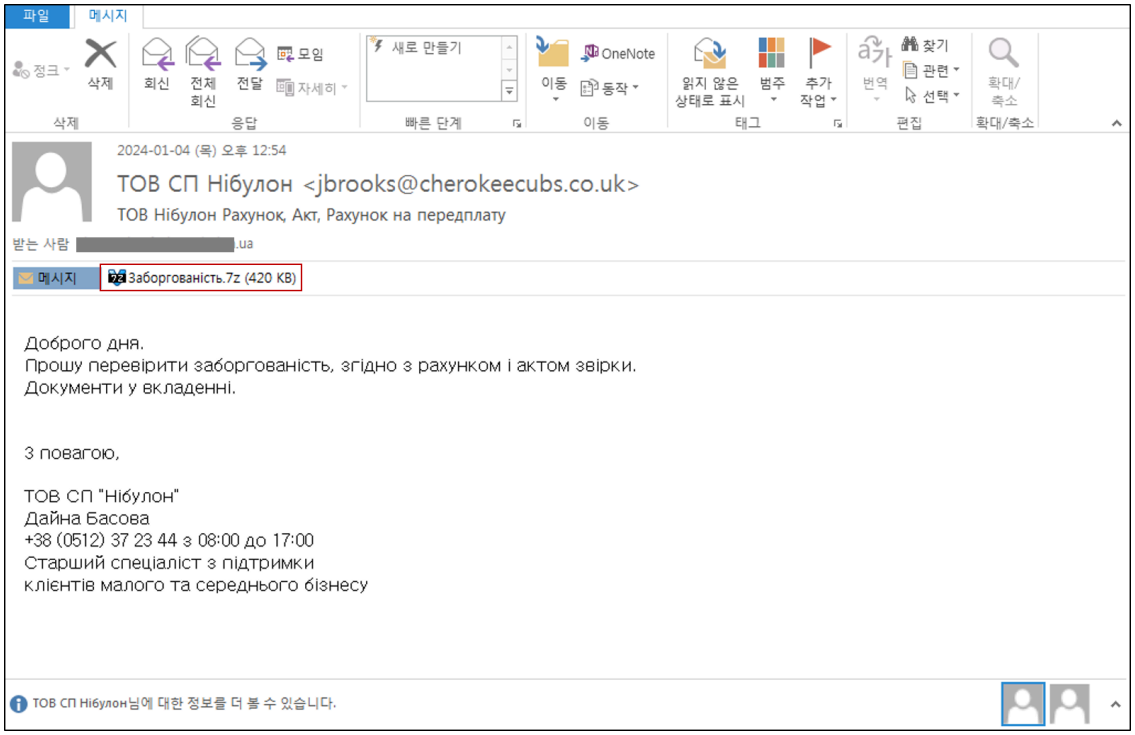
Distribution of SmokeLoader Targeting Ukrainian Government and Companies - ASEC

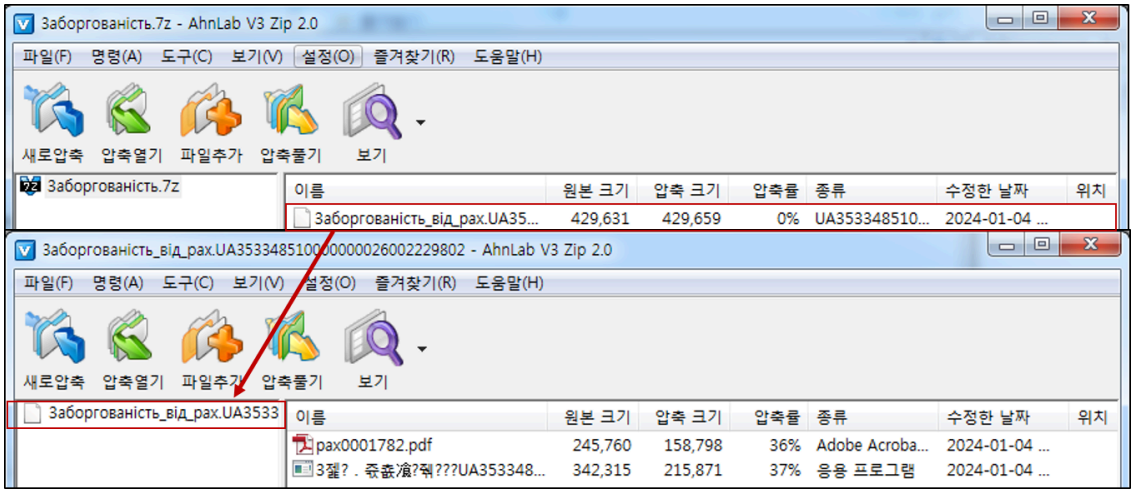
By ATCP

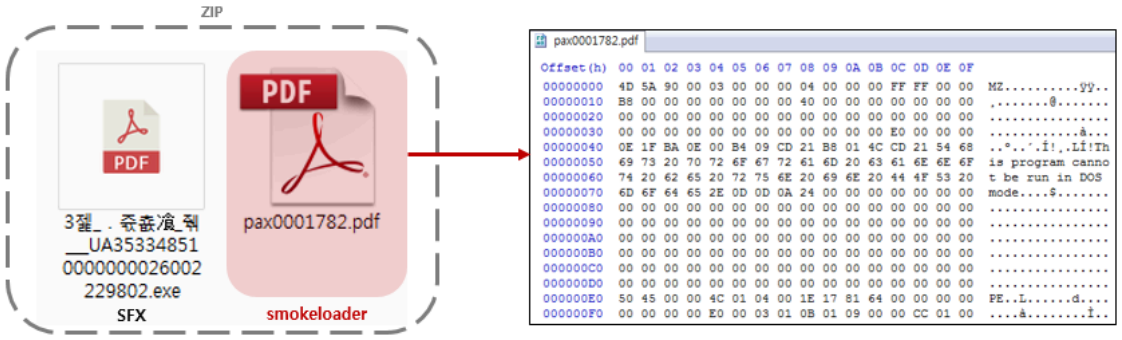
Published: 2024-01-15 · Archived: 2026-04-05 20:03:07 UTC

AhnLab SEcurity intelligence Center (ASEC) discovered that multiple SmokeLoader malware are being distributed to the Ukrainian government and companies. It seems that the number of attacks targeting Ukraine has increased recently. The targets confirmed so far include the Ukrainian Department of Justice, public institutions, insurance companies, medical institutions, construction companies, and manufacturing companies. The distributed email follows the format shown in Figure 1 written in Ukrainian. The body included information related to an invoice, prompting the reader to execute the attached file.



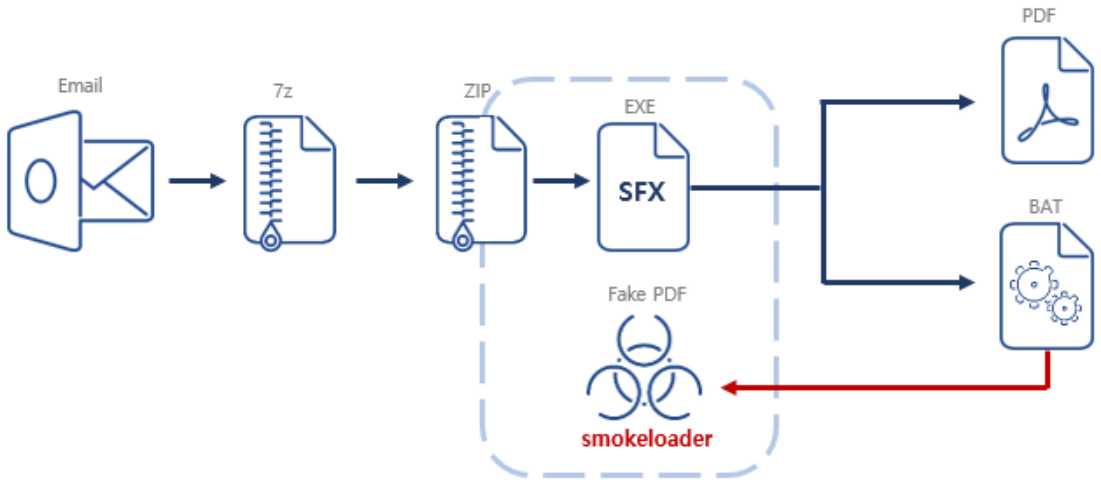
The attached file is a compressed file (7z) with another compressed file (ZIP) inside. Within this compressed file, an EXE file in an SFX format and SmokeLoader disguised with a PDF extension are found.





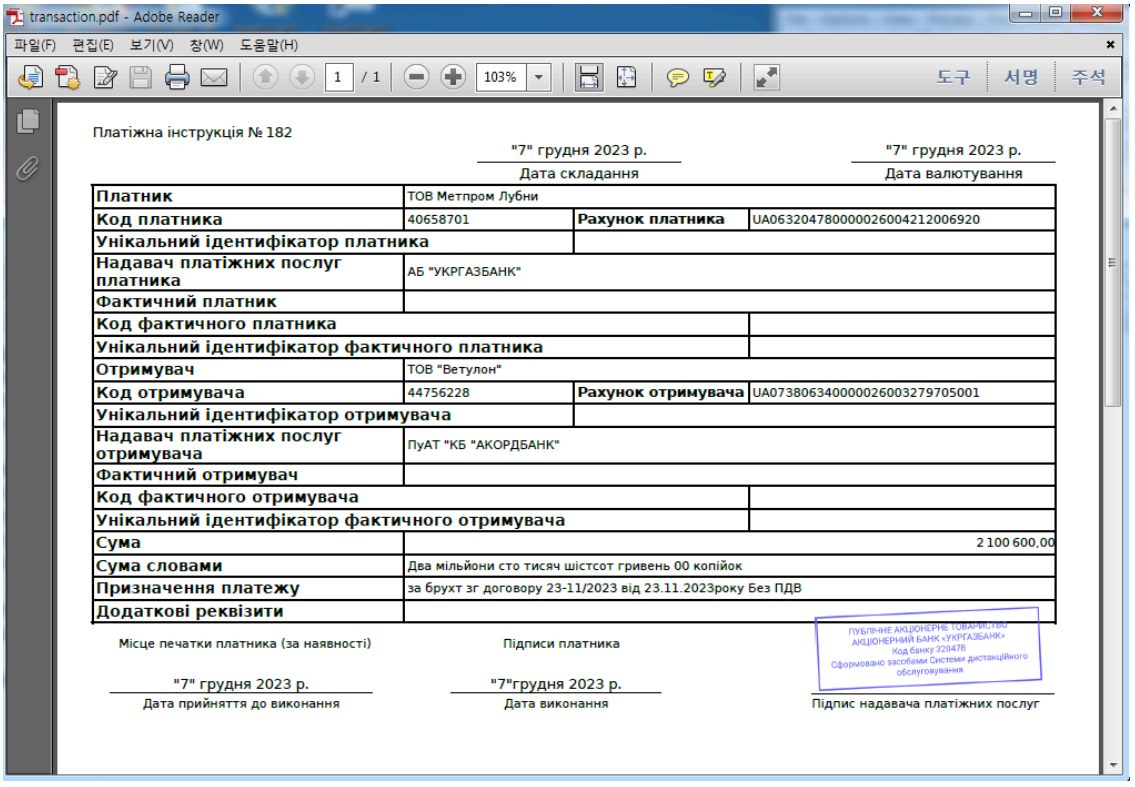
SmokeLoader has its extension set as a PDF, so it fails to run properly when the user clicks on the file to execute. The file is executed by the SFX that is also inside the compressed file. The overall process can be seen in Figure

4.



First, the SFX file creates and executes the PDF and BAT files. The PDF is just a bait file used to deceive the user, and the BAT file uses the command below to execute SmokeLoader.

- **BAT command** start = pax0001782.pdf



SmokeLoader is a downloader malware, and it can download additional modules or malware by receiving commands after connecting to the C&C server. When executed, it injects into the explorer.exe, and the malicious activity is carried out through the following process. First, it duplicates itself as “ewuabsi” in the %AppData% path, where it hides itself and grants system file properties. Then, it attempts to connect to the C&C servers listed below, where Lockbit ransomware and various other malware can be additionally downloaded. •

hxxp://lumangilocino[.]ru/index.php • hxxp://limanopostserver[.]ru/index.php • hxxp://numbilonautoparts[.]ru/index.php • hxxp://specvestniknuk[.]ru/index.php • hxxp://agropromnubilon[.]ru/index.php • hxxp://specvigoslik[.]ru/index.php • hxxp://avicilombio[.]ru/index.php • hxxp://germagosuplos[.]ru/index.php • hxxp://niconicalucans[.]ru/index.php • hxxp://civilomicanko[.]ru/index.php [File Detection]
Trojan/Win.FakePDF.R626460 (2023.12.03.02) Dropper/Win.DropperX-gen.R630443 (2024.01.05.01) **[Behavior Detection]** Malware/MDP.Execute.M1567

MD5

7ccf5bb03e59b8c92ad756862ecb96fd

852ce0cea28e2b7c4deb4e443d38595a

Additional IOCs are available on AhnLab TIP.

URL

http[:]//agropromnubilon[.]ru/index[.]php

http[:]//avicilombio[.]ru/index[.]php

http[:]//civilomicanko[.]ru/index[.]php

http[:]//germagosuplos[.]ru/index[.]php

http[:]//limanopostserver[.]ru/index[.]php

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.