Operation MIDAS

Tracking Fraudulent Financial Program Organizations

Financial Security Institute

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

About us

- **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

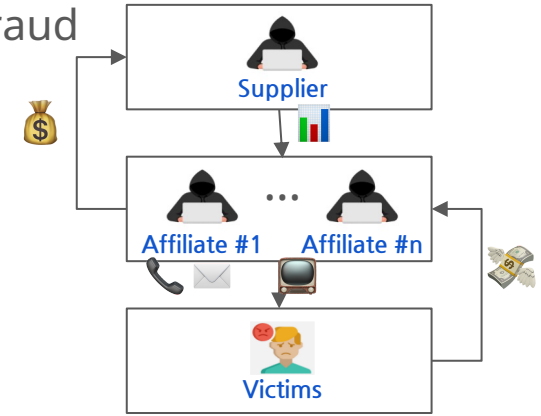
Background

➔ 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

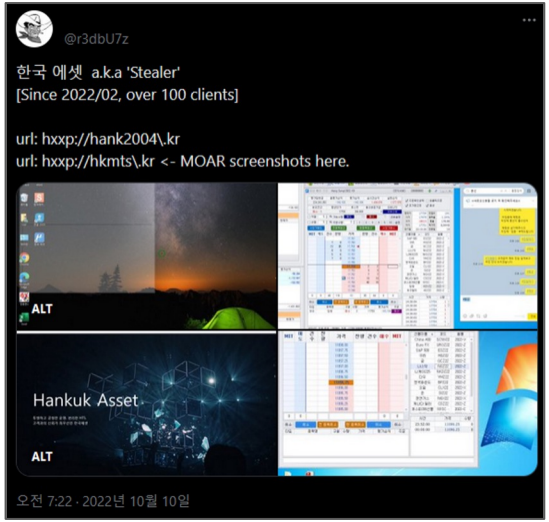
- Supplier : An organization that develops and distributes fake HTS
- Affiliate : An organization that uses fake HTS to commit fraud (there are several groups)
- 3rd party service : Legitimate & Not Legitimate Services (e.g, Youtube, Money Launderers, Messenger Service, …)

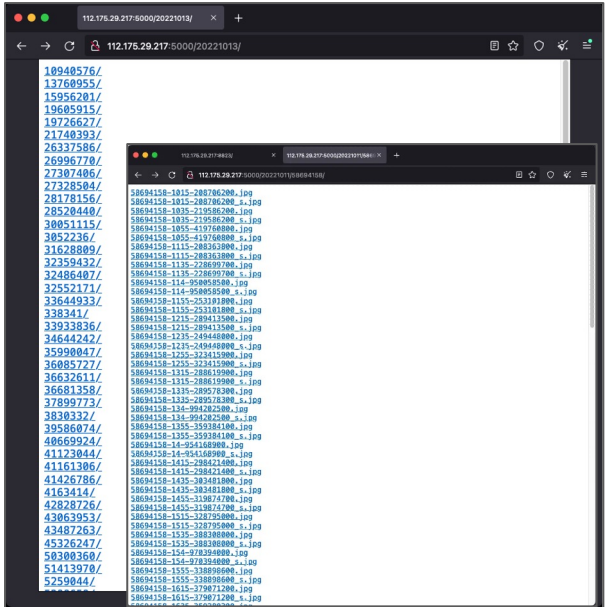


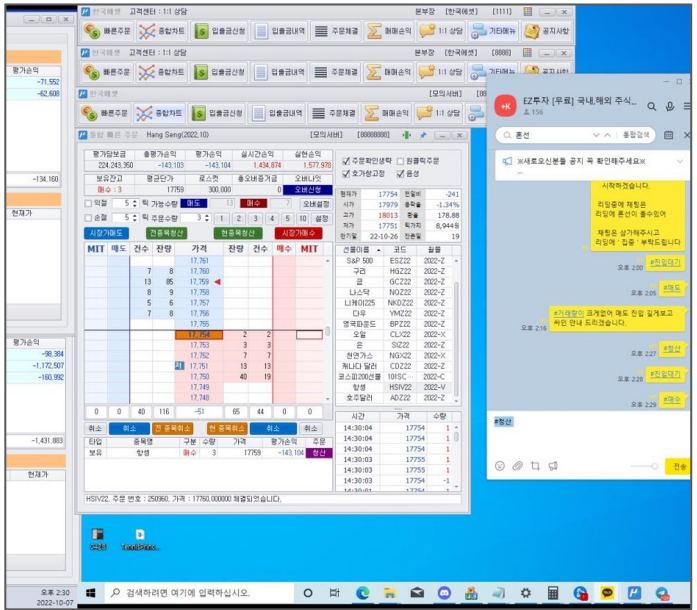
Initial Findings(1/2)

➔ 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!





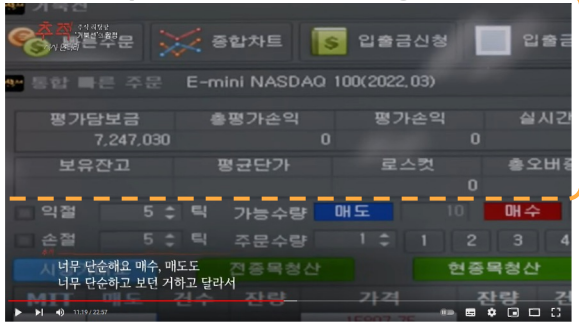


* https://x.com/r3dbU7z/status/1579235837833011201

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

본부장 = General Manager
모의서버 = Demonstration Server

Don't chat while leading. please be 'concentrated'!

#wait
#sell
#sell
#wait
#buy

Scam messages (156 audience)

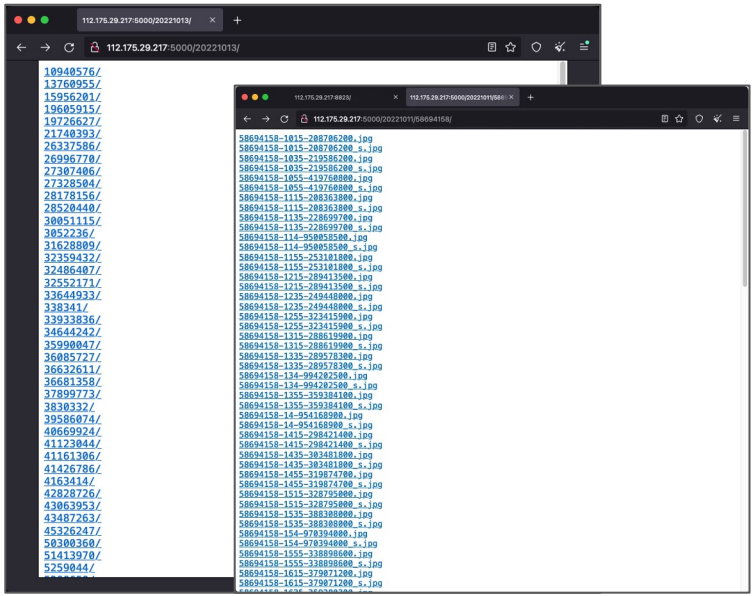
OPSEC Failures

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

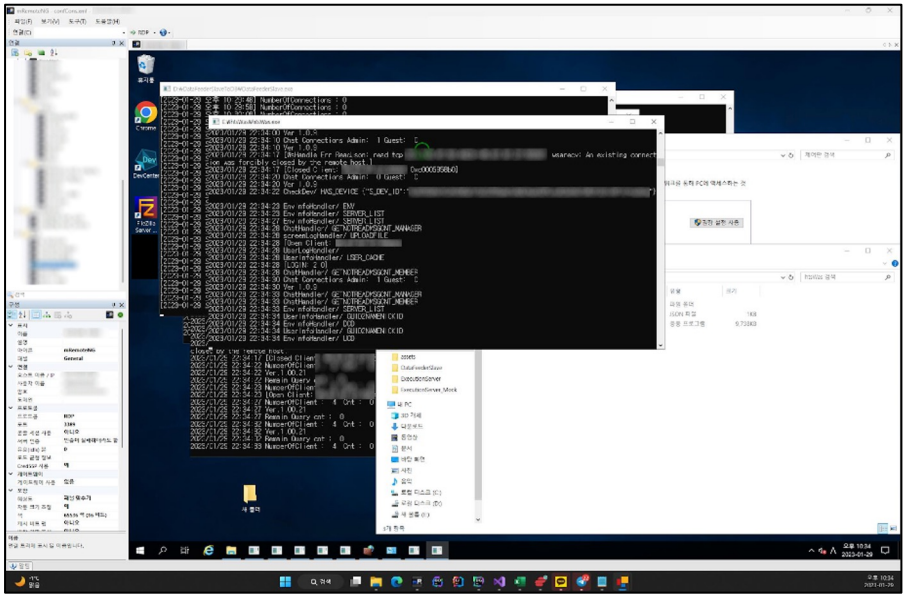
#1 : Leaked screenshots by directory indexing

➔ 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

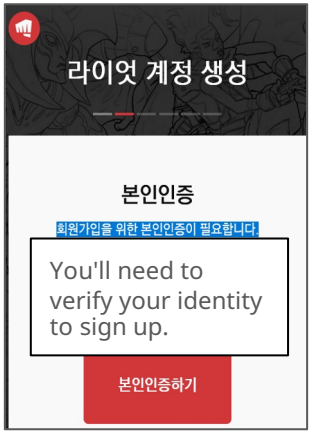


Server management using mRemoteNG
(Supplier's screenshot)

#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

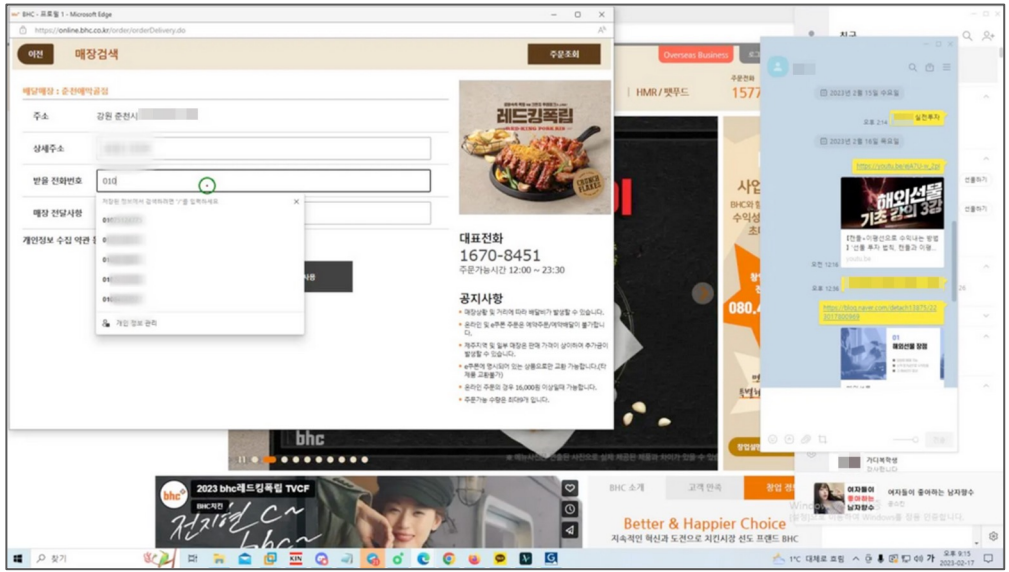
(HMAC-SHA Hashed value using SSN with Password)

wEi9oYSuekQGxT9MV4rKHG4CO+Zrp+onhLIluembI8jx/0PLF5Ne3oM
BxvUFIN4UmsgjeNErZfmpCVUFHsv8nq==...

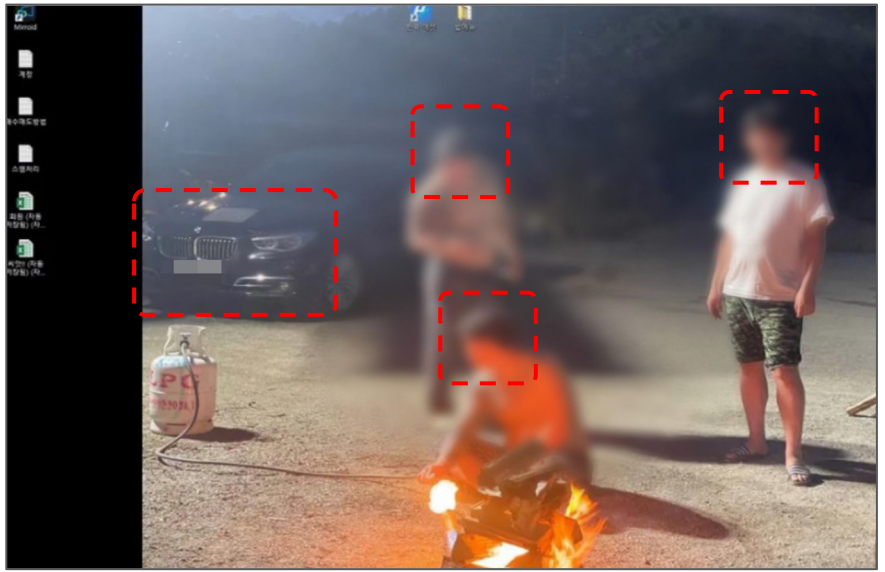
#2 : Lack of device isolation(2/2)

➔ No separation between crime / personal device

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



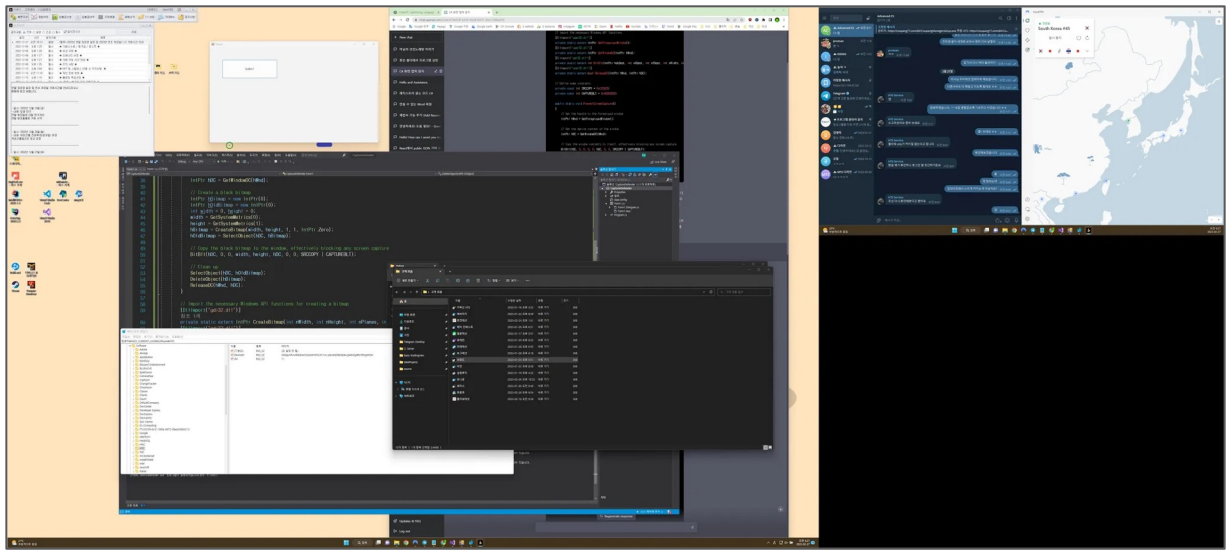
Location exposure in food delivery ordering



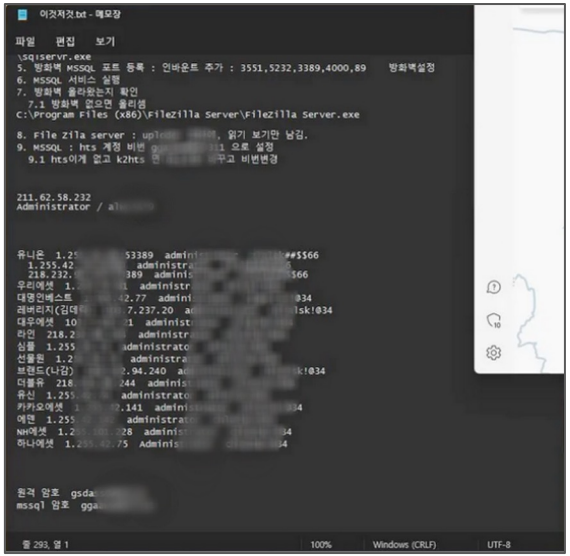
Identified car license plate, face of affiliate members by wallpaper

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

➔ Insecure software development and testing



Screenshot of Supplier uploaded during development



RDP/RDBMS credentials

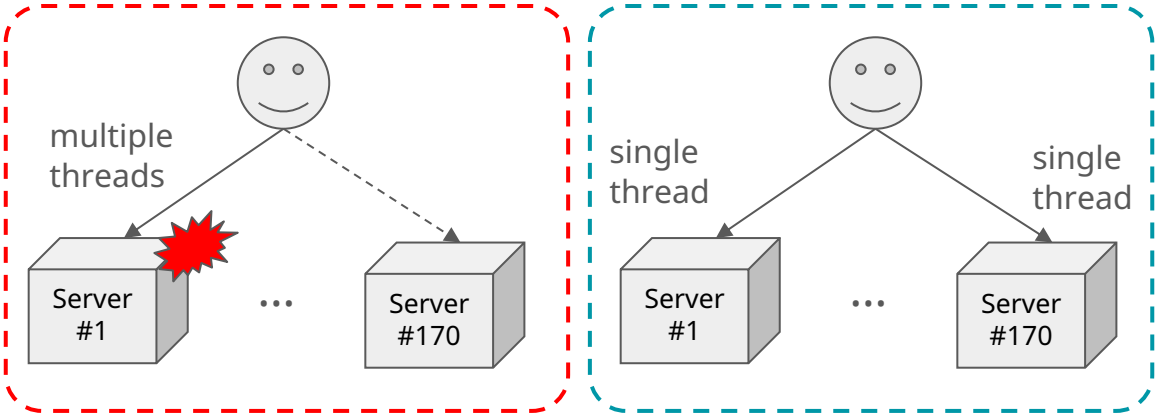
Tracking Criminals

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)



Example of unsafe collection

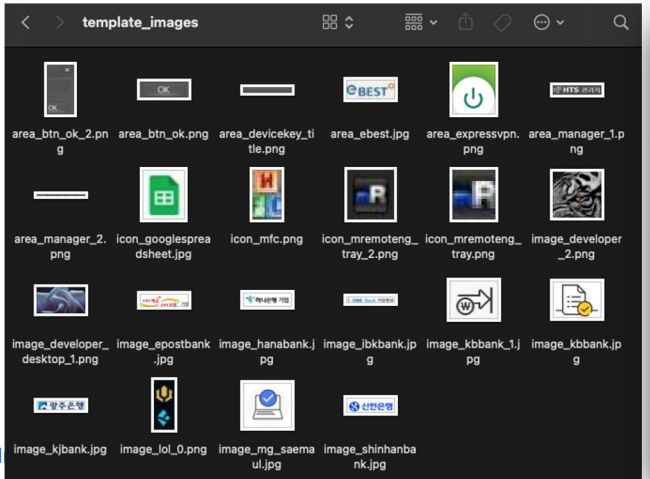
Example of safe collection

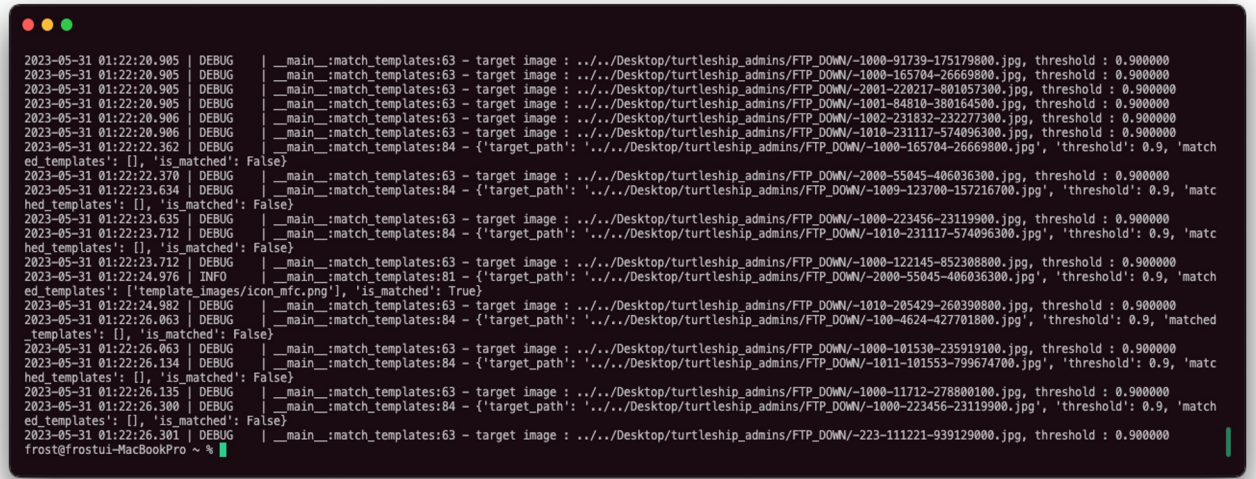
Collection & Triage of Screenshots(2/2)

➔ 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

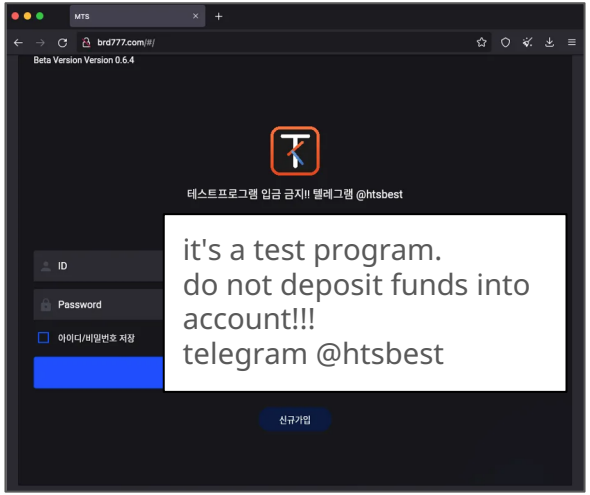




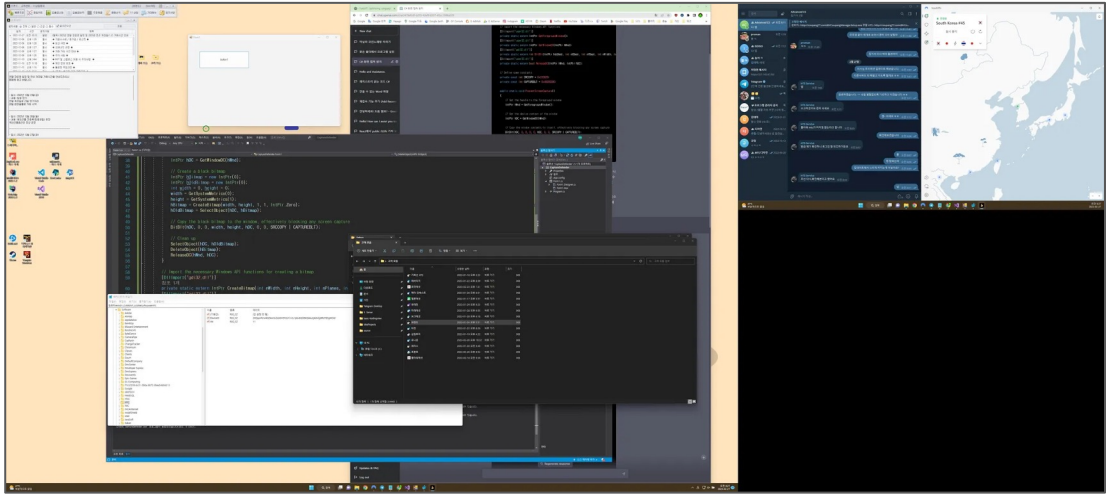
Deep-dive analysis of screenshots(1/2)

➔ 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

Correlation analysis of infrastructure

➔ Find another Fake HTS Server using Intelligence Services

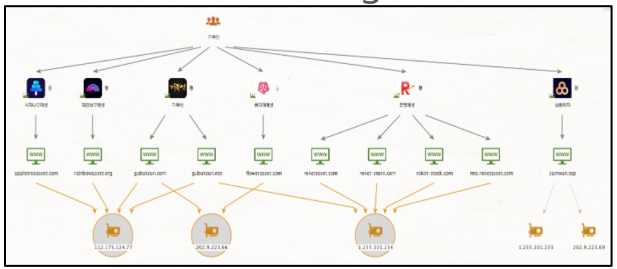
- Use Censys Search to search for hosts with the same Software + same port criteria

Installer Deployment Port

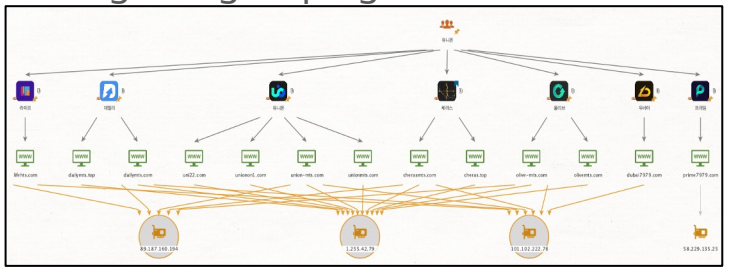
```
services.software.product=`FileZilla Server` and
(services.port:4000 and services.port:2127 and services.port:80 and services.port:89)
```

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

- Track & Analyze Passive DNS History using Virustotal
  - useful for tracking server reuse, rebranding and grouping same affiliate



'Turtleship' Affiliate Group

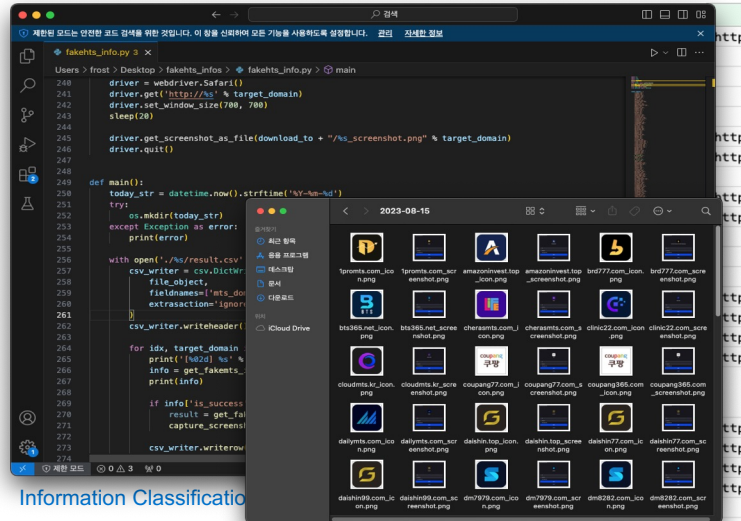


'Union' Affiliate Group

Correlation analysis of infrastructure

➔ 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

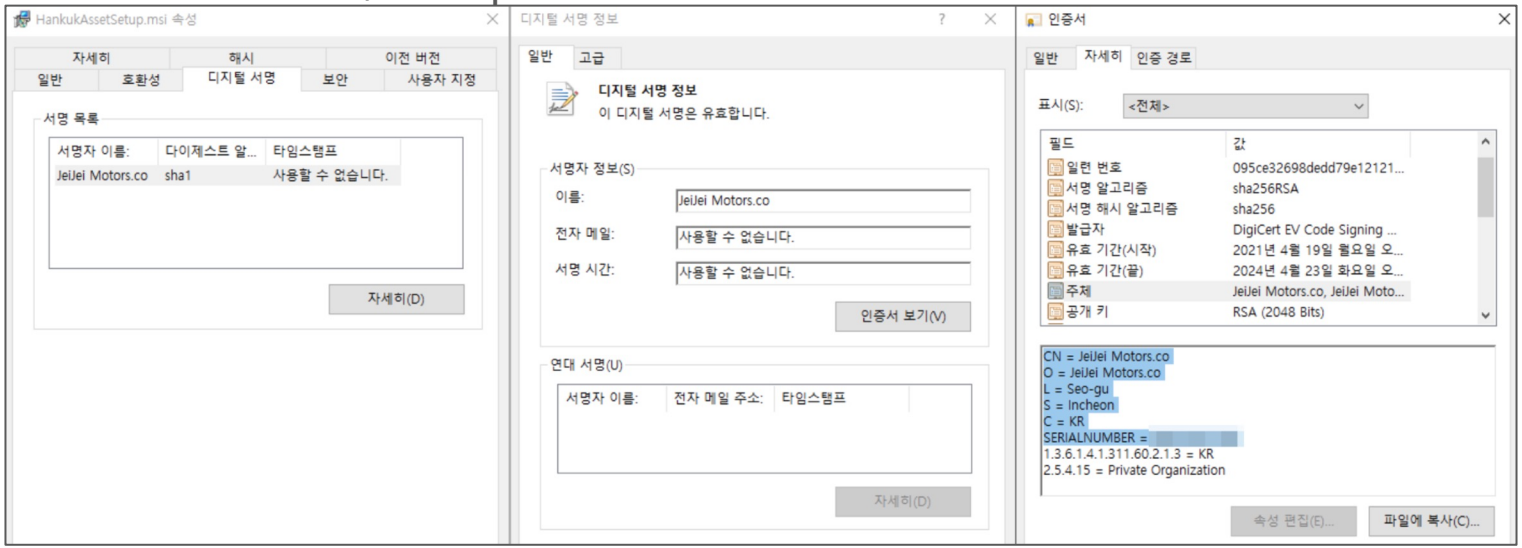


N	O	P	Q	R
http://101.102.223.81:4423/	http://101.102.223.81:4423/	http://metainvest7.com:4423/	http://metainvest7.com:4423/	http://metainvest7.com:4423/
				http://103.97.209.210:4423/
http://101.102.221.16:4423/	http://101.102.221.16:4423/			
http://mtsspace.net:4423/	http://mtsspace.net:4423/	http://mtsspace.net:4423/	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://orangemts.com:4423/	http://orangemts.com:4423/	http://orangemts.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://101.102.221.21:4423/	http://101.102.221.21:4423/			
http://researmts.com:4423/	http://researmts.com:4423/	http://researmts.com:4423/	http://researmts.com:4423/	http://researmts.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://roket-stock.com:4423/	http://roket-stock.com:4423/	http://roket-stock.com:4423/
		http://roketasset.com:4423/	http://roketasset.com:4423/	http://roketasset.com:4423/

Correlation analysis of infrastructure

➔ 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



Correlation analysis of infrastructure

➔ 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	goldmts.com	whois.namesilo.com	Succeed	Registered

```
Registrant Name: Jong
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: htsman@protonmail.com
```

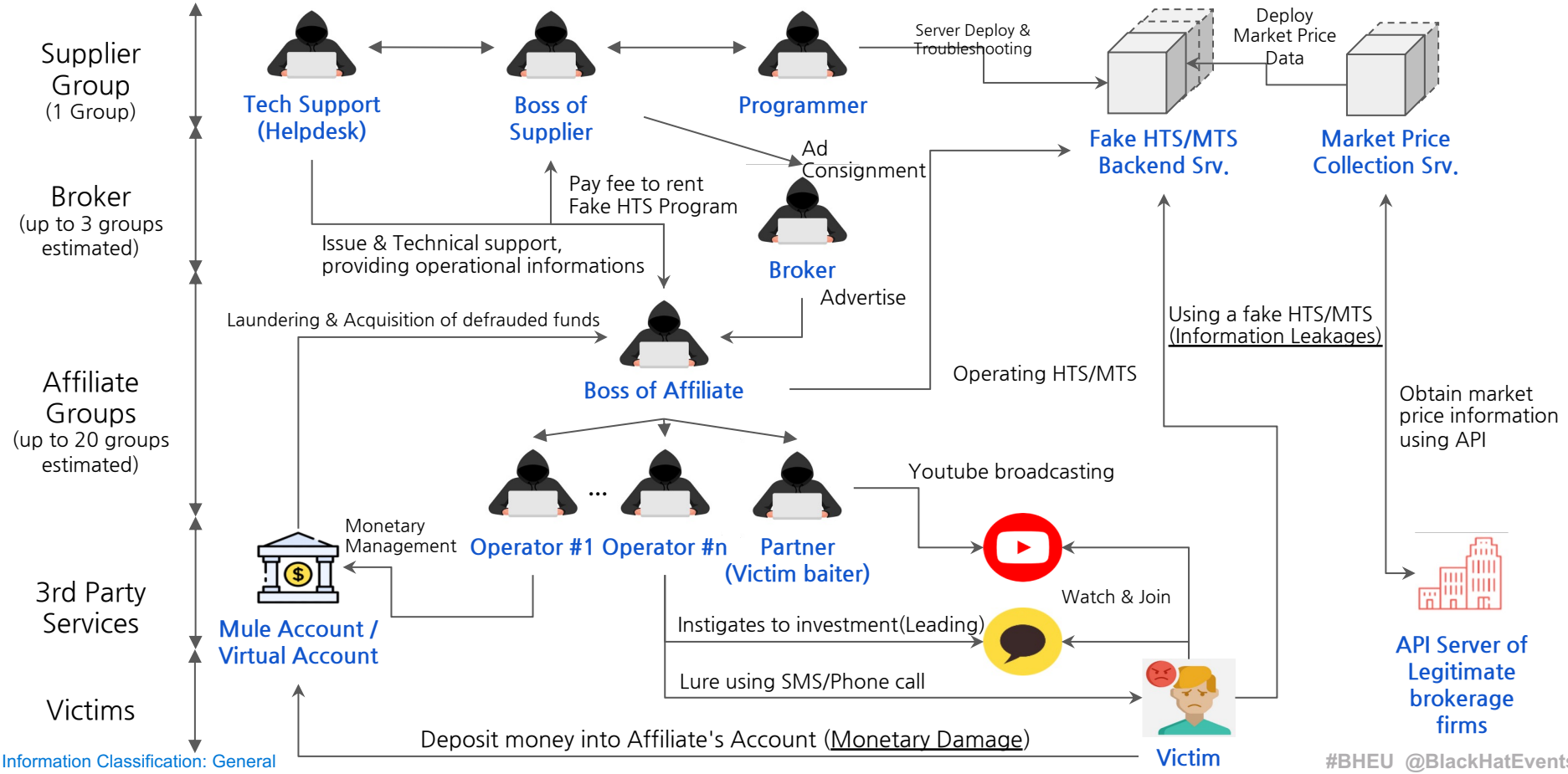
d-brg[.]com	smilemts[.]com	smileasset[.]top	benest[.]top

```
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 Email: htsman@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)

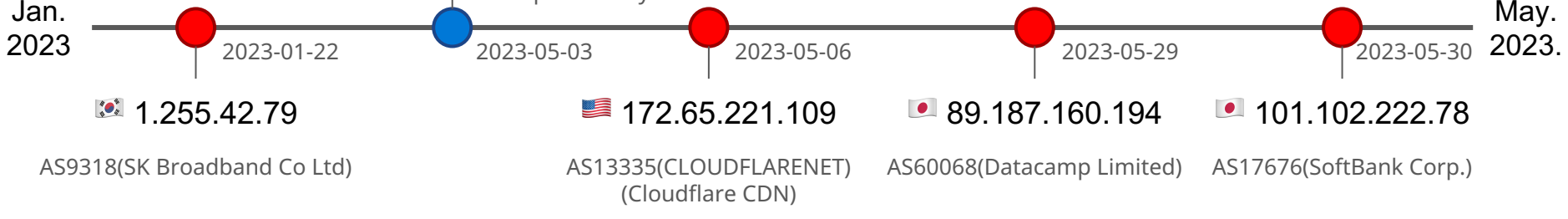
송고시간 | 2023-05-03 11:41

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

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

* 200 million dollars

* https://www.yna.co.kr/view/AKR20230503039451060



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

[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. 최신개발툴 활용한 빠르고 버그 없는 시스템.
3. 버그가 없으며 고객이나 관리자나 사용하기 편리한 UI
4. 최신 트렌드 UI및 트레이딩뷰 차트 적용.
5. 24시간 실시간 응대및 에로 사항 즉시 해결.
6. 해외선물,주식,코인 거래 시스템 구축
7. 네트워크 전문가 보유. 디도스 클린존 보호가능.
8. 빠른서버구축및 운영준비(3~5일 완료)
성실하고 신의있는 팀과 이제 함께 하십시요.

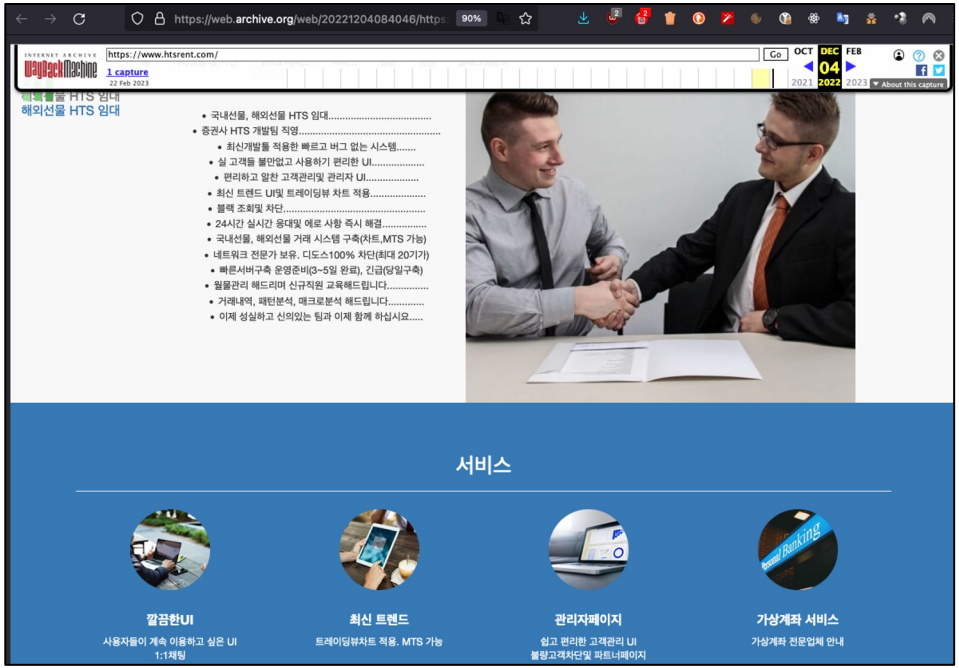
문의 텔레그램 @htsman

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...]



[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

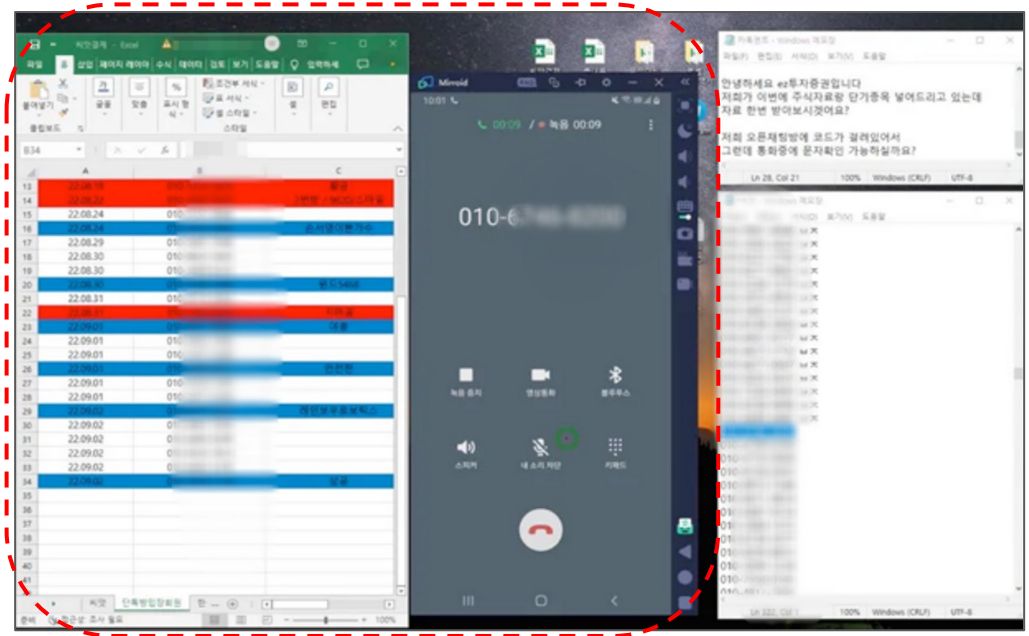
	A	money laundering fee	Fake HTS Rental fee ($5,300/M)	Virtual Account fee	Blog(advertisement) fee DB(phone number list) fee SMS(Text message) fee			Meal allowance ($2,600/M)
1	날짜	롤링	ＨＴＳ비용	가상계좌비용	블로그비용	디비	문발	식대
2	1일	109,600						3,720,000
3	2일	96,000						
4	3일	224,000	7,500,000					
5	4일	136,000				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

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



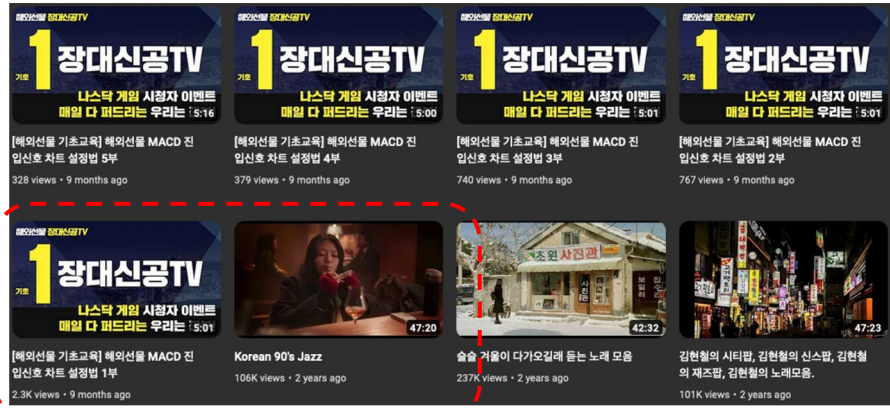
[Advertisement Script]
Hello, we are 'EZ securities'!
I'd like to put in some stock informations and some short-term stuff.
Would you like to take a look at it?

Record the call recipient's reaction
'ㅂ ㅈ' = 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

YouTube Broadcast to Lure Investors

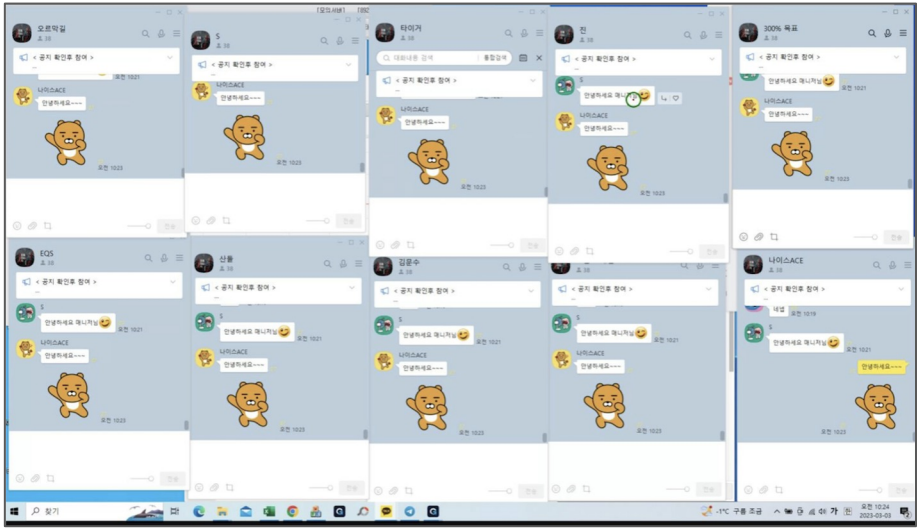


Gaps in YouTube video uploads and changes in topic

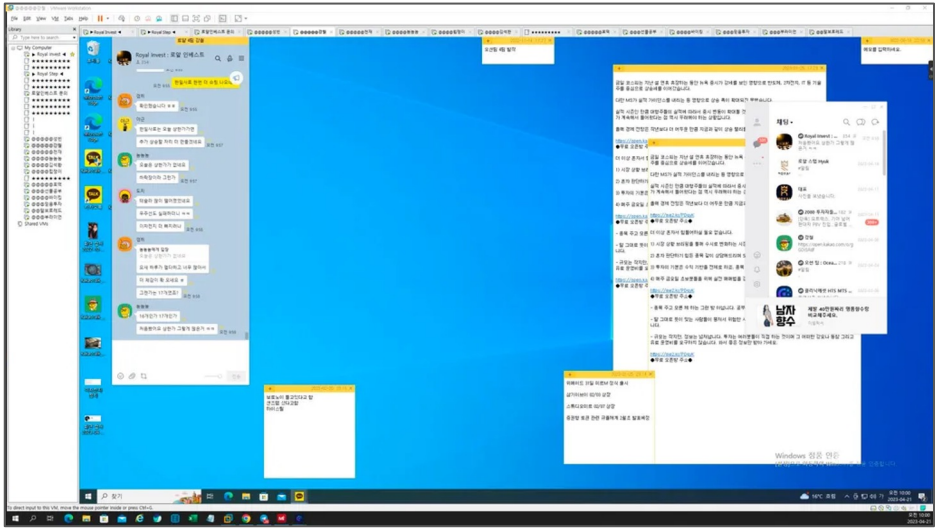
[Affiliates] Theft of money from victims(1/2)

➔ 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'

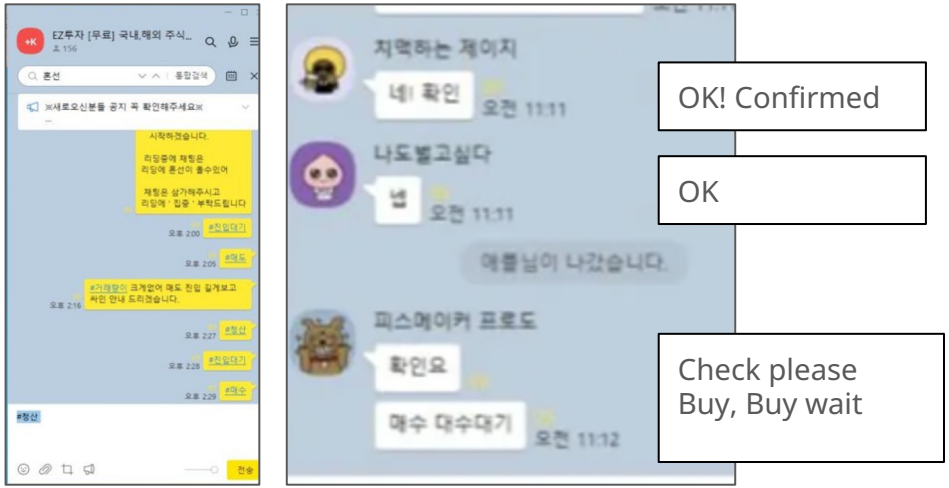


multiple execution using 'VMware Workstation'

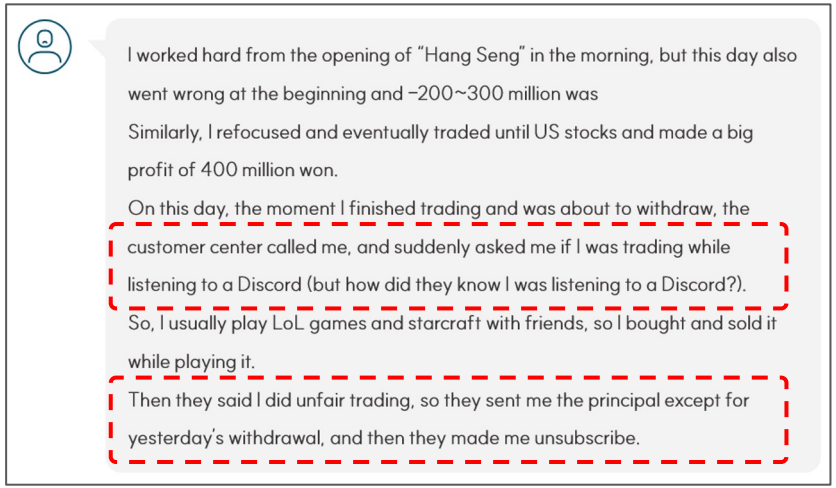
[Affiliates] Theft of money from victims(2/2)

➔ 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



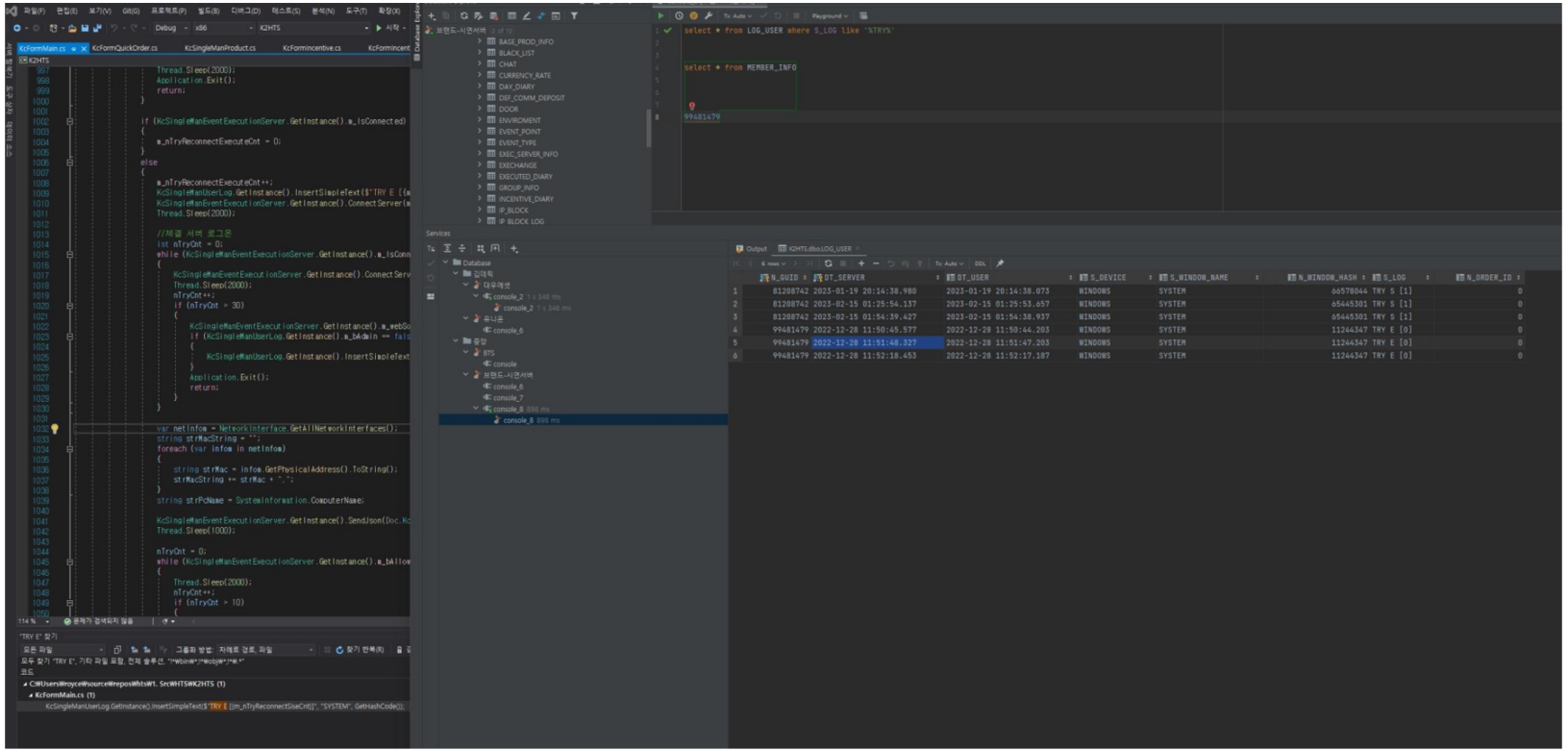
Surveillance of users and banning with unconvincing excuses

Fake HTS Program Analysis

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

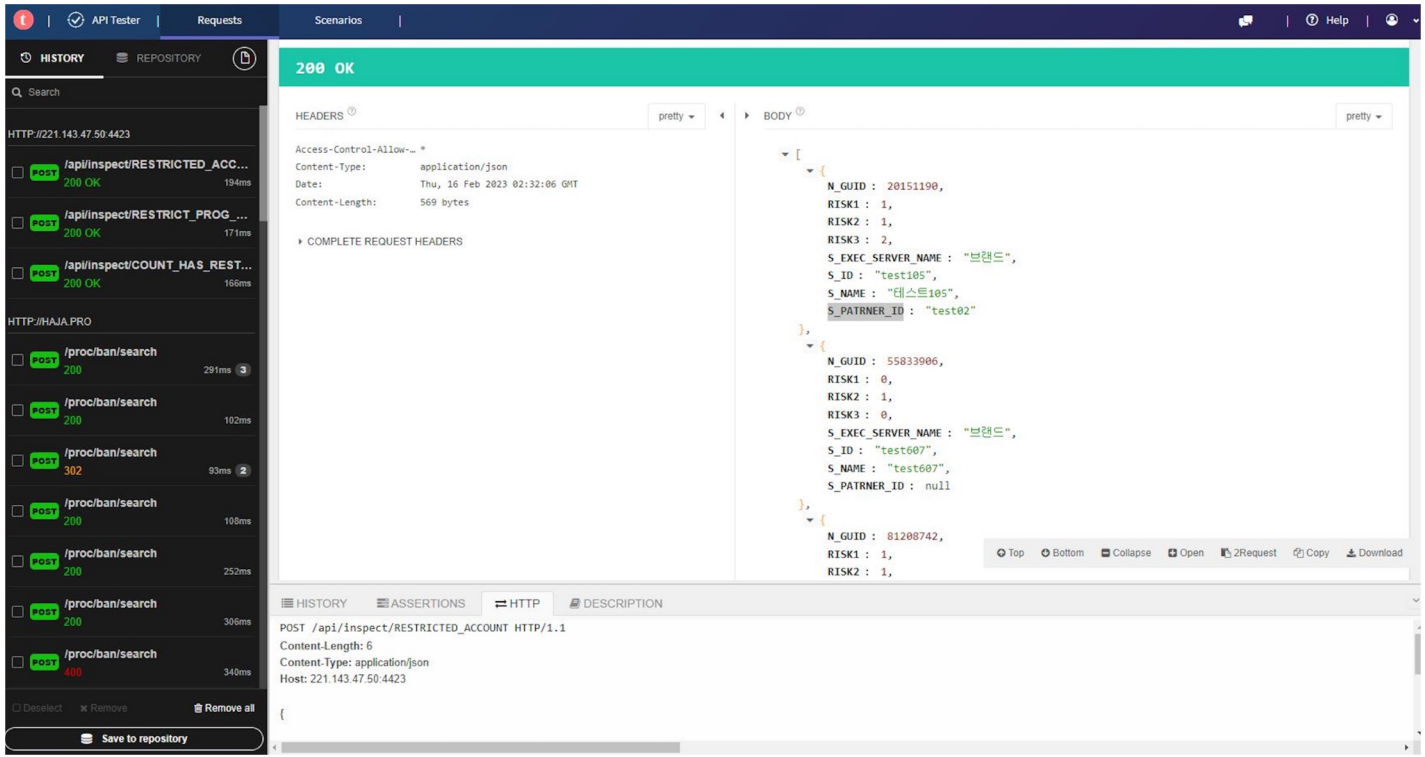
Identify threats

➔ Lots of screenshot data, including developers and infrastructure operators



Identify threats

➔ Lots of screenshot data, including developers and infrastructure operators



Identify threats

➔ **Interesting! What is this program?**

CodeView Info

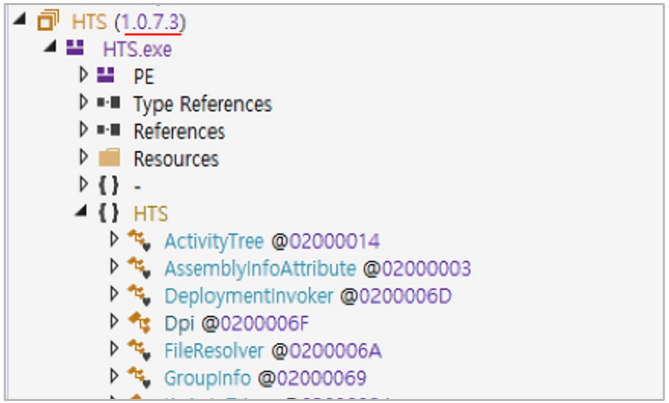
Offset	Name	Value
F90E3C	CvSig	RSDS
F90E40	Signature	{9235A2CF-0C49-4473-A15E-B9EB9D4FC633}
F90E50	Age	1
F90E54	PDB	C:₩Develop₩Project₩hts₩2. Obfuscator₩x86₩HTS.pdb

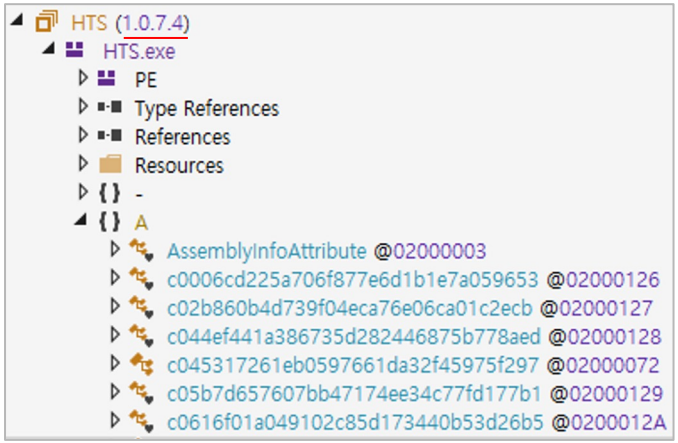
CodeView Info

Offset	Name	Value
89B7A4	CvSig	RSDS
89B7A8	Signature	{CB5EF8DA-C015-4999-B9AF-B43A738E0680}
89B7B8	Age	1
89B7BC	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

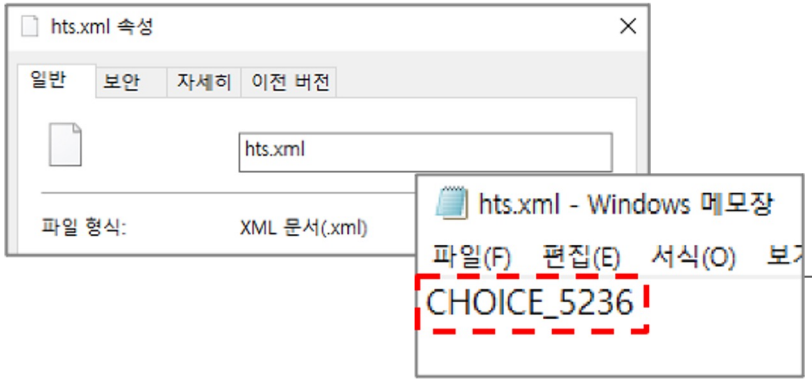




Program analysis

➔ **Interesting! What is this program?**

Read

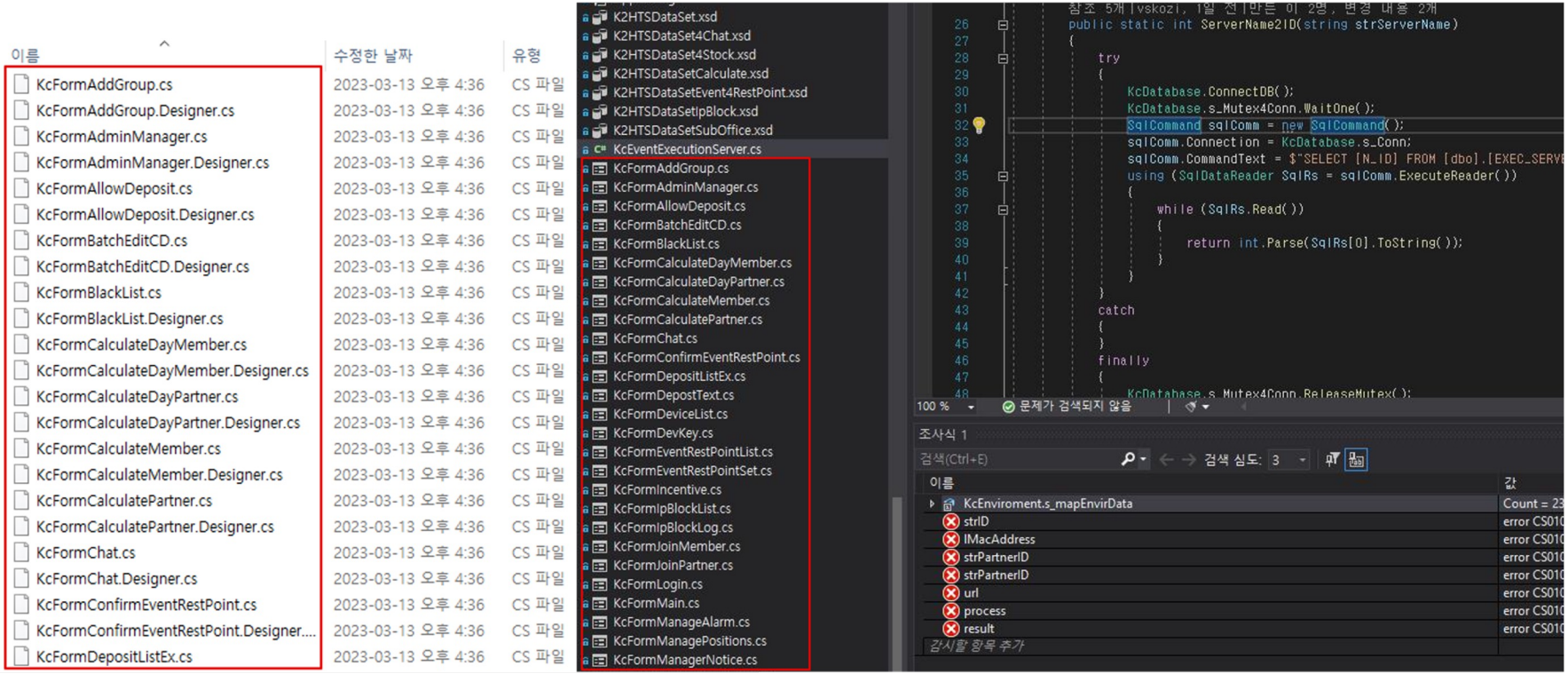



```
case "HALLYM_3494721":
  return GClass36.GEnum4.const_59;
case "INVEST_COM_42342":
  return GClass36.GEnum4.const_60;
case "CHOICE_5236":
  return GClass36.GEnum4.const_61;
case "NANUM_672345":
  return GClass36.GEnum4.const_62;
case "LAB_FIN_766234":
  return GClass36.GEnum4.const_63;
case "LH_6345":
  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":
```

```
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://172.65.190.37:4423/";
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/";
```

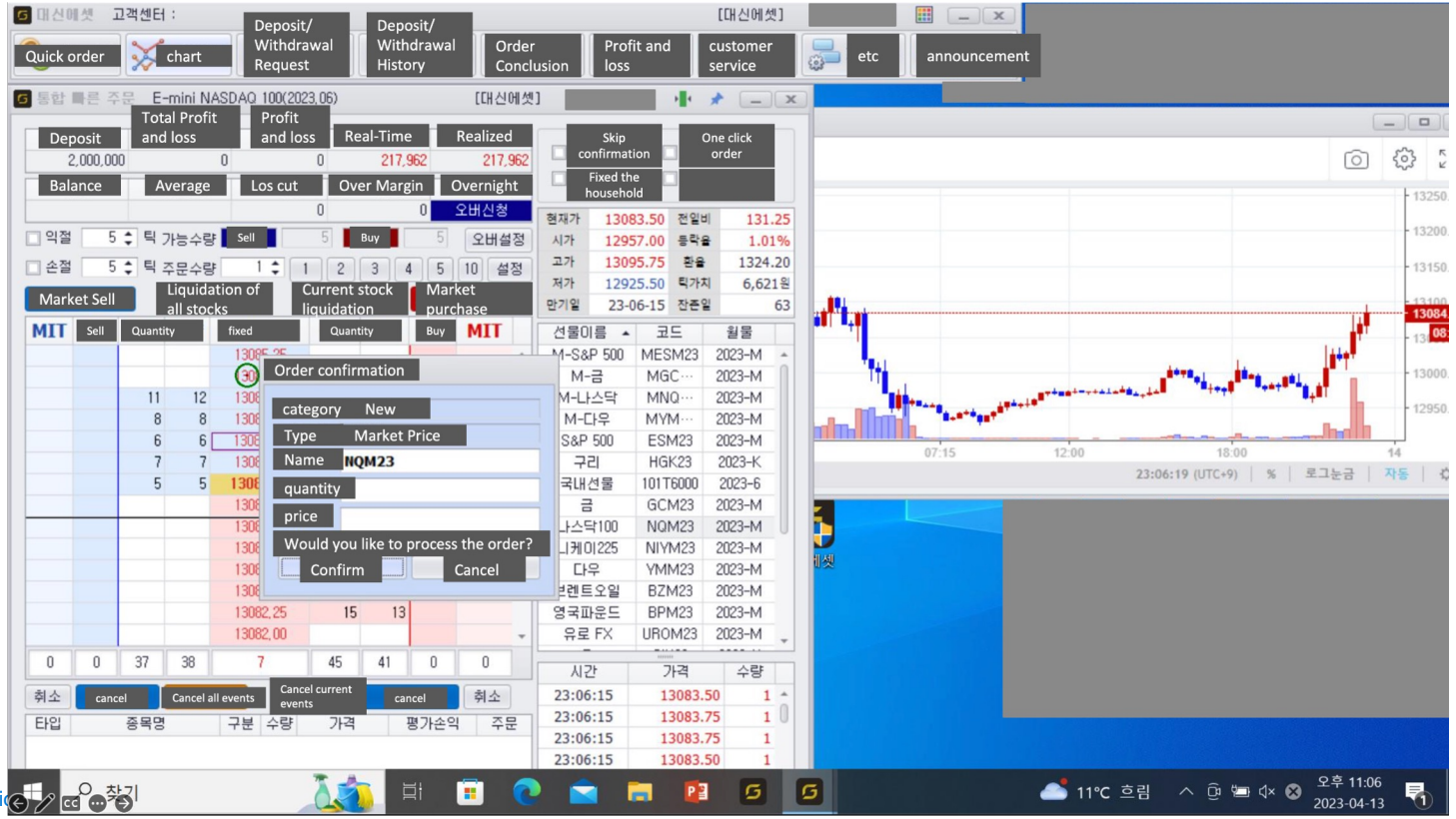
Program analysis

➔ Correlating programs and screenshots



Malicious behavior analysis

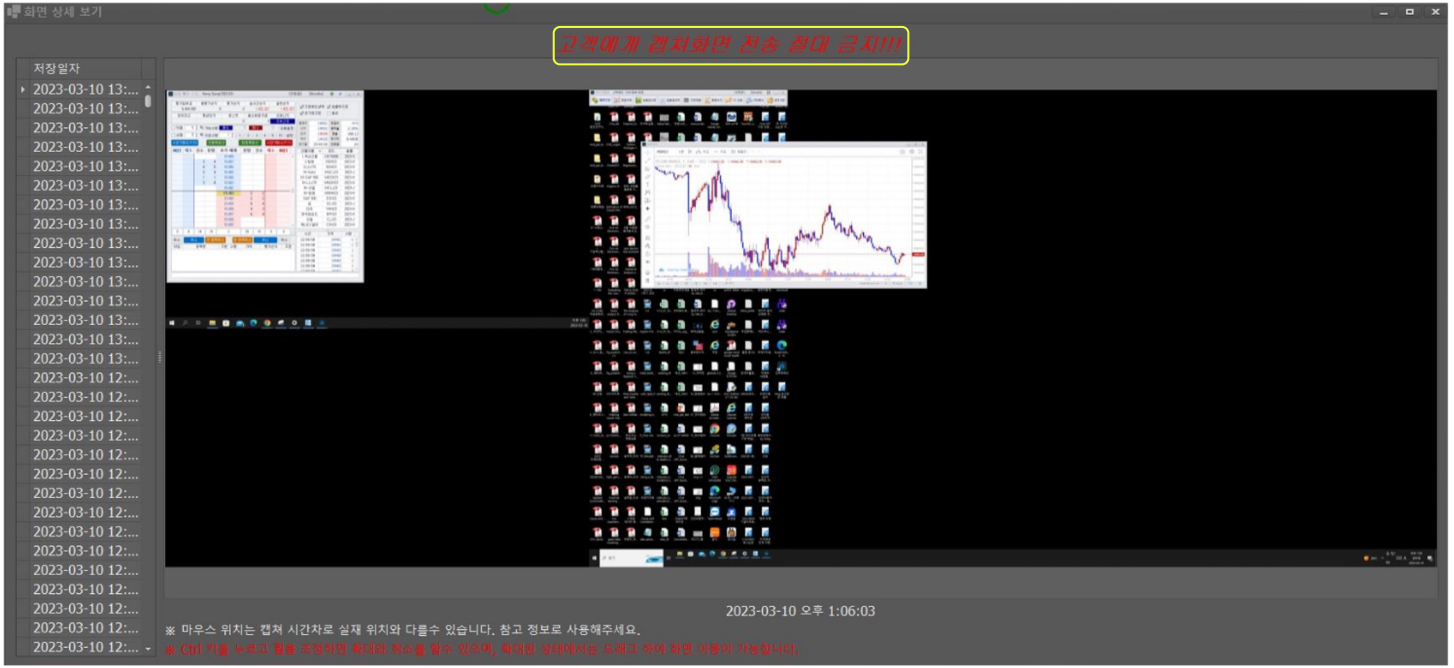
➔ They think they're making an investment



Malicious behavior analysis

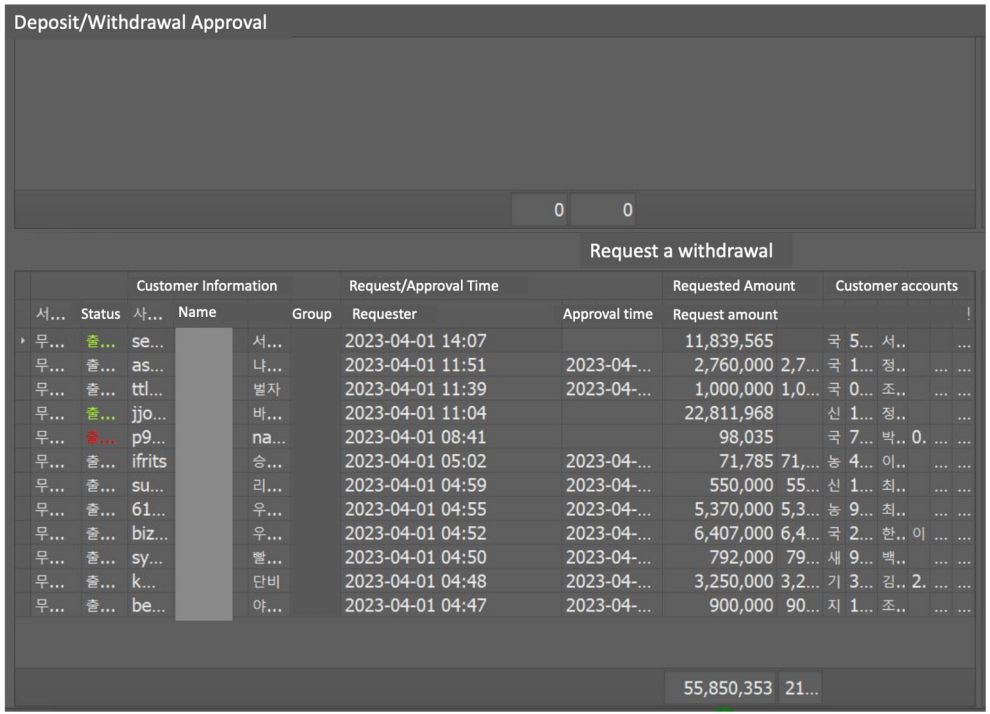
➔ There is someone watching over this

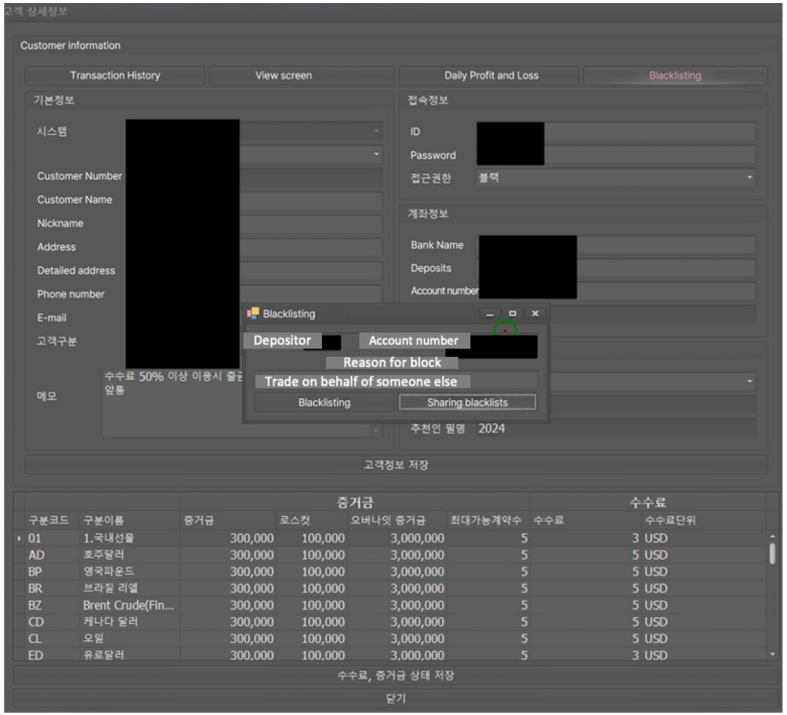
Sending captured screens to customers is absolutely prohibited!!!



Malicious behavior analysis

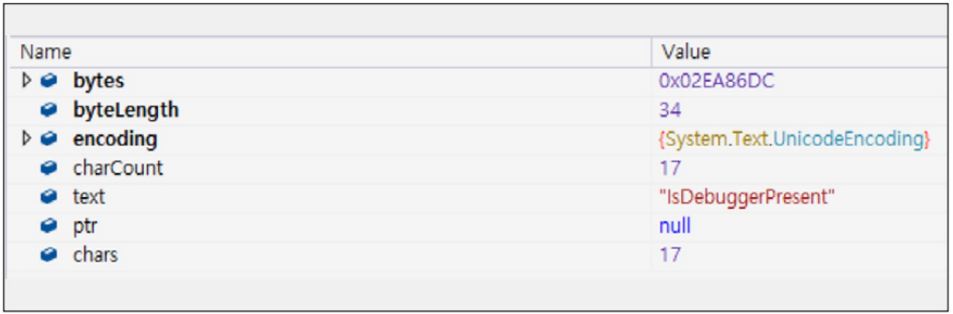
➔ There is someone watching over this

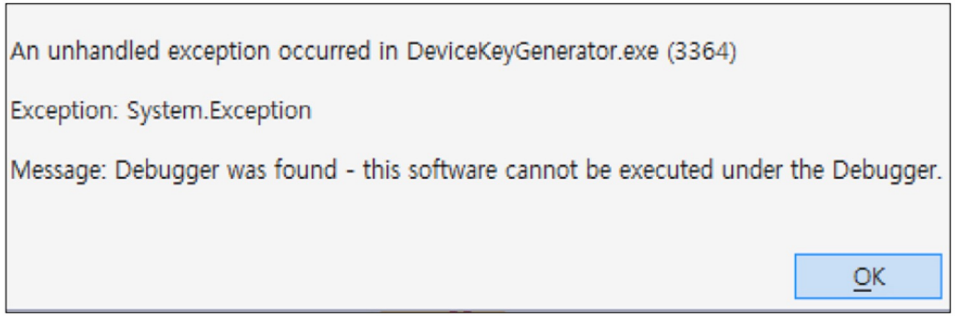




Malicious behavior analysis

➔ There is someone watching over this





Malicious behavior analysis

➔ 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

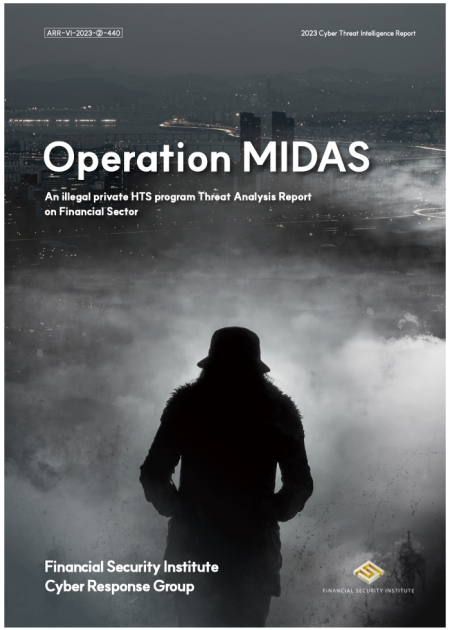
1. Response for Financial Companies

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

Black Hat Europe Sound Bytes

- ➔ **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?

Antiforensic script by ChatGPT

black hat EUROPE 2024
DECEMBER 11-12, 2024
BRIEFINGS

Report Download

Thank you

Financial Security Institute

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