

Remcos RAT Being Distributed to Korean Users

A asec.ahnlab.com/en/92160

ATCP

January 15, 2026



AhnLab SEcurity intelligence Center (ASEC) has confirmed the RAT distribution of the Remcos RAT targeting users in South Korea. While the original distribution pages remain unknown, the malware appears to masquerade as VeraCrypt installers or software associated with illegal gambling websites.

1. Malware Distribution

One of the initial malware samples displays an interface labeled “Blocklist User DB Lookup *****Club”. In this context, “Blocklist User” refers to gambling-site account status category. The program pretends to query a remote database (acting as a C2 server) to look up these restricted accounts.

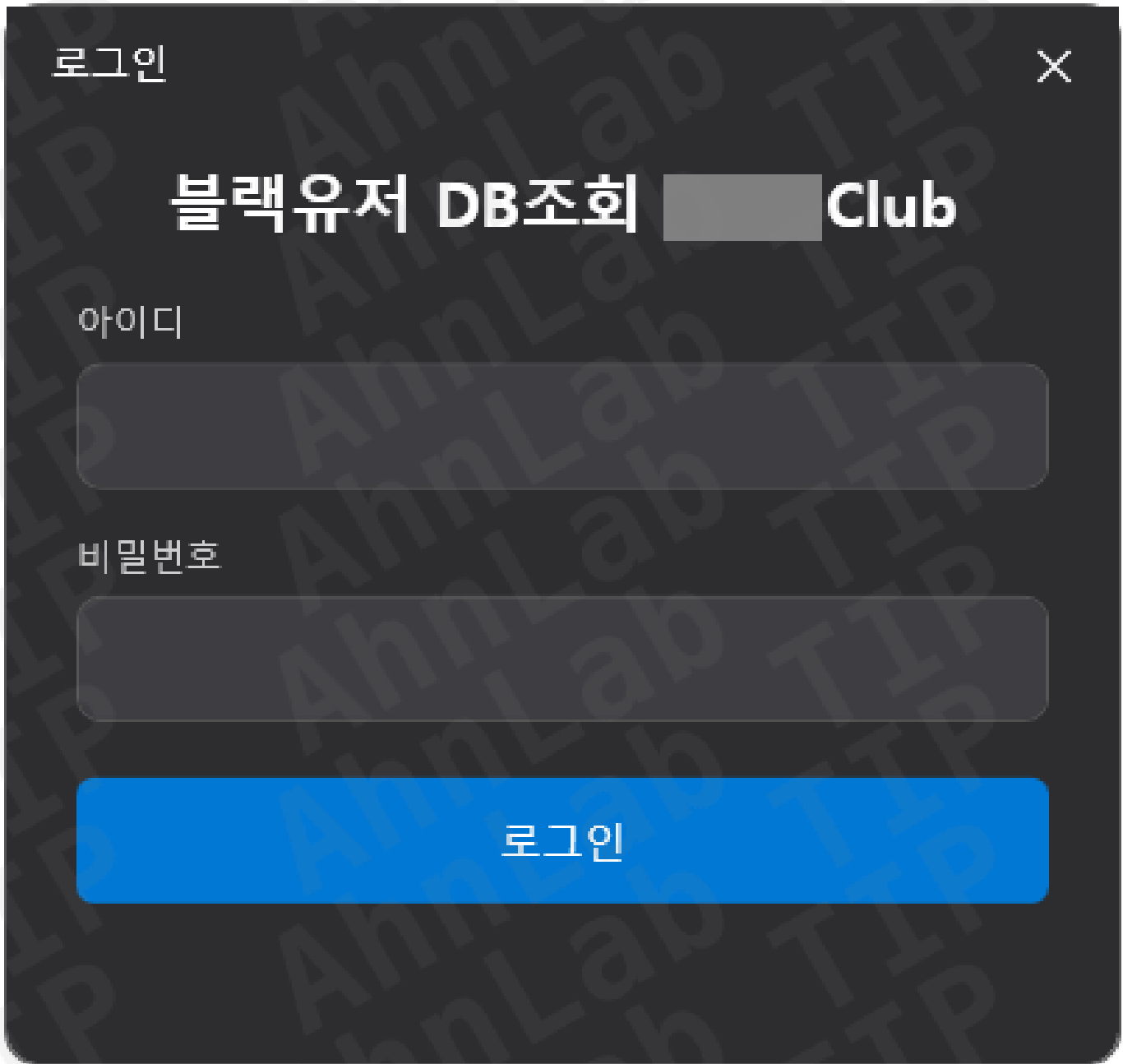


Figure 1. GUI screen of the distributed Remcos RAT

Distribution has occurred through web browsers and Telegram, using file names such as "*****usercon.exe" or "blackusernon.exe."

Distribution Name

%USERPROFILE%\downloads\programs*****usercon.exe

%USERPROFILE%\downloads\telegram desktop*****usercon.exe

%USERPROFILE%\downloads\programs\blackusernon.exe

Table 1. File names used when distributing Malware

The keywords displayed in the GUI—such as “*****Club”—and the terms embedded in the filenames are associated with so-called “Blocklist user lookup site” used within illegal online gambling ecosystems. In this context, a “Blocklist user lookup site” refers to platforms used by operators or users of private sports-betting or casino services to look up accounts that have been flagged or blocked. Although the exact distribution page remains unknown, the GUI and filenames strongly suggest that the malware is being distributed by impersonating tools that claim to offer blocklist-lookup functionality for illegal gambling operators or users.

2. Dropper Malware (DB lookup program/VeraCrypt installer impersonation)

3. VBS/PowerShell Downloader and Injector

The threat actor used multiple stages of obfuscated VBS and PowerShell scripts before deploying the Remcos RAT. These scripts include dummy comments, junk data, and misleading extensions. In one sample, the file masquerades as a JPG image while embedding a Base64-encoded PE payload between separators.

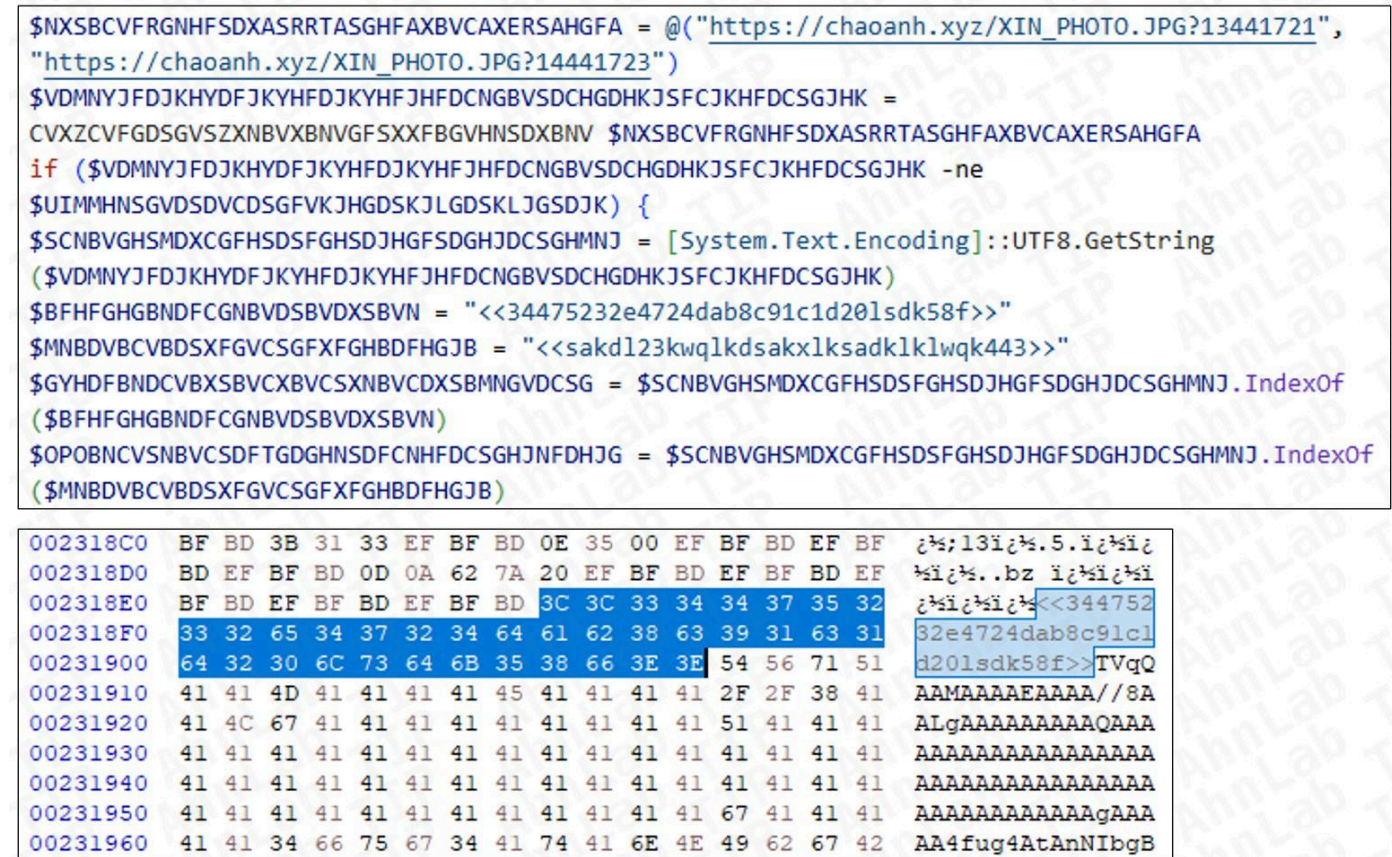


Figure 4. Malware inside the obfuscated routine and dummy data

Stage	Type	Name
1	Installer	
2	VBS downloader	%TEMP%[Random].vbs
3	VBS dropper	XX12.JPG
4	VBS downloader	Config.vbs
5	VBS downloader	L1k9.JPG
6	PowerShell downloader	NMA1.JPG
7	Injector	XIN_PHOTO.JPG
8	Remcos RAT	Aw21.JPG

Table 2. Malware Flow

After progressing through five scripted stages, the chain delivers a .NET-based injector. The injector sends logs to the attacker via Discord Webhooks. It then downloads Remcos RAT payload from a URL passed as an argument, decrypts it, and injects it into the AddInProcess32.exe process. Notably, this injector contains Korean-language messages not commonly seen in other Remcos workflows.



Figure 5. Routine of the injector malware

4. Remcos RAT

Remcos is a commercially sold remote administration tool that has long been abused by threat actors. Beyond conventional remote-control capabilities—such as command execution, file management, and process control—it supports a range of data-theft functions, including keylogging, screenshot capture, webcam and microphone control, and credential extraction from web browsers.

The malware stores configuration data within an encrypted resource named “SETTINGS”, which reveals attacker-defined settings upon decryption.

Dump 1	Dump 2	Dump 3	Dump 4	Dump 5	Watch 1	[x=] Locals
Address	Hex				ASCII	
00577148	31 34 32 2E	32 34 38 2E	32 33 31 2E	32 35 32 3A	142.248.231.252:	
00577158	34 38 31 39	32 3A 31 1E	7C 1E 1E 1F	7C BF F8 B0	48192:1. ... ¿0°	
00577168	DD 20 C8 A3	BD BA C6 AE	7C 1E 1E 1F	7C 31 7C 1E	Y È f½°Æ® ... 1 .	
00577178	1E 1F 7C 00	7C 1E 1E 1F	7C 01 7C 1E	1E 1F 7C 01		
00577188	7C 1E 1E 1F	7C 31 7C 1E	1E 1F 7C 30	7C 1E 1E 1F	... 1 ... 0 ...	
00577198	7C 00 7C 1E	1E 1F 7C 38	7C 1E 1E 1F	7C 72 00 65	 8 ... r.e	
005771A8	00 6D 00 63	00 6F 00 73	00 2E 00 65	00 78 00 65	.m.c.o.s...e.x.e	
005771B8	00 00 00 7C	1E 1E 1F 7C	00 7C 1E 1E	1F 7C 00 7C		
005771C8	1E 1E 1F 7C	30 7C 1E 1E	1F 7C C1 F5	B1 C7 20 BD	... 0 ... Å ð ± Ç ½	
005771D8	C3 BC BC 20	C7 A5 BD C3	B1 E2 2D 59	4A 30 39 4C	Å¼¼ Ç¥¼Å±â-YJ09L	
005771E8	56 7C 1E 1E	1F 7C 31 7C	1E 1E 1F 7C	38 7C 1E 1E	V ... 1 ... 8 ..	
005771F8	1F 7C 5C B8	F8 3F 00 64	00 61 00 74	00 00 00 7C	. \,ø?.d.a.t...	

Figure 6. Settings of Remcos RAT

Case	C&C server	Name	Mutex, registry key
A	142.248.231[.]252:48192 (TLS)	Remote Host	Stock Price Ticker-YJ09LV
B	142.248.231[.]251:2404 (TLS)	RemoteHost	Rmc-BTQ3H5
C	205.198.88[.]94:2255 (TLS)	?? ???	?? ?? ???-3SDRQJ

Table 3. Some configurations of the used Remcos RAT

Some variants of Remcos RAT disguise themselves as a “stock price ticker” and even use Korean strings in their mutex names and registry keys. In addition, because certain variants have offline keylogging enabled, the captured keystroke strings are stored in the %ALLUSERSPROFILE%\remcos\ directory.

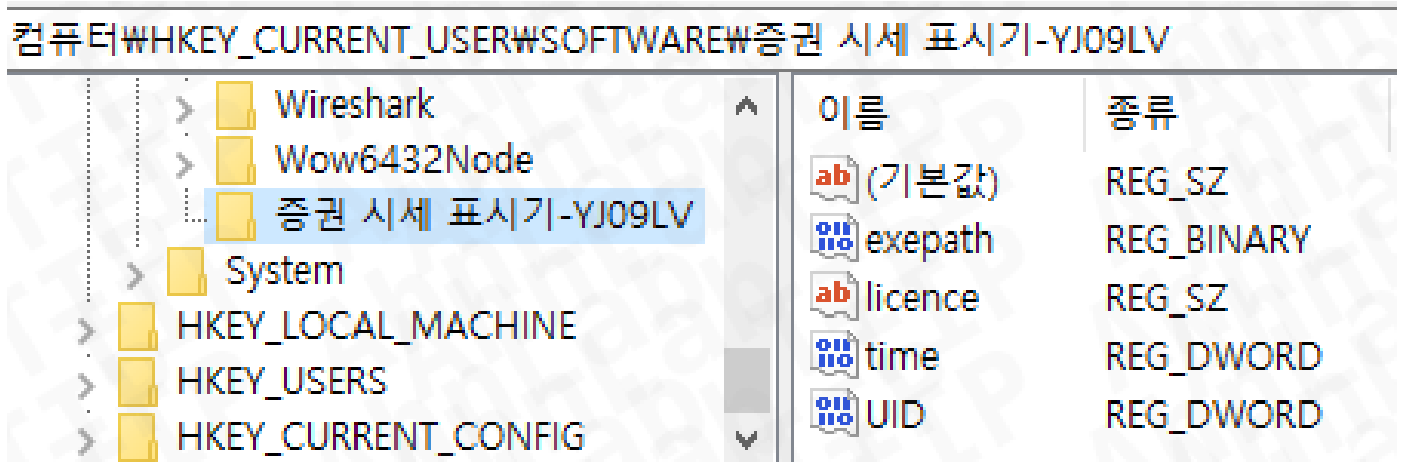


Figure 7. Korean strings stored in the registry

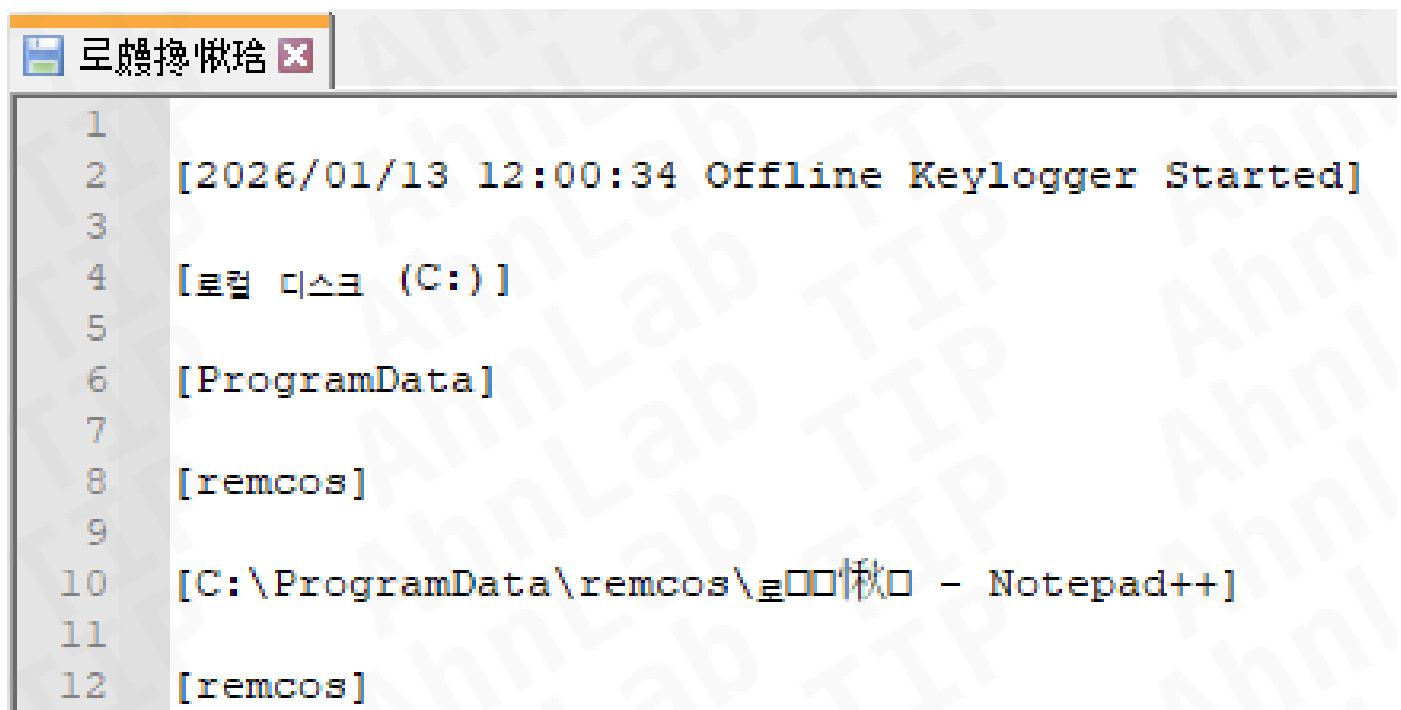


Figure 8. Logged keystroke data

5. Conclusion

Recent cases indicate that attackers have been actively distributing Remcos RAT to users in South Korea. Based on the file names used in the campaign, it appears that the primary targets may be operators or users of illegal online gambling platforms. However, the presence of malware disguised as VeraCrypt utility suggests that general users may also be included in the attackers' distribution scope.

Because Remcos is a RAT capable not only of remote control but also of extensive data-theft activities—including keylogging, screenshot capture, webcam and microphone access, and extraction of web browser credentials—users infected with Remcos RAT face a significant risk of having sensitive information compromised.

MD5

06c71658466d1dcd067ff0f23a8c488e

0e7a97c8ecf83f26b23c394d0e06001b

12756d1d21d6656d909502f7418c106b

2530035bacbab54ce2637f81b2d218d5

2c5b7c2fa8f3cea3324ae6044c5c61bb

Additional IOCs are available on AhnLab TIP.

URL

[https://chaoanh\[.\]com/XX12\[.\]JPG](https://chaoanh[.]com/XX12[.]JPG)

[https://chaoanh\[.\]xyz/Aw21\[.\]JPG](https://chaoanh[.]xyz/Aw21[.]JPG)

[https://chaoanh\[.\]xyz/L1k9\[.\]JPG](https://chaoanh[.]xyz/L1k9[.]JPG)

[https://chaoanh\[.\]xyz/NMA1\[.\]JPG](https://chaoanh[.]xyz/NMA1[.]JPG)

[https://chaoanh\[.\]xyz/XIN_PHOTO\[.\]JPG?13441721](https://chaoanh[.]xyz/XIN_PHOTO[.]JPG?13441721)

Additional IOCs are available on AhnLab TIP.

IP

142[.]248[.]231[.]251

142[.]248[.]231[.]252

205[.]198[.]88[.]94

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.



AhnLab TIP

Stay Ahead of Rapidly Evolving Threats Make the Best-Informed Decisions

Get Started with AhnLab's State-of-the-Art Threat Intelligence

atip.ahnlab.com