Journal of Students‘ Research in Computer Science

e-ISSN: 2722 – 290X
Vol. 5 No. 2 (November 2024), Page: 167 – 184
https://doi.org/10.31599/288ab341
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/JSRCS

Anticipating Cyber Espionage: Open Source Intelligence (OSINT) Investigation and Cyber Counterintelligence

M. Yusuf Samad[1,*], Beta Kurniawati Ningtiyas[2], Fiqih[2], Fauzy Rosny[3], Diah Ayu Permatasari[4]

* Korespondensi: e-mail: ahmadyusad@gmail.com

[1] Communication & Information System Security Research Center (CISSReC); Moh. Kahfi Street 1 No. 88 Jagakarsa South, Jakarta; e-mail: ahmadyusad@gmail.com
[2] Master of Cyber Security; Monash University Indonesia; Green Office 9 Building, Jl. BSD Green Office Park,Tangerang, Banten; e-mail: bnin0001@student.monash.edu, fiqi0001@student.monash.edu
[3] Ministry of Home Affairs of the Republic of Indonesia; North Merdeka Street No. 7, RT.5/RW.2, Gambir, Gambir District, Central Jakarta City, Special Capital Region of Jakarta 10110; e-mail: fauzykantor@gmail.com
[4] Communication Science; Bhayangkara Jakarta Raya University; Perjuangan Street, Mulya Marga, North Bekasi, West Java 17121, Tel: 021-88955882; e-mail: pepy@ubharajaya.ac.id

Submitted : **21 September 2024**
Revised : **24 Oktober 2024**
Accepted : **18 November 2024**
Published : **30 November 2024**

Abstract

This research was conducted to analyse the use of OSINT and cyber counterintelligence in investigating cyber espionage operations using Advanced Persistent Threat (APT). Indonesia as one of the victims of cyber espionage conducted by Australia, raises the urgency of preventing cyber espionage. The purpose of this research is to answer the questions of how the utilisation of OSINT in the prevention of cyber espionage and how cyber counterintelligence can prevent cyber espionage. This research uses a qualitative method with case study on APT groups affiliated with China. The results of the analysis of cyber espionage cases conducted by I-SOON and its affiliates, which were then carried out by cyber counterintelligence efforts and investigations through OSINT with dorking techniques, can find a comprehensive picture of cyber espionage operations carried out by I-SOON, including operating practices and the underlying motivation for cyber espionage..

Keywords: *Advanced Persistent Threat, Cyber Counterintelligence, Cyber Espionage, Dorking, OSINT*

Abstrak

Penelitian dilakukan untuk menganalisis pemanfaatan OSINT dan kontra intelijen siber dalam menginvestigasi operasi spionasi siber yang menggunakan *Advanced Persistent Threat* (APT). Indonesia sebagai salah satu korban spionase siber yang dilakukan oleh Australia, memunculkan urgensi pencegahan spionase siber. Tujuan penelitian untuk menjawab pertanyaan bagaimana pemanfaatan OSINT dalam pencegahan spionase siber dan bagaimana kontra intelijen siber dapat mencegah spionase siber. Penelitian menggunakan metode kualitatif dengan studi kasus tentang kelompok APT yang terafiliasi dengan Cina. Hasil analisis kasus spionase siber yang dilakukan oleh I-SOON dan afiliasinya, kemudian dilakukan upaya kontra intelijen siber serta investigasi melalui OSINT dengan teknik *dorking*, dapat menemukan gambaran komprehensif operasi spionasi siber yang dilakukan oleh I-SOON, ermasuk praktik operasi serta motivasi yang mendasari spionase siber tersebut.

Kata Kunci: Spionase Siber, Ancaman Persisten Tingkat Lanju*t*, OSINT, Dorking, Kontra Intelijen Siber.

JSRCS status is accredited by the Directorate General of Research Strengthening and Development No. 225/E/KPT/2022 with Indonesian Scientific Index (SINTA) journal-level of S5, starting from Volume 1 (2) 2020 to Volume 6 (1) 2025

1. Introduction

The Indonesian government must build and strengthen a cyber security system because Indonesia has already felt the impact of cyber attacks, especially as Indonesia is ranked as the country with the highest number of cybercriminals targeting it. The large number of losses means that cyber security and defense must be evaluated (Rizki, 2022). In addition, Indonesia is classified as the most vulnerable country in Asia and an easy target for cyber attacks in the form of damage to private and government information systems and data theft. Cybercrime is the best choice for perpetrators because of its effectiveness and anonymity and without territorial boundaries (Suratman, 2017).

Indonesia demonstrates strengths in cybersecurity, as evidenced by its growing awareness of cybersecurity issues, its leadership role in Southeast Asia, and the speed of digital transformation that facilitates the implementation of advanced cybersecurity measures. Nevertheless, Indonesia faces challenges such as a shortage of skilled human resources in cybersecurity, limited resources to implement a comprehensive cybersecurity strategy, and a regulatory and legal framework that requires continuous refinement and adaptation (Susila & Salim, 2024). Indonesian law in the face of cyber espionage is still unable to accommodate because Indonesian law on cyber espionage does not explicitly regulate, only partially explains the act of spying. It is also carried out conventionally, so norms are blurring, and extensive interpretation is required in its application (Hastri, 2021).

Cyber threats are one of the many serious threats whose scope can target from the individual to the country level. The methods consist of several types: attacks on electricity networks, sabotage, vandalism, and cyber espionage (Aditya et al., 2022). Cyber espionage is a form of proliferation of cybercrime threats along with the development of cyber technology. Cyber espionage itself is a combination of three crimes carried out in a cycle, including wiretapping (interception), telematics crimes (information technology), and espionage (spying). Cyber espionage between countries is often used to discover activities or steal important data from other countries, both in the political, economic, and military fields. Cybersecurity is critical to prevent various criminal acts, maintain the security of the technology industry, and secure data at both the personal and big data levels of a country (Ramadhan & Avalokitesvari, 2022).

Cyber espionage, as an act that violates the provisions of international diplomatic law, impacts diplomatic relations between countries, especially the country that is the object of cyber espionage and the country that conducts cyber espionage. Some of these impacts are losses obtained by the object country of cyber espionage, namely the successful theft or the loss of several important confidential data, documents, and information due to cyber espionage practices carried out by the perpetrator country against its country. Another loss that may be experienced is damage to the object's computer system in the country due to viruses/malware left by the perpetrator of cyber espionage. Indonesia became a victim of espionage, although it is unclear whether this action is included in cyber espionage. However, in terms of its characteristics, this is included in the practice of cyber espionage, namely espionage activities carried out by Australia by tapping the phones of state officials, including President Joko Widodo and his wife. The wiretapping case was revealed after one of the outgoing CIA agents, Edward Snowden, leaked classified information to the public (Heriyanto, 2020).

Previously, a cyber espionage case occurred in Indonesia in 2013. The case of wiretapping carried out by the Australian Embassy on several high-ranking Indonesian officials was a form of cyber espionage. This is because this action was carried out by utilizing technology in the form of a cell phone communication network owned by these officials and then illegally listening to and taking the information from the Australian Embassy in Jakarta for Australia's interests (Mirza et al., 2024). Due to this incident, the Indonesian Government immediately responded by recalling the Indonesian Ambassador to Australia in Canberra and suspending cooperative relations between the two countries (Pardede et al., 2024; Salehun & Sulaiman, 2019). This response was carried out based on the insecurity felt by the Indonesian Government regarding threats to privacy and information security resulting from Indonesia's vulnerabilities, especially in the information technology sector (Shaffan, 2018).

In order to prevent repeated incidents of cyber espionage, various efforts need to be made to build cyber security and cyber resilience through the use of Open Source Intelligence (OSINT). This is because extracting knowledge from public sources is a way to solve existing problems from a different and innovative perspective. In particular, search results via OSINT can benefit cyber security and cyber resilience (Pastor-Galindo et al., 2020). Cyber counterintelligence is also needed to deal with cyber espionage (Setiyadi & Keliat, 2020). Thus, this research aims to answer the question of how to use OSINT in preventing cyber espionage and how cyber counterintelligence can prevent cyber espionage.

2. Research Methods

This study adopts a post-positivistic paradigm in a qualitative approach. The data obtained was analyzed descriptively using various techniques, such as qualitative content analysis according to the Philipp Mayring model, analysis using NVivo software, and other models such as Bogdan and Biklen and Miles and Huberman (Wijaya, 2018). This research focuses on state-sponsored cyber espionage using China's cyber espionage activities as a case study. The reason for using China as a case study is that China has carried out cyber espionage throughout Southeast Asia. Reports indicate that hackers affiliated with security vendors linked to the Chinese government have targeted government agencies across the region for years. This cyber attack has infiltrated the systems of countries in Southeast Asia, one of which is Indonesia (Bajak & Kang, 2024; Kelliher, 2024).

This will start with an explanation of the process and analysis of cyber espionage, followed by a discussion of Advanced Persistent Threat (APT), which is attributed to state and alternative cyber counterintelligence efforts. Specifically related to APT, the data search method uses OSINT. In general, OSINT covers the methodology of various techniques for collecting and analyzing publicly available data. In particular, publicly available data refers to sources containing free, legally disclosed, accessible to everyone, and not confidential information. This data can be found on social media networks or directly queried via search engines like Google. The data collected can then be used to create profiles for specific targets, including behavioral characteristics (Tziampazis, 2021).

In this research, the technique used is Google Dorks because this technique has advantages over other search techniques, namely access effectiveness, time efficiency, and accuracy of results (Haq, 2017). Cyber security professionals use this Google Dorks technique for information gathering, reconnaissance, vulnerability detection, and cybercrime investigation tasks (Abasi, 2020). Google Dork, as it is widely known, is a term that denotes a sophisticated way of using a search engine like Google. In addition to general search terms, search engines also accept more advanced operators such as intext: , inurl: , site: , language: AND, OR, and so on. This technique allows users to exploit the web simply by using their search engines and nothing more. Dorking applies not only to Google, but also to other search engines such as Yahoo, DuckDuckgo, and Bing. Even though it seems simple, Dorking is a powerful way to collect data on public websites (Tziampazis, 2021). In the context of this research, other search engines are used, such as search engines from China, namely Baidu and Sogou. This is because information relating to China-attributed APTs may be available on one of these search engines but not on another.

Search results from Google Dork are recorded, collected, and then searched again using the latest search results. Each search result is validated and developed continuously so that information is interconnected between one search result and another. Further searches were carried out using other sources related to the research, such as digital archives and cyber security websites. After that, the existing findings are connected and visualized using browser-based diagramming software, namely draw.io.

3. Results and Discussion

3.1. Cyber Espionage Process

In general, the cyber espionage process consists of several stages. Rivera et al. (2022) developed Wangen's (2015) research results related to cyber espionage. The development was based on a summary of relevant cyber espionage cases. The stages in question are reconnaissance, preparation, attack, information gathering, maintenance, information leakage, information sale, and escape. In detail, it is explained as follows (Rivera et al., 2022).

Reconnaissance. The first stage is an investigation where the attacker collects important information about the target, such as email addresses, IP addresses, and employee names. Sophisticated social and technical engineering techniques can be used to find vulnerabilities in target systems. This phase requires computer security experts; some reconnaissance activities can be automated.

Preparation, the preparatory stage depends on the aim of the attack. There are two possible attack vectors to use. First, social engineering requires resources, time, and knowledge of human psychology, language, and culture. Second is computer exploitation, which utilizes malware and the attacker's technical knowledge to attack previously detected vulnerabilities in the target computer system.

Attack, after analyzing the target's vulnerabilities, the attack will be performed by selecting the most effective attack vectors and techniques. Next, the attacker will attempt to gain access credentials to the target system using malware, backdoors, or Advanced Persistent Threats (APT). After a successful attack, the intruder will try to escalate privileges by looking for users and passwords that can provide access to more resources. During this stage, the intruder will gather information from the victim's system to learn about the environment. During this phase, the intruder uses various methods to remain undetected while still being able to enter and exit the victim's system safely.

Information gathering, attackers know the environment they are spying on and look for the type of information they want. To facilitate this process, attackers need to know the victim's language and use malware, such as advanced keyloggers, to gather the desired information.

Maintenance, if espionage continues over a long time, the attacker must adapt to environmental changes. If an already implemented backdoor is detected or compromised, the attacker will analyze the cause and prevent the same thing from happening to other backdoors. They will also look for new ways to maintain their presence in attacked systems and examine whether they can carry out broader attacks or adapt current intrusions to continue gathering information. The maintenance phase is continuous as long as the espionage takes place.

Information leak, the attacker collects all the necessary information and then compresses it using formats such as RAR or 7z. They also protect information with passwords or implement encryption. Attackers use proxy networks such as the Tor network (the deep web) to send the obtained information to hide their identity. In some cases, backdoors implemented in previous stages are also used to transmit information.

Sale of stolen information, attackers offer stolen information or technology as a service to specific customers. These customers can leverage this information to reduce their research and development costs. In this case, attackers use the stolen information as a bargaining chip to encourage future purchases and profit from their espionage process.

Escape, this phase can occur for several reasons. Once the attacker has finished gathering the information he is seeking, he proceeds to leave the system, perhaps leaving some backdoors open for future espionage. On the other hand, if an attacker is detected and has to abandon the mission, then he will try to remove traces that might compromise his identity before leaving the system.

3.2. Cyber Espionage Analysis

Fitzpatrick & Dilullo's (2015) research explains the use of the S.P.I.E.S taxonomy. to analyze and evaluate an organization's vulnerability to cyber espionage. This taxonomy comprises five elements: Situational Threats, Penetration Methodologies, Information Targets, Espionage Enforcement, and Security Vulnerabilities. Through this taxonomy, organizations can identify the actors responsible for conducting espionage, the methods used, the information targeted, the law enforcement undertaken, and the existing security vulnerabilities. This taxonomy aims to assist organizations in conceptualizing and evaluating threat vectors to their information and trade secrets. By using this taxonomy, companies can improve their security against conventional cyber and industrial espionage.

A study discusses the significant threat of cyber espionage and the importance of identifying and attributing activities to cyber espionage. The study introduces a synthesis approach and framework for holistically identifying cyber espionage to define cyber espionage events. This approach leverages detection capabilities and integrates the results into a framework called the Espionage Probability Matrix (EPM). This framework considers the context of individual events to determine the likelihood of cyber espionage using the Espionage Threshold Matrix (ETM). The advantage behind this synthesis approach is that intrusion, malware, or exfiltration detection can be viewed in the context of the entire event (Merritt & Mullins, 2011).

Intelligence agencies and adversaries use cyber espionage as a strategy to steal data, disrupt critical infrastructure, and obtain early warning of enemy attacks. The main targets of cyber espionage are large corporations, government agencies, military intelligence, academic institutions, and other organizations with valuable intellectual property. Cyber espionage seeks to access research and development data, academic research, intellectual property, business objectives, strategic plans and marketing tactics, political strategies, affiliations, and military communications. Cyber espionage has proven effective in data collection and manipulation, theft of technology and patents, and providing early warning of enemy attacks. This shows the importance of cyber security protection for companies and institutions with valuable assets (Ciluvi et al., 2022). Poor cyber security in the government and private sectors makes a country a target for other countries to carry out attacks, which can lead to a country's operations and services collapsing (Samad & Persadha, 2022).

3.3. *Advanced Persistent Threat*

Cyber espionage activities are mainly categorized as APT. APT attacks are sophisticated and sustained cyberattacks that steal sensitive data over time. These attacks are carefully planned and designed to infiltrate organizations and circumvent existing security measures. Social engineering is also often used in these attacks to obtain target information. These methods often tap into human emotions such as excitement, curiosity, empathy, or fear. Using this method, cybercriminals can trick victims into providing personal information, clicking on malicious links, downloading *malware*, or paying a ransom (Ciluvi et al., 2022). Countries (including intelligence agencies) worldwide use cyber espionage as a tradecraft technique to obtain information confidentially, either during storage or during the delivery process, from a country's computer system (Adzel, 2021).

One of the countries attributed to APT is China. China's Ministry of Public Security is collaborating with an information security vendor based in China, namely I-SOON or Anxun. This information was obtained from hundreds of documents leaked and published on the GitHub platform (Cary & Milenkoski, 2024; Krebsonsecurity, 2024). The leaked data was grouped into several groups: complaints about companies, chat records, financial information, products, employee information, and details about foreign infiltration. According to leaked data, I-SOON's structure includes three penetration teams, one security research team, and one essential support team of about 70 people. The data also leaked I-SOON activities that infiltrated several government departments, including those from India, Thailand, Vietnam, South Korea, NATO, and Indonesia (Arntz, 2024; Bajak & Kang, 2024). Several cybersecurity researchers believe the leaked data is genuine (Poireault, 2024).

From this data leak, I-SOON has several capabilities, including the ability to steal X's social media accounts by obtaining emails and telephone numbers, reading private messages, monitoring activity in real-time, and uploading tweets; Remote Access Trojans (RATs) or Remote Access Trojans which are designed with comprehensive features and can obtain information remotely, including carrying out remote removal and installation; exploitation of Android and iOS based mobile devices; portable devices to attack networks from within; Special equipment for officers working abroad to establish secure communications; and user search databases that list user data including phone number, name, and email, and can be linked to social media accounts (Arntz, 2024; Karpf, 2024).

Analysis shows that I-SOON operates as a chartered APT and serves key Chinese government agencies. This shows state support in these cyber operations (Karpf, 2024). I-SOON is already on the radar of several cybersecurity researchers after being sued by a company from the same city, a company known as 'Chengdu 404' based in Chengdu. I-SOON operates with a similar business model to Chengdu 404 (Natto Team, 2023; Uren, 2024). According to the United States Department of Justice, Chengdu 404 is related to the cyber espionage group known as APT41, Chengdu 404 is led by Qian Chuan as leader, Jiang Lizhi as his deputy and Fu Qiang as manager of significant data development (U.S. Department of Justice, 2020). Based on data from *the Federal Bureau of Investigation* (FBI), the three of them and actors named Zhang Haoran and Tan Dailin were declared members of the Chinese hacking group known as APT 41 and BARIUM (FBI, 2019). However, several studies say that APT41 is also known as BARIUM (Group-IB, 2021; Mandiant, 2022). The five people have several similar charges: identity theft, fraud, and money laundering (FBI, 2019).

Based on information from the cyber security website attack.mitre.org, by entering the keyword APT41 in the search column, information was obtained that APT41 is a threat group that researchers assess as an espionage group sponsored by the Chinese government, which also carries out financially motivated operations. Active since at least 2012, APT41 has been observed targeting various industries, including but not limited to the healthcare, telecommunications, technology, finance, education, retail, and video game industries in 14 countries (Htet et al., 2019).

I-SOON has documented business relationships with Chengdu 404, an important company for APT41 operators. The investigation results showed that I-SOON operated in a very similar way to Chengdu 404, namely by establishing relationships with government security agencies and universities. From leaked data, I-SOON Chief Executive Officer Wu Haibo used the nickname "shutdown" for its existence in cyberspace. This is the basis for revealing various attributions of real-life identities and their digital traces (Bansal, 2024).

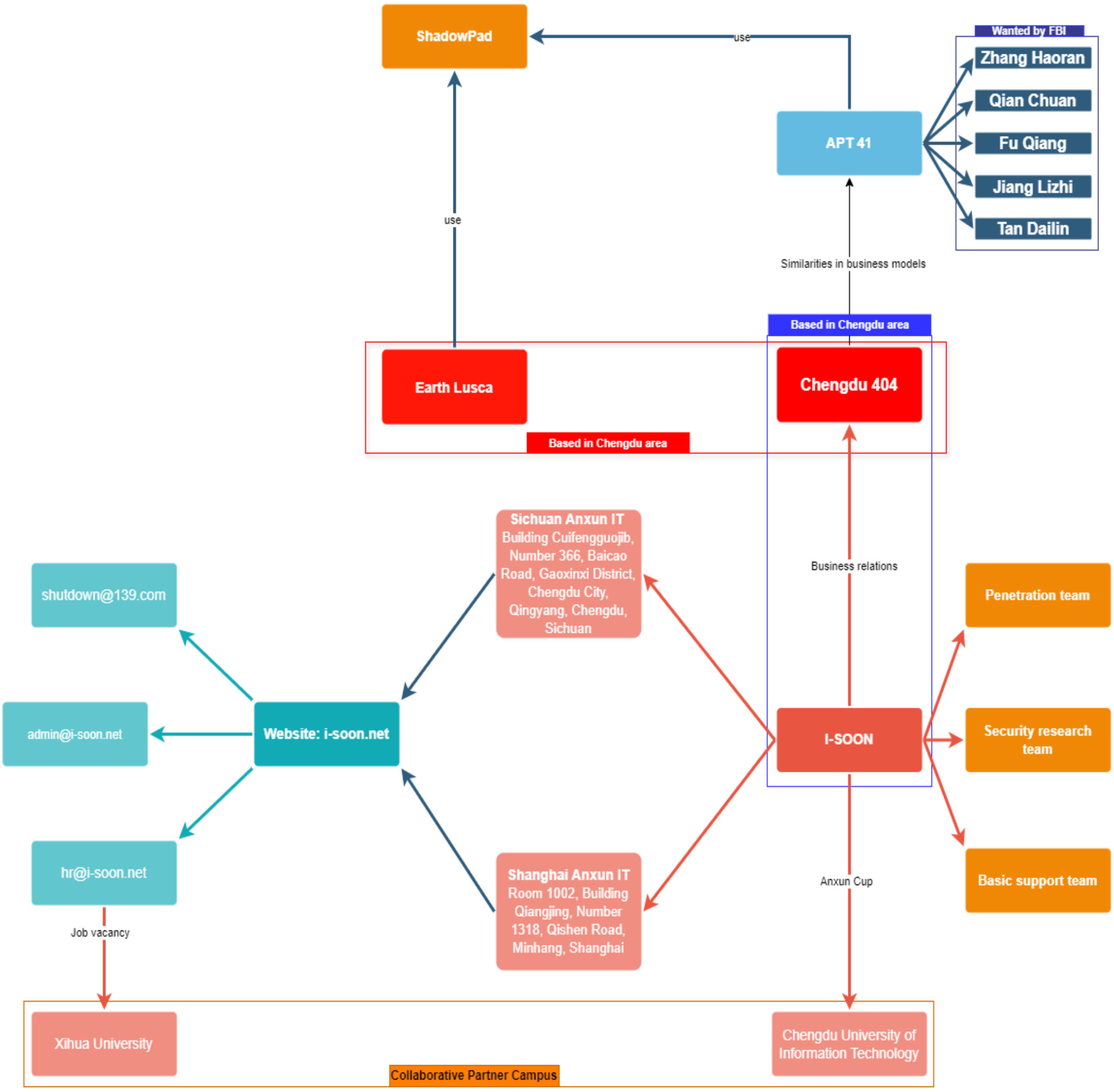
One of the universities connected to I-SOON is Chengdu University of Information Technology, which has collaborated in holding a Student Information Security Technology Competition called "Anxun Cup" in 2020; the general manager of I-SOON attended this activity, Chen Cheng (Chengdu University of Information Technology, 2020). The university is closely associated with Chengdu 404 and other APT41 hackers (Bernsen, 2024).

Another university connected to I-SOON is Xihua University in the Chengdu area. I-SOON uses this campus website to open job vacancies or recruit employees by attaching the website address (www.i-soon.net) and email hr@i-soon.net (Xiaolan, 2019). The i-soon.net domain was then investigated via the Whoisfreaks platform, which is reliable for accessing detailed information about any domain online. Search results via the link https://whoisfreaks.com/tools/whois/history/lookup/i-soon.net show that the I-SOON company uses the email shutdown@139.com. These findings confirm information indicating that Wu Haibo's (I-SOON CEO) nickname is "shutdown". Apart from that, there is another email address related to I-SOON, namely admin@i-soon.net. The email was found through a search on a website https://web.archive.org/, which archives websites digitally by entering the keyword "http://www.i-soon.net/".

Research results from Sentinel Lab show that APT41 has been identified as one of the users of a modular malware platform called ShadowPad. ShadowPad is malware used for espionage operations in several campaigns, including CCleaner attacks, NetSarang, and ASUS supply chain attacks (Hsieh & Chen, 2021). One way APT41 works is spear phishing or sending messages (emails) to targeted victims so that it appears as if the message comes from a trusted source or sender (Mandiant, 2022; Threatcop, 2023). Besides APT41, ShadowPad is also used by the Earth Lusca group operating in Chengdu, such as APT41 (Natto Team, 2023; Pernet & Horejsi, 2024). Earth Lusca is a highly skilled and dangerous threat actor, primarily motivated by cyber espionage and financial gain (Trend Micro, 2022).

In the case of Earth Lusca, the malware has the same features. However, it has added security features that differentiate it from the Shadowpad samples used by other groups. In this case, the ShadowPad sample includes an encrypted payload. Earth Lusca works through spear phishing using proven social engineering techniques. One motivation is financial gain, as evidenced by their targeting of gambling companies and cryptocurrencies. The group also targets public-facing servers by exploiting known vulnerabilities in servers running outdated versions of applications. Earth Lusca also uses vulnerability scanning tools to find possible vulnerabilities within targeted victim websites (Chen et al., 2022).

Based on the OSINT investigation, the findings are combined and visualized to illustrate the relationship between one finding and another. The colors in the figure also convey the meaning of similarities in each finding.



Source: Research Result (2024)

Figure 1. Findings Related to I-SOON and Their Correlation with the APT

The figure above depicts a cyber espionage group's operational network that is predominantly based in Chengdu, China. The group has a complex organizational structure with several subteams with specific roles, such as penetration, security research, and support. This group is connected to several universities in China, indicating collaboration between academics and cybercriminals. The targets of this group's attacks are most likely organizations or companies that have sensitive data. Their activities include various techniques such as vulnerability exploitation, data theft, and malware distribution. The image above shows how sophisticated and organized the current cyber espionage threat is that is affiliated with countries, especially China.

3.4. Cyber Counterintelligence

Duvenage & von Solms (2013) revealed that with new technological resources that continue to be developed, it can be found that cyber espionage has two aspects as its basis: human and technical. Some cyber espionage techniques emphasize the exploitation of human aspects, such as in the case of social engineering, a common way to access intrusions for espionage is through social engineering techniques (Rivera et al., 2022).

A study of motivations for carrying out espionage activities in the context of cyber security. Payne & Mienie's (2023) study explains that MICE+G, consisting of Money, Ideology, Compromise, Ego, and Grievance, motivates someone to carry out espionage activities. Another motivation is RASCLS, which consists of Reciprocation*, Authority, Scarcity, Commitment/Consistency, Liking, and Social Proof.* These motivations are applied to cyber security, and the results show that MICE+G and RASCLS can be used to prevent, detect, and address potential social engineering and other malicious cyber activities.

In the context of Chinese intelligence, there is a broader and more accurate motivation for characterizing Chinese intelligence recruiting methods. Eftimiades (2023) shares six motivations why ethnic Chinese want to carry out espionage activities, which are abbreviated by the acronym "BEWARE" consisting of Business Opportunities referring to establishing and building a competitive business in China; Ethno-nationalism refers to wherever ethnic Chinese are located and whatever their nationality, they are still considered part of the Chinese people; Wealth/Money is financial transactions in cash and non-cash; Academic Advancement means success by obtaining an academic position based on research that has been stolen; Repression/Coercion, which means direct and indirect (implied) threats to individuals, families, and organizations; and Emotional bonds refer to obligations and friendly relationships.

The most basic counterintelligence concept for empowering society in the face of social engineering and other cyberattacks is “everyone is a target.” All computer and internet users should be aware of security. Cybercriminals, terrorist organizations, and hostile nation-state actors continue to seek out vulnerable individuals who may be tricked into handing over their personally identifiable and sensitive/confidential information. A counterintelligence approach to cybersecurity begins with a heightened awareness of the existence of malicious actors (Payne & Mienie, 2023).

Cyber counterintelligence consists of defensive cyber counterintelligence and offensive cyber counterintelligence. Counterintelligence defensive methods aim to block an opponent's access and gather information about the opponent. Meanwhile, counterintelligence offensive methods aim to manipulate, control, and thwart opponents' actions (Duvenage & von Solms, 2013). Defensive procedures in the form of cyber counterintelligence require conducting counterintelligence analysis to understand the enemy's Modus Operandi (MO) and Tactics, Techniques, and Procedures (TTP) and review cyber attack incidents. That way, this can be a reference for predicting future trends in cyber attacks. This information collection includes the 5W + 1H aspects (*Who, What, When, Where, Why, and How*) to get a valuable picture of the enemy for policymakers (Bodström, 2022). The results of an analysis of the threat of cyber attacks in the form of cyber espionage against a country show that the threat level of cyber espionage perpetrators is in the high category so that it endangers the interests of the country and can affect national resilience (Setiyadi & Keliat, 2020). This cyber counterintelligence can also be applied to an intelligence agency to strengthen the security assessment of ministries/agencies in the context of the Global Cybersecurity Index (Samad, 2021).

3.4. Discussion

The use of OSINT techniques, predominantly dorking in this research, has obtained much partial information. The pieces of information are then arranged and connected to form comprehensive information, as in Figure 1. Previously, the information obtained was minimal or did not provide any meaning. However, when these pieces of information are combined, the information obtained can be analyzed to provide meaningful meaning. Based on this, this research supports research by Tziampazis (2021), which states that data collected from OSINT results can be used to create profiles for specific targets, including behavioral characteristics. In the context of this research, I-SOON's profile can be identified, including its activities and affiliation with the APT group.

Viewed from a technical perspective, this research supports the results of Haq's (2017) research, which states that using *the Google Dorking* technique can produce accurate information, especially since the information obtained is mutually confirmed. Apart from that, this research also supports research by Abasi (2020), which states that cyber security investigators can use this technique to carry out their duties. When viewed from a utilization perspective, this research's findings align with research by Pastor-Galindo and colleagues (2020), who argue that search results via OSINT can be helpful for cyber security and resilience. In the context of this research, information about I-SOON can be used as a basis for building cyber defense and resilience for a country so that it can anticipate similar attacks, especially those from China, because the MO and TTP have been identified.

Based on the research results of Duvenage & von Solms (2013), I-SOON and its affiliates combine two main aspects of cyber attacks, namely humans and techniques. The human aspect refers to spear phishing and social engineering to obtain important information from targets, while the technical aspect refers to using RATs and ShadowPad. Findings from the OSINT investigation show that I-SOON operations are affiliated with a highly organized APT group. This affiliation is also strengthened by allegations that I-SOON tends to be linked to China to steal sensitive data and hack various important systems. The cyber espionage activities of I-SOON and its affiliates involve advanced techniques such as RATs, ShadowPad, and social engineering, indicating that they follow stages quite similar to the cyber espionage process that Rivera et al. (2022) have described, with an emphasis on reconnaissance, attacks, and information gathering. Their involvement with various universities and use of highly planned techniques show a high level of professionalism in their efforts to obtain and manipulate information from targets.

Referring to the S.P.I.E.S. taxonomy conceived by Fitzpatrick & Dilullo (2015), the situational threat refers to China's presence in operations launched by I-SOON and its affiliates capable of accessing sensitive data and intellectual property from international targets. Targeted countries include India, Thailand, Vietnam, South Korea, Indonesia, and institutions such as NATO. The existence of I-SOON linked to Chengdu 404 indicates that they have strong support from the Chinese government and links to universities and companies that support espionage activities. This threat is particularly significant as their operations focus on stealing strategic data from vital sectors, including governments, large corporations, and academic institutions.

They leveraged various penetration methodologies, including phishing and ShadowPad, to access highly valuable information from the public and private sectors in various countries. I-SOON and its affiliates exploit the capabilities of RATs to extract data and control infected systems secretly. The threat posed is enormous, to steal intellectual property, government data, and strategic business information. Based on existing data, vulnerabilities that are often exploited by I-SOON and its affiliates include vulnerabilities in mobile devices in the form of exploiting Android and iOS devices to access the target's personal data; Vulnerabilities in information technology systems by using ShadowPad and other malware to exploit vulnerabilities in poorly protected hardware or software; Use of outdated applications by exploiting vulnerabilities in applications that are no longer updated or have known security holes; and human error in the form of the use of spear phishing to exploit human emotions and negligence in accessing or opening malicious emails, which can allow malware to enter the network.

In the context of motivation for carrying out cyber espionage, the motivation for the activities of I-SOON and its affiliates tends to be financial gain, which means *money* for MICE+G and *wealth* for BEWARE. Another motivation is ideology (MICE+G) because the espionage carried out by I-SOON was driven by ethno-nationalism (BEWARE) and loyalty to the Chinese state. I-SOON operates in support of Chinese government institutions, reflecting broader ideological motives. Support from these countries allows operations to take place under Chinese authority, allowing protection and resources to be provided to them to carry out attacks with long-term objectives. In this case, the motivation is known as authority motivation in RASCLS.

The analysis results regarding the cyber espionage process and the motivation for carrying out cyber espionage become a database for determining the cyber counterintelligence strategy to be implemented. From the defensive side of cyber counterintelligence, countries and organizations targeted by APT must increase cyber security awareness at all levels of society and government agencies to reduce the successful use of social engineering on sure victims. Early detection of RATs, ShadowPad, and spear phishing is critical to reducing the chances of becoming a victim of cyber espionage. On the other hand, a cyber counterintelligence offensive in the form of an offensive approach can include cyber confrontation by counterattacking to damage infrastructure used by opposing groups or disrupt their operations. Destruction of digital traces and manipulation of their operations in cyberspace can slow down their activities and even discourage them from carrying out efforts related to cyber espionage.

Offensive and defensive approaches can be taken in a more technical direction, such as using Blockchain technology. This technology can potentially be used in counterintelligence, especially in improving information security and detecting threats to a country. Blockchain technology has features such as transparency, immutability, and decentralization (Ramadoss, 2022). It can be utilized for various defensive counterintelligence purposes because it protects data, information, and infrastructure from external threats, including state-affiliated APT activities. Meanwhile, from the offensive side, blockchain can record and track digital transactions or activities transparently. In counterintelligence, this could help track funds used by spy groups or rival organizations.

4. Conclusion

Cyber espionage by its affiliate I-SOON shows that threats can threaten state sovereignty, national resilience, and information security. Using social engineering, RATs, and ShadowPad, this group was able to penetrate vital state systems and steal sensitive information. Research proves that using OSINT techniques, especially dorking, can obtain partial information, which is compiled and linked into comprehensive information. The research results support the use of OSINT, especially the Google Dorking technique, and show its benefits for cyber security. For this reason, it is important to implement effective cyber counterintelligence measures, both defensively and offensively, one of which is by finding complete information and the motivation of the attacker through OSINT, especially docking. Apart from that, efforts are needed to increase cyber security awareness for all cyber network users to prevent exploitation, which results in more significant losses. In the international context, it is necessary to increase cooperation between countries by increasing cooperation in the field of cyber security to face threats together.

The case of cyber espionage carried out by I-SOON and its affiliates illustrates that the motivation is financial gain related to the theft of strategic data or intellectual property with high business value. Additionally, ideological motivations related to ethno-nationalism and loyalty to the Chinese state are also illustrated, so I-SOON and its affiliates operate to support China's agenda and interests. An increase in suspicious activity on a network, such as the emergence of new malware or social engineering efforts, can be early signs of a cyber espionage attack, so comprehensive intelligence analysis of information from various sources is needed to detect threats early as a form of defensive cyber counterintelligence. This research has limitations in the data studied, only a few APTs and one country so that future researchers can develop this research by examining other APT groups affiliated with several countries.

Acknowledgements

Thanks to those who helped directly or indirectly, Communication & Information System Security Research Centre (CISSReC), OSINTCombine, SIBERKU, Monash University Indonesia, Universitas Bhayangkara Jakarta Raya, K. Z. Sahela, and A. Novianto. The contributions of all parties were instrumental in the process of completing this research.

References

Abasi, R. (2020). Google dorks: Use cases and Adaption study University. University of Turku.

Aditya, A. R. M., Putri, A. W. O. K., Aditya, A. R. M., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). Global Political Studies Journal, 6(1), 35–46. https://doi.org/10.34010/gpsjournal.v6i1.6698

Adzel, Z. (2021). Analisis Tradecraft: Penggunaan Advanced Persistent Threats (APTs) Pada Operasi Spionase Siber oleh Rusia. Jurnal Penelitian & Kajian Intelijen, 2(1).

Arntz, P. (2024). A first analysis of the i-Soon data leak. Malwarebytes. https://www.malwarebytes.com/blog/news/2024/02/a-first-analysis-of-the-i-soon-data-leak

Bajak, F., & Kang, D. (2024). An online dump of Chinese hacking documents offers a rare window into pervasive state surveillance. Apnews.Com. https://apnews.com/article/china-cybersecurity-leak-document-dump-spying-aac38c75f268b72910a94881ccbb77cb

Bansal, M. (2024). Chinese APT Tactics and accesses uncovered after analyzing the I-SOON repository. Cloudsek.Com. https://www.cloudsek.com/blog/chinese-apt-tactics-and-accesses-uncovered-after-analyzing-the-i-soon-repository

Bernsen, W. (2024). Same Same, but Different. Margin Research. https://margin.re/2024/02/same-same-but-different/

Bodström, T. T. (2022). Strategic Cyber Environment Management with Zero Trust and Cyber Counterintelligence. Journal of Information Warfare, 21(3). https://www.jinfowar.com/subscribers/journal/volume-21-issue-3/strategic-cyber-environment-management-zero-trust-cyber-counterintelligence

Cary, D., & Milenkoski, A. (2024). Unmasking I-Soon | The Leak That Revealed China’s Cyber Operations. Sentinelone.Com. https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/

Chen, J. C., Lu, K., Chen, G., Horejsi, J., Lunghi, D., & Pernet, C. (2022). Delving Deep: An Analysis of Earth Lusca’s Operations. https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/a/earth-lusca-employs-sophisticated-infrastructure-varied-tools-and-techniques/technical-brief-delving-deep-an-analysis-of-earth-lusca-operations.pdf

Chengdu University of Information Technology. (2020). 2020 年“安洵杯”四川省第十二届大学生信息安全技术大赛在我校成功举办. Jwc.Cuit.Edu.Cn. https://jwc.cuit.edu.cn/info/1182/1695.htm?ref=margin.re

Ciluvi, A., Luma-Osmani, S., Rufati, E., & Arifi, G. (2022). Cyber Espionage: A Growing Threat? Journal of Natural Sciences & Mathematics (JNSM), 7(13/14), 12–20. http://nuuance.net/work/Cyber Espionage.pdf

Duvenage, P., & von Solms, S. (2013). The case for cyber counterintelligence. 2013 International Conference on Adaptive Science and Technology, 1–8. https://doi.org/10.1109/ICASTech.2013.6707493

Eftimiades, N. (2023). China’s Espionage Recruitment Motivations Getting Rid of the MICE (Issue Research Paper Series #5). Shinobi Enterprises, LLC. https://www.euintelligenceacademy.eu/sites/eia/files/2023 1204 EIA Paper 5.pdf

FBI. (2019). APT 41 Group. https://www.fbi.gov/wanted/cyber/apt-41-group

Fitzpatrick, W. M., & Dilullo, S. A. (2015). Cyber Espionage and the SPIES Taxonomy. Competition Forum, 13(2), 307–336. https://search-proquest-com.ezproxy1.apus.edu/docview/1755486045/fulltextPDF/4C279679B5C54F08PQ/1?accountid=8289

Group-IB. (2021). Big airline heist APT41 likely behind a third-party attack on Air India. Group-Ib.Com. https://www.group-ib.com/blog/colunmtk-apt41/

Haq, M. Z. ul. (2017). Googledork, Sebuah Pendekatan Lanjutan Pemanfaatan Mesin Pencari Sebagai Penunjang Literasi Informasi. Jurnal Perpustakaan, 8(1), 1. http://lontar.ui.ac.id/il/

Hastri, E. D. (2021). Cyber Espionage sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia. Law & Justice Review Journal, 1(1), 12–25. https://doi.org/10.11594/lrjj.01.01.03

Heriyanto, D. S. N. (2020). International Regulatory Vacuum of Cyber Espionage. 1st Borobudur International Symposium on Humanities, Economics and Social Sciences (BIS-HESS 2019), 436, 106–111. https://doi.org/10.2991/assehr.k.200529.022

Hsieh, Y.-J., & Chen, O. (2021). Shadowpad: A Masterpiece of Privately Sold Malware in Chinese Espionage. https://assets.sentinelone.com/c/Shadowpad?x=P42eqA

Karpf, B. (2024). The I-Soon data leak unveils China’s cyber espionage tactics, techniques, procedures, and capabilities. Thecyberwire.Com. https://thecyberwire.com/stories/05ba5c2ff18f4af5abc30ebe28c968bf/the-i-soon-data-leak-unveils-chinas-cyber-espionage-tactics-techniques-procedures-and-capabilities

Kelliher, F. (2024). China data leak spotlights cyber-spying across Southeast Asia. Nikkei Asia. https://asia.nikkei.com/Politics/International-relations/China-data-leak-spotlights-cyber-spying-across-Southeast-Asia

Krebsonsecurity. (2024). New Leak Shows Business Side of China’s APT Menace. Krebsonsecurity.Com.

Htet, K.P., Rostovcev, N., & Group-IB. (2019). APT41. MITRE ATT&CK®. https://attack.mitre.org/groups/G0096/

Rizki, M. (2022). Perkembangan Sistem Pertahanan/Keamanan Siber Indonesia dalam Menghadapi Tantangan Perkembangan Teknologi dan Informasi. Politeia: Jurnal Ilmu Politik, 14(1), 54–62. https://doi.org/10.32734/politeia.v14i1.6351

Mandiant. (2022). APT41, A Dual Espionage and Cyber Crime Operation. https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf

Merritt, D., & Mullins, B. (2011). Identifying cyber espionage: Towards a synthesis approach. International Conference on Information Warfare and Security, 180–187. https://www.proquest.com/openview/20d7ed26bf4cc3d505b398e76bf24590/1?pq-origsite=gscholar&cbl=396500

Mirza, I. M. M., Sujadmiko, B., & Shofura, A. Y. (2024). Legalitas Cyber Espionage Dalam Hukum Diplomatik (Studi Kasus Penyadapan Kedutaan Besar Australia di Indonesia pada 2013). Res Nullius Law Journal, 6(2), 154–169.

Natto Team. (2023). i-SOON: Another Company in the APT41 Network. Natto Thoughts. https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41

Pardede, B. L., Maulana, M. I., Madaniyah, A. S., T, B. W., & Sophianandita, D. P. (2024). Indonesia ’ s Response to Australia ’ s Wiretapping of Several Important People in Indonesia in 2013. Synergisia (SG), 1(1).

Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Payne, B., & Mienie, E. (2023). RASCLS vs Ransomware: a Counterintelligence Framework for Cybersecurity Education. Journal of Security, 16(8).

Pernet, C., & Horejsi, J. (2024). Earth Lusca Uses Geopolitical Lure to Target Taiwan Before Elections. Trendmicro.Com. https://www.trendmicro.com/en_us/research/24/b/earth-lusca-uses-geopolitical-lure-to-target-taiwan.html

Poireault, K. (2024). I-Soon GitHub Leak: What Cyber Experts Learned About Chinese Cyber Espionage. Infosecurity-Magazine.Com. https://www.infosecurity-magazine.com/news-features/isoon-github-leak-chinese-cyber/

Ramadhan, Y. S., & Avalokitesvari, N. N. A. N. (2022). Urgensi Kerjasama Internasional Dalam Menangkal Ancaman Spionase Siber. Jurnal Penelitian Dan Kajian Intelijen, 3(1).

Ramadoss, R. (2022). Blockchain technology: An overview. IEEE Potentials, 41(6). https://doi.org/10.1109/MPOT.2022.3208395

Rivera, R., Pazmiño, L., Becerra, F., & Barriga, J. (2022). An Analysis of Cyber Espionage

Process. In Á. Rocha, C. H. Fajardo-Toro, & J. M. R. Rodríguez (Eds.), Developments and Advances in Defense and Security (pp. 3–14). Springer Singapore.

Salehun, L. W., & Sulaiman, Y. (2019). Kebijakan Luar Negeri Indonesia dan Kepemimpinan Susilo Bambang Yudhoyono: Studi Kasus Spionase Australia. Jurnal Agregasi : Aksi Reformasi Government Dalam Demokrasi, 7(2), 147–162. https://doi.org/10.34010/agregasi.v7i2.2561

Samad, M. Y. (2021). Optimalisasi Layanan Publik Badan Intelijen Negara Dalam Perspektif Global Cybersecurity Index. Al Ulum Sains Dan Teknologi, 7(1).

Samad, M. Y., & Persadha, P. D. (2022). Memahami Perang Siber dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman di Siber. JURNAL IPTEKKOM Jurnal Ilmu Pengetahuan & Teknologi Informasi, 24(2), 135–146. https://doi.org/10.17933/iptekkom.24.2.2022.135-146

Setiyadi, B. E., & Keliat, M. (2020). Kontra Intelijen Aksi Spionase Siber Terhadap Anggota Democratic National Committee Menjelang Pemilihan Presiden AS Tahun 2016. Jurnal Kajian Stratejik Ketahanan Nasional, 3(1), 5–18. https://doi.org/10.7454/jkskn.v3i1.10032

Shaffan, A. M. (2018). Respons Indonesia terhadap Kasus Penyadapan Australia. Journal of International Relations, 4(2), 285–294.

Suratman, Y. P. (2017). Penggunaan Strategi Operasi Kontra Intelijen Dalam Rangka Menghadapi Ancaman Siber Nasional. Jurnal Pertahanan dan Bela Negara, 7(2).

Susila, M. E., & Salim, A. A. (2024). Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany. 11(1), Padjadjaran Jurnal Ilmu Hukum (PJIH).

Threatcop. (2023). APT41 (HOODOO): A Hacker Group Exploiting Google’s Red Teaming Tool. Threatcop. https://threatcop.com/blog/apt41-exploited-googles-red-teaming-tool/

Trend Micro. (2022). Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques. Trendmicro.Com. https://www.trendmicro.com/en_us/research/22/a/earth-lusca-sophisticated-infrastructure-varied-tools-and-techni.html

Tziampazis, C. (2021). Open-Source Intelligence Pro Filing, Analysis and Countermeasures. Universitat Polit`ecnica de Catalunya.

U.S. Department of Justice. (2020). Seven International Cyber Defendants, Including “Apt41” Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally. https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

Uren, T. (2024). Risky Biz Briefing: The i-SOON Data Leak. News.Risky.Biz. https://news.risky.biz/risky-biz-briefing-the-i-soon-data-leak/

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. Information (Switzerland), 6. https://doi.org/10.3390/info6020183

Wijaya, H. (2018). Analisis Data Kualitatif Model Spradley (Etnografi). Sekolah Tinggi Theologia Jaffray.

Xiaolan, S. (2019). 安洵信息技术有限公司2019秋季校园招聘简章. Universitas Xihua. https://cs.xhu.edu.cn/2a/7a/c1762a141946/page.htm