electronics

Article

Research on Cyber ISR Visualization Method Based on BGP Archive Data through Hacking Case Analysis of North Korean Cyber-Attack Groups

Jaepil Youn [1,2], Kookjin Kim [1,3], Daeyoung Kang [4], Jaeil Lee [5], Moosung Park [1,6] and Dongkyoo Shin [1,3,*]

[1] Department of Computer Engineering, Sejong University, Seoul 05006, Republic of Korea
[2] Cyber Operations Center, Republic of Korea Army (ROKA), Gyeryong 32800, Republic of Korea
[3] Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul 05006, Republic of Korea
[4] Department of Military Digital Convergence, Ajou University, Suwon 16499, Republic of Korea
[5] Korea Internet & Security Agency (KISA), Naju 58324, Republic of Korea
[6] The 2nd R&D Institute 3rd Directorate, Agency for Defense Development (ADD), Seoul 05661, Republic of Korea
* Correspondence: shindk@sejong.ac.kr

Abstract: North Korean cyber-attack groups such as Kimsuky, Lazarus, Andariel, and Venus 121 continue to attempt spear-phishing APT attacks that exploit social issues, including COVID-19. Thus, along with the worldwide pandemic of COVID-19, related threats also persist in cyberspace. In January 2022, a hacking attack, presumed to be Kimsuky, a North Korean cyber-attack group, intending to steal research data related to COVID-19. The problem is that the activities of cyber-attack groups are continuously increasing, and it is difficult to accurately identify cyber-attack groups and attack origins only with limited analysis information. To solve this problem, it is necessary to expand the scope of data analysis by using BGP archive data. It is necessary to combine infrastructure and network information to draw correlations and to be able to classify infrastructure by attack group very accurately. Network-based infrastructure analysis is required in the fragmentary host area, such as malware or system logs. This paper studied cyber ISR and BGP and a case study of cyber ISR visualization for situational awareness, hacking trends of North Korean cyber-attack groups, and cyber-attack tracking. Through related research, we estimated the origin of the attack by analyzing hacking cases through cyber intelligence-based profiling techniques and correlation analysis using BGP archive data. Based on the analysis results, we propose an implementation of the cyber ISR visualization method based on BGP archive data. Future research will include a connection with research on a cyber command-and-control system, a study on the cyber battlefield area, cyber ISR, and a traceback visualization model for the origin of the attack. The final R&D goal is to develop an AI-based cyber-attack group automatic identification and attack-origin tracking platform by analyzing cyber-attack behavior and infrastructure lifecycle.

Keywords: cyber ISR; Kimsuky; MITRE ATT&CK; BGP archive data analysis; visualization

Citation: Youn, J.; Kim, K.; Kang, D.; Lee, J.; Park, M.; Shin, D. Research on Cyber ISR Visualization Method Based on BGP Archive Data through Hacking Case Analysis of North Korean Cyber-Attack Groups. *Electronics* **2022**, *11*, 4142. https://doi.org/10.3390/electronics11244142

Academic Editors: Aryya Gangopadhyay and Rameez Asif

Received: 19 September 2022
Accepted: 9 December 2022
Published: 12 December 2022
Corrected: 12 December 2023

1. Introduction

As COVID-19 became a global issue, hackers quickly changed their attack methods. Numerous hackers, including advanced persistent threat (APT) attack groups, are actively exploiting the COVID-19 issue. Attacks that exploit COVID-19 are mainly social-engineering techniques and phishing attacks, and are classified into four types of cyber threats: malicious code, phishing site, financial scam, and malicious app distribution, according to the behavior required by users. In addition, most of the APT attack groups attempt attacks using malicious codes and malicious apps [1–3]. A North Korean hacker group is implementing a strategy of attacking APT after infiltrating the target system with

a spear-phishing strategy that exploits social issues, including COVID-19. In January 2022, a hacking attack, presumed to be Kimsuky, a North Korean cyber-attack group, intended to steal research data related to COVID-19. In addition, in August 2022, an attack aimed at stealing information took place against the Russian Ministry of Foreign Affairs, and in October 2022, it targeted foreign and defense professors and North Korean civilian experts. Kimsuky is currently performing the most active cyber-attack, and the US Cyber Security Office continues to warn of "the danger of North Korean Kimsuky APT attacks" [2,3].

The problem is that the activities of cyber-attack groups are continuously increasing, and it is difficult to accurately identify cyber-attack groups and attack origins only with limited analysis information. Analyst's scope is narrow due to the lack of analysis data, and it is difficult to trace the origin of cyber-attack groups and analyze associations. In addition, only a small number of known attack groups is being identified, depending on the capabilities of the analyst. As it takes too much time to respond with limited manpower and manual analysis, the reliability of analysis results decreases.

To solve this problem, it is necessary to expand the scope of data analysis by using BGP archive data. It is necessary to combine infrastructure and network information to draw correlations and to be able to classify infrastructure by attack group very accurately. Network-based infrastructure analysis is required in the fragmentary host area, such as malware or system logs. In response to this need, we have proposed a cyber ISR visualization method to quickly identify, track, and respond to cyber-attack origins with various analysis information.

The importance of the proposed solution is that when a cyber-attack occurs using a model to trace the origin of a cyber-attack, it is the most important element to visually show in connection with network infrastructure information. Through this, it is possible to trace the origin of the attack, identify the attack group quickly, and respond effectively.

In this paper, a profiling technique was used to analyze attack cases of distributing malicious documents attached to the hacking mail of the North Korean cyber-attack group Kimsuky, which attempted to steal research data related to COVID-19 in January 2022. Furthermore, the origin of the attack was estimated by analyzing the association based on cyber information collection data using border gateway protocol (BGP) archive data.

Most of the previous studies were cases in which various visualization methods were applied for cyber situation awareness. However, it did not consider the cyber ISR performance process and had limitations in focusing on visualizing anomaly detection for cyber threats. As for the academic significance of this study, the actual hacking cases of North Korean cyber-attack groups were analyzed using profiling techniques. By applying the MITRE ATT&CK framework, attack procedures, attack tactics, and attack techniques were derived. Through this, the cyber ISR process and visualization elements were established. Furthermore, we designed a framework architecture for cyber ISR visualization based on various related data, including BGP archive data, and this is the first case of visualizing it in a prototype form. It is expected that it will make great academic contributions to the fields related to cyber command and control systems and cyber operation systems in the future.

The remainder of this paper is organized as follows. Section 2 deals with research content focusing on visualization research cases for cyber intelligent surveillance and reconnaissance (ISR). Section 3 deals with research on the hacking-case profiling analysis of North Korean cyber-attack groups for cyber ISR battlefield visualization. Section 4 covers the research on the implementation of a model that traces back the origin of the attack on the Kimsuky group through the visualization of the cyber ISR battlefield based on the BGP archive data. Through this, we propose a method to visualize cyber ISR based on BGP archive data. The conclusion is presented in Section 5.

2. Related Works

In Section 2, cyber ISR overview is explained and research cases are reviewed through the latest references related to cyber ISR visualization for cyber situational awareness (SA). Fifteen domestic and foreign research cases from 2006 to the present related to cyber ISR

visualization for cyber situational awareness were reviewed. In addition, each study was analyzed in detail by dividing it into visualization technology, core function, visualization level, and use case. The BGP Route View Project related to the BGP archive data, which is the basis of this study, is explained. In addition, for profiling analysis, hacking trends by North Korean cyber-attack group and research cases on backtracking of cyber-attacks are reviewed. The related research is described to enhance readers' understanding and to increase the importance and qualitative value of research.

2.1. Cyber ISR Overview

The fifth battlefield, the cyber battlefield, is a battlespace to defend against attacks such as disturbing, rejecting, controlling, and destroying the enemy's information system in a virtual space where digitized information is circulated. Cyber operations in cyber space are carried out under the concept of cyberspace activities, which are cyber-attack, cyber defense, cyber ISR, and cyber operation environment [4,5]. Cyber intelligence is the result of analyzing collected information for a specific purpose. Cyber surveillance refers to intensive observation while observing a target, and cyber reconnaissance refers to actions to achieve a specific goal for a specific target. Cyber target selection and information are collected through cyber ISR. For successful cyber operations, we support the commander's correct decision-making by collecting and analyzing information on allied and enemy forces [5]. As a result, the process of cyber command and control (C2), cyber defense, and cyber battle-damage assessment (BDA) are carried out through cyber ISR. In addition, the process of collecting and analyzing cyber information that can deliver useful information is very important.

2.2. Related Work on Cyber ISR Visualization for Cyber Situational Awareness

The concept of cyber SA in the US joint doctrine refers to current or predictable knowledge of cyberspace and the operational environment and cyberspace on which cyber operations depend, including all factors that affect cyberspace and allies and enemies [5,6]. Using the common operational picture (COP), the commander continuously evaluates the operational environment through intelligence on troops in the operating environment, reporting functions, personnel monitoring, threat warning, and various activities. The defense network is the primary means of collecting information used by commanders to recognize the operational environment's situation, including the current system status. Therefore, managing the collection means, communication channels, information programs (data feed), user interfaces, etc., of the defense network is a major activity of the defense network operation [5,6].

The realm of cyber operations is gradually expanding from domestic to global. It is difficult to identify an enemy that quickly adapts to a constantly changing operational environment. For this reason, commanders must be aware of the situation accurately and comprehensively for rapid decision-making. For effective cyber SA, BGP archive data, which are data collected from network collection centers worldwide, are utilized, and open-source intelligence (OSINT) information, which is public-source information applying cyber battlefield information-analysis theory, must be quickly fused and linked to visualize. A typical case of cyber ISR visualization research for cyber situation recognition was analyzed, as shown in Table 1. Through theoretical consideration, each research case was analyzed by a visualization technique, core function, level of detail, and use cases.

Table 1. Visualization work related to cyber ISR for cyber SA.

Year	Work	Visualization Techniques	Core Function	Level of Detail	Use Cases
2006	"BGP Eye," Soon Tee Teoh et al. [7]	Node-link diagram, 3D display, matrix, charts	Alternative graph layouts, home-centric view, event classification, clustering	Multiple views	Routing change detection, prefix hijacking
2008	"BGPeep," James Shearer et al. [8]	Prefix visualizer using line-based visualization	Timeline, tag cloud	Low-level IP view	Reveal potential router misconfiguration, route flapping, prefix hijacking
2012	"VIS-SENSE," Ernst Biersack et al. [9]	Charts, timelines, map	Open for public usage, web-based implementation	Multiple AS views	Getting historic details for AS or specific IP prefixes
2016	"MN CD2-WP2," William. Heinbockel et al. [10]	XML-based GraphML, cyber resiliency analysis methodology, GeoMap	Crown jewels analysis, cyber command system, CyGraph, SCENARIO	Multiple AS views	Combines isolated data and events into an ongoing overall picture for decision support and SA
2016	"Bigfoot," Syamkumar et al. [11]	Internet Atlas web-based UI, 2D polygon, ArcGIS	Anomaly detector, inconsistency solver, analyze and visualize BGP updates	High-level AS view	Visualizing the announcements of network prefixes via IP geolocation
2018	"Global Geo-IP Changes," Alex Ulmer et al. [12]	React/D3.js, timelines, graph, GeoMap	Statistics/detail view, information on changes in IP between two points in time	Multiple AS views	Provides insight into the global distribution of IP blocks
2018	"A Scalable Framework," R. Vinayakumar et al. [13]	Charts, graph, timelines, map	Web-scale analysis in near real-time, capable of analyzing more than 2 million events per second	Multiple AS views	The scalability and real-time detection of malicious activities from early warning signals
2019	Paulo Fonseca et al. [14]	Charts, timelines, graph, GeoMap	Extracts volume and AS path, ML methods to BGP control plane data, observation of BGP traffic changes	Multiple AS views	BGP behavior can be used to distinguish regular traffic from anomalies, different types of anomalies
2020	"BigBen," Syamkumar et al. [15]	OWD Graph, GeoMap, ESRI ArcGIS, geographic footprint visualizer	Cloud-based implementation, cluster OWD graph visualizer, daily report generator	Multiple AS views	Process large NTP data sets and provide daily event reporting
2020	"Upstream Visibility," Massimo Candela et al. [16]	Stacked area charts, graph, heuristics	Global/local/graph animation view	Multiple AS views	Identify visual patterns that can be used to spot networking issues
2020	"Botnet Detection System," R. Vinayakumar et al. [17]	Module of data visualization (scatter/histogram /density plot), charts, graph	Similarity measures of DNS queries, classify normal and abnormal domain names	Multiple-layer view	Various methods have been used to understand the characteristics of data sets and visualize embedded features
2021	"Cyber ISR Framework," Jaepil Youn et al. [18]	Elastic stack, timelines, GeoMap, BGP di-graph	Cyber IBP analysis, anomaly detector, BGP/OSINT fusion	Multiple levels AS/Netblock /IP views	Cyber warfare map, BGP hijacking detection, routing change

Table 1. *Cont.*

Year	Work	Visualization Techniques	Core Function	Level of Detail	Use Cases
2022	"LSTM Stacking Model," Filipe Fernandes et al. [19]	GeoMap, charts, graph	Time-series forecasting, time-series with nonlinearities, predict future of a specific variable	Multiple-layer view	Used to forecast the growth of the pandemic of COVID-19, based on the increase in the number of infections and deaths in the State of Brazil
2022	"Fog and Blockchain SW," Humberto Jorge De Moura Costa et al. [20]	Charts, graph, XML, GeoJSON	Blockchain platform (hyperledger), latency, scalability, data integrity, privacy	Multiple-layer view	Used an approach based on network latency, software scalability, blockchain, and fog-computing technologies
2022	"MLPA (Multi Layers Protection Approach)," Nachaat Mohamed et al. [21]	Node-link diagram, charts, graph	Detect APT attacks based on central processing unit utilization, entire information of APT attack	Multiple-layer view	Implementing the CPU utilization method based on the "Mimi Katz" malicious application in the credential-dumping technique on all internal devices

Soon Tee Teoh et al. (2006) [7] proposed a model called BGP Eye, a visualization tool for analyzing the root cause of BGP abnormalities. Unlike previous approaches, BGP Eye analyzed BGP's abnormal symptoms in real-time through hierarchical analysis. In addition, through several valuable points, it provided the ability to analyze BGP anomalies on the Internet-centric view and the home-centric view of a specific autonomous system (AS). James Shearer et al. (2008) [8] proposed a model called BGPeep that visualizes BGP traffic at a detailed level using a novel depiction of internet protocol (IP) space. This tool highlights aspects of BGP archive data that have received less attention in previous visualization applications to help form a complete picture of an important part of the Internet communications infrastructure. Ernst Biersack et al. (2012) [9] proposed the VISSENSE model for analysts to detect abnormal routing patterns in vast amounts of BGP archive data through network visualization. Emphasis was placed on how to visualize BGP monitoring to identify prefix-hijacking attacks through malicious intent. Heinbockel et al. (2016) [10] proposed a model called MN CD2-WP2, a hierarchical graph-based tool that shows interdependencies between mission objectives, operations, information, and cyber assets. It was developed based on military scenarios at the strategic level within a structured methodology for cyber resilience analysis. Syamkumar et al. (2016) [11] proposed a model called Bigfoot, a BGP update-visualization system designed to highlight and evaluate various actions in an update stream. It is a concept to visualize network prefixes through the geographic location of an IP and was developed to filter, organize, analyze, and visualize BGP updates so that the characteristics and behaviors of interest can be effectively identified. Alex Ulmer et al. (2018) [12] proposed a model called Global Geo-IP Changes, an interactive visualization system that relies solely on Geo-IP data to raise awareness of data sources. Over time, it was developed to analyze suspicious cases through an IP-block owner and location information in Geo-IP data. Vinayakumar et al. (2018) [13] proposed an extensible framework model for cyber threat situational awareness based on domain-name-system data analysis. Web-scale analytics can be performed in near real-time, analyzing more than 2 million events per second. It was developed for the purpose of confirming and detecting malicious activity in real-time from early warning signals. Paulo Fonseca et al. (2019) [14] proposed a model that can simply observe the volume and AS route functions and BGP traffic changes most commonly used in BGP anomaly-detection technology. It was developed to analyze the trend of BGP behavior that can be used to distinguish abnormal behavior and various types of abnormal traffic and general traffic.

Syamkumar et al. (2020) [15] proposed a model called BigBen, a network telemetry-processing system designed to report Internet events (interruptions, attacks, configuration changes, etc.) in an accurate and timely manner. It was developed to identify a wide range of Internet events, characterized by location, range, and duration, and to compare detected events with events detected by large, active probe-based detection systems. Candela et al. (2020) [16] proposed a model called Upstream Visibility for scenario-based monitoring of Internet events (interruptions, attacks, configuration changes, etc.). The global view based on the stack-area chart provides a high trend for the visibility of IP prefixes and has been developed to provide a local view to check the impact of IP prefix-visibility time. Vinayakumar et al. (2020) [17] proposed a deep learning-based visualized botnet-detection system for the Internet of Things in smart cities. Based on deep-learning architecture, a domain-generation algorithm is applied to classify normal and abnormal domain names. Various methods have been used to understand the characteristics of data sets and visualize embedded features. In addition, significant improvements have been made in terms of detection speed and false-alarm rate. Youn et al. (2021) [18] proposed a cyber IPB-visualization model based on BGP archive data for cyber situational awareness. BGP archive data were analyzed and preprocessed and a cyberspace prototype was implemented in the form of a di-graph based on the elastic stack. It has established battlefield-visualization elements for the three layers of cyberspace and is characterized by applying "cyber intelligence preparation of the battlefield (IPB)." Fernandes et al. (2022) [19] proposed a high-efficiency model for time-series prediction of LSTM (long short-term memory). It can handle large amounts of data in time series with non-linearities and was developed to be used to predict future growth based on the increase in a specific variable. De Moura Costa et al. (2022) [20] proposed a fog and blockchain software architecture for making accurate decisions. To make fast and accurate decisions, an approach based on network latency, software scalability, blockchain, and fog computing technologies was used. With this, a decentralized infrastructure was developed to enable scalable solutions. Mohamed et al. (2022) [21] proposed a model for multi-layer protection-approach (MLPA) detection for advanced persistent threat detection. Using MITRE ATT&CK, the MimiKatz malicious application was used as a credential-dumping technique for all internal devices. It was developed to apply the approach to the entire infrastructure, starting with implementing CPU utilization methods.

2.3. BGP Route View Project Overviews

The BGP is a protocol for exchanging routing information, which is IP prefix connection information, and is a protocol that is the basis for gateway hosts around the world. Oregon University's Route Views Project is the best repository of BGP routing data and plays an important role in understanding the global Internet routing system. Starting with the accumulation of routing information since 2001, BGP routing information transmitted from more than 140 peer-observation monitors from a total of 24 collection points has been collected and recorded in the form of BGP archive data [18,22]. Many studies have been done on BGP routing analysis. Among them, CAIDA's AS Core Internet Graph research is representative [22]. BGP routing information analysis produces diverse information, such as topology changes, routing connections, network instability, network threats, and network attributes [22–26]. Through this, the BGP archive data accumulated in the BGP Route View Project (http://archive.routeviews.org (accessed on 1 June 2022)) are utilized for research.

2.4. Hacking Trends by North Korean Cyber-Attack Groups

According to a recent analysis of cyber threat cases based on public information, Kimsuky is the most active in cyber-attacks by North Korean attack groups, and in Lazarus, including Andariel, many infringement indicators have been identified compared to cyber-attacks. In addition, Venus 121 has slowed its activity against cyber-attacks and infringement indicators [1–3]. To confirm the attack pattern of each attack group, as shown in

Table 2, the main attack targets, types, and techniques for each North Korean cyber-attack group were analyzed.

Table 2. Major targets and techniques for each cyber-attack group in North Korea.

Attack Group	Target	Attack Type	Attack Technique
Kimsuky	North Korean adversary, COVID-19, politics, defense, cryptocurrency	It collects strategic information related to North Korea, such as national defense, security, and nuclear security, from key government and military personnel, and continuously attacks domestic foreign policy and national-security secrets. Representatively, Korea Hydro and Nuclear Power were hacked in 2014, and attacks that exploited the COVID-19 pandemic have been continuously attempted since 2020.	Attacks using social engineering, spear phishing, and watering-hole techniques (targeted attacks, APT attacks, new malware (KGH_SPY, CSPY) attacks that bypass vaccine products).
Lazarus	COVID-19, defense, finance	Mainly targeting the financial sector and hacking by infiltrating the computer networks of domestic and foreign financial institutions to steal financial information. They hacked the Central Bank of Bangladesh in 2016, the Bank of Chile in 2018, and USD 400 million worth of cryptocurrencies in 2021.	Online job-search platforms (LinkedIn) perform attacks based on the trust of targets, such as spear-phishing techniques that disguise personnel in charge and transmit job-change proposals.
Andariel (a subgroup of Lazarus)	Defense, finance, cryptocurrency	Performing information-gathering missions for defense and defense industries, security companies, and ICT companies. A cryptocurrency-user remote support-solution attack was carried out in 2017. Recently, gambling games, ATMs, financial companies, and travel agencies have been hacked for economic gain.	The ransomware is designed to encrypt all files on the system except the ".exe," ".dll," ".sys," ".msiins," and ".drv" extensions that are important to the system in exchange for payment in bitcoins. Sets a unique key to decrypt and unlock scrambled files.
Venus 121	North Korean adversary	Attempt to steal information on contest participants.	Dissemination of hacking emails with document-type malware attached.

As North Korea has recently officially secured a COVID-19 vaccine through international organizations, it is expected that Lazarus' attacks on the theft of COVID-19 vaccine information will increase further [3].

In addition, the possibility that bitcoin, a cryptocurrency that can play a role as a new safe asset replacing gold, is emerging, and continuous hacking attacks aimed at stealing cryptocurrency are expected [1,3].

2.5. A Study on Cyber-Attack Traceback

Yogesh et al. (2020) [27] built Root Tracker, a network forensics framework for identifying real sources of cybercrime beyond network Internet service providers (ISP). This was done in a real-time environment to identify the attacker's device and generate a partial-evidence-match report, even if the attacker formats the system or modifies device parameters. Nur et al. (2021) [28] proposed an AS trace-packet marking technique to infer the AS-level forward path from the attacker to the victim site. Using this, it was shown that the victim site can construct an AS-level forwarding path from the attacker site after receiving a single packet. Nur et al. (2018) [29] proposed a probabilistic packet-marking method that infers a forward path from an attacker site to a victim site and allows the victim to delegate the defense to an upstream Internet service provider. This was implemented by utilizing the record path function of the IP protocol, and compared to other technologies, it showed that the number of packets required to construct a path from the attacker site to the victim site is small. Wang et al. (2018) [30] proposed a countermeasure against specifically targeted ransomware by trapping the attacker through a network deception environment and then using a backtracking technique to identify the attack source. The deception environment consisted of an analysis system that collects tracking clues and automatically extracts and analyzes the collected clues while trapping the attacker.

3. Hacking Case Profiling Analysis of North Korean Cyber-Attack Groups for Cyber ISR Battlefield Visualization

A sequence diagram was conceived to profile and analyze the hacking cases of North Korean cyber-attack groups. Following this procedure, we first analyzed the attacker's

behavior based on the MITRE ATT&CK framework. We extracted actual North Korean infringement indicators by profiling and analyzing Kimsuky phishing attacks that exploited the COVID-19 vaccine issue. In addition, malicious HWP document-structure analysis was performed and malicious phishing sites and C2 servers were analyzed. The information obtained through this process was used for visualization implementation and verification.

3.1. Sequence Diagram for Hacking Case Profiling Analysis

As COVID-19 spreads around the world, cyber threats that exploit this situation in cyberspace continue. Attackers are conducting various types of attacks, such as distributing malicious codes and malicious apps, leaking personal information, and committing financial fraud using social-engineering techniques that exploit COVID-19, such as phishing and smishing. In particular, amid the ongoing cyber-attacks targeting domestic medical personnel, the cyber threat to steal related research data continues as the domestic COVID-19 vaccination becomes visible. Entering the second half of 2020, changes in the Hangul Word Processor (HWP) document file attack technique were detected. It changed from the PostScript method, which has been widely used in the past, to the object linking and embedding (OLE) method [1]. OLE means object connection and insertion, and the HWP application uses the word expression of the entity instead of the object. Accordingly, an in-depth analysis looked at hacking cases presumed to be the North Korean cyber-attack group Kimsuky.

The procedure for in-depth analysis of hacking cases of North Korean cyber-attack groups is shown in Figure 1.

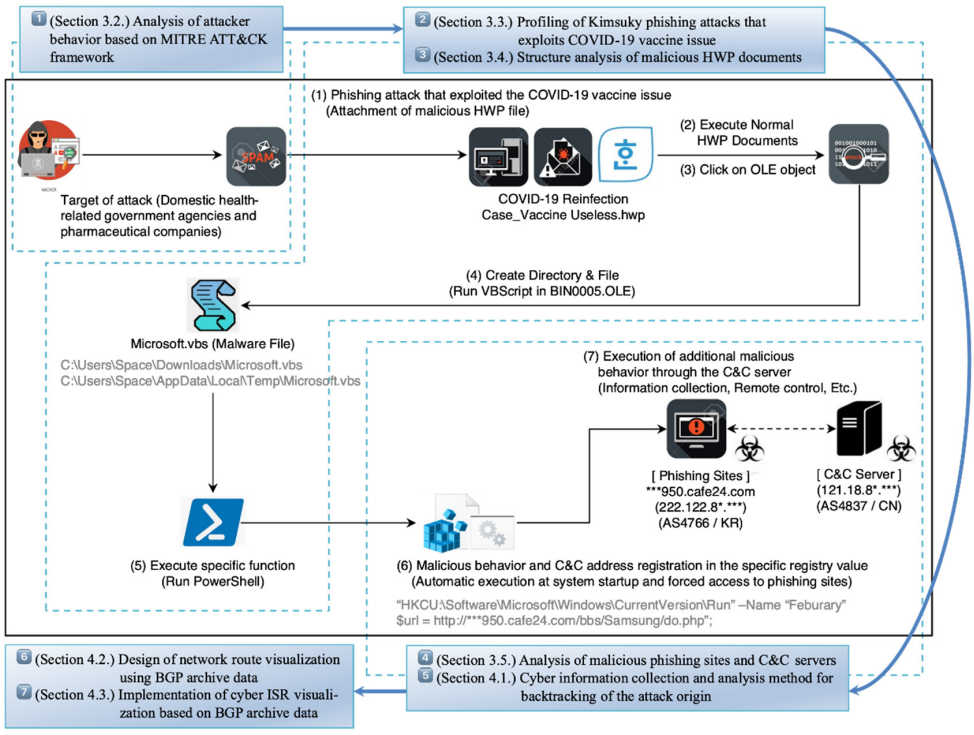

Figure 1. Sequence diagram for profiling Kimsuky's phishing attack.

-- First, the MITRE ATT&CK framework is applied to analyze the attacker's behavior. Through this, the tactics and strategies of each North Korean hacker group are predicted.

--Second, an in-depth analysis of hacking cases presumed to be Kimsuky, a North Korean cyber-attack group, is conducted using profiling techniques.

--Third, the malicious code structure of the HWP document is analyzed. Through this, the malicious function and the purpose of the attacker are identified.

--Fourth, phishing sites and C2 servers that have been exploited are analyzed through malicious code analysis.

--Fifth, based on the BGP archive data, cyber information collection and analysis are performed to trace the origin of the attack.

--Sixth, we visualize the di-graph-based network path through cyber information collection and analysis.

--Seventh, we implement cyber ISR visualization based on the prototype architecture. Through this, the origin of the attack from the North Korean cyber hacking group is identified and estimated.

3.2. Analysis of Attacker-Behavior Based on the MITRE ATT&CK Framework

Recently, North Korean hacker groups have continuously attempted spear-phishing attacks that exploit social-engineering attack techniques and social issues. As shown in Table 3, tactics and strategies for each North Korean hacker group were predicted through attacker behavior analysis based on the MITRE ATT&CK framework for related cases. In particular, the study focused on phishing hacking cases from Kimsuky, a North Korean cyber-attack group.

Table 3. Analysis of attacker behavior based on the MITRE ATT&CK framework.

Tactic	Analysis of Attacker Behavior
Reconnaissance	Collection of information by selecting targets for attack and building various websites, SNS, search engines, and phishing pages.
Resource development	Establish infrastructure to be used for attacks and develop attack tools, malware, and trust accounts.
Initial access	Send phishing emails with malicious codes and malicious links attached, or utilize publicly disclosed vulnerabilities.
Execution	Execute the CMD command desired by the attacker and execute additional malicious code.
Persistence	Automatic execution of malicious code through the registry, and downloading of malicious code through task scheduler.
Credential access	Stealing account information through keylogging or stealing password-saving files.
Defense evasion	Disguise malicious code and attacker's server address bypass security program, delete infringement indicators.
Lateral movement	Sending emails impersonating internal employees.
Collection of internal information	Keylogging, screen-capture function stealing internal information.
Exfiltration	Divide data to minimize traffic exposure when information is leaked and leaked through web services.

3.3. Profiling of Kimsuky Phishing Attack That Exploits COVID-19 Vaccine Issue

It is estimated that in January 2022, the North Korean cyber-attack group Kimsuky deployed a malicious HWP file to steal information to exploit the COVID-19 vaccine issue [3]. The distribution targets were employees of domestic health-related government agencies and pharmaceutical companies, and the attack technique used a tactic of distributing hacking emails and operating phishing sites by attaching a malicious HWP file with a malicious OLE entity inserted in the email [31–34]. The threat actor induces curiosity in the recipient when sending an attack email and induces them to download and execute the attached file titled "COVID-19 Reinfection Case_Vaccine Useless.hwp," as shown in Figure 2.

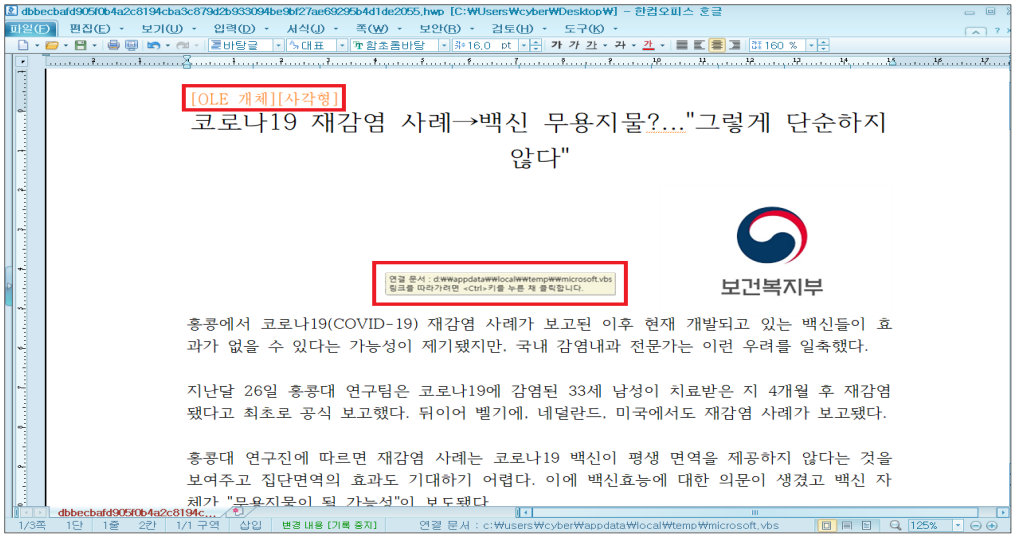

Figure 2. Execution screen of malicious HWP file using a news article.

The malicious-code-insertion HWP document uses the contents of the domestic medical media as they are and has the characteristic of being disguised as a document issued by a government agency using the logo of Korea's Ministry of Health and Welfare. The document does not show any special features to the naked eye, but in fact, the square-shaped transparent entity is set to the size of the entire area. When the transparent entity is clicked, the malicious executable OLE file (Microsoft.vbs) included in the HWP document is called.

To summarize the phishing-attack process, a malicious HWP document is attached to an email and delivered to the attack target. It was designed to go through the process of inducing execution after inserting the malicious module in the document by exploiting the normal OLE function, which is not a security vulnerability [34–36]. In particular, since the OLE method is not a security-vulnerability technique, there is a possibility of risk exposure even if the latest product and updated version are used.

As a result of applying the ATT&CK Framework to the phishing attack that exploited the COVID-19 vaccine issue, the ATT&CK-based attack technology exploited by the Kimsuky group was analyzed as shown in Table 4.

Table 4. ATT&CK-based attack technology exploited by Kimsuky.

Tactic	Platform	ID	Technology Name of Top Level	Technology Used	Data Source
Execution	Windows	T1059	Command and scripting interpreter	PowerShell (T1059.001)	PowerShell Log, parameters, process command line, process monitoring, Windows event log
Collection	Windows	T1005	Data from local system	Command and scripting interpreter (T1059) Automatic collection (T1119)	File monitoring, parameters, process command line, process monitoring log
Exfiltration	Windows	T1041	Exfiltration through the C2 channel	Email C&C channel	NetFlow/Enclave NetFlow, packet capture, process monitoring, process use of network
Initial access	Windows	T1566	Phishing	Attachment file (T1566.001) Malicious link (T1566.002) Service abuse (T1566.003)	Anti-virus, SSL/TLS inspection, web proxy, detonation chamber, email gateway, file monitoring, mail server, NIDS, packet capture, DNS records
Discovery	Windows	T1082	System information discovery	System info tool	Process CLI, parameters, process monitoring, stack-driver logs

3.4. Structure Analysis of Malicious HWP Documents

The following analysis shows the malicious codes that were added to the HWP document and the functions they perform. The malicious HWP files used for analysis related to phishing attacks were obtained through cooperation with the private security-response center. To check the reliability of the malicious file used for hacking, it was also obtained through the dark web and a hash-value comparison process was performed. Table 5 shows the properties of the "COVID-19 Reinfection Case_Vaccine Useless.hwp" file attached to the email.

Table 5. Property information of malicious HWP documents and malicious OLE files.

Document Name	Malicious File Name	File Type (Capacity)	C2 Domain (IP Address)	MD5
COVID-19 Reinfection Case_Vaccine Useless.hwp	Microsoft.vbs	VBA/5.15 KB (5263 bytes)	***950.cafe24.com (222.122.8*.***)	72e5b8ea33aeb083 631dle8b302e76af

Looking at the internal structure of the HWP document in Figure 3, the "BIN0005.OLE" stream is included. The "BIN0005.OLE" stream contains a malicious file designated by the "Microsoft.vbs" file name inside.

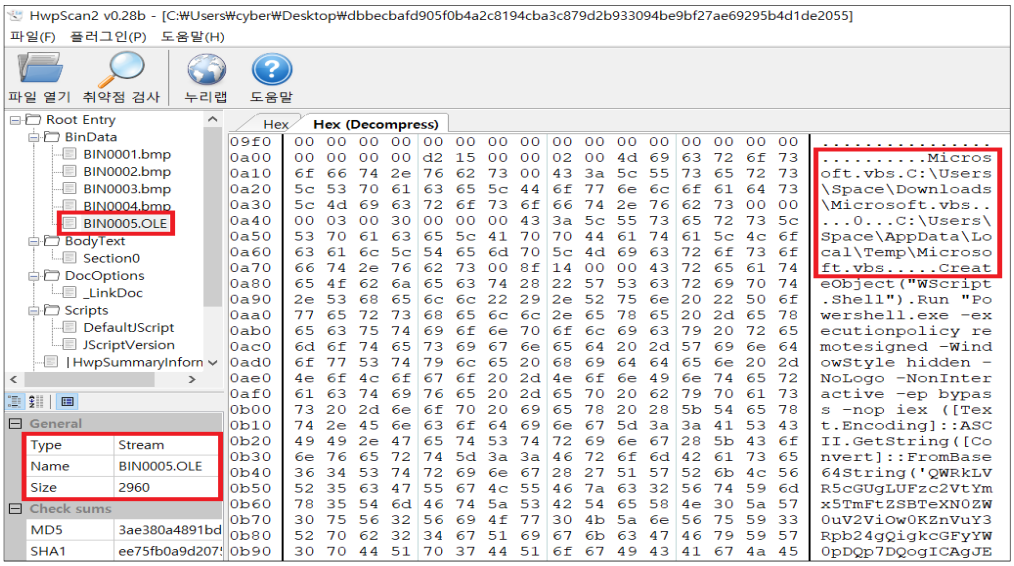

Figure 3. Malware screen included in the "BIN0005.OLE" area.

Looking at the visual basic script (VBS) code of the "Microsoft.vbs" malicious file, the main functions and core routines are encoded in Base64 and hidden as shown in Figure 4. Then, when the code is executed, decoding is performed and loaded into the memory, and then additional commands are executed by bypassing the detection of security devices [36,37].

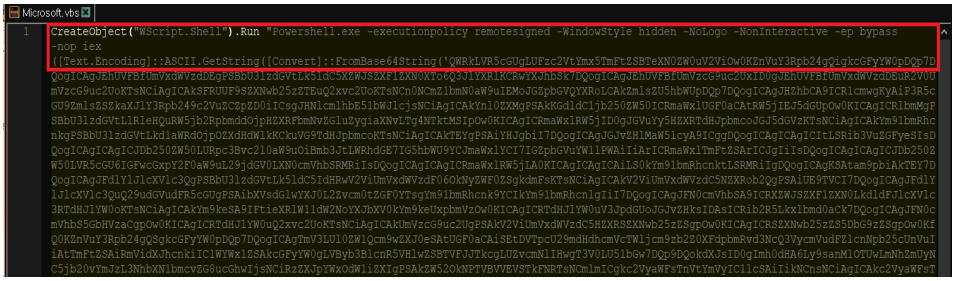

Figure 4. PowerShell command and Base64 encoding screen of the malicious file (Microsoft.vbs).

In addition, as shown in Figure 5, there is a command register in the registry named "February" in the Run value and is set to run automatically when the system starts. It secretly communicates by combining the PowerShell command and the encrypted C2 server address (http://***950.cafe24.com/bbs/Samsung/do.php (accessed on 1 January 2021)).

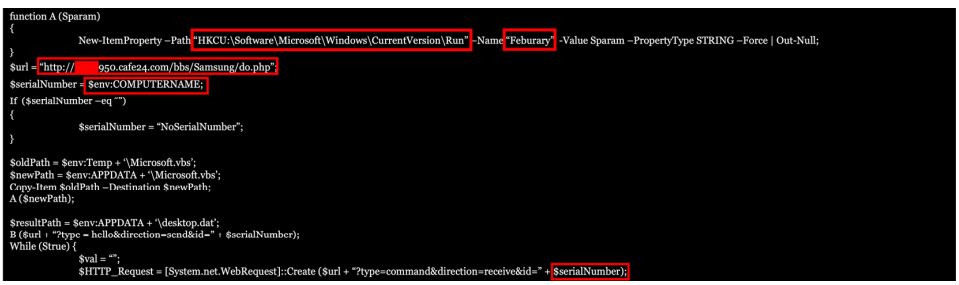

Figure 5. Registration screen of registry and screen for setting communication with C2 server.

In addition, as shown in Figure 5, the script communicates with the C2 server using the computer name of the attack target. Through this, actions such as information stealing and remote control can be performed according to additional responses and commands prepared by the threat actor [34,35].

3.5. Analysis of Malicious Phishing Sites and C2 Server

The C2 server identified through malicious-code analysis was a private site (Korea NICE credit information) for a debt-collection service using a domestic hosting company. In addition, a space for the attack was built in the server after taking authority of the poorly managed web server. As a result of searching for all virus information about the domain and IP of the server, as shown in Figure 6, the domain was discovered to be http://***950.cafe24.com (accessed on 1 January 2021), the IP 222.122.8*.***, and the AS 4766 (KR).

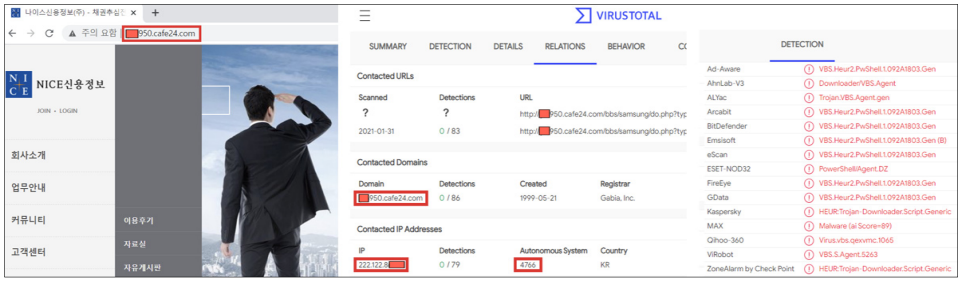

Figure 6. Screen of malicious phishing sites and total virus information.

After analyzing the web access and error log for the abused C2 server, a list of attack IPs in the victim server was identified and is shown in Table 6.

Table 6. Attack IP range confirmed on the abused server.

Section	Access IP	Collection Type	Who	ASN
C2 Server	121.18.8*.***	Web Log	China (CN)	AS4837/ China Unicom 169

4. Implementation of Kimsuky's Attack-Origin Backtracking Model through Cyber ISR Battlefield Visualization Based on BGP Archive Data

Section 4 describes cyber information collection and analysis methods for tracing the attack origin back. Through this, network path visualization was designed based on BGP archive data, and cyber ISR visualization implementation are described.

4.1. Cyber Information Collection and Analysis Method for Backtracking of the Attack Origin

Network forensics was carried out to identify abnormal behavior in network flow through packet analysis. In addition, through Maltego, the topology object was checked from the North Korean network topology view to the terminal OSINT information, and through this process, the effectiveness of the cyber ISR and the backtracking process for the origin of the attack was verified. In the case of hacking attacks, North Korea mainly uses it as a technique to bypass the IP through various transit points, and many reports also state that bypassing IPs through proxy servers is a general technique [38,39].

However, due to the advancement of the backtracking technique, the IP backtracking method is effective, and the backtracking technology is largely classified into two types. First, it is an IP-packet backtracking technology to identify the distributed denial of service (DDoS) attack point, and second, there is a TCP-connection backtracking method that is mobilized to identify the target according to the bypass attack. Each technology has its limitations, but it is still an important method in discovering the subject of hacking through IP analysis as it overcomes the technical difficulties [39].

Two types of IP ranges frequently appear in relation to North Korean hacking, as shown in Table 7. One is the IP band of North Korea's Ministry of Posts and Telecommunications, which is renting and using the Internet of China, and the other is the IP band managed by Star Joint Venture. Star Joint Venture is a joint venture between North Korea's Ministry of Posts and Telecommunications and Thailand's Loxley Pacific Group. If

the computer IP address mobilized for hacking is included in the band, the government presumes that it was North Korea's actions [39].

Table 7. List of hacking IP ranges in North Korea.

Section	IP Ranges	ASN	Nation
China Unicom IP	121.16.0.0~121.18.88.255	AS4837	China (CN)
Star Joint Venture IP	175.45.176.0~175.45.179.255	AS131279	North Korea (KP)

Through this analysis, the attacking IP 121.18.8*.***, which was identified in the web-access log of the server abused as a phishing site, was identified as an AS4837 node managed in China.

4.2. Design of Network Route Visualization Using BGP Archive Data

After the data-processing process to convert the published BGP, OSINT, and IP geolocation data into GeoJSON format, an integrated intelligence DB for visualization was built, and the structure was designed to be linked with ElasticSearch and Kibana's ElasticMap, as shown in Figure 7 [40]. Although only fragmentary host-area information was analyzed, it was designed to analyze the cyber-attack lifecycle through network-area information analysis. It was identified with the analyst's manual analysis, but it was designed to implement macroscopic visualization through network characteristic information. Limited individual information for each institution was collected and analyzed, but based on BGP archive data, TTPs and MITRE ATT&CK of various cyber-attack groups were combined. Through this profiling analysis data was used to verify and to see new information inside.

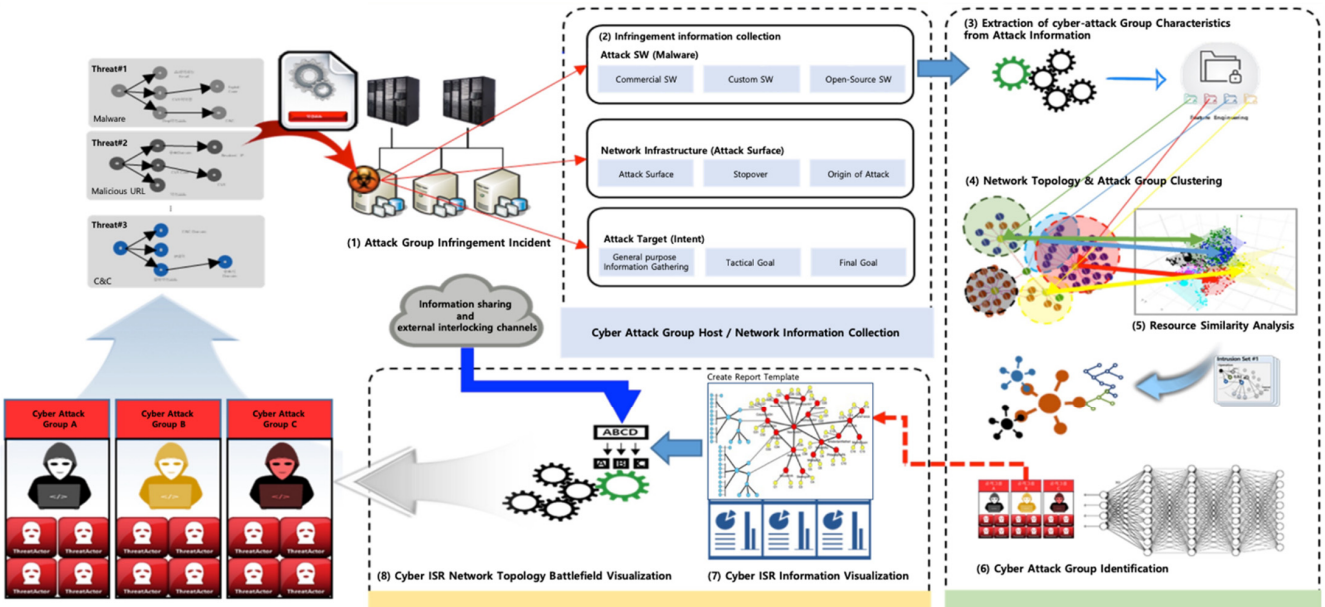

Figure 7. Design of cyber ISR visualization framework architecture. (Adapted from Go et al. Proc AIS 2022; p. 9, with permission from Dailysecu Press [40].)

To visualize the global network based on GeoMap, first, the BGP archive data must be dumped and pre-processed. For this research, the BGP archive data used the Route Views Project Repository of the University of Oregon, which has been evaluated as the best in the world. To shorten the data-preprocessing process, a Python-based BGP archive-data downloader and a BGP archive-data parser were created as programs and used in the research process. After executing the program, the parsing data that went through the preprocessing process were extracted and built into an integrated DB, as shown in Figure 8 [40]. Information related to cyber-attacks was collected as data, pre-processed, and organized

into a DB for management. The collection channel of information related to attack behavior and infrastructure was expanded, and the DB for data relation configuration was expanded.

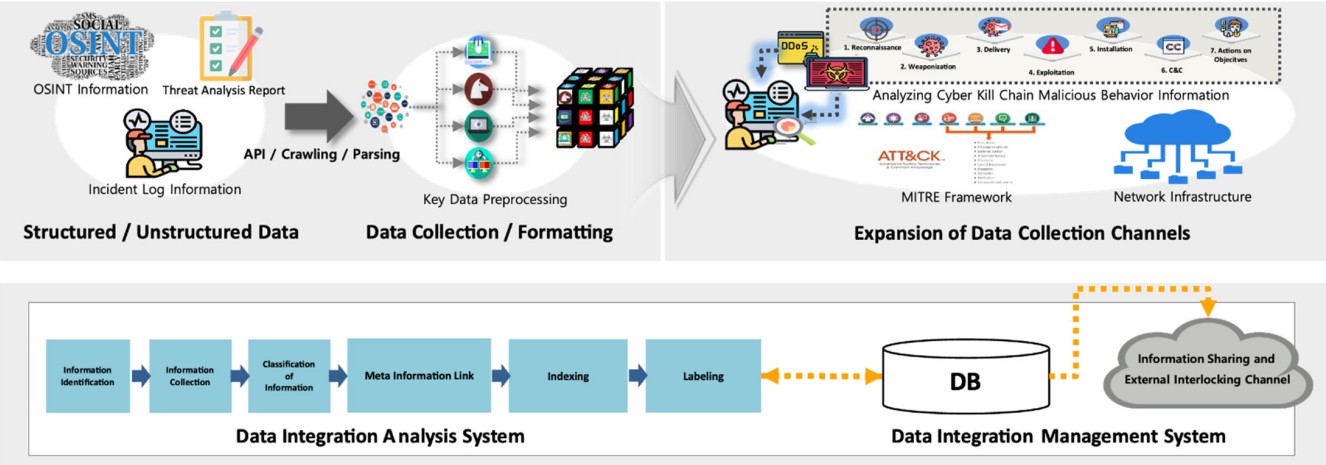

Figure 8. Design of DB for collection and pre-processing data relation. (Adapted from Go et al. Proc AIS 2022; p. 10, with permission from Dailysecu Press [40].)

To analyze the AS path, a di-graph was drawn with the information extracted from the BGP archive data. The BGP AS route map between North Korea and China was visualized in the form of a di-graph, as shown in Figure 9, and the command code for the di-graph visualization is as follows.

```
cat rib.20220601.1000.AS131279.tsv | tr "(" " "| tr ")" " " | awk '$2!=$4{print $2 "\t" $4}'
| awk 'BEGIN{print "digraph{"} {print $0} END{print "}"}' | dot -T png -o
rib.20220601.1000.AS131279.cntry.png
```

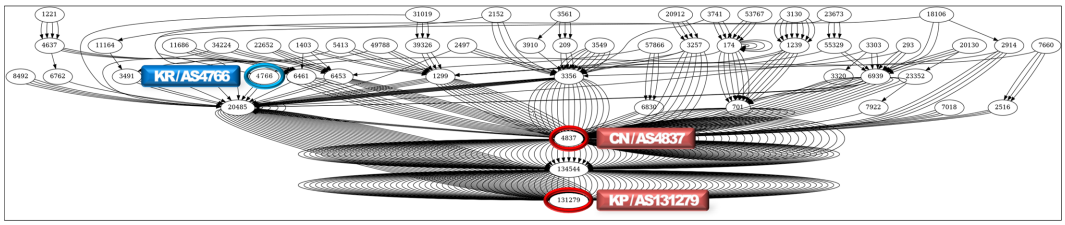

Figure 9. Di-graph visualization of BGP network topology between North Korea and China.

Through this, it was possible to create and analyze not only the AS network unit between North Korea and China, but also the global network topology autonomous system number (ASN), detailed AS route, core node, and relay node information. As shown in Figure 10, the attack path was confirmed from AS4837 in China to AS4766 in Korea, and AS4837 in China was connected to AS131279 in North Korea through a single path, so the origin of the attack is assumed to be North Korea.

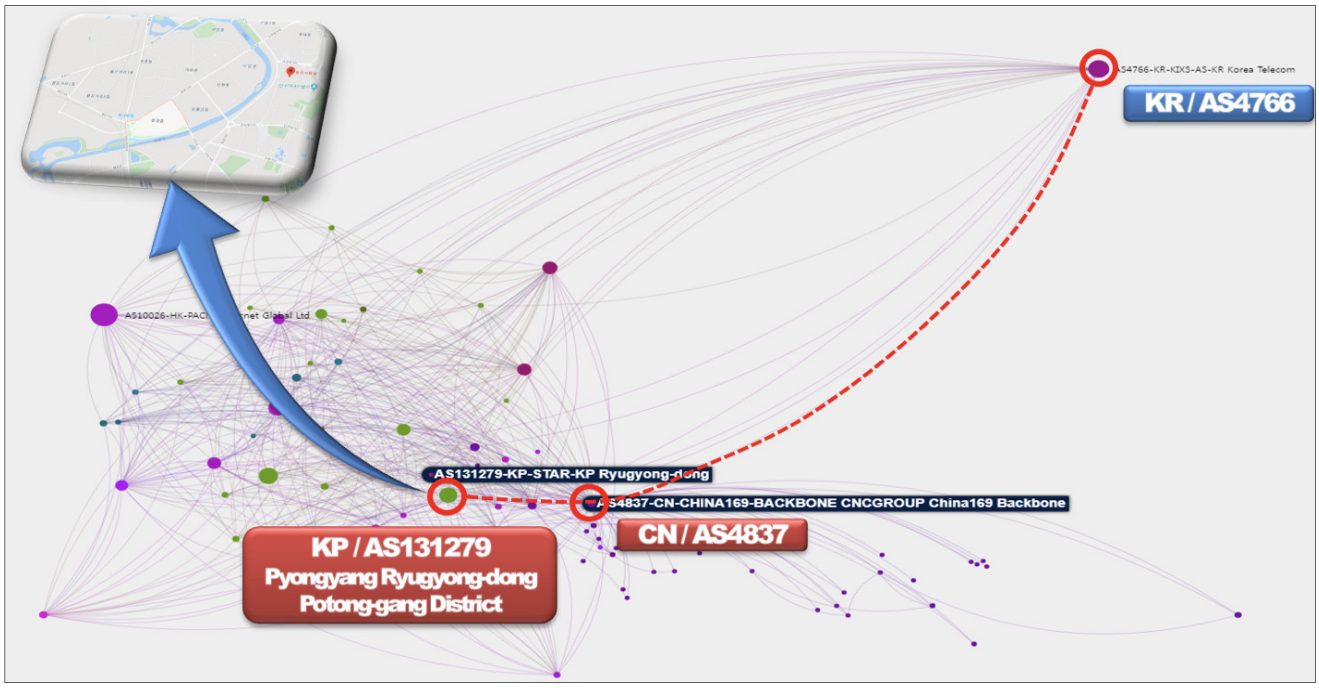

Figure 10. Visualization of North Korean network routes based on BGP archive data.

4.3. Implementation of Cyber ISR Visualization Based on BGP Archive Data

After the data-processing process to convert the published BGP, OSINT, and IP geolocation data into GeoJSON format, an integrated intelligence DB for visualization was built, and the structure was designed to be linked with ElasticSearch and Kibana's ElasticMap [18]. Using the prototype architecture, we proceeded to visualize the IP traceback. In the ISP managed by Star Joint Ventures, the IP band that North Korea used for hacking was estimated as the origin of the attack, and the IP traceback process was carried out. In addition, it was possible to check the public IP, which is believed to have been used for hacking within the North Korean network. Through this, based on BGP archive data, North Korea's cyber ISR prototype was visualized, as shown in Figure 11.

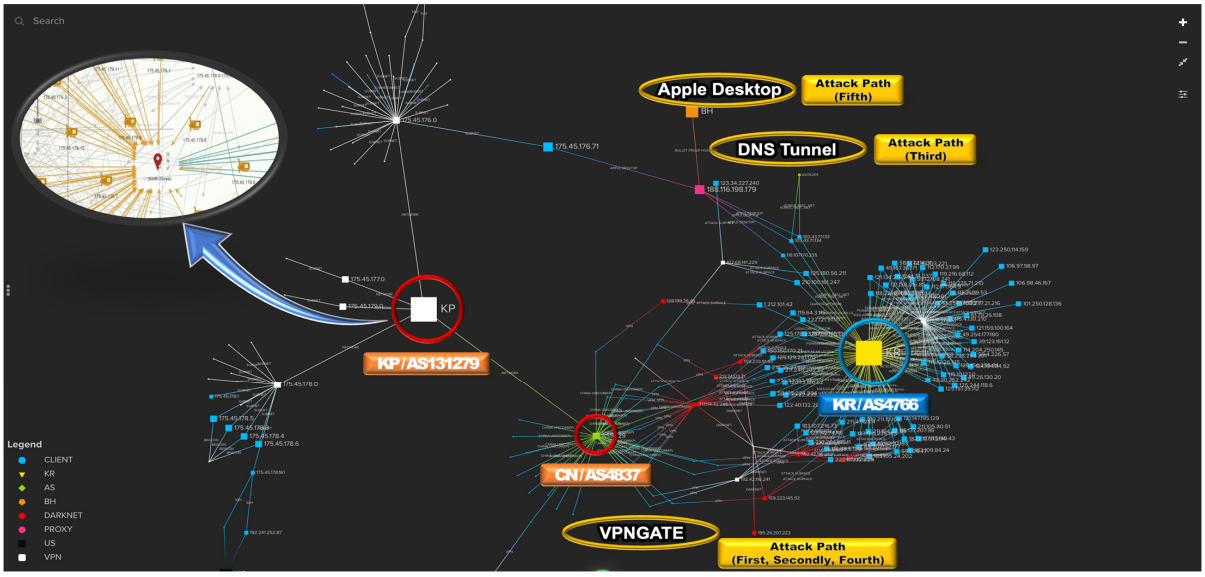

Figure 11. Visualization of North Korean cyber ISR based on BGP archive data.

An interesting fact was discovered during the analysis and visualization process. If we analyze the network connection diagram of North Korea's network topology, we can classify a total of five attack routes from North Korea to South Korea via China.

--First, a route utilizes a virtual private network (VPN) gate. This route leads from North Korea to South Korea via Japan.

--Second, a route utilizes a commercial VPN (Nord VPN). This route leads from North Korea to South Korea via Japan.

--Third, a route utilizes domain-name-system (DNS) tunneling. This route connects North Korea to South Korea via Europe (Switzerland, London) and other areas (Singapore, etc.).

--Fourth, a route utilizes a private L3 VPN. This route leads from North Korea to South Korea via Kenya.

--Fifth, a path uses an Apple desktop based on MacOS. This route connects North Korea to South Korea via the United States and Middle Eastern countries (Bahrain, etc.).

In particular, from around September 2021, the fifth route rapidly changed from a Windows-based desktop environment to an Apple desktop environment, and Apple Remote Desktop communication rapidly increased in North Korea's networks. In addition, traffic from North Korea that attempted hacking attacks after passing through the Middle East was continuously increasing. Analyzing this phenomenon, as the size and activity area of the attack group grew, there was a limit to the tactical operation of hacking activities based on Windows and Linux. Accordingly, it is estimated that the operating environment was changing to a more versatile Apple MacOS-based operating environment.

The added test type was conducted to analyze the attack infrastructure and communication to the infected area. For the data for analysis, two-way communication data collected from domestic and overseas sections based on the IP of the affected area were used. The relay point was derived based on the communication fact that occurred at the infected IP. We proceeded in a way to secure additional data on this. Data for analysis were obtained from the Pure Signal Recon Company. As a result of analyzing the communication log for the seven IPs specified as the affected area, it was confirmed that the network service exposed to the outside exists in the six IPs, as shown in Table 8.

Table 8. Externally exposed network service operating in the victim IP.

Victim	Domain	ASN	Port	Network Service
222.122.8*.***	http://***950.cafe24.com	AS4766	80	Microsoft IIS httpd
210.221.9*.***	Eng.hwang***.com	AS9318	80 | 443	Microsoft IIS httpd
123.142.5*.***	None	AS3786	8080 | 10443	Apache Tomcat
125.130.6*.***	None	AS4766	10443 | 443 | 22	Fortinet—FortiClient
119.204.25*.***	None	AS4766	1433	MSSQL
128.134.10*.***	None	AS4766	3389	MSRDP

There was an Internet section communication log for analysis among the affected areas, and the average number of bytes per packet for the seven IPs was analyzed, as shown in Figure 12.

As a result of the analysis, most of the inbound communications were unconnected communications that occurred in network scans, etc. Outbound communication was mostly connectionless communication. However, both signal-transmission-type and data-transmission-type communication occurred among connectivity communication. When the inbound and outbound ratios of communications originating from the victim IP were checked, the outbound ratio appeared as 99.97%. This means that the attacker took control of the affected area and obtained illegal access rights. Through this, it can be seen that not only was a cyber-attack on the internal system but also that the damaged area was being

used as a new attack base. The structure of communication traffic generated in the affected area is shown in Figure 13.

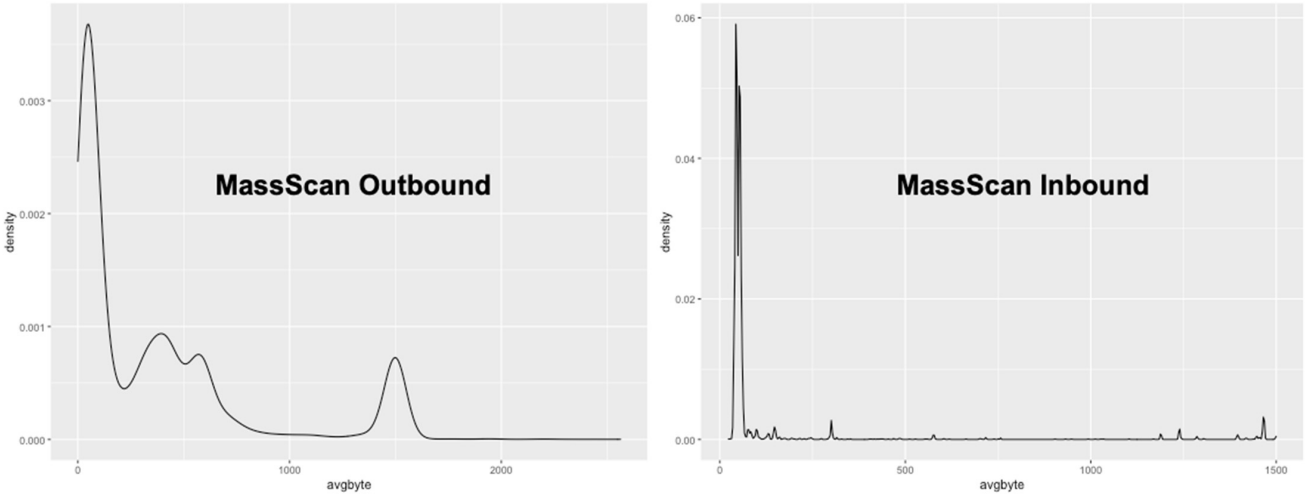

Figure 12. Outbound (left)/inbound (right) of average bytes from 7 victim IPs.

The part marked in blue is the victim IP located in the Republic of Korea, and the arrow shows the direction of communication. What is unusual is the fact that most domestic IPs were being attacked for network vulnerabilities. At the same time, it can be seen that the damaged base was conducting a network vulnerability attack on the server in the overseas section.

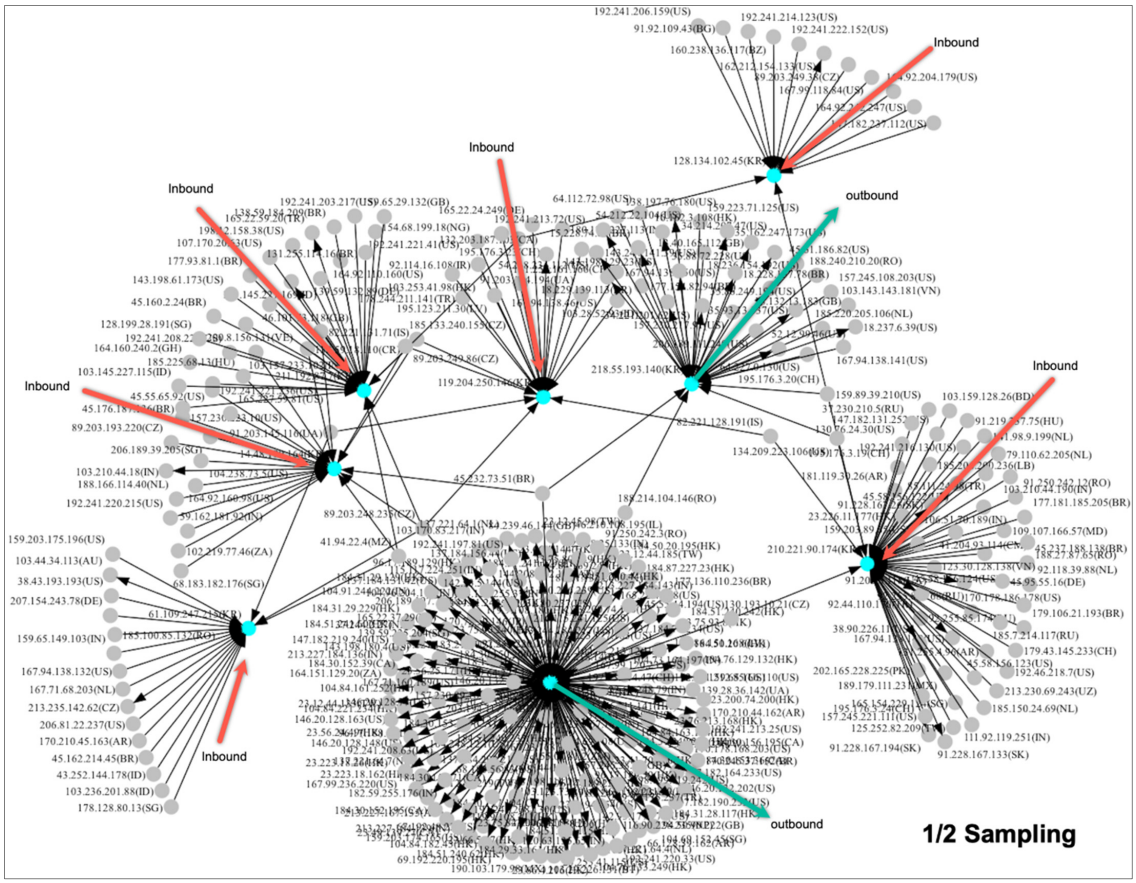

Figure 13. Sampling the structure of communication traffic generated in the affected area.

5. Conclusions

This paper provided an overview of cyber ISR and BGP and studied cyber ISR visualization for situational awareness, hacking trends of North Korean cyber-attack groups, and cyber-attack tracking. In particular, the hacking attack case of Kimsuky, a North Korean cyber-attack group that attempted to steal research data related to COVID-19 in January 2022, was analyzed using a profiling technique. The origin of the attack was estimated from the verified North Korean hacking IP band through correlation analysis using cyber information-based profiling techniques and BGP archive data.

This research enables a commander to recognize the cyber situation at the level of command and control. The network space of the cyber battlefield was visualized, and a cyber ISR visualization method based on BGP archive data was proposed. This paper proposed an architecture for a visualization model and implemented a prototype in terms of prior research to make a better model. For that reason, Section 3 of the thesis analyzed hacking cases, and Section 4 of the thesis focused on applying the cyber ISR visualization model by correlating the analyzed breach index and BGP archive data. As such, it has not been fully developed and implemented, and thus further evaluation is limited.

In the future, in connection with cyber command-and-control-system research, we plan to research the cyber battlefield area, cyber ISR, and a traceback visualization model for the origin of an attack. The final R&D goal is to develop an AI-based cyber-attack group automatic identification and attack-origin tracking platform by analyzing cyber-attack behavior and infrastructure lifecycle. First, we will develop technologies to collect and manage information related to cyber-attack behavior and infrastructure. Lifecycle information (structured/unstructured) data of cyber-attacks will be collected and pre-processed to compose the DB. Attack behavior and infrastructure-related information collection channels will be expanded, as will DB for data-relation configuration. Second, cyber-attack group-clustering technology based on network infrastructure and network domain-characteristic information will be developed. The characteristics of the cyber-attack group's network-infrastructure and network-weakness information will be extracted through feature engineering and a multi cyber-attack group-clustering model will be constructed. Third, an AI-based attack group-infrastructure identification technology will be developed by analyzing the cyber-attack lifecycle. We plan to develop an AI-based group identification module to extract connection and differential characteristics for each cyber-attack group to link network-area information and to learn characteristic information.

The final performance goal of the study is 90% identification accuracy of attack groups and 129 identifiable attack groups. The number of pre-matrix tactics and techniques is 30, and the number of attack group-related feature data is 300. In addition, AI-based attack-infrastructure identification shows a performance improvement of over 80% compared to manual work. Accordingly, the main scientific contribution is the ability to identify and effectively respond to fast attack groups based on network infrastructure-information linkage. It is possible to secure national information-protection technology by securing the source technology for cyber warfare response. Based on the lifecycle analysis of the attack infrastructure, the effect of creating new research and technology fields can be expected.

Author Contributions: Conceptualization, J.Y., K.K., and D.S.; funding acquisition, D.S.; methodology, J.Y., D.K., and J.L.; design of cyber ISR visualization, J.Y., K.K., and J.L.; supervision, D.S.; validation, J.L. and M.P.; writing—original draft, J.Y., K.K., and D.K.; writing—review and editing, D.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Future Challenge Defense Technology Research and Development Project (9129156) hosted by the Agency for Defense Development Institute in 2020.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

APT	Advanced persistent threat
ISR	Intelligent surveillance and reconnaissance
BGP	Border gateway protocol
C2	Command and control
BDA	Battle damage assessment
SA	Situational awareness
COP	Common operational picture
OSINT	Open-source intelligence
IP	Internet protocol
AS	Autonomous system
ASN	Autonomous system number
HWP	Hangul word processor
OLE	Object linking and embedding
VBS	Visual basic script
VPN	Virtual private network
DNS	Domain name system
OS	Operating system
KR	Republic of Korea
DDoS	Distributed denial of service

References

1. Joint Cybersecurity Advisory. *North Korean Advanced Persistent Threat Focus: Kimsuky*; Cybersecurity and Infrastructure Security Agency (CISA): Arlington, VA, USA, 2020.
2. Joint Cybersecurity Advisory. *Guidance on the North Korean Cyber Threat*; Cybersecurity and Infrastructure Security Agency (CISA): Arlington, VA, USA, 2020.
3. Kim, H.K.; Kim, H.J.; No, Y.H. *KISA Cyber Security Issue Report: Q4 2020*; Korea Internet & Security Agency (KISA): Seoul, Republic of Korea, 2021.
4. Miller, K.S. *ATP 2-01.3 Intelligence Preparation of the Battlefield*; Department of the Army: Washington, DC, USA, 2019.
5. Scott, K.D. *Joint Publication (JP) 3-12 Cyberspace Operation*; The Joint Staff: Washington, DC, USA, 2018.
6. Robert, G. *Situation Awareness in Defensive Cyberspace Operations: An Annotated Bibliographic Assessment through 2015*; NIWC Pacific: San Diego, CA, USA, 2019.
7. Soon, T.T.; Supranamaya, R.; Antonio, N.; Chen, N.C. BGP Eye: A New Visualization Tool for Real-time Detection and Analysis of BGP Anomalies. In Proceedings of the 3rd International Workshop on Visualization for Computer Security, Alexandria, VA, USA, 3 November 2006; ACM: New York, NY, USA, 2006; pp. 81–90.
8. Shearer, J.; Ma, K.L.; Kohlenberg, T. BGPeep: An IP-Space Centered View for Internet Routing Data. In Proceedings of the International Workshop on Visualization for Computer Security, Cambridge, MA, USA, 15 September 2008; Springer: Berlin/Heidelberg, Germany, 2008.
9. Biersack, E.; Jacquemart, Q.; Fischer, F.; Fuchs, J.; Thonnard, O.; Theodoridis, G.; Tzovaras, D.; Vervier, P.-A. Visual analytics for BGP monitoring and prefix hijacking identification. *IEEE Netw.* **2012**, *26*, 33–39. [CrossRef]
10. Heinbockel, W.; Noel, S.; Curbo, J. Mission Dependency Modeling for Cyber Situational Awareness. In Proceedings of the NATO IST-148 Symposium on Cyber Defence Situation Awareness, McLean, VA, USA, 30 October 2016; pp. 1–14.
11. Syamkumar, M.; Duraiajan, R.; Barford, P. Bigfoot: A Geo-based Visualization Methodology for Detecting BGP Threats. In Proceedings of the 2016 IEEE Symposium on Visualization for Cyber Security (VizSec), Baltimore, MD, USA, 24 October 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–8.
12. Ulmer, A.; Schufrin, M.; Sessler, D.; Kohlhammer, J. Visual-Interactive Identification of Anomalous IP-Block Behavior Using Geo-IP Data. In Proceedings of the 2018 IEEE Symposium on Visualization for Cyber Security (VizSec), Berlin, Germany, 22 October 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–8.
13. Vinayakumar, R.; Poornachandran, P.; Soman, K.P. Scalable Framework for Cyber Threat Situational Awareness Based on Domain Name Systems Data Analysis. In *Big Data in Engineering Applications*; Roy, S.S., Samui, P., Deo, R., Ntalampiras, S., Eds.; Springer: Singapore, 2018; pp. 113–142.
14. Fonseca, P.; Mota, E.S.; Bennesby, R.; Passito, A. BGP Dataset Generation and Feature Extraction for Anomaly Detection. In Proceedings of the 2019 IEEE Symposium on Computers and Communications (ISCC 2019), Barcelona, Spain, 9 June–3 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.

15. Syamkumar, M.; Gullapalli, Y.; Tang, W.; Barford, P.; Sommers, J. BigBen: Telemetry Processing for Internet-wide Event Monitoring. *arXiv* **2022**, arXiv:2011.10911. [CrossRef]
16. Candela, M.; Di Battista, G.; Marzialetti, L. Multi-view Routing Visualization for the Identification of BGP Issues. *J. Comput. Lang.* **2020**, *58*, 100966. [CrossRef]
17. Vinayakumar, R.; Alazab, M.; Srinivasan, S.; Pham, Q.V.; Padannayil, S.K.; Simran, K. A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities. *IEEE Trans. Ind. Appl.* **2020**, *56*, 4436–4456. [CrossRef]
18. Youn, J.; Oh, H.; Kang, J.; Shin, D. Research on Cyber IPB Visualization Method based on BGP Archive Data for Cyber Situation Awareness. *KSII Trans. Internet Inf. Syst. (TIIS)* **2021**, *15*, 749–766.
19. Fernandes, F.; Stefenon, S.F.; Seman, L.O.; Nied, A.; Ferreira, F.C.S.; Subtil, M.C.M.; Klaar, A.C.R.; Leithardt, V.R.Q. Long short-term memory stacking model to predict the number of cases and deaths caused by COVID-19. *J. Intell. Fuzzy Syst.* **2022**, *42*, 6221–6234. [CrossRef]
20. Costa, H.J.D.M.; Costa, C.A.D.; Righi, R.D.R.; Antunes, R.S.; Santana, J.F.D.P.; Leithardt, V.R.Q. A Fog and Blockchain Software Architecture for a Global Scale Vaccination Strategy. *IEEE Access* **2022**, *10*, 44290–44304. [CrossRef]
21. Mohamed, N.; Alam, E.; Stubbs, G.L. Multi-Layer Protection Approach MLPA for the Detection of Advanced Persistent Threat. *J. Posit. Sch. Psychol.* **2022**, *6*, 4496–4518.
22. Lee, Y.; Lee, Y. Yet Another BGP Archive Forensic Analysis Tool Using Hadoop and Hive. *J. KIISE* **2015**, *42*, 541–549. [CrossRef]
23. Ozarslan, O.F.; Sarac, K. ZIDX: A Generic Framework for Random Access to BGP Records in Compressed MRT Datasets. In Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 3–6 August 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–8.
24. Salido, J.; Nakahara, M.; Wang, Y. An Analysis of Network Reachability Using BGP Data. In Proceedings of the 3rd IEEE Workshop on Internet Applications (WIAPP 2003), San Jose, CA, USA, 23–24 June 2003; IEEE: Piscataway, NJ, USA, 2003; pp. 10–18.
25. Demchak, C.C.; Shavitt, Y. China's Maxim–Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. *Mil. Cyber Aff.* **2018**, *3*, 7. [CrossRef]
26. Douzet, F.; Pétiniaud, L.; Salamatian, L.; Limonier, K.; Salamatian, K.; Alchus, T. Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis. In Proceedings of the 2020 12th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 26–29 May 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 157–182.
27. Yogesh, P.R. Backtracking Tool Root-tracker to Identify True Source of Cybercrime. *Procedia Comput. Sci.* **2020**, *171*, 1120–1128. [CrossRef]
28. Nur, A.Y.; Tozal, M.E. Single Packet AS Traceback against DoS Attacks. In Proceedings of the 2021 IEEE International Systems Conference (SysCon), Virtual, 15 April–15 May 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–8.
29. Nur, A.Y.; Tozal, M.E. Record Route IP Traceback: Combating DoS Attacks and the Variants. *Comput. Secur.* **2018**, *72*, 13–25. [CrossRef]
30. Wang, Z.; Liu, C.; Qiu, J.; Tian, Z.; Cui, X.; Su, S. Automatically Traceback RDP-based Targeted Ransomware Attacks. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 7943586. [CrossRef]
31. Lee, J.; Lee, Y.; Lee, D.; Kwon, H.; Shin, D. Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. *IEEE Access* **2021**, *9*, 80866–80872. [CrossRef]
32. Suganya, V. A Review on Phishing Attacks and Various Anti Phishing Techniques. *Int. J. Comput. Appl. Found. Comput. Sci. (FCS)* **2016**, *139*, 20–23. [CrossRef]
33. Chiew, K.L.; Yong, K.S.C.; Tan, C.L. A Survey of Phishing Attacks: Their Types, Vectors and Technical Approaches. *Expert Syst. Appl.* **2018**, *106*, 1–20. [CrossRef]
34. Qabajeh, T.F.; Chiclana, F. A Recent Review of Conventional vs. Automated Cybersecurity Anti-Phishing Techniques. *Comput. Sci. Rev.* **2018**, *29*, 44–55. [CrossRef]
35. Kim, J.Y.; Bu, S.J.; Cho, S.B. Zero-day Malware Detection Using Transferred Generative Adversarial Networks based on Deep Autoencoders. *Inf. Sci.* **2018**, *460*, 83–102. [CrossRef]
36. Gangavarapu, T.; Jaidhar, C.; Chanduka, B. Applicability of Machine Learning in Spam and Phishing Email Filtering: Review and Approaches. *Artif. Intell. Rev.* **2020**, *53*, 5019–5081. [CrossRef]
37. Lawson, P.; Pearson, C.J.; Crowson, A.; Mayhorn, C.B. Email Phishing and Signal Detection: How Persuasion Principles and Personality Influence Response Patterns and Accuracy. *Appl. Ergon.* **2020**, *86*, 103084. [CrossRef]
38. Kong, J.Y.; Lim, J.I.; Kim, K.G. The All-Purpose Sword: North Korea's Cyber Operations and Strategies. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–20.
39. Shin, C.; Lee, S.J. A Study of Countermeasure and Strategy Analysis on North Korean Cyber Terror. *J. Police Sci.* **2013**, *13*, 201–226.
40. Go, W. Technology to Attack groups identify based on cyber-attack life-cycle information learning. In Proceedings of the 2th Artificial Intelligence Information Security Conference 2022 (AIS 2022), Dailysecu, Seoul, Republic of Korea, 15 November 2022; pp. 9–10.