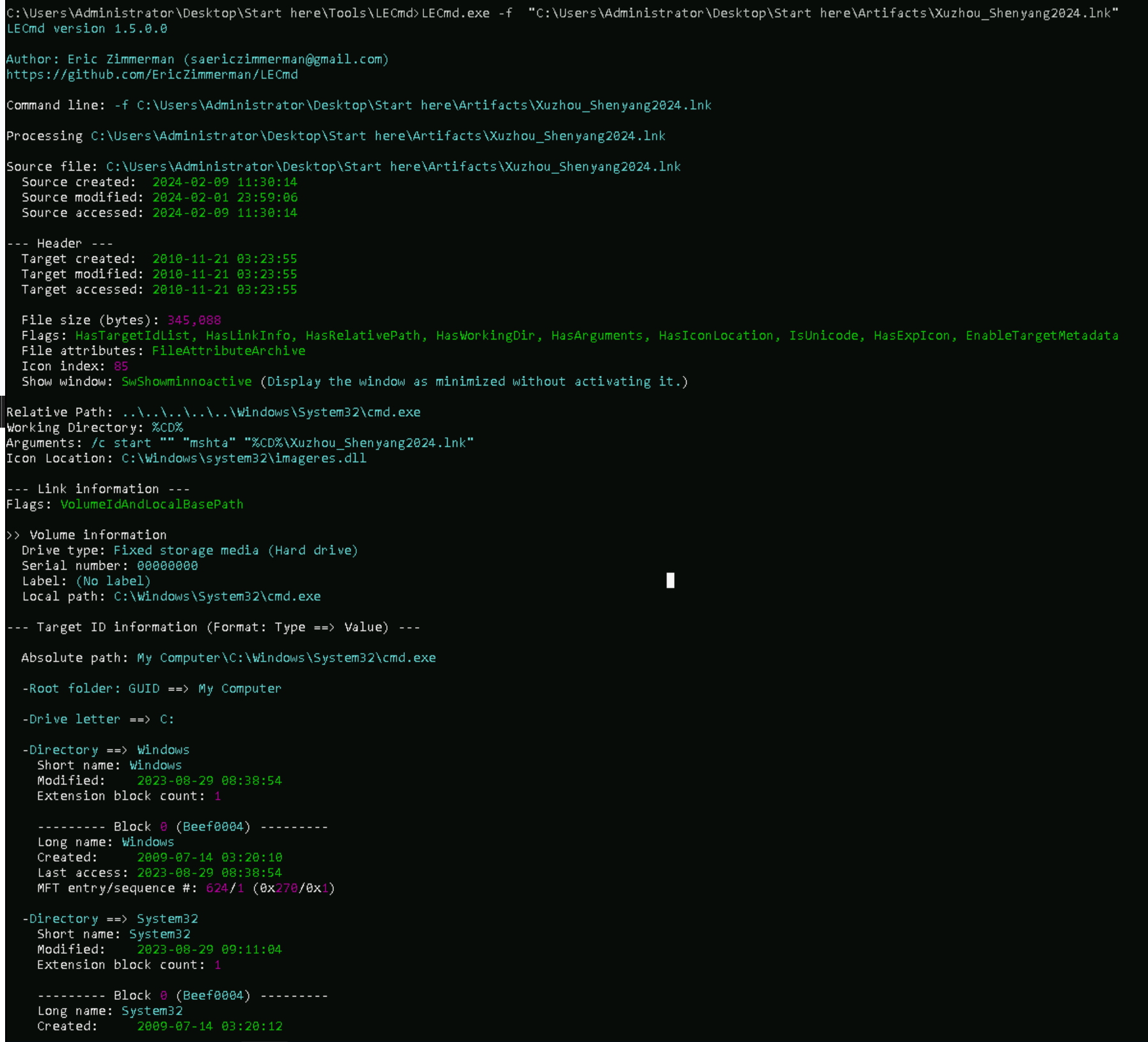
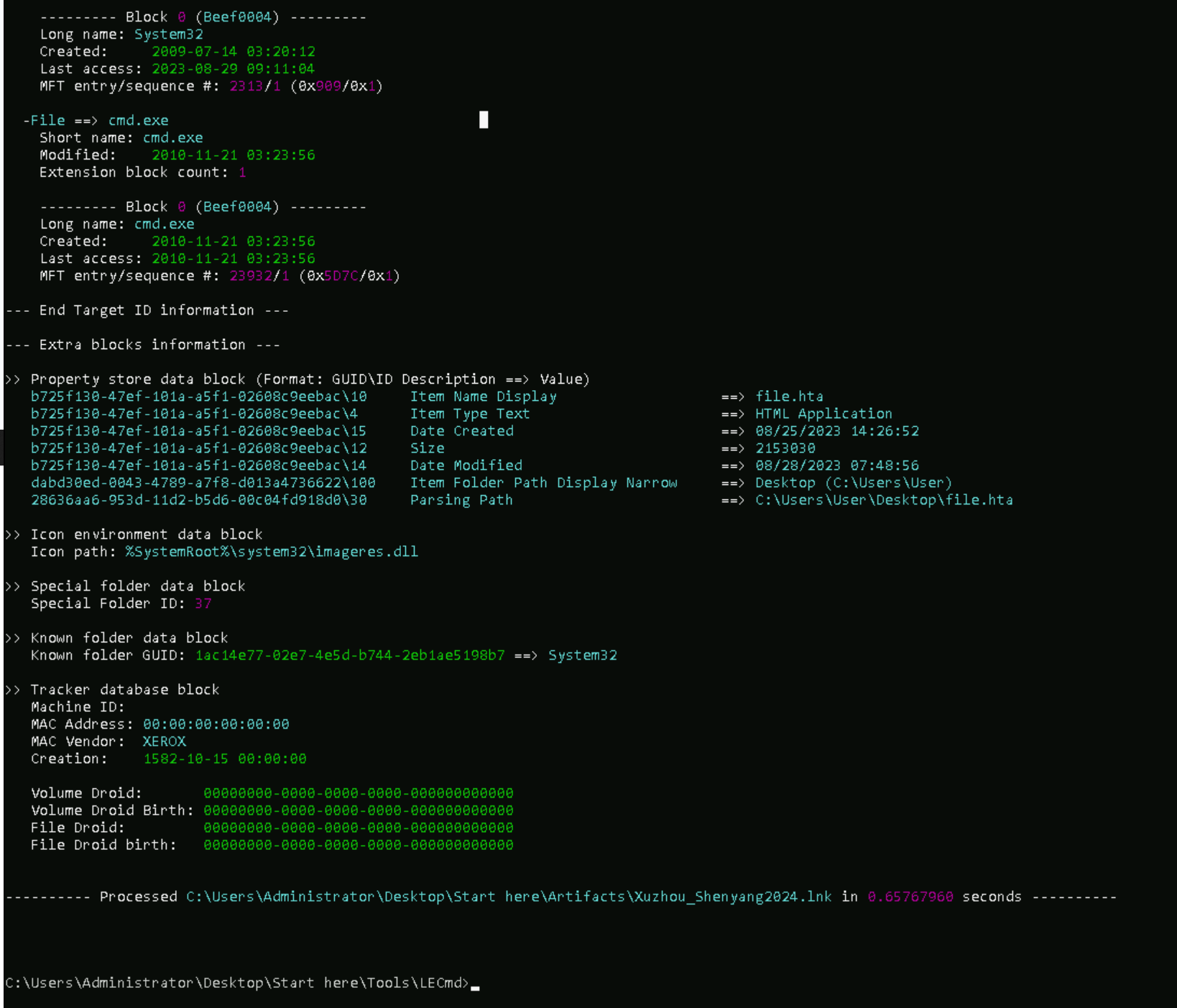
1. I employed the LECmd tool to investigate the contents of a lnk file, which serves as a shortcut to the original harmful file activated upon its execution. During the examination, I uncovered an embedded hta file, an HTML Application, likely containing a script capable of triggering subsequent actions.





2. To delve deeper into the lnk file, I utilized strings.exe, which revealed base64 encoded text and a camouflaged script. By using an online tool to reverse the obfuscation, I unearthed a vital segment of the script that not only initiates the download of a secondary payload but also includes a decryption key for an encrypted message.









3. Through thorough analysis, I was able to confirm that this incident was an authentic malware assault carried out by the GhostWriter (UAC-0057) hacker collective targeting a Ukrainian state organization.

Source:

https://cert.gov.ua/article/5661411