessment on SCADA devices using both Shodan and Nessus revealed more than 500,000 devices discovered by the scanners, providing information on thousands of vulnerable devices and models exploitable by malicious hackers. In other words, rich

information returned by network scanners and other tools may allow offenders to identify and select the ideal devices and “targets” for the cyber-attacks. Playing an important role in the reconnaissance stage within a cyber kill-chain, successful vulnerability identification and planning of a cyber-attack using data gathering tools and techniques can possibly lead to a variety of available cybercrime methods suitable for targeted devices.

When analyzing discussions in the darknet forum, the plethora of contents were on the topic of operational security (OPSEC). Specifically, OPSEC-related posts were popular among members in which advice about optimal OPSEC settings and methods to conceal online identities were discussed. The forums were also used by some users to share anti-forensic methods used to evade law enforcement investigations. The emphasis on the popularity and importance of OPSEC were consistent with previous literature (Ablon et al., 2014; Bancroft & Reid, 2016; Barratt, 2011; Buxton & Bingham, 2015). Within the underground online communities, hackers were often expected not to disclose any personal identifiable information (Gehl, 2021; Jordan & Taylor, 1998). For individuals intending to participate in controversial or illicit activities such as hacking, the deidentification process was then particularly important. This was illustrated in Shakarian et al.’s (2016) discovery that hackers were concerned about the potential legal consequences of discussing and sharing evidence proofing cyber-attacks against computers. To avoid law enforcement’s attention, OPSEC methods such as PGP encryptions and fake identities or obscured online personas were frequently used by malicious actors when accessing darknet hacker forums. Further, law enforcement agencies’ recent effort to combat darknet marketplaces have also alerted members to exert greater levels of encryption and anonymization when accessing illicit contents in the darknet (Ablon et al., 2014). In accordance with previous studies, results in the current study suggested that logistics such as OPSEC settings may be paramount to users when accessing and collecting illicit content useful for hacking CI facilities from darknet forums. In attempt to avoid law enforcement’s attention, better OPSEC settings and anti-forensic methods may be discussed and are likely applied by forum users to cover online footprints as well as to destroy any self-incriminating evidence in the cyberspace.

Although it was a small part of my findings, discussions about social engineering strategies in conferences, presentations, and darknet forum threads may also be a factor

increasing the risk of cyber-attacks. With the ever-increasing popularity of social media and online socialization, the gathering and exploitation of open-source personal data is attracting both researchers and offenders' attention. For instance, Hayes and Cappa's (2018) study reported on series of information on social networking websites useful for hackers during the process of finding desirable social engineering targets. Their finding suggested that exposed individual characteristics such as marital status, level of education, age, as well as political preferences would affect the risk of social phishing (Hayes & Cappa, 2018). As employees used the internet with greater frequency and posted more personal information on social media websites, more opportunities may be provided to hackers in conducting cyber-attacks through methods such as social engineering. More relevant to my findings, the discussions of social engineering methods and specific personal profiles of vulnerable targets might aid hackers in the progress of learning social engineering, adopting the strategies, and identifying favorable targets.

4.3. Proof-of-concept Codes, Re-creation, and Improvisation of Malware

While the current study displayed an extensive number of collectable information relevant to data gathering and reconnaissance stages of cyber-attacks, a small portion of the OSINT data retrieved for this study also contained proof-of-concept (PoC) codes of malware against CI facilities. The publication of PoC codes found in the study may negatively impact the security of industrial systems; hackers could potentially conduct cyber-attacks through the re-creation of the zero-day exploit against unpatched industrial devices.

The starting point of disclosing PoC codes of malware was to consider the positive collaboration and exchange of opinions between information technology (IT) professionals and experts (Kaspersky ICS CERT, 2020; Peterson, 2012; S4 Events, 2016). The idea was attractive because as proposed by researchers, such publication would benefit the community and ultimately push for better security strategies and methods to protect critical infrastructure. In practice, however, researchers suggested that the sharing of these codes in public may provide attackers opportunities to reverse-engineer the source code and use the malware against unpatched devices (Positive Technologies, 2018). Wang et al. (2019) discovered that fully disclosed PoC exploits

online could be turned into active exploitable codes through successful alteration to the states of the disclosed codes. The existence of PoC codes in the public, therefore, may put CI facilities at higher risk by allowing hackers to potentially reverse-engineer and modify the available malware exploits. For example, after the discovery of the Stuxnet[28] malware in 2010, analyses and PoC codes of the malware were shared and published online, allowing cybercriminals to study the malware, reverse-engineer the programs, and potentially establish new malware against computer systems or critical infrastructure facilities (Farwell & Rohozinski, 2011; Stevens, 2020). Being detected and suggested to be variants of the Stuxnet worm, both data collecting worm Duqu, as well as the cyberespionage malware Flame could potentially be products created based off from the PoC of Stuxnet (F-Secure, 2022; Kushner, 2013). Another underlying issue relevant to the publication of PoC codes is the owners' lack of awareness on cybersecurity and their reluctance to maintain and protect their devices. An example of this is given in Positive Technologies' report of technical analysis and PoC exploits (Positive Technologies, 2018). Despite observing a rising trend in the variety and frequency of cyber-attacks against companies and devices, many vendors were reluctant to upgrade the system and patch the vulnerabilities upon the release of the fixes (Positive Technologies, 2018). Two years after the publication of Positive Technologies' report, statistical data from Kaspersky ICE CERT (2020) also found evidence that 32% of all industrial devices in the year of 2019 were exposed to cyber-attacks due to unpatched vulnerabilities and outdated programs. In short, industrial devices not receiving required maintenance or fixes may be at higher risks of being hacked.

4.4. Hacking-as-a-Service and the Cybercrime Economy

When analyzing data collected from the darknet, of novelty were the findings on the subject of hacking-as-a-service. Despite against subdread's content posting rules, a handful of threads explicitly advertised their hacking services toward potential clients in the forum. This suggests the emerging trend of skilled hackers or IT experts offering for-hire services, revealing the potential growing underground cybercrime economy. The findings aligned with Ablon et al.'s prediction early in 2014, that hacking for-hire services

[28] Stuxnet is a malicious malware targeting industrial Simens S7 PLC controllers and SCADA systems; the malware is also known for causing damages to the Iranian nuclear facilities in 2010 (Farwell & Rohozinski, 2011).

would likely increase due to the rising black-market economy and sharing and selling of zero-day exploits. Nonetheless, social networks and communications among cybercriminals were found to provide opportunities for forum members to recruit and join organized hacking groups across the world (Leukfeldt et al., 2017). As Leukfeldt et al. (2017) discovered in their research, various illicit hacking services were promoted and advertised within hacker communities. A recent paper published by Huang et al. (2018) also discussed various cybercrime services offered by malicious actors in detail; services associated with the cyber kill-chain model, including *deception as a service* where fake information is created for phishing and social engineering purposes, or *exploit as a service* where an exploit was developed using hacking tools and proof-of-concept codes, were offered in the darknet. Based off from the descriptions and contents of job-related posts discovered in the current study, it is advised that a wide range of hacking services are provided by hackers, and that these hackers for-hire services may contribute to the growth of the underground economy.

Moreover, the current research findings also demonstrated the potential for malicious actors with little or no hacking skills to become threats against CI facilities. Specifically, the data from this study informed researchers about the feasibility for individuals to openly recruit one or groups of skillful hackers to conduct attacks against selected targets. These results reflect those of Shakarian et al. (2016) who also mentioned that the commercialization of hacking services may increase the frequency and number of cyber-attacks. By hiring hackers from darknet forums and black markets, individuals are no longer required to be sophisticated or advanced in hacking, malware development, or data gathering: Newbies and aspired hackers may now become cyber-threats against CI facilities.

4.5. Educational Materials, Learning, and Hacking Skills Training

Finally, the exploration of the types of OSINT data available in publicly available platforms and forums has also shown several types of educational materials relevant to hacking, including blogs, tutorials, and courses. A portion of the results in the current study were able to provide tutorials and hacking courses, allowing hackers to learn specific data-gathering strategies and attack methods against targeted devices. One specific type of data discovered from the surface web research, demonstration videos of

successful hacks against ICS systems, were yet being discussed in previous research. Although I was unable to locate related literature discussing the effects and usefulness of demonstration videos, I can hypothesize based on criminological learning theories, that hackers may gather and learn programming-related data through watching these demo videos and educational materials. In other words, all publicly available educational materials may be gathered and could be helpful for hackers throughout their learning processes.

Like traditional crimes, an individual's involvement in cybercrimes could be explained by Aker's social learning theory. According to the theory, an individual's engagement in deviant behavior was associated with interactions, or differential associations, with others (Akers, 2009; Dearden & Parti, 2021). Upon establishing the connection and adopting deviant thoughts, individuals may engage in similar criminal behavior through imitating their deviant peers (Akers, 2009). In the case of cyber offending, hackers are more likely to engage in computer crimes when differentially associated with other hackers and imitating their behavior (Holt et al., 2010). Communications and observations of other cybercriminals in virtual environments, therefore, provide opportunities for individuals to understand and learn methods or techniques effective in conducting cybercrimes.

There is a growing body of literature recognizing the importance of online interactions and social learning when it comes to cyber offending (Holt et al., 2010; Miller & Morris, 2016). The study by Nodeland and Morris (2020), for example, showed how peer interactions in hacker forums impact individuals' participation in various cybercrimes. The anonymous environment and observation of deviant peers' successful cyber-attacks may significantly encourage other members' participation in similar criminal behavior. Further, in their analysis of social ties within hacker forums, Leukfeldt et al. (2017) suggested that online discussion forums may be the "university for cybercriminals" (p.17), where hacking tools, software vulnerabilities, and educational materials may be obtained and experimented by curious attackers.

This is in line with the hacker-ideal on self-directed education; hacking skills are often acquired by individuals through imitating, practicing, and learning behavior performed by experienced hackers (Shakarian et al., 2016). The construct of self-directed education was first articulated by Levy (1984) and popularized in his book,

Hackers: Heroes of the Computer Revolution. In his description of the hacker ethics/ideal, hackers should have access to all available information about computer systems, and encouraged them to learn hacking through hands-on practices (Levy, 1984). In fact, self-taught hackers are considered as more skillful and are superior than those who went through standardized ethical hacking or cybersecurity educational programs (Armerding, 2014). Consistent with the literature on social learning and cyber offending, my findings showed that there is an abundance of hacking-related information circulating in open-source platforms (Dearden & Parti, 2021; Goldsmith & Brewer, 2015). The availability of educational materials and the potential establishment of virtual peer communications in different platforms may provide rich resources and opportunities for malicious attackers to learn hacking, thus increasing their likelihood in engaging in online criminal activities (Dearden & Parti, 2021; Goldsmith & Brewer, 2015; Holt et al., 2010; Miller & Morris, 2016; Nodeland & Morris, 2020). In fact, increasing accessibility of information on the internet may also have a profound impact on people's involvement in computer-based crimes by means of self-empowerment and self-facilitated learning. Participation and communication with deviant peers in the underground discussion forums may aid the process of self-empowerment (Barak et al., 2008). For malicious hackers, the sense of personal empowerment is relevant to aspects which members shared and exchanged knowledge and skills relevant to hacking and cybersecurity. Evidence from Bilandzic's (2016) research also supported the idea of personal empowerment through peer interactions. In their research, uncoordinated social interactions were found to play an important role during the learning process. As existing literature illustrate, virtual environments such as publicly accessible platforms and discussion forums, served as significant resources for people to acquire and exchange new ideas on various topics including hacking (Barak et al., 2008; Bilandzic, 2016).

As presented in the current study, peer engagement and association in discussion forums also indicated the plausibility of applying social learning theory to explain individuals' criminal behavior online (Holt et al., 2010; Jordan & Taylor, 1998). Prior research on social learning have discovered that virtual association with peers would increase the likelihood of one's involvement in cyber offending (Miller & Morris, 2016; Nodeland & Morris, 2020). In the process of social learning, cybercriminals may differentially associate with members by sharing experiences and hacking resources, thus encouraging other members to learn and participate in hacking activities. Through

associating with hackers experienced in attacking CI facilities, malicious actors may be motivated to plan and conduct cyber-attacks against industrial devices. Moreover, these established connections with hackers in the forums also provided opportunities for malicious actors to imitate others' behavior and conduct similar cyber-attacks to targeted facilities (Holt et al., 2012).

The findings presented in this research contribute to such a prediction that the increased availability of educational materials and deviant peer interactions in discussion forums may increase the likelihood of malicious individuals learning and conducting cyber-attacks against businesses and CI facilities. Findings presented in my research could also suggest that, other than the more technically advanced hackers, novice hackers may now obtain hacking skills through self-learning and become a potential threat to CI facilities. While it can be advised that online tutorials and educational courses could teach malicious individuals hacking and malware development skills against CI devices, these demonstration videos may also aid hackers during the self-learning process. It is also possible that hackers could obtain excerpts of the codes presented in the videos and re-create the malware source code through reverse engineering techniques.

4.6. Comparison: Surface vs. Darknet Platform

In examining findings which emerged from surface web websites and darknet forums, both platforms were shown to provide rich information relevant to hacking and CI facilities. Thus, malicious actors aiming to plan and conduct cyber-attacks against critical infrastructure may gather and utilize OSINT data in either platform during different stages of the cyber-attack kill-chain. This finding is consistent with prior literature expressing the dangers of open-source intelligence on critical infrastructure (Samtani et al., 2018; Solberg, n.d.). My analysis highlights how both surface and underground platforms may serve as sources for information relevant to target devices operating in various CI sectors. This included collecting reconnaissance data potentially useful for preparing and planning cyber-attacks, seeking advice about hacking, or exchanging experiences, tools, and educational materials. One of the main reasons why threat-related OSINT information are circulating in both surface web and darknet platforms may be due to the sharing of these legitimate contents in public domains (Guccione, 2021). As contents relevant to cybersecurity and CI facilities were often published by legitimate

governmental websites, cybersecurity companies, or academic journals and conferences, search results and data may not be removed by surface web platforms (Google Search Help, 2021; Reddit, 2021). Consequently, offenders with malicious intentions may gather such legitimate information, gain understanding of computer systems and CI facilities, and potentially plan out cyber-attacks against these facilities.

While similar types of information were found circulating in both the surface web and darknet, PoC codes were found only in the surface web platforms. In this study, PoC codes were mainly discovered in official analysis reports, or were shared by cybersecurity professionals in platforms including GitHub or Exploit Database. Despite observing occasional discussions and inquiries about PoC codes of certain exploits in the darknet forum, members often redirected the original posters to obtain these codes from the surface web. A possible explanation for this finding may be that the disclosure of PoC codes on malware and software zero-day exploits were initially proposed by information security experts striving for a better understanding of the exploits (Kaspersky ICS CERT, 2020; Peterson, 2012; S4 Events, 2016). Since the PoC codes were not shared by malicious hackers and the intention of disclosing the codes was benign, it was not expected that individuals may access and abuse these codes against computer systems or CI facilities (Cimpanu, 2019; Positive Technologies, 2018). Without such expectation, surface web platforms such as GitHub and Exploit Database thus provide opportunities for individuals to share hacking tools and PoC codes and gradually become the largest platforms holding source codes and coding tools useful for hackers, penetration testers, and computer program researchers (Exploit Database, 2022; GitHub, 2021). Due to the public nature of the source codes in these platforms, both security professionals and malicious actors are granted access and may analyze and engineer these PoC codes for personal reasons.

Proof-of-concept codes were not the only unique category of information discovered in the current research. Interestingly, hacking-related job postings and advertisements promoting hacking as a service was observed to exist only within the darknet. Analysis of forum data indicated the gradual development of hacking as a business through the provision of hacking services by skilled cybercriminals. As a consequence, more people may be inspired to become hackers and consider hacking as a career. These findings not only corresponded with Ablon et al.’s (2014) prediction on the increasing likelihood of hacking for-hire services available in the black-market, but

also connected with previous literature discussing the growth of illicit contents and services shared in the darknet (Guccione, 2021; Hurlburt, 2017). Due to the illegitimate nature of the advertisements, the contents are often prohibited and removed by surface web platforms (Google Search Help, 2021; Reddit, 2021). However, sharing contents promoting hacking services in unindexed networks was unrestricted and law enforcement agencies were less likely to detect these illicit services (Bermudez Villalva et al., 2018). In addition, the existence of hacking communities and discussion forums provide individuals opportunities to share OPSEC techniques and remain untraceable when seeking illicit hacking services (Barratt, 2011; Deb et al., 2018; Shakarian et al., 2016). The additional OPSEC features would further increase the privacy and security of the individual, thus making investigations on hacking for-hire services more difficult. In that light, the hidden nature of these darknet advertisements and illicit content may help explain the discovery of hacking services only in the darknet. The increased availability of hacking services also suggests that less sophisticated hackers, script kiddies, or aspiring potential hackers may become cyberthreats against businesses and CI facilities. Hacking-as-a-service content discovered in the darknet, therefore, could make critical infrastructure and the overall cyberspace more vulnerable and susceptible to cyber-attacks.

4.7. Limitations

A few potential limitations should be addressed for this study. Firstly, the current sample cannot be generalized to all publicly available information from both surface web and darknet platforms. Further, the keyword searches may not have returned all available information. Search engines such as Google tend to omit repetitive search results, thus containing only a limited number of websites for each of the keywords. Policies prohibiting illegal information such as content promoting unlawful activities, sharing illegal malware, or posting hacking-related information are often actively implemented among many indexed websites (Google Search Help, 2021; Reddit, 2021; YouTube Help, 2021). Detection of illegal content violating open web policies may result in a removal of said content (Reddit, 2021). While this may not be the concern for darknet forum analysis, the unindexed nature of the websites suggested there could be other undiscovered open access discussion forums available in the darknet but were not included in this study. In the current study, I have included all available results returned

from surface web search engines and the Dread forum and conducted analysis on these datasets. For surface web platforms like YouTube or Reddit where the total quantity of results was not provided, I was able to analyze a random selection of the results until saturation was reached. Thus, it seemed reasonable to assume generalizability toward the keyword search results emerged from these open-source platforms, not including results from additional keywords and other search engines or forums.

Similar to other research on OSINT data, the authenticity of the textual contents analyzed in the current study may be an issue. Open-source information can be difficult to validate since individuals can easily share any experiences or information on the internet. Part of my study relied on the analysis of real-life social networking forum data from the darknet; a small portion of subjective publications were also included in the surface web dataset. While the portion of the data containing official announcements, conferences, and open-access white papers published by cybersecurity experts may not be an issue, the accuracy and validity of the subjective content included in the sample may be questioned.

Additionally, it is also important to address the limitation of the data collection method used in the current research. Like all of the qualitative research involving analysis over both textual and video/audio contents online, the manual extraction and analysis of data would increase the time required for data collection, making researcher fatigue a rising issue. Enhancement of data extraction and analysis is particularly needed for OSINT data, as open-source platforms can contain rich information relevant to the topic of interest. To address this issue, it is recommended that researchers use computerized techniques and automated programs in future studies to automatically extract and filter data relevant to the research topic.

4.8. Implications and Future Research

Notwithstanding the above limitations, this study has contributed new information that had not been addressed in previous literature. Particularly, I was unable to find any studies discussing the use of videos demonstrating successful attacks toward exploitable vulnerabilities. I hypothesize from the results that the discovery of these videos may serve as educational channels and facilitate ill-intended individuals to learn hacking skills online. Further, the increasing variety of learning materials and individual

engagement in the learning progresses may be used to predict one's involvement in cyber-attack behavior. My observation indicated the plausibility of applying criminological learning theories to help researchers understand the types of OSINT data useful for hackers to self-learn and to carry out deviant hacking behaviors. Therefore, future research could investigate the potential impact of demo videos and online learning materials in the field of cybersecurity.

Additional studies may also pay attention to the impact and predicting power of social learning in the context of open-source data. Through analysing the relationship between different types of OSINT resources and individuals' engagement in online deviant behavior, researchers could identify the types of materials more likely to affect individuals' cybercrime engagement. Based on findings in this study, the identification of contents motivating malicious actors attempting to attack CI may help with the design and implementation of more proactive policing and mitigating strategies. Further research on the impact of publicly available PoC codes is also recommended as the potential danger of fully disclosed PoC exploits against critical infrastructure remains under-studied. Since large source code sharing platforms such as GitHub or Exploit Database may be ideal places for malicious hackers to gather hacking tools or PoC codes, security specialists should pay attention and practice caution when sharing and uploading hacking-related tools or codes to these platforms. Current policies regarding sharable resources in the public domain should be reviewed with the intention to limit the amount of open access information exploitable by hackers while balancing people's right to learn and read relevant cybersecurity materials. In that light, designers and owners of various open-access platforms may consider implementing more rigorous website policies to restrict users' access to codes and tools that may pose cyber-threats against CI facilities. Lastly, it is recommended that law enforcement agencies establish relationships with these open-access platforms to obtain necessary information for cybercrime investigations.

Further, the current research could be extended to other OSINT resources using additional keyword queries and toward additional OSINT platforms. As this current study only acknowledged a partial list of keywords related to critical infrastructure, more in-depth analysis could be designed to discover additional open-source information useful to attackers in various cyber-attack phases. Furthermore, future analysis on the impact of various OSINT resources on the security of CI sectors is also recommended, as such

information will allow cybersecurity technicians to gain a better understanding of the vulnerabilities and enforce more effective mitigation strategies to protect the CI industry.

Building off from the current findings, mitigation strategies such as implementation of mandatory cybersecurity training, routine vulnerability assessments toward devices and facilities, as well as enforcement of stronger security measures are recommended to ICS vendors. Governing different CI sectors and ensuring the provision of essential services, the current assigned sector-specific federal agencies should consider recruiting cybersecurity professionals to provide awareness training, cybersecurity consultation, and risk assessment to ICS vendors on a regular basis. Businesses and contractors working in the CI sectors should also be inspected by their corresponding governing agencies to ensure the implementation of security policies and guidelines, as well as proper maintenance of all ICS devices. To further improve the efficiency of the inspections, a standardized risk assessment model may be developed by the federal government and implemented to evaluate the security of essential components of CI facilities.

Lastly, pseudonymous environments, such as ones provided in the darknet forums, may facilitate hackers to freely exchange and learn information related to CI threats and vulnerabilities. For law enforcement agencies and security specialists, research and surveillance of contents circulating in darknet platforms and forums may help to proactively detect potential threatening information against CI companies and prevent attacks from happening. Attention may be paid toward users actively engaging in discussions on topics related to CI vulnerabilities and exploits, as well as those who openly express desire or plan to conduct cyber-attacks against CI devices or governmental agencies. In addition, cybersecurity professionals and law enforcement authorities should pay more attention to the commercialization of hacking services available in the darknet. With the recent surge of services provided by hackers, more malicious actors with or without hacking skills may become threats toward CI facilities. Future studies may identify and track activities of specific hackers or hacking organizations, predict the targets selected by malicious actors, and enforce strategies to prevent or defend the likelihood of the cyber-attacks.

Chapter 5. Conclusion

The development of technology has allowed society to access almost everything with smart devices and the internet. While the majority of industries and infrastructures are becoming more reliant on electronic systems and the convenience brought by the internet, it has also increased cybersecurity risks against these industrial systems (Quigley & Roy, 2012).

Aiming to understand the types and content of information obtainable to malicious hackers from open-source platforms against the critical infrastructure industry, I analyzed publicly available OSINT resources from both the surface web and darknet through a qualitative research method approach. This study mainly focused on CI-related data that was able to either directly or indirectly help hackers throughout different cyber-attack kill-chain phases. Within the results, I noticed the increasing amount of information that could be used by malicious attackers against various industrial devices. Open access cybersecurity information originally published for security professionals with benign intents and educational purposes are now at risk of being used maliciously by hackers. In addition, darknet discussion forums allowed malicious actors to exchange thoughts about attack strategies, as well as to advertise and promote hacking services. Incorporating data gathered from open-source platforms and skills learned from hacking tutorials and courses, malicious hackers could plan out efficient cyber-attacks against ideal targets, resulting in disruptions to critical infrastructure.

The findings from the study also suggested that novice hackers such as script kiddies may pose an increasing threat toward CI facilities in their abilities to facilitate the low-skill data gathering reconnaissance process, to hire other hackers, as well as the potential to self-learn to become skilled hackers. The popularization of hacking may also motivate independent hackers to conduct cyber-attacks against CI facilities for monetary gain or reputational needs. Although many known cyber-attacks against CI facilities are identified to be sponsored by nation states, it is still possible for independent, motivated hackers to use OSINT data and gather information related to CI facilities and devices. For some motivated script kiddies or individuals without proper hacking skills, they could seek services from grey or black hat hackers in the darknet communities. The commercialization of hacking provides opportunities for hackers to form organizations

sponsored by private individuals or by nation states. For example, governmental agencies with sufficient resources and funding may recruit and hire motivated hackers to gather OSINT data relevant to CI vulnerabilities and exploits, social engineer selected targets, or to conduct cyber-attacks. Despite the lack of evidence of cyber-attacks being launched depending solely on the use of OSINT data, it is still remarkably important for researchers to recognize the possibility of OSINT-based attacks in the future and to identify potential threats at early stages as institutions are becoming more reliant on remote controlling and accessing of CI facilities.

References

Ablon, L., Libicki, M. C., & Abler, A. M. (2014). Markets for cybercrime tools and stolen data: hacker's bazaar. *RAND National Security Research Division.* Retrieved June 05, 2022, from https://www.rand.org/pubs/research_reports/RR610.html

Admin. (2021, April 29). How to access Dread (Darknet market forum). *Dark Net Daily.* Retrieved May 25, 2022, from https://darknetdaily.com/2020/12/31/how-to-access-dread-darknet-market-forum/

Advantech. (2022). WebAccess. *Advantech.* Retrieved August 25, 2022, from https://www.advantech.com/industrial-automation/webaccess

Akers, R. L. (2009). *Social Learning and Social Structure: A General Theory of Crime and Deviance.* New York: Routledge.

Albataineh, A., & Alsmadi, I. (2019). IoT and the risk of internet exposure: Risk assessment using Shodan queries. In *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)* (pp.1-5).

AMCI. (n.d.). What is a PLC?. *AMCI.* Retrieved June 24, 2022, from https://www.amci.com/industrial-automation-resources/plc-automation-tutorials/what-plc/

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I., & Timorin, A. A. (2016). Industrial control systems and their online activity. *Kaspersky Lab.* Retrieved June 27, 2022, from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190427/KL_REPORT_ICS_Availability_Statistics.pdf

Armerding, T. (2014, April 23). Self-taught hackers rule. *CSO*. Retrieved June 20, 2022, from https://www.csoonline.com/article/2146363/self-taught-hackers-rule.html

Australian Cyber Security Centre. (2021, October 6). Defending against the malicious use of the Tor network. *Australian Government.* Retrieved June 27, 2022, from https://www.cyber.gov.au/acsc/view-all-content/publications/defending-against-malicious-use-tor-network#:~:text=The%20Tor%20network%20consists%20of,a%20website%20or%20web%20server.

Bancroft, A., & Reid, P. S. (2016). Concepts of illicit drug quality among darknet market users: purity, embodied experience, craft and chemical knowledge. *International Journal of Drug Policy, 35*, 42-49.

Barak, A., Boniel-Nissim, M., & Suler, J. (2008). Fostering empowerment in online support groups. *Computers in Human Behavior, 24*(5), 1867-1883.

Barratt, M. J. (2011). Discussing illicit drugs in public internet forums: visibility, stigma, and pseudonymity. In *Proceedings of the 5th International Conference on Communities and Technologies* (pp.159-168).

Basheer, R., & Alkhatib, B. (2021). Threats from the dark: a review over dark web investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications, 2021,* 1-21.

Ben-Chitrit, D. (2021, March 12). OSINT data collection: you still need humans, but automation is well worth the investment. *Security Boulevard.* Retrieved June 25, 2022, from https://securityboulevard.com/2021/03/osint-data-collection-you-still-need-humans-but-automation-is-well-worth-the-investment/

Bergal, J. (2021, March 10). Florida hack exposes danger to water systems. *PEW.* Retrieved June 09, 2022, from https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems

Bermudez Villalva, D. A., Onaolapo, J., Stringhini, G., & Musolesi, M. (2018). Under and over the surface: a comparison of the use of leaked account credentials in the dark and surface web. *Crime Science, 7*(1), 17.

Bilandzic, M. (2016). Connected learning in the library as a prodct of hacking, making, social diversiity and messiness. *Interactive Learning Environments, 24*(1), 158-177.

Boyle, P. J., & Speed, S. T. (2018). From protection to coordinated preparedness: a genealogy of critical infrastructure in Canada. *Security Dialogue, 49*(3), 217-231.

Bodenheim, R., Butts, J., Dunlap, S., & Mullins, B. (2014). Evaluation of the ability of the Shodan search engine to identify internet-facing industrial control services. *International Journal of Critical Infrastructure Protection, 7*(2), 114–123.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Buxton, J., & Bingham, T. (2015). *The rise and challenge of dark net drug markets*. Global Drug Policy Observatory. Retrieved June 04, 2022, from https://www.swansea.ac.uk/media/The-Rise-and-Challenge-of-Dark-Net-Drug-Markets.pdf

Cartagena, A., Rimmer, G., Van Dalsen, T., Watkins, L., Robinson, W. H., & Rubin, A. (2020). Privacy violating opensource intelligence threat evaluation framework: A security assessment framework for critical infrastructure owners. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)* (pp.0494–0499).

Chen, T. M. (2014). *Cyberterrorism after Stuxnet*. Strategic Studies Institute, US Army War College. Retrieved August 10, 2020, from http://www.jstor.org/stable/resrep11324

Chen, Y., Lian, X., Yu, D., Lv, S., Hao, S., & Ma, Y. (2020). Exploring Shodan from the perspective of industrial control systems. *IEEE Access, 8*, 75359–75369.

Cimpanu, C. (2019, March 18). Is it still a good idea to publish proof-of-concept code for zero-days?. *Zdnet.* Retrieved August 24, 2022, from https://www.zdnet.com/article/is-it-still-a-good-idea-to-publish-proof-of-concept-code-for-zero-days/

Cisco. (2022a). Networking software (IOS & NX-OS). *Cisco.* Retrieved May 28, 2022, from https://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

Cisco. (2022b). CCNP security certification and training. *Cisco.* Retrieved May 29, 2022, from https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/professional/ccnp-security-v2.htmlUbuntu. (2022). Enterprise open source and Linux | Ubuntu. *Canonical.* Retrieved May 27, 2022, from https://ubuntu.com/

Coffey, K., Smith, R., Maglaras, L., & Janicke, H. (2018). Vulnerability analysis of network scanning on SCADA systems. *Security and Communication Networks, 2018*, 1–21.

Computer Security Resource Center. (n.d.). Operations security (OPSEC). *National Institute of Standards and Technology.* Retrieved May 27, 2022, from https://csrc.nist.gov/glossary/term/operations_security

Darknetlive. (n.d.). Dread. *Darknetlive*. Retrieved May 24, 2022, from https://darknetlive.com/forums/dread/

Dearden, T. E., & Parti, K. (2021). Cybercrime, differential association, and self-control: knowledge transmission through online social learning. *American Journal of Criminal Justice*, 1–21.

Deb, A., Lerman, K., & Ferrara, E. (2018). Predicting cyber-events by leveraging hacker sentiment. *Information, 9*(11), 280.

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: monitoring of online offenders by researchers. *The European Review of Organised Crime, 2*(2), 122-141.

Diaz, D. (2021, October 5). The 4 best Linux distros for helping you stay anonymous. *Sitepoint.* Retrieved June 03, 2022, from https://www.sitepoint.com/anonymous-linux-distros/

dnstats. (n.d.). Dread forum. *dnstats*. Retrieved May 24, 2022, from https://dnstats.net/site/dread/

DuckDuckGo. (2021). Privacy. *DuckDuckGo*. Retrieved December 16, 2021, from https://duckduckgo.com/privacy

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *Computers & Security, 69*, 18–34.

Electronic Frontier Foundation. (n.d.). What is a Tor relay? *Electronic Frontier Foundation.* Retrieved June 27, 2022, from https://www.eff.org/pages/what-tor-relay

Enghoff, O., & Aldridge, J. (2019). The value of unsolicited online data in drug policy research. *International Journal of Drug Policy, 73*, 210-218.

Exploit Database. (2022). About the Exploit Database. *Exploit Database.* Retrieved June 08, 2022, from https://www.exploit-db.com/

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23-40.

F-Secure. (2022). Flame. *F-Secure.* Retrieved August 23, 2022, from https://www.f-secure.com/v-descs/flame.shtml

Gehl, R. W. (2021). Dark web advertising: the dark magic system on Tor hidden service search engines. *Continuum, 35*(5), 667-678.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing, 74*(10), 4986–5002.

GitHub. (2021). GitHub's frequently asked questions. *GitHub.* Retrieved June 08, 2022, from https://resources.github.com/faq/

Goebel, M., Dameff, C., & Tully, J. (2019). Hacking 9-1-1: infrastructure vulnerabilities and attack vectors. *Journal of Medical Internet Research, 21*(7), e14383.

Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130.

Google Search Help. (2021). Policies for content posted by users on Search. *Google*. Retrieved December 14, 2021, from https://support.google.com/websearch/answer/7408270?hl=en

Green, B., Prince, D., Busby, J., & Hutchison, D. (2015). The impact of social engineering on industrial control system security. In *Proceedings of the 1st ACM Workshop on Cyber-physical Systems – Security and/or Privacy* (pp.23–29).

Greenberg, A. (2022, April 12). Russia's Sandworm hackers attempted a third blackout in Ukraine. *Wired.* Retrieved June 09, 2022, from https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/

Greenberg, A. (2017, June 20). How an entire nation became Russia's test lab for cyberwar. *Wired.* Retrieved June 09, 2022, from https://www.wired.com/story/russian-hackers-attack-ukraine/

Guccione, D. (2021, July 1). What is the dark web? How to access it and what you'll find. *CSO.* Retrieved June 03, 2022, from https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html

Hahn, A., Thomas, R. K., Lozano, I., & Cardenas, A. (2015). A multi-layered and kill-chain based security analysis framework for cyber-physical systems. *International Journal of Critical Infrastructure Protection, 12*, 39–50.

Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons, 61*(5), 689–697.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2010). Social learning and cyber-deviance: examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice,33*(2), 31–61.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891-903.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: a survey. *ACM Computing Surveys, 51*(4), 70.

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards automating social engineering using social networking sites. *2009 International Conference on Computational Science and Engineering, 3*, 117–124.

Hunt, B. (2021, December 2). To prevent cyberattacks, make reconnaissance harder. *Forbes.* Retrieved June 07, 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/12/02/to-prevent-cyberattacks-make-reconnaissance-harder/?sh=165c4b7f19b2

Hurlburt, G. (2017). Shining light on the dark web. *Computer, 50*(4), 100-105.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2010). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill-

chains. In *Proceedings of the 6th International Conference on Information Warfare and Security* (pp.113-125).

IBM. (2022a, May 16). Operating system shells. *IBM.* Retrieved August 23, 2022, from https://www.ibm.com/docs/en/aix/7.2?topic=administration-operating-system-shells

IBM. (2022b, August 10). Root account. *IBM.* Retrieved August 23, 2022, from https://www.ibm.com/docs/en/aix/7.2?topic=passwords-root-account

IBM Cloud Education. (2021, March 17). Networking. *IBM.* Retrieved June 27, 2022, from https://www.ibm.com/cloud/learn/networking-a-complete-guide

Imperva. (2021). Buffer overflow attack. *Imperva.* Retrieved July 4, 2022, from https://www.imperva.com/learn/application-security/buffer-overflow/

INE. (2022). Expert IT training for networking, cyber security and cloud. *INE.* Retrieved May 29, 2022, from https://ine.com/

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review, 46*(4), 757-780.

Judd, A., & Little, S. (2020, December 3). Metro Vancouver's transit system hit by ransomware attack. *Global News.* Retrieved June 25, 2022, from https://globalnews.ca/news/7499986/translink-suspicious-network-activity-update/

Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J., & Kompatsiaris, I. (2016). OSINT and the Dark Web. In Akhgar, B., Bayerl, P., & Sampson, F. (Eds.), *Open-source Intelligence Investigation: From Strategy to Implementation.*(pp. 111–132). Cham, Switzerland: Springer International Publishing.

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: A qualitative content analysis of darknet forums. *International Journal of Drug Policy, 73*, 281-287.

Kaspersky. (2022a). What is the Deep and Dark Web?. *Kaspersky.* Retrieved June 03, 2022, from https://www.kaspersky.com/resource-center/threats/deep-web

Kaspersky. (2022b). Internet of Things security threats. *Kaspersky.* Retrieved June 27, 2022, from https://www.kaspersky.com/resource-center/threats/internet-of-things-security-risks

Kaspersky. (2022c). What is a honeypot?. *Kaspersky.* Retrieved August 22, 2022, from https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

Kaspersky. (2022d). What is an advanced persistent threat (APT)?. *Kaspersky.* Retrieved August 23, 2022, from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kaspersky ICS CERT. (2020). *Threat landscape for industrial automation systems: H2 2019*. Retrieved August 18, 2020, from https://ics-cert.kaspersky.com/media/KASPERSKY_H22019_ICS_REPORT_FINAL_EN.pd

Kaur, S., & Randhawa, S. (2020). Dark web: a web of crimes. *Wireless Personal Communications, 112*(4), 2131-2158.

Kranenbarg, M. W., Ruiter, S., & Van Gelder, J. (2021). Do cyber-birds flock together? Comparing deviance among social network members of cyber-dependent offenders and traditional offenders. *European Journal of Criminology*, *18*(3), 386–406.

Kushner, D. (2013). The real story of Stuxnet. *IEEE Spectrum, 50*(3), 48-53.

Kwon, K. H., & Shao, C. (2021). Dark knowledge and platform governance: a case of an illicit e-commerce community in Reddit. *The American Behavioral Scientist, 65*(6), 779-799.

Leon, H. (2020, February 9). An inside look at the good, bad and complicated parts of the Dark Web. *Observer.* Retrieved May 25, 2022, from https://observer.com/2020/02/dark-web-tor-unindexed-internet-guide/

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704-722.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution.* New York: Anchor Press/Doubleday.

Lutkevich, B. (n.d.). Script kiddie. *TechTarget.* Retrieved June 25, 2022, https://www.techtarget.com/searchsecurity/definition/script-kiddy-or-script-kiddie

Mansfield-Devine, S. (2018). Critical infrastructure: understanding the threat. *Computer Fraud & Security, 7*, 16–20.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security, 92*, 101762.

Miller, B., & Morris, R. G. (2016). Virtual peer effects in social learning theory. *Crime and Delinquency, 62*(12), 1543-1569.

Miller, B., & Rowe, D. C. (2012). A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on research in information technology* (pp.51-56).

Mirea, M., Wang, V., & Jung, J. (2018). The not so dark side of the darknet: a qualitative study. *Security Journal, 32*(2), 102-118.

Mitre. (2022, March 14). Software: Industroyer, CRASHOVERRIDE. *MITRE ATT&CK.* Retrieved August 23, 2022, from https://collaborate.mitre.org/attackics/index.php/Software/S0001

Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (2016). CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp.860-867).

National Institute of Standards and Technology. (2015). *Supplemental information for the interagency report on strategic U.S. government engagement in international standardization to achieve U.S. objectives for cybersecurity.* Retrieved August 12, 2020, from https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of cyber-warfare. *Computers and Security, 31*(4), 418–436.

Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior, 41*(1), 41-56.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health Services Research, 42*(5), 533-544.

Palys, T., & Atchison, A. J. (2013). Text, image, audio, and video: Making sense of non-numeric data. In *Research decisions: Quantitative, qualitative, and mixed method approaches* (5th ed., pp. 303-332). Toronto: Nelson Education.

Papastergiou, S., Mouratidis, H., & Kalogeraki, E. (2020). Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. *Evolving Systems, 12*(1), 91-108.

Parent, M., & Beatty, D. R. (2021, June 15). The increase in ransomware attacks during the COVID-19 pandemic may lead to a new internet. *The Conversation.* Retrieved June 06, 2022, from https://theconversation.com/the-increase-in-ransomware-attacks-during-the-covid-19-pandemic-may-lead-to-a-new-internet-162490

Pastor-Galindo, J., Nespoli, P., Marmol, F. G., & Perez, G. M. (2020). The not yet exploited goldmine of OSINT: opportunities, open challenges and future trends. *IEEE Access*, *8*, 10282–10304.

Peterson, D. (2012, January 19). Project Basecamp at S4. *Dale Peterson*. Retrieved August 16, 2020, from https://dale-peterson.com/2012/01/19/project-basecamp-at-s4/

Petters, J. (2020, April 6). What is PGP encryption and how does it work?. *Varonis.* Retrieved June 03, 2022, from https://www.varonis.com/blog/pgp-encryption

Plant Automation Technology. (2022). Top 10 industrial automation companies in the world. *Plant Automation Technology.* Retrieved June 25, 2022, from https://www.plantautomation-technology.com/articles/top-industrial-automation-companies-in-the-world

Positive Technologies. (2018). *Cybersecurity threatscape: Q4 2018.* Retrieved from https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-2018-Q4-eng.pdf

Powers, E., Peasley, S., Waslo, R., Fletcher, B., & Dinh, D. (2015). Examining the industrial control system cyber risk gap. *Deloitte.* Retrieved June 27, 2022, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-ics-white-paper.pdf

Proofpoint. (2022). What is a Remote Access Trojan (RAT)? *Proofpoint.* Retrieved May 28, 2022, from https://www.proofpoint.com/us/threat-reference/remote-access-trojan

Public Safety Canada. (2009). *National strategy for critical infrastructure.* Public Safety Canada. Retrieved August 10, 2020, from https://central.bac-lac.gc.ca/.item?id=PS4-65-2009-eng&op=pdf&app=Library

Public Safety Canada. (2016). *Fundamentals of Cyber Security for Canada's Critical Infrastructure Community.* Public Safety Canada. Retrieved June 06, 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx

Public Safety Canada. (2021, October 14). Guidance on essential services and functions in Canada during the COVID-19 pandemic. *Public Safety Canada.* Retrieved June 09, 2022, from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/esf-sfe-en.aspx

Python. (2022). Python. Retrieved June 24, 2022, from https://www.python.org/

Quigley, K., & Roy, J. (2012). Cyber-security and risk management in an interoperable world: An examination of governmental action in North America. *Social Science Computer Review*, *30*(1), 83–94.

Ranum, M. J. (2014, October 29). Breaking cyber kill chains. *Tenable.* Retrieved June 07, 2022, from https://www.tenable.com/blog/breaking-cyber-kill-chains

Reddit. (2021). Reddit content policy. *Reddit*. Retrieved December 14, 2021, from https://www.redditinc.com/policies/content-policy

Rehg, J., & Sartori, G. (2010). Instructional algorithms enhance student understanding of Plc ladder logic programming. In *2010 Annual Conference & Exposition* (pp.15.751.1-15.751.13).

Ridings, C. M., & Gefen, D. (2004). Virtual community attraction: why people hang out online. *Journal of Computer-Mediated Communication, 10*(1), JCMC10110.

Rockwell Automation. (2022). Allen-Bradley PLC Programmable Controllers. *Rockwell Automation.* Retrieved June 25, 2022, from https://www.rockwellautomation.com/en-us/products/hardware/allen-bradley/programmable-controllers.html

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection, 25*, 14–35.

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. *Journal of Management Information Systems*, *34*(4), 1023–1053.

Samtani, S., Yu, S., Zhu, H., Patton, M., Matherly, J., & Chen, H. (2018). Identifying SCADA systems and their vulnerabilities on the Internet of Things: A text-mining approach. *IEEE Intelligent Systems, 33*(2), 63–73.

Schneider Electric. (2022). Modicon: edge control for industrial IoT. *Schneider Electric.* Retrieved June 25, 2022, from https://www.se.com/ca/en/work/products/master-ranges/modicon/

Security Studio. (2021, November 5). What is operational security? The five-step OPSEC process. *Security Studio.* Retrieved June 10, 2022, from https://securitystudio.com/operational-security/

Shakarian, J., Gunn, A. T., & Shakarian, P. (2016). Exploring malicious hacker forums. In Jajodia, S., Subrahmanian, V. S., Swarup, V., & Wang, C. (Eds.), *Cyber Deception: Building the Scientific Foundation* (pp.259-282). Springer International Publishing.

Shodan. (n.d.). Industrial Control Systems. *Shodan.* Retrieved June 26, 2022, from https://www.shodan.io/explore/category/industrial-control-systems

Solberg, T. (n.d.). Recognizing the seven stages of a cyber-attack. *DNV.* Retrieved June 08, 2022, from https://www.dnv.com/cybersecurity/cyber-insights/recognizing-the-seven-stages-of-a-cyber-attack.html

Stannard, E. (2021, June 22). OSINTifying targets. *Medium.* Retrieved August 22, 2022, from https://ellisstannard.medium.com/osintifying-targets-93134da0d485

Stevens, C. (2020). Assembling cybersecurity: the politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy, 41*(1), 129-152.

Stouffer, C. (2021, September 3). What is a zero-day exploit?. *Norton.* Retrieved June 27, 2022, from https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work.html

S4 Events. (2016, December 11). Project Basecamp – PLC Hacking Intro. *YouTube*. Retrieved August 16, 2020, from https://www.youtube.com/watch?v=BKJje3Ram2I&t=12s

Tariq, N., Asim, M., & Khan, F. A. (2019). Securing SCADA-based critical infrastructures: Challenges and open issues. *Proocedia Computer Science, 155*, 612–617.

Techslang. (n.d.). What is an Industrial Control System? A short definition of Industrial Control System. *Techslang.* Retrieved August 22, 2022, from https://www.techslang.com/definition/what-is-an-industrial-control-system/

TechTarget Contributor. (2009). Ubuntu. *TechTarget*. Retrieved May 27, 2022, from https://www.techtarget.com/searchdatacenter/definition/Ubuntu#:~:text=Ubuntu%20(pronounced%20oo%2DBOON%2D,be%20used%20on%20servers

TechTerms. (2017, July 3). Root. *TechTerms.com,* Retrieved August 23, 2022, from https://techterms.com/definition/root

Tor. (2021). Censorship. *Tor Project*. Retrieved December 16, 2021, from https://support.torproject.org/censorship/

Tor. (n.d.). Tor: overview. *Tor Project.* Retrieved June 27, 2022, from https://2019.www.torproject.org/about/overview.html.en#overview

TransLink. (2022). TransLink cyber incident. *TransLink.* Retrieved June 09, 2022, from https://www.translink.ca/about-us/about-translink/cyber-incident

Trend Micro. (2021, July 22). IoT security issues, threats, and defenses. *Trend Micro.* Retrieved June 27, 2022, from https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

Trend Micro. (2022). Denial of Service (DOS). *Trend Micro.* Retrieved June 24, 2022, from https://www.trendmicro.com/vinfo/us/security/definition/denial-of-service-dos#:~:text=Denial%20of%20service%20(DoS)%20is,inaccessible%20for%20a%20certain%20period.

Verton, D. (2001). Black hat highlights real danger of script kiddies. *Computerworld*. Retrieved December 24, 2021, from https://www.computerworld.com/article/2581986/black-hat-highlights-real-danger-of-script-kiddies.html

Wang, Y., Wu, W., Zhang, C., Xing, X., Gong, X., & Zou, W. (2019). From proof-of-concept to exploitable. *Cybersecurity, 2*(1), 1–25.

Watson, J. (2017, February 15). Qubes, Whonix, or Tails: which Linux distro should you use to stay anonymous?. *Comparitech.* Retrieved June 03, 2022, from https://www.comparitech.com/blog/vpn-privacy/anonymity-focused-linux-distributions/

Yadav, T., & Rao, A. M. (2015). Technical aspects of cyber kill chain. In Abawajy, J. H., Mukherjea, S., Thampi, S. M., & Ruiz-Martinez, A. (Eds.), *Security in Computing and Communications: Third International Syymposium, SSCC 2015* (pp.438-452). Springer, Cham.

YouTube Help. (2021). Harmful or dangerous content policy. *Google*. Retrieved December 14, 2021, from https://support.google.com/youtube/answer/2801964?hl=en&ref_topic=9282436

Zajko, M. (2015). Canada's cyber security and the changing threat landscape. *Critical Studies on Security, 3*(2), 147-161.

Zetter, K. (2016, March 3). Inside the cunning, unprecedented hack of Ukraine's power grid. *Wired.* Retrieved June 09, 2022, from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zhang, E. (2020, December 1). What is Operational Security? The five-step process, best practices, and more. *Digital Guardian*. Retrieved May 27, 2022, from https://digitalguardian.com/blog/what-operational-security-five-step-process-best-practices-and-more

Appendix

List of keyword queries searched in darknet forums

Table 1. Keyword terms and phrases

Keywords and Phrases		
SCADA	“chemical plant”	“water 0day”
"supervisory control and data acquisition"	“chemical sector”	“water exploit”
"programmable logic controller"	“chemical vulnerability”	“water zero day”
"programmable logic controllers"	“chemical hack”	“plant vulnerability”
PLC	“chemical malware”	“plant hack”
PID	“chemical intrude”	“plant malware”
“PID controller”	“chemical access”	“plant intrude”
“three-term controller”	“chemical zero day”	“plant access”
RTU	“chemical attack”	“plant zero day”
“remote terminal unit”	“chemical 0day”	“plant attack”
Modbus	“chemical exploit”	“plant 0day”
DNP3	“dam vulnerability”	“plant exploit”
Modicon	“dam hack”	“energy plant”
Unitronics	“dam malware”	“energy vulnerability”
Eaton	“dam intrude”	“energy hack”
“Eaton industrial”	“dam access”	“energy malware”
Honeywell	“dam zero day”	“energy intrude”
“Midas gas detector”	“dam attack”	“energy access”
“Midas gas”	“dam 0day”	“energy zero day”
CirCarLife	“dam exploit”	“energy attack”
Advantech	“emergency sector”	“energy 0day”
Laquis	“emergency service”	“energy exploit”
“SINEMA Siemens”	“emergency vulnerability”	“blackout vulnerability”
SINEMA	“emergency hack”	“blackout hack”
Siemens	“emergency malware”	“blackout malware”
Industrial	“emergency intrude”	“blackout intrude”
“server exploit”	“emergency access”	“blackout access”
“server vulnerability”	“emergency zero day”	“blackout zero day”
“server hack”	“emergency attack”	“blackout attack”
“server malware”	“emergency 0day”	“blackout 0day”
“server intrude”	“emergency exploit”	“blackout exploit”
“server access”	Nuclear	Electricity
“server zero day”	Transportation	“power system”
“server attack”	“hydro service”	“power plant”

Keywords and Phrases		
“server 0day”	“water plant”	“power vulnerability”
PROFIBUS	“water vulnerability”	“power hack”
“Honeywell HART”	“water hack”	“power malware”
Simatic	“water malware”	“power intrude”
Schneider	“water attack”	“power access”
Cisco	“water intrude”	“power zero day”
Infrastructure	“water access”	“power attack”
Pipeline	“advanced process control”	“power 0day”
“gas plant”	Industroyer	“power exploit”
“gas vulnerability”	“manufacturing cascading failure”	“OMRON PLC”
“gas hack”	“industrial control system”	“Mitsubishi PLC”
“gas malware”	ICS	“Mitsubishi electric PLC”
“gas intrude”	“critical infrastructure”	“very small aperture terminal”
“gas access”	PCS	VSAT
“gas zero day”	“process control”	“power grid”
“gas attack”	“process control system”	“smart grid”
“gas 0day”	“distributed control system”	Dragonfly
“gas exploit”	DCS	Havex
“OMRON industrial controller”	“GE Automation”	Crashoverride
Stuxnet	Duqu	“crash override”
EKANS	BlackEnergy	Triton
MegaCortex	“Black Energy”	Trisis
OSINT		
		Total keywords and phrases (*N*) = 169