RokRAT Malware Using Malicious Hangul (.HWP) Documents - ASEC

By ATCP

Published: 2025-07-20 · Archived: 2026-04-05 17:07:40 UTC

AhnLab SEcurity intelligence Center (ASEC) recently discovered the distribution of RokRAT malware using a Hangul Word Processor document (.hwp). RokRAT is typically distributed by including a decoy file and malicious script inside a shortcut (LNK) file. However, ASEC found a case where the malware was distributed through HWP documents instead of an LNK file.

File Name
250615_Operation status of grain store.hwp
Recent major portal site.hwpx
[Notice] Q1 VAT Return Filing Deadline (Final)

Table 1. Document file names used to distribute RokRAT

The document ‘250615_Operation status of grain store.hwp’ is shown in the following figure.

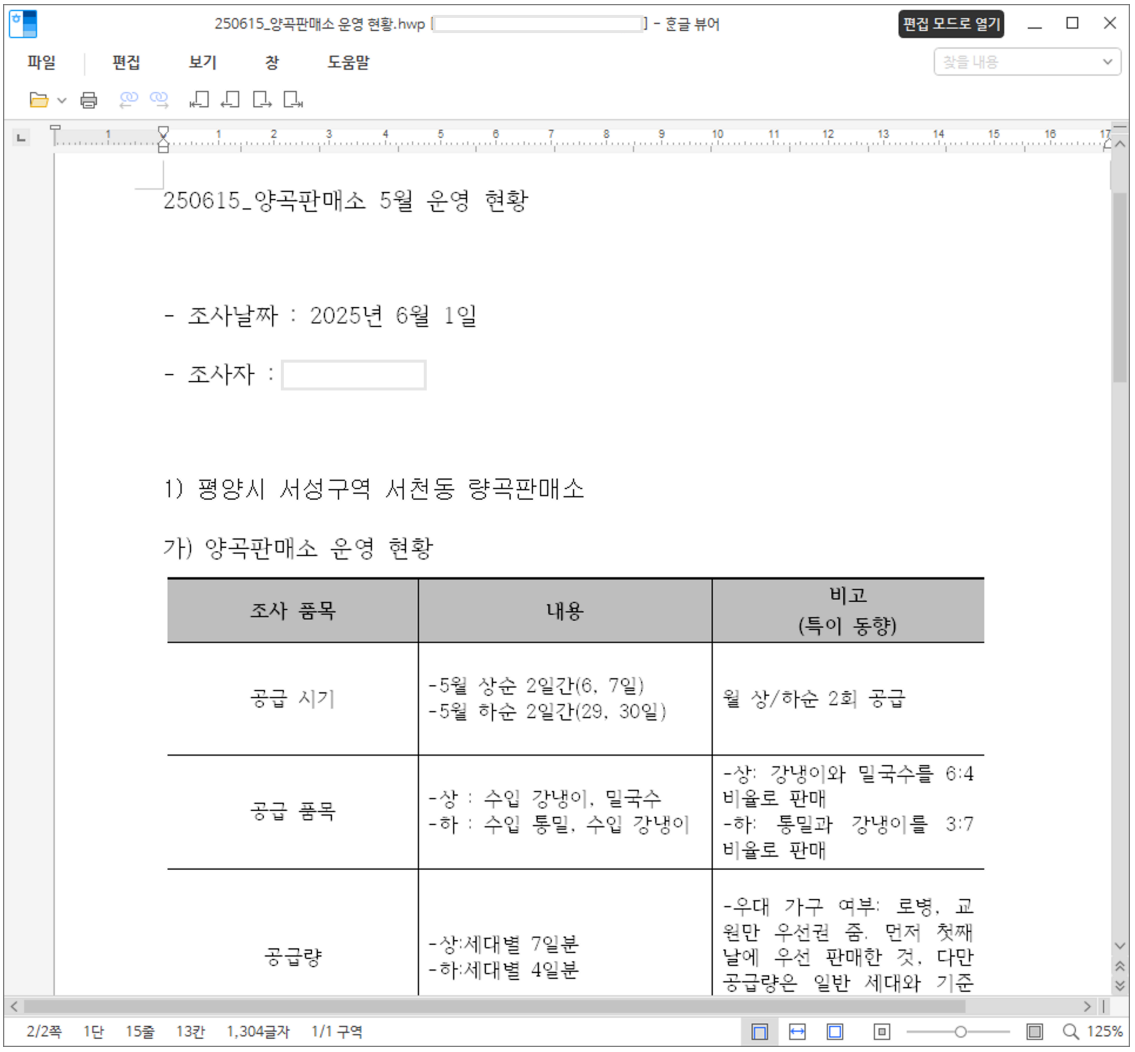

Figure 1. Document content

To avoid suspicion, the document covers North Korea’s grain distribution points, matching the file name ‘250615_Operation status of grain store’.

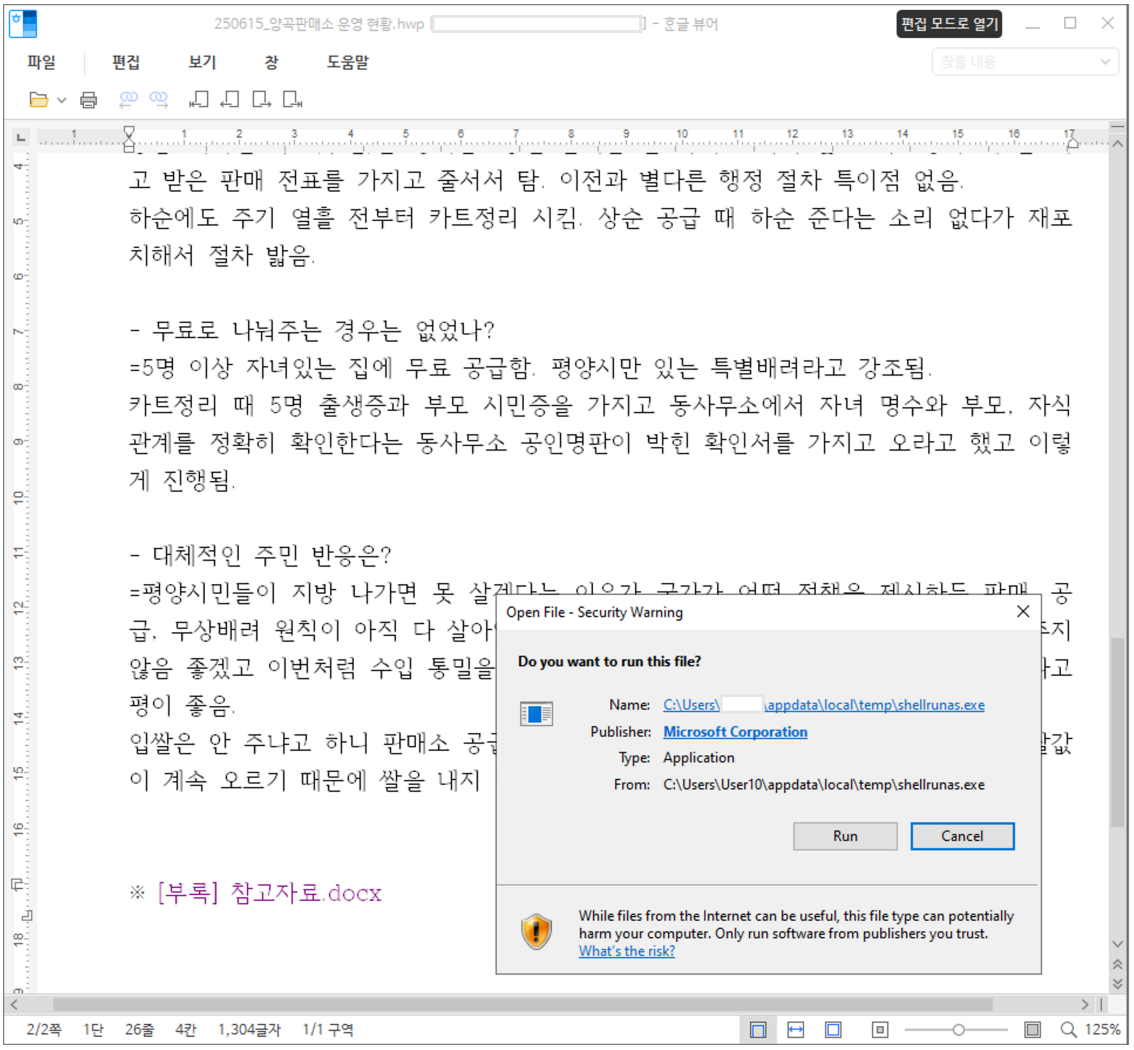

Figure 2. Hyperlink to execute ShallRunas.exe

At the bottom of the document, a hyperlink to '[Appendix] Reference Materials.docx' is inserted. When users click this link, a warning window is displayed asking whether to execute ShellRunas.exe located in the %TEMP% path. If users select 'Run', their system will be infected with malware. This ShellRunas.exe is not downloaded from the threat actor's C2 server, but is instead embedded in the document as an OLE object. When users access the document page where the OLE object is located, it is automatically created in the %TEMP% path by the Hangul process.

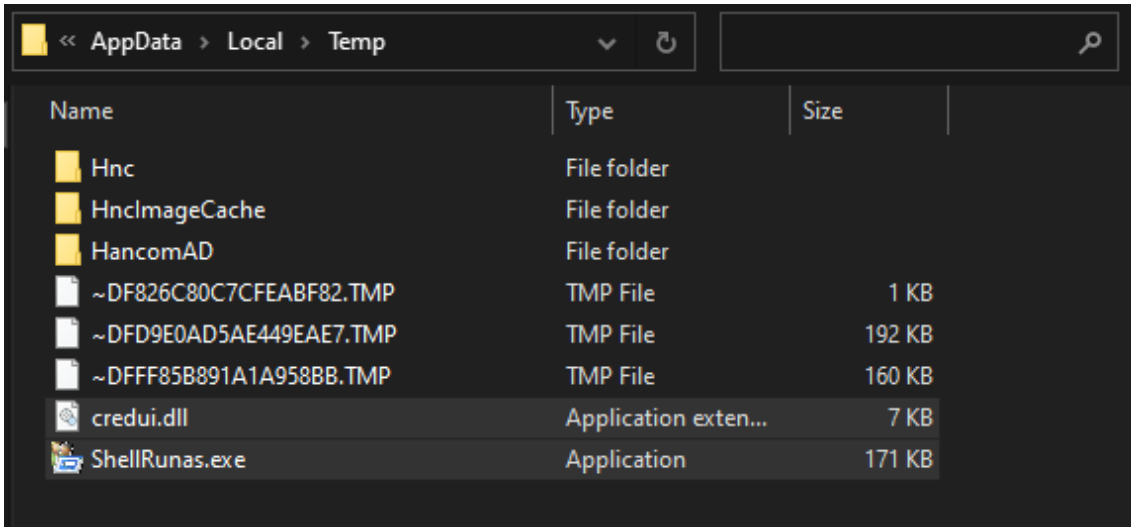

Figure 3. OLE objects automatically created by the Hangul process (ShellRunas.exe, credui.dll)

The threat actor specified %TEMP%\ShellRunas.exe as the hyperlink path. This way, the Hangul process automatically creates and executes ShellRunas.exe. In addition, the document contains an OLE object that corresponds to ShellRunas.exe and another OLE object that corresponds to credui.dll. Both of these objects are inserted into the document, and they are created together in the %TEMP% folder. ShellRunas.exe is a legitimate program signed with a Microsoft certificate. When it is executed, the malicious DLL, credui.dll, which is located in the same path, is loaded using the DLL side-loading technique. In this type of attack, the following legitimate executables were used by the threat actor along with ShellRunas.exe:

Legitimate Program	**Malicious Files Loaded**
accessenum.exe	mpr.dll
ShellRunas.exe	credui.dll
hhc.exe	hha.dll

Table 2. Legitimate programs used in DLL side-loading technique

The credui.dll file downloads the Father.jpg file from Dropbox. The JPG file is actually an image that contains a shellcode to load RokRAT into the memory at a specific location.

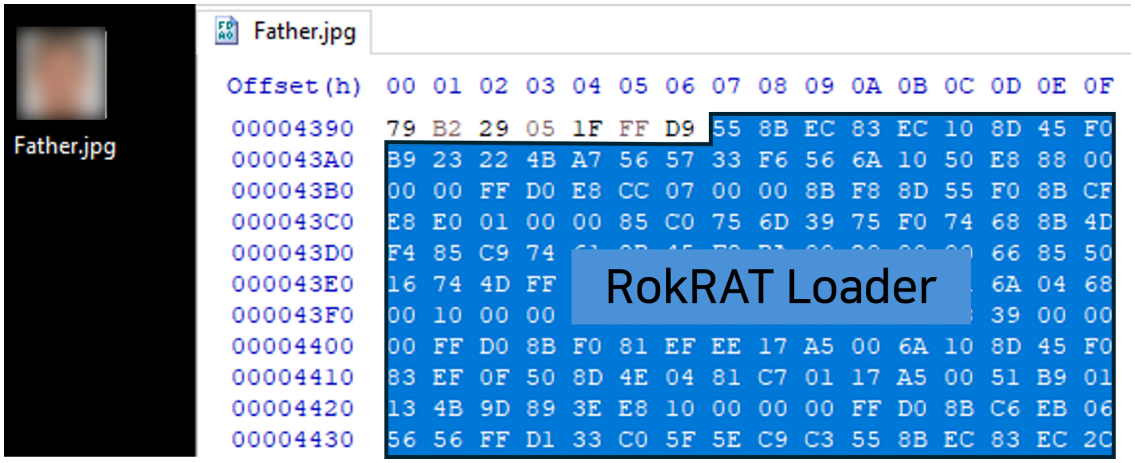

Figure 4. Shellcode inserted into the image

RokRAT, which is ultimately executed, can collect user information and perform various malicious behaviors according to the threat actor’s commands, so extra caution is advised.

MD5

a2ee8d2aa9f79551eb5dd8f9610ad557

d5fe744b9623a0cc7f0ef6464c5530da

e13c3a38ca58fb0fa9da753e857dd3d5

e4813c34fe2327de1a94c51e630213d1

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/89130/