

랜섬웨어를 유포하는 사설 HTS 프로그램

A asec.ahnlab.com/ko/95464

ATCP

September 18, 2026



AhnLab SEcurity intelligence Center(ASEC)은 최근 사설 홈트레이딩시스템(HTS : Home Trading System)을 통해 랜섬웨어가 유포된 사례를 확인하였다. 랜섬웨어 유포에 사용된 HTS 프로그램은 “UBP 에셋”이라는 이름이며 과거부터 온라인 투자 사기에 악용되어 왔다. 2025년 9월 공개된 국내 법무법인의 블로그 포스팅에서도 동일한 HTS 사진이 확인되는 것을 보면 투자 사기 조직이 최근에는 피해자들을 대상으로 랜섬웨어를 유포한 것으로 보인다.

1. 사설 HTS (Home Trading System)

홈트레이딩시스템(HTS)은 투자자가 주식을 사고팔기 위해 증권사 객장에 나가거나 전화를 거는 대신 집이나 사무실에 설치된 PC를 통해 거래할 수 있는 시스템을 말한다. [1] 일반적으로 과거와 달리 요즘은 대부분의 개인들이 주식이나 펀드, 선물과 같은 금융 상품을 거래할 때 핸드폰이나 PC에 HTS를 설치하여 온라인으로 거래하고 있다.

대부분의 경우 사용자들은 거래하는 제도권 금융회사들이 제공하는 HTS를 설치하고 해당 업체를 통해 금융 거래를 진행한다. 하지만 최근에는 불법 금융 투자 업체들이 합법적인 금융회사로 가장해 사설 HTS를 설치하도록 유도한 뒤 투자금을 가로채는 사건이 다수 발생하고 있다.

대부분의 무인가 금융 투자 업체들은 인터넷 광고나 문자 메시지 광고를 통해 사용자들을 속인 후 카카오톡과 같은 SNS 단체 대화방으로 가입을 유도한다. 일반적으로 소액의 증거금만으로

해외 선물 거래가 가능하다는 점이나 수수료 면제, 대출과 같은 광고를 사용하는 것으로 알려져 있다. [2] 단체 대화방의 운영자는 이렇게 모집한 사용자들에게 자체 제작한 사설 HTS를 설치하고 투자금을 입금하도록 유도한다.

사설 HTS를 이용하는 사기 집단들은 다양한 방식으로 사용자들의 투자금을 가로채는데, 예를 들어 수익이 발생하는 것처럼 속이고 투자자가 출금 요구 시 잠적하는 경우가 있다. [3] 또는 투자자가 예치금을 넣도록 유인한 후 예치금 전액을 거래 수수료 명목으로 가로채는 경우도 존재한다. [4] 이러한 사기 행위에 사용되는 사설 HTS들은 사용자로 하여금 정상적인 거래가 발생하고 있는 것처럼 인식시키기 위해 증권사들이 제공하는 HTS와 구분하기 힘들 정도로 유사하게 제작하는 것이 특징이다. [5]

2. 과거 유사 공격 사례

사설 HTS 프로그램을 통해 악성코드를 유포하는 사례는 과거부터 존재해 왔다. ASEC은 2023년과 2024년에 HPlus라는 이름의 사설 HTS가 Quasar RAT을 유포한 사례를 공개하였다. [6] [7] 검색이나 약관에서 업체의 이름이 확인되지 않는 것을 보면 피해자들은 제도권 금융 회사에서 제공하는 HTS가 아닌 무인가 또는 위장 금융 투자 업체를 통해 HPlus HTS를 설치한 것으로 추정된다.



Figure 1. 악성코드와 함께 설치된 사설 HTS

해당 사례에서 업데이트 서버 주소를 설정하는 “config.ini” 파일에 악성코드가 업로드된 FTP 주소가 존재하였으며 이를 통해 Quasar RAT이 설치되었다. Quasar RAT은 오픈 소스 RAT 악성 코드로서 기본적인 원격 제어 기능 외에도 키로깅, 계정 정보 수집 기능들을 제공하여 사용자 환경의 정보를 탈취할 수 있고, 원격 데스크탑을 통해 실시간으로 감염 시스템을 제어할 수 있다. 이에 따라 HPlus HTS를 설치한 사용자들은 공격자에 의해 언제든지 계정 정보를 포함한 다양한 개인 정보들을 탈취당할 수 있었다.

3. 최신 공격 사례

3.1. UBP 에셋 – 사기 조직

2025년 9월 국내 모 법무법인의 블로그에 “UBP에셋 사기 사이트 ub900[.]org 사칭 사이트 피해 주의”라는 이름의 포스팅이 업로드되었다. [8] 해당 포스팅에 따르면 해당 사기 조직은 실제 스위스 기반의 금융기관 “Union Bancaire Privée(UBP)”의 이름과 로고를 사칭하였으며 대부분 텔레그램 리딩방이나 밴드방에서 사이트 가입을 유도당했다고 한다. 피해자들은 실제 투자로 생각해 돈을 입금하지만 추가 송금 요구를 거절하면 접속을 차단하는 방식으로 사기 행각을 벌였다.

3.2. UBP 에셋 HTS

최근 랜섬웨어를 유포한 HTS 프로그램은 위에서 다룬 UBP 에셋 HTS와 동일한 UI를 지원하며 버전 정보에도 UBP 관련 문자열들이 존재하는 것을 보면 위의 사기 사례에서 사용된 HTS로 보인다.

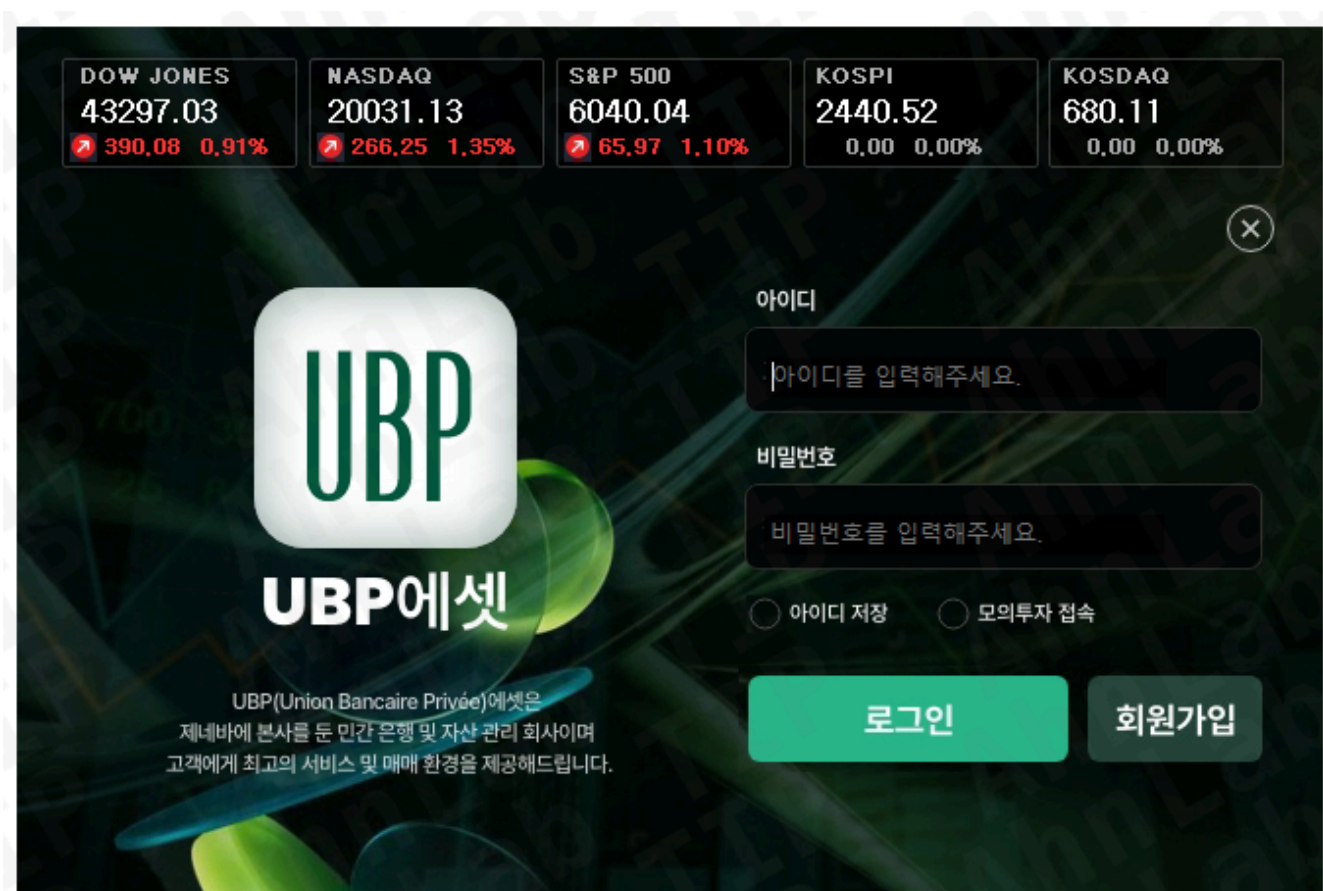


Figure 2. UBP 에셋 HTS 로그인 화면

UBP 에셋 HTS는 기본적으로 드라이브의 루트 경로에 “UBP-Asset”이라는 폴더에 설치된다. 바탕화면에 설치된 바로가기 파일을 실행할 경우 “UBPUpdater.exe”가 실행되며 이는

“UBPPatch.psh” 파일을 실행한다. “UBPPatch.psh” 파일은 확장자와 달리 실행 파일로서 HTS 업데이트 서버에 접속해 업데이트 대상이 포함된 설정 파일인 “Update.lst”를 다운로드한다. 이후 “Update.lst” 파일을 참고해 업데이트를 진행하는데 현재 HTS 업데이트 서버에 접속이 불가해 설정 파일의 내용은 알 수 없다.

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 에셋 HTS 설치 폴더

하지만 ASD 로그를 보면 “UBPPatch.psh”는 HTS 서버로부터 랜섬웨어 다운로드 설정이 포함된 “Update.lst”를 다운로드한 후 랜섬웨어 “HTSPnew.exe”를 설치한 것으로 보인다.

Target Type	File Name	File Size	File Path ⓘ
Current	 httpnew.exe	2.09 MB	%SystemDrive%\ubp-asset\httpnew.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
 httpnew.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	 httpnew.exe	Creates process	N/A
 httpnew.exe	N/A	N/A	Attempted to change decoy file extension	N/A

Figure 4. ASD 로그에서 확인되는 랜섬웨어 설치 행위

참고로 “UBP.exe”는 “UBP.dll”을 로드하고 Main() 함수를 실행하는 행위만 수행하며 실질적인 HTS의 메인 기능은 “UBP.dll”에 포함되어 있다. 최근 공격 사례에서 “UBP.dll”은 과거 유형과 달리 차이점이 존재하는데 동일 경로에 위치한 “HTSPnew.exe” 파일을 즉 랜섬웨어를 실행하는 명령이 추가되어 있다는 점이다. 즉 공격자는 HTS 서버에 랜섬웨어를 업로드하고 설정 파일을 수정하였으며 이외에도 “UBP.dll”에도 랜섬웨어를 실행하는 기능을 추가한 것으로 보인다.

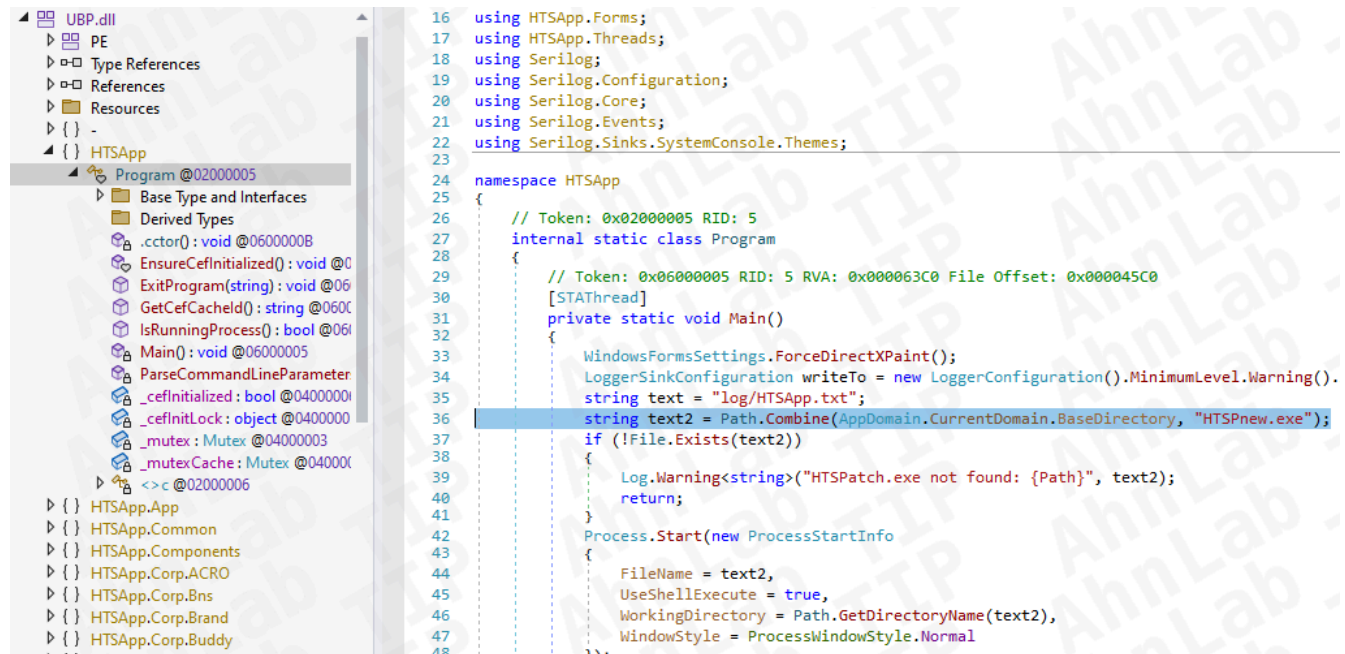


Figure 5. 최신 UBP.dll 파일에 추가된 루틴

3.3. KRSID 랜섬웨어

공격에 사용된 파일 “HTSPnew.exe”는 랜섬웨어로서 Rust 언어로 제작되었으며 랜섬노트를 보면 AI를 활용해 제작한 것으로 추정된다. 여기에서는 분류를 위해 랜섬웨어 확장자를 기반으로 KRSID 랜섬웨어라는 이름을 사용한다.

개요

설명

확장자	.krsid
랜섬노트	README_KRSID.txt
암호화 알고리즘	AES-256 / RSA-2048
암호화 제외 폴더	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
암호화 대상 확장자	아래 항목에서 정리
공격자 정보	텔레그램 사용

Table 1. KRSID 랜섬웨어

KRSID 랜섬웨어는 인자 없이 실행될 경우 전체 드라이브를 대상으로 암호화를 수행한다. 암호화 제외 폴더 및 랜섬노트 파일 이름 “README_KRSID.txt”를 제외하면 지정된 확장자의 파일들을 암호화하는데 인자에 따라 특정 경로의 파일들만 암호화하거나 암호화 대신 대상 파일들의 목록을 로그에 출력하기도 한다. 이외에도 다른 랜섬웨어들과 달리 볼륨 웨도우 복사본을 지우는 기능을 포함하지 않는 것이 특징이다.

인자

기능

-path	암호화 디렉터리 지정
-batch	한 배치에서 처리할 최대 파일 수
-pause	배치 사이 대기 시간
-dry-run	암호화하지 않고 암호화 대상 파일들을 로그에 기록
-h, -help	도움말을 로그 파일로 출력

Table 2. 지원하는 인자

로그 파일은 동일 경로에 생성되는 “ransomware-silent.log”에 저장되며 파일 암호화 대상 폴더에는 랜섬노트가 생성된다. 랜섬노트는 다음과 같이 한글이 사용되었으며 텔레그램을 통해 연락하도록 설명한다.

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): [@██████████]

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. 랜섬노트

랜섬웨어 대상 확장자 : 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. 결론

공격자는 과거 피해자들의 투자금을 가로채는 수단으로서 사설 HTS를 사용하였지만, 최근에는 피해자 PC에 악성코드를 설치하는 용도로 사용하고 있다. 이에 따라 피해자들은 과거에는 단순히 투자금을 돌려받지 못하는 것에 그쳤다면 이제는 랜섬웨어에 의해 시스템 내의 파일들이 암호화되어 복구를 위해 금전을 요구받는다. 해당 공격자의 HTS를 이용한 사기 행각을 보면 비용을 지불한다고 하더라도 실제 복구가 가능할지 알 수 없다.

금융감독원에 따르면 “제도권 금융회사라면 메신저 등을 통해 사설 HTS를 배포하지 않는다”고 한다. [9] 사용자들은 공식 홈페이지를 통해 제도권 금융회사들이 제공하는 HTS를 설치하여야 한다. 이외에도 설치된 소프트웨어를 최신 버전으로 패치하여 취약점 공격을 사전에 방지하고 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

MD5

6d2cd65dbd0df30404b08ff007359e54

a9cce44c4d42b07f114dd2b340f0046a

f86b2ece324cfd36e832a3b48cc3719b

URL

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

FQDN