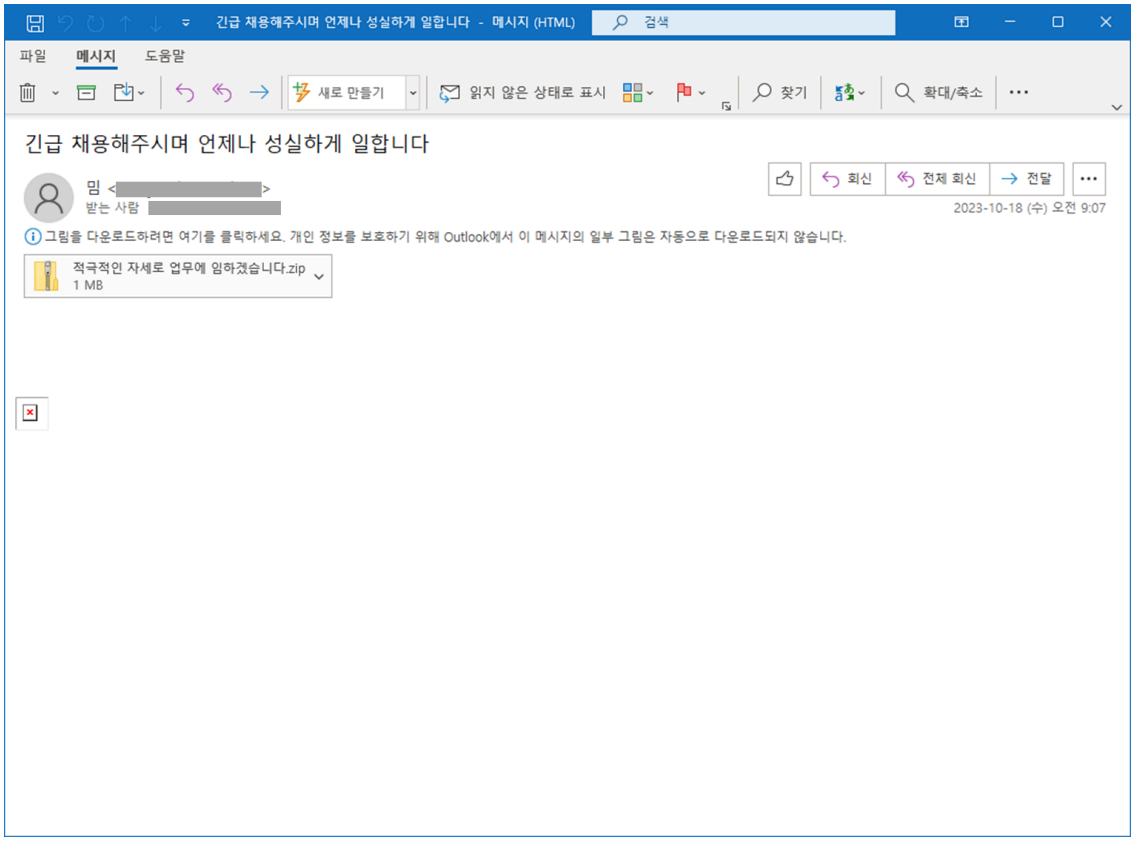
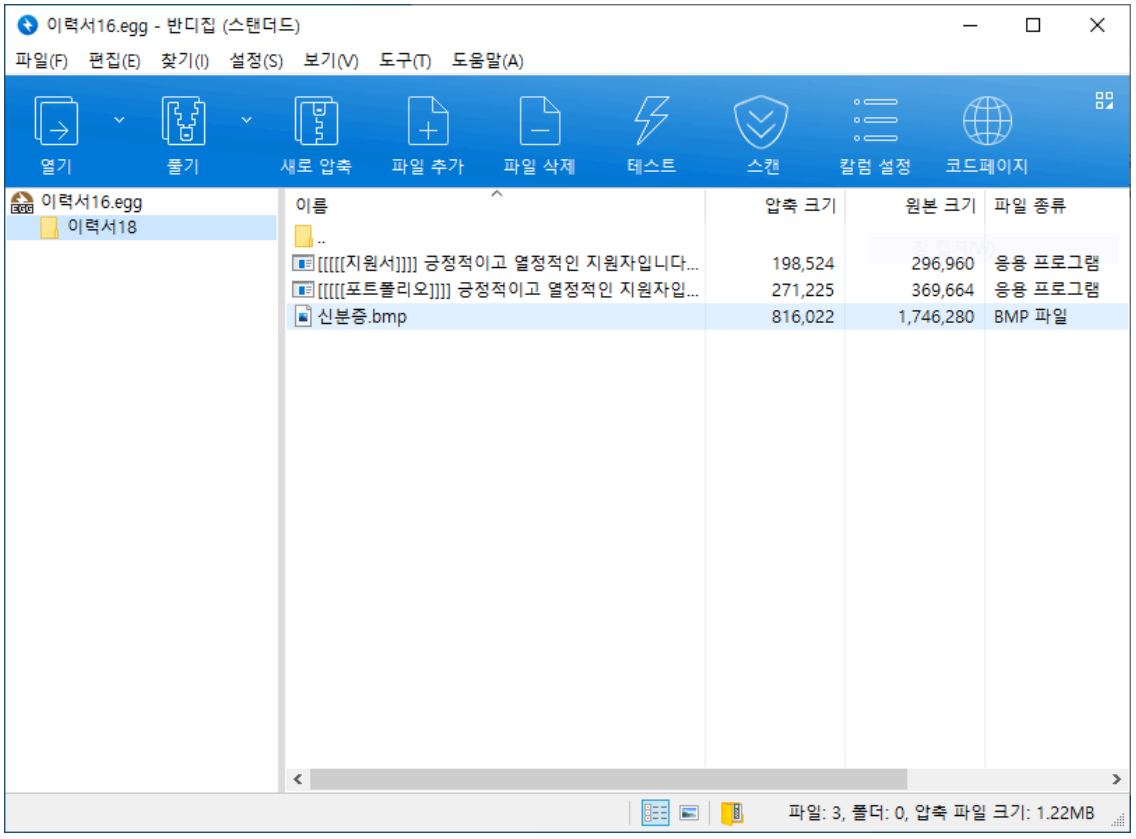
Distribution of LockBit Ransomware and Vidar Infostealer Disguised as Resumes - ASEC

By ATCP

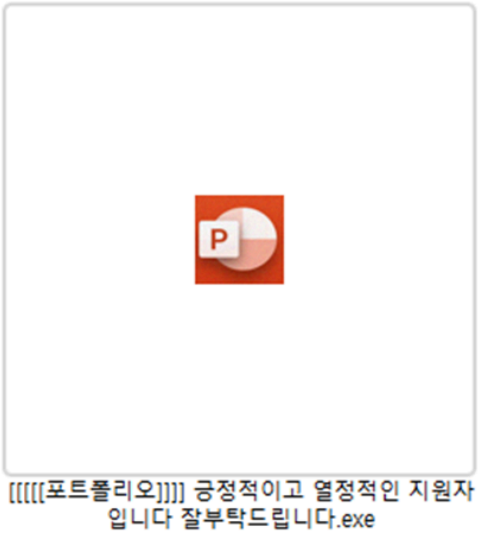
Published: 2023-11-02 · Archived: 2026-04-05 14:58:22 UTC

The distribution method involving the impersonation of resumes is one of the main methods used by the LockBit ransomware. Information related to this has been shared through the ASEC Blog in February of this year. [1] In contrast to the past where only the LockBit ransomware was distributed, it has been confirmed that an Infostealer is also being included in recent distributions. [2] (This link is only available in Korean.)

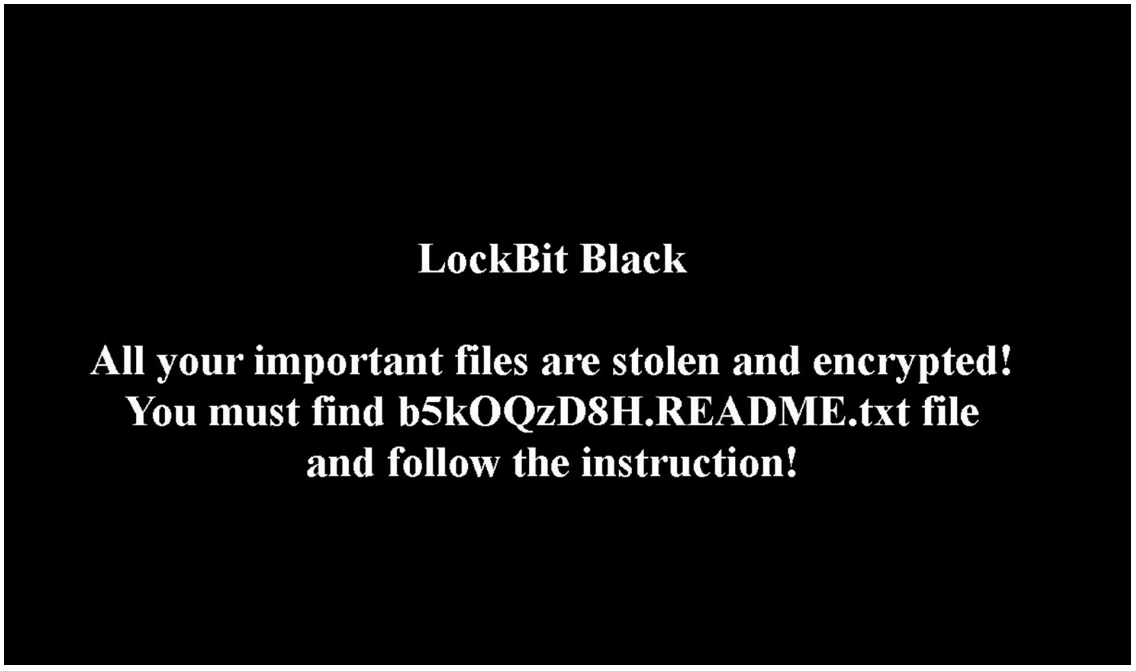


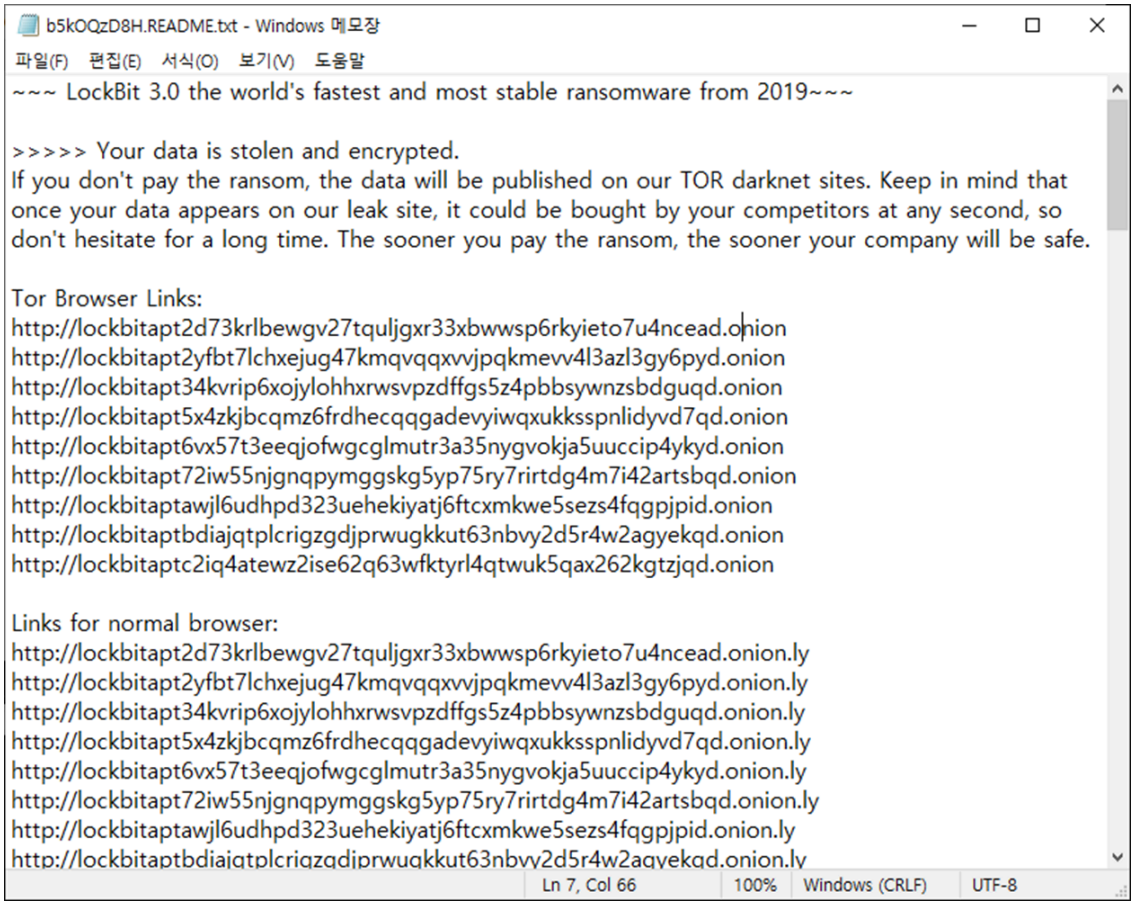


'Resume16.egg' holds the LockBit ransomware disguised as a PDF file (left) and the Vidar Infostealer disguised as a PPT file (right).

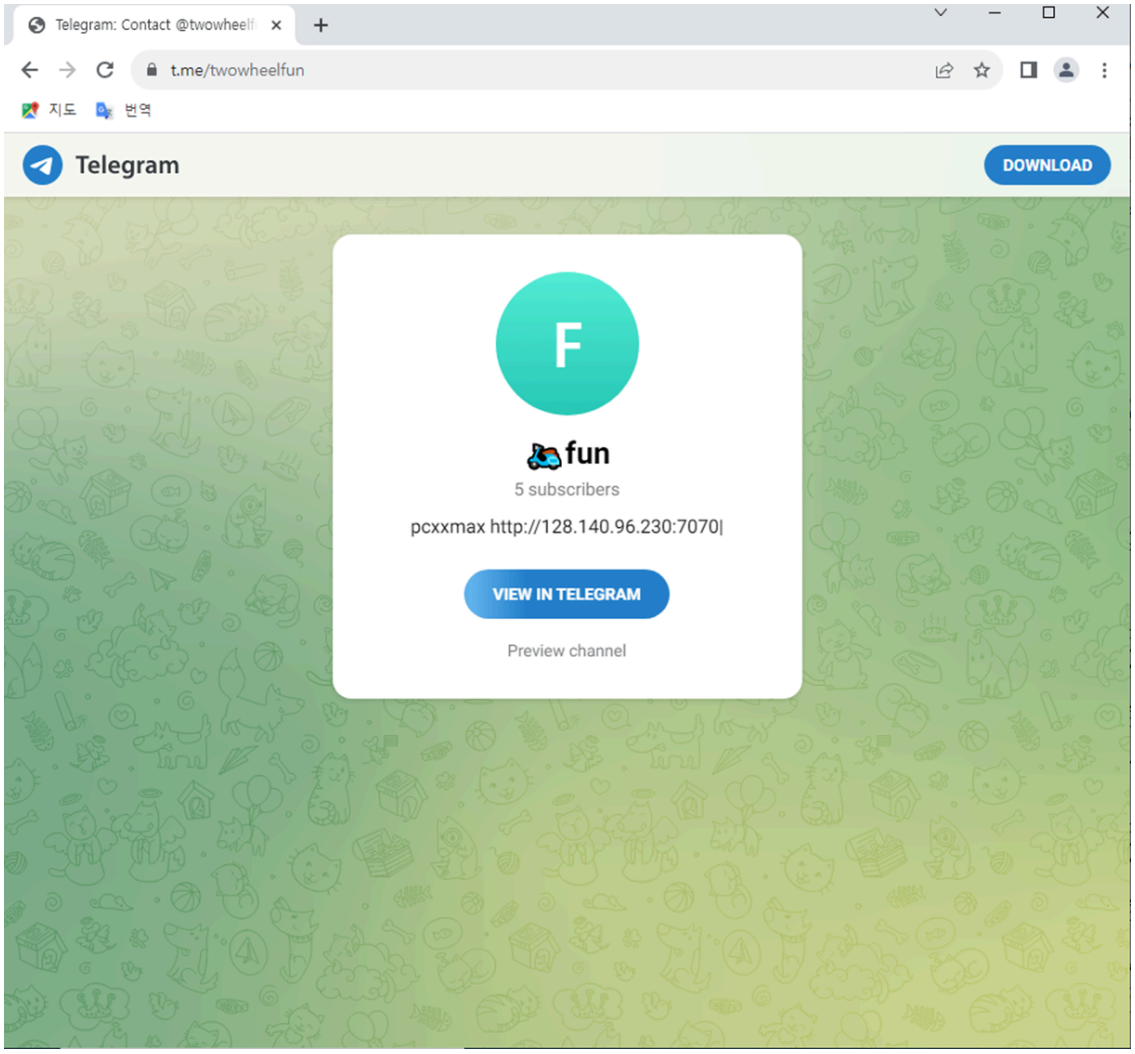


The executed ransomware is LockBit 3.0, which encrypts files on the user's PC environment, excluding PE files.

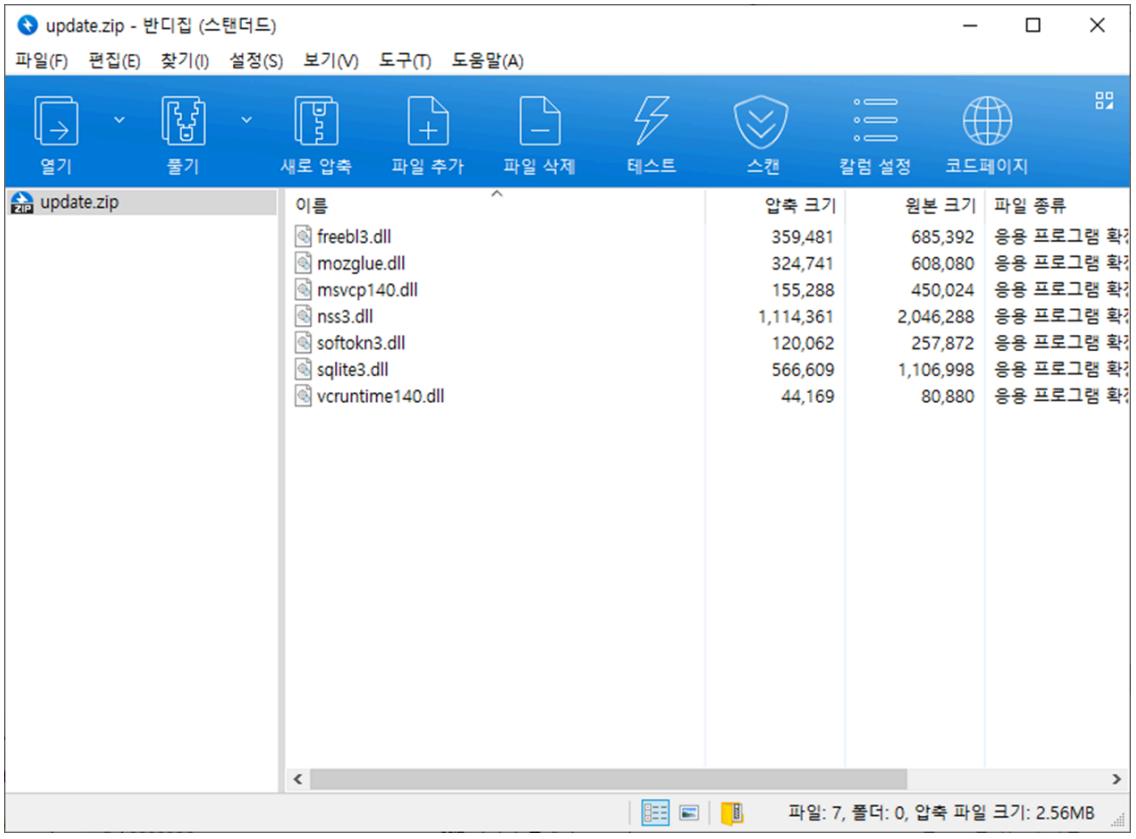




The Vidar Infostealer, which is distributed alongside the LockBit ransomware, connects to a Telegram website before engaging in C2 communication. The website is the Telegram channel called “twowheelfun”. It uses a certain string mentioned on the page as the C2 server address. This method can often be observed from the Vidar Infostealer, and it allows bypassing network detection by periodically changing C2 servers.



Following this, it connects to the actual C2 server to download the necessary DLL files for performing malicious activities and tranfers the exfiltrated information to the C2 server.




```
64
1,1,1,1,0,9b778979d08c730b781c6495b77b84ff,1,1,1,1,0,Default%DOCUMENTS%₩:*.txt:50:true:*windows*:,0
0
```

Malware disguised as resumes target corporations and are distributed along with not only the LockBit ransomware but an Infostealer 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.R613812

[Behavior Detection]
Ransom/MDP.Event.M4353
Win-Trojan/MalPeP.mexp

MD5

0d4967353b6e48ab671aed24899827aa

92350da914ba55c3137c9a8a585f7750

Additional IOCs are available on AhnLab TIP.

URL

http[:]//128[.]140[.]96[.]230/

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/58750/