Continuous Distribution of LockBit 2.0 Ransomware Disguised as Resumes - ASEC

By ATCP

Published: 2023-02-02 · Archived: 2026-04-05 15:43:21 UTC

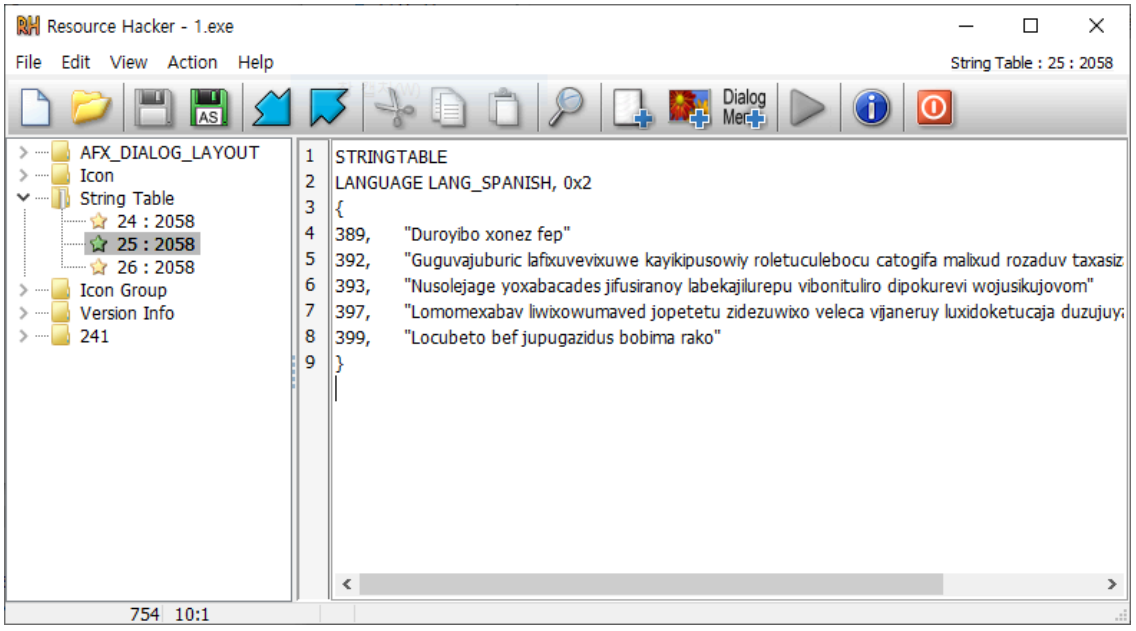
The ASEC analysis team has identified that Lockbit 2.0 is being distributed in a MalPE format instead of the NSIS format which the team had introduced it with previously. The MalPE format is a type of packing method that disrupts the analysis of the actual malware. It then decrypts and executies its PE files through an internal shell code.

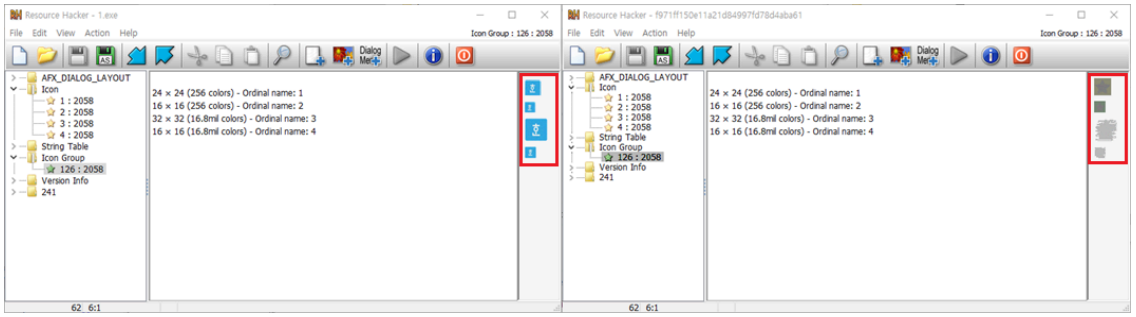
We have recently discovered during our monitoring of ransomware that the distribution of LockBit has risen since January. As it was introduced before, LockBit is still being distributed with filenames that make them seem like job applications. Newly discovered filenames, as well as the existing ones, are as follows.

- _Resume_220926 (Experience details are included Thank you).exe
- #Resume_221116 (Experience details are included Thank you).exe
- (Resume_221112 (I'll show that I'm a hard worker).exe
- 221208_Resume (I'll do my best I will be in your case Thank you).exe
- ~Resume_230116.exe
- $Resume_230108.exe
- Re_su_me [230124 (Experience details are included Thank you].exe

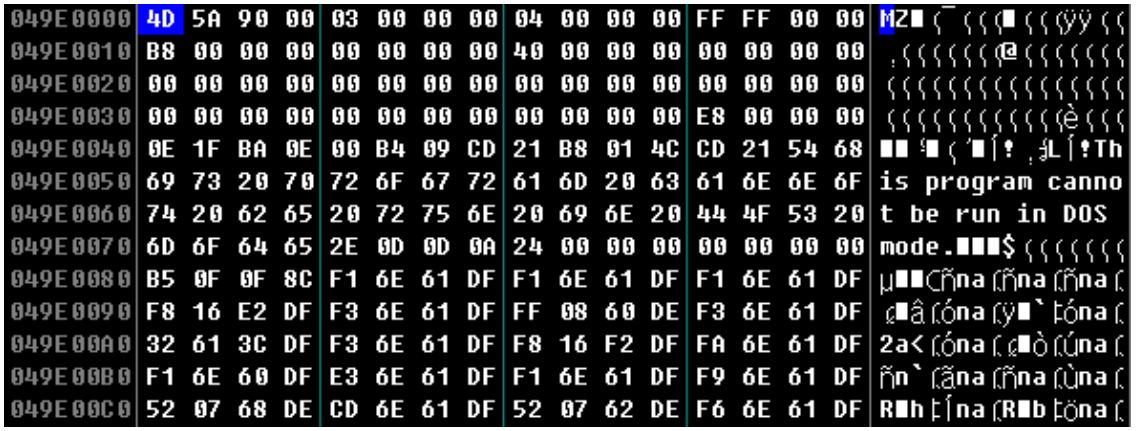
- [Re_su_me] 230130 Please note that my experience details are also included.exe

The Lockbit 2.0 ransomware distributed with its filename as “Re_su_me [230124 (Experience details are included Thank you].exe” is in a MalPE format that has a specific string in the resource area as shown in Figure 1. General MalPE format malware cases have the characteristic of being distributed with identical icons, but the Lockbit 2.0 ransomware is being distributed with its icon changed to that of Hangul, reflecting its disguise as a resume.





Similar to the typical MalPE packing method, this malware decodes and executes the shellcode and PE data.

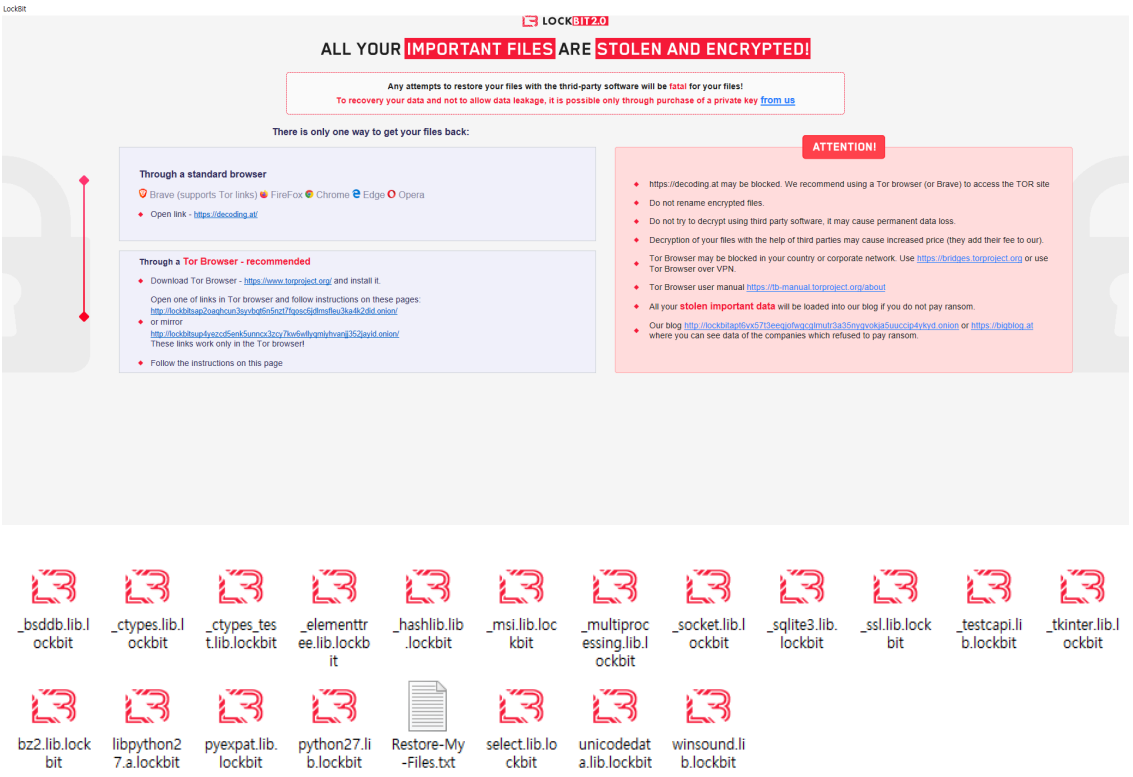


As seen in the previous blog post, the executed ransomware deletes copies of the volume shadow, registers run keys, and shuts down services and processes to evade file infection and analysis; while doing so, this ransomware also deletes event logs, which is a behavior that has never been introduced.

```
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
wevutil cl application
wevutil cl system
```

Table 1. Execution command

Afterward, it encrypts user system files. Encrypted files are made to have the same .lockbit extension and icon. The command also generates a ransom note with the filename, “Restore-My-Files.txt”, before changing the wallpaper.



The MalPE format malware that is being distributed has recently been targeting companies with emails disguised as job applications. Not only is it spreading LockBit through this method, but all sorts of other malware as well. Therefore, companies must update their anti-malware software to the latest versions, and users must take extra caution. AhnLab’s anti-malware software, V3, detects and blocks the malware using the following aliases:

[File Detection]

- Trojan/Win.Generic.R553808 (2023.01.25.03)
- Ransomware/Win.LockBit.R487041 (2022.04.22.01)

[Behavior Detection]

- Ransomware/MDP.Command.M1751

MD5

6a98b2b6e37c7c92368548e902e9a139

cfbc3e71c945dd9918f0013acb652cbd

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/47739/