비상계엄 테마 APT 공격

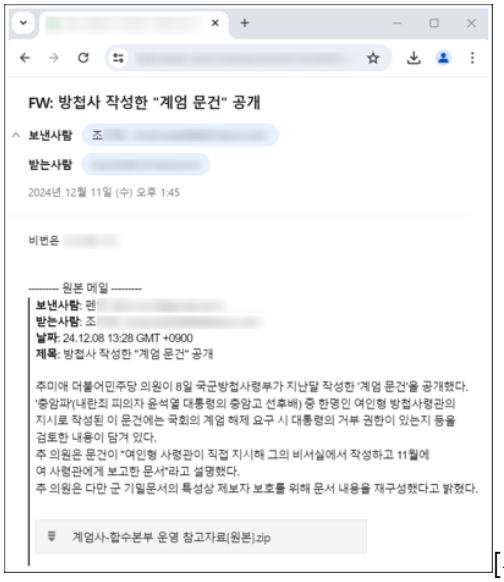
개요

2024년 12월 11일, "FW: 방첩사 작성한 '계엄 문건' 공개" 제목의 스피어 피싱 이메일이 대북 분야 종사자들에게 유포되었다. 이메일은 비상계엄 이슈를 악용하여 수신자의 호기심을 자극하고, CPL 확장자의 악성 제어판 파일을 활용하여 악성코드를 유포했다. 이러한 공격은 기존 보안 솔루션의 탐지를 회피하고, EDR 시스템의 필요성을 강조한다.

배경

지니언스 보안센터(GSC)는 해당 APT 공격을 발견하고, 한국인터넷진흥원(KISA)과 협력하여 대응에 나섰다. 공격 이메일은 실제 존재하는 기자의 아이디를 변형한 'chamssae'를 사용하고, 한글 문화권에서 사용하는 '비번' 등의 단어를 포함하여 사회공학적 기법을 활용했으며, 이러한 언어적 분석은 공격자의 국적이나 배경을 추정하는 데 도움이 된다.

스피어 피싱 분석

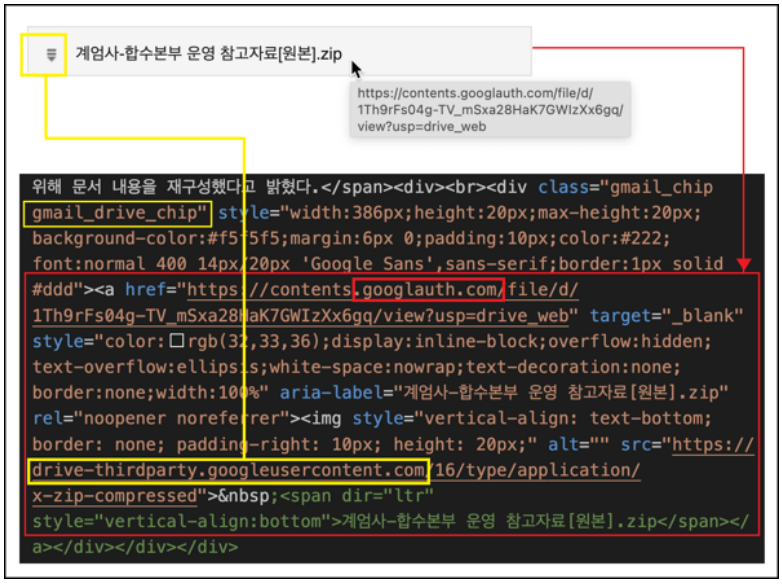


[계엄 내용으로 위장한 스피어 피싱 공격 화면]

```
00000C30 41 6C 42 39 67 41 6F 78 38 59 3D 0D 0A 58 2D 4D  AlB9gAox8Y=..X-M
00000C40 61 69 6C 65 72 3A 20 6D 69 6E 74 0D 0A 58 2D 4F  ailer: mint..X-O
00000C50 72 69 67 69 6E 61 74 69 6E 67 2D 49 50 3A 20 5B  riginating-IP: [
00000C60 31 31 32 2E 31 37 35 2E 31 38 35 2E 35 39 5D 0D  112.175.185.59].
00000C70 0A 58 2D 48 4D 2D 55 54 3A 20 2F 41 4C 71 7A 59  .X-HM-UT: /ALqzY
00000C80 51 50 6C 50 6B 6E 65 54 4F 64 4A 4C 74 65 77 4F  QPlPkneTOdJLtewO
00000C90 67 70 5A 62 48 66 64 30 47 71 58 63 68 49 79 51  gpZbHfd0GqXchIyQ
```
[발신지 아이피 정보]

공격 이메일은 '112.175.185[.]59' IP에서 발송되었으며, 과거 '김수키(Kimsuky)' 그룹의 피

싱 캠페인과 유사한 IP 대역이 사용되었다.

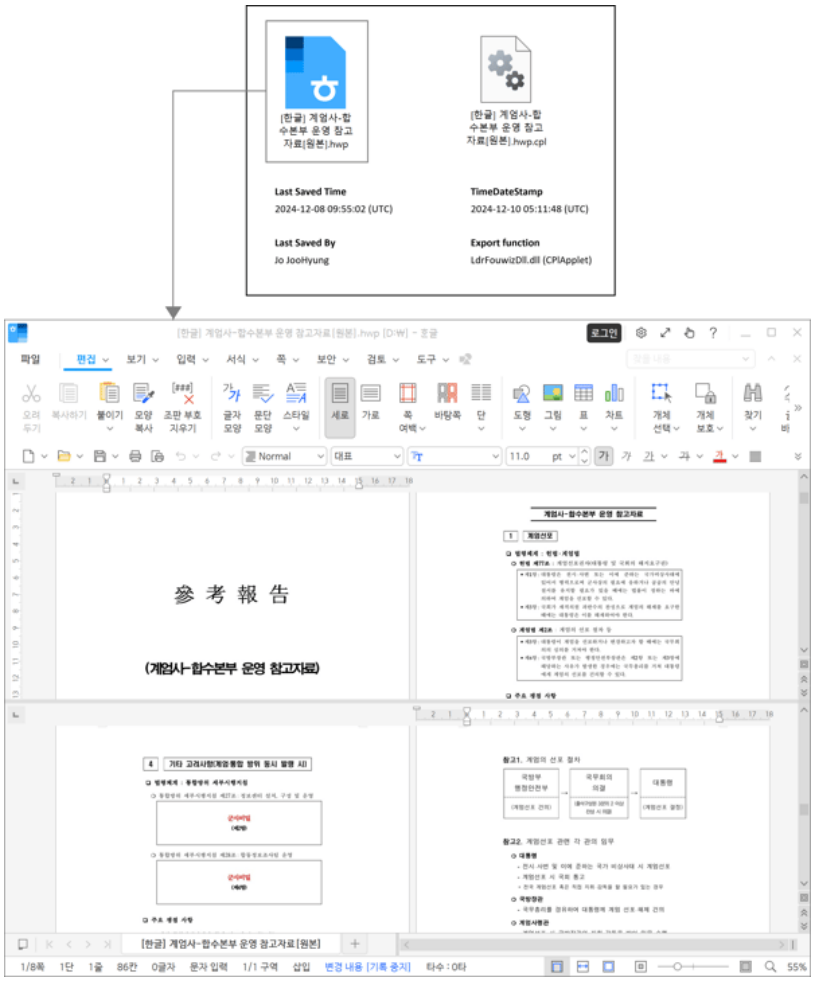


[이메일 첨부파일 링크 정보]

이메일에는 'googlauth[.]com' 도메인을 통해 악성 ZIP 파일이 다운로드되며, 운영체제에 따라 다른 파일이 제공된다.

[운영체제에 따라 다운로드된 압축파일 비교]

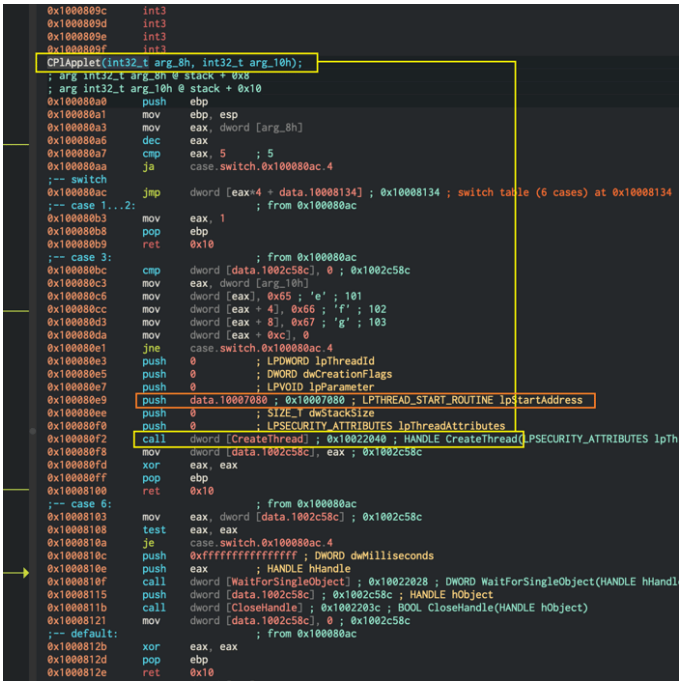
macOS에서는 정상 HWP 문서가, Windows에서는 악성 CPL 파일이 포함된 압축파일이 제공되어, 운영체제에 따른 맞춤형 공격이 이루어졌음을 확인할 수 있다.



[각 파일 정보와 문서 실행 화면]

악성파일 분석

- [한글]계엄사-합수본부 운영 참고자료[원본].hwp.cpl



[CPLApplet 함수와 CreateThread 호출루틴]

문서로 위장한 이중 확장자의 제어판 항목 파일로, 실행 시 'control.exe'를 통해 악성 모듈을 실행한다.

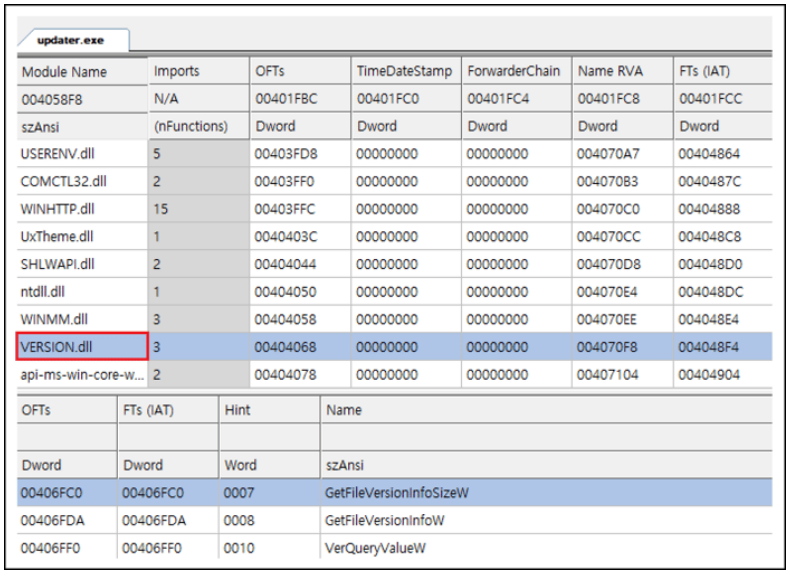
[깃허브 C2 통해 추가 파일 다운로드 명령 화면]

이후, 깃허브 주소에서 추가 파일을 다운로드하고, AES 암호화를 사용하여 데이터를 복호화한다.

'GoogleUpdater.zip' 압축 내부에는 두개의 파일이 포함되어 있고, 아래의 경로에 각각 압축을 해제한다.

- %programdata%\GoogleUpdater\
  - updater.exe
  - version.dll

압축이 해제된 후, 'updater.exe' 파일이 실행되는데 이 파일은 유효한 디지털 서명이 탑재된 정상적인 구글 업데이터(x86) 응용 프로그램이다. 그러나 실행 시 동일 경로에 존재하는 악성 'version.dll' 파일을 함께 호출하는 'DLL Side Loading' 기법을 사용한다.



updater.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
004058F8	N/A	00401FBC	00401FC0	00401FC4	00401FC8	00401FCC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
USERENV.dll	5	00403FD8	00000000	00000000	004070A7	00404864
COMCTL32.dll	2	00403FF0	00000000	00000000	004070B3	0040487C
WINHTTP.dll	15	00403FFC	00000000	00000000	004070C0	00404888
UxTheme.dll	1	0040403C	00000000	00000000	004070CC	004048C8
SHLWAPI.dll	2	00404044	00000000	00000000	004070D8	004048D0
ntdll.dll	1	00404050	00000000	00000000	004070E4	004048DC
WINMM.dll	3	00404058	00000000	00000000	004070EE	004048E4
VERSION.dll	3	00404068	00000000	00000000	004070F8	004048F4
api-ms-win-core-w...	2	00404078	00000000	00000000	00407104	00404904

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00406FC0	00406FC0	0007	GetFileVersionInfoSizeW
00406FDA	00406FDA	0008	GetFileVersionInfoW
00406FF0	00406FF0	0010	VerQueryValueW

['updater.exe' 파일과 함께 실행되는 'version.dll' 화면]

- version.dll

  'updater.exe'와 함께 실행되는 악성 DLL 파일로, 정상 파일처럼 위장하여 탐지를 회피한다. 파일 속성에는 'Version Checking and File Installation Libraries' 등의 정보를 포함하여 정상 파일로 가장하는 것을 확인할 수 있다.

결론 및 대응

사회공학적 기법을 활용한 APT 공격은 사람의 심리나 행동을 이용하여 정보를 탈취하거나 시스템에 침투하는 방식을 의미한다. 이번 사례처럼 CPL 제어판 기능의 악성파일이나, 깃허브 저장소를 C2 서버로 사용하는 등 공격 기술이 발전하고 있다. 이에 따라, EDR(Endpoint Detection and Response) 시스템의 도입이 중요하며, Genian EDR 제품은 이러한 공격 행위별 위협 요소를 탐지하고 차단할 수 있다.