Hindawi
Security and Communication Networks
Volume 2022, Article ID 1699657, 12 pages
https://doi.org/10.1155/2022/1699657

Research Article

Focusing on the Weakest Link: A Similarity Analysis on Phishing Campaigns Based on the ATT&CK Matrix

Youngsup Shin,[1,2] **Kyoungmin Kim**,[1,2] **Jemin Justin Lee**,[1] **and Kyungho Lee**[1]

[1] *School of Cybersecurity, Korea University, Seoul 02841, Republic of Korea*
[2] *R. O. K., Cyber Operations Command, Seoul 04383, Republic of Korea*

Correspondence should be addressed to Kyungho Lee; kevinlee@korea.ac.kr

Received 27 January 2022; Revised 15 March 2022; Accepted 1 April 2022; Published 26 April 2022

Academic Editor: Ilsun You

In the past, phishing techniques were a common means of attack carried out by individuals or small groups via spam mail on a randomly selected target. However, in recent years, phishing techniques have been adopted by advanced persistent threat (APT) groups to attack organizations such as the Sony Pictures Enterprise and Korea Hydro & Nuclear Power. As such, our study aims to analyze the past campaigns conducted by the APT groups. We aim to propose a countermeasure that corresponds to the phishing campaign by collecting datasets pertaining to the phishing techniques. Based on our past study, we collected private and public data from 16 different cases that utilize a phishing attack. Our research adopted MITRE's ATT&CK framework and tactic, techniques, and procedures (TTPs) to extract and examine the various campaigns. The framework proposed in this study makes considerable contributions to both the private and public sectors, as the framework aids the organizations in counteracting the malicious threats performed by the APT groups.

1. Introduction

Countering the Red Queen effect in cybersecurity has become much more difficult, as new adversarial campaigns are implementing new techniques and procedures. In spite of the new updates and patches that are released, the state-sponsored advanced persistent threat (APT) groups are constantly finding new vulnerabilities to exploit their targets. In order to gain a better understanding of the APT groups, cyber threat intelligence focused on various formats such as Common Attack Patterns Enumerations and Characteristics (CAPEC) and Common Vulnerabilities and Exposures (CVE). These formats were actively shared with standard formats, such as STIX 1.0, STIX 2.0, and OpenIoC [1], and shared standards, such as Trusted Automated eXchange of Indicator Information (TAXII). Analyzing the APT group's tactic, technique, and procedures (TTPs) is crucial for cyber threat intelligence. MITRE developed the ATT&CK Framework to better adopt these bits of information [2]. Despite the efforts of various organizations, the malicious cyber campaign by APT groups continues. In particular, phishing tailored to a specific target exploits social engineering vulnerabilities and requires further examination.

In spite of the extensive research conducted on phishing [3], the problem is nearly untraceable. *PhishPrint*, a low-cost framework, evaluated web security crawlers such as Microsoft Outlook e-mail scanners and Google Safe Browsing against cloaking attacks [4]. *PhishTime*, a framework that identifies unmitigated phishing websites by replicating key aspects of the configuration, enhanced the protections for mobile devices [5]. Das et al. [6] identified the lack of metrics, comparison issues, and lack of generalization studies as the cause for the methodological issues. Our study proposes a process to analyze the phishing campaign of three malicious nation-state threat groups by applying the similarity analysis methodology and determining an appropriate response strategy. In summary, our contributions in this paper are as follows:

(i) We present a methodology to quantitatively analyze the similarity between TTPs of a cyber campaign expressed by the ATT&CK matrix, and through this, introduce a decision-making process for selecting the optimal countermeasure to respond to an adversarial cyber campaign.

(ii) We analyzed the phishing campaigns performed by the nation-state threat group through the experiment results to derive critical tactics that is often the weakest link in the attack chain. Since our approach is not limited to phishing campaigns, it will provide insight to security officers and researchers in organizations responding to real cyber threats.

(iii) In addition, we have summarized previous studies on phishing mitigation and introduced the flow of research related to phishing so far to the readers.

2. Literature Review

Phishing exploits the weakest link in the system by impersonating a trusted entity for sensitive information (i.e., account credentials) [7, 8], and the annual financial loss from the phishing activities in the U.S. accounts of 61 million USD to 3 billion USD [9]. According to the FBI's Internet Crime Report, phishing was the most common type of cybercrime in 2020. Consequently, the number of phishing victims in the United States has doubled from 114,702 to 241,352 from 2019 to 2020 [10]. Cyber threat actors (CTAs) commonly target specific individuals or victims using spear-phishing techniques, and phishing attacks that involve SMS are known as smishing [11]. MITRE's ATT&CK classifies spear-phishing into three techniques: (i) spear-phishing attachment, (ii) spear-phishing link, and (iii) spear-phishing via service [2]. In this section, literature reviews of phishing detection, phishing campaigns, and cyber campaign analysis are introduced.

2.1. Phishing Detection. Depending on the APT groups' intentions, the phishing attacks can be carried out in various methods. As mentioned above, phishing attacks via e-mail, web page, URL, and SMS have been a constant problem. Thus, past studies have attempted to detect the phishing attacks through various modules and frameworks. Our study examines the key findings of the prior studies by performing a literature review of the recent studies.

Components of the web page can be key features to detect malicious phishing web pages. Mao et al. [12] proposed *Phishing-Alarm*; phishing attack detection solution extracts CSS-based web page features. While Corona et al. [13] presented *DeltaPhish*, a compromised phishing web page detection solution by highlighting HTML code and visual difference. Recent studies commonly use machine learning methods to detect phishing web pages. Adebowale et al. [14] presented schemes utilized three different conventional classification algorithms (SVM, K-NN, and ANFIS) using the integrated features of text, images, and frames for phishing detection. Abdelnabi et al. [15] proposed a detection model based on triplet convolutional neural networks, as shown in Table 1. While the heuristic method is mainly used to detect phishing URLs, a hybrid approach that combines a heuristic method and a machine learning method has also been proposed. Jain and Gupta [16] presented an autoupdate whitelist of legitimate sites to protect users against phishing attacks. Jeeva and Rajsingh [17] presented a phishing URL detection method by extracting features from the URL and generating the rule using Apriori algorithm. Sonowal and Kuppusamy [18] proposed a 5-step multifilter approach to detect phishing URL, consisting of a whitelist layer, a URL feature layer, a lexical signature layer, a string matching layer, and an accessibility score comparison layer. Johnson et al. [19] compared the performance of popular deep learning framework models such as Fast.ai and Keras-TensorFlow against traditional machine learning algorithms across CPU, GPU, and TPU architectures, as shown in Table 2. Phishing e-mail detection methods use natural language processing and machine learning. Peng et al. [20] presented an approach for detecting inappropriate statements that can detect phishing e-mail through natural language. Gangavarapu et al. [21] applied state-of-the-art machine learning algorithms to extract most discriminating feature set for phishing e-mail detection, as shown in Table 3. While previous studies have focused on detecting web pages, URLs, or emails used for phishing, studies on attack techniques and tactics accompanying phishing are lacking. Our research focuses on analyzing phishing campaigns conducted by threat groups and establishing procedures to help decision-making to respond effectively.

2.2. Phishing Campaigns. In recent years, the attacks have been tailored to the specific target to extract valuable information from senior-level experts from the financial sectors [22]. While phishing campaigns were carried out by sending large volumes of spam emails to an unspecified number of victims in the past [23]. The victim has naturally shifted as the phishing campaigns have been carried out by state-sponsored groups such as Kimsuky and Lazarus group [24, 25]. Kimusky have performed cyber campaigns on the U.S. national security think tank using Microsoft Visual Basic script-based malware [25] and attacked Korea Hydro & Nuclear Power (KHNP) in 2014 [24]. In recent years, the APT group has carried out spear phishing attacks that target government and nongovernment victims. Majority of the spear phishing techniques delivered malicious files that were masqueraded document files to .doc, .docx, or .hwp (Hangul file extension) format [26]. The documents impersonated COVID-19 related documents, which aimed to obtain initial access of the victim's network [27, 28]. Phishing is an attack vector used by many nation-sponsored threat groups and is mainly used as a method of initial access, such as attaching documentation containing malware or inducing access to malicious websites. According to a report from Seoul Central District Public Prosecutors' Office (2015) [24], Kimsuky sent phishing emails that include malicious Hangul document file to business partners and retirees of KHNP. Malicious Hangul document contained a remote administration tool. Kimsuky collected e-mail accounts and passwords of victims and exfiltrated more than 94 files from victims' e-mail accounts. Exfiltrated files through phishing e-mail include employee addresses, employee phonebook,

Table 1: Literature review on phishing techniques pertaining to the web.

Focus	Study	Research design	Major findings
Web	Mao et al. (2017)	Collected 9,307 verified phishing websites from *PhishTank* as an experiment sample set. It consists of phishing pages targeting popular website (e.g., PayPal, eBay, Apple).	*Phishing-Alarm,* phishing attack detection solution extracts CSS-based page features, evaluates the similarity between whitelisted web pages and suspicious web page, and focuses on visual features that are hard to be tampered. This study presents techniques to identify effective CSS features as well as efficient algorithms for page similarity analysis. Authors prototyped Phishing-Alarm as an extension to the Google Chrome browser and evaluated it using a wild phishing web pages.
	Corona et al. (2017)	Empirically evaluated it on more than 5,500 web pages from compromised websites in the wild.	*DeltaPhish* detects compromised phishing web page by highlighting HTML code and visual difference with respect to legitimate pages hosted within a compromised website. Web pages collected in the wild from infected websites were evaluated and performed capability of detecting more than 99% of phishing web pages, while less than 1% of false detection of legitimate pages.
	Adebowale et al. (2018)	Dataset consisted of 4,898 phishing websites, 1,945 suspicious sites, and 6,157 legitimate websites from 2 prior studies (Rami et al., 2015a, 2015b) and *PhishTank*.	Presents an Adaptive Neuro-Fuzzy Inference System (ANFIS) using integrated features of the text, images, and frames. This study utilized three different conventional classification algorithms (SVM, K-NN, and ANFIS). ANFIS algorithm achieved accuracies of 98.3% on web-phishing detection.
	Abdelnabi et al. (2020)	*VisualPhishNet* examined 155 trusted phishing websites, which consists of 9,363 pages.	*VisualPhishNet,* a similarity-based detection model based on triplet convolutional neural networks (CNN), examined *VisualPhish*.

Table 2: Literature review on phishing techniques pertaining to the URL.

Focus	Study	Research design	Major findings
URL	Jeeva and Rajsingh (2016)	Experiment done by using an input data set of 1,200 phishing URLs and 200 legitimate URLs.	Analyzed phishing URL to figure significant features to discriminate between legitimate and phishing URLs based on apriori and predictive apriori rule generation algorithm.
	Jain and Gupta (2016)	Dataset of 1,120 phishing URLs and 405 legitimate URLs were used to evaluate the performance of the proposed approach. The URLs were collected between June 2015 and November 2015.	Research focused on fast access time for a real-time environment and high detection rate based on auto updated whitelist of legitimate web sites. The whitelist consists of access of individual users. The performance of the phishing URL detection showed 86.02% of true positive rate while 1.48% of false negative rate.
	Sonowal and Kuppusamy (2020)	Collected 667 phishing URLs from *PhishTank*, 995 legitimate URLs from *Phishload* in November 2016.	*PhiDMA*, multilayer model to detect phishing based on hybrid approach that incorporates 5 layers of whitelist layer, URL feature layer, lexical signature layer, string matching layer, and accessibility comparison layer. *PhiDMA* achieved accuracy of 92.72% to detect phishing URLs.
	Johnson et al. (2020)	Used ISCX-URL-2016 dataset to train deep learning frameworks.	Compared the performance of the state-of-the-art deep learning framework models and traditional machine learning algorithms.

and nuclear powerplant drawings (DRAWING_WOLSONG32.zip) [24]. Kimsuky also conducted phishing attacks targeting 12 government agencies related to the French ministries of foreign affairs. Malicious URL, masquerading as a diplomatic portal, "portalis.diplomatie.gouv.fr.doc-view[.]work" was hosted on the IP 157.7.184[.]15, which has several subdomains that designed to impersonate e-mail providers. The IP and subdomains were also employed to various phishing campaigns aimed at think tank based on the United States and United Kingdom, United Nations delegation, and the Ministry of Foreign and European Affairs of the Slovak Republic [29]. The Sony Pictures Entertainment (SPE) hacking, a cyber attack carried out by the Lazarus Group, also used a phishing e-mail in its

Table 3: Literature review on phishing techniques pertaining to the mail.

Focus	Study	Research design	Major findings
Mail	Peng et al. (2018)	Used datasets and library set such as *accord.net* to detect phishing mail sent to the organization in real-time environment.	The study presents phishing mail detection method using natural language processing and support vector machine. Features such as account of sender and receiver, IP address, subject and body of the e-mail, date, and time are analyzed to detect phishing mail.
	Gangavarapu et al. (2020)	Dataset consisted of 2,551 ham (legitimate) emails and 793 phishing emails, 500 spam emails collected from a variety of sources.	Presented study focused on detecting unsolicited bulk emails (UBEs) including spam emails and phishing emails. The study proposed technique for extraction and selection of the most discriminating e-mail contents and behavior-based feature set. Furthermore, it proposed detection model after comparative study using several state-of-the-art machine learning algorithms.

initial step. In McClure's presentation at RSA conference 2015 suggests that senior Sony executives, including CEO Michael Lynton, received fake Apple ID verification emails that contained a link to "ioscareteam.net" [30]. Kim et al. [8] pointed out the spear phishing techniques were most widely used as "Initial Access" in the SPE hacking which carried out spreading malwares, deleting files, and corrupt master boot records (MBR).

2.3. Cyber Campaign Analysis. As the volume of cyber incidents got larger and cyber warfare between countries began in earnest [31, 32], cyber campaign analysis requires research from a variety of different perspectives from IoCs (Indicator of Compromise), malware to TTPs (Tactics, Techniques, and Procedures). Malware analysis is commonly categorized into static analysis and dynamic analysis. Static analysis allows reverse engineering of a low-level assembly code, while dynamic analysis is a behavior analysis that observes the malware activities such as file deletion, file modification, change in registry, and stealing confidential information [33, 34]. Willems et al. [35] state that the process of reverse engineering and using manual methods for detecting threats is not sufficient to combat automated threats. The study further iterates that the drawback of dynamic analysis is the execution time, as only a single malware can be analyzed at once. Yet, static analysis is difficult to perform as the source code is oftentimes not available. During the past-decade hybrid analysis, a method that combines both the dynamic and static analysis has been widely adopted [36–38]. Various automated malware analysis tools are often used for cyber campaign analysis. Sandboxes such as Cuckoo, Malware, ThreatExpert, and Joe Sandbox provide an in-depth look into the malicious file's context, motivation, and goal by outlining the behavior of the file in an isolated environment [39, 40]. Joe Sandbox [39] is a sandbox that allows a combination of static and dynamic analysis by uploading APK files for automated testing [40]. Automated tools are not used only for analyzing malwares. TRAM, Threat Report ATT&CK Mapper, is an automated tool for extracting ATT&CK matrix from security reports using natural language processing [41]. Reports Classification by Adversarial Tactics and Techniques (rcATT) is a tool designed by Legoy et al. [42], which predicts tactics and techniques from cyber threat reports. MITRE's s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) have been used as a common language to define and categorize TTPs and threat groups [43]. MITRE's ATT&CK framework has released ATT&CK v10 on 21st of October, 2021. However, our study adopted ATT&CK Enterprise v9 which contains 14 tactics, 185 techniques, and 367 subtechniques [2]. Recent studies of Shin et al. [44] and Kim et al. [45] have adopted the ATT&CK framework to propose a malware analysis tool. Shin et al. [44] adopted the ATT&CK Enterprise Framework, while Kim et al. [45] employed the ATT&CK Mobile framework as the study focused on the mobile threats. CTI (Cyber Threat Intelligence) is information of cyber threats or threat actors which is considered as a solution for counter rising threats [46]. Liao et al. [47] present automated IoC (Indicator of Compromise) extraction solution based on grammatical relations in open-source CTI, while Qamar et al. [48] devise a threat analytics framework allowing the derivation of network associated threats from large volumes of CTI. Noor et al. [49] state that the CTI documents provided by the security experts are incapable of attributing cyber attacks in a timely manner. As such, this study profiled cyber threat actors (CTAs) based on the CTI reports using five machine learning classifiers.

3. Methodology

We introduce the similarity analysis method for examining and mitigating phishing campaigns. Our framework is largely composed of data collection and campaign analysis, as depicted in Figure 1. First, cyber incident (operation) data using phishing is collected. The data are in the form of a report or malwares disclosed in the public information. Through this data, the victim, the purpose of the cyber attack, and the TTPs are extracted. The ATT&CK matrix is used to represent the TTPs. When the ATT&CK matrix, attack purpose, and attack target are collected, they are stored in the cyber incident database. The second step is to classify and analyze the campaign. We classify cyber campaigns through a campaign classification method suitable for phishing campaigns and calculate the ATT&CK matrix that

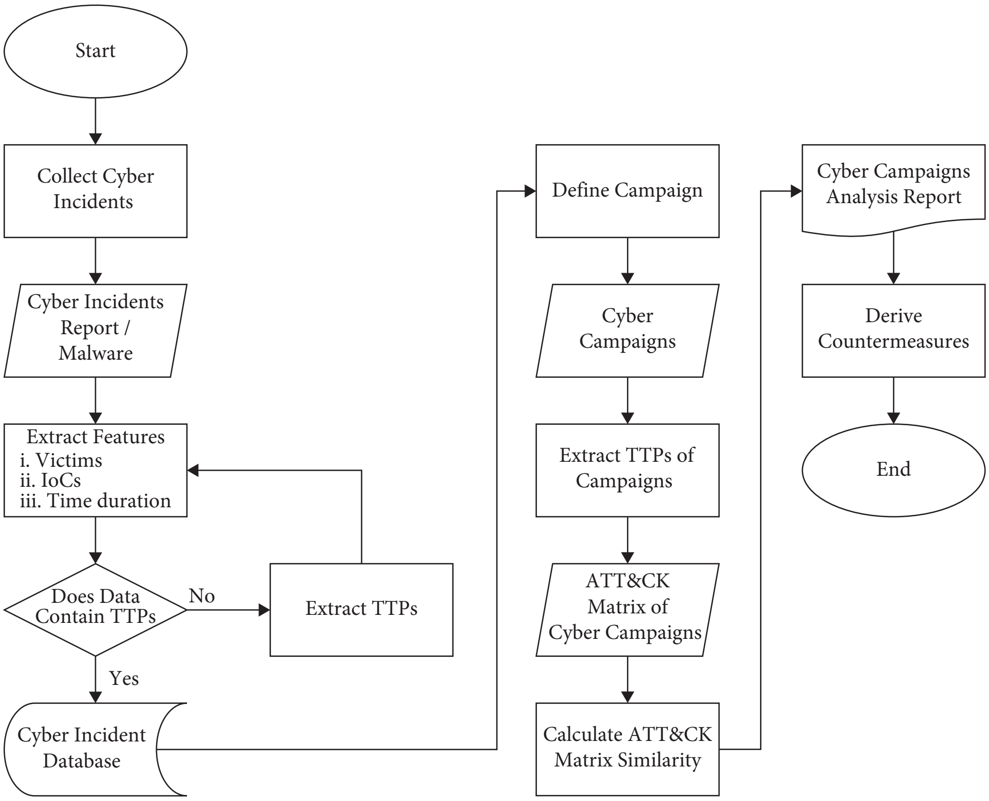


Figure 1: The methodology consists of 6 steps. (a) Collect cyber incidents. (b) Extract features. (c) Define campaign. (d) Extract TTPs of campaigns. (e) Calculate ATT&CK matrix similarity. (f) Derive countermeasures.

represents the campaign through the sum of the ATT&CK matrix. Finally, the matrix for each campaign is vectorized, and the tactic similarity for each cyber campaign is expressed through cosine similarity. After that, the analysis results are discussed.

3.1. Data Collection. The following subsections describe detailed information for each stage of the framework. In order to collect data for analysis, we first collected cyber incidents, which are the smallest unit of a campaign. Cyber incidents are saved in the form of a report or known malware that is used for the incident. We selected 16 credible SOC vendors, collected reports, and included private reports analyzed through collaboration with related organizations. In the case of malware, we collected through private channels or through VirusTotal's detection Yara rules. There are also cases where malware was collected from public information. For example, in the case of CISA [26], the description of the case is not elaborated, it provides only malware information.

3.2. Feature Extraction. When incidents and malicious codes are collected, several IoCs that are good to classify into campaigns are extracted. At this time, the target of the attack and the purpose of the attack are classified. The attack target and attack purpose are collected in the report, or if this is not written, the link and attachment used during phishing are analyzed to infer the content and victim and store it. We also collect the ATT&CK matrix to consider the TTPs that the methodology has the most meaning for. Basically, we used the TTP of each incident in the report as it is when it is provided as it is mapped to the ATT&CK matrix. Otherwise, automated ATT&CK matrix retrieval was performed through previous studies [39, 41] described above. In the case of a report, it is collected through TRAM, and if only the malware hash was provided to the incident, malware was collected through VirusTotal and a matrix was obtained through Joe Sandbox.

3.3. Defining the Adversarial Campaigns. When classifying cyber campaigns, previous studies compared and classified the Indicator of Compromise (IoC) of individual cyber events, the malwares, and the purpose of the attack in a complex way. In various public information, campaigns were described by attaching names to each vendor, and the same campaign was being used with different names. We needed to reclassify these campaigns and also to reinterpret the campaign methods divided by malware and IoC. We set the campaign definition method to consider "target, attack purpose, and timing" through known malware or intrusion indicators. In general, it is often difficult to determine the exact path of a malicious code or attack damage. Because the collection path is often private, who is victim and how the attack started is difficult. However, due to the characteristics of phishing, the victim and the attack purpose can be specified through social engineering in the process. For example, the "US Biden Administration" disguised document-type malware sent by Kimsuky in the past is an incident that collected information by sending it to political and diplomatic officials interested in the Biden Administration. Just by looking at the masqueraded title of the document, we can infer the target of the attack and the purpose of the attack to some extent. Therefore, we distinguished and defined cyber campaign with target and purpose rather than determine only with used malicious codes. This method was able to consider two problems that occur when tying cyber operations based on malicious code. (i) If the same APT group uses the same malicious code and uses it for different purposes for different attack targets, or (ii) another APT groups recycle the malicious code and give a false flag.

3.4. Extracting the TTPs from the Adversarial Campaigns. We adopted ATT&CK matrix to analyze TTPs of each collected incident. TTPs of incidents were collected at the data collection step by manual malware analysis and automated methods such as automated malware analyzer (sandbox) [39] and automated CTI report analysis tool [41]. We grouped the collected incidents based on cyber campaigns defined in the previous step, "define campaign." By integrating the ATT&CK matrix of the incident included in each campaign, it is possible to create a cyber campaign ATT&CK matrix representing the campaign. When examining ATT&CK matrix, the matrix consists of 14 tactics. However, it is difficult to identify which techniques are used at the stage of *Reconnaissance* and *Resource Development* [44]. In this study, we excluded the tactics of *Reconnaissance* and *Resource Development* and examined the 12 tactics.

3.5. Calculating the ATT&CK Matrix Similarity. We vectorized ATT&CK matrix using the method presented in previous studies [44, 45]. Although this study is a methodology used to reestablish indiscriminately made apt group names, we consider this an excellent method to determine the TTP of a campaign quantitatively and intend to borrow it. The vectorized ATT&CK matrix enables calculation of the similarity between TTPs of campaigns quantitatively. Quantitative similarity calculation between TTPs of campaigns enables screening important tactics and techniques in phishing campaigns and identifying the most effective countermeasure to mitigate phishing campaigns. The ATT&CK matrix representing the phishing campaign can be created by integrating the ATT&CK matrix of all incidents constituting the campaign. We convert the incidents' tactics into a vector that expresses whether techniques are used or not. In each vector, the used technique is expressed as 1, and the unused technique is expressed as 0. Scheme of vectorizing tactic *Initial Access* is followed (see Figure 2).

Equation (1) describes the integration of ATT&CK matrix of campaign X. X_i is ith tactic of campaign X (e.g., X_1 is 1st tactic (*Initial Access*) of campaign X), X_{i_n} represents the ith tactic of incident defined as campaign X. N is a total number of incidents defined as campaign X.

$$X_i = \sum_{n=1}^{N} X_{i_n}, \quad X = \{X_1, X_2, \ldots, X_i, \ldots, X_{12}\}. \tag{1}$$

The similarity between campaigns conducted by the same APT group can be identified by the TTPs expressed in ATT&CK matrix. In this study, in order to analyze the similarity of the cyber campaigns, we calculated the cosine similarity of ATT&CK matrix by each tactic. The cosine similarity refers to the degree of similarity measured by using the cosine value of the angle between two vectors. Since cosine similarity can be applied to any number of dimensions, it is often used to measure similarity in multidimensional positive space. Therefore, it is a suitable method for measuring the similarity between tactic vectors corresponding to a multidimensional positive space. Since the vector size does not affect the similarity measurement, it is applicable even if the number of incidents for each campaign is different. The cosine similarity of tactic is described as equation (2). $\operatorname{sim}(X_i, Y_i)$ represents similarity of campaign X and campaign Y. X_i and Y_i represent the ith tactic of each campaign.

$$\operatorname{sim}(X_i, Y_i) = \begin{cases} 0, \text{one of } X_i \text{ or } Y_\text{i} \text{ is zero vector}, \\ \\ \dfrac{X_i \cdot Y_i}{X_i Y_i}, \text{otherwise}. \end{cases} \tag{2}$$

3.6. Derive Countermeasures. After going through the steps described above, the most effective countermeasure can be derived from the collected similarity analysis results between campaigns. When cyber campaigns are viewed as a series of procedures, the way to mitigate cyber campaigns is to break the chain of procedures. At this time, if the defender identifies and prepares for the most frequent tactics and techniques, it can be said to be an effective countermeasure. When the average value of similarity for each tactic is obtained, the closer to 1, the more commonly the technique is used in the campaign, and the closer to 0, the more diverse the technique. Therefore, a tactic with high similarity to each tactic is the weakest link among the full-chain cyber campaigns. We can find the tactic corresponding to the weakest link through the similarity analysis method described above and suggest the most effective response strategy by mitigating the restrictive technique used in the tactic. An effective countermeasure can be suggested through D3FEND. D3FEND is a knowledge graph of cybersecurity that is complementary to the MITRE's ATT&CK framework [50]. D3FEND presents the countermeasures by mapping with the techniques of ATT&CK framework and the defensive techniques of D3FEND. The techniques of D3FEND are provided in five tactics: Harden, Detect, Isolate, Deceive, and Evict. Therefore, an effective countermeasure can be established by mapping the techniques used at the weakest link to the defensive techniques of D3FEND. The techniques of D3FEND can be presented more specifically when digital artifacts are considered together, and by providing a related patent, it helps to implement practical response strategies

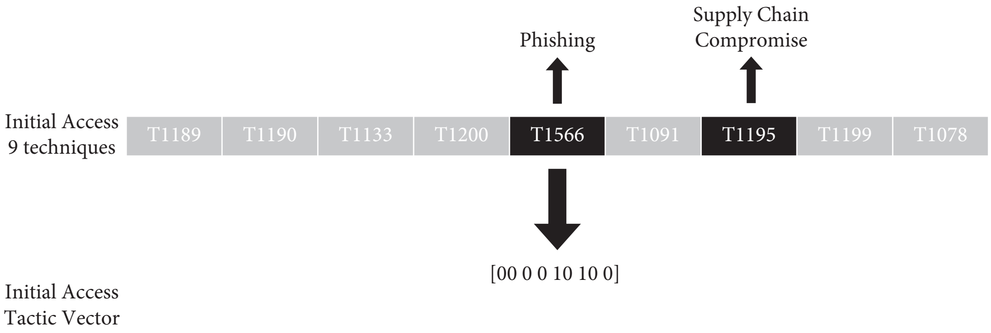


Figure 2: Vectorization of Tactic *Initial Access*. When techniques of *Phishing* and *Supply Chain Compromise* are used, they are expressed as 1. On the other hand, unused techniques are expressed as 0.

[50]. Specific examples are described in the Experiment and Result sections.

3.7. Experiment. Our dataset consists of 79 incidents, which are considered to utilize phishing since 2019. Collected data is malwares and reports related to 3 North Korean threat actors, Kimsuky, Lazarus group, and APT 37. These threat actors are known for carrying out large volumes of phishing attacks. Phishing incidents can be defined as 16 phishing campaigns. 6 phishing campaigns are conducted by Kimsuky, 7 campaigns by Lazarus group, and 3 campaigns done by APT 37. Dataset was collected from both public, such as CTI reports from SOC vendors, and private data. Private data consist of directly reported incidents, shared data from relevant organizations, and collected malware from VirusTotal by undisclosed Yara rules. Through this, we were able to collect relatively clear cases by the victim, and in each campaign, we were able to identify several malware variants and different types of malwares for each period.

The aforementioned dataset utilized 79 incidents known to have been carried out by three North Korean threat actors collected over three years from 2019 to 2021 (see Table 4). The 79 incidents in the dataset can be classified into 16 campaigns based on the characteristics such as attack targets, used malicious codes, and indicators of compromise. K, L, and A stand for Kimsuky, Lazarus, and APT37’s campaign, as depicted in Table 5. For example, the Kimsuky group typically used a malicious code known as babyshark, and the attack campaign using this malicious code seems to have attacked two groups: diplomatic and security officials. The reason for classifying the campaigns into 16 campaigns has the advantage of including the campaign’s attack purpose and the technical TTP of the campaign.

Our methodology defined a phishing campaign from collected phishing incident data and performed similarity analysis by converting TTPs for each campaign into ATT&CK matrix. Our analysis focuses on specifying major techniques used in phishing techniques and measuring diversity of used techniques in each tactic. The lack of technique diversity means that defense capabilities can be focused on fewer techniques, which can be interpreted as the weakest link in the cyber kill chain. So, we calculated similarities of each tactic that consists of phishing campaigns. A high value of tactic similarity indicates relatively low diversity of the used techniques, and conversely, a low similarity value indicates high diversity of the used techniques.

4. Results and Discussion

4.1. Result. We computed the average similarity of tactic vectors for all campaigns. The average similarity value is calculated through 120 similarity comparisons for a total of 16 campaigns. In general, phishing campaigns use the TA0007 (*Discovery*) stage, which has the highest average tactic similarity of 0.5888, the most (see Table 6). This TA0007 can be seen as a critical tactic of the overall phishing campaign to which defenders should pay the most attention. TA0007 is a tactic that attackers can use to learn about systems and internal networks. Although it is slightly different for each campaign, according to our experiment, it seemed that T1083 (*File and Directory Discovery*) and T1057 (*Process Discovery*) techniques were used the most. However, in this data set, there is no significant difference in the average values of other tactics other than TA0007, so it is challenging to explain TA0007 as a critical tactic typically used in a phishing campaign. Therefore, we also performed similarity comparisons of campaigns classified by threat actors. We separately calculated the average value of the tactic similarities of campaigns conducted by Kimsuky (see Table 7), Lazarus group (see Table 8), and APT 37 (see Table 9). As this average value converges to 1, it can be judged that the threat actor mainly used the tactic in their phishing campaigns. The detailed interpretation of the experiment is as follows. As we explained in the methodology, when no technology is used in a tactic, the tactic similarity between campaigns is marked as 0, so it is not considered a critical tactic. For example, in the case of Kimsuky’s TA0008 (*Lateral Movement*), it is judged to be a tactic that is not utilized in most of Kimsuky’s campaigns and can be judged to converge to 0. As the main tactics we consider, it is judged that Kimsuky’s various campaigns most frequently used TA0003 (*Persistence*) and TA0006 (*Credential Access*) tactics. On the other hand, in the case of Lazarus, the same technique was most frequently used in TA0002 (*Execution*), and it seems that APT37 used TA0005 (*Defense Evasion*) and TA0007 (*Discovery*) most often. The key tactics for each threat actor and the most frequently used techniques in the tactics are as follows (see Figure 3). The point is that different

Table 4: Campaigns of the Kimsuky and Lazarus group.

APT group	Campaign	Campaign description
Kimsuky	K1	A phishing campaign targeting ROK defense officials from January to June 2019. Distributes document files of various file extension types and utilizes the method of distributing backdoors through HTA files (known as babyshark).
	K2	A phishing campaign targeting ROK politicians from August 2019 to March 2020. Distributes malicious files through vba macro, and most of the C2 servers are developed with wordpress platform (presumed to be a babyshark variant).
	K3	A phishing campaign targeting ROK Ministry of National Defense officials from October 2019 to August 2020. Drops JS backdoor and self-deleting bat file using Wscript (known as appleseed).
	K4	A phishing campaign targeting academia and infrastructure such as professors and hospitals that occurred from January to August of 2021. Utilizes Wscript and drops backdoor DLL disguised as antivirus program (appleseed variant).
	K5	A phishing campaign circulated to the Ministry of Unification of the Republic of Korea and North Korean human rights activists from December 2019 to September 2020. Loads Powershell script through Word document macro and drops additional malware with a specific extension such as .down is downloaded (known as flowerpower).
	K6	A phishing campaign distributed from February 2020 to May 2021 with contents such as financial transactions and corporate management to general corporations.
Lazarus Group	L1	A phishing campaign circulated to cryptocurrency investors and cryptocurrency exchange officials from June 2018 to January 2020. Distributes malware disguised as a trading program by creating an exchange page that does not exist.
	L2	A phishing campaign targeting US companies and government agencies from June 2018 to November 2019. Made of fake SSL communication and the mida packing and executes malicious behavior by option (known as hoplight).
	L3	A phishing campaign using BMP images from June 2018 to November 2019.
	L4	A phishing campaign for job seekers from June 2018 to August 2019. Downloads additional information stealing malicious code through shellcode by executing eps script when document macro in Word is allowed (known as Operation DreamJob).
	L5	Phishing campaigns conducted from June 2018 to August 2019 targeting coronavirus vaccine companies and infrastructure such as nuclear power plants. Utilize C2 server consisting of Wordpress to decode shellcode and download additional malware via base64 (variant of Operation DreamJob).

Table 5: Campaigns of the Lazarus group and APT37.

APT group	Campaign	Campaign description
Lazarus group	L6	A phishing campaign distributed to US military defense sectors from January to August 2020. Uses RAT called DRATzarus and collects all installed disk information and OS information, such as disk shape and remaining space (known as Blindingcan).
	L7	A phishing campaign distributed in the US aerospace sector from April to June 2020. Uses RAT called DRATzarus and collects all installed disk information and OS information, such as disk shape and remaining space (known as Blindingcan).
APT37	A1	A phishing campaign distributed to North Korean defectors and North Korean human rights groups from January 2019 to May 2019. Performs command control through communication with various drives such as Dropbox, Yandex, and pCloud by disguising an executable program.
	A2	A phishing campaign distributed to lawmakers from June 2020 to December 2020. Performs command control through communication with various drives such as Dropbox, Yandex, and pCloud by disguising an executable program.
	A3	A phishing campaign distributed to reporters from June to September 2021. Performs command control through communication with various drives such as Dropbox, Yandex, and pCloud by disguising an executable program.

TTPs were used in the phishing campaigns for each publicly disclosed attacker, and the attack tactics and techniques preferred by each attacker exist in common.

Countermeasures of techniques frequently used by APT groups can be provided through D3FEND [50]. For example, D3FEND suggests 8 techniques as countermeasure for T1056 (*Input Capture*): *Process Segment Execution Prevention*, *Segment Address Offset Randomization*, *Memory Boundary Tracking*, *Process Code Segment Verification*, *Software Update*, *Input Device Analysis*, *IO Port Restriction*, and *Service Binary Verification*.

4.2. Discussion.

Through this study, it was found that the key tactics of TTP used by each threat actor are different even within the phishing campaign, and it was found that

Table 6: Average similarity by tactics of collected campaigns.

	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
Avg.	1	0.4785	0.2113	0.1379	0.3893	0.4375	0.5888	0.0083	0.2450	0.4131	0.4583	0

Table 7: Similarity of phishing campaigns conducted by Kimsuky.

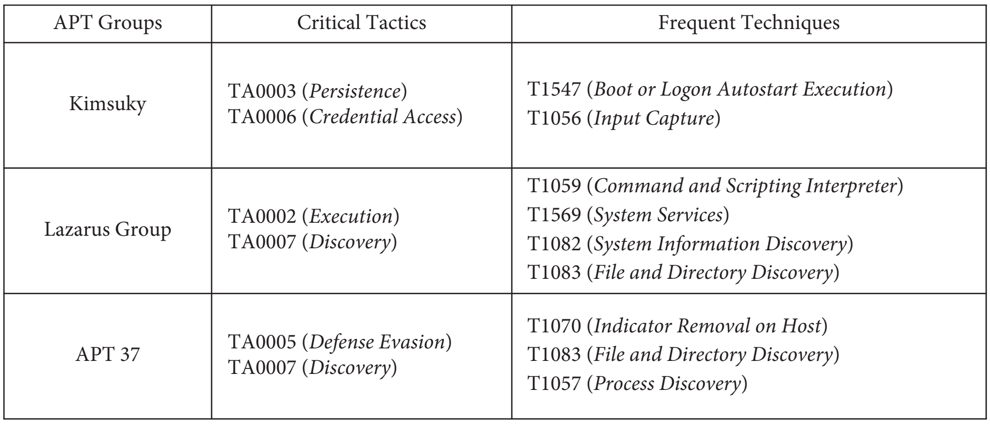
	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
(K1, K2)	1	0.9788	1	0.8944	0.9508	0.8944	0.9613	0	0.9896	0.9989	0	0
(K1, K3)	1	0.5822	0.8944	0	0.6868	1	0.7499	0	0.4352	0	0	0
(K1, K4)	1	0.5083	0.8944	0	0.6868	1	0.8504	0	0.4352	0	0	0
(K1, K5)	1	0.6509	1	0	0.4150	1	0.5458	0	0.4352	0	0	0
(K1, K6)	1	0.6509	1	0	0.2899	1	0.6967	0	0.4352	0	0	0
(K2, K3)	1	0.6508	0.8944	0	0.5726	0.8944	0.6931	0	0.3203	0	0	0
(K2, K4)	1	0.5682	0.8944	0	0.5892	0.8944	0.7704	0	0.3203	0	0	0
(K2, K5)	1	0.7276	1	0	0.3845	0.8944	0.4777	0	0.3203	0	0	0
(K2, K6)	1	0.7276	1	0	0.3234	0.8944	0.6484	0	0.3203	0	0	0
(K3, K4)	1	0.9778	0.9999	1	0.8003	1	0.9476	0	1	0.8944	0	0
(K3, K5)	1	0.8944	0.8944	0	0.4924	1	0.7505	0	1	0.9923	0	0
(K3, K6)	1	0.8944	0.8944	0	0.4924	1	0.7505	0	1	0.9923	0	0
(K4, K5)	1	0.7809	0.8944	0	0.7389	1	0.6577	0	1	0.9430	0	0
(K4, K6)	1	0.7809	0.8944	0	0.5563	1	0.8521	0	1	0.96	0	0
(K5, K6)	1	1	1	1	0.9256	1	0.8701	0	1	0.9985	0	0
Avg.	1	0.7584	0.9437	0.1930	0.5937	0.9648	0.7481	0	0.6674	0.5186	0	0

Table 8: Similarity of phishing campaigns conducted by Lazarus group.

	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
(L1, L2)	1	0.8536	0.5547	0.5477	0.3351	0	0.1474	0	0	0.6882	1	0
(L1, L3)	1	0.8427	0.5262	0.5774	0.3796	0	0.2649	0	0	0.4924	1	0
(L1, L4)	1	0.6372	0.2631	0	0	0	0.3625	0	0	0	1	0
(L1, L5)	1	0.5238	0	0	0	0	0.5443	0	0	0	1	0
(L1, L6)	1	0.6146	0	0	0.7393	0	0.4523	0	0	0.5669	1	0
(L1, L7)	1	0.6003	0	0	0.6465	0	0.2132	0	0	0.4629	1	0
(L2, L3)	1	0.9918	0.9487	0.9487	0.9713	1	0.8593	0	1	0.9319	1	0
(L2, L4)	1	0.7742	0	0	0.2362	0.2425	0.2316	0	0	0.4199	1	0
(L2, L5)	1	0.6348	0	0	0.3210	0	0.2809	0	0	0.3709	1	0
(L2, L6)	1	0.7385	0	0	0.5637	0	0.4446	0	0	0.6018	1	0
(L2, L7)	1	0.7213	0	0	0.4495	0	0.3772	0	0	0.6018	1	0
(L3, L4)	1	0.7479	0	0	0.1768	0.2425	0.3601	0	0	0.3411	1	0
(L3, L5)	1	0.6105	0.2236	0	0.2404	0	0.4506	0	0	0.3489	1	0
(L3, L6)	1	0.7991	0	0	0.6155	0	0.5791	0	0	0.3489	1	0
(L3, L7)	1	0.7805	0	0	0.4327	0	0.4801	0	0	0.4558	1	0
(L4, L5)	1	0.9224	0.6708	0.9707	0.9767	0.9412	0.9043	1	0	0.9738	1	0
(L4, L6)	1	0.4901	0	0	0	0	0.7104	0	0	0.3336	1	0
(L4, L7)	1	0.4784	0	0	0	0	0.6955	0	0	0.3742	1	0
(L5, L6)	1	0.4428	0	0	0	0	0.8616	0	0	0.4146	1	0
(L5, L7)	1	0.4388	0	0	0	0.2425	0.7543	0	0	0.3742	1	0
(L6, L7)	1	0.9989	0	0	0.8555	0	0.9000	0	0.7071	0.8165	1	0
Avg.	1	0.6972	0.1517	0.1450	0.3781	0.1271	0.5179	0.0476	0.0813	0.4723	1	0

Table 9: Similarity of phishing campaigns conducted by APT37.

	TA0001	TA0002	TA0003	TA0004	TA0005	TA0006	TA0007	TA0008	TA0009	TA0011	TA0010	TA0040
(A1, A2)	1	0.6869	0	0	0.6885	0.8321	0.9970	0	0.9268	0.9970	1	0
(A1, A3)	1	0.6633	0	0.8391	0.9744	0	0.9744	0	0.8812	0.7908	1	0
(A2, A3)	1	0.9048	0	0	0.9611	1	0.9685	0	0.7864	0.7803	1	0
Avg.	1	0.7517	0	0.2797	0.8747	0.6107	0.9800	0	0.8648	0.8560	1	0



APT Groups	Critical Tactics	Frequent Techniques
Kimsuky	TA0003 (*Persistence*) TA0006 (*Credential Access*)	T1547 (*Boot or Logon Autostart Execution*) T1056 (*Input Capture*)
Lazarus Group	TA0002 (*Execution*) TA0007 (*Discovery*)	T1059 (*Command and Scripting Interpreter*) T1569 (*System Services*) T1082 (*System Information Discovery*) T1083 (*File and Directory Discovery*)
APT 37	TA0005 (*Defense Evasion*) TA0007 (*Discovery*)	T1070 (*Indicator Removal on Host*) T1083 (*File and Directory Discovery*) T1057 (*Process Discovery*)

Figure 3: Critical tactics and frequently used techniques by the APT groups are described. Critical tactics and frequent techniques are considered as weakest link to mitigate.

the key tactics commonly used by each attacker can be distinguished. Our methodology has the advantage of predicting and defending key tactics that can be applied within each TTP if the attacker can be identified in the event of a subsequent breach. However, the methodology needs several developments. The first is the legitimacy of the campaign classification method. We divided the phishing campaigns into three criteria: victim, period, and malware used. Although it is the most used standard so far, this is a method in which analysts manually classify the disclosed information. If there is a method for automatically classifying campaigns, it is necessary to compare them with those classified by the method. The second is the lack and reliability of cyber threat intelligence data sets. Because state-sponsored threat actors cannot generate many attack events due to their limited number of people, there is insufficient data. In addition, we must suspect that the reliability of each threat actor's classified label may not be accurate. Our datasets used only the cases in which various SOC vendors agreed to specify the threat actors. However, since several cyber attributions are often overturned, additional studies need to remeasure the similarity when the threat actors are remodified. Finally, there is a limit to the number of techniques that the attack matrix can represent. Even if the average itself is not well calculated, it is natural that there are outliers in the case of a cosine comparison between campaigns in which the technique itself is not used at all, or the malicious code reuses the code at all. ATT&CK has recently been continuously adding techniques that can be expressed, and it can also be solved if the data set is further increased. We believe that the three developments identified above can be resolved by automating methodology presented in this paper and applying public data set of cyber campaigns. Cross-examining a cyber attribution is an essential part that future study should focus on. Although these limitations exist, we were able to quantitatively compare the hacking procedures of various state-sponsored threat actors through this method, and it is meaningful in that we were able to classify the tactics that should be considered the most from the defender's point of view.

5. Conclusion

Despite the experts' effort, cyber campaigns posed by state-sponsored threat actors are continuously occurring and have grown to become the biggest threat we face in the information age. In particular, phishing is used as one of the most effective first steps of advanced persistent threats. Our study proposes a method to select the most effective strategy for responding to threats by analyzing the similarity of TTPs (Tactics, Techniques, and Procedures) of cyber campaigns. The similarity analysis method presented in this paper is a practical approach to cyber threat analysis that can effectively respond to cyber threats and reclassify the names of threat actors. In order to show that this study can effectively suggest countermeasures for cyber campaigns, we collected phishing incidents by three country-based threat groups, classified them into 16 campaigns, and expressed them as ATT&CK matrix. When the similarity of each tactic of the phishing campaigns expressed by the ATT&CK matrix was calculated, the tactic with a high average similarity could identify the stage where mitigation should be focused on during the phishing campaign through the approach that the technique used had little diversity. This study analyzed phishing campaigns of 3 APT groups, Lazarus group, Kimsuky, and APT 37, which are well known as North Korean cyber threat groups. Although these three organizations prefer to use phishing as the first step, the target and purpose of the attack and the techniques used are different. We analyzed the similarity between cyber campaigns posed by threat actors by applying the cyber campaign similarity analysis method described above. Our methodology has the advantage of finding the most effective countermeasure when responding to the phishing campaign performed by the corresponding threat group. Our methodology is not limited to the threat group used in the experiment and can be applied to various cases. Our research will contribute to information security officers of public and government agencies, SOC vendors, and researchers to establish defense strategies to respond to threats. Future studies should develop into automating our methodology and applying it to information security systems. A study on the methodology to set a strategy to respond to the current cyber threat is a research field that needs attention in technical and policy areas.

Data Availability

The incident data used to support the findings of this study have not been made available because information protection policy of affiliations.

Disclosure

This paper is an extended version of a conference paper published in ART: Automated Reclassification for Threat Actors based on ATT&CK Matrix Similarity (Shin, Y.; Kim, K.; Lee, J. J.; Lee. K.), in Proceedings of the 2021 World Automation Congress (WAC), Jeju Island, Korea, August 1–5, 2021. A preprint has previously been published [44].

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Defense Acquisition Program Administration and Agency for Defense Development under the contract UD190016ED. This work was supported by the Ministry of Education of the Republic of the Korea, and National Research Foundation of Korea (NRF-2018S1A5B6075594). This work was supported by a Korea University Grant.

References

[1] A. Zibak and A. Simpson, "Cyber threat information sharing: perceived benefits and barriers," in *Proceedings of the 14th International Conference on Availability, reliability and security*, pp. 1–9, Canterbury CA, UK, 2019, August.

[2] Mitre, "MITRE ATT&CK®. MITRE ATT&CK®," 2021, https://attack.mitre.org/.

[3] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, no. 1, pp. 139–154, 2021.

[4] B. Acharya and P. Vadrevu, "{PhishPrint}: evading phishing detection crawlers by prior profiling," in *30th USENIX Security Symposium*, vol. 21, pp. 3775–3792, USENIX Security, 2021.

[5] A. Oest, Y. Safaei, P. Zhang et al., "PhishTime: continuous longitudinal measurement of the effectiveness of anti-phishing blacklists," in *Proceedings of the 29th {USENIX} Security Symposium ({USENIX} Security 20)*, pp. 379–396, San Diego, CA, USA, 2020, August.

[6] A. Das, S. Baki, A. El Aassal, R. Verma, and A. Dunbar, "SoK: a comprehensive reexamination of phishing research from the security perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 671–708, 2019.

[7] R. Verma, M. Kantarcioglu, D. Marchette, E. Leiss, and T. Solorio, "Security analytics: essential data analytics knowledge for cybersecurity professionals and students," *IEEE Security & Privacy*, vol. 13, no. 6, pp. 60–65, 2015.

[8] Y. K. Kim, J. J. Lee, M. H. Go, and K. Lee, "Analysis of the asymmetrical relationships between state actors and APT threat groups," in *Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 695–700, IEEE, Jeju, Korea (South), 2020, October.

[9] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha, and M. Guizani, "Systematization of knowledge (sok): a systematic review of software-based web phishing detection," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2797–2819, 2017.

[10] Federal Bureau of Investigation, "2020 Internet Crime Report," 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[11] A. Kang, J. Dong Lee, W. M. Kang, L. Barolli, and J. H. Park, "Security considerations for smart phone smishing attacks," in *Advances in Computer Science and its Applications*, pp. 467–473, Springer, Berlin, Germany, 2014.

[12] J. Mao, W. Tian, P. Li, T. Wei, and Z. Liang, "Phishing-alarm: robust and efficient phishing detection via page component similarity," *IEEE Access*, vol. 5, Article ID 17020, 2017.

[13] I. Corona, B. Biggio, M. Contini et al., "Deltaphish: detecting phishing webpages in compromised websites," in *European Symposium on Research in Computer Security*, pp. 370–388, Springer, New York, NY, USA, 2017.

[14] M. A. Adebowale, K. T. Lwin, E. Sánchez, and M. A. Hossain, "Intelligent web-phishing detection and protection scheme using integrated features of Images, frames and text," *Expert Systems with Applications*, vol. 115, pp. 300–313, 2019.

[15] S. Abdelnabi, K. Krombholz, and M. Fritz, "Visualphishnet: zero-day phishing website detection by visual similarity," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1681–1698, Virtual Event USA, 2020, October.

[16] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," *EURASIP Journal on Information Security*, vol. 2016, no. 1, pp. 1–11, 2016.

[17] S. C. Jeeva and E. B. Rajsingh, "Intelligent phishing url detection using association rule mining," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1–19, 2016.

[18] G. Sonowal and K. S. Kuppusamy, "PhiDMA - a phishing detection model with multi-filter approach," *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 99–112, 2020.

[19] C. Johnson, B. Khadka, R. B. Basnet, and T. Doleck, "Towards detecting and classifying malicious URLs using deep learning," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl*, vol. 11, no. 4, pp. 31–48, 2020.

[20] T. Peng, I. Harris, and Y. Sawa, "Detecting phishing attacks using natural language processing and machine learning," in *Proceedings of the 2018 Ieee 12th International Conference on Semantic Computing (Icsc)*, pp. 300-301, IEEE, Laguna Hills, CA, USA, 2018, January.

[21] T. Gangavarapu, C. D. Jaidhar, and B. Chanduka, "Applicability of machine learning in spam and phishing email

filtering: review and approaches," *Artificial Intelligence Review*, vol. 53, no. 7, 2020.

[22] R. Alabdan, "Phishing attacks survey: types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, p. 168, 2020.

[23] A. Sundararaj and G. Kul, "Impact analysis of training data characteristics for phishing email classification," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 12, pp. 85–98, 2021.

[24] Y. Choi, "Interim investigation result of korea Hydro & nuclear power cyber terror. Seoul central District public Prosecutors' Office," 2015, https://cybercid.spo.go.kr/attachment/cfile30.uf@2331FF4357689A1E1ECA31.PDF.

[25] Unit 42, "New BabyShark malware targets U.S. National security think tanks. Paloalto networks," 2019, https://unit42.paloaltonetworks.com/new-babyshark-malware-targets-u-s-national-security-think-tanks/.

[26] Cybersecurity and Infrastructure Security Agency, "North Korean advanced persistent threat focus: Kimsuky," 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-301a.

[27] Threat Intelligence Team, "APTs and COVID-19: how advanced persistent threats use the coronavirus as a lure. Malwarebytes Labs," 2020, https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/.

[28] Alyac, "Kimsuky's APT attack impersonating Korean cryptocurrency exchange EstSecurity," 2019, https://blog.alyac.co.kr/2336.

[29] Anomali Threat Research, "Suspected North Korean cyber espionage campaign targets multiple foreign ministries and think tanks. The anomali blog," 2019, https://www.anomali.com/blog/suspected-north-korean-cyber-espionage-campaign-targets-multiple-foreign-ministries-and-think-tanks.

[30] Rsa Conference, "Hacking exposed: next generation attacks [video]," 2015, https://www.youtube.com/watch?v=4TjPwadYsc8.

[31] H. Kim, "5G core network security issues and attack classification from network protocol perspective," *J. Internet Serv. Inf. Secur.*vol. 10, no. 2, pp. 1–15, 2020.

[32] A. Kitana, I. Traore, and W. Isaac, "Towards an epidemic SMS-based cellular botnet," *J. Internet Serv. Inf. Secur*, vol. 10, no. 4, pp. 38–58, 2020.

[33] D. Oktavianto and I. Muhardianto, *Cuckoo Malware Analysis*, Packt Publishing Ltd, Birmingham, UK, 2013.

[34] V. Sihag, M. Vardhan, P. Singh, G. Choudhary, and S. Son, "De-lady: deep learning based android malware detection using dynamic features," *Journal of Internet Services and Information Security (JISIS)*, vol. 11, no. 2, pp. 34–45, 2021.

[35] C. Willems, T. Holz, and F. Freiling, "Toward automated dynamic malware analysis using cwsandbox," *IEEE Security and Privacy Magazine*, vol. 5, no. 2, pp. 32–39, 2007.

[36] Z. Tzermias, G. Sykiotakis, M. Polychronakis, and E. P. Markatos, "Combining static and dynamic analysis for the detection of malicious documents," in *Proceedings of the Fourth European Workshop on System Security*, pp. 1–6, Salzburg, Austria, 2011, April.

[37] M. Eskandari, Z. Khorshidpour, and S. Hashemi, "HDM-Analyser: a hybrid analysis approach based on data mining techniques for malware detection," *Journal of Computer Virology and Hacking Techniques*, vol. 9, no. 2, pp. 77–93, 2013.

[38] A. La Marra, F. Martinelli, F. Mercaldo, A. Saracino, and M. Sheikhalishahi, "D-BRIDEMAID: a distributed framework for collaborative and dynamic analysis of android malware," *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*vol. 11, no. 3, pp. 1–28, 2020.

[39] L. LC. Joe Security, "Deep malware analysis - Joe sandbox," 2021, https://www.joesecurity.org/.

[40] D. Maier, T. Müller, and M. Protsenko, "Divide-and-conquer: why android malware cannot be stopped," in *Proceedings of the 2014 Ninth International Conference on Availability, Reliability and Security*, pp. 30–39, IEEE, Fribourg, Switzerland, 2014, September.

[41] The Center for Threat-Informed Defense, "TRAM is an open-source platform designed to advance research into automating the mapping of cyber threat intelligence reports to MITRE ATT&CK®. GitHub," 2021, https://github.com/center-for-threat-informed-defense/tram/.

[42] V. Legoy, M. Caselli, C. Seifert, and A. Peter, "Automated retrieval of ATT&CK tactics and techniques for cyber threat reports," 2020, https://arxiv.org/abs/2004.14322.

[43] R. Howard and R. Olson, "Implementing intrusion kill chain strategies," *The Cyber Defense Review*, vol. 5, no. 3, pp. 59–76, 2020.

[44] Y. Shin, K. Kim, J. J. Lee, and K. Lee, "ART: automated reclassification for threat actors based on ATT&CK matrix similarity," in *Proceedings of the 2021 World Automation Congress (WAC)*, pp. 15–20, IEEE, Taipei, Taiwan, 2021, August.

[45] K. Kim, Y. Shin, J. Lee, and K. Lee, "Automatically attributing mobile threat actors by vectorized ATT&CK matrix and paired indicator," *Sensors*, vol. 21, no. 19, p. 6522, 2021.

[46] M. Sahrom Abu, S. Rahayu Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence - issue and challenges," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, no. 1, pp. 371–379, 2018.

[47] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the ioc game: toward automatic discovery and analysis of open-source cyber threat intelligence," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 755–766, Vienna, Austria, 2016, October.

[48] S. Qamar, Z. Anwar, M. A. Rahman, E. Al-Shaer, and B.-T. Chu, "Data-driven analytics for cyber-threat intelligence and information sharing," *Computers & Security*, vol. 67, pp. 35–58, 2017.

[49] U. Noor, Z. Anwar, T. Amjad, and K.-K. R. Choo, "A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise," *Future Generation Computer Systems*, vol. 96, pp. 227–242, 2019.

[50] P. E. Kaloroumakis and M. J. Smith, "Toward a knowledge graph of cybersecurity countermeasures," Technical report, 2021.