# Changes of Cyber Hacking Attack Aspect of North Korea Cyber-Attack Groups Applying MITRE ATT&CK

GwangHyun Ahn[1], Seon-a Lee[2], and Won-hyung Park[2]*

[1]Department of Computer Engineering, Sejong University, Seoul, South Korea
rhkdgus8781@sju.ac.kr

[2]Department of Information Protection Engineering, Sangmyung University, Cheonan, South Korea
sunnie39@naver.com, whpark@smu.ac.kr

**Abstract**

In the process of preparing cyber security and space security enhancement plans worldwide, cyber attacks such as North Korean cyber attacker groups Thallium, Kimsuky, Geumseong 121, and Lazarus have developed into advanced levels and continue to threaten cyber security and space security. The North Korean cyber attack team has been strengthening cyber attacks by using social engineering techniques through political and social issues for unspecified numbers of people using detailed attack stages, procedures, technologies and tools using cyber kill chain technology, starting with APT attacks in the past. In this paper, we use the enemy cyber threat analysis data to analyze the correlation between North Korean cyber attack groups by applying MITRE's ATT&CK, and estimate the source of attack origin such as open vulnerability, malicious code information, attack group cyber attack characteristics, and attack cases. Through this, we propose Aspect change in cyber hacking attacks by North Korean cyber attack groups based on ATT&CK.

**Keywords**: MITRE ATT&CK, Kimsuky, Thallium, Lazarus, Geumseong 121, APT, Cyber KillChain, North Korea

## 1 Introduction

As measures are being prepared to strengthen cybersecurity and space security policies worldwide, it is increasingly necessary to analyze and respond to attack groups occurring in cyberspace. The level of North Korea's cyber attack groups, which maximizes damage by conducting cyber attacks on major countries, could threaten pan-national security. Specifically, based on the time it penetrates the network for hacking, North Korea is ranked second in the world after Russia [7]. In addition, attack techniques and step-by-step procedures are being developed to a high-tech level, and cyber attacks are being strengthened by using detailed attack procedures, techniques, and tools by exploiting social engineering techniques to target unspecified people using political or social issues [11]. Recently, as vaccines that can prevent COVID-19 became a global issue, cyber attack groups quickly changed their attack methods. Numerous hackers, including the Lazarus attack group, use social engineering techniques such as spear phishing and camouflage tactics to steal COVID-19 and vaccines, depending on the actions required by an unspecified majority, such as malware, watering holes, phishing, and pharming. It is classified as a cyberthreat using social engineering techniques such as web Parameter Tampering attack. In addition, most North Korean cyber attack groups continued to attempt attacks using spear phishing, malicious links, and impersonation [4, 5, 12–15]. North Korea's cyber-attacks groups has recently infiltrated the target system with social engineered attack techniques that exploited social issues including corona, and is implementing strategies that utilize APT attacks and cyberkillchain techniques [4, 5, 12–15].

*Research Briefs on Information & Communication Technology Evolution (ReBICTE)*, Vol. 7, Article No. 7 (October 5, 2021)
DOI:*10.22667/ReBiCTE.2021.10.05.007*

*Corresponding author: Department of Information Security Engineering, Sangmyung University, 31066 South Korea, Tel: +82-(0)41-550-5301

# 2 Related Research

## 2.1 MITRE ATT&CK Framework

North Korea's cyber-attack method has evolved from an attack method using viruses and hacking to a DDoS attack and an advanced persistent threat attack method [16]. The North Korean cyber attacker group continues to operate through spear phishing, camouflage tactics, and supply chain attacks that use social engineering techniques to create political and social chaos. As shown in Table 1, strategies and patterns of major North Korean hacking groups were analyzed through attack techniques and cases based on ATT&CK(adversarial Tactics, Techniques and Common Knowledge). The strategy and pattern analysis of North Korea's major hacking groups allowed prediction of North Korea's cyber operations, tactics, technologies and procedures, and applied to the analysis of changes in cyber attacks by Lazarus, Kimsuky, Thallium and Geumseong 121.

**Table 1.** Attacker tactics and strategy pattern analysis based on ATT&CK

| Division | Tactics, Strategy | Description |
|---|---|---|
| TA0043 | Reconnaissance | Gather information they can use to plan future operations |
| TA0042 | Resource Development | Establish resources they can use to support operations |
| TA0001 | Initial Access | Get into your network |
| TA0002 | Execution | Run malicious code |
| TA0003 | Persistence | Maintain their foothold |
| TA0004 | Privilege Escalation | Higher-level permissions |
| TA0005 | Defense Evasion | Avoid being detected |
| TA0006 | Credential Access | Steal account names and password |
| TA0007 | Discovery | Figure out your environment |
| TA0008 | Lateral Movement | Move through your environment |
| TA0009 | Collection | Gather data of interest to their goal |
| TA0010 | Exfiltration | Steal data |
| TA0011 | C&C | Communicate with compromised systems to control them |
| TA0040 | Impact | Manipulate, interrupt, or destroy your systems and data |

## 2.2 Cyber threat trends by major North Korean hacking groups

Analyzing the recent cyber operation activities of North Korean hacking groups using open source information (OSINT), they are classified into the major North Korean hacker organizations Lazarus, Kimsuky, Thallium, and Geumseong121, and the most active attack groups are Lazarus and Kimsuky. Lazarus attempted hacking into banks and film companies, and had activities to pay Bitcoin through ransomware attacks [8]. Geumseong 121 confirmed a slowdown in activity through an invasion indicator of cyber-activity [4, 5, 12–15] and it is Talium believed to be a group renamed by expanding the range and target of attacks in the Kimsuky organization [6]. In order to analyze the process of change in attack patterns of major North Korean hacking groups, it is first necessary to understand the affiliation, characteristics, targets, techniques, and types of the hacker groups. The status of North Korean military cyber unit organization is shown in Fig. 1., North Korea's Workers' Party's cyber organization is shown in Fig. 2 [1, 10].

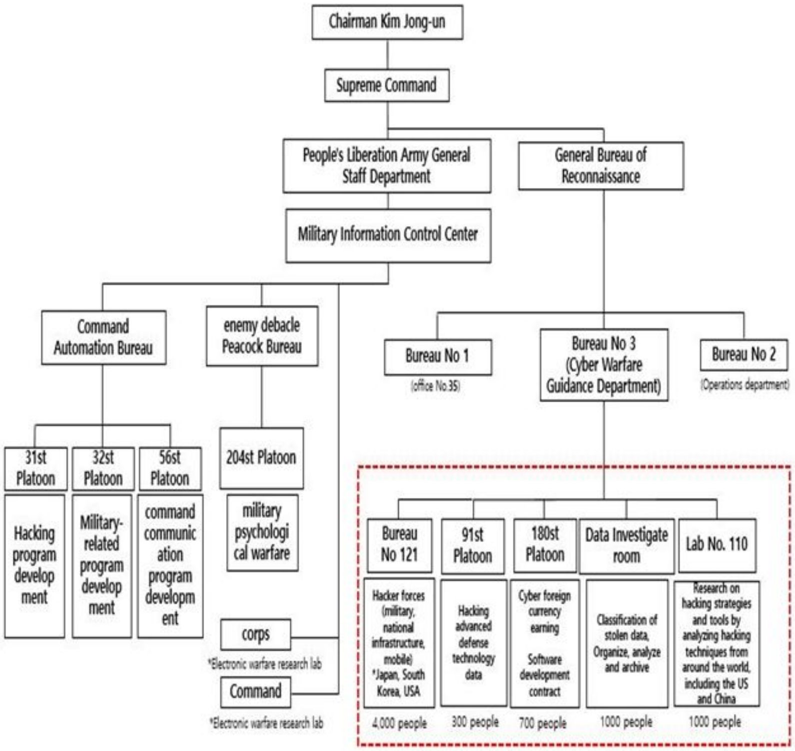
Chairman Kim Jong-un
Supreme Command
People's Liberation Army General Staff Department
General Bureau of Reconnaissance
Military Information Control Center
Command Automation Bureau
enemy debacle Peacock Bureau
Bureau No 1
(office No.35)
Bureau No 3 (Cyber Warfare Guidance Department)
Bureau No 2
(Operations department)
31st Platoon
32st Platoon
56st Platoon
204st Platoon
Hacking program development
Military-related program development
command communication program development
military psychological warfare
corps
*Electronic warfare research lab
Command
*Electronic warfare research lab
Bureau No 121
91st Platoon
180st Platoon
Data Investigate room
Lab No. 110
Hacker forces (military, national infrastructure, mobile) *Japan, South Korea, USA
Hacking advanced defense technology data
Cyber foreign currency earning
Software development contract
Classification of stolen data, Organize, analyze and archive
Research on hacking strategies and tools by analyzing hacking techniques from around the world, including the US and China
4,000 people
300 people
700 people
1000 people
1000 people

Figure 1: Status of North Korean military cyber force organization

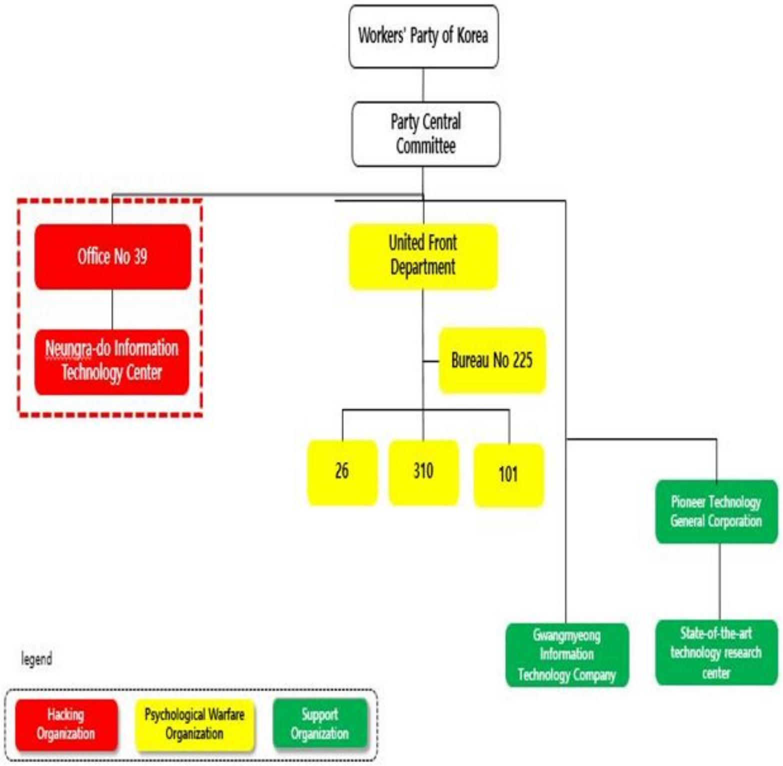
Workers' Party of Korea
Party Central Committee
Office No 39
Neungra-do Information Technology Center
United Front Department
Bureau No 225
26
310
101
Pioneer Technology General Corporation
Gwangmyeong Information Technology Company
State-of-the-art technology research center
legend
Hacking Organization
Psychological Warfare Organization
Support Organization

Figure 2: Status of North Korea's Workers' Party Cyber Organization

Table 2 shows the results of analyzing the main attack targets, types, and attack techniques of major North Korean hacking groups.

**Table 2.** Analysis result of attack targets, types, and attack techniques of major North Korean hacker organizations

| **Groups** | Targets | Type | Technique |
|---|---|---|---|
| Lazerus | COVID-19,<br>Finance,<br>Government,<br>Technology,<br>Bitcoin,<br>North Korea | Hacking,<br>Steal Info<br>Spy, Obstruction and destruction,<br>Monetary, gain | Spear Phishing,<br>Ransomware,<br>Cryptocurrency,<br>Malware, DDos<br>Social engineering |
| Kimsuky (Thallium) | COVID-19,<br>Politics,<br>Diplomacy,<br>Defense,<br>Cryptocurrency,<br>North Korea | Hacking,<br>Steal Info<br>Spy | Spear Phishing,<br>Phishing,<br>Social Engineering,<br>Malware,<br>APT |
| Geumseong121 | Diplomacy,<br>Unification,<br>Security,<br>North Korean defectors,<br>North Korean human rights activist | Hacking,<br>Steal Info<br>Spy | Spear Phishing,<br>Malicious,<br>Hacking,<br>App,<br>Social Engineering |

# 3 Analysis of Hacker Organization Activities in North Korea and Method of Collecting Backtracking Information on Attack Origin

## 3.1 Implementation of analysis diagram of North Korean hacker organization attack origin traceback using Open Source Intelligence (OSINT)

Targeting Lazarus, Thallium, Kimsuky, and Geumseong 121, the major North Korean hacker organizations, using OSINT, VirusTotal, Malwares.com, and shodan.io were used to analyze the activities of major hacking groups and trace the origin of the attack using VBScript diagram was implemented to make it possible. The diagram using the implemented VBScript is shown in Fig. 3. Same as. Furthermore, the hacker organization identified 406 exploited C&C server addresses, including sanlorenzoyacht.com and longdevlab.com, and 77 IPs, including 120.138.8.26 (AS18229/India), 199.89.55.0/24 (NA27640/USA) [2,3]. The list of exploited C&C servers and attack IPs and URLs is shown in Table 3.

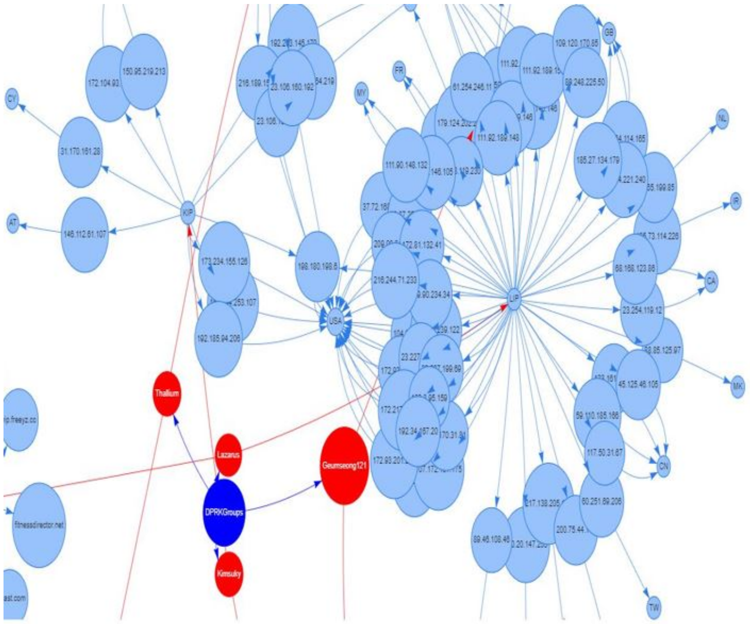

Figure 3: Diagram implementation of VBScript based North Korea cyber-attack activity analysis

**Table 3.** Attack IP and URL identified by the abused C&C server

| Division | IP | URL | Whois |
|---|---|---|---|
| Lazarus C&C | 120.138.8.26<br>199.89.55.218<br>99.83.154.118<br>198.54.117.197<br>198.54.117.198<br>212.19.101.220<br>37.35.106.100<br>217.19.147.100<br>185.176.43.98 | www.advamtimes.com<br>crrmute.com<br>dorusio.com<br>sanlorenzoyacht.com<br>beilksa.scienceontheweb.net | IN<br>US<br>US<br>IT<br>CH<br>IT |
| Kimsuky C&C | 27.0.236.139<br>23.152.0.232<br>209.99.64.76<br>216.239.38.21<br>107.178.246.49<br>54.197.173.238<br>185.176.43.98 | hahee.co.kr<br>forecareer.com<br>org-help.com<br>driver.cfg<br>srtb.msn.com<br>download.riseknite.life<br>onlinewebshop.net | KR<br>US<br>US<br>US<br>US<br>US<br>BG |
| Geumsong 121 C&C | 183.111.174.80<br>116.125.112.241<br>216.189.157.89 | m.ssbw.co.kr<br>naver.pm<br>alps.travelmountain.ml | KR<br>KR<br>US |

| | | | |
|---|---|---|---|
| Thallium C&C | 185.176.43.98 | yezu212.myartsonline.com | BG |
| | 185.176.43.104 | quarez.atwebpages.com | BG |
| | 103.125.219.119 | b.smtper.co | JP |
| | 202.111.173.67 | kasse-v1.hdac-wallet.com | US |
| | 211.13.196.134 | kasse.hdac-tech.com | US |
| | 185.176.43.98 | tksRpdl.atwebpages.com | BG |

Table 4 shows the CVE (Public Vulnerability List) results used by major hacking groups through the Shodan.io site among open source information.

**Table 4.** List of public vulnerabilities exploited by major North Korean hacking groups

| Division | CVE ID | Vulnerability |
|---|---|---|
| Lazarus | CVE-2019-1458 | Windows OS Zero-day Attack |
| | CVE-2019-13720 | Chrome Vulnerability Attack |
| | CVE-2018-4878 | Adobe Flash Player Vulnerability |
| | CVE-2018-20250 | ACE Vulnerability |
| Kimsuky | CVE-2012-0158 | WordPress(docx) Vulnerability |
| | CVE-2017-0199 | MS Office Zero-day |
| | CVE-2017-11882 | Ms Office Vulnerability |
| Geumseong 121 | CVE-2018-4878 | Adobe Flash Player Vulnerability |
| | CVE-2017-8291 | MS Office Vulnerability |

# 4 Changes in cyber hacking patterns of major North Korean hacking groups based on MITRE ATT&CK data

## 4.1 Changes in hacking patterns of North Korean cyber-attack groups

In the past, North Korea used a small number of hacking organizations to conduct DDoS attacks against the South Korean government, starting with hacking for self-promotion such as website paralysis and website defacement. Lazarus, a North Korean hacking organization, not only attacked the internal network of hacking film companies, but also leaked various documents as well as personal information of employees [9]. However, with the increasing number of fast-developing ICTs and scientific technologies, North Korea's cyber attacks technology are also gradually evolving to a state-of-art. Representative examples include computer network hacking of government agencies, finance, and broadcasting companies, infiltration and attack patterns of closed networks, development and attack of ransomware, distribution of ransomware using SMB ports, supply chain attacks, control of autonomous vehicles, drones, airplanes, and Cyber attack patterns that can cause enormous damage to people and property, such as threatening the safety of airspace such as unmanned aerial vehicles, are changing. Using MITRE ATT&CK, data on changes in hacking patterns (tactics, code, attack technology, etc.) of North Korea's cyber attack groups were identified and analyzed.

## 4.2 Analysis of changes in Lazarus group cyber attack pattern based on ATT&CK data

Table 5 shows the results by classifying and analyzing the Lazarus Group cyber attack pattern change data (tactics, codes, attack techniques, etc.) using MITER ATT&CK.

**Table 5.** Lazarus Cyber Attack Changing of Patterns Data Analysis Results

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 1 | Defense Evasion | T1134002 | Access Token Manipulation | Keylogger KiloAlfa obtains user tokens from interactive sessions to execute itself with API call CreateProcessAsUser A under that user's context. |
| 2 | Persistence | T1098 | Account Manipulation | Malware WhiskeyDelta-Two contains a function that attempts to rename the administrator's account. |
| 3 | Discovery | T1010 | Application Windows Discovery | Malware IndiaIndia obtains and sends to its C2 server the title of the window for each running process. The KilaAlfa keylogger also reports the title of the window in the foreground. |
| 4 | Persistence | T1542003 | Bootkit | Malware WhiskeyAlfa-Three modifies sector 0 of the Master Boot Record(MBR) to ensure that the malware will persist even if a victim machine shuts down. |
| 5 | Credential Access | T1110 | Brute Force Attack | Malware attempts to connect to Windows shares for lateral movement by using a generated list of usernames, which center around permutations of the username Administrator, and weak passwords. |
| 6 | Execution | T1059 | Command and Scripting Interpreter | Malware uses cmd.exe to execute commands on victims. A Destover-like variant used by Lazarus Group uses a batch file mechanism to delete its binaries from the system. |
| 7 | C&C | T1571 | Non-Standard Port | Malware uses a list of ordered port numbers to choose a port for C2 traffic, creating port-protocol mismatches. |

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 8 | Resource Development | T1583 | Acquire Infrastructure | Acquired infrastructure related to their campaigns to act as distribution points and C2 channels. |
| 9 | C&C | T1071 | Application Layer Protocol | Malware has conducted C2 over HTTP and HTTPS. |
| 10 | Collection | T1560 | Archive Collected Data | Malware RomeoDelta archives specified directories in .zip format, encrypts the .zip file, and uploads it to its C2 server. |
| 11 | Persistence | T1547 | Boot or Logon Autostart Execution | Malware attempts to maintain persistence by saving itself in the Start menu folder or by adding a Registry Run key. |
| 12 | Privilege Escalat | T1547 | Boot or Logon Autostart Execution | Malware sample adds persistence on the system by creating a shortcut in the user's Startup folder. |
| 13 | Persistence | T1543 | Create or Modify System Process | Malware families install themselves as new services on victims. |
| 14 | Privilege Escalation | T1543 | Create or Modify System Process | Malware families install themselves as new services on victims. |
| 15 | Impact | T1485 | Data Destruction | Used a custom secure delete function to overwrite file contents with data from heap memory. |
| 16 | C&C | T1132 | Data Encoding | Malware sample encodes data with base64. |
| 17 | Resource Development | T1587 | Develop Capabilities | Developed several custom malware for use in operations. |
| 18 | Collection | T1005 | Data from Local System | Malware IndiaIndia saves information gathered about the victim to a file that is uploaded to one of its 10 C2 servers. Lazarus Group malware RomeoDelta copies specified directories from the victim's machine, then archives and encrypts the directories before uploading to its C2 server. Lazarus Group has used wevtutil to export Window security event logs. |

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 19 | C&C | T1001 | Data Obfuscation | Malware also uses a unique form of communication encryption known as FakeTLS that mimics TLS but uses a different encryption method, evading SSL man-in-the-middle decryption attacks. |
| 20 | Collection | T1074 | Data Staged | Malware India saves information gathered about the victim to a file that is saved in the %TEMP% directory, then compressed, encrypted, and uploaded to a C2 server. |
| 21 | Impact | T1491 | Defacement | Replaced the background wallpaper of systems with a threatening image after rendering the system unbootable with a Disk Structure Wipe. |

Table 6 shows the results by classifying and analyzing the Kimsuky Group cyber attack pattern change data (tactics, codes, attack techniques, etc.) using MITER ATT&CK.

**Table 6.** Kimsuky Cyber Attack Changing of Patterns Data Analysis Results

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 1 | Persistence | T1176 | Browser Extensions | Used Google Chrome browser extensions to infect victims and to steal passwords and cookies. |
| 2 | Resource Development | T1583001 | Acquire Infrastructure : Domain | Registered domains to spoof targeted organizations and trusted third parties. |
| 3 | C&C | T1071002 | Application Layer Protocol : FTP | FTP to download additional malware to the target machine. |
| 4 | C&C | T1071003 | Application Layer Protocol : Mail | e-mail to send exfiltrated data to C2 servers. |
| 5 | Collection | T1560003 | Archive Collected Data : via Custom Method | RC4 encryption before exfiltrated. |
| 6 | Persistence | T1547 | Boot or Logon Autostart Execution | Placed scripts in the startup folder for persistence. |

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 7 | Execution | T1059001 | Command and Scripting Interpreter : PowerShell | Executed a variety of PowerShell scripts. |
| 8 | Resource Development | T1059005 | Command and Scripting Interpreter : Visual Basic | Visual Basic to download malicious payloads. |
| 9 | Persistence | T1059006 | Command and Scripting Interpreter : Python | Mac OS Python implant to gather data. |
| 10 | Credential Access | T1059007 | Command and Scripting Interpreter : JavaScript | JScript for logging and downloading additional tools. |
| 11 | Collection | T1586002 | Email Accounts | Compromised web portal email accounts to send spear phishing e-mails. |
| 12 | Collection | T1543003 | Windows Service | Created new services for persistence. |
| 13 | Resource Development | T1555003 | Credentials from Password Stores: Credentials from Web | browser extensions including Google Chrome to steal passwords and cookies from browsers. |
| 14 | Collection | T1005 | Browsers Data from Local System | Collected Office, PDF, and HWP documents from its victims. |
| 15 | Privilege Escalation | T1074001 | Data Staged : Local Data Staging | Staged collected data files under C: \Program Files\Common Files \System\Ole DB\ |
| 16 | Exfiltration | T1587 | Develop Capabilities | Created and used a mailing toolkit to use in spear phishing attacks. |
| 17 | Initial Access | T1114003 | Email Collection : Email Forwarding Rule | Set auto-forward rules on victim's e-mail accounts. |
| 18 | Discovery | T1546001 | Event Triggered Execution : Change Default File Association | HWP document stealer module which changes the default program association in the registry to open HWP documents. |
| 19 | Defense Evasion | T1041 | Exfiltration Over C2 Channel | Exfiltrated data over its email C2 channel. |
| 20 | Resource Development | T1133 | External Remote Services | RDP to establish persistence. |
| 21 | C&C | T1083 | File and Directory Discovery | The ability to enumerate all the drives on an infected system. |

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 22 | C&C | T1562001 | Impair Defense : Disable or Modify Tools | Observed turning off Windows Security Center. |

Table 7 shows the results by classifying and analyzing the Geumseong 121 Group cyber attack pattern change data (tactics, codes, attack techniques, etc.) using MITER ATT&CK.

**Table 7.** Geumseong 121 Cyber Attack Changing of Patterns Data Analysis Results

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 1 | Collection | T1123 | Audio Capture | Audio capturing utility known as SOUNDWAVE that captures microphone input. |
| 2 | Privilege Escalation | T1548 | Abuse Elevation Control Mechanism | function in the initial dropper to bypass Windows UAC in order to execute the next payload with higher privileges. |
| 3 | C&C | T1071001 | Application Layer Protocol : Web | Geumseong121 uses HTTPS to conceal C2 communications. |
| 4 | Persistence | T1547001 | Boot or Logon Autostart Execution | Geumseong121 has added persistence via the Registry key HKCU\Software\Microsoft\CurrentVersion\Run\. |
| 5 | Execution | T1059003 | Command and Scripting Interpreter | Geumseong121 used the command-line interface. |
| 6 | Execution | T1059005 | Command and Scripting Interpreter | Geumseong121 executes shellcode and a VBA script to decode Base64 strings. |
| 7 | Credential Access | T1555003 | Credentials from Password Stores | Credential stealer known as ZUMKONG that can harvest usernames and passwords stored in browsers. |
| 8 | Collection | T1005 | Data from Local System | Collected data from victims' local systems. |
| 9 | Impact | T1561002 | Disk Wipe: Disk Structure Wipe | Access to destructive malware that is capable of overwriting a machine's Master Boot Record (MBR). |
| 10 | Initial Access | T1189 |  | Strategic web compromises, particularly of South Korean websites, to distribute malware. |

| Division | Tactics | code | Attack Name | Explanation |
|---|---|---|---|---|
| 11 | Execution | T1203 | Drive-by Compromise | The group has also used torrent file-sharing sites to more indiscriminately disseminate malware to victims. As part of their compromises, the group has used a Javascript based profiler called RICECURRY to profile a victim's web browser and deliver malicious code accordingly. |
| 12 | C&C | T1105 | Exploitation for Client Execution | Flash Player (CVE-2016-4117, CVE-2018-4878) and Word (CVE-2017-0199) exploits for execution. |
| 13 | Execution | T1559002 | Ingress Tool Transfer | Downloaded second stage malware from compromised websites. |
| 14 | Execution | T1106 | Inter-Process Communication : Dynamic Data Exchange | Windows DDE for execution of commands and a malicious VBS. |
| 15 | Discovery | T1120 | Native API | Leverages the Windows API calls: VirtualAlloc(), WriteProcessMemory(), and CreateRemoteThread() for process injection. |
| 16 | Initial Access | T1566001 | Peripheral Device Discovery | Bluetooth device harvester, which uses Windows Bluetooth APIs to find information on connected Bluetooth devices. |
| 17 | Defense Evasion | T1055 | Phishing : Spear Phishing Attachment | Delivers malware using spear phishing emails with malicious HWP attachments. |
| 18 | Discovery | T1082 | Process Injection | Injects its malware variant, ROKRAT, into the cmd.exe process. |
| 19 | Discovery | T1033 | System Information Discovery | Collects the computer name, the BIOS model, and execution path. |
| 20 | Impact | T1529 | System Owner /User Discovery | Identifies the victim username. |
| 21 | Execution | T1204002 | System Shutdown/Reboot | Malware that will issue the command shutdown \r \t 1 to reboot a system after wiping its MBR. |

# 5 DISCUSSION AND CONCLUSIONS

In this paper, data of the North Korean cyber hacking groups, which has been publicly engaged in cyber attacks since 2007, was applied to MITER ATT&CK and analyzed. The attack origin was estimated with the actually verified malicious IP band, URL, malicious code information, and public vulnerability information through correlation analysis using public source information and ATT&CK data. Through this, it was possible to analyze North Korean cyber attacks groups and use ATT&CK data to implement diagrams of North Korean cyber attacks based on VBScript and propose the results of cyber attacks analysis data of major hacker organizations in North Korea. In the future, it will establish visualization models for attack processes such as identifying hacker organizations' intentions, identifying cyber threats trends, securing cyber attack technologies, and securing attack origin precision tracking and bridgehead using open source intelligence-based analysis data.

# References

[1] Hacker power north korea.. what are the counter-measures? `http://www.digitaltoday.co.kr` [Online; Accessed on September 10, 2021].

[2] Shodan.io. `https://www.shodan.io/` [Online; Accessed on September 10, 2021].

[3] Virustotal. `https://www.virustotal.com/gui/home/upload` [Online; Accessed on September 10, 2021].

[4] J. C. ADVISORY. Guidance on the north korean cyber threat. *Cybersecurity and Infrastructure Security Agency (CISA)*, 2020.

[5] J. C. ADVISORY. North korean advanced persistent threat focus: Kimsuky. *Cybersecurity and Infrastructure Security Agency (CISA)*, 2020.

[6] EstSecurity. Security trend report: North korea-linked thallium groups continues 'blue estimate' apt campaign. *ESTsecurity*, 2020.

[7] S. B. et al. China's cybersecurity strategy and its application to north korea: Focusing on identity and awareness. *Asia Review*, 10(1):53–79, 2020.

[8] N. Jang. Ransomware and north korea's cyber-threat. *JPI Research Series*, 40:73–77, 2017.

[9] J. L. J.W. Kim and H. Chang. Current status and prospects of industrial technology leakage through cyber attacks. *Review of KIISC*, 31(3):7–12, 2021.

[10] J. Kim. North korea's cyber organization-related information research. *Journal of the Korean Society of Computer and Information Engineers*, 2020.

[11] Y. Y. Kim and N. S. Baek. A study on the countermeasures to the cyber-psychological war in north korea. *Journal of Korean Terrorist Association*, 12(2):29–49, 2019.

[12] KISA. Cybersecurity issue report: TTPs #1 analysis of internal network penetration cases through the website. *Korea Internet & Security Agency (KISA)*, 2020.

[13] KISA. Cybersecurity issue report: TTPs #2 analysis of attack network composition method that collects information through spear phishing. *Korea Internet & Security Agency (KISA)*, 2020.

[14] KISA. Cybersecurity issue report: TTPs #3 analysis of attacker's strategy of using malicious code. *Korea Internet & Security Agency (KISA)*, 2020.

[15] KISA. Cybersecurity issue report: TTPs #4 phishing target reconnaissance and attack resource analysis. *Korea Internet & Security Agency (KISA)*, 2020.

[16] J. L. M.K. Chung and H. Kwon. A study on north korea's cyber attacks and countermeasures. *Journal of Information Technology Services*, 15(1):67–79, 2016.

## Author Biography

**GwangHyun Ahn** was received a B.S. degree in cybersecurity from Far East University, Chung-cheong bukdo, South Korea, in 2018. He is currently pursuing a Ph.D. degree with the Department of Computer Engineering, Sejong University, South Korea, Since 2020. He was commissioned as an officer specializing in cyber security in the Republic of Korea and served in the military for three years before moving to a state civil service. His research interests include cybersecurity, industrial security, Incident Response, Forensic, Self-driving car hacking, Profiling of major hacking groups and Dark Web.

**Seon-a Lee** is an undergraduate student in Department of Information Security Engineering, Sangmyung University, South Korea. Her research interests include Cybersecurity, Industrial security, Incident Response, Forensic, Web Hacking, Android mobile Hacking, Network system security and Artificial intelligence.

**Won-hyung Park** is a professor in Department of Information Security Engineering, Sangmyung University, South Korea. He received Ph.D. degree in Department of Information Security from the Kyonggi University, South Korea, in 2009. He co-authored more than 50 technical papers in the area of information security. Also, he has been reviewer for International Journal(Computer-Journal) of Oxford University. press and IEEE Conference.