LockBit Ransomware Disguised as Copyright Claim E-mail Being Distributed

asec.ahnlab.com/en/35822/

June 24, 2022

The ASEC analysis team has once again discovered the distribution of LockBit ransomware using phishing e-mail, and disguising itself as copyright claims e-mail which was introduced in the previous blog. The filename of the attachment in e-mail had password included, which is similar to that of phishing e-mail distributed last February (see the link below).

LockBit Ransomware Being Distributed Using Resume and Copyright-related Emails

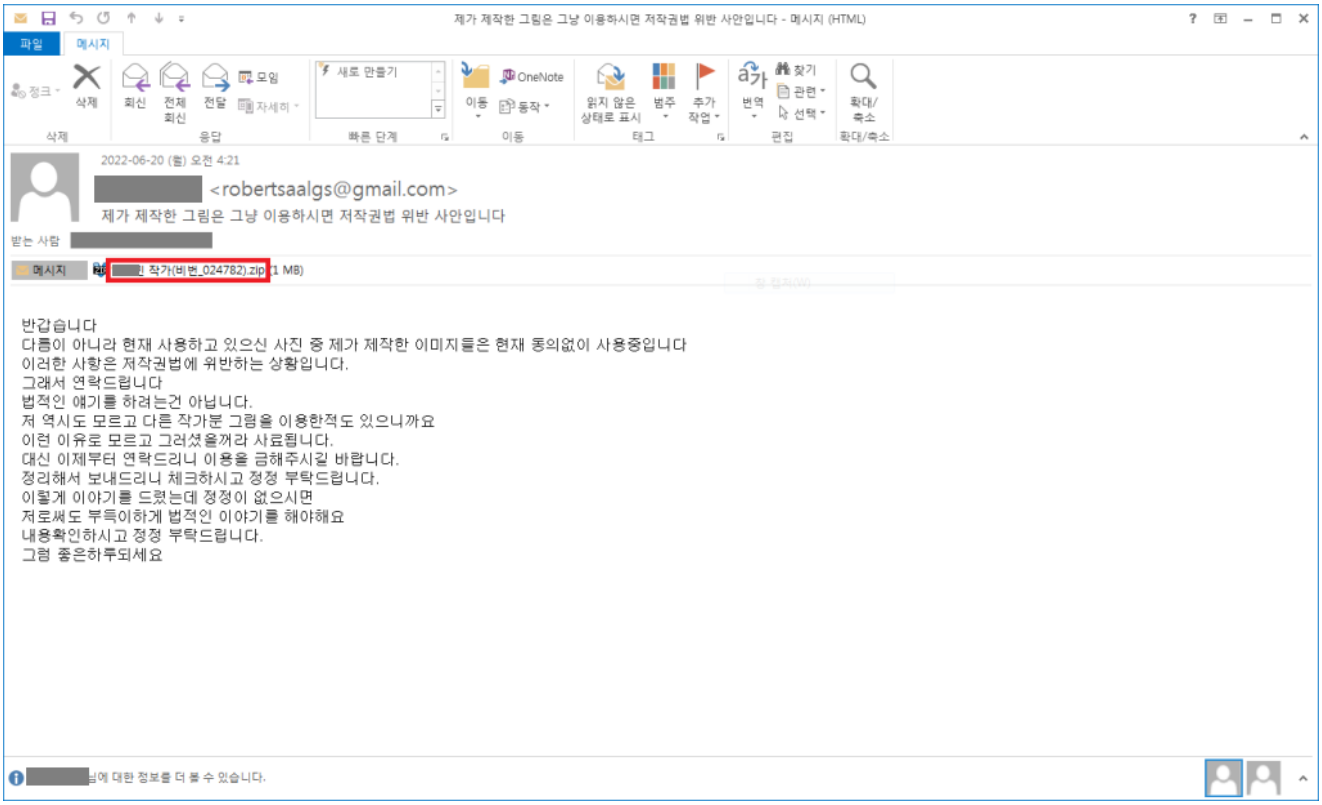

Figure 1. E-mail details

As shown in Figure 2, the phishing e-mail has a compressed file as an attachment that contains another compressed file inside.

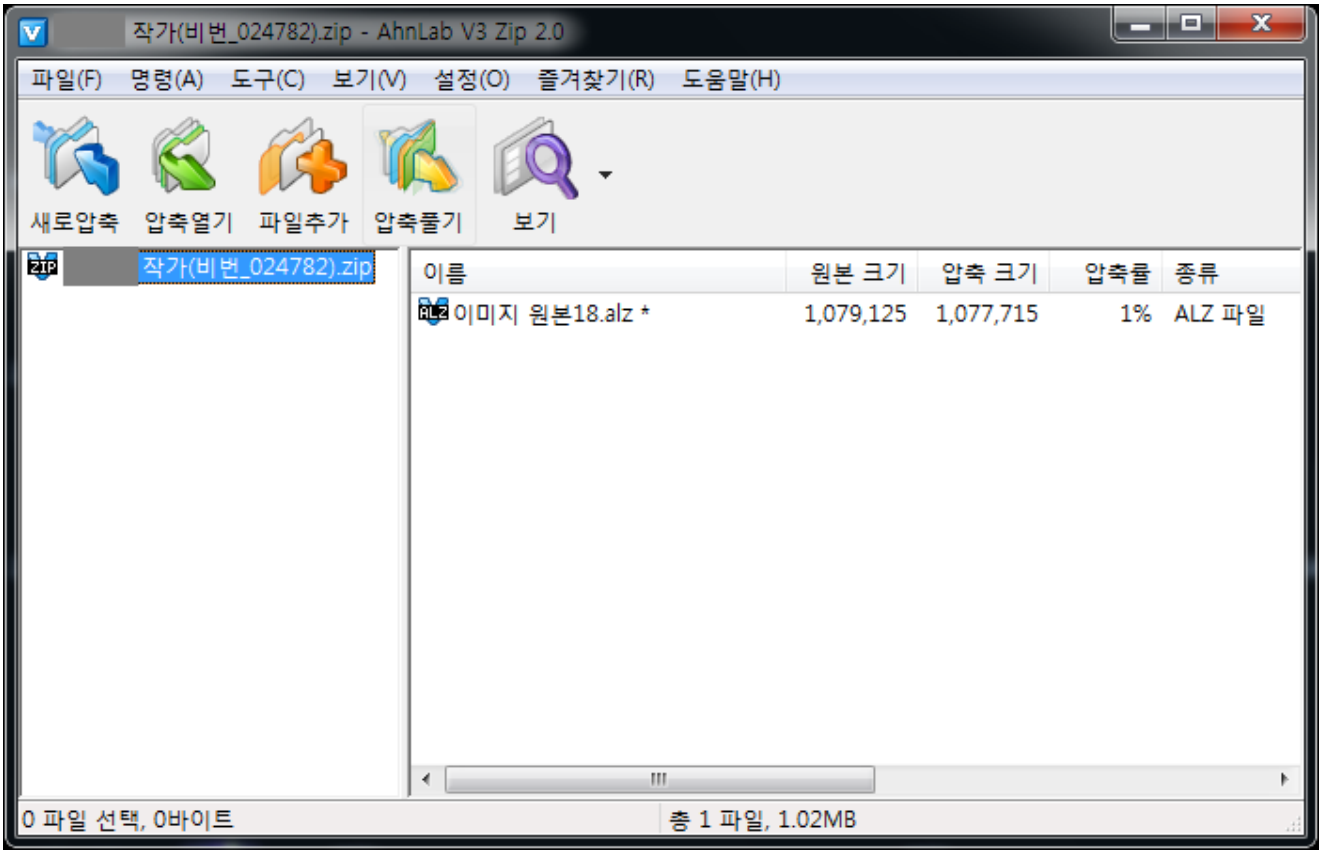

Figure 2. Inside the compressed file

Upon decompressing the file in the compressed file, an executable disguised using a PDF file icon is found.

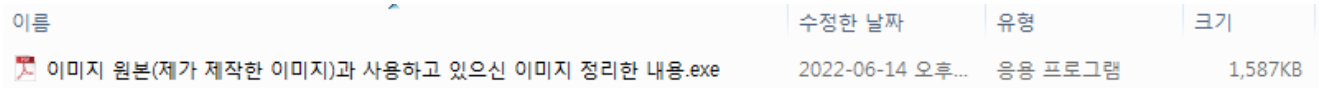

Figure 3. Executable disguised as a PDF file

As shown in Figure 4, this file is confirmed to be a NSIS File. Looking into the nsi script detail, it decodes the data file '162809383' and performs malicious behaviors through recursions and injections.

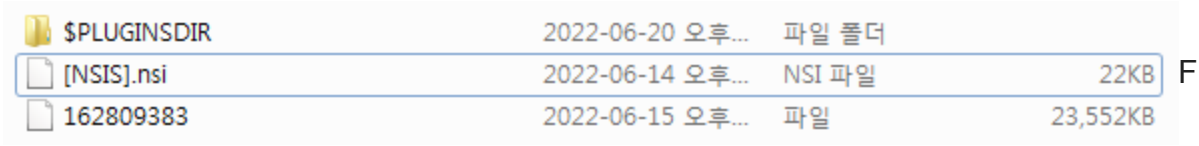

Figure 4. Inside the NSIS file

```
SetOverwrite on
AllowSkipFiles on
File 162809383
Sleep 17000
System::Call "*(&t255)            $\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t                p            $\t$\t$\t$\t$\t$\t$\t            .r5"
  ; Call Initialize____Plugins
  ; SetOverwrite off
  ; AllowSkipFiles off
  ; File $PLUGINSDIR\System.dll
  ; SetDetailsPrint lastused
  ; Push "*(&t255)            $\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t$\t                p            $\t$\t$\t$\t$\t$\t$\t            .r5"
  ; CallInstDLL $PLUGINSDIR\System.dll Call
```
Figure 5. Part of nsi script

This ransomware prevents recovery by deleting volume shadow copy. Furthermore, to make sure the ransomware runs continuously, it registers Run Key to registry and drops LockBit_Ransomware.hta on the desktop to keep it running even after a desktop change or a reboot.

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

Table 1. Execution command

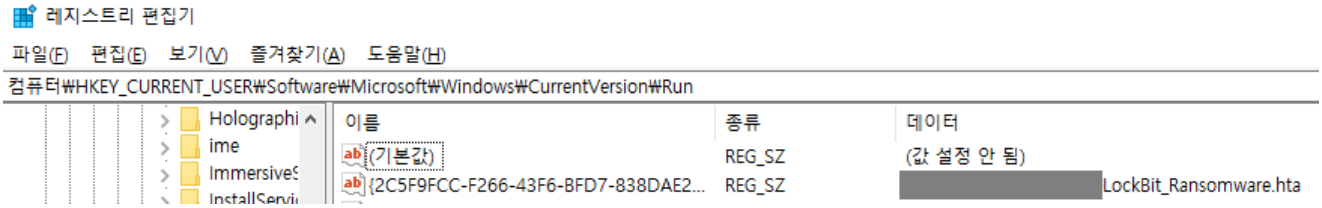

Figure 6. Registry registered

It then terminates multiple services and processes to avoid detection of file infection behavior and analysis.

wrapper, vmware-converter, vmware-usbarbitator64, MSSQL, MSSQL$, sql and etc.

Table 2. Terminated services

winword.exe, QBDBMgr.exe, 360doctor.exe, Adobe Desktop Service.exe, Autorunsc64a.exe, Sysmon.exe, Sysmon64.exe, procexp64a, procexp64a.exe, procmon.exe, procmon64.exe, procmon64a, procmon64a.exe, Raccine_x86, ProcessHacker.exe and etc.

Table 3. Terminated processes

The encryption happens after certain services and processes are terminated. If the drive type is DRIVE_REMOVABLE, DRIVE_FIXED, or DRIVE_RAMDISK, it will also be encrypted. Extensions and name of folders or files that are excluded from encryption are as follows:

system volume information, windows photo viewer, windowspowershell, internet explorer, windows security, windows defender, $recycle.bin, Mozilla, msbuild, appdata, windows and etc.

Table 4. Folders excluded from encryption

.mp4 .mp3 .reg .ini .idx .cur .drv .sys .ico .lnk .dll .exe .lock .lockbit .sqlite .accdb .lzma .zipx .7z .db and etc.

Table 5. Extensions excluded from encryption

Encrypted files have an extension named .lockbit and a certain icon. Also, a ransom note named ‘Restore-My-Files.txt’ is created in the encrypted folder.

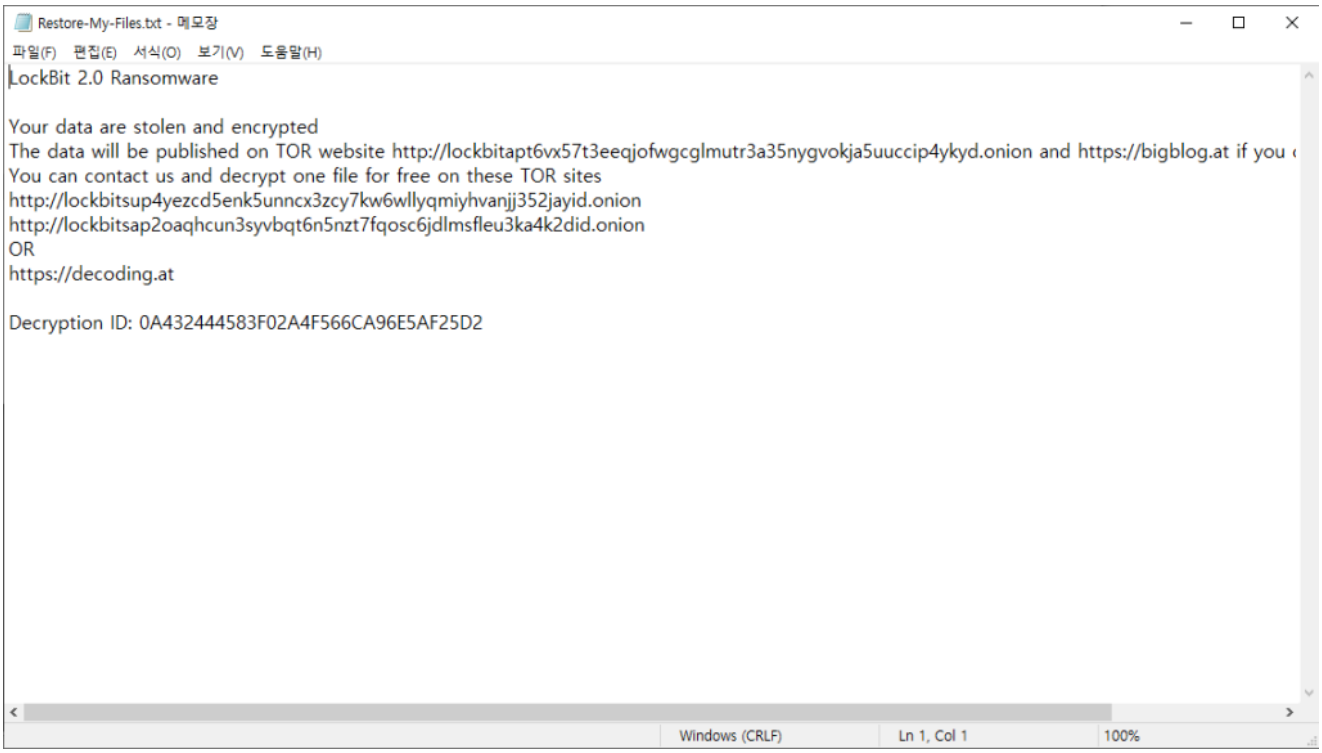

Figure 7. Ransom note

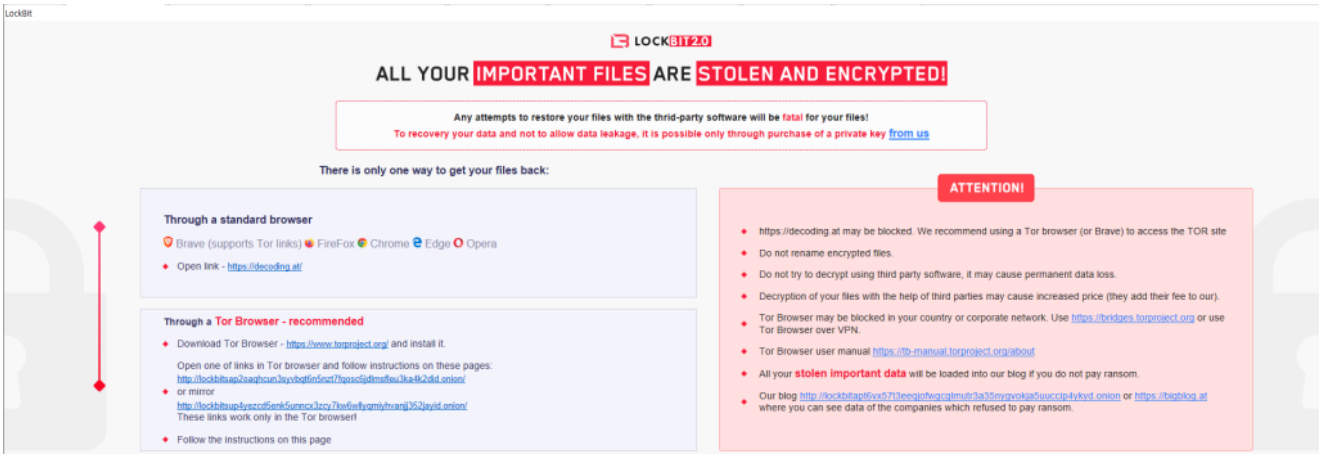

Figure 8. When infected by ransomware

As shown above, the distribution of ransomware disguised as copyright-related claims has been continually done in the past. Because emails distributing such malware types may include names of actual illustrators, users may run attached files without realizing it. Hence they should take extreme caution.

[File Detection]

Malware/Gen.Reputation.C4312359

[Behavior Detection]

Malware/MDP.SystemManipulation.M1751

Figure 9. Behavior block

[IOC Info]

- 3a05e519067bea559491f6347dd6d296 (eml)
- 74a53d9db6b2358d3e5fe3accf0cb738 (exe)

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

Categories:Malware Information

Tagged as:Copyright Phishing E-mail, LockBit, NSIS Ransomware, Phishing email, Ransomware