

Private HTS programs that spread ransomware

A asec.ahnlab.com/en/95469

ATCP

September 15, 2026



AhnLab SEcurity intelligence Center (ASEC) recently identified a case in which ransomware was distributed through a private home trading system (HTS). The HTS program used to distribute the ransomware is called “UBP Asset” and has long been exploited in online investment scams. Given that a photo of the same HTS program was also found in a blog post by a law firm in Korea published in September 2025, it appears that investment fraud organizations have recently been distributing ransomware to their victims.

1. Private HTS (Home Trading System)

A Home Trading System (HTS) is a system that allows investors to trade through a PC installed at home or in the office, rather than having to visit a securities firm’s trading floor or make a phone call to buy or sell stocks. [1] Unlike in the past, most individuals today trade financial products such as stocks, mutual funds, and futures online by installing an HTS on their cell phones or PCs.

In most cases, users install the HTS provided by regulated financial institutions and conduct their financial transactions through those firms. However, there have recently been numerous incidents in which illegal financial investment firms, posing as legitimate financial institutions, have induced users to install private HTS software and then stolen their investment funds.

Most unlicensed financial investment firms deceive users through online ads or text messages and then lure them into joining group chat rooms on social media platforms like KakaoTalk. They typically use advertisements claiming that overseas futures trading is possible with only a small margin deposit, or promoting commission-free trading and loans. [2] The administrators of these group chats then persuade the recruited users to install their self-developed private HTS and deposit their investment funds.

Fraud groups using these private HTS platforms steal users' investment funds in various ways; for example, they may pretend that profits are being generated and then disappear when an investor requests a withdrawal. [3] In other cases, they lure investors into depositing funds and then steal the entire amount under the pretense of trading fees. [4] The unauthorized HTS platforms used in such scams are typically designed to be so similar to those provided by securities firms that they are nearly indistinguishable, in order to make users believe that legitimate trading is taking place. [5]

2. Past Attack Cases

Cases of malware distribution through unauthorized HTS programs have existed for some time. ASEC disclosed cases in 2023 and 2024 where an unauthorized HTS named “HPlus” distributed the Quasar RAT. [6] [7] Given that the company's name does not appear in search results or in the terms of service, it is presumed that victims installed the HPlus HTS through unlicensed or fraudulent financial investment firms, rather than through HTS provided by regulated financial institutions.



Figure 1. Private HTS Installed Alongside Malware

In this case, the “config.ini” file—used to configure the update server address—contained an FTP address where the malware was uploaded, and Quasar RAT was installed through this address. Quasar RAT is an open-source RAT malware that, in addition to basic remote control functions, provides keylogging and account information collection capabilities, enabling it to

steal information from the user environment and control the infected system in real time through remote desktop. Consequently, users who had installed HPlus HTS were at risk of having various personal details, including account information, stolen by threat actors at any time.

3. Recent Attack Cases

3.1. UBP Asset – Fraudulent Organization

In September 2025, a post titled “Warning: UBP Asset Fraud Site—Beware of the ub900[.]Org Impersonation Site” was uploaded to the blog of a law firm in Korea. [\[8\]](#) According to the post, the fraud ring impersonated the name and logo of the actual Swiss-based financial institution “Union Bancaire Privee (UBP),” and most victims were lured into registering on the site through Telegram or Band group chats. The scam operated by convincing victims to deposit money under the pretense of a legitimate investment; if victims refused requests for additional transfers, their access was blocked.

3.2. UBP Asset HTS

The HTS program that recently distributed ransomware features the same user interface as the UBP Asset HTS discussed above, and given that UBP-related strings are present in its version information, it appears to be the same HTS used in the scam case described above.

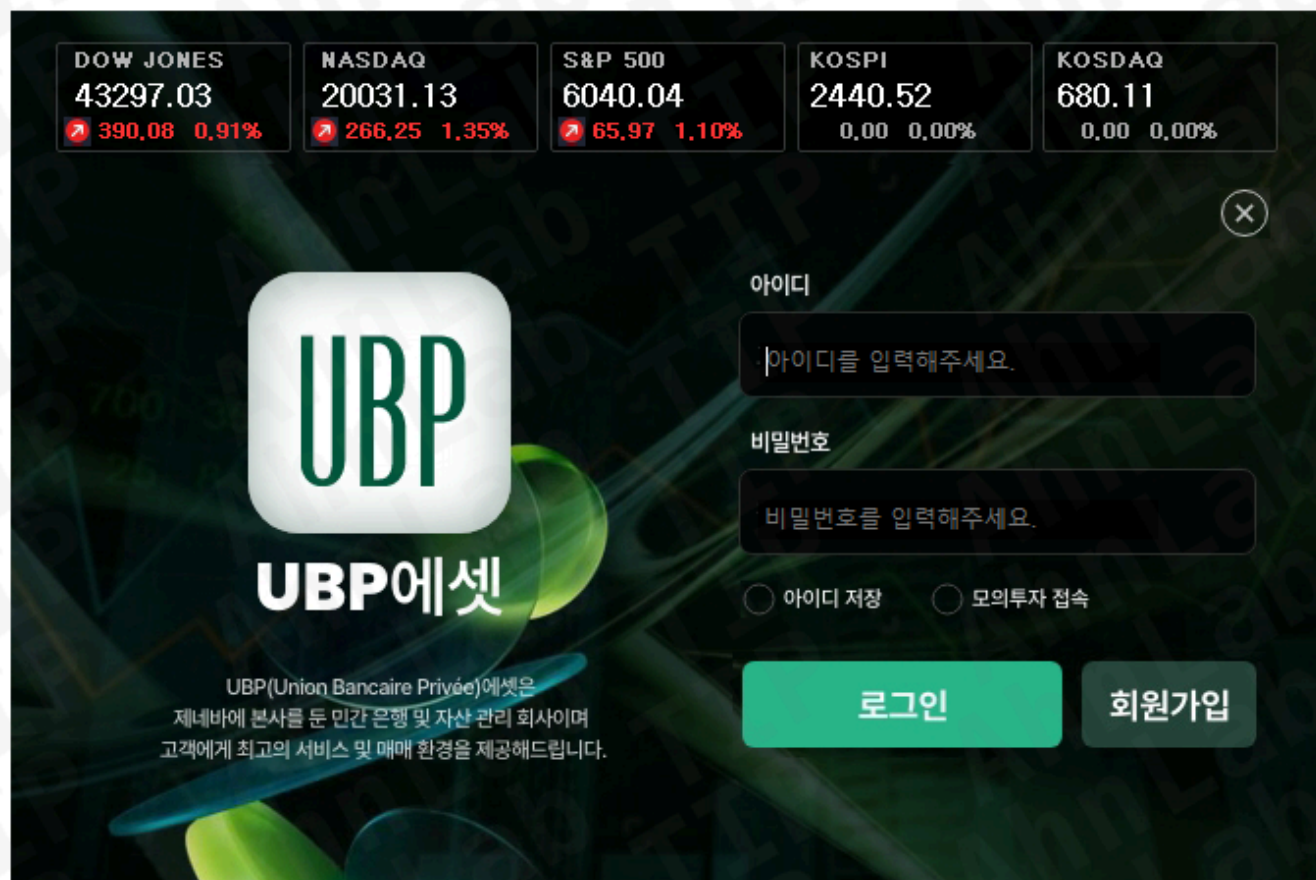


Figure 2. UBP Asset HTS Login Screen

UBP Asset HTS is typically installed in a folder named “UBP-Asset” in the root directory of the drive. When the shortcut on the desktop background is clicked, “UBPUpdater.Exe” runs, which in turn executes the “UBPPatch.Psh” file. Contrary to its file extension, the “UBPPatch.Psh” file is an executable that connects to the HTS update server and downloads “Update.Lst,” a configuration file containing the items to be updated. It then proceeds with the update based on the “Update.Lst” file; however, since the HTS update server is currently inaccessible, the contents of the configuration file are unknown.

PC > 로컬 디스크 (C:) > UBP-Asset					UBP-Asset 검색
이름	수정한 날짜	유형	크기		
WTS.dll	2024-12-18 오후 7:08	응용 프로그램 확장	193KB		
Update.lst	2026-09-12 오후 2:16	LST 파일	22KB		
unins000.exe	2026-09-12 오후 2:11	응용 프로그램	3,629KB		
unins000.dat	2026-09-12 오후 2:11	DAT 파일	41KB		
UBPUpdater.exe	2026-08-05 오후 1:54	응용 프로그램	4,475KB		
UBPPatch.psh	2026-09-08 오후 12:04	PSH 파일	4,483KB		
UBP.runtimeconfig.json	2026-02-27 오후 4:21	JSON 파일	1KB		
UBP.exe	2026-08-12 오후 1:02	응용 프로그램	183KB		
UBP.dll.config	2025-02-05 오후 3:39	CONFIG 파일	2KB		
UBP.dll	2026-08-12 오후 1:02	응용 프로그램 확장	5,514KB		
UBP.deps.json	2026-06-26 오전 11:06	JSON 파일	94KB		
TcpSharp.dll	2026-08-12 오후 12:59	응용 프로그램 확장	46KB		
System.Text.Json.dll	2024-09-17 오전 8:12	응용 프로그램 확장	568KB		
System.Text.Encodings.Web.dll	2023-11-01 오전 12:00	응용 프로그램 확장	70KB		

Figure 3. UBP Asset HTS Installation Folder

However, based on the ASD logs, it appears that “UBPPatch.Psh” downloaded “Update.Lst”—which contains settings for downloading ransomware—from the HTS server and then installed the ransomware “HTSPnew.Exe.”

Target Type	File Name	File Size	File Path ⓘ
Current	 htspnew.exe	2.09 MB	%SystemDrive%\ubp-asset\htspnew.exe
Parent	 ubp.exe	182.5 KB	%SystemDrive%\ubp-asset\ubp.exe
DropperOfCurrent	 ubppatch.psh	4.38 MB	%SystemDrive%\ubp-asset\ubppatch.psh

Process	Module	Target	Behavior	Data
 htspnew.exe	N/A	N/A	Decoy file deleted	N/A
 ubppatch.psh	N/A	 cmd.exe	Executes exploitable process	N/A
 ubp.exe	N/A	 htspnew.exe	Creates process	N/A
 htspnew.exe	N/A	N/A	Attempted to change decoy file extension	N/A

Figure 4. Ransomware installation behavior observed in the ASD log

For reference, “UBP.Exe” only loads “UBP.Dll” and executes the Main() function; the actual main functionality of HTS is contained within “UBP.Dll.” In recent attack cases, “UBP.Dll”

differs from previous variants in that it includes a command to execute the “HTSPnew.Exe” file —i.E., The ransomware—located on the same Path. In other words, the threat actor uploaded the ransomware to the HTS server, modified the configuration file, and appears to have also added functionality to “UBP.Dll” to execute the ransomware.

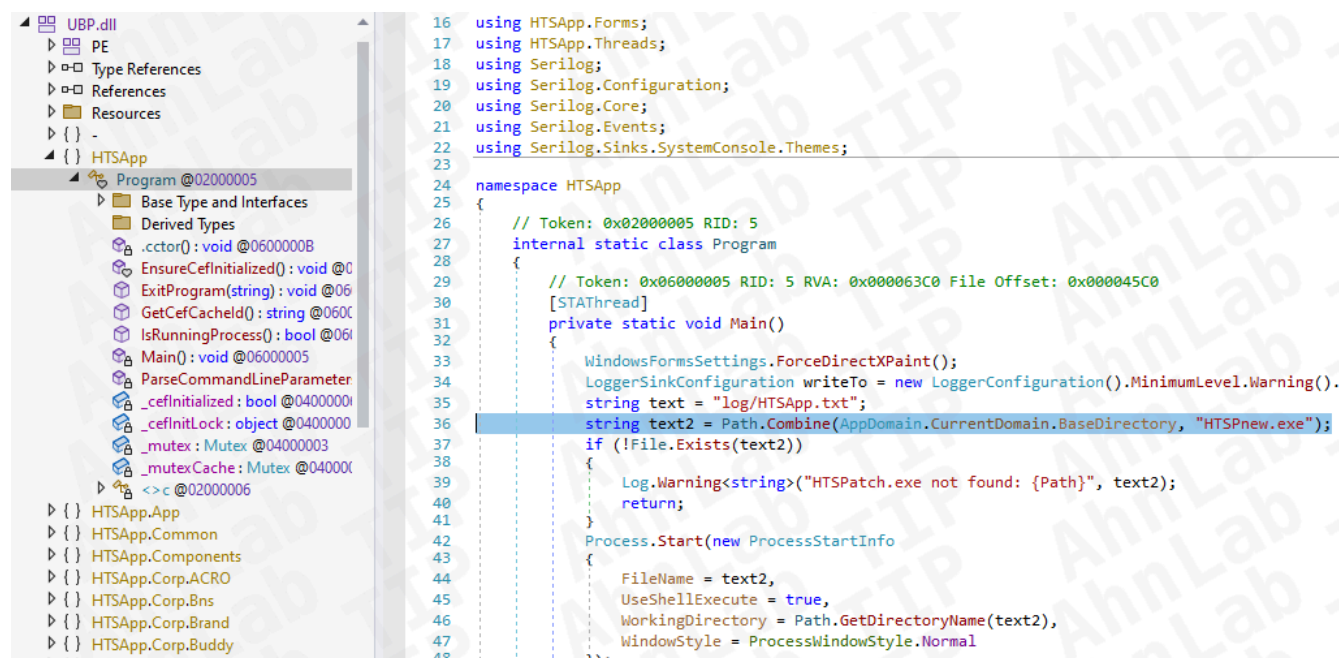


Figure 5. Routines added to the latest “UBP.Dll” file

3.3. KRSID Ransomware

The file “HTSPnew.Exe” used in the attack is ransomware written in the Rust programming language; based on the ransom note, it is presumed to have been created using AI. For classification purposes, we use the name “KRSID ransomware” based on its ransomware file extension.

Overview	Description
File Extension	.Krsid
Ransom note	README_KRSID.Txt
Encryption algorithm	AES-256 / RSA-2048
Folders Excluded from Encryption	Windows, program files, program files (x86), ProgramData, \$recycle.Bin, system volume information, \$winreagent, winre, boot, efi, recovery, windowsapps, accountpictures, node_modules, target, .Git, .Cargo, .Rustup, AppData
Encryption Extensions	Listed below
Threat Actor Information	Bratteam88 (Telegram)

Table 1. KRSID ransomware

When executed without parameters, the KRSID ransomware encrypts the entire drive. With the exception of folders excluded from file encryption and the ransom note file name “README_KRSID.Txt,” it performs file encryption using specified file extensions; however, depending on the command-line arguments, it may encrypt only files in specific paths or output a list of target files to a log instead of encrypting them. Additionally, unlike other ransomware strains, it is notable for not including a feature to delete volume shadow copies.

Arguments	Function
-Path	Specify the directory to encrypt
-Batch	Maximum number of files to process in a single batch
-Pause	Pause time between batches
-Dry-run	List the files to be subjected to file encryption in the log without actually performing file encryption on them
-H, -help	Output help to a log file

Table 2. Supported Arguments

The log file is saved as “ransomware-silent.Log” in the same Path, and a ransom note is created in the folder containing the files subject to file encryption. The ransom note is written in Korean as shown below and instructs the victim to contact the attackers through Telegram.

파일이 잠겼습니다! (!!! YOUR F1L3S H4V3 B33N 3NCRYPT3D !!!)

=====

안녕하세요!

이 컴퓨터의 파일은 암호화되어 잠긴 상태입니다.

걱정하지 마세요. 모든 데이터는 안전하게 보존되어 있으며,
아무것도 삭제되지 않았습니다. 파일이 잠겨 있을 뿐입니다!
시간 초과일시 파일삭제, 암시장에 유통될수도있습니다!

복구 방법 (How to recover):
잠긴 파일을 원래대로 복구혹은 왜 이렇게 됐는지 궁금하시면 아래 연락처로 연락해 주세요.

문의처 (Contact):

- 텔레그램 (Telegram): [@bratteam88]

지불 방법 (Payment):
비트코인(BTC) 또는 기타 암호화폐로 결제 가능합니다.

참고사항 (Note):
24시간 이내에 연락 주시면 할인된 가격으로 복구해 드립니다.
답변을 기다리겠습니다. 감사합니다!

[Info] 32880 file(s) encrypted · key fingerprint:

Figure 6. Ransom Note

Ransomware target file extensions: txt, md, log, json, xml, yml, yaml, toml, ini, cfg, conf, csv, html, htm, css, js, py, rs, go, c, cpp, h, java, sh, bat, ps1, sql, env, properties, config, rst, markdown, doc, docx, xls, xlsx, ppt, pptx, rtf, odt, ods, odp, epub, mobi, pdf, zip, RAR, 7z, png, jpg, jpeg, gif, bmp, tif, tiff, webp, svg, heic, ico, mp3, mp4, wav, flac, aac, ogg, m4a, mkv, avi, mov, wmv, webm, db, mdb, accdb, sqlite, sqlite3, dbf, frm, myd, myi, pem, key, crt, cer, bak, backup, old, orig, cs, ts, tsx, jsx, vue, kt, swift, dart, csproj, sln, scss, less, dockerfile, makefile, php, aspx, jsp, asp, cshtml, vb, vbs, rb, pl, lua, r, m, scala, hs, ml, ex, erl, clj, groovy, gradle, coffee, mjs, cjs, pug, twig, ejs, hbs, psd1, psm1, eml, msg, psd, ai, dwg, dxf

4. Conclusion

Threat actors previously used private HTS platforms as a means to siphon off victims' investment funds, but recently they have been using them to install malware on victims' computers. Consequently, while victims in the past simply failed to recover their investment funds, they are now faced with files on their systems being encrypted by ransomware and being demanded to pay a ransom for recovery. Given the nature of the threat actors' fraudulent schemes using HTS, it is unclear whether actual recovery is even possible, even if the ransom is paid.

According to the Financial Supervisory Service, "Legitimate financial institutions do not distribute private HTS software through messaging apps or similar channels." [9] Users should install HTS provided by regulated financial institutions through their official websites. In addition, they should take care to patch installed software to the latest version to prevent attacks exploiting vulnerabilities and update V3 to the latest version to block Malware infections in advance.

MD5

6d2cd65dbd0df30404b08ff007359e54

a9cce44c4d42b07f114dd2b340f0046a

f86b2ece324cfd36e832a3b48cc3719b

URL

https[:]//phf-ubp[.]com/UBPA/_hts_tv/user

FQDN