Remcos RAT Distributed via Webhards - ASEC

By ATCP

Published: 2024-01-08 · Archived: 2026-04-05 20:17:52 UTC

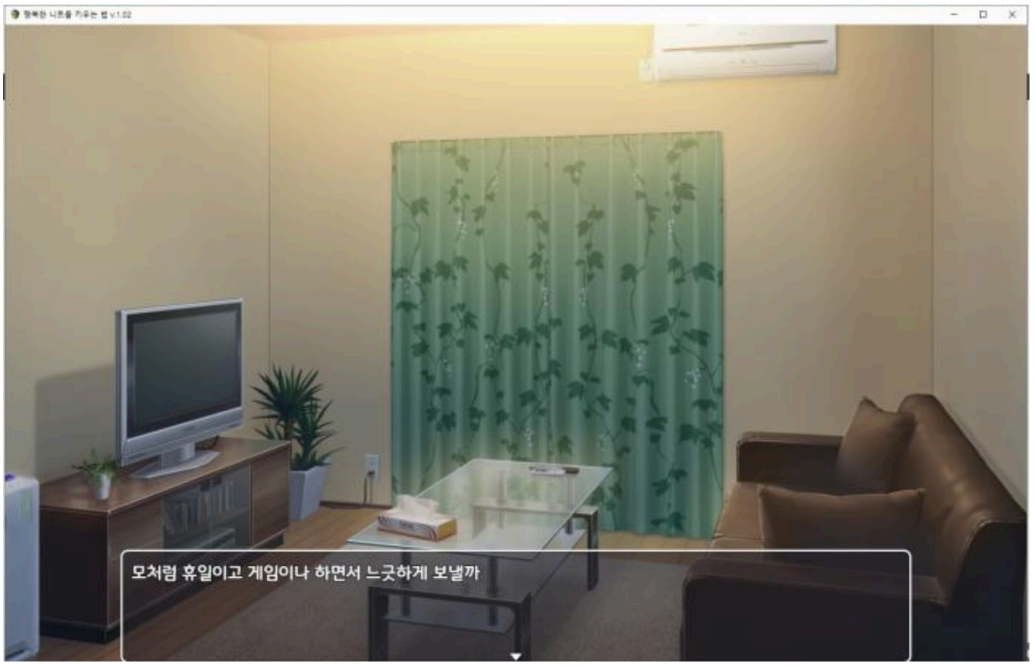
While monitoring the distribution sources of malware in South Korea, AhnLab SEcurity intelligence Center (ASEC) recently found that the Remcos RAT malware disguised as adult games is being distributed via webhards. Webhards and torrents are platforms commonly used for the distribution of malware in Korea.

Attackers normally use easily obtainable malware such as njRAT and UDP RAT, and disguise them as legitimate programs such as games or adult content for distribution. Similar cases were introduced in the previous ASEC blogs multiple times:

- UDP RAT Malware Being Distributed via Webhards
- njRAT Being Distributed through Webhards and Torrents
- njRAT Malware Distributed via Major Korean Webhard

	등록번호	제목	용량	분류	판매자	잔여일
☐	100306338	은하경병 아오바[번역/율회상]	179.0M	+19	[redacted]	28일
☐	99742529	[19게임/한글번역/+DLC/v1.9.1]호신술도	708.0M	+19	[redacted]	28일
☐	99136724	[19게임/손번역/v1.02]행복한 니트를 키	465.1M	+19	[redacted]	28일
☐	93856468	[19게임/한글번역]용희는 배고팠기 때문	5.4G	+19	[redacted]	28일
☐	99519440	[강추/최신/네토] 아멜리· 브랑셰트는	1.7G	+19	[redacted]	28일
☐	99221187	[19게임/손번역]들키지 않게 나체 코트로	1.4G	+19	[redacted]	28일
☐	99519439	[최신/강추] 미궁마을의 창관촌장	1.2G	+19	[redacted]	28일
☐	99519441	[최신/강추] 엔코도 앙코르! Ver1.22	511.7M	+19	[redacted]	28일
☐	96444373	[19게임/손번역/v1.10]마그멜의 창녀	258.5M	+19	[redacted]	28일

◀ PREV 1 NEXT ▶

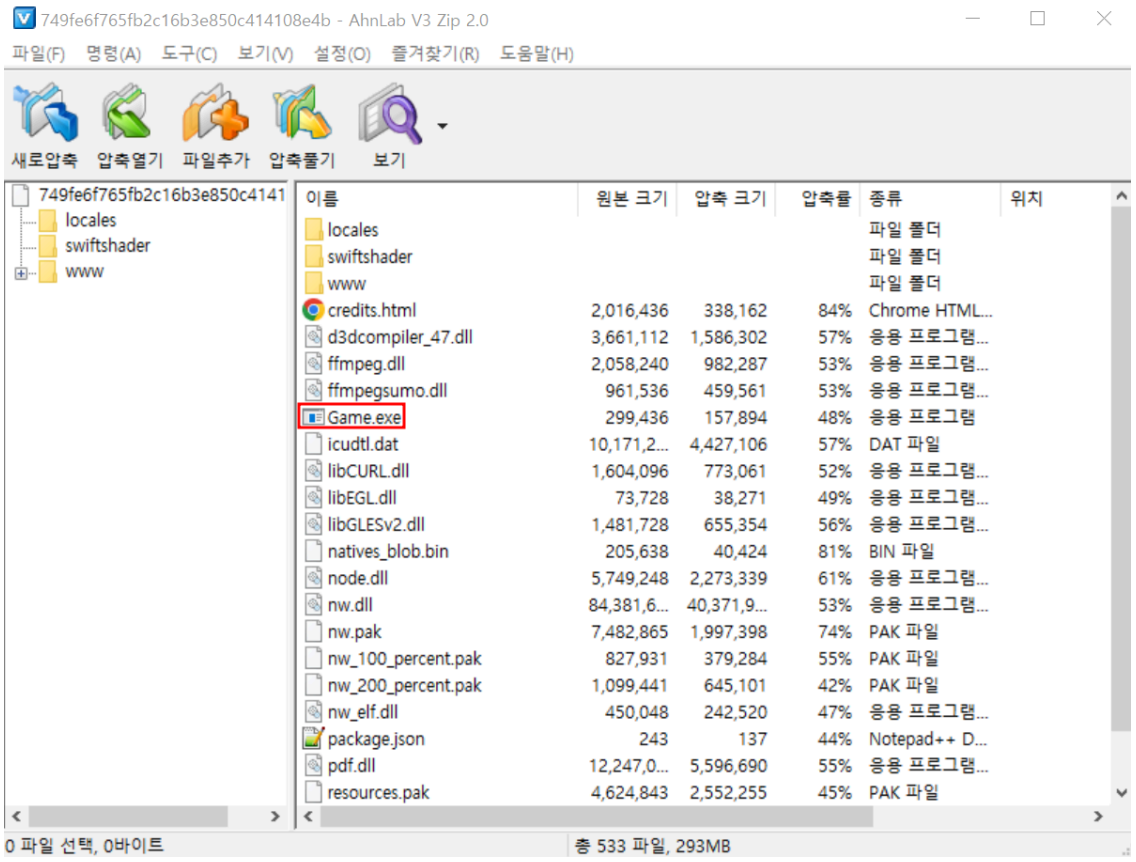


반디집으로 꼭 압축풀어주세요

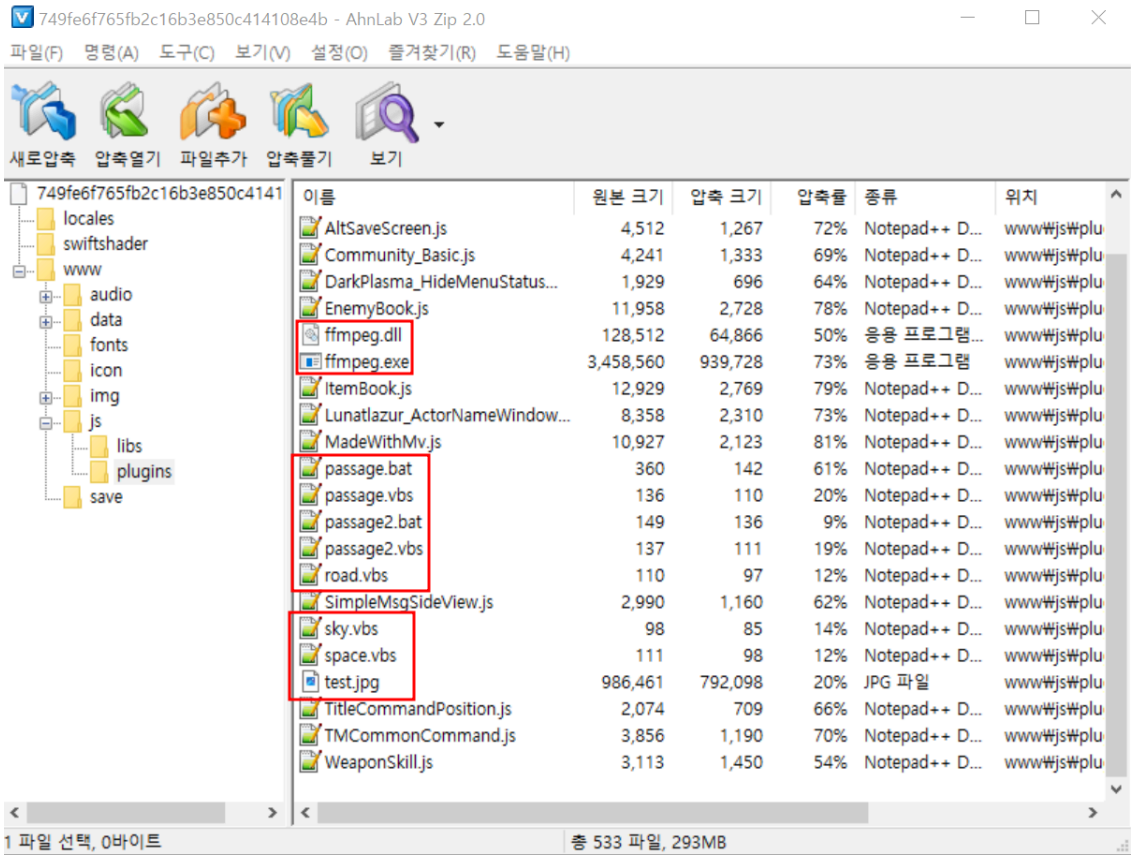
실행:game.exe

As shown in Figure 1, malware are being distributed via multiple games using the same method. The posts all have a guide that tells users to run the Game.exe file.

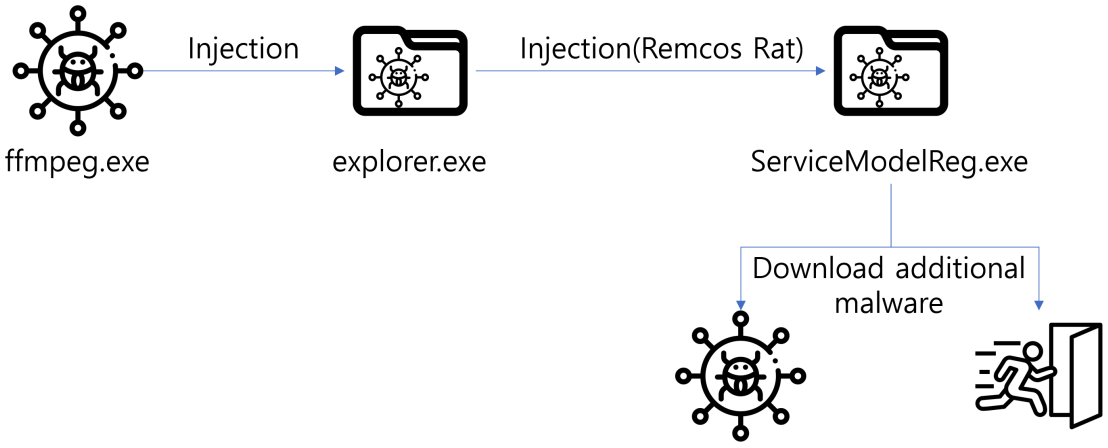
When the file is decompressed, the Game.exe file is present. Although it looks like a regular game launcher, the actual dll used to run the game exists separately, and the malicious VBS scripts are executed with the game file when you run Game.exe.



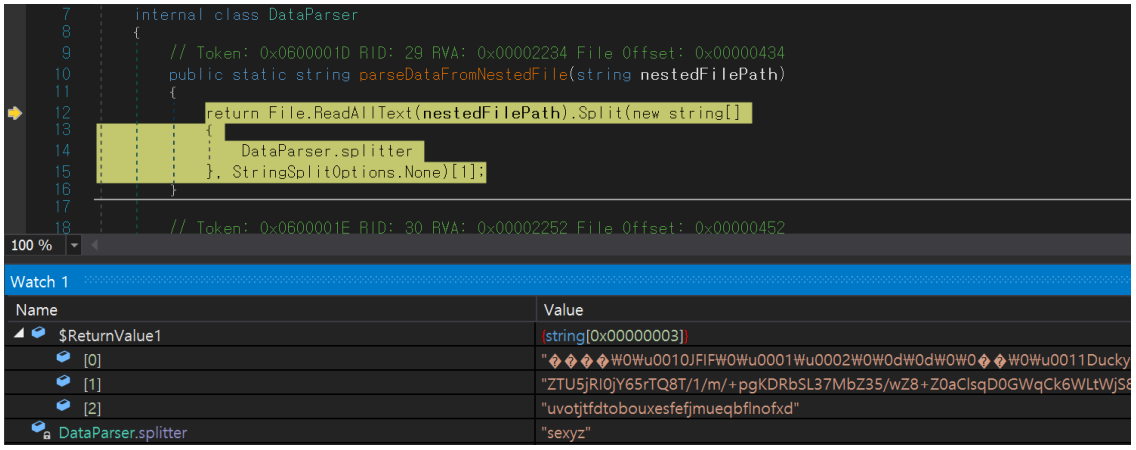

```
{
  sub_140001650();
  WinExec("libCURL.dll", 1u);
  WinExec("wscript .\\www\\js\\plugins\\passage.vbs", 0);
  WinExec("wscript .\\www\\js\\plugins\\passage2.vbs", 0);
  return 0i64;
}
```

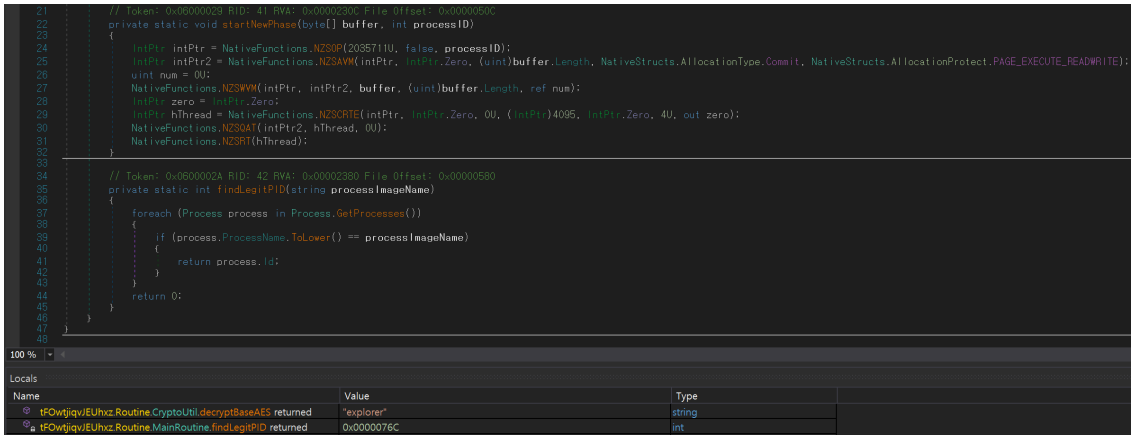


As shown in Figure 5, malware with malicious VBS exist in the www\js\plugins folder. What is ultimately executed is the ffmpeg.exe malware. The infection flow of the malware when it is executed is shown below.

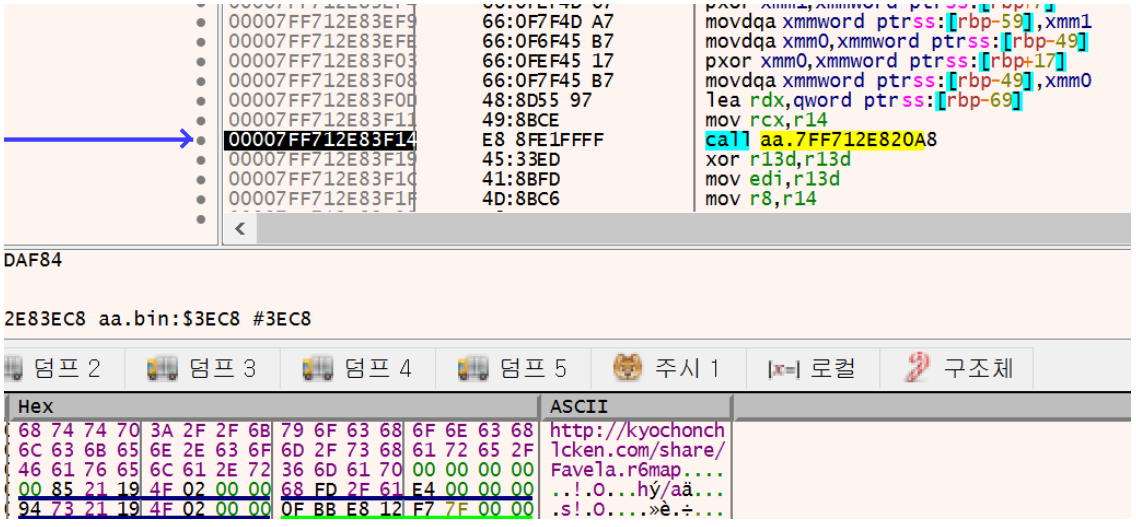


When ffmpeg.exe is executed, the “sexyz” string is split to extract the encrypted binary and the Key value from test.jpg. They are then injected into explorer.exe.





The injected malware downloads Remcos RAT through the C&C server shown in Figure 9 and attempts to perform additional behaviors by injecting it to ServiceModelReg.exe.



```
AllocConsole();
v2 = (HWND)dword_474B18();
hWnd = v2;
if ( !a1 )
  ShowWindow(v2, 0);
v3 = __acrt_iob_func(1u);
freopen("CONOUT$", "a", v3);
SetConsoleOutputCP(0x4E4u);
sub_41CCAA();
memset(Destination, 0, sizeof(Destination));
strcat(Destination, "\n\tRemcos v");
strcat(Destination, "4.9.1 Pro");
strcat(Destination, asc_46CF18);
return sub_407200(Destination, v5);
```

As shown in the example, users need to take caution as malware are being distributed actively via file-sharing websites such as Korean webhards. As such, caution is advised when running executables downloaded from a file-sharing website. It is recommended that users download programs from the official websites.

[File Detection]
Trojan/Win.Injector.R630725 (2024.01.08.02)
Trojan/Win.Injector.R630726 (2024.01.08.02)
Trojan/VBS.Runner.SC195782 (2024.01.08.02)
Trojan/VBS.Runner.SC195783 (2024.01.08.02)
Trojan/BAT.Agent.SC195781 (2024.01.08.02)
Trojan/BAT.Agent.SC195785 (2024.01.08.02)
Trojan/VBS.Runner.SC195786 (2024.01.08.02)
Trojan/VBS.Runner.SC195787 (2024.01.08.02)
Trojan/VBS.Runner.SC195784 (2024.01.08.02)

MD5

00bfd32843a34abf0b2fb26a395ed2a4

2e6796377e20a6ef4b5e85a4ebbe614d

2f6768c1e17e63f67e173838348dee58

36aa180dc652faf6da2d68ec4dac8ddf

4d04070dee9b27afc174016b3648b06c

Additional IOCs are available on AhnLab TIP.

URL

http[:]//kyochonchlcken[.]com/share/1[.]exe

http[:]//kyochonchlcken[.]com/share/BankG[.]r6map

http[:]//kyochonchlcken[.]com/share/Favela[.]r6map

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/60270/