



Operation MIDAS

Tracking Fraudulent Financial Program Organizations

Financial Security Institute

Sung-Wook Jang
Yong-Hyun Kim (@copy_and_paster)

→ **Sung-Wook, Jang** : Senior, Financial Security Institute(FSI)

- ◆ 6 years of CTI, DFIR, Malware analysis

→ **Yong-Hyun, Kim** : Principal, Financial Security Institute(FSI)

- ◆ 8 years of SOC & CTI & DFIR, 4 years of DAST SW Developer
- ◆ Past presentations
 - FS-ISAC 2023 APAC : Building CTI Service from 2B NIDS events over 8 years
 - ISCR 2019(KNPA) - Fight Against Cybercrime : GANDCRAB Threat Groups

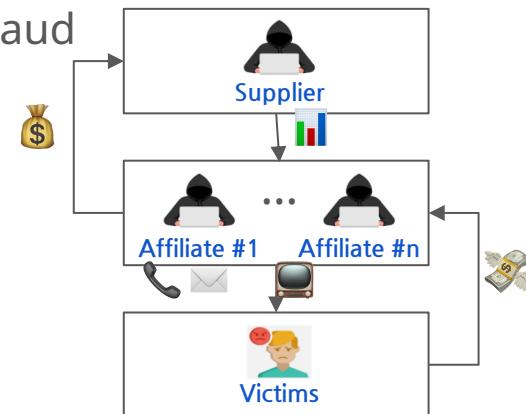
Background

→ Fake Trading System Scam

- ◆ A Cybercrime that impersonates an investment professional to trick and defraud people into using a fake trading system*
* HTS(Home Trading System), MTS(Mobile Trading System)
- ◆ In Korea, there are many cases that impersonates existing financial companies

→ Terms in this presentation

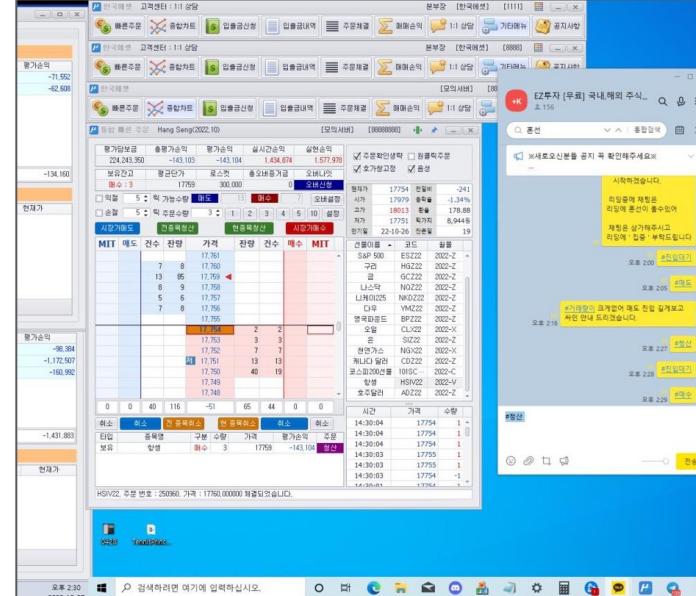
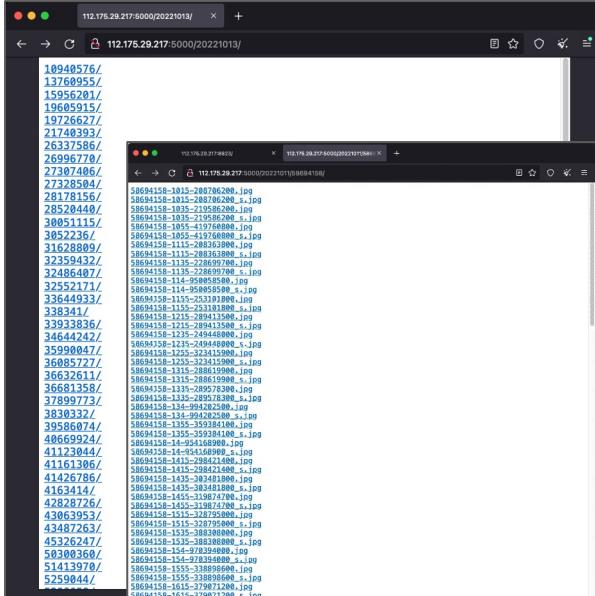
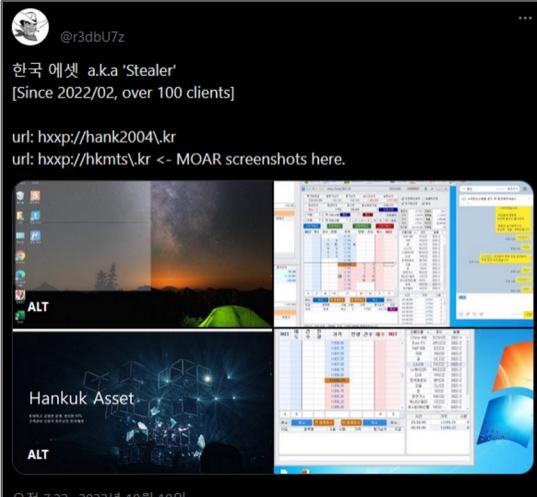
- ◆ Supplier : An organization that develops and distributes fake HTS
- ◆ Affiliate : An organization that uses fake HTS to commit fraud
(there are several groups)
- ◆ 3rd party service : Legitimate & Not Legitimate Services
(e.g, Youtube, Money Launderers, Messenger Service, ...)



Initial Findings(1/2)

→ Monitoring social media threat information

- ◆ A tweet found about fake HTS threat information on Twitter (@r3dbU7z, '22.10)
 - ◆ a lot of screenshot files were being exposed from a specific port
 - not only were victims being exposed, but also screenshots of the criminals!



* <https://x.com/r3dbU7z/status/1579235837833011201>

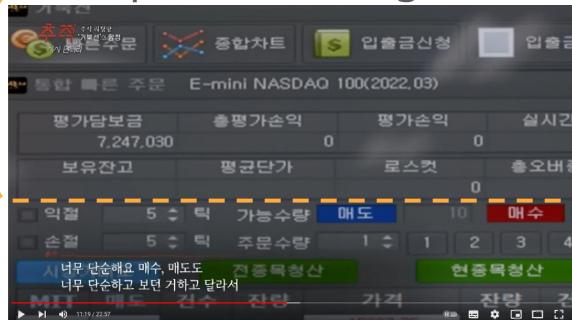
Information Classification: General

Initial Findings(2/2)

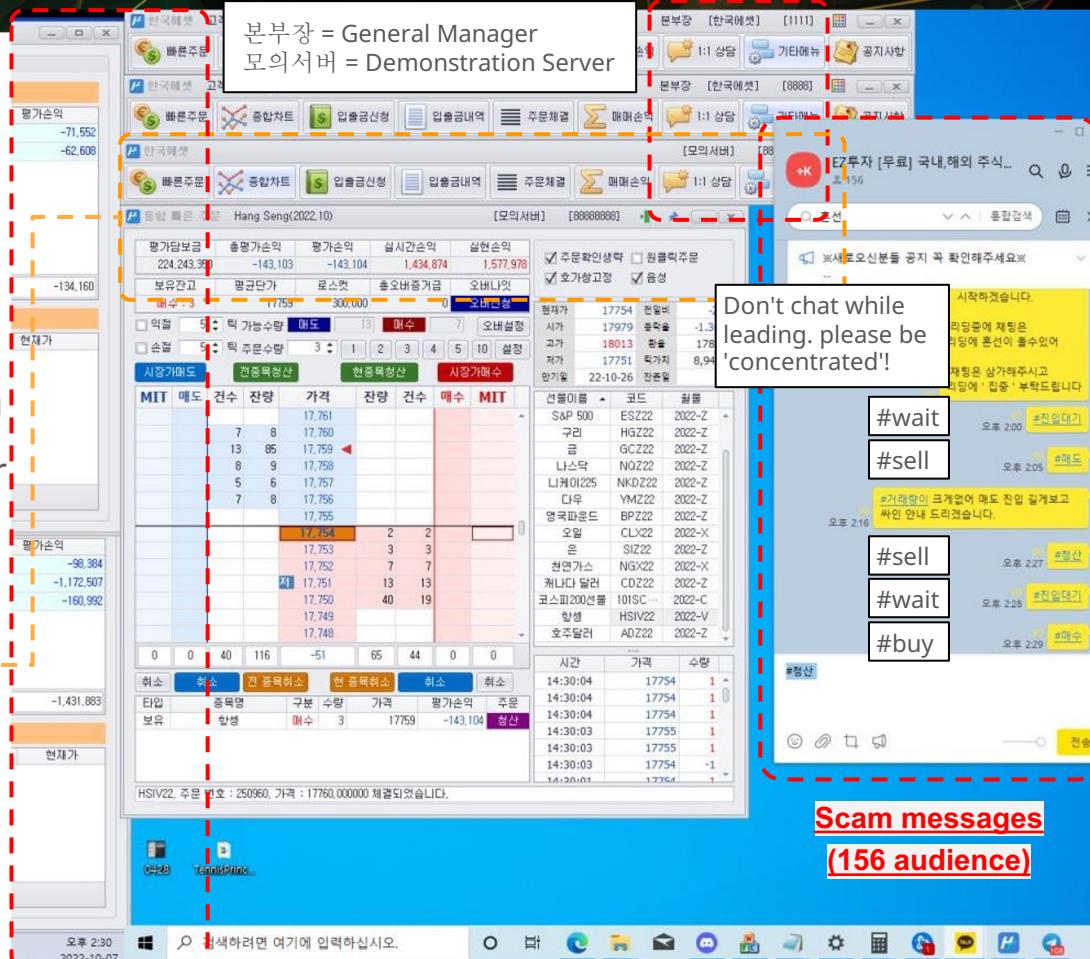
→ Victims? or Criminals?

- ◆ Title bar on Trading SW
 - 'General Manager' keyword
 - Multiple Execution of HTS
- ◆ Scam messages in chat room
 - sent from current computer

◆ Suspicious Management SW



* <https://www.youtube.com/watch?v=Zhnf9CNVb-A>



A screenshot of a Korean trading software interface. A red dashed box highlights the title bar and the top menu area. A white box with black text overlays the top right of the interface, stating "본부장 = General Manager" and "모의서버 = Demonstration Server". Another white box on the right side of the interface contains the text "Don't chat while leading. please be 'concentrated!'". A blue dashed box highlights a separate window titled "#chat" which lists several scam messages. The text in the "#chat" window includes:

- #wait
- #sell
- #sell
- #wait
- #buy
- #정산

Scam messages (156 audience)

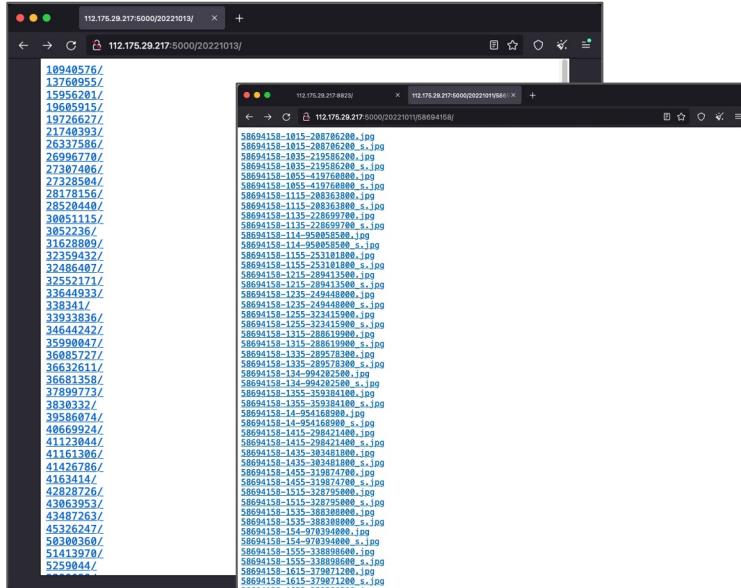
OPSEC Failures

1. Leaked screenshots by directory indexing
2. Lack of device isolation
3. Insecure software development process

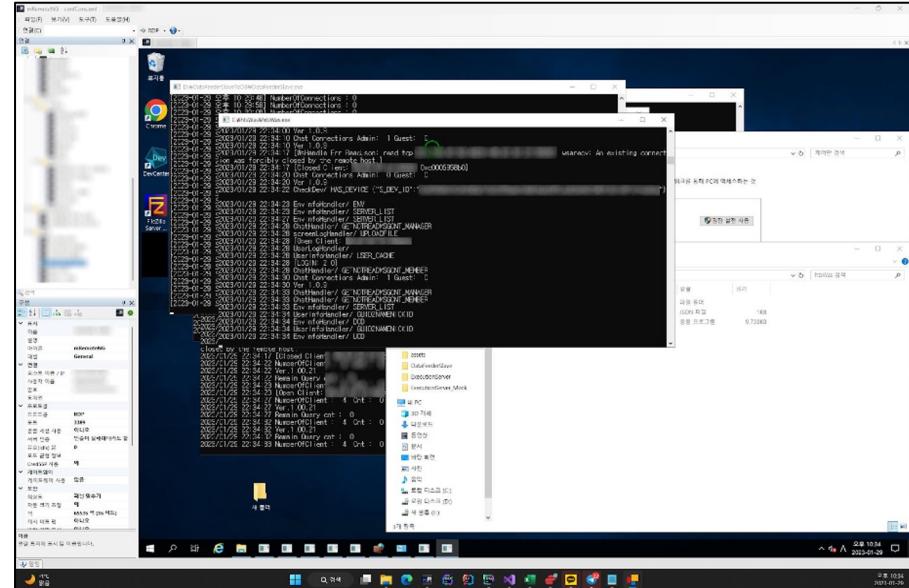
#1 : Leaked screenshots by directory indexing

→ Leaked Screenshots by directory listing, including developer's screenshot

- ◆ Most of them were screenshots of the victim, but a few were of the supplier.
- /YYYYMMDD/{USER_NUMBER}/{USER_NUMBER}-YYYYMMDD-{RANDOM}.jpg



Directory Listing page



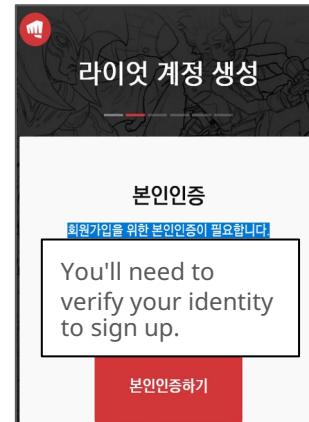
Server management using mRemoteNG
(Supplier's screenshot)

#BHEU @BlackHatEvents

#2 : Lack of device isolation(1/2)

→ No separation between crime / personal device

- ◆ Not only the victims' screens were recorded, but also the criminals' screens



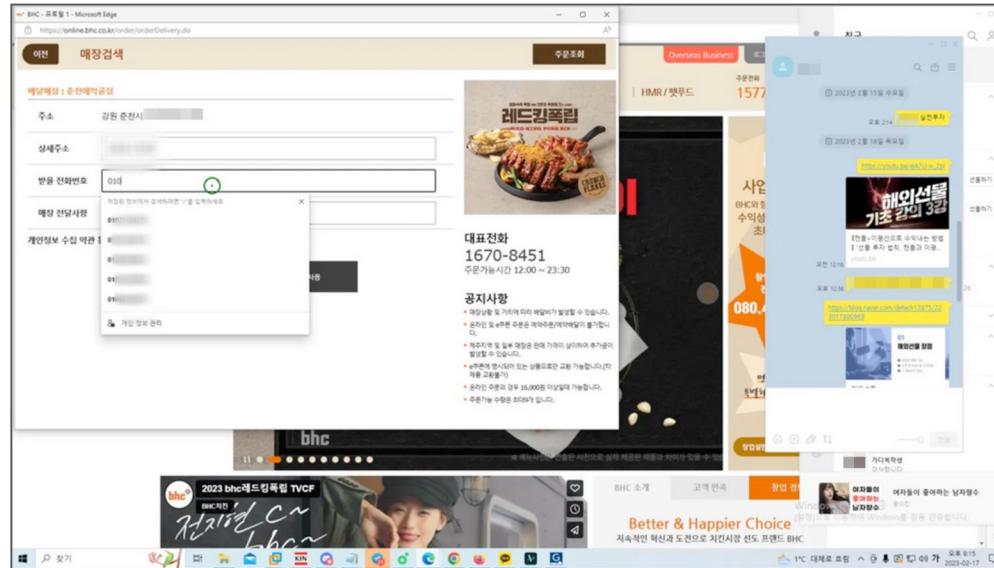
Identity verification Process

(HMAC-SHA Hashed value using SSN with Password)
wEi9oYSuekQGxT9MV4rKHG4CO+Zrp+onhLlIuembl8jx/0PLF5Ne3oM
BxvUFIN4UmsgjeNERZfmpCVUFHsv8nq==...

#2 : Lack of device isolation(2/2)

→ No separation between crime / personal device

- ◆ Not only the victims' screens were recorded, but also the criminals' screens



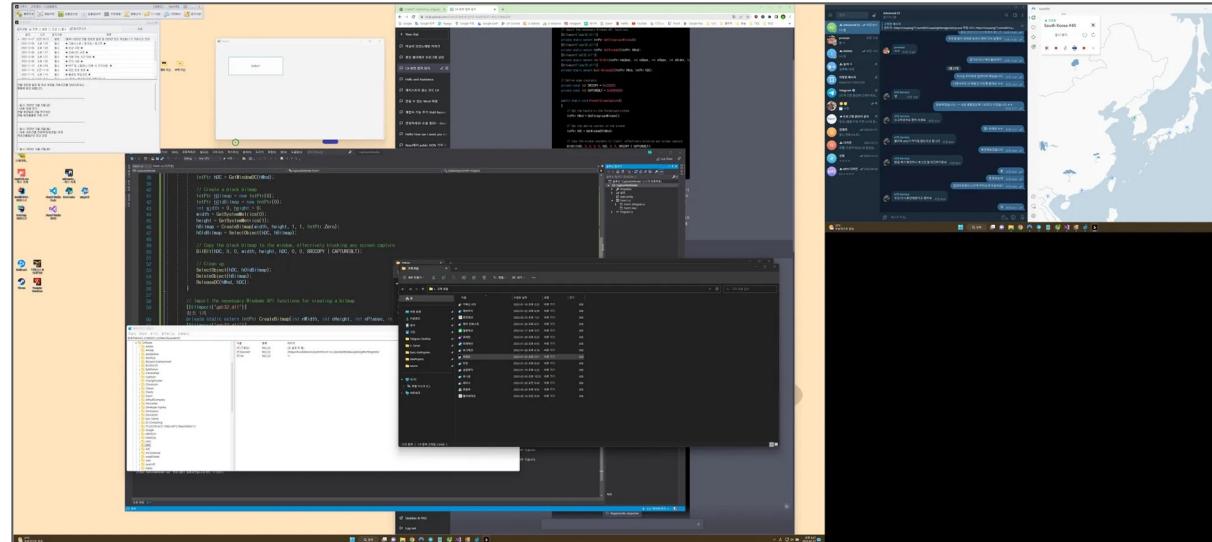
Location exposure in food delivery ordering



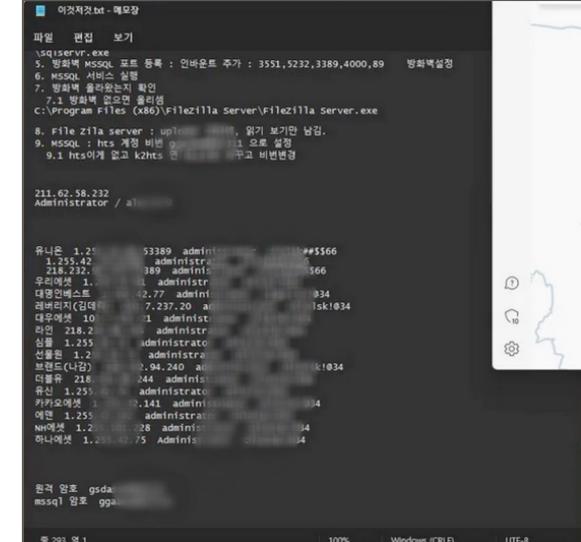
Identified car license plate, face of affiliate members by wallpaper

#3 : Insecure software development process(1/2)

→ Insecure software development and testing



Screenshot of Supplier uploaded during development



RDP/RDBMS credentials

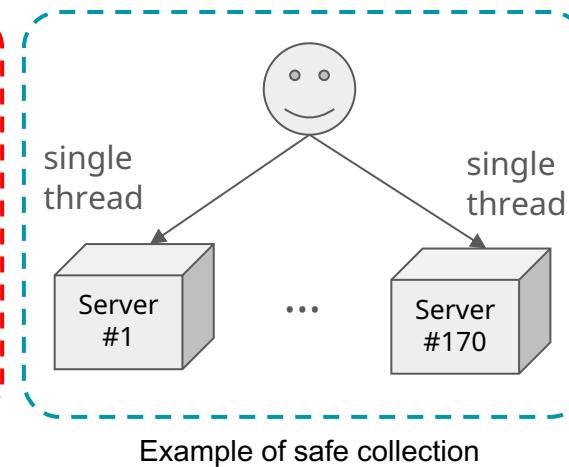
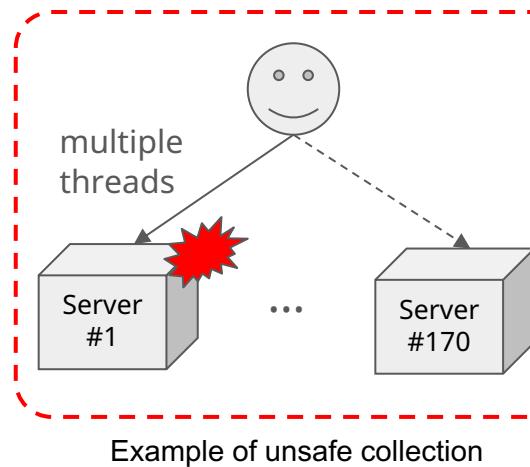
Tracking Criminals

1. Screenshot Collection & Triage
2. Deep-dive analysis of screenshots
3. Correlation analysis of infrastructure

Collection & Triage of Screenshots(1/2)

→ Collection of Screenshots

- ◆ Automatically collect screenshots from fake HTS servers
 - Collect each server as a separate process & single thread to minimizing server load
- ◆ Analytics identified 170+ fake HTS servers, collected 24/7 for nearly 2 months
 - Collected 12 TB of screenshots(Total 2.7million files, 200GB per day)



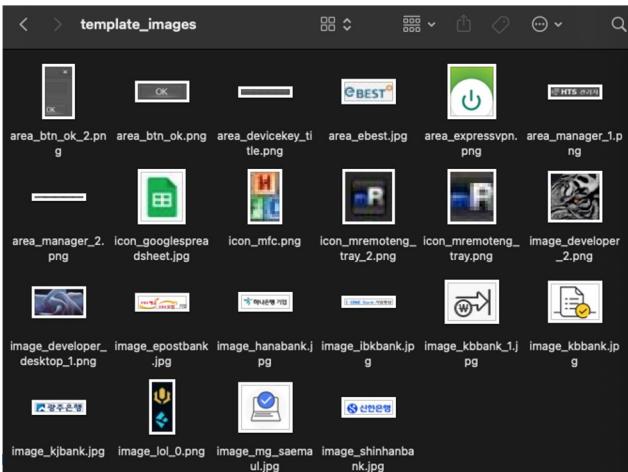
Collection & Triage of Screenshots(2/2)

→ Triage for 12TB of screenshot files

- ◆ High-profile screenshot triage using template matching script
 - Development Tools(VSCode, Jetbrains IDE, ...), VPN(ExpressVPN...), Mirroid
- ◆ Skip analyzing victim screenshots with user numbering patterns
 - 0 & n < 0 : Supplier(Boss / Fake HTS Developer / Helpdesk, ...) / Affiliates
 - n > 1000 : Victims



Template Matching



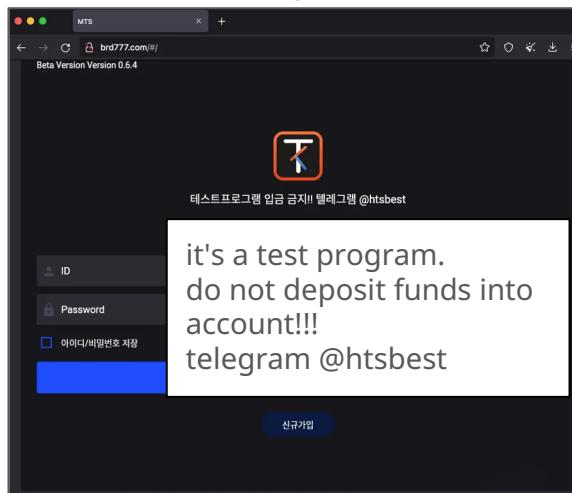
```

2023-05-31 01:22:20.905 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-91739-175179800.jpg, threshold : 0.900000
2023-05-31 01:22:20.905 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-165704-26669800.jpg, threshold : 0.900000
2023-05-31 01:22:20.905 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-2001-220217-801057300.jpg, threshold : 0.900000
2023-05-31 01:22:20.905 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1001-84810-380164500.jpg, threshold : 0.900000
2023-05-31 01:22:20.906 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1002-231832-232277300.jpg, threshold : 0.900000
2023-05-31 01:22:20.906 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1010-231117-574096300.jpg, threshold : 0.900000
2023-05-31 01:22:22.362 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-1000-165704-26669800.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:22.370 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-2000-55045-852308800.jpg, threshold : 0.900000
2023-05-31 01:22:23.634 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-1000-123700-157216700.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:23.635 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-223456-23119900.jpg, threshold : 0.900000
2023-05-31 01:22:23.712 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-1010-231117-574096300.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:23.712 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-122145-852308800.jpg, threshold : 0.900000
2023-05-31 01:22:24.974 | INFO | __main__:_match_templates:81 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-2000-55045-406036300.jpg', 'threshold': 0.9, 'matched_templates': ['../../template_images/icon_mfc.png'], 'is_matched': True}
2023-05-31 01:22:24.982 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1010-205429-260390800.jpg, threshold : 0.900000
2023-05-31 01:22:26.063 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-100-4624-427701800.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:26.063 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-101530-235919100.jpg, threshold : 0.900000
2023-05-31 01:22:26.134 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-1011-101553-799674700.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:26.135 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-1000-11712-278800100.jpg, threshold : 0.900000
2023-05-31 01:22:26.300 | DEBUG | __main__:_match_templates:84 - {'target_path': '../../Desktop/turtleship_admins/FTP_DOWN/-1000-223456-23119900.jpg', 'threshold': 0.9, 'matched_templates': [], 'is_matched': False}
2023-05-31 01:22:26.301 | DEBUG | __main__:_match_templates:63 - target image : ../../Desktop/turtleship_admins/FTP_DOWN/-223-111221-939129000.jpg, threshold : 0.900000
frost@frostui-MacBookPro ~ %

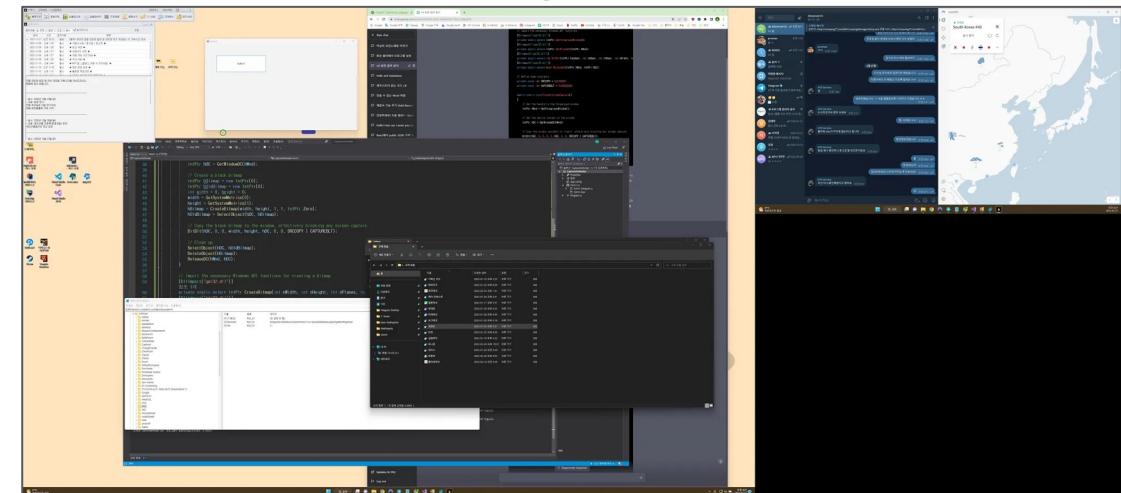
```

→ Development environment of Supplier(Developer)

- ◆ Typically, Supplier test their new feature using a publicly accessible testing server
- ◆ We have identified valuable information, including the supplier's identity, development environment, and infrastructure through their screenshots



Testing & Preview Server of Supplier



Development environment of Supplier
(C#, Jetbrains IDEs, ChatGPT, NordVPN, ...)

Deep-dive analysis of screenshots(2/2)

→ Technical stacks of suppliers

Port	Purpose	Protocol	SW
21	Update of the fake HTS and the administrator program (before May 2023)	FTP	- Filezilla Server
80	Fake MTS website port	HTTP	- IIS
89	Distribution of a fake HTS installation program	HTTP	- IIS
2127	Update of the fake HTS and the administrator program (after May 2023)	FTP	- Filezilla Server
3389	Remote control for server maintenance	RDP	- Windows RDP
4000	Expression of price information by means of TradingView	HTTP	- IIS - TradingView Chart Library
4423	REST API communication for running the HTS/ MTS (backend server)	HTTP	- Presumed to have been developed on its own
12323	Price lookup	HTTP (WebSocket)	- Presumed to have been developed on its own
12324	Price lookup assistance	HTTP (WebSocket)	- Presumed to have been developed on its own

FTP 2127/TCP

11/25/2024 17:48 UTC

[VIEW ALL DATA](#)

FILE SHARING

Software

- Filezilla-Project FileZilla Server *
- Microsoft Windows

Details

Banner 220-FileZilla Server 1.9.3
220 Please visit https://filezilla-project.org/

Auth TLS Response 234 Using authentication type TLS.

Status Code 220

Status Meaning Service ready for new user.

TLS

Handshake

Version Selected TLSv1_3

Cipher Selected TLS_CHACHA20_POLY1305_SHA256

Certificate

Fingerprint 0a3de7e18ed26d7b845ab51bb54976b0445c1b5eae3206c447d9858991f3e86a

Subject CN=filezilla-server self signed certificate

Issuer CN=filezilla-server self signed certificate

→ Find another Fake HTS Server using Intelligence Services

- ◆ Use Censys Search to search for hosts with the same Software + same port criteria

Installer Deployment Port

```
services.software.product='FileZilla Server' and
(services.port:4000 and services.port:2127 and services.port:80 and services.port:89)
```

TradingView Chart Port	Automatic Update Port	MTS Web Page	Installer Deployment Port
---------------------------	-----------------------	--------------	---------------------------

FTP 2127/TCP

FILE SHARING

Software

- Filezilla-Project FileZilla Server *
- Microsoft Windows *

Details

Banner: 229-FileZilla Server 1.9.3
229 Please visit https://filezilla-project.org/
Auth TLS Response: 234 Using authentication type TLS.

Status Code: 220
Status Meaning: Service ready for new user.

TLS

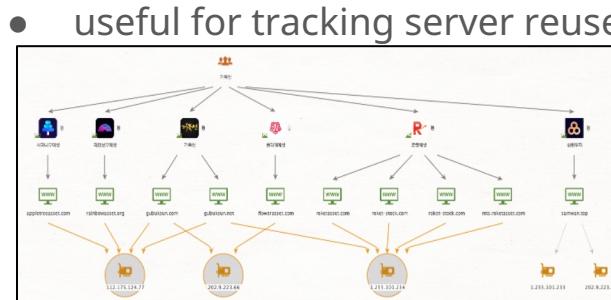
Handshake

Version Selected: TLSv1.3
Cipher Selected: TLS_CHACHA20_POLY1305_SHA256

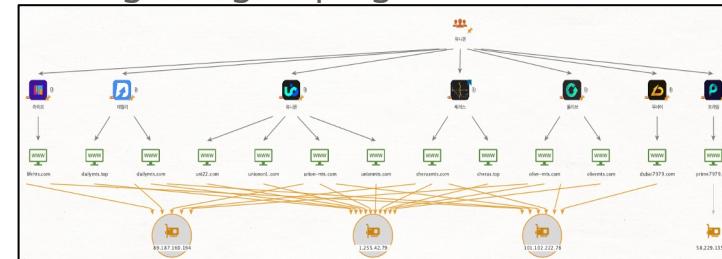
Certificate

Fingerprint: 0a3de7e18ed26d7b845ab51bb54976b8445c1b5eae3296c447d9858991f3ee86a
Subject: CN=filezilla-server self signed certificate
Issuer: CN=filezilla-server self signed certificate

- ◆ Track & Analyze Passive DNS History using Virustotal



'Turtleship' Affiliate Group

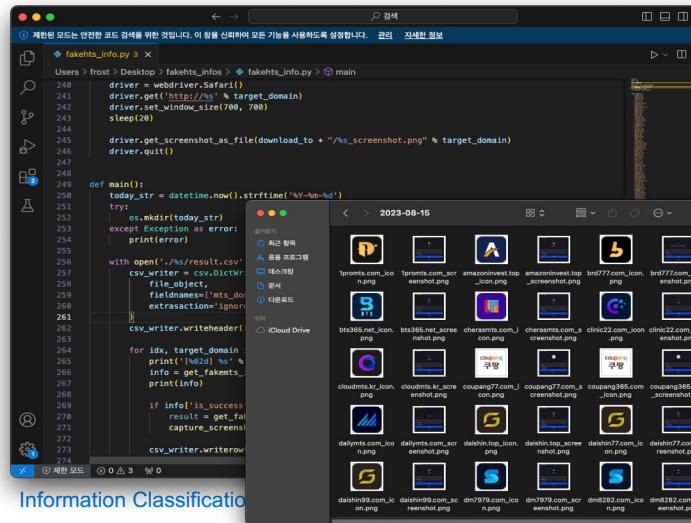


'Union' Affiliate Group

#BHEU @BlackHatEvents

→ Tracking known(and newly registered) domains and IP address of backend

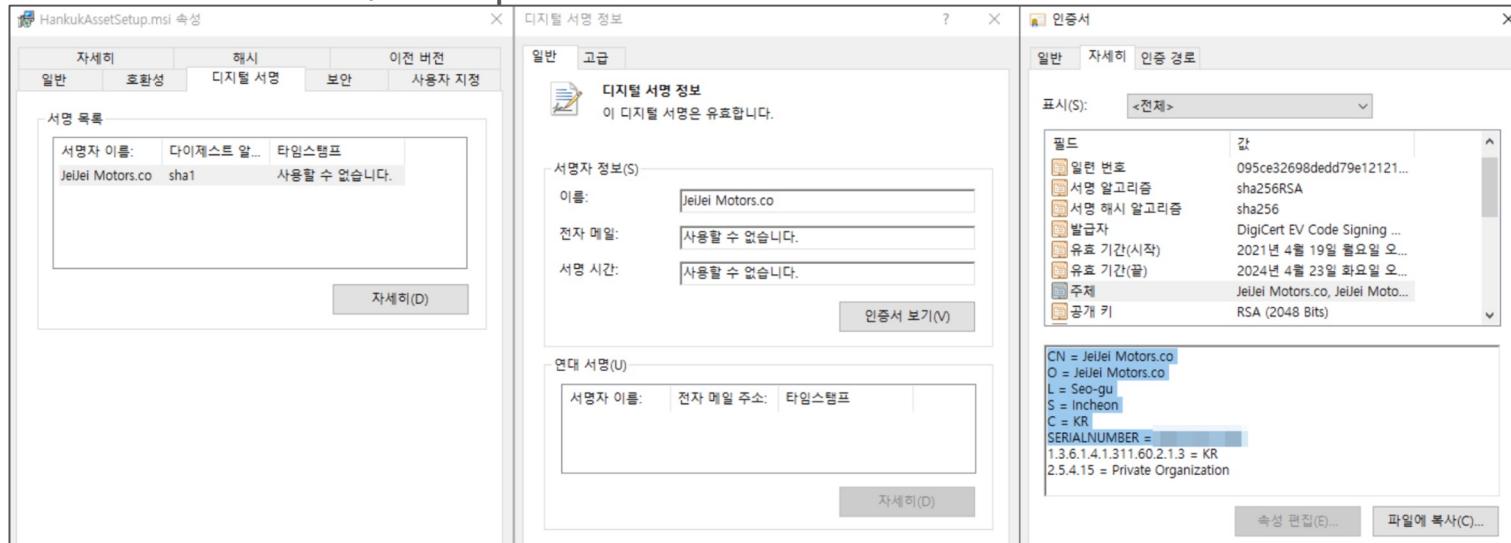
- ◆ Fake HTS are constantly being created, renamed, and shut down (dormant)
- ◆ We have monitored activation of Fake HTS domain, Screenshots, Icons, Backend IP
- ◆ Sometimes, Supplier forgot to apply Cloudflare CDN and leaks real IP address



N	O	P	Q	R
http://101.102.223.81:4423/	http://101.102.223.81:4423/	http://metainvest7.com:4423/	http://metainvest7.com:4423/	http://metainvest7.com:4423/
http://103.102.221.16:4423/	http://101.102.221.16:4423/			http://103.97.209.210:4423/
http://mtsspace.net:4423/	http://mtsspace.net:4423/	http://mtsspace.net:4423/	http://mtsspace.net:4423/	http://mtsspace.net:4423/
http://101.110.5.93:4423/	http://101.110.5.93:4423/	http://101.110.5.93:4423/	http://101.110.5.93:4423/	http://101.110.5.93:4423/
http://olive-mts.com:4423/	http://olive-mts.com:4423/	http://olive-mts.com:4423/	http://olive-mts.com:4423/	http://olive-mts.com:4423/
http://101.102.222.13:4423/	http://101.102.222.13:4423/	http://orangenmts.com:4423/	http://orangenmts.com:4423/	http://orangenmts.com:4423/
http://plus8282.com:4423/	http://plus8282.com:4423/	http://plus8282.com:4423/	http://plus8282.com:4423/	http://plus8282.com:4423/
http://prime7979.com:4423/	http://prime7979.com:4423/	http://prime7979.com:4423/	http://prime7979.com:4423/	http://prime7979.com:4423/
http://101.102.221.21:4423/	http://101.102.221.21:4423/			
http://researnts.com:4423/	http://researnts.com:4423/	http://researnts.com:4423/	http://researnts.com:4423/	http://researnts.com:4423/
http://202.9.223.69:4423/	http://202.9.223.69:4423/	http://202.9.223.69:4423/	http://202.9.223.69:4423/	http://202.9.223.69:4423/
http://rich7979.com:4423/	http://rich7979.com:4423/	http://rich7979.com:4423/	http://rich7979.com:4423/	http://rich7979.com:4423/
http://101.102.221.16:4423/	http://101.102.221.16:4423/	http://roketasset.com:4423/	http://roketasset.com:4423/	http://roketasset.com:4423/
		http://roketasset.com:4423/	http://roketasset.com:4423/	http://roketasset.com:4423/

→ Business License Number from Codesign Certificate

- ◆ License number can be identified from the code sign certificate
- ◆ Use code sign certificates issued in the name of an auto parts company, architecture firm, or IT parts vendor



→ Lack of applying Domain Privacy Protection Service

- ◆ Some domains are not protected by domain privacy protection services
- ◆ It was useful in identifying potential helpers(or supplier) for this campaign

Index	Domain	Source	Status	Domain Status
99	timeasset.net	whois.namesilo.com	Succeed	Registered
100	timeasset.top	whois.namesilo.com	Succeed	Registered
89	smileasset.top	whois.namesilo.com	Succeed	Registered
90	smilemts.com	whois.namesilo.com	Succeed	Registered
91	smw66.com	whois.namesilo.com	Succeed	Registered
128	globaltrading7.com	whois.godaddy.com	Succeed	Registered
42	aoldmts.com	whois.namesilo.com	Succeed	Registered

<

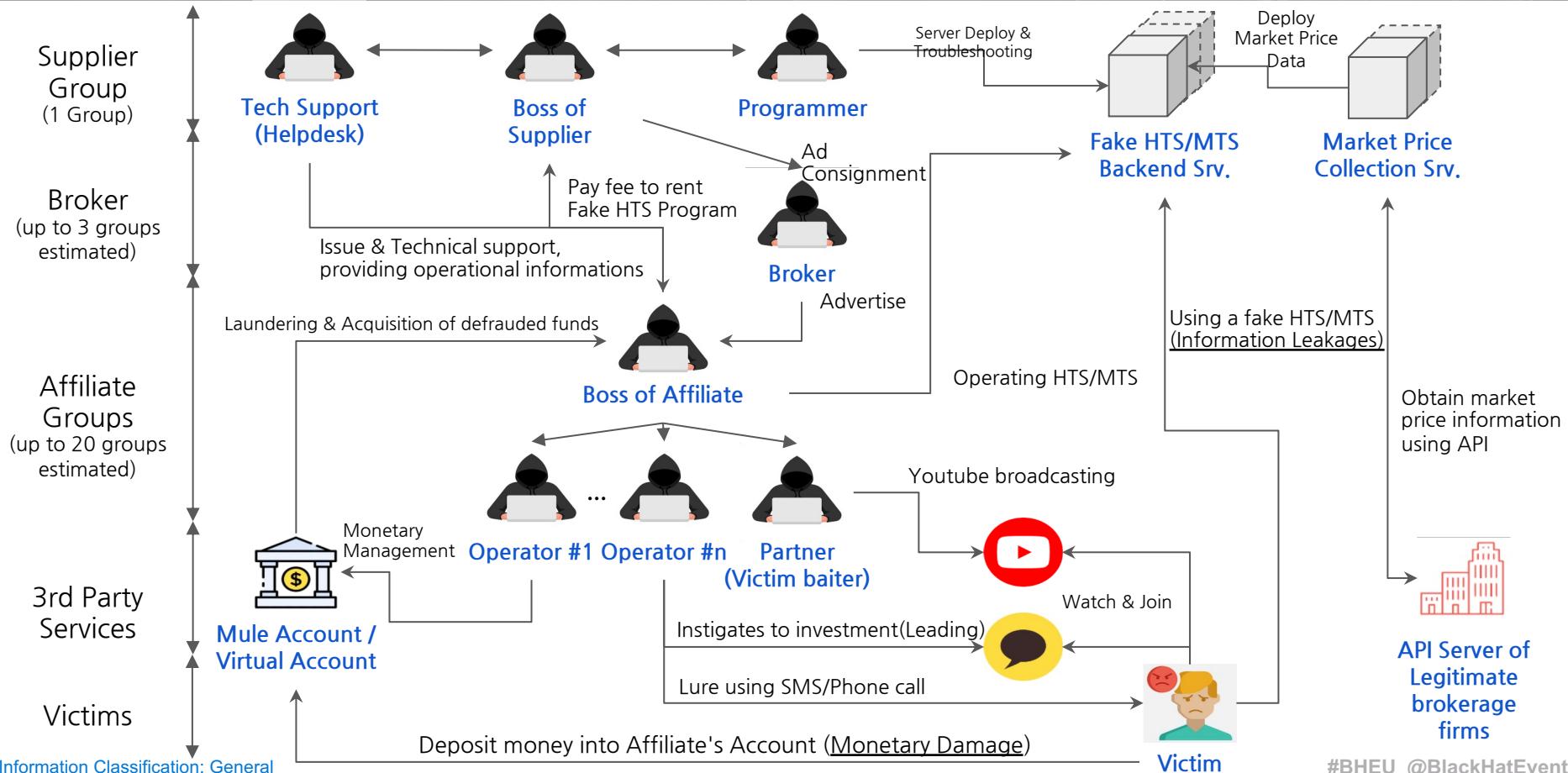
Registrant Name: Jong*** Kim	Registrant Organization: j***** motors	Registrant Street: ***-5-*** 13, *****-ro ***beon-gil, ***-gu, Incheon	Registrant City: ***-gu
Registrant State/Province: Incheon	Registrant Postal Code: 22***	Registrant Country: KR	Registrant Phone: +82.1048***13
Registrant Phone Ext:	Registrant Fax:	Registrant Fax Ext:	Registrant Email: htzman@protonmail.com

d-brg[.]com	smilemts[.]com	smileasset[.]top	benest[.]top
Registrant Name: Jong*** Kim			
Registrant Organization: j***** motors			
Registrant Street: ***-5-*** 13, *****-ro ***beon-gil, ***-gu, Incheon			
Registrant City: ***-gu			
Registrant State/Province: Incheon			
Registrant Postal Code: 22***			
Registrant Country: KR			
Registrant Phone: +82.1048***13			
Registrant Phone Ext:			
Registrant Fax:			
Registrant Fax Ext:			
Registrant Email: htzman@protonmail.com			

Analyze fraud schemes

1. Fake HTS Scam Process Overview
2. Schemes of Supplier
3. Schemes of Affiliate

Process overview



[Supplier] Building Infrastructure(1/2)

→ Uses Co-location Server in South Korea & Japan

- ◆ To collect market price information with low-latency, they uses nearest datacenter
- ◆ After the KNPA arrests some affiliate, supplier moved their servers to japan('2023.5)
(2023-05) KNPA arrests an affiliate group

가짜 HTS로 리딩방 운영한 일당 검거…피해 규모
3천억원 추산(종합)

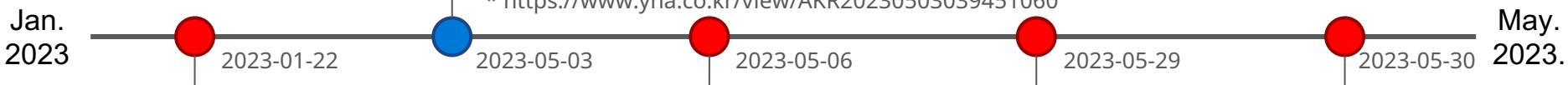
송고시간 | 2023-05-03 11:41

| 해외에 거점…총책 등 13명 구속·해외도피 2명 추적
고령자·주부 수백만~10억 원 투자…범인들 외제차에 고급 클럽서 파티

* <https://www.yonhapnews.co.kr/view/AKR20230503039451060>

Arrest of a worker who operated a leading room with fake HTS... Damage estimated at 300 billion won*

* 200 million dollars



 1.255.42.79

AS9318(SK Broadband Co Ltd)

 172.65.221.109

AS13335(CLOUDFLARENED)
(Cloudflare CDN)

 89.187.160.194

AS60068(Datacamp Limited)

 101.102.222.78

AS17676(SoftBank Corp.)

Passive DNS History of Fake HTS Domain 'unionmts[.]com'

#BHEU @BlackHatEvents

[Supplier] Building Infrastructure(2/2)

→ Advertise their fake HTS softwares using internet forums and websites

Home > 코인 > 홍보 및 소개

홍보 해외선물 HTS 본사 직영 HTS 임대 및 개발 2022-01-05 00:32:19

hts임대 Foreign Futures HTS Headquarters Direct HTS Leasing and Development

해외선물 HTS, MTS 임대

문의 텔레그램 @htsman

1. 증권사 HTS 개발팀 직영
2. 최신개발팀 활용한 빠르고 버그 없는 시스템.
3. 버그 없으며 고객이나 관리자나 사용하기 편리한 UI.
4. 최신 트렌드 UI 및 트레이딩뷰 차트 적용.
5. 24시간 실시간 응대및 예로 사항 즉시 해결.
6. 해외선물, 주식, 코인 거래 시스템 구축
7. 네트워크 전문가 보유. 디도스 클린존 보호가능.
8. 빠른서버구축 및 운영준비(3~5일 완료)
성실하고 신의있는 팀과 이제 함께 하십시오.

문의 텔레그램 @htsman

Foreign Futures HTS, MTS Leasing
Contact Telegram @htsman

1. Directly under the HTS development team of a securities company
2. Fast and bug-free system utilizing the latest development tools
[...snip...]

https://web.archive.org/web/20221204084046/https://www.htsrent.com/ 22 Feb 2023

해외선물 HTS 임대
해외선물 HTS 임대

- 국내선물, 해외선물 HTS 임대...
- 증권사 HTS 개발팀 적용...
- 최신개발팀을 적용한 빠르고 버그 없는 시스템...
- 실 고객들 불안없고 사용하기 편리한 UI...
- 편리하고 일관 고객관리 및 관리자 UI...
- 최신 트렌드 UI 및 트레이딩뷰 차트 적용...
- 블록 조회 및 차단...
- 24시간 실시간 응대및 예로 사항 즉시 해결...
- 국내선물, 해외선물거래 시스템 구축(차트, MTS 가능)
- 네트워크 전문가 보유. 디도스 100% 차단(최대 20기)
- 빠른서버구축 운영준비(3~5일 완료). 긴급(당일구축)
- 월별관리 웨드리리 허브지원 교육해드립니다...
- 거래내역, 패턴분석, 예상분석 해드립니다...
- 이제 성실하고 신의있는 팀과 이제 함께 하십시오...



서비스



깔끔한UI
사용자들이 계속 이용하고 싶은 UI
1:1화면



최신 트렌드
트레이딩뷰차트 적용. MTS 가능



관리자페이지
쉽고 편리한 고객관리 UI
불량고객차단 및 패션페이지



가상계좌 서비스
가상계좌 전문업체 안내

[Affiliates] Lure victims using 3rd party platform(1/3)

→ Management scam team to operate fake trading system campaign

- ◆ Pay a fee to obtain the fake hts usage rights : 7,500,000 KRW(\$5,300) / Month

	A	money laundering fee	Fake HTS Rental fee (\$5,300/M)	Virtual Account fee	Blog(advertisement) fee DB(phone number list) fee SMS(Text message) fee	Meal allowance (\$2,600/M)
1	날짜	틀림	HTS 비용	가상계좌비용	블로그비용	디비
2	1일		109,600			
3	2일		96,000			
4	3일		224,000	7,500,000		
5	4일		136,000			
6	5일		16,000			
	총					3,720,000

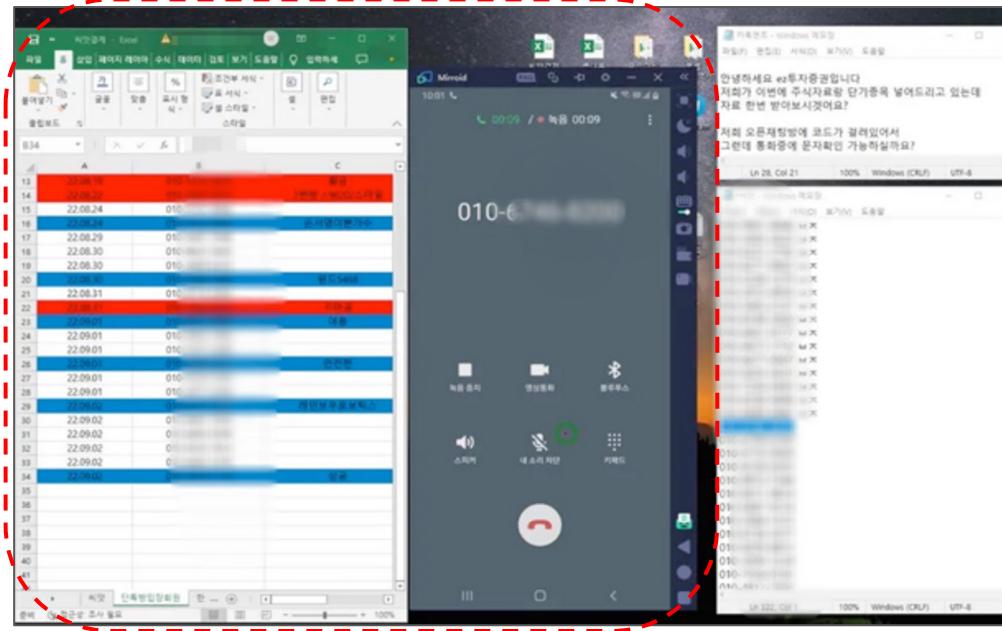
Ledger of affiliate from screenshot

[Affiliates] Lure victims using 3rd party platform(2/3)

→ Lure victims to use fake HTS through text messages, calls and YouTube

- ◆ (Spam Call & Text) Purchase a list of phone numbers list(DB) and send random calls or text message

DB(Phone number list)
and advertising using
phone calls



[Advertisement Script]
Hello, we are 'EZ securities'
I'd like to put in some stock
informations and some
short-term stuff.
Would you like to take a
look at it?

Record the call recipient's
reaction
'남자' = missed

[Affiliates] Lure victims using 3rd party platform(3/3)

→ Lure victims to use fake HTS through text messages, calls and YouTube

◆ (Youtube) Some affiliates take over ownership of Youtube accounts with a large number of subscribers and utilize them for advertising purposes



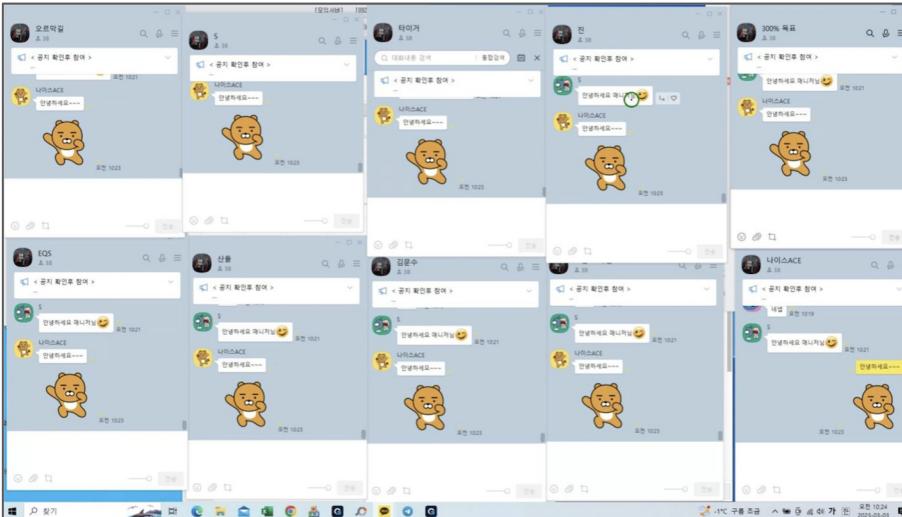
Gaps in YouTube video uploads and changes in topic

YouTube Broadcast to Lure Investors

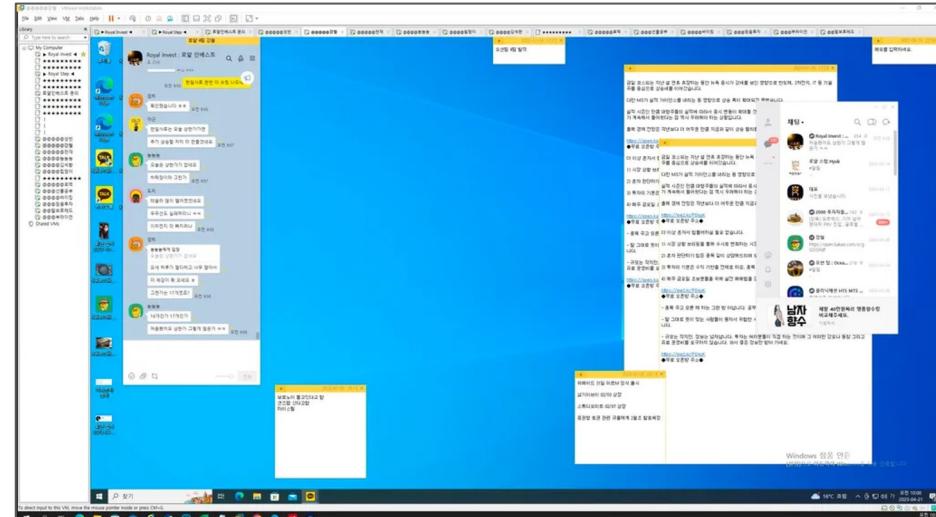
[Affiliates] Theft of money from victims(1/2)

→ Leading through one-man-show deception to avoid suspicion

- ◆ To multiple execution, Affiliate uses a various methods
 - (Patch based) V5 Multiloader
 - (Sandbox / Virtual Machines) Sandboxie, VMware workstation, ...



multiple execution using 'V5 Multiloader'

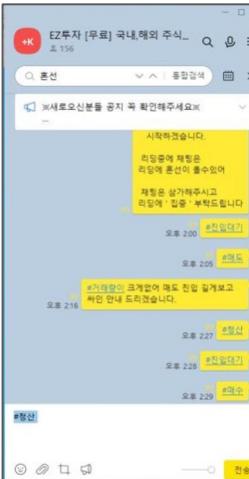


multiple execution using 'VMware Workstation'

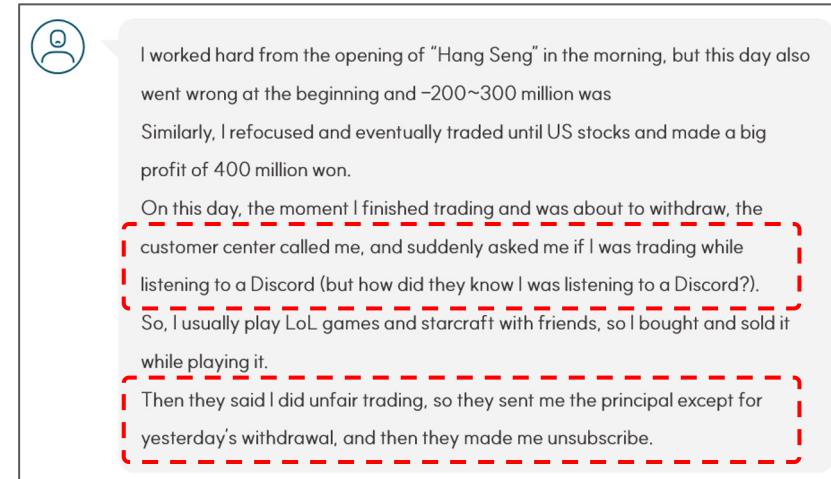
[Affiliates] Theft of money from victims(2/2)

→ Two methods to money theft tricks

- ◆ Basically, affiliates do sending the wrong signals to victims, leading to losses
- ◆ Ban the victim for reasons that don't make sense to them
- ◆ Needless to say, the money deposited by the victim is not returned and becomes the property of the affiliate



Send wrong signals(order hints) to victims



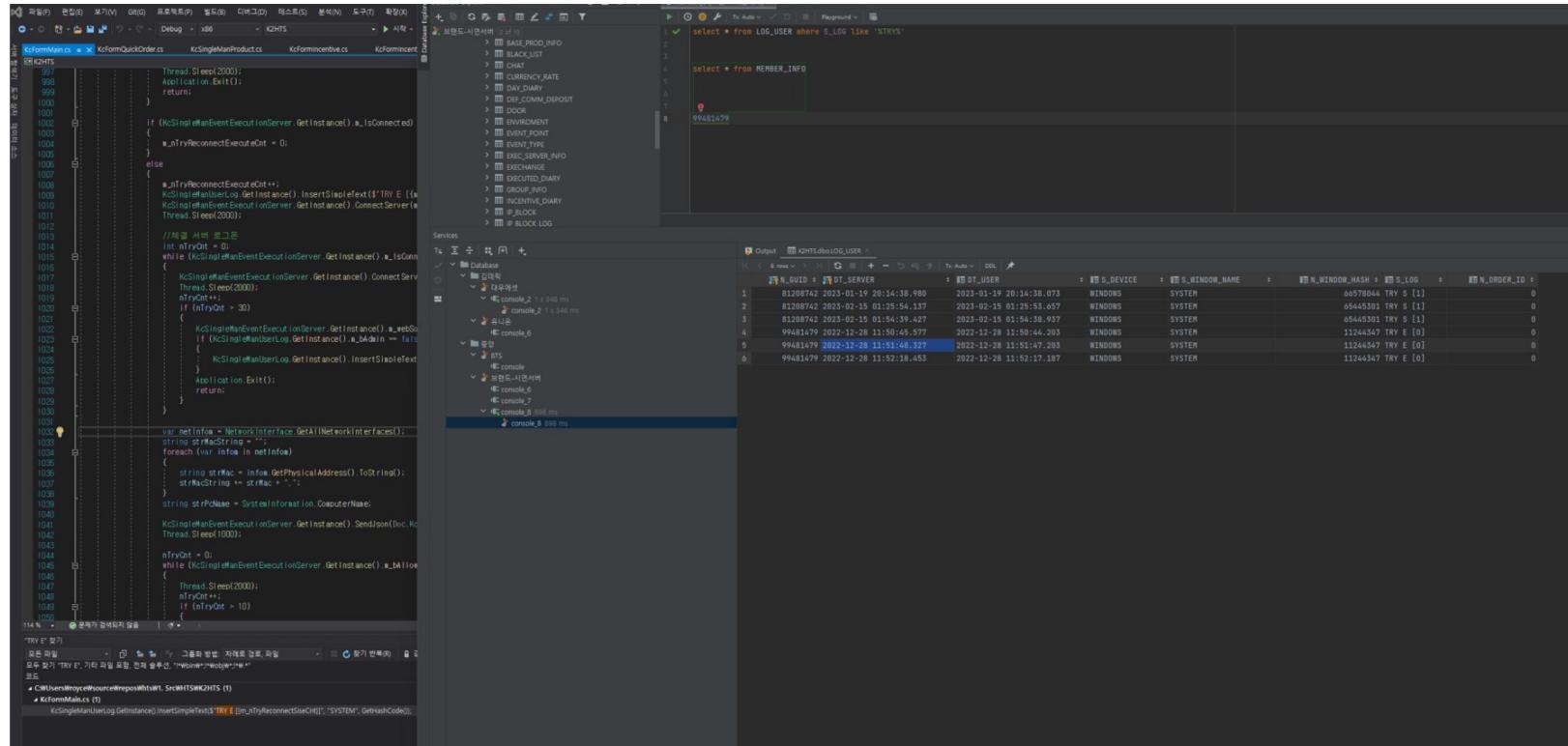
Surveillance of users and banning with unconvincing excuses

Fake HTS Program Analysis

1. Identify threats
2. Program analysis
3. Malicious behavior analysis

Identify threats

→ Lots of screenshot data, including developers and infrastructure operators



The screenshot displays a developer's environment with multiple windows open:

- Code Editor:** Shows C# code for a Windows service named KHTS. The code includes logic for connecting to an event server, handling log entries, and performing network interface scans.
- Terminal:** Shows command-line output related to the service's configuration and logs.
- Database Query:** A screenshot of a database query tool showing two SQL queries:

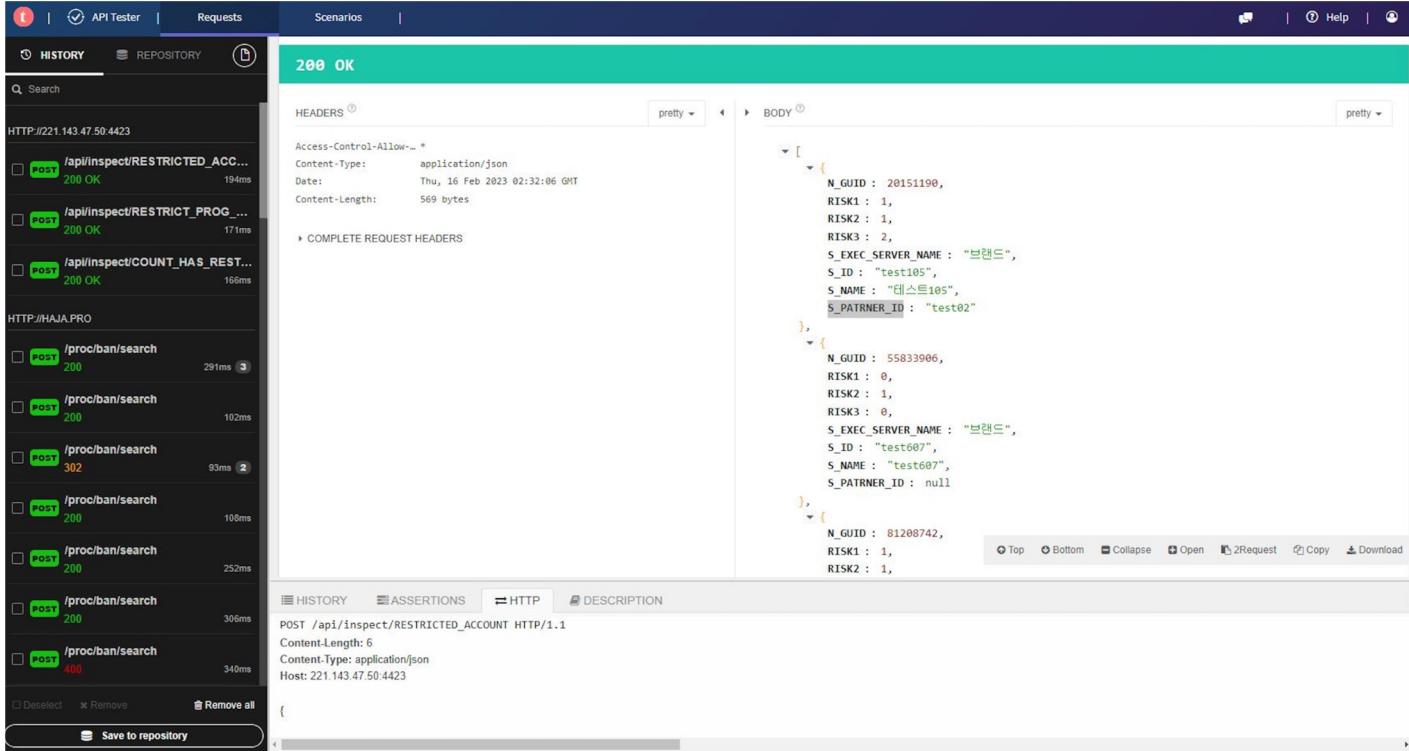

```
select * from LOG_USER where S_LOG like '%TRY%'
```

```
select * from MEMBER_INFO
```

 The results show several log entries and member information, with one specific entry highlighted:

ID	S_LOG	LOG_DATE	LOG_TYPE	LOG_DETAIL
99481479	06578044 TRY S [1]	2023-01-19 20:14:38.973	WINDOWS	SYSTEM
2	0654450501 TRY S [1]	2023-02-15 01:25:53.057	WINDOWS	SYSTEM
3	0654450501 TRY S [1]	2023-02-15 01:54:38.977	WINDOWS	SYSTEM
4	11244547 TRY E [0]	2022-12-28 11:58:44.203	WINDOWS	SYSTEM
5	11244547 TRY E [0]	2022-12-28 11:51:47.203	WINDOWS	SYSTEM
6	11244547 TRY E [0]	2022-12-28 11:52:17.187	WINDOWS	SYSTEM
- Services:** A list of running services on the system, including various log and event-related services.

→ Lots of screenshot data, including developers and infrastructure operators



The screenshot shows the API Tester interface with two main sections: 'Scenarios' and 'Requests'.

Scenarios: A list of scenarios grouped by URL. The first group is for `HTTP://221.143.47.50:4423` containing three POST requests to `/api/inspect/RESTRICTED_ACC...`, `/api/inspect/RESTRICT_PROG...`, and `/api/inspect/COUNT_HAS_REST...`. The second group is for `HTTP://HAJA.PRO` containing five POST requests to `/proc/ban/search` with various status codes (200, 200, 200, 302, 200) and response times (194ms, 171ms, 166ms, 93ms, 108ms).

Requests: A detailed view of a single request to `POST /api/inspect/RESTRICTED_ACCOUNT HTTP/1.1`. The response status is 200 OK. The Headers section shows:

```
Access-Control-Allow-Methods: *  
Content-Type: application/json  
Date: Thu, 16 Feb 2023 02:32:06 GMT  
Content-Length: 569 bytes
```

The BODY section displays a JSON array of three objects, each representing a restricted account:

```
[  
  {  
    "N_GUID": 20151190,  
    "RISK1": 1,  
    "RISK2": 1,  
    "RISK3": 2,  
    "S_EXEC_SERVER_NAME": "브랜드",  
    "S_ID": "test105",  
    "S_NAME": "테스트105",  
    "S_PARTNER_ID": "test02"  
  },  
  {  
    "N_GUID": 55833906,  
    "RISK1": 0,  
    "RISK2": 1,  
    "RISK3": 0,  
    "S_EXEC_SERVER_NAME": "브랜드",  
    "S_ID": "test007",  
    "S_NAME": "테스트007",  
    "S_PARTNER_ID": null  
  },  
  {  
    "N_GUID": 81208742,  
    "RISK1": 1,  
    "RISK2": 1,  
    "RISK3": 0  
  }]
```

Below the BODY are navigation buttons: Top, Bottom, Collapse, Open, 2Request, Copy, Download.

At the bottom of the Requests section, there are buttons for Deselect, Remove, Remove all, and Save to repository.

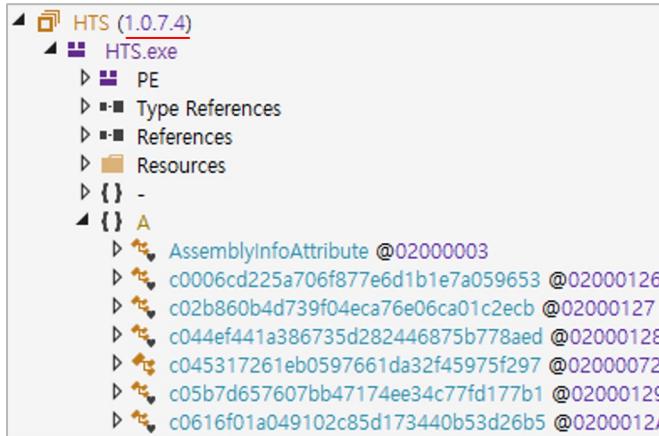
Identify threats

→ Interesting! What is this program?

CodeView Info		
Offset	Name	Value
F90E3C	CvSig	RSDS
F90E40	Signature	{9235A2CF-0C49-4473-A15E-B9EB9D4FC633}
F90E50	Age	1
F90E54	PDB	C:\#Develop\#Project\hts\2. Obfuscator\x86\HTS.pdb

CodeView Info		
Offset	Name	Value
8987A4	CvSig	RSDS
8987A8	Signature	{CB5EF8DA-C015-4999-B9AF-B43A738E0680}
8987B8	Age	1
8987BC	PDB	C:\#Develop\#Project\#MidasHTS\4. Obfuscator\x86\HTS.pdb

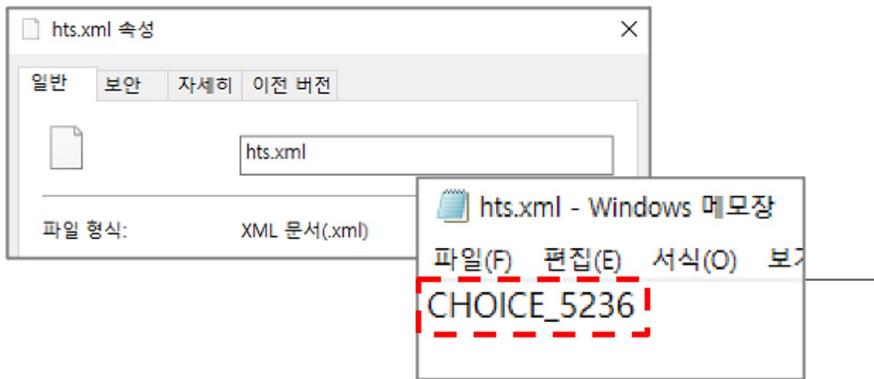
CodeView Info		
Offset	Name	Value
1007F4	CvSig	RSDS
1007F8	Signature	{A7AB130E-ABCD-4DF0-ADE4-CC80D4528282}
100808	Age	1
10080C	PDB	C:\#Develop\#Project\hts\2. Obfuscator\x86\MANAGER.pdb



→ Interesting! What is this program?



Read



```
case "HALLYM_3494721":  
    return GClass36.GEnum4.const_59;  
case "INVEST_COM_42342":  
    return GClass36.GEnum4.const_60;  
case "CHOICE_5236":  
    return GClass36.GEnum4.const_61;  
case "NANUM_672345":  
    return GClass36.GEnum4.const_62;  
case "LAB_FIN_766234":  
    return GClass36.GEnum4.const_63;  
case "LH_6345":  
    return GClass36.GEnum4.const_64;  
case "HB_7345":  
    return GClass36.GEnum4.const_65;  
case "BLACK_STONE_16343":  
    return GClass36.GEnum4.const_66;  
case "NEW_TOWN_67234":  
    return GClass36.GEnum4.const_67;  
case "FIVE_STAR_4234":  
    return GClass36.GEnum4.const_68;  
case "NEW_STOCK_3343":  
    return GClass36.GEnum4.const_69;  
case "INVESCO_6234":  
    return GClass36.GEnum4.const_70;  
case "INFINITY_72435":  
    return GClass36.GEnum4.const_71;  
case "PYTH_52343":  
    return GClass36.GEnum4.const_72;  
case GClass36.GEnum4.const_57:  
    return "http://172.65.173.53:4423/";  
case GClass36.GEnum4.const_58:  
    return "http://172.65.244.29:4423/";  
case GClass36.GEnum4.const_59:  
    return "http://172.65.170.183:4423/";  
case GClass36.GEnum4.const_60:  
    return "http://172.65.198.37:4423/";  
case GClass36.GEnum4.const_61:  
    return "http://172.65.166.246:4423/";  
case GClass36.GEnum4.const_62:  
    return "http://172.65.173.53:4423/";  
case GClass36.GEnum4.const_63:  
    return "http://172.65.171.188:4423/";  
case GClass36.GEnum4.const_64:  
    return "http://172.65.164.25:4423/";  
case GClass36.GEnum4.const_65:  
    return "http://172.65.164.25:4423/";  
case GClass36.GEnum4.const_66:  
    return "http://172.65.182.136:4423/";  
case GClass36.GEnum4.const_67:  
    return "http://172.65.189.138:4423/";  
case GClass36.GEnum4.const_68:  
    return "http://172.65.223.181:4423/";  
case GClass36.GEnum4.const_69:  
    return "http://172.65.177.219:4423/";  
case GClass36.GEnum4.const_70:  
    return "http://172.65.242.127:4423/";  
case GClass36.GEnum4.const_71:  
    return "http://172.65.194.214:4423/";  
case GClass36.GEnum4.const_72:  
    return "http://172.65.230.231:4423/";
```

→ Correlating programs and screenshots

이름	수정한 날짜	유형
KcFormAddGroup.cs	2023-03-13 오후 4:36	CS 파일
KcFormAddGroup.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormAdminManager.cs	2023-03-13 오후 4:36	CS 파일
KcFormAdminManager.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormAllowDeposit.cs	2023-03-13 오후 4:36	CS 파일
KcFormAllowDeposit.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormBatchEditCD.cs	2023-03-13 오후 4:36	CS 파일
KcFormBatchEditCD.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormBlackList.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateDayMember.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateDayMember.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateDayPartner.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateDayPartner.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateMember.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculateMember.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculatePartner.cs	2023-03-13 오후 4:36	CS 파일
KcFormCalculatePartner.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormChat.cs	2023-03-13 오후 4:36	CS 파일
KcFormChat.Designer.cs	2023-03-13 오후 4:36	CS 파일
KcFormConfirmEventRestPoint.cs	2023-03-13 오후 4:36	CS 파일
KcFormConfirmEventRestPoint.Designer...	2023-03-13 오후 4:36	CS 파일
KcFormDepositListEx.cs	2023-03-13 오후 4:36	CS 파일
KcHTSDataSet.xsd		
KcHTSDataSet4Chat.xsd		
KcHTSDataSet4Stock.xsd		
KcHTSDataSetCalculate.xsd		
KcHTSDataSetEvent4RestPoint.xsd		
KcHTSDataSetSetupBlock.xsd		
KcHTSDataSetSubOffice.xsd		
KcEventExecutionServer.cs		C# 파일
KcFormAddGroup.cs		CS 파일
KcFormAdminManager.cs		CS 파일
KcFormAllowDeposit.cs		CS 파일
KcFormBatchEditCD.cs		CS 파일
KcFormBlackList.cs		CS 파일
KcFormCalculateDayMember.cs		CS 파일
KcFormCalculateDayPartner.cs		CS 파일
KcFormCalculateMember.cs		CS 파일
KcFormCalculatePartner.cs		CS 파일
KcFormChat.cs		CS 파일
KcFormConfirmEventRestPoint.cs		CS 파일
KcFormDepositListEx.cs		CS 파일
KcFormDepositText.cs		CS 파일
KcFormDeviceList.cs		CS 파일
KcFormDevKey.cs		CS 파일
KcFormEventRestPointList.cs		CS 파일
KcFormEventRestPointSet.cs		CS 파일
KcFormIncentive.cs		CS 파일
KcFormIpBlockList.cs		CS 파일
KcFormIpBlockLog.cs		CS 파일
KcFormJoinMember.cs		CS 파일
KcFormJoinPartner.cs		CS 파일
KcFormLogin.cs		CS 파일
KcFormMain.cs		CS 파일
KcFormManageAlarm.cs		CS 파일
KcFormManagePositions.cs		CS 파일
KcFormManagerNotice.cs		CS 파일

Red box highlights the KcEventExecutionServer.cs file and its associated assembly files.

```

    참조 5개 [vscode], 1일 전 [만든 이] 2명, 변경 내용 2개
public static int ServerName2ID(string strServerName)
{
    try
    {
        KcDatabase.ConnectDB();
        KcDatabase.s.Mutex4Conn.WaitOne();
        SqlCommand sqlComm = new SqlCommand();
        sqlComm.Connection = KcDatabase.s.Conn;
        sqlComm.CommandText = $"SELECT [N_ID] FROM [dbo].[EXEC_SERVICE]"
        using (SqlDataReader SqIRs = sqlComm.ExecuteReader())
        {
            while (SqIRs.Read())
            {
                return int.Parse(SqIRs[0].ToString());
            }
        }
    }
    catch
    {
    }
    finally
    {
        KcDatabase.s.Mutex4Conn.ReleaseMutex();
    }
}
  
```

문제가 검색되지 않음

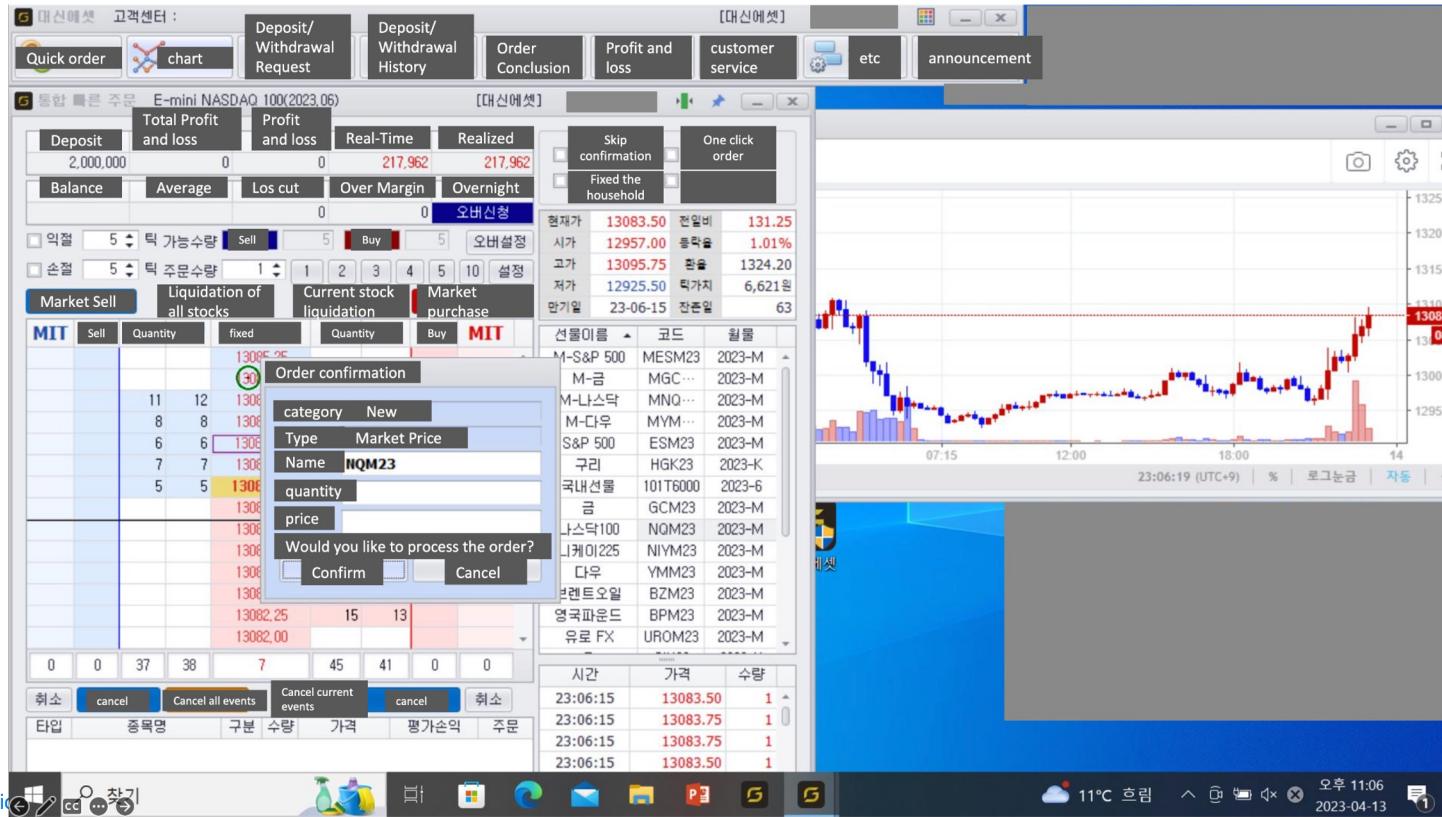
조사식 1

검색(Ctrl+E) 검색 십도: 3

이름	Count
KcEnvironments_mapEnvirData	Count = 23
strID	error CS0101
IMacAddress	error CS0101
strPartnerID	error CS0101
strPartnerID	error CS0101
url	error CS0101
process	error CS0101
result	error CS0101

검색을 험복 추가

→ They think they're making an investment



The screenshot shows a financial trading application window titled "E-mini NASDAQ 100(2023.06)". The main interface includes tabs for "Deposit/Withdrawal Request", "Deposit/Withdrawal History", "Order Conclusion", "Profit and loss", "customer service", "etc", and "announcement". Below these tabs, there are sections for "Total Profit and loss", "Profit and loss", "Real-Time", and "Realized". A "Skip confirmation" checkbox is checked.

A modal dialog box is open, titled "Order confirmation", with the following details:

- category:** New
- Type:** Market Price
- Name:** NQM23
- quantity:** 15
- price:** 13082.25

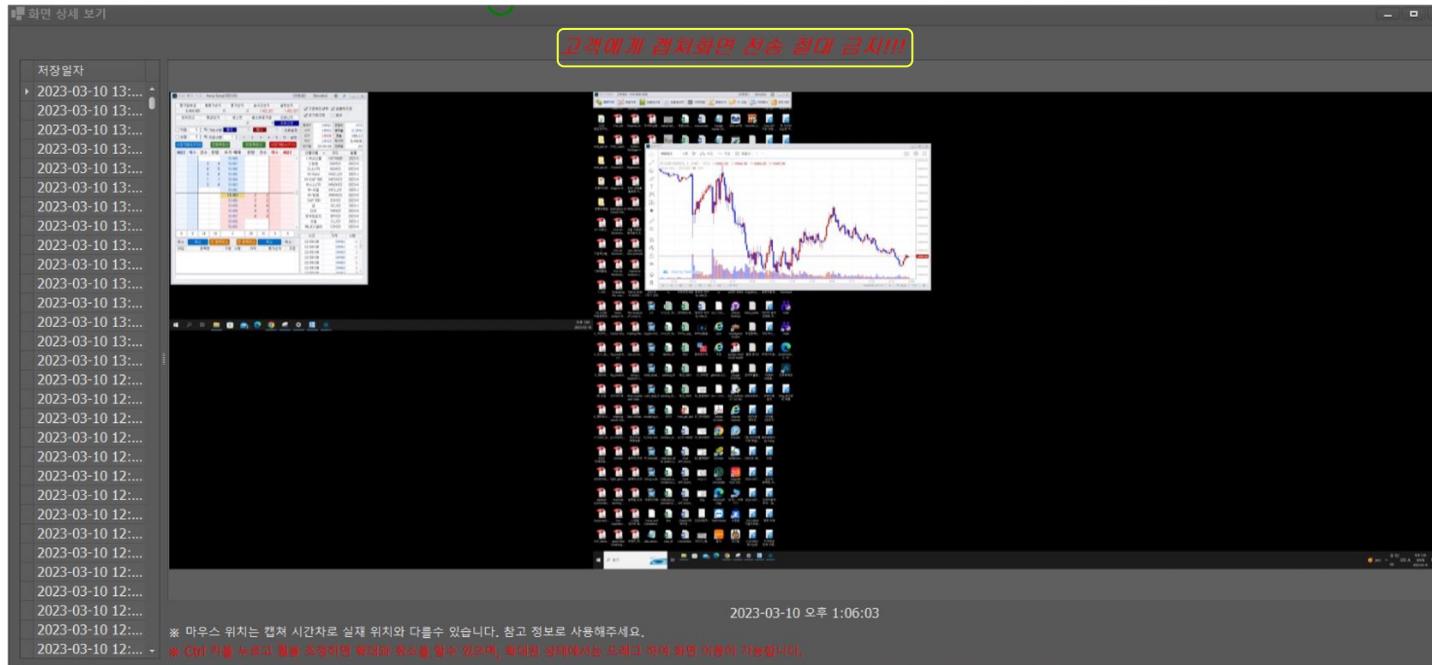
At the bottom of the dialog, there are "Confirm" and "Cancel" buttons.

The right side of the screen displays a candlestick chart for the E-mini NASDAQ 100 index, showing price movement over time. A red vertical line highlights a specific price point around 13083.50.

At the bottom of the screen, there is a taskbar with various icons and a system tray showing the date and time (2023-04-13 11:06).

→ There is someone watching over this

Sending captured screens to customers is absolutely prohibited!!!



→ There is someone watching over this

→ There is someone watching over this

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY_CURRENT_USER\Software\HTC

컴퓨터
 > HKEY_CLASSES_ROOT
 > HKEY_CURRENT_USER
 > AppEvents

이름	종류	데이터
ab (기본값)	REG_SZ	(값 설정 안 됨)
DeviceID	REG_SZ	Kdu

Name	Value
bytes	0x02EA86DC
byteLength	34
encoding	{System.Text.UnicodeEncoding}
charCount	17
text	"IsDebuggerPresent"
ptr	null
chars	17

An unhandled exception occurred in DeviceKeyGenerator.exe (3364)

Exception: System.Exception

Message: Debugger was found - this software cannot be executed under the Debugger.

OK

→ Eventually they run away

2023.04.

```
case "AONE_295732":  
    return GClass43.GEnum5.const_51;  
  
case GClass43.GEnum5.const_51:  
    return "http://154.83.21.79:4423/";
```



2023.06.

```
case "AONE_295732":  
    return GClass35.GEnum4.const_46;  
  
case GClass35.GEnum4.const_46:  
    return "http://0.0.0.0:4423/";
```

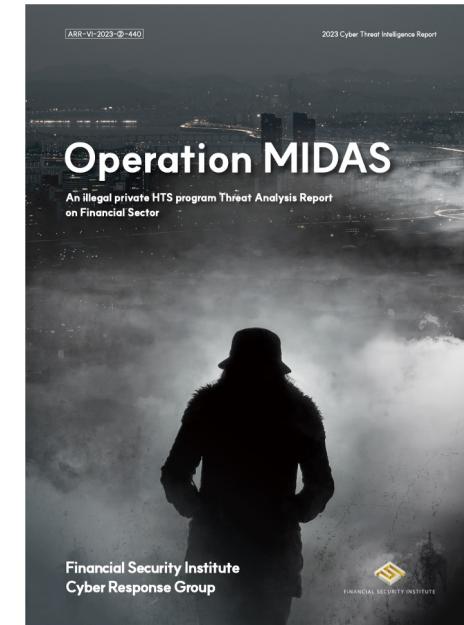


Response

1. Response for Financial Companies

→ Create detailed analysis and detection rules

- ◆ OSINT and programmatic analysis identified approximately 125 identical fake HTS
- ◆ Writing detection rules
 - YARA : Livehunt from virustotal
 - Snort : Apply to Financial Security SOC('23.3)





Conclusion

→ Large undiscovered cybercrime clusters

- ◆ Potential losses could reach hundreds of billions due to fake trading platforms, hidden fees, long operations, and large member bases.
- ◆ Many victims often viewing their losses as personal investment failures rather than the result of targeted fraud.

→ Contextual Literacy and Continuous Monitoring in OSINT

- ◆ Threat assessment demands understanding your country's laws, culture, and context.

→ Criminals are also actively utilizing GenAI like ChatGPT

- ◆ GenAI is very effective at unit-level function development
- ◆ How do we adapt to counter this new wave of malware?



```
작업 이름: clean
작업 설명: 매일 아침 7시 30분에 D 드라이브에 있는 clean.bat 파일을 실행될 수 있게 스케줄러 명령어를 바탕으로 만들어줘

작업 세부 정보
작업 이름: clean
작업 설명: 아래는 매일 아침 7시 30분에 D 드라이브의 clean.bat 파일을 실행하도록 스케줄러를 등록하는 bat 파일 예시입니다.

코드
@echo off
set taskname="MyScheduledTask"
REM 기본에 포함된 스케줄러 삭제
schtasks /Delete /TN "%taskname%" /F
REM 새로운 스케줄러 등록
schtasks /Create /TN "%taskname%" /TR "D:\clean.bat" /SC DAILY /ST 0730 /F
```

Antiforensic script by ChatGPT
#BHEU @BlackHatEvents



Report Download

Thank you

Financial Security Institute

Sung-Wook Jang

Yong-Hyun Kim (@copy_and_paster, yhkim@fsec.or.kr)