

Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups

JAEIL LEE¹, YONGJOON LEE², DONGHWAN LEE³, HYUKJIN KWON⁴, AND DONGKYOO SHIN^{ID}³

¹Korea Internet & Security Agency (KISA), Naju 58324, Republic of Korea

²Department of Cyber Security, Far East University, Eumseong-gun 27601, Republic of Korea

³Department of Computer Engineering, Convergence Engineering for Intelligent Drone, Sejong University, Seoul 05006, Republic of Korea

⁴Center for Military Analysis Planning, Korea Institute for Defense Analyses (KIDA), Seoul 02455, Republic of Korea

Corresponding author: Dongkyoo Shin (shindk@sejong.ac.kr)

This work was supported in part by the Defense Acquisition Program Administration, and in part by the Agency for Defense Development under Contract UD190016ED.

ABSTRACT In recent years, there has been an increase in the number of phishing attacks targeting people in the fields of defense, security, and diplomacy around the world. In particular, hacking attack group Kimsuky has been conducting phishing attacks to collect key information from public institutions since 2013. The main feature of the attack techniques used by the Kimsuky attack group are to conceal malicious code in phishing e-mails disguised as normal e-mails to spread a document file that is vulnerable to security, such as a Hangul file, or to induce interest through a social engineering attack technique to collect account information. This study classified the types of phishing e-mail attacks into spoofed e-mails, e-mail body vulnerability use, and attached file spoofing, and detailed analyses of their attack methods, such as commonality and characteristic analyses, were performed to analyze the profile of this phishing e-mail attack group. Based on the results, the purpose of the attacking group was determined to be intelligence gathering because it focused on phishing attacks targeting Korean diplomatic and defense public institutions and related foreign institutions. Finally, a countermeasure that can be used by mail service providers and mail users to respond to phishing e-mails is suggested.

INDEX TERMS Phishing mail, hacking, cyber attack group, profiling.

I. INTRODUCTION

Recently, phishing attacks targeting people in the fields of defense, security, and diplomacy have rapidly been increasing around the world. In particular, the hacking attack group Kimsuky has been engaged in phishing attacks since 2013 to collect major information from public institutions [1]. This attack group was given the name Kimsuky because a report released in 2013 by the anti-virus company Kaspersky confirmed that the mail account used by this group for certain cyber attacks was registered as Kimsuky. This group is known to use e-mail to conduct cyber attacks to collect sensitive information from officials in the fields of defense, national security, and diplomacy. Its main techniques seem to be collecting account information by distributing document files such as vulnerable Hangul documents created by

the Hangul Word Processing (HWP) application that conceal malicious code in phishing e-mails disguised as regular e-mails and attracting users' attention with social engineering attack techniques [2].

The Kimsuky attack group has been reported to pursue targets around the world and gain information on various topics of interest from the North Korean government [3]. The cases of cyber attacks by the Kimsuky attack group within South Korea are listed in Table 1. A joint investigation team of the South Korean government concluded in 2014 that the Kimsuky attack group was operating based on the composition and operation method of the malicious code examined. Its usage was similar to that of the shellcode used by the existing Kimsuky attack group, and the IP address used in the previous attack was a partial match to the Chinese IP band used in the previous attack. Since then, cyber attacks have continued to be carried out against public institutions in Korea [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang^{ID}.

TABLE 1. Cases of cyber attack by kimsuky attack group in South Korea.

Date	Incident
2013.09	Kaspersky, Named Kimsuky
2014.12	KHNP (Korea Hydro & Nuclear Power) Attack
2016.01	Sent e-mail impersonating Blue House (Presidential office)
2018.05	Sent e-mail impersonating Blue House
2019.01	Sent e-mail impersonating Ministry of Unification
2019.01	Sent e-mail impersonating Ministry of Foreign Affairs
2019.02	Sent e-mail impersonating Ministry of National Defense

The attacks by the Kimsuky attack group are different from a general phishing attack because it is actively targeting Korea, Japan, and the United States for political purposes [3]. Unlike general phishing attacks targeting civilians for financial purposes, the Kimsuky attack group's activities have focused on phishing attacks targeting Korean diplomatic and defense public institutions and related foreign institutions. Thus, it has been concluded that these have had the purpose of intelligence gathering. This study determined the main characteristics of and countermeasures to attacks by this attack group by analyzing the correlation between the phishing mail, mail destinations, and malicious code distribution by the Kimsuky attack group since 2018.

II. TYPES OF PHISHING MAIL ATTACKS

The social engineering method used by the Kimsuky attack group is the spear phishing method, which is a social engineering attack targeting a specific organization [4]. Public information such as the e-mail addresses and names of the employees of diplomatic and defense public institutions was collected in the first stage. Documents and e-mails about recent issues related to diplomacy and defense were forged in the second stage, and a social engineering method was used to send e-mails disguised as coming from workers in the diplomatic and defense fields in the third stage.

Phishing refers to an attack method using an e-mail that combines the terms private data and fishing. This technique is a method in which an attacker conceals malicious code in an e-mail or messenger, disguising it as normal content to steal information (that is confidential, important, personal, etc.) from an Internet user. The Kimsuky attack group continues to carry out cyberattacks such as account information capture and malicious code distribution by using phishing mail as a major attack route. This kind of attack can be applied to mobile networks, wireless sensor networks, ad hoc networks, and fog computing environments [5, 6, 7, 8, 9].

This paper reports the results of an analysis of the association of the phishing e-mails used by the Kimsuky group. The group was comprehensively analyzed by investigating phishing e-mails, disguised documents, malware, waypoint IPs, and 13 victim servers.

A. DISGUISED E-MAIL

1) PORTAL SITE INFORMATION MAIL PHISHING ATTACK

In recent times, personal information is being stolen continuously, and account theft and sales are occurring as a result

of leaked personal information [10]. As shown in Fig. 1, a portal site provides users with an e-mail for access to accounts and password change records. The attacker uses these guide e-mails to send e-mails disguised as e-mails from portal site customer centers, which are used in an attack technique to induce users to provide account information. This is a typical social engineering attack method that impersonates a trusted sender called the customer center of the portal site.

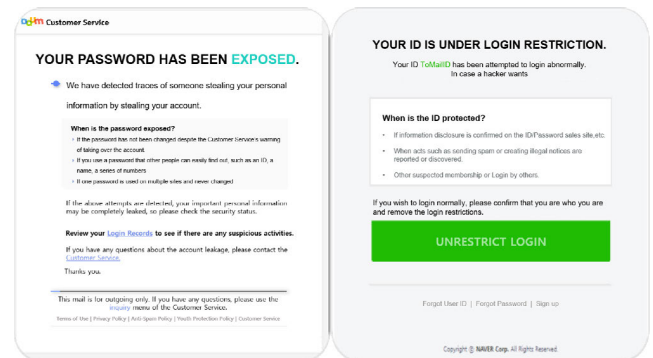


FIGURE 1. Phishing attack as counterfeit portal reminder mail. The hacking group sent an e-mail to induce additional logins to expose the member's password.

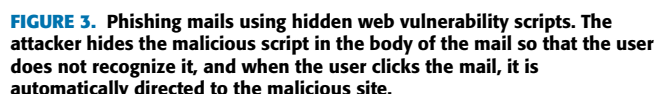
2) SECURE E-MAIL PHISHING ATTACK

Recently, as cyber-attacks using phishing e-mail have increased, more and more companies are using secure e-mail to enhance the security of mail text [11]. Secure e-mail is also widely used in government and financial institutions. However, as seen in Fig. 2, an attacker can send phishing e-mails disguised as secure e-mail. The body of the secure e-mail can only be read after entering a specific password. However, phishing e-mails automatically connect to phishing sites without entering passwords when the user presses the Mail View button, induces the user to enter their account information, and provides attachments when acquiring account information.

B. E-MAIL BODY VULNERABILITY

An attacker could insert a vulnerability into the body of the e-mail, causing the user to connect to a phishing site simply by reading the e-mail. Traditional methods require mail users to click on links, read attached files, and so on. In the case of using the e-mail body vulnerability, a hidden malicious script is executed immediately when the e-mail is read and connects to a phishing site [12].

As shown in Fig. 3, it is automatically connected to the phishing site immediately when the mail is read and the attacker induces the user to enter their account information. In the case of an attack using mail body Web vulnerabilities, webmail or a mail client program supporting HTML is used.




1) PHISHING SITE CONNECTION THROUGH DISGUISED ATTACHED FILES

2) MALICIOUS CODE HIDDEN E-MAIL

U.S.-North xxxxx Summit and U.S.-South Korea Relations.2.18

File(F) Edit(E) View(V) Tool(T) Message(M) Help(H)

Reply Reply All Forward Print Delete Previous Next

From : =?EUC-KR?B??=
Date : Wednesday, February 18, 2019, 15:47
To : [REDACTED]
Subject : U.S.-North xxxxx Summit and U.S.-South Korea Relations.2.18
Attached :  U.S.-North xxxxx Summit and U.S.-South Korea Relations.2.18.hwp

U.S.-North xxxxx Summit and U.S.-South Korea Relations.2.18

FIGURE 4. Phishing mails using counterfeit attached files. The hacking group attaches malicious code to a document file related to defense and diplomacy, and downloads the malicious code when the document file is clicked.

Host Entry	Hex	Hex (Decompress)
BinData		
BIN0001.jpg	0000 2f 73 68 65 6c 6c 63 6f 64 65 20 3c 39 30 39 30	/shellcode <9090
BIN0002.eps	0010 39 30 39 30 39 30 39 30 39 30 39 30 39 30 39 30	90909090909090909090
BodyText	0020 45 38 30 30 30 30 30 30 30 30 35 45 42 39 33 34	E8000000005EB934
Section()	0030 31 34 45 32 30 30 38 31 45 39 30 38 31 34 45 32	14E20081E90814E2

FIGURE 5. HWP files containing malicious code. This is the process of executing the malicious code by hiding it in Hangul Word Processing (HWP) documents used by public institutions in Korea.

A. COMMON CHARACTERISTICS OF PHISHING MAIL ATTACKS

1) PHISHING SITE SOURCE CODE

Recently, personal information has been stolen continuously, and account theft and sales are occurring as a result of leaked personal information [10]. As shown in Table 2, a portal site provides users with an e-mail for accessing accounts and password change records. The attacker uses these guide e-mails to produce disguised e-mails that appear to be sent from portal site customer centers and then uses them as an attack technique to induce users to provide

TABLE 2. Comparative analysis of similarities in phishing page's source codes.

Analysis Case	Comparison of phishing page's source codes
2016 Phishing mail (KHNP)	<pre>// TopController.php // Write the log to a file. protected function writingLog(\$argLog) // Get the user's ip \$userip = \$_SERVER['REMOTE_ADDR']; // Writes the log \$logfilename = "log_" . \$userip . ".info.txt"; \$logfplog = fopen(RESET_PATH . "/" . \$logfilename, "a"); fwrite(\$logfplog, \$argLog); fclose(\$logfplog); // Check if you should get a user's password. protected function mustGetPassword(\$userid)</pre>
2019 Phishing mail (Portal)	<pre>// TopController.php // Write the log to a file. protected function writingLog(\$argLog) // Get the user's ip \$userip = \$_SERVER['REMOTE_ADDR']; // Writes the log \$logfilename = "log_" . \$userip . ".info.txt"; \$logfplog = fopen(RESET_PATH . "/" . \$logfilename, "a"); fwrite(\$logfplog, \$argLog); fclose(\$logfplog); // Check if you should get a user's password. protected function mustGetPassword(\$userid)</pre>

account information. This is a typical social engineering attack method that impersonates a trusted sender called the customer center of the portal site.

2) FTP ACCESS AND MAIL ORIGIN ADDRESS

As shown in Table 3, the attacker accessed many website FTP accounts hacked through a specific IP address, and sent phishing mail. This was because attackers prefer FTP access and sending mail via a specific server.

3) ATTACKER MAIL ACCOUNT

The attacker used the prxxxxxxx@hanmail.net e-mail account to send phishing e-mails. As shown in Table 4, this account was identical to the attacker's mail account exploited as a phishing site.

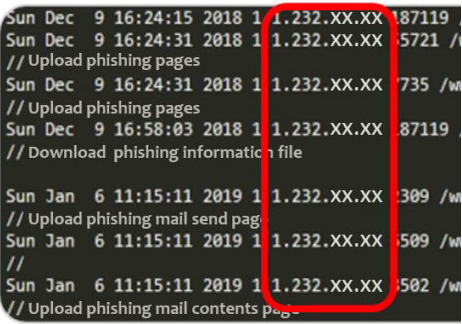
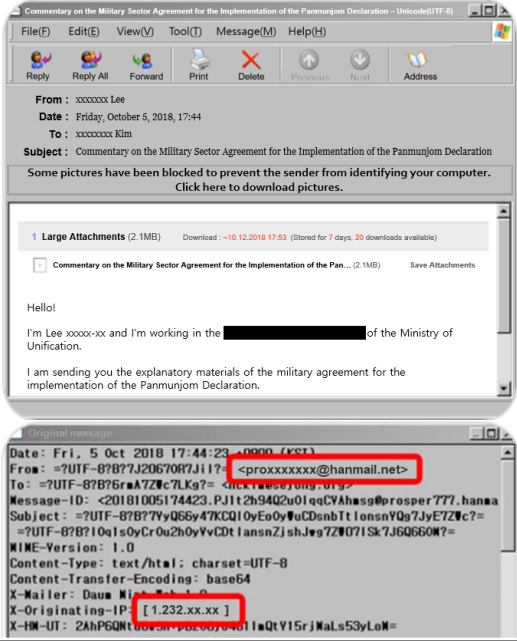
It was also confirmed that the victim server exploited as a phishing site had another attacker account, paxxxxxx@○○○.net. In addition, in the mail log of the phishing mail sending server, it was confirmed that the paxxxxxx account had a record of receiving phishing mail from attackers. The attacker is believed to have conducted a send test to the attacker account to test whether the mail was sent smoothly before the actual phishing mail attack.

The attacker sent a phishing e-mail using the mail function from several mail-sending servers, and the PHPMailer open-source mail library was used for the sending page to test with an attacker's account. It is assumed that this library was used to avoid leaving mail logs on the server because the SMTP service is not used on that server, but it uses an external SMTP server.

4) REUSE PHISHING MAIL SERVER

The server that the attacker hacked and exploited as a phishing mail server was reused by the hacked server to distribute

TABLE 3. Comparative analysis of similarities in FTP's addresses and mail's addresses.

Addresses	Comparison of phishing page's source codes
FTP Hacking Access IP	
Phishing mail Source IP	

malicious code. The attackers also exploited the history of the websites that were previously exploited as malware distribution sites. It is estimated that the affected server has a security vulnerability and is constantly being exploited by attackers.

5) PASS THROUGH IP ADDRESS BAND

The Kimsuky attack group continued to use the 175.167.x.x IP band when attempting cyberattacks. This IP band is used in Shenyang, China. The IP band was also used in hacking mail attacks on KHNP (Korea Hydro & Nuclear Power) and Blue House. Table 5 shows the IP of the attacker in the corresponding IP band based on an analysis of the FTP log and weblog of the abused server.

6) PASS THROUGH HOSTING SERVICE

Specific hosting services were mainly used on phishing sites used by attackers. Hostinger, an overseas hosting service, has been used, which makes it difficult to request information to

TABLE 4. Analysis of connection accounts of phishing servers and phishing mails.

Analysis Case	Comparison of phishing page's source codes
Phishing mail sending Account	<pre> \$mail->Username = "proxxxxxxx@hanmail.net"; \$mail->Password = " \$mail->CharSet = 'UTF-8'; \$mail->From = \$fmail; \$mail->FromName = \$fname; \$mail->Subject = \$subject; </pre>
Phishing site access Account	<pre> postfix/smtp[18399]: 2BF9664066A: to= relay postfix/smtp[18400]: 2D46A640769: to= relay~ postfix/smtp[26459]: 02B876406F6: to= reason. See https://help.yahoo.com/kb/postmaster/SLN7253.html postfix/smtp[26458]: 004C26406F5: to= </pre>

TABLE 5. Attack ip bands on damaged servers.

Abused Server	Connected IP	Collected Place	First Connection Time	Who
Religious Sites	175.167.xxx.xx	Web Log	2017.10.03	Shenyang
	175.167.xxx.xx	Web Log	2019.02.10	Shenyang
	175.167.xxx.xx	Web Log	2019.02.11	Shenyang
Academic Sites	175.167.xxx.xxx	Web Error Log	2018.08.19	Shenyang
	175.167.xxx.xxx	Web Error Log	2018.08.22	Shenyang
Dokdo Related Sites	175.167.xxx.xxx	Web Log	2019.03.17	Shenyang
	175.167.xxx.xxx	Web Log	2019.03.18	Shenyang
	175.167.xxx.xxx	Web Log	2019.03.20	Shenyang
	175.167.xxx.xx	Web Log	2019.03.20	Shenyang
	175.167.xxx.xxx	Web Log	2019.03.20	Shenyang
	175.167.xxx.xxx	Web Log	2019.03.21	Shenyang

analyze for a hacking incident investigation in South Korea. Moreover, anonymity is guaranteed, and it is presumed that it was used as the main route because it can be used by opening other domains even if blocked. As shown in Table 6, the attacker opened seven free domains on Hostinger and used them for the attack, combining the domain list with addresses similar to normal sites to create domains and use them for phishing attacks.

TABLE 6. Lists of domains opened through overseas hosting company (hostinger).

Hostinger Free Domain List			
.esy.es	96.lt	pe.hu	hol.es
16mb.com	000webhostapp.com	890m.com	

B. ANALYSIS OF PHISHING MAIL ATTACK CHARACTERISTICS

1) COMPARATIVE ANALYSIS OF SIMILARITIES IN PHISHING MAIL DAMAGE SERVERS

The analysis of the servers exploited by the Kimsuky attack group confirmed common ground. As shown in Fig. 6, the attacker not only accessed the FTP accounts of multiple websites with the same IP address but also sent phishing mail to the mail sender. In addition, a mail sending test was

Attack Method	Damaged Server	Busan xxxxx Academy	Copy xxxxx	Meixxxx	xxxxxx Middle Church	Conxxx	xxxx Friends	Itxx	xxxxx Math Academy	xxxxx Sarang	Epxxxx	KRxxx	xxxxx Thai	Wxxxxx
FTP account outflow		●	●	●	●	●	●	●	●	●	●	●	●	●
Send phishing mail		●	●		●	●	●			●	●		●	
Phishing site abuse		●	●			●				●	●			●
Distribution of malicious code			●		●	●	●	●	●	●				
Attacker IP		●	●	●		●	●	●			●		●	
Attacker Accounts				●		●					●			
Using webshell				●	●	●		●	●	●				
175.167. IP Band					●	●				●		●		

FIGURE 6. Comparative analysis of similarities in damaged servers. Comprehensive analyses of the attack IP, victim server, and related e-mail transmission evidence for the hacking group were conducted.

performed using a specific account, where a similar domain address was used.

2) KEY FEATURES OF ATTACK GROUPS

South Korea and foreign professional security companies analyzed the above phishing sites, malicious codes, etc., and identified Kimsuky as an attack group that wants to collect sensitive and important information such as that related to defense, security, and diplomacy. The characteristics of the attack group identified through Kimsuky's phishing mail attack analysis are as follows.

First, because it was confirmed that the login was successful without failure with the FTP account for most of the exploited servers, it was estimated that attempts were made to access the server through the leaked FTP account.

Second, the mail sender, phishing site, and malicious code were uploaded through FTP, and the acquired account information was downloaded through the same FTP.

Third, some of the servers used as phishing mail origins and phishing sites were used to distribute not only phishing mail but also additional uploaded malicious codes.

Fourth, because most of the malicious code focused on information collection and keylogging rather than remote control, it was presumed that the attacker was aiming to collect specific important information rather than taking actions for monetary purposes.

Fifth, it continuously generated new phishing pages and used various methods such as inducing phishing page connections using zero-day attacks.

IV. PURPOSE OF AND COUNTERMEASURES TO PHISHING MAIL ATTACKS

A. PURPOSE OF PHISHING MAIL ATTACKS

The purpose of the attacker sending phishing e-mail was to gain intelligence by spreading malicious code and stealing account information. The theft of personal information and account information was carried out by sending phishing e-mails to e-mail addresses posted on the Internet.

There are two ways to falsify the origin of phishing e-mails, by disguising it as coming from a portal site customer center or a public institution or company related to the target. The portal site disguise makes it easy to collect e-mail addresses and e-mails can be sent immediately, but the success rate is low because mail users can suspect it. When disguising the origin as a public institution or company, additional information collection is necessary to forge mail with content related to the target of the attack, but it shows a high attack success rate.

B. PHISHING MAIL ATTACK COUNTERMEASURES

1) E-MAIL SERVICE PROVIDER

First, e-mail service providers need to strengthen their security to prevent hacking from phishing mail attackers. The phishing attack group collects FTP account information through analyses and uses it for hacking. Thus, enhanced authentication of the FTP account is required. Additionally, it is necessary to separate the network to prevent access to FTP remotely and continuously manage FTP history. A firewall must also be built to block access to the mail server from the outside. In particular, because the attack group uses an external hosting company domain, the firewall needs to block overseas hosting domains. The attacker hacked and exploited a vulnerable website as well as an FTP account. Therefore, web service providers need to block external attacks such as the insertion of malicious scripts by building a web firewall to prevent hackers from hacking through webmail access. Considering the characteristic of hacking groups reusing similar malicious scripts, the detection pattern should be registered in the web firewall. Phishing mail attackers used scripts that used web vulnerabilities in the body of the mail. Therefore, mail service operators should provide mail services after pre-validation of secure coding to avoid cross-site scripting (XSS) vulnerabilities on their mail reading pages in case the mail service is hacked and an attacker sends phishing mail.

2) E-MAIL SERVICE USERS

E-mail users need increased awareness of social engineering methods to prevent phishing e-mails. First, they need to thoroughly manage their account, using an e-mail password with more than 9 digits that include uppercase letters, lowercase letters, numbers, and special symbols. In addition, this password should be changed once every three months, and if necessary, a two-factor authentication login using SMS and OTP should be used. To prevent account leakage, a function should be set to block login from overseas, and the login history should be checked from time to time. If a file is attached to an e-mail or contains an external link, a check should be made to determine whether the e-mail was sent from a valid address before it is read, and re-checked to determine whether there was a send and receive e-mail history.

If it is necessary to enter the user's account information before downloading a file attached to an e-mail, their

access should be blocked. In addition, the software related to HWP documents, MS-Office documents, and PDF documents exploited by malicious codes should be patched and managed with the latest version.

If a link to an external site is included in the body of an e-mail, do not click the link but check whether it is a valid site in a new window and then connect.

V. CONCLUSION

This study analyzed a phishing attack group that is targeting those involved in defense, security, and unification, which has been rapidly increasing in recent years. Since 2013, the hacking attack group Kimsuky has been working to gather key information from public institutions through phishing attacks. An investigation of the attack techniques of the Kimsuky group since 2018 showed that the phishing pages used in the attack were not only sophisticated enough to be difficult for security experts to distinguish, but also used various disguises such as customer centers and e-mails. It pretends to be a defense and government agency using typical social engineering attack techniques. In addition, from a technical perspective, as analyzed in this paper, it was difficult for ordinary e-mail users to respond only with their interest because it used advanced attack techniques such as exploiting large attachment spoofing vulnerabilities.

Therefore, regular users' e-mail accounts are constantly being leaked, and countermeasures are urgently needed. In the case of remote control using leaked account information or the sending of phishing e-mails, it is very difficult to take action because it is not possible to immediately check whether the actual account has been stolen, and because sensitive information such as a password is included, a careful approach is required.

This study conducted a profiling analysis of the Kimsuky phishing mail attack group to determine its phishing mail attack types and the purpose of their attacks. In addition, it was shown that these attacking organizations are continuously advancing phishing e-mail attack techniques to collect important information such as that related to defense, security, and diplomacy. Moreover, a countermeasure that could be used by mail service providers and mail users to respond to phishing e-mails was presented.

ACKNOWLEDGMENT

(Jaeil Lee and Yongjoon Lee are co-first authors.)

REFERENCES

- [1] K. Ji-Young, L. J. In, and K. K. Gon, "The all-purpose sword: North Korea's cyber operations and strategies," in *Proc. 11th Int. Conf. Cyber Conflict (CyCon)*, Tallinn, Estonia, May 2019, pp. 1–20.
- [2] V. Suganya, "A review on phishing attacks and various anti phishing techniques," *Int. J. Comput. Appl.*, vol. 139, no. 1, pp. 20–23, Apr. 2016.
- [3] Cybersecurity & Infrastructure Security Agency, *North Korean Advanced Persistent Threat Focus: Kimsuky*. Accessed: Mar. 31, 2021. [Online]. Available: <https://us-cert.cisa.gov/ncas/alerts/aa20-301a>

- [4] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018.
- [5] M. Adil, M. A. Almaiah, A. O. Alsayed, and O. Almomani, "An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks," *Sensors*, vol. 20, no. 8, p. 2311, Apr. 2020.
- [6] A. K. A. Hwaitat, M. Amin, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, "Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks," *Quintana*, vol. 11, no. 4, pp. 614–624, 2020.
- [7] M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, "A new hybrid text encryption approach over mobile ad hoc network," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6461–6471, 2020.
- [8] A. K. Al Hwaitat, S. Manaseer, R. M. Al-Sayed, M. A. Almaiah, and O. Almomani, "An investigation of digital forensics for shamoon attack behaviour in FOG computing and threat intelligence for incident response," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 7, pp. 277–290, 2020.
- [9] A. K. Al Hwaitat, S. Manaseer, R. M. Al-Sayed, M. A. Almaiah, and O. Almomani, "An investigator digital forensics frequencies particle swarm optimization for detection and classification of APT attack in FOG computing environment (IDF-FPSO)," *J. Theor. Appl. Inf. Technol.*, vol. 98, no. 7, pp. 937–952, 2020.
- [10] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," *Comput. Sci. Rev.*, vol. 29, pp. 44–55, Aug. 2018.
- [11] Y. J. Lee and C. B. Lee, "An fingerprint authentication model of ERM system using private key escrow management server," *J. Korea Academia Ind. Cooperation Soc.*, vol. 20, no. 6, pp. 1–8, 2019, doi: [10.5762/KAIS.2019.20.6.1](https://doi.org/10.5762/KAIS.2019.20.6.1).
- [12] J.-Y. Kim, S.-J. Bu, and S.-B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders," *Inf. Sci.*, vols. 460–461, pp. 83–102, Sep. 2018.
- [13] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs," in *Proc. 15th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, 2009, p. 1245.
- [14] Y. J. Lee and T. Y. Jeon, "A malware detection method using analysis of malicious script patterns," *J. Korea Academia Ind. Cooperation Soc.*, vol. 20, no. 7, pp. 613–621, 2019, doi: [10.5762/KAIS.2019.20.7.613](https://doi.org/10.5762/KAIS.2019.20.7.613).
- [15] R. Verma and K. Dyer, "On the character of phishing URLs: Accurate and robust statistical learning classifiers," in *Proc. 5th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2015, pp. 111–122.



interests include information security and convergence security.

JAEL LEE received the B.S. and M.S. degrees in statistics from Seoul National University, South Korea, in 1986 and 1988, respectively, and the Ph.D. degree in computer science from Yonsei University, South Korea, in 2006. From 1996 to 2018, he was a General Manager at the Korea Internet & Security Agency (KISA), where he is currently a Chief Researcher. He is the Vice-President of the Korea Institute of Information Security & Cryptology (KIISC). His research



interests include industrial security, cybersecurity, and internal information leakage prevention.

YONGJOON LEE received the Ph.D. degree in computer science from Soongsil University, in 2005. From 2006 to 2009, he was a Deputy Researcher at the LG CNS Technology Research Department. From 2010 to 2015, he was a Senior Research Fellow with the Korea Internet & Security (KISA). From 2016 to 2019, he was a Digital Forensic Research Officer at Information Security Office, Defense Security Support Command, South Korea. He is currently an Assistant Professor with the Department of Cyber Security, Far East University, South Korea.



DONGHWAN LEE received the B.S. degree in computer science from Soongsil University, in 2018. He is currently pursuing the M.S. degree with Sejong University. His research interests include machine learning, data mining, and cyber security.



HYUKJIN KWON received the B.S., M.S., and Ph.D. degrees in industrial engineering from Sungkyunkwan University, Seoul, South Korea, in 1989, 1991, and 2000, respectively. From 1991 to 2017, he was the Director of the Research Planning Division, Korea Institute for Defense Analyses (KIDA), and researched information system assessment and information system development. From 2017 to 2020, he was the Director General of the Information Planning Bureau, Ministry of National Defense, South Korea. He is currently a Senior Research Fellow with the Center for Military Analysis Planning, KIDA. He is the author and coauthor of a number of academic articles. His research interests include cyber security and performance for information systems.



DONGKYOO SHIN received the B.S. degree in computer science from Seoul National University, South Korea, in 1986, the M.S. degree in computer science from the Illinois Institute of Technology, Chicago, IL, USA, in 1992, and the Ph.D. degree in computer science from Texas A&M University, College Station, TX, USA, in 1997. From 1986 to 1991, he worked with the Korea Institute of Defense Analyses, where he developed database application software. From 1997 to 1998, he worked with the Multimedia Research Institute, Hyundai Electronics Company, South Korea, as a Principal Researcher. He is currently a Professor with the Department of Computer Engineering, Sejong University, South Korea. His research interests include information security, data mining, and ubiquitous computing.

...