Observation of phishing criminal groups related to illegal money transfers and Mizuho Bank's countermeasures -Fighting against phishing site malware 'KeepSpy'-

みずほ銀行 / Mizuho Bank

みずほフィナンシャルグループ / Mizuho Financial Group

サイバーセキュリティ統括部/Cyber Security Management Dpartment
Tsukasa Takeuchi, Takuya Endo, Hiroyuki Yako

January 22, 2025

ともに挑む。ともに実る。
MIZUHO

発表者紹介 (発表順)

MIZUHO

ともに挑む。
ともに実る。

竹内　司
Tsukasa Takeuchi

Cybercrime

遠藤　拓也
Takuya Endo

Technical

八子　浩之
Hiroyuki Yako

CSIRT

Engineer

西川　昌広　Masahiro Nishikawa

Technical team

近藤　一成　Kazunari Kondo
笹村　直樹　Naoki Sasamura
小山　昌樹　Masaki Koyama

Cybercrime team

森　三千代 Michiyo Mori
堀口　健　Ken Horiguchi
中島　陵太　Ryota Nakashima
中野　嘉寿美　Kasumi Nakano
久世　拓海　Takumi Kuze

Automation Measures

大迫　結花　Yuka Osako
土井　優大　Masahiro Doi

Special thanks

浅谷さん　Asatani-san
常盤さん　Tokiwa-san

In this announcement, we will discuss the challenges and solutions associated with Mizuho Bank's response to phishing.

Background

・Many financial institutions suffered from phishing. Mizuho Bank is also a target.

・Monitoring of illegal money transfers and prevention of damage caused by takedown of phishing sites are being implemented.
Even so, damage will still occur.

Challenges

・There is a limit to monitoring the access of criminals and stopping them immediately, and it is urgent to find phishing sites.
・There's a lot of work to be done in dealing with phishing, and there's a limit to how many people can handle it.

Countermeasure

・Detect phishing sites as quickly and accurately as possible
→Monitoring Phishing Actors Who Spread Fake SMS Using Malware
・Automate some of the responses
→Automate site discovery to takedown

Agenda

1. Current status of phishing damage in Japan
2. Mizuho‘s system and process for dealing with fraudulent transfers and take down phishing sites
3. Phishing targeting Mizuho Bank
4. Malware used by criminal groups sending fake SMS
5. Attempts at early detection of phishing sites
6. Mizuho's Automation Initiatives and Future Direction

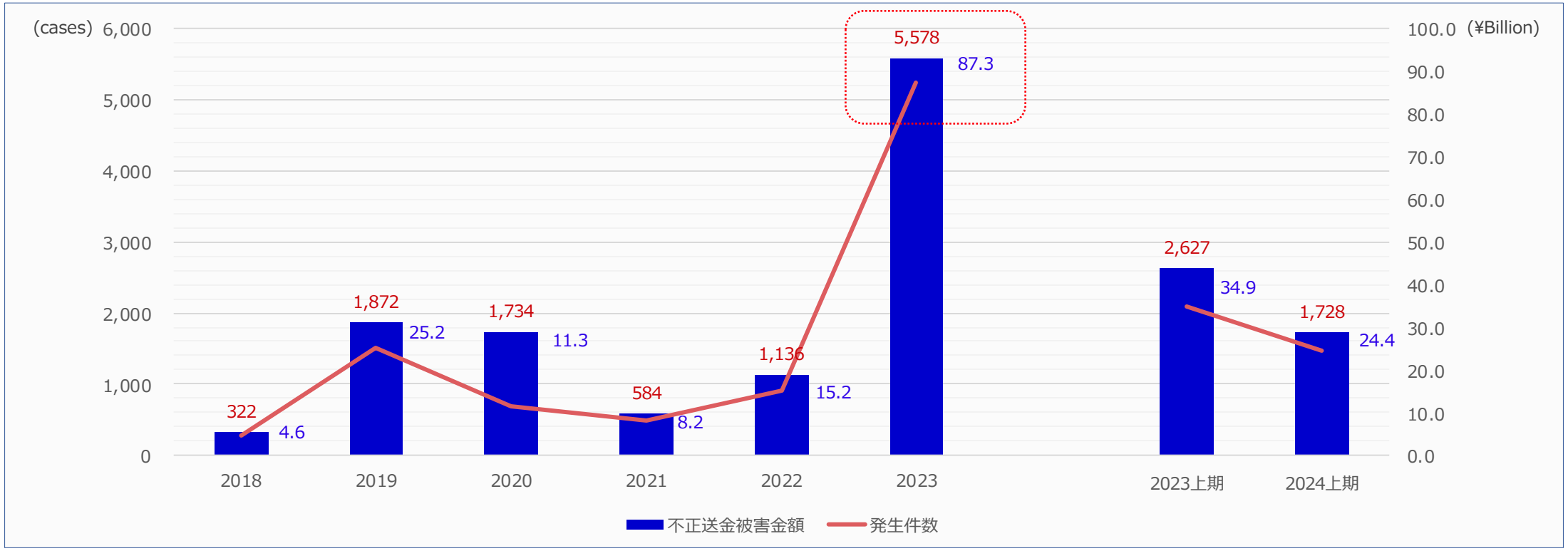
1. Current status of phishing damage in Japan

Current status of phishing damage in Japan

2023	Number of fraudulent internet banking transfers	5,578	Total damage amount	¥8.73 billion ($56 million)

・In 2024, the number of fraudulent remittance losses will increase at a similar pace to the previous year. Various financial institutions continue to be affected.
・Financial institutions that have never been targeted before can also become targets, and it is believed that major damage can occur if the response to phishing is delayed.
・However, there is no silver bullet to combat phishing, and it is necessary to combine and implement multiple various countermeasures.

As one such countermeasure, a reference case will be explained on the following pages.



【 National Police Agency :令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について】

2. Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

First, before I go into the details, in order to make the content easier to understand,
I would like to explain the roles of each department within the bank, something that is not often discussed outside the company.

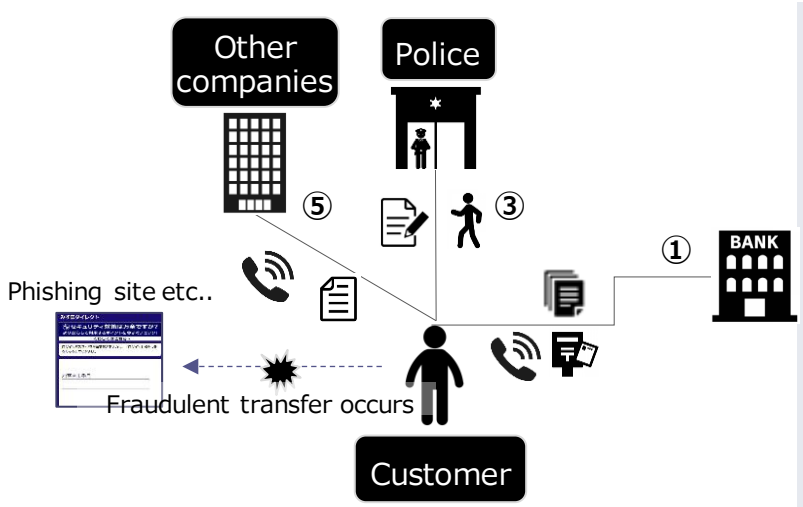
Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

Mizuho has three departments and two centers that are primarily involved in responding to and taking measures against fraudulent transfers.

1. The department that handles internet banking and its monitoring (the department in charge of Mizuho Direct) and its call center
2. The financial crime countermeasures department (compliance division) and its call center that considers customer warnings and compensation, etc.
3. The Cybersecurity Management Department that handles phishing sites and cybercrime across the board

The reception and response process at Mizuho when a fraudulent transfer occurs is as follows

① The call center (Direct Banking Center) calls the customer (or the customer calls the call center).
② The customer checks the status of deposits and withdrawals and their account. If there is a suspicious transfer, the Direct Banking Center will conduct a detailed interview with the customer.
③ In parallel with ②, the customer consults the police.
④ Once it is confirmed that the transfer is fraudulent, responsibility is transferred to the Security Support Center of the Compliance Department, which considers whether compensation is necessary and conducts a more detailed investigation.
⑤ In parallel with ① to ③ above, if there is a possibility that passwords, PINs, etc. may have been leaked, the customer will also contact other companies (other banks or credit card companies).



Internet Banking Department

Damage report・Monitoring

Direct Banking Center

② Call Reception・IB-Account Suspension

Compliance Department

Compensation review/Website announcement

Security Support Center

④ Consideration of compensation・Suspension of account

Cyber Security Department

Phishing site response
Unauthorized access investigation

Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

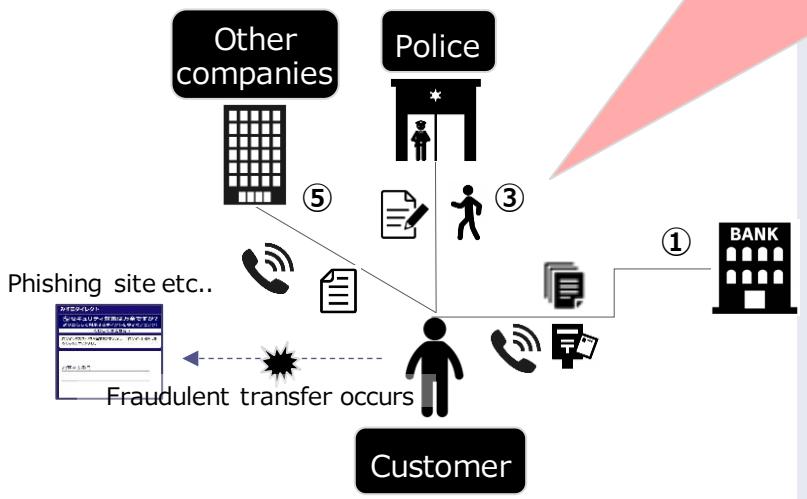
Mizuho has three departments and two centers that are primarily involved in responding to and taking measures against fraudulent transfers.

1. The department that handles internet banking and its monitoring (the department in charge of Mizuho Direct) and its call center
2. The financial crime countermeasures department (compliance division) and its call center that considers customer warnings and compensation, etc.
3. The Cybersecurity Management Department that handles phishing sites and cybercrime across the board

The reception and response process at Mizuho when a fraudulent transfer occurs is as follows

① The call center (Direct Banking Center) calls the customer (or the customer calls the call center).
② The customer checks the status of deposits and withdrawals and their account. If there is a suspicious transfer, the Direct Banking Center will
③ In parallel with ②, the custome
④ Once it is confirmed that the tra ter of the Compliance Department, which conside sation is necessary and conducts a more detailed investigation.
⑤ In parallel with ① to ③ above, if there is swords, PINs, etc. may have been leaked, the customer will also contact other companies (other banks d compa es).

One fraudulent remittance case incurs a large burden and cost for both the customer and the bank.



Internet Banking Department

Damage report・Monitoring

Direct Banking Center

② Call Reception・IB-Account Suspension

Compliance Department

Compensation review/Website announcement

Security Support Center

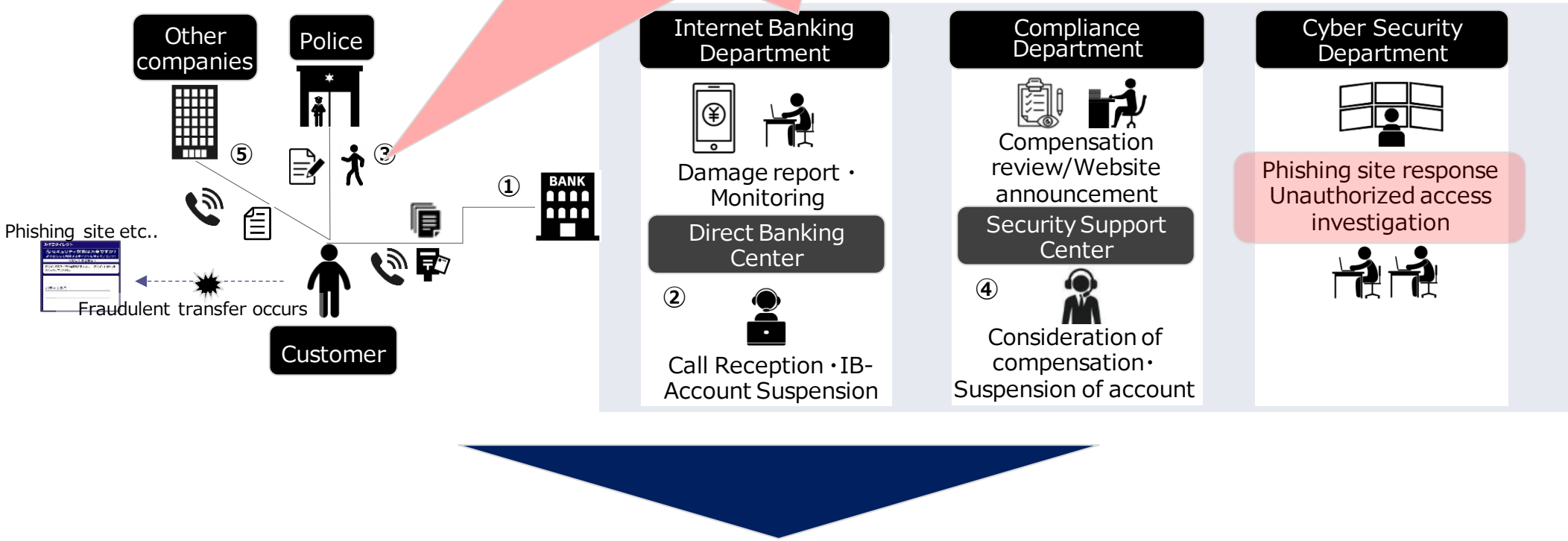
④ Consideration of compensation・Suspension of account

Cyber Security Department

Phishing site response
Unauthorized access investigation

Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

One fraudulent remittance case incurs a large burden and cost for both the customer and the bank.



Therefore, it is necessary to destroy the phishing sites (phishing crimes) that cause these fraudulent remittances.

Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

Projection Only

Projection Only

Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

Countermeasures against phishing sites can be categorized into detection, response (takedown), and management. The specific measures are as follows:

Detection

- Anti-phishing vendors
- SNS monitoring (X, etc.)
- Threat intelligence tools
- External agencies such as JC3
- Intranet suspicious email monitoring
- Post Blog
- Domain/IP address monitoring
- URLScan (Brand monitoring)
- Customer web contact point (reports from)
- Malware communication monitoring

Response

Outside

- Obtain screenshots and source code
- Contact your hosting provider
- Contact your domain registrar
- Apply to browser providers such as Google Safe-Browsing
- Apply to security providers such as Trendmaicro and Netcraft
- Link with JC3, etc.

Inside

- Analyze phishing sites
- Introduce dummy accounts
- Analyze unauthorized access
- Contact relevant departments
- Notify customers
- Check phishing emails/SMS (in person)
- (Register blacklist)
- (Change/strengthen monitoring rules)

Management

- Identifying the number of phishing sites
- Monitoring the distribution status of emails/SMS
- Monitoring the status of phishing sites
  →Checking domain status
  Checking whether a site can be accessed from a mobile device

Cyber Security Department

Phishing site response
Unauthorized access investigation

Mizuho's system and process for dealing with fraudulent transfers and take down phishing sites

Countermeasures against phishing sites can be categorized into detection, response (takedown), and management. The specific measures are as follows:

Detection

- Anti-phishing vendors
- SNS monitoring (X, etc.)
- Threat intelligence tools
- External agencies such as JC3
- Intranet suspicious email monitoring
- Post Blog
- Domain/IP address monitoring
- URLScan (Brand monitoring)
- Customer web contact point (reports from)
- Malware communication monitoring

Response

Outside

- Obtain screenshots and source code
- Contact your hosting provider
- Contact your domain registrar
- Apply to browser providers such as Google Safe-Browsing
- Apply to security providers such as Trendmaicro and Netcraft
- Link with JC3, etc.

Inside

- Analyze phishing sites
- Introduce human accounts
- Analyze unauthorized access
- Contact relevant departments
- Notify customers
- Check phishing emails/SMS (in person)
- (Register blacklist)
- (Change/strengthen monitoring rules)

Management

- Identifying the number of phishing sites
- Monitoring the distribution status of emails/SMS
- Monitoring the status of phishing sites
  →Checking domain status
  Checking whether a site can be accessed from a mobile device

It requires 24/7 support, and there's a lot to do, so it's pretty tough...

Cyber Security Department

Phishing site response
Unauthorized access investigation

3. Phishing targeting Mizuho Bank

Phishing targeting Mizuho Bank

It is believed that there are multiple groups that set up phishing sites and make fraudulent transfers.
The sites are slightly different, and each has its own differences and characteristics in the methods they use to make fraudulent transfers.
Examples:
- A group of criminals whose phishing sites are messy and full of typos.
- A group of criminals who are particular about site design and are diligent in their research.
- A group that lures users by email, a group that lures users by SMS, etc.

Among them, Group 3, which is still successfully making large amounts of fraudulent transfers using SMS, is particularly troublesome, and countermeasures are urgently needed.

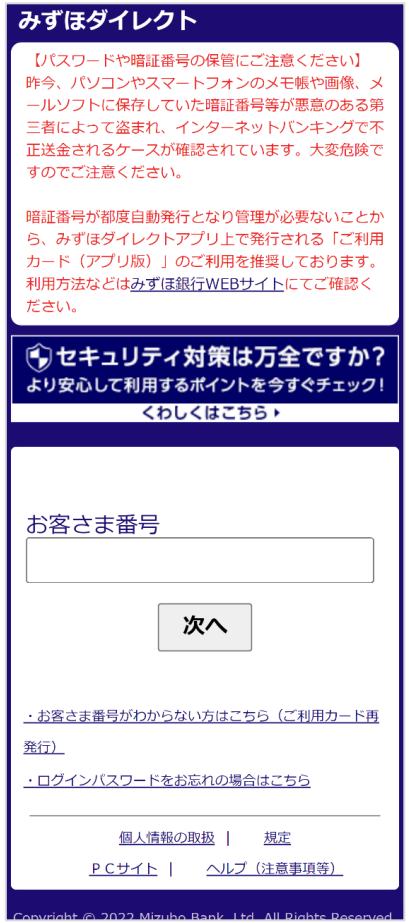
【Examples from 2024】 *: Japan Cybercrime Control Center

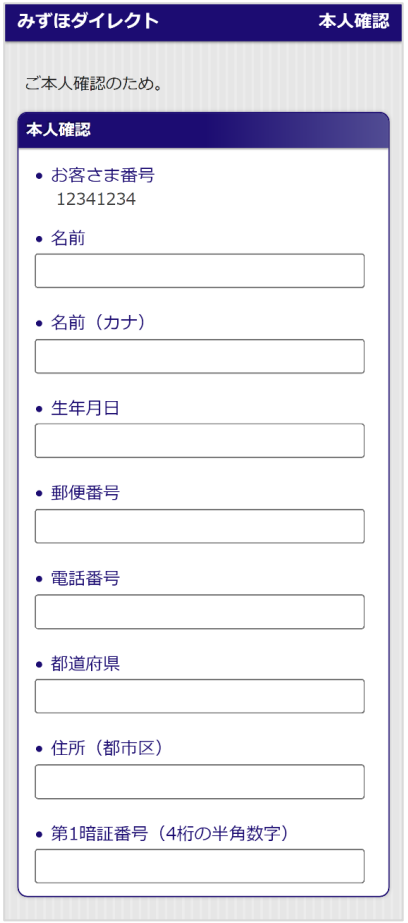
Group	Classification in JC3*	Banks that were confirmed to have been targeted	Main outgoing infrastructure	Non-Bank
Group 1	CP29	Mizuho Bank, Mitsubishi UFJ Bank, PayPay Bank, Mitsui Sumitomo Bank	Email	Apple、auID、Mercari, ETC, Kurashitepco
Group 2	UKN 432	Mizuho Bank	Email	
Group 3	BP1	Mizuho Bank, Mitsubishi UFJ Bank, Mitsui Sumitomo Bank	SMS	auID, Docomo, Kurashitepco
Group 4	CP20	Mizuho Bank, GMO Aozora Net Bank, Mitsubishi UFJ Bank, Rakuten Bank, Resona Bank, Sony Bank	Email	Amazon、MasterCard, Mercari, Rakuten Card

On the following pages, we will explain the details of each group and site in order of occurrence.

Phishing targeting Mizuho_Group 1_CP29 (March and June 2024)

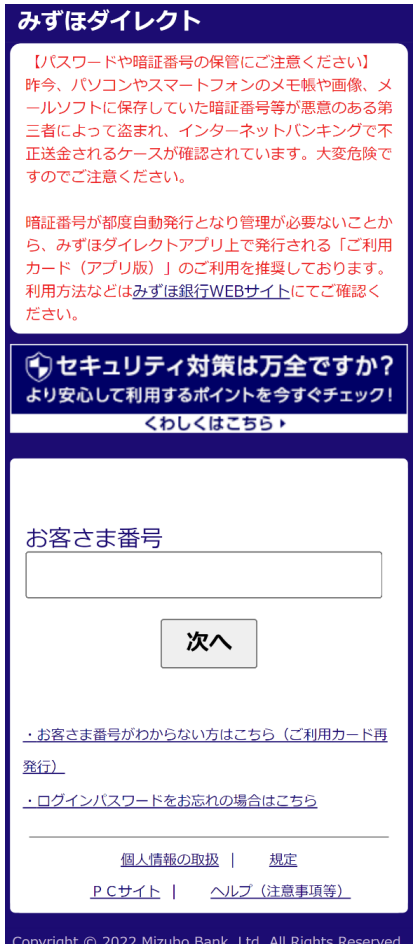
The main spreading method	**Email (and SMS?)**	**Site Features**	The screen is carefully crafted	**Example URL**	hxxps://direct.mizuho-helpdisk.is hxxps://www.index-cr-mizu.cc hxxps://www.index-web-ib-mizuho.is hxxps://www.index-webib-mizuho.online
Type	**Real time**	**Others**	・This group has been appearing in large numbers at our bank since the summer of 2023. Many damages caused by this group have been confirmed at Japanese banks. ・They have shifted from using .info and .net domains to mainly using ".is". ・The number of URLs launched is small, but highly destructive ・Many methods are used to take over apps on the criminals' devices.	Registrar (Registry)	isnic.is.etc…
Frequency of occurrence	**High**				

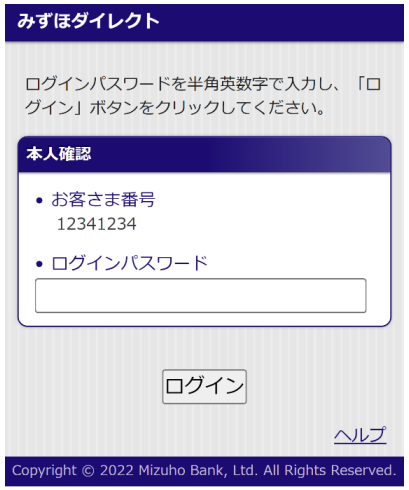


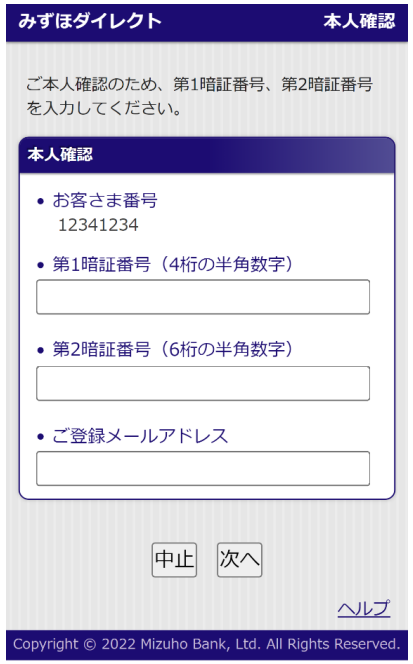


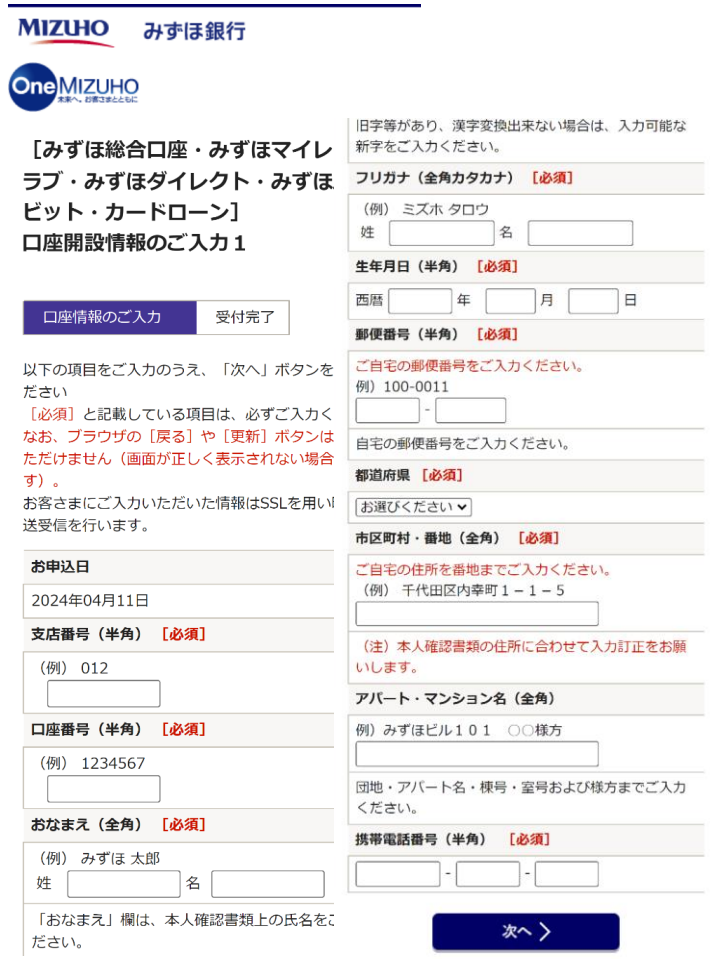
Phishing targeting Mizuho_Group 2_UKN432 (April 2024)

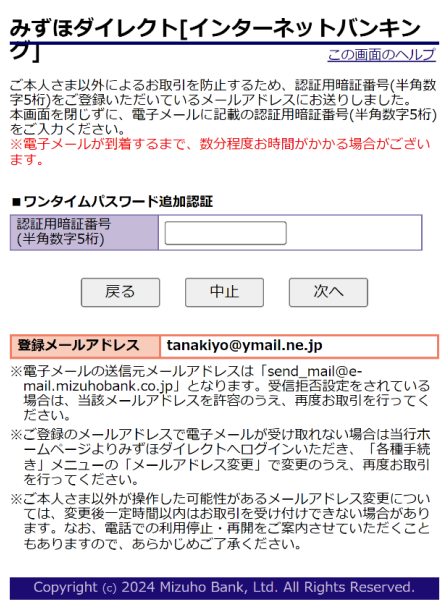
The main spreading method	**Email**	**Site Features**	・Real-time type where the page transitions based on the actual response of internet banking	**Example URL**	hxxps://web.ib.mazizuzsfshodbank.co.jp.findhighpower.com/ hxxps://web.ib.mazizuzsfshodbank.co.jp.wowpalmbay.com
Type	**Real time**	**Others**	・A new group that emerged on 4/11. There are other similar groups, but the site construction code is different, so it is assumed that the perpetrators are a different group. ・The registrar is GMO, and the name server is A.SSHARE-DNS (Gname), making it relatively easy to compromise.	Registrar (Registry)	GMO INTERNET,INC etc...
Frequency of occurrence	**Low**				





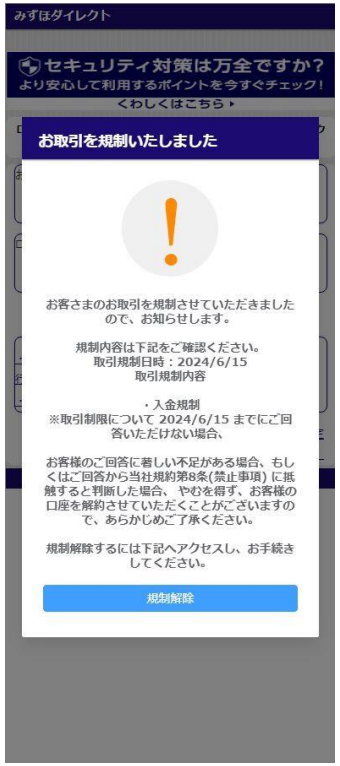


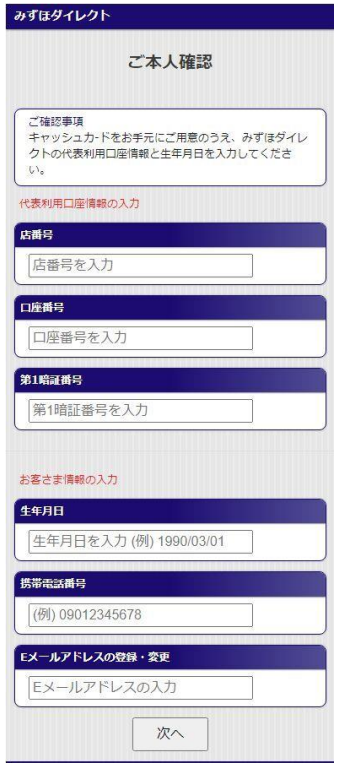


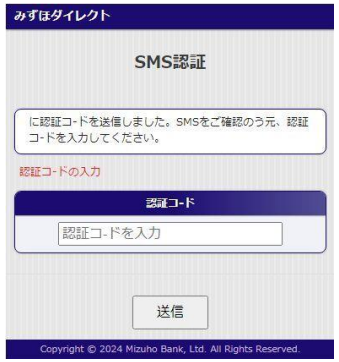


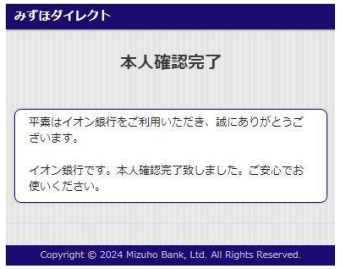
Phishing targeting Mizuho_Group 3_BP1 (Around June 2024)

The main spreading method	**SMS(MW:KeepSpy)**	**Site Features**	・Attackers use duckdns, which allows free subdomain generation (mass generation possible and hard to crash) ・Phishing sites display an exclamation mark「！」on the top screen to avoid GSB and other methods	**Example URL**	hxxps://feyusb6.duckdns.org hxxps://gfpbq452s.duckdns.org
Type	**Real time**	**Others**	・Many cases of criminals taking over customers' Direct apps on their own devices ・Criminals change registered email addresses for Direct ・This scam has wreaked havoc at a certain bank, and is said to have caused large-scale fraudulent transfer damage around 2023	Registrar (Registry)	duckdns.org etc..
Frequency of occurrence	**High**				









Phishing targeting Mizuho_Group 3 (revisited)_BP1 (Around June 2024)

The main spreading method	SMS(MW:KeepSpy)
Type	Real time
Frequency of occurrence	High

Site Features	・Attackers use duckdns, which allows free subdomain generation (mass generation possible and hard to crash) ・Phishing sites display an exclamation mark「！」on the top screen to avoid GSB and other methods
Others	・Continued from the previous page. Originally, there was no screen to enter a “second PIN”, but since our bank immediately implemented measures to prevent the app from being hijacked, we have now prepared a screen for entering a "second PIN" so that you can transfer money immediately.

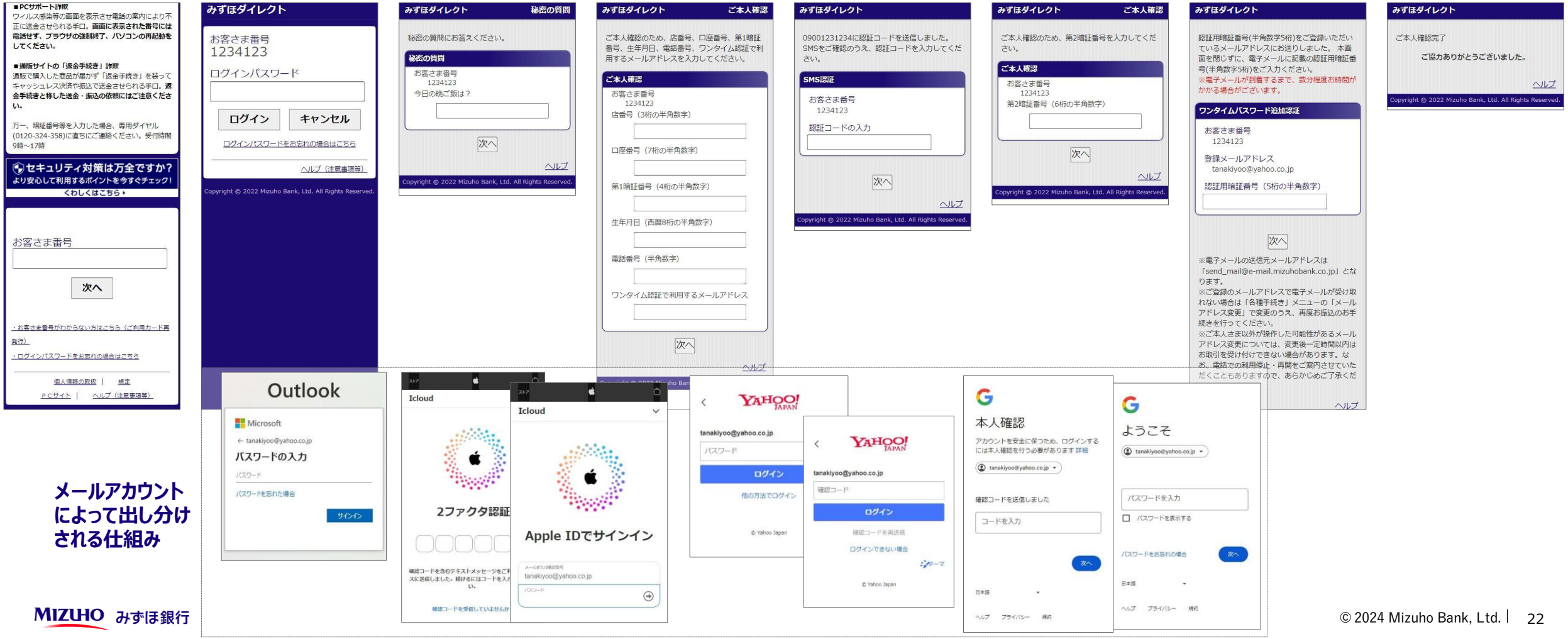
Example URL	hxxps://uv2r90.duckdns.org hxxps://mzgel01.duckdns.org
Registrar (Registry)	duckdns.org etc..

Phishing targeting Mizuho_Group 4_CP20 (August 2024)

The main spreading method	Email
Type	Real time
Frequency of occurrence	High

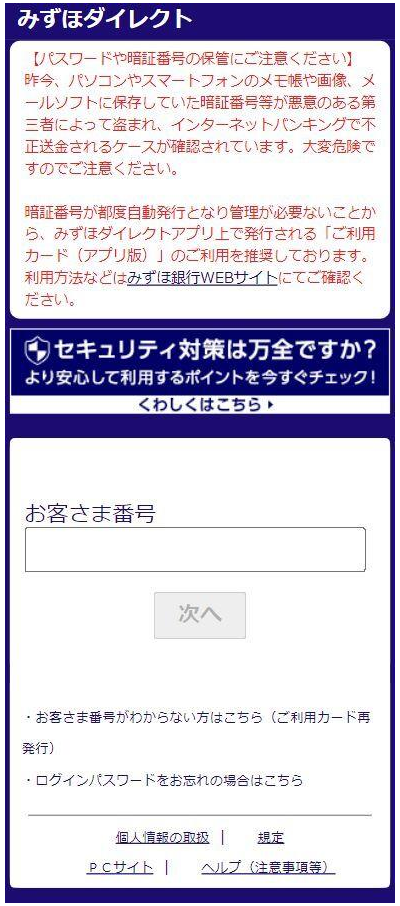
Site Features	・Originally, the group's main crime was the accumulation type, but from around 2023, they also started using the real-time type ・Added a new screen aimed at hijacking email accounts to steal email OTPs
Others	・The attacks are believed to have been occurring since around September 2022 ・Various domains use different character strings (from long to short)

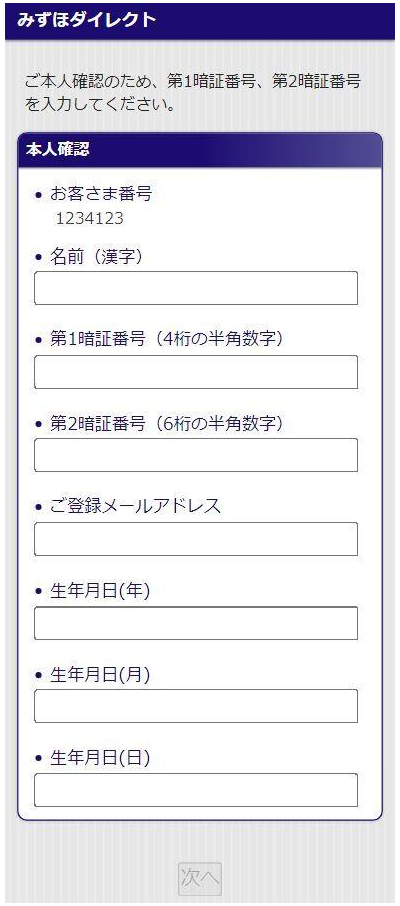
Example URL	hxxps://cdshyj.com hxxps://dizichina.com Hxxps://qigehangmo.com
Registrar (Registry)	Gname.com Pte. Ltd.等

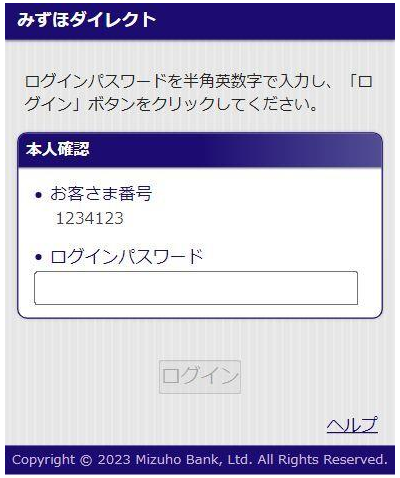


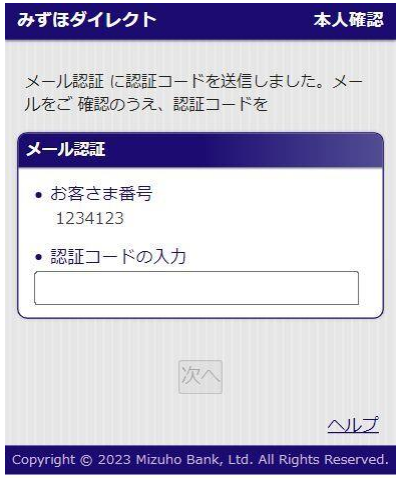
メールアカウントによって出し分けされる仕組み

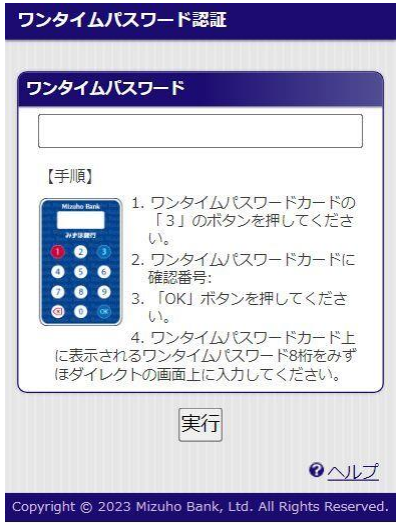
Reference: BP5_December 2024, which occurred while this manuscript was being prepared

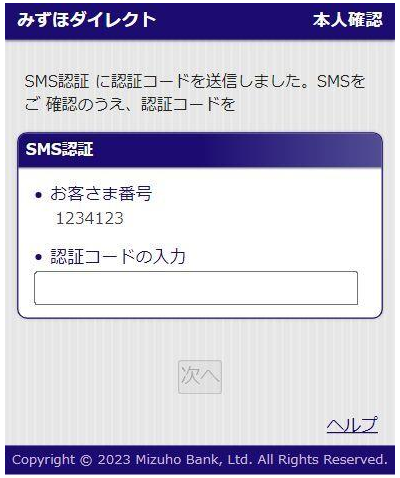




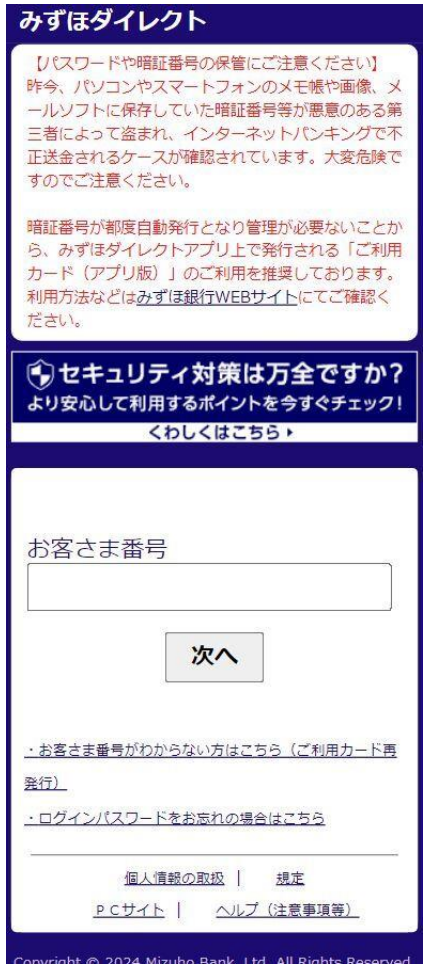


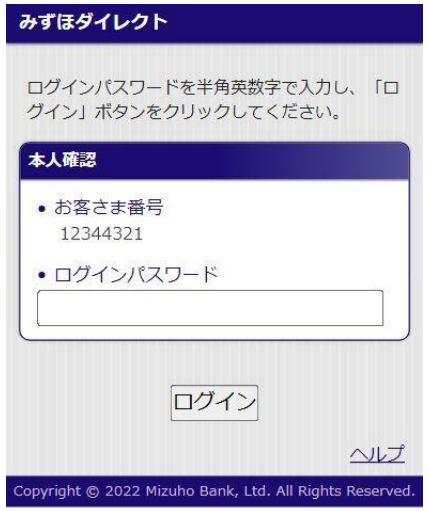


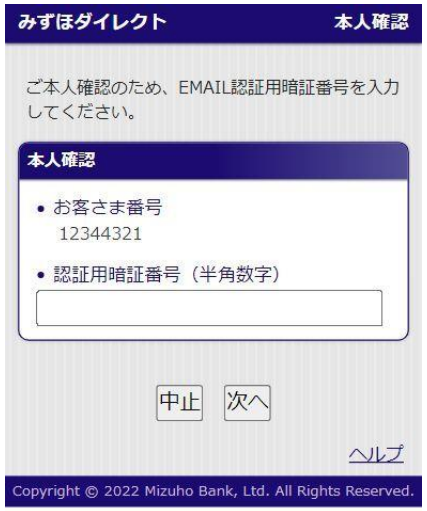


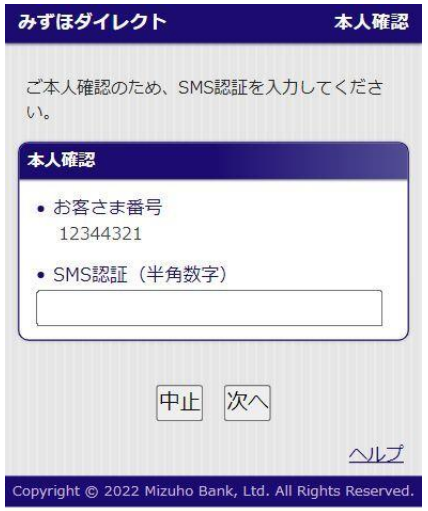


Reference: CP29_December 2024, which occurred while this manuscript was being prepared









Reference: Environmental information when phishing criminals access the site

Projection Only

Projection Only

Projection Only

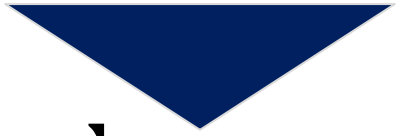
Reference: Phishing victim around June 2024②

Projection Only

Projection Only

【Issues】

- There are limitations to monitoring the criminal's access and immediately suspending the victim's account
- There is a lot of work that needs to be done, and there are limitations to the manpower available to deal with it.

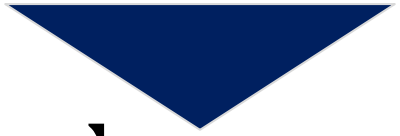


【Countermeasures】

- Detect phishing sites as soon as possible
- Automate some of the response

【Issues】

- There are limitations to monitoring the criminal's access and immediately suspending the victim's account
- There is a lot of work that needs to be done, and there are limitations to the manpower available to deal with it.



【Countermeasures】

- Detect phishing sites as soon as possible
- Automate some of the response

4． Malware used by criminal groups sending fake SMS

Motivation for the investigation

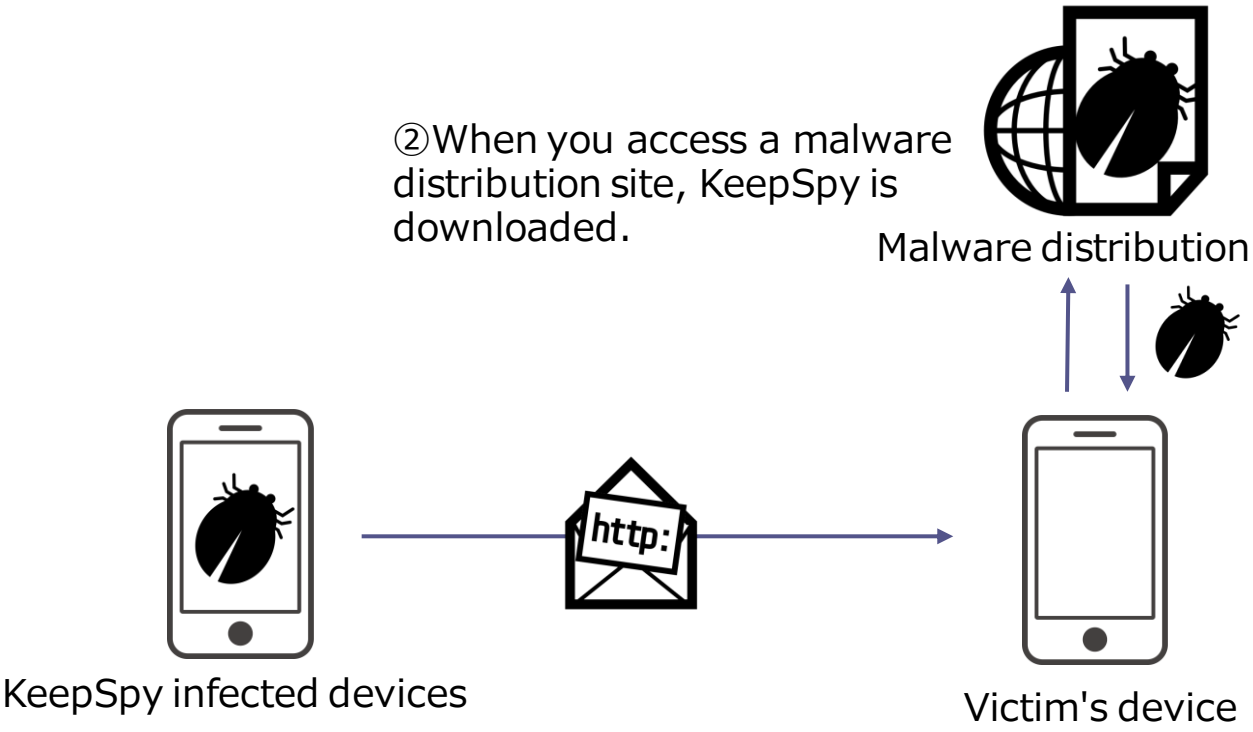
- **Background**
  - While the amount of damage caused by phishing is increasing year by year, phishing damage caused by SMS masquerading as a bank is particularly serious.
  - We need to be able to detect phishing sites using this method early on.
  - We rely on postings by well-intentioned fish hunters on X (formerly Twitter) to detect phishing sites and take them down, and we felt that the system of relying on other companies (other banks) was unstable.

- **the purpose**
  - We will analyze KeepSpy, which is used to send SMS impersonating banks, and investigate phishing sites, aiming to detect the launch of phishing sites early.

<Reference> Posted by a well-intentioned fish hunter

About KeepSpy

- **Overview**
  - Mobile malware primarily targeting Android devices.
- **Transmission**
  - They mainly pose as telecommunications carriers and direct users to malware distribution sites via links contained in SMS messages, where they disguise themselves as offering legitimate security software for download, and encourage victims to download and install it, thereby infecting the user.

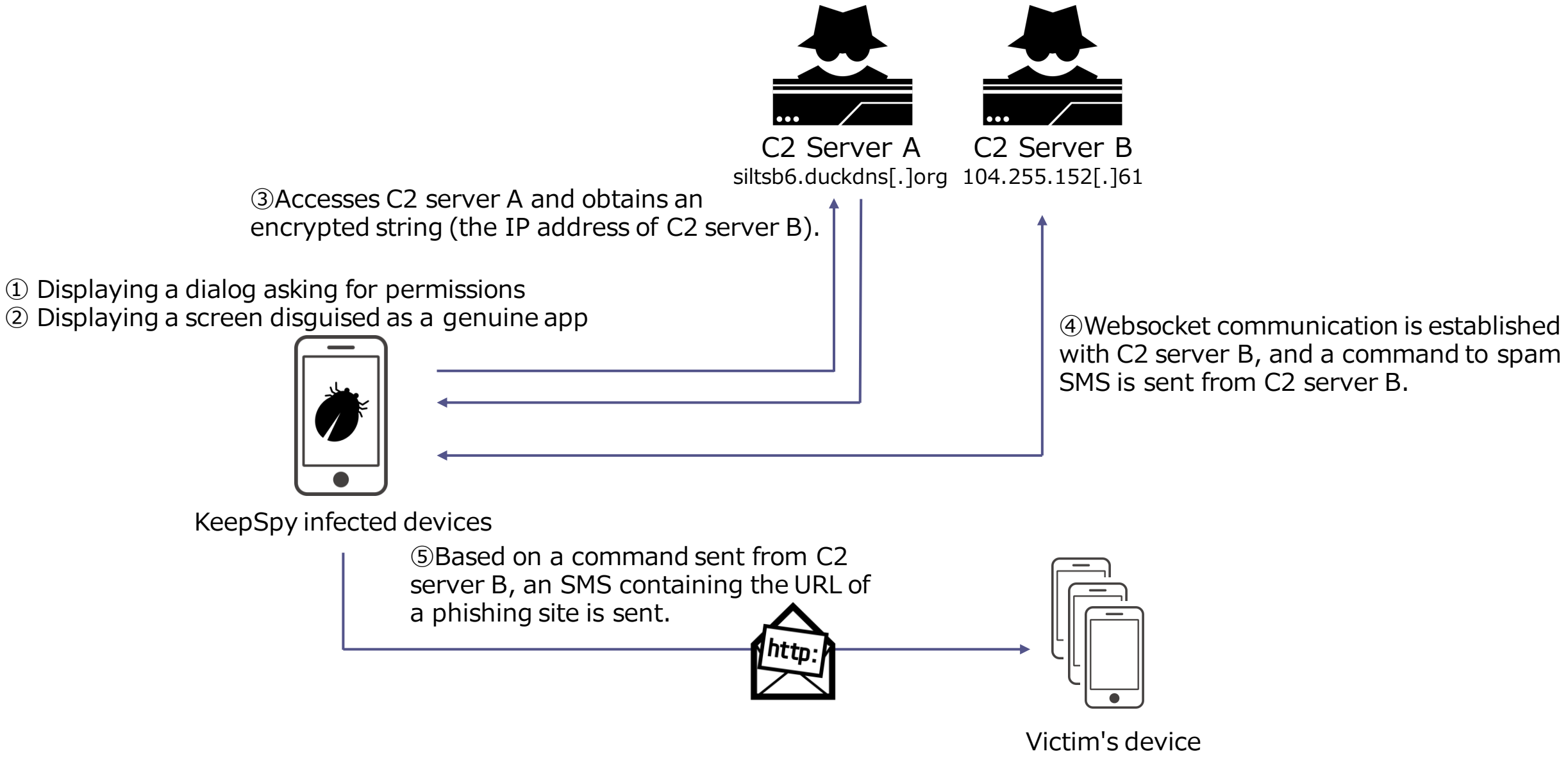


<Example> Spoofing Docomo and having security software installed.

KeepSpy samples used for analysis

Item	Value
File name	DOC2024.apk
Hash(SHA256)	66b118b5c63a3c8e30941b2e620211d04febbb21e3c90feb1f283b0b598fb46c
Icon Image	
First Submission (VirusTotal)	2024-05-09 02:23:38 UTC

<Analysis results: Overall picture>The mechanism from KeepSpy infection to sending SMS



<Analysis results: details> KeepSpy on-screen behavior

① Displaying a dialog asking for permissions

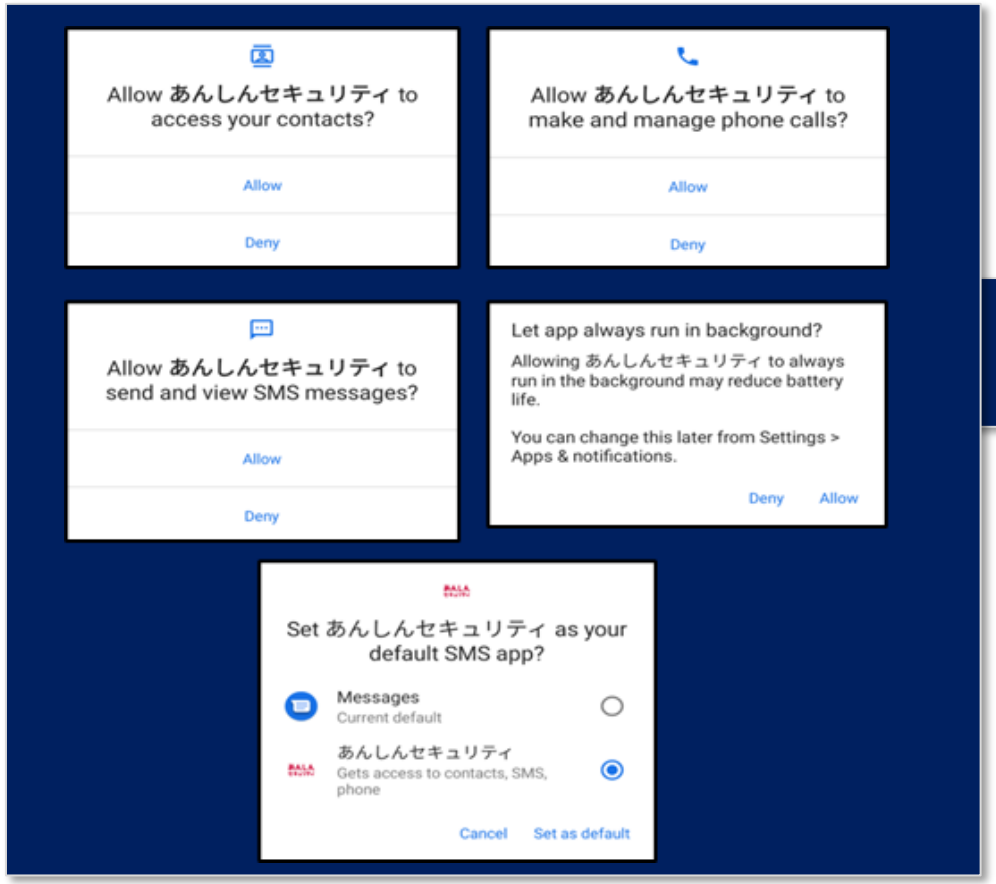
・Access to contacts

・Call management

・Send and display SMS messages

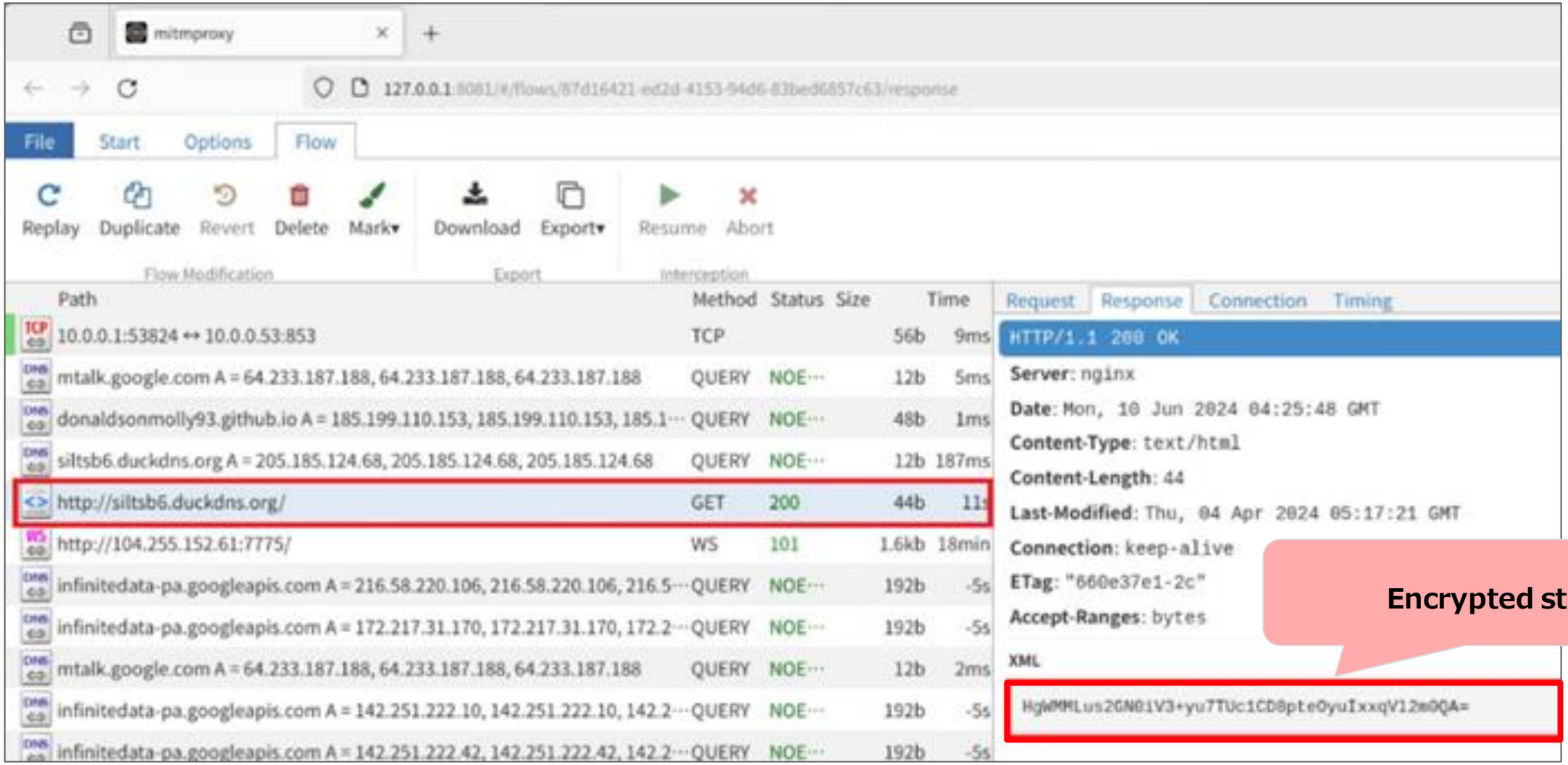
・Change of SMS application

・Continuously running in the background



②A screen similar to the original “あんしんセキュリティ" screen is displayed.
There is no change in behavior no matter where you tap.

③Access C2 server A and obtain the encrypted string (IP address of C2 server B).



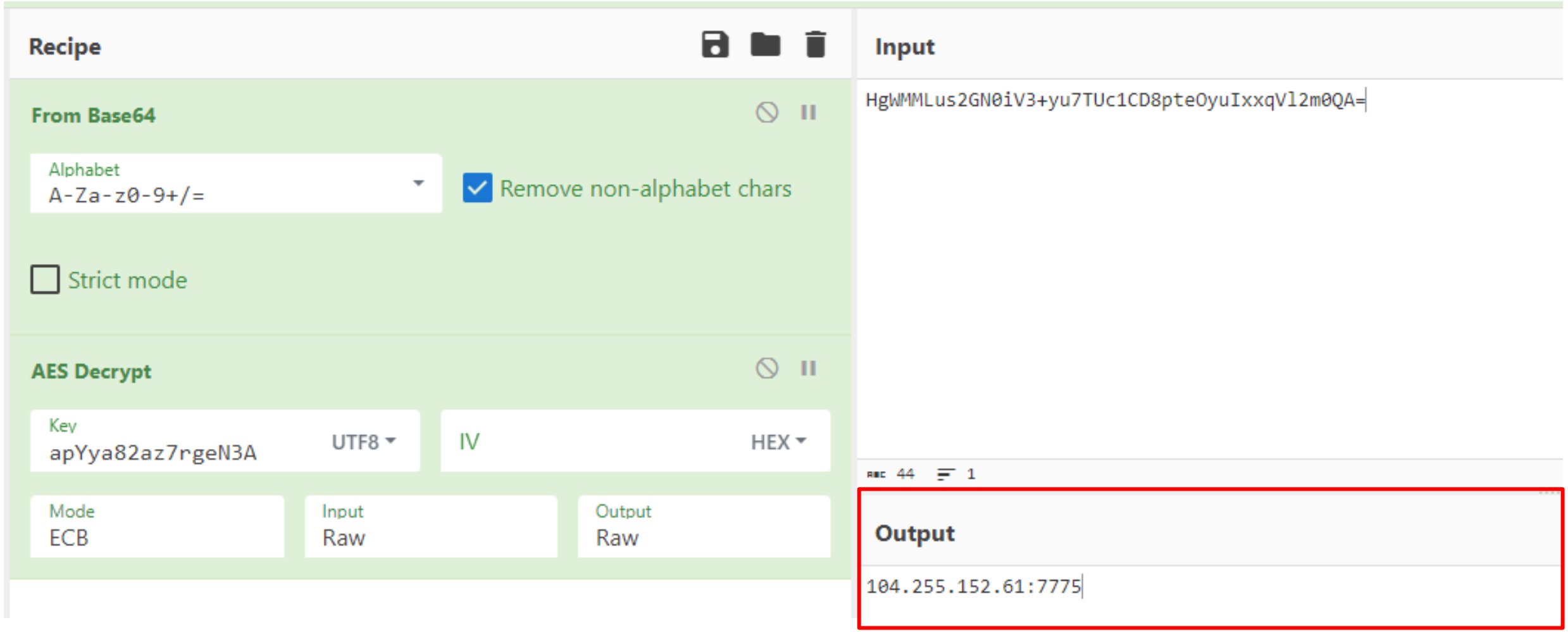
About decrypting the IP address of C2 server B

- Using Base64 and AES, decode the string received from C2 server A and obtain the IP address of C2 server B.
- The encryption method and private key are obfuscated and hard-coded in the source code.

```
public static String gjqbrbweff(String str) {
    try {
        byte[] decode = Base64.decode(str, 2);  ←Base64Decode
        Cipher cipher = Cipher.getInstance(f4411bkrdrfezfl);  ←"AES/ECB/PKCS5Padding"(Encryption method)
        String str2 = f4412dwygyiog;  ←"apYya82az7rgeN3A"(key)
        String str3 = f4416wxyvgvzr;  ←"0"(Padding Value)
        int length = str2.length();
        if (length < 16) {
            StringBuilder sb = new StringBuilder();
            sb.append(str2);
            for (int i = 0; i < 16 - length; i++) {
                sb.append(str3);
            }
            str2 = sb.toString();
        }
        Charset charset = f4413fwpstitn;
        cipher.init(2, new SecretKeySpec(str2.getBytes(charset), f4415hepjaxvtj));
        return new String(cipher.doFinal(decode), charset);  ← Timing of final decoding
    } catch (Exception e) {
        e.printStackTrace();
        String str4 = f4414gjqbrbweff;
        Log.e(str4, str4 + e);
        return null;
    }
}
```

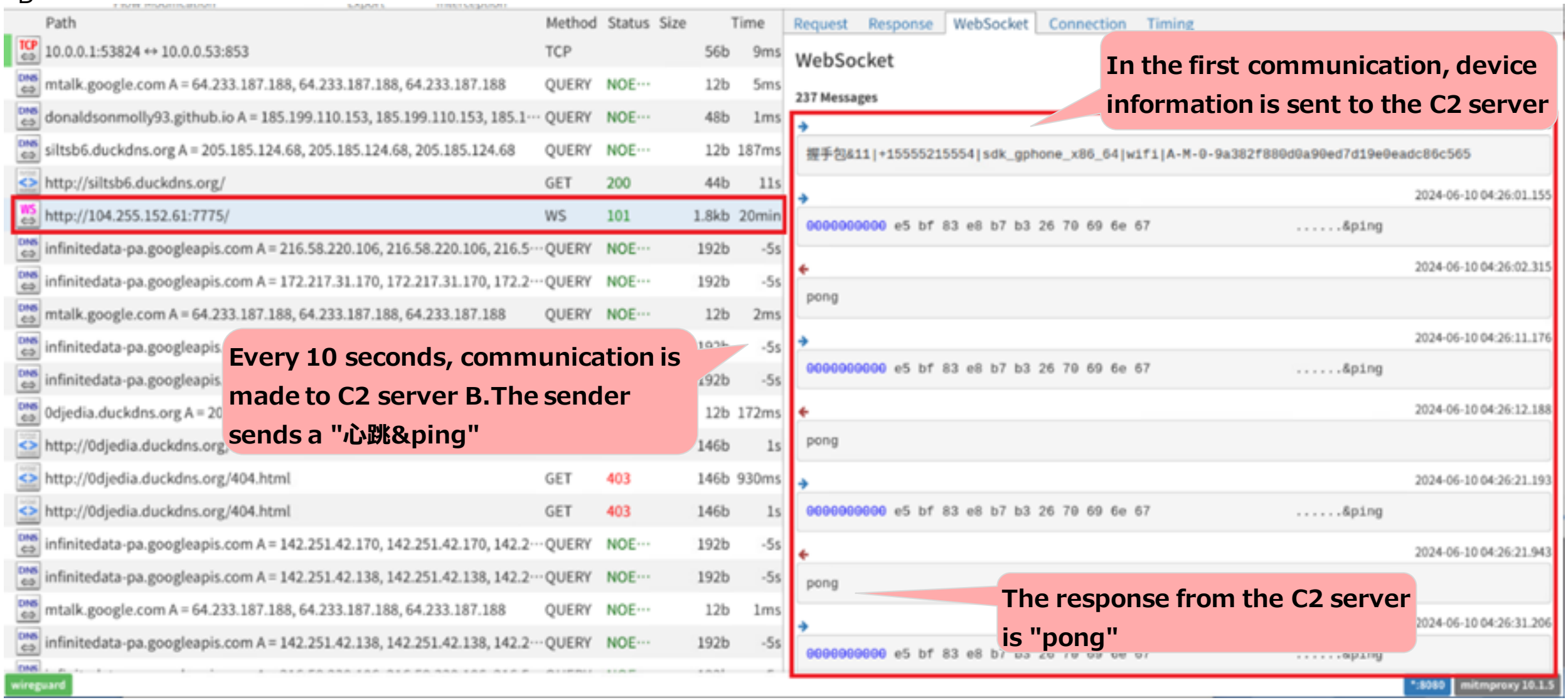
About decrypting the IP address of C2 server B

The decryption result by CyberChef is as follows:



Dynamic Analysis of KeepSpy

④Establishes websocket communication with C2 server B (http[:]//104.255.152[.]61:7775/) and receives commands from C2 server B

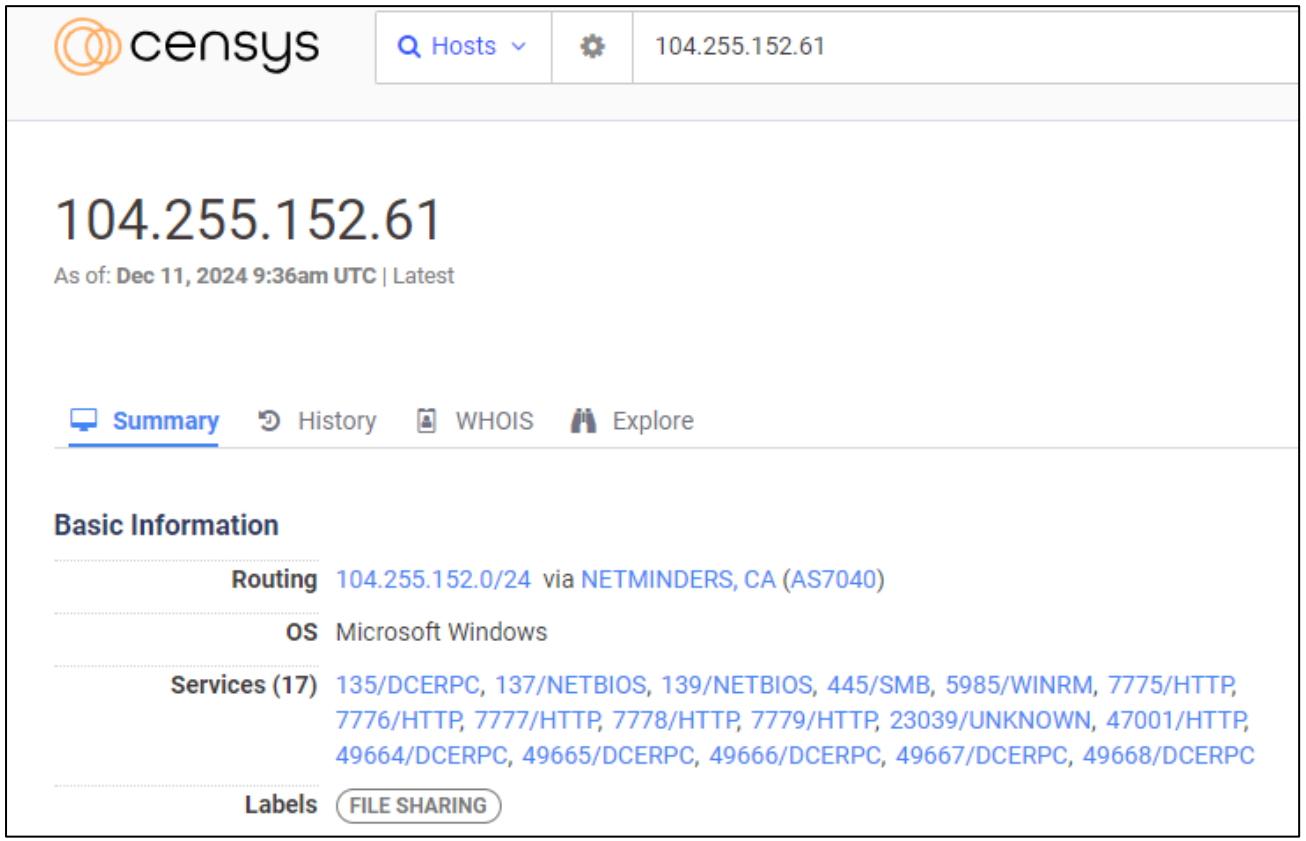


The commands that may be received from C2 server B are as follows.
(Since the operation has not been verified, the specific operation is unconfirmed)

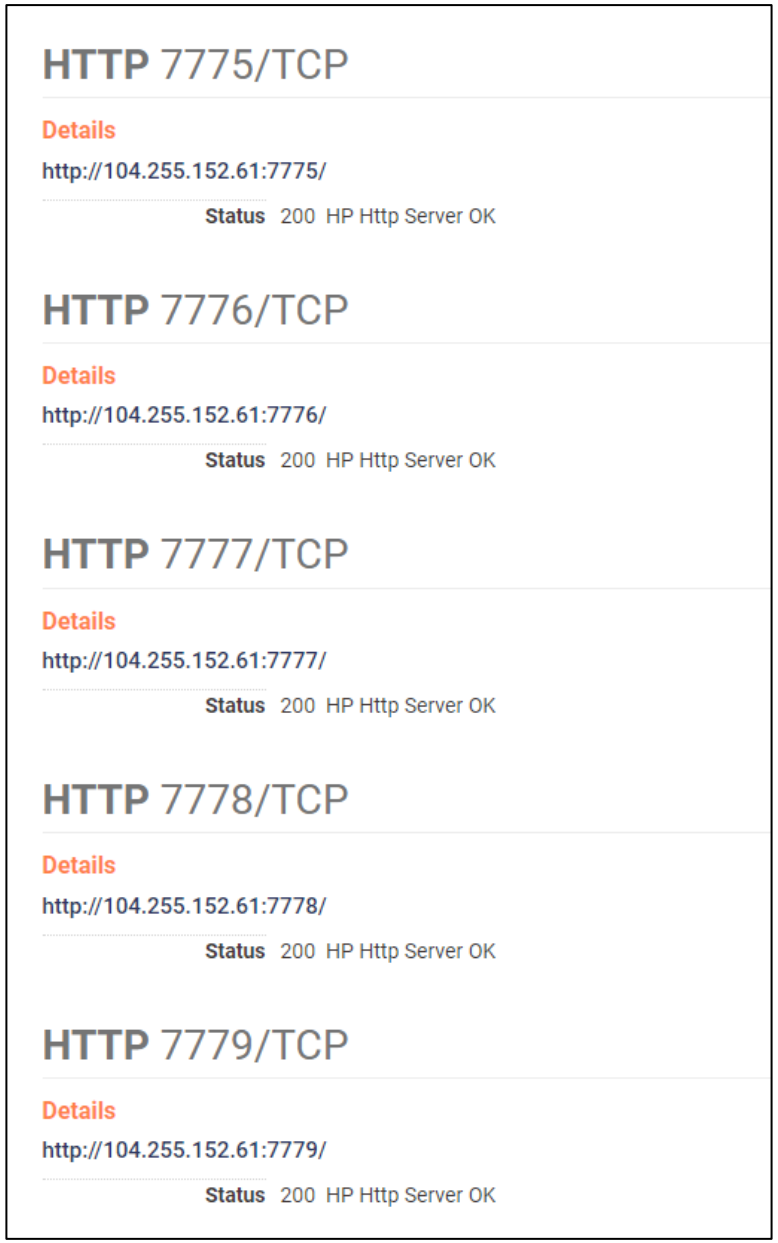
Command	English Translation
通讯录	Telephone directory
收件箱	Inbox
拦截短信&open	Intercept SMS&open
拦截短信&close	Intercept SMS&close
发信息&	Send message
清除短信&	Clear SMS
普通通知栏&	Ordinary notification bar
通知栏&	Notification bar
应用列表&	Application list
更新&	Update

About KeepSpy's C2 server B

The results confirmed using Censys* are as follows.
In addition to port 7775, ports 7776, 7777, 7778, and 7779 are available,
and the response for ports 7775 to 7779 is the same as "HP Http Server OK".
→**<u>Similar commands are expected to be returned from ports 7776 to 7779.</u>**



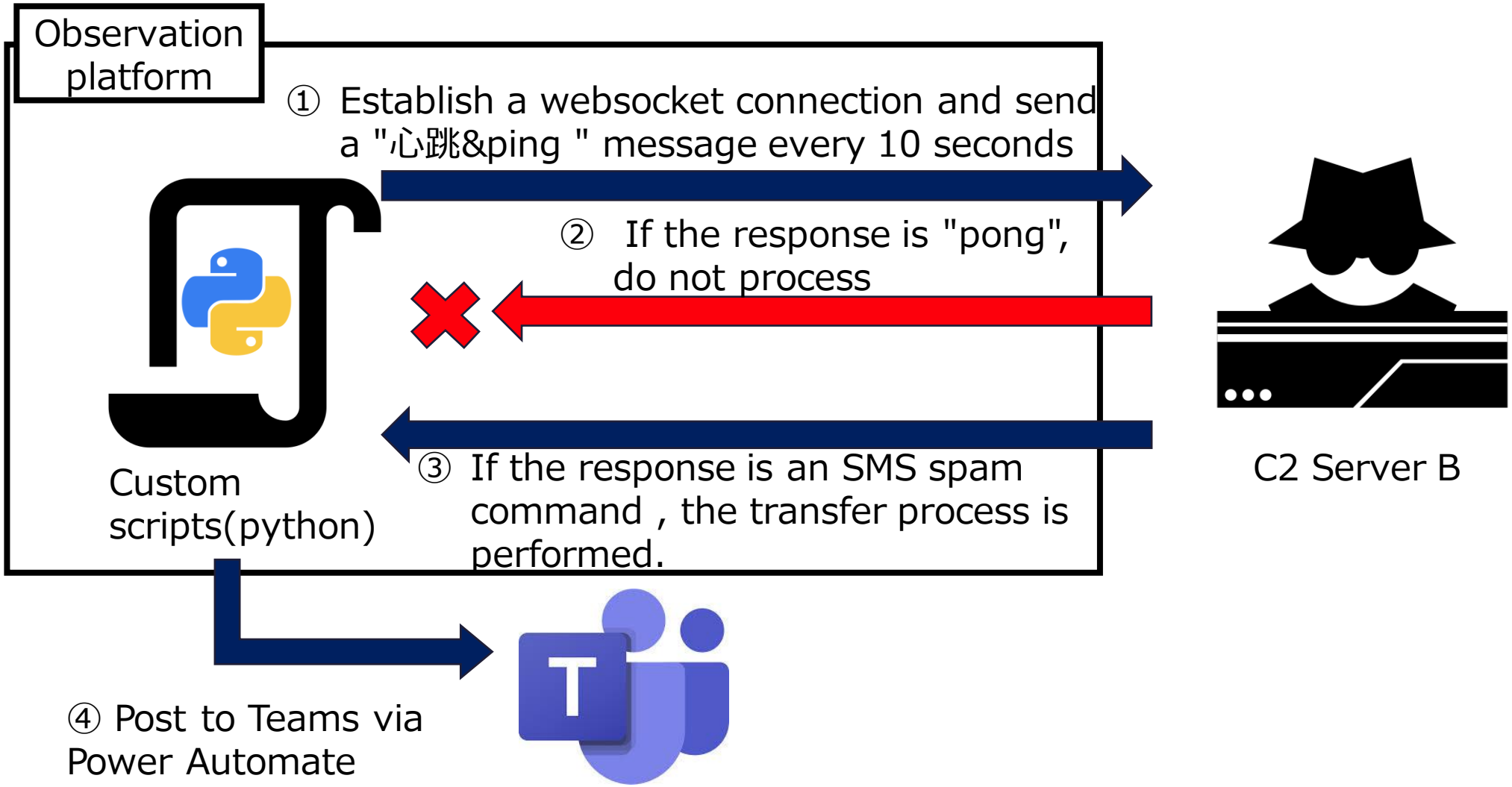
*https://search.censys.io/hosts/104.255.152.61



Building a fake SMS Observation platform

Now that we know the content of the communication to C2 server B, we will consider how to obtain the SMS spam command from C2 server B.

We built an Observation platform that notifies Teams when an SMS spam command is received from C2 server B.

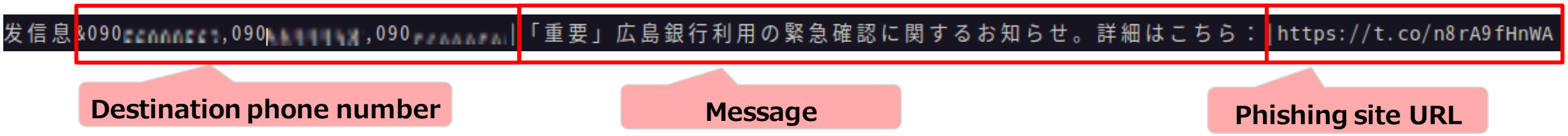


Observation results

Successfully received SMS spam command from C2 server B!

Receives SMS spam commands from five ports, 7775 to 7779, once or twice a day.

Example of SMS spam command sent on Wednesday, November 27th:



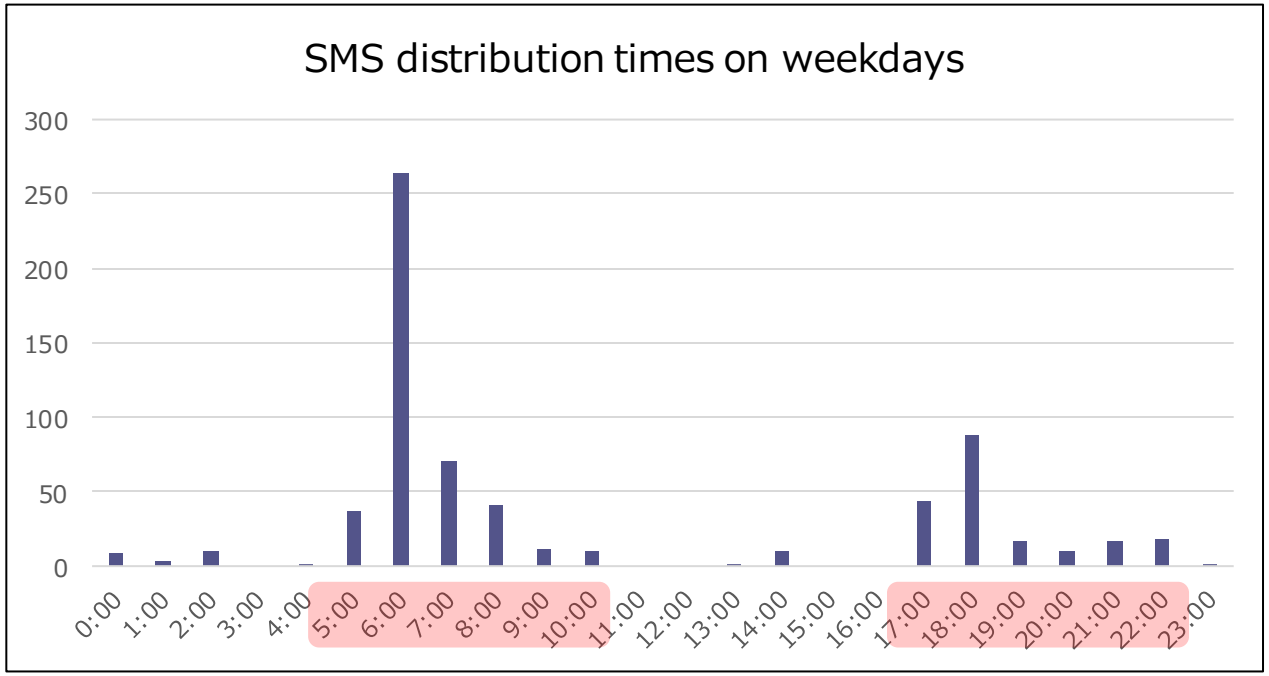
Post on Teams (also add C2 server port number and redirect destination) ：

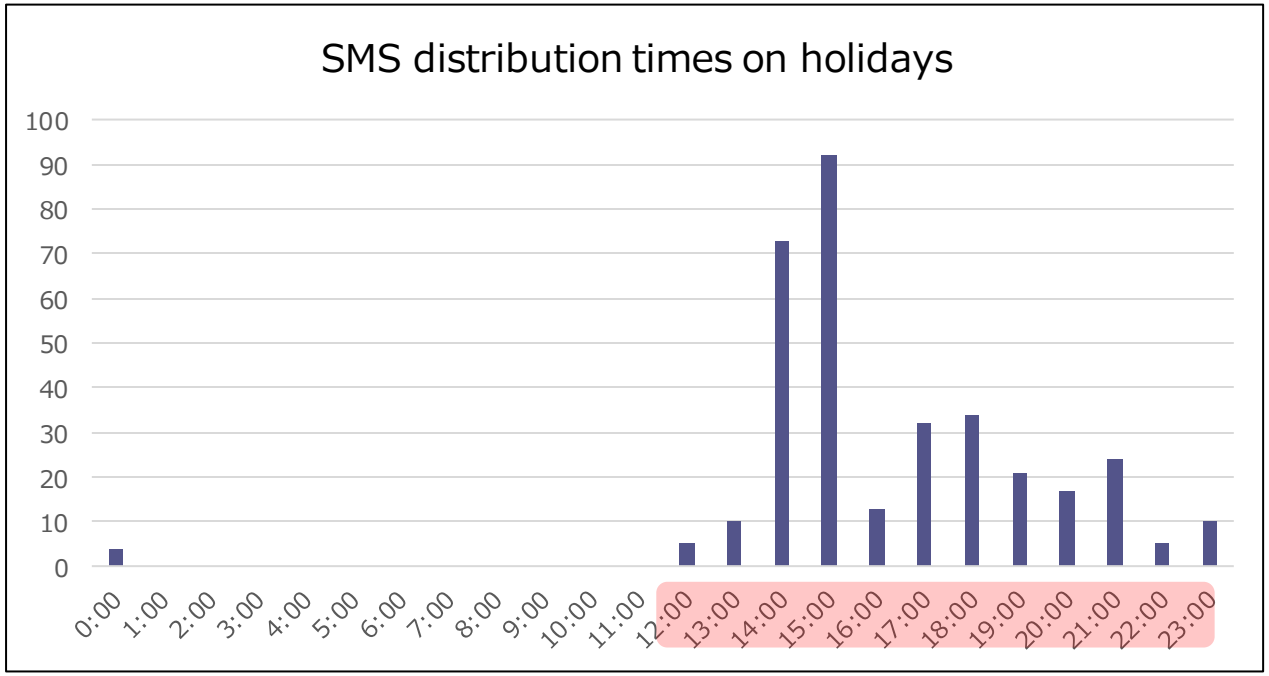
Results

If Mizuho Bank is targeted, it can quickly take down the phishing site. It can also notify other targeted banks.

Features of SMS spam commands (distribution time period)

- **Observation period :** 2024/06/19 ~ 2024/12/11
- **Observation Port :** 7775,7776,7777,7778,7779
- **Results**
  - Weekdays : It is often distributed between **6:00~7:00 and 17:00~18:00.**
  - Holidays : They are often distributed at **14:00 or 15:00, with most being in the afternoon.**
- **Considerations**
  - They may be targeting times when SMS can be viewed.
  - Weekdays : Start and finish times for work each day.
  - Holidays : The timing is when you complete your schedule in the morning and take a break in the afternoon.





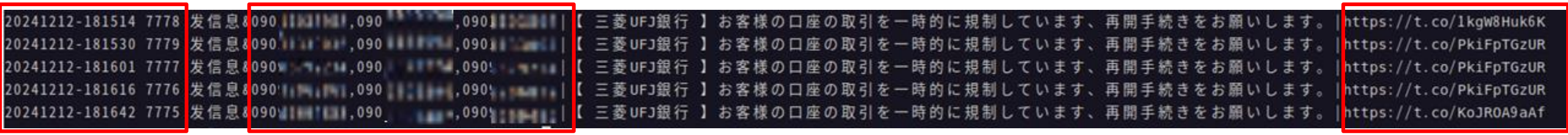
Features of SMS spam commands (by port)

- Investigate whether there are differences in SMS spam commands for each port.
  - Frequency: **1-2 times** a day from each port.
  - Time period：SMS spam commands will be sent from each port **at the same time**.
  - Phone number: **No two numbers are the same at the same time**, all are different phone numbers
  - URL： Multiple shortened URLs exist. The destination URL from the shortened URL is generally the same (although the destination URL may change over time).

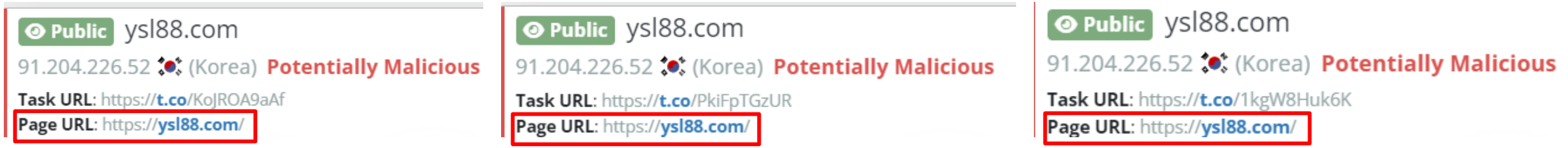
Commands are sent from each port at the same time.

All SMS sent to different destinations at the same time

There are multiple shortened URLs



Example: 12/12 (Thu): Sent SMS spam command



Example: 12/12 (Thu): Destination from shortened URL

5． Attempts at early detection of phishing sites

About the premise of this survey

- **Target phishing site:** Phishing site of BP1 (actor conducting SMS spammers)
- **Survey period :** 2024/4 ~ 2024/10
- **Survey data :** Data on phishing sites held by JC3, public data on the Internet, etc.
- **Survey Contents :**
  - Target brand name (company name)
  - Phishing site server certificate

Statistics on brand names (company names) impersonated by BP1

- Counting method: Counting the number of FQDNs of BP1 phishing sites
- Targeted companies are listed in ranking order (excluding those that cannot be classified)
  - **MUFG Bank**, which is said to have suffered the greatest damage, ranks at the top.
  - **Regional banks are also targeted**
  - From April to August 2024, there will be **more than 5,000 FQDNs**, but the number will **decrease since September**.

順位	Apr(Number of FQDNs)	May	Jun	Jul	Aug	Sep	Oct
1位	MUFG Bank(4862)	MUFG Bank(4198)	MUFG Bank(4442)	MUFG Bank(5331)	MUFG Bank(1678)	MUFG Bank(613)	Resona Bank(688)
2位	docomo(1226)	docomo(2663)	Mizuho(1884)	TEPCO(53)	Hokkaido Bank(1074)	SHIZUOKA BANK(16)	MUFG Bank(610)
3位	KDDI(617)	TEPCO(33)	docomo(1076)	TOKYO GAS(5)	Resona Bank(971)	Resona Bank(8)	Hokkoku Bank(135)
4位	TEPCO(12)		Resona Bank(263)	Resona Bank(2)	Iwate Bank(507)	TEPCO(8)	Nanto Bank(7)
5位			SMBC(58)	Fukuoka Bank(1)	KANSAI MIRAI BANK(417)	Nanto Bank(2)	TEPCO(4)
6位			SMCC(28)	77 Bank(1)	SMBC(233)		Nagoya Bank(2)
7位			TEPCO(5)		AEON BANK(189)		
8位					LIFECARD(106)		
9位					TEPCO(33)		
10位					JCB(2)		
合計	**6717**	**6894**	**7756**	**5393**	**5210**	**647**	**1446**

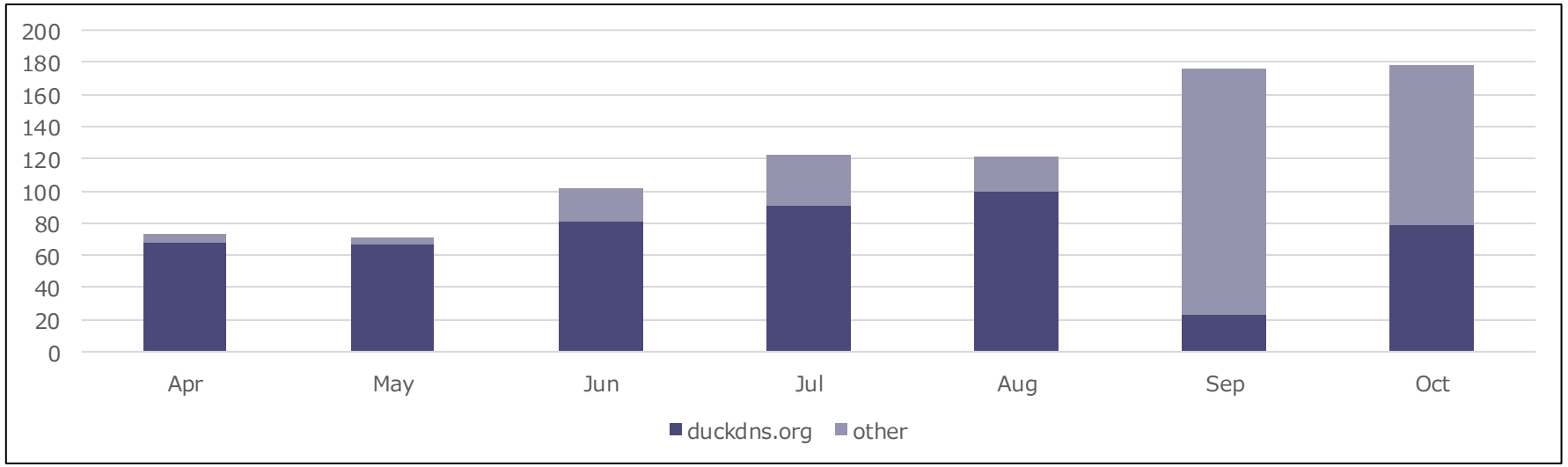
About server certificates issued by BP1

- The number of server certificates issued by BP1 is as follows:

	Apr	May	Jun	Jul	Aug	Sep	Oct
Number of issues	73	71	102	123	121	176	178

  - The number of issued server certificates is **on the rise**
  - **The number of server certificates issued is small** compared to the number of FQDNs of phishing sites.

- Survey results on the reason why the number of issued server certificates is less than the number of FQDNs.
  - April to August： **A high percentage** of phishing sites have certificates with CN **[subdomain].duckdns.org**
  - September to October： **A low percentage** of phishing sites have certificates with CN **[subdomain].duckdns.org**



Number of server certificates issued by BP1 (duckdns and others)

About server certificates issued by BP1

- Survey results on the reason why the number of issued server certificates is less than the number of FQDNs.
  - For server certificates with CN [subdomain].duckdns.org, **multiple phishing site domains are often registered in the SAN** (Subject Alternative Name).

There are multiple FQDNs in the SAN.
In this example, there are 100.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:60:05:14:83:68:d6:3a:08:35:87:47:4a:5a:1c:9b:ea:b4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: (CA ID: 295815)
            commonName                = R11
            organizationName          = Let's Encrypt
            countryName               = US
        Validity (Expired)
            Not Before: Jul 31 20:24:50 2024 GMT
            Not After : Oct 29 20:24:49 2024 GMT
        Subject:
            commonName                = 307ebru4p.duckdns.org
```

```
X509v3 Subject Alternative Name:
    DNS:00qfezzs.duckdns.org
    DNS:0iry10.duckdns.org
    DNS:0lkx9b.duckdns.org
    DNS:0ouqf4q.duckdns.org
    DNS:13tfxab.duckdns.org
    DNS:1c65z0.duckdns.org
    DNS:1cs6r0ow.duckdns.org
    DNS:1k4t8ew.duckdns.org
    DNS:2c6fwj7x3.duckdns.org
    DNS:2ez5zpq.duckdns.org
    DNS:307ebru4p.duckdns.org
    DNS:36o2rsez8.duckdns.org
    DNS:378vnxbx.duckdns.org
```

Example: Certificate issued on 2024-07-31

Summary of Results

Because DuckDNS is heavily used, the number of FQDNs of phishing sites tends to be larger than the number of server certificates from April to August.

Early detection using CT logs

- **Considerations**
  - The reason for heavy use of DuckDNS is thought to be **to build a large number of phishing sites at low cost, increasing the response costs for defenders.**
  - In order to reduce the hassle of issuing server certificates, **multiple FQDNs are registered in the SAN of the server certificate, and one server certificate is likely to be used**.
  - By checking the SAN of the server certificate, **it is possible to obtain multiple FQDNs of phishing sites on the date the server certificate was issued**.

- **Verification items**
  - We used **CT logs** to verify whether it was possible to detect the issuance of server certificates used for BP1 phishing sites.
  - The search conditions are as follows,
    - The number of FQDNs in the SAN is **20 or more**
    - Issuer OrganizationName is **Let's Encrypt**
    - CN is ***.duckdns.org**

- **Results**
  - **From April to August**, there were many duckdns.org domains, and **phishing sites can generally be detected at the time the server certificate is issued.**
  - **From September to October**, the number of duckdns.org domains decreased, **making it difficult to detect phishing sites** (BP1 may have taken measures)

Chapter 4_Summary

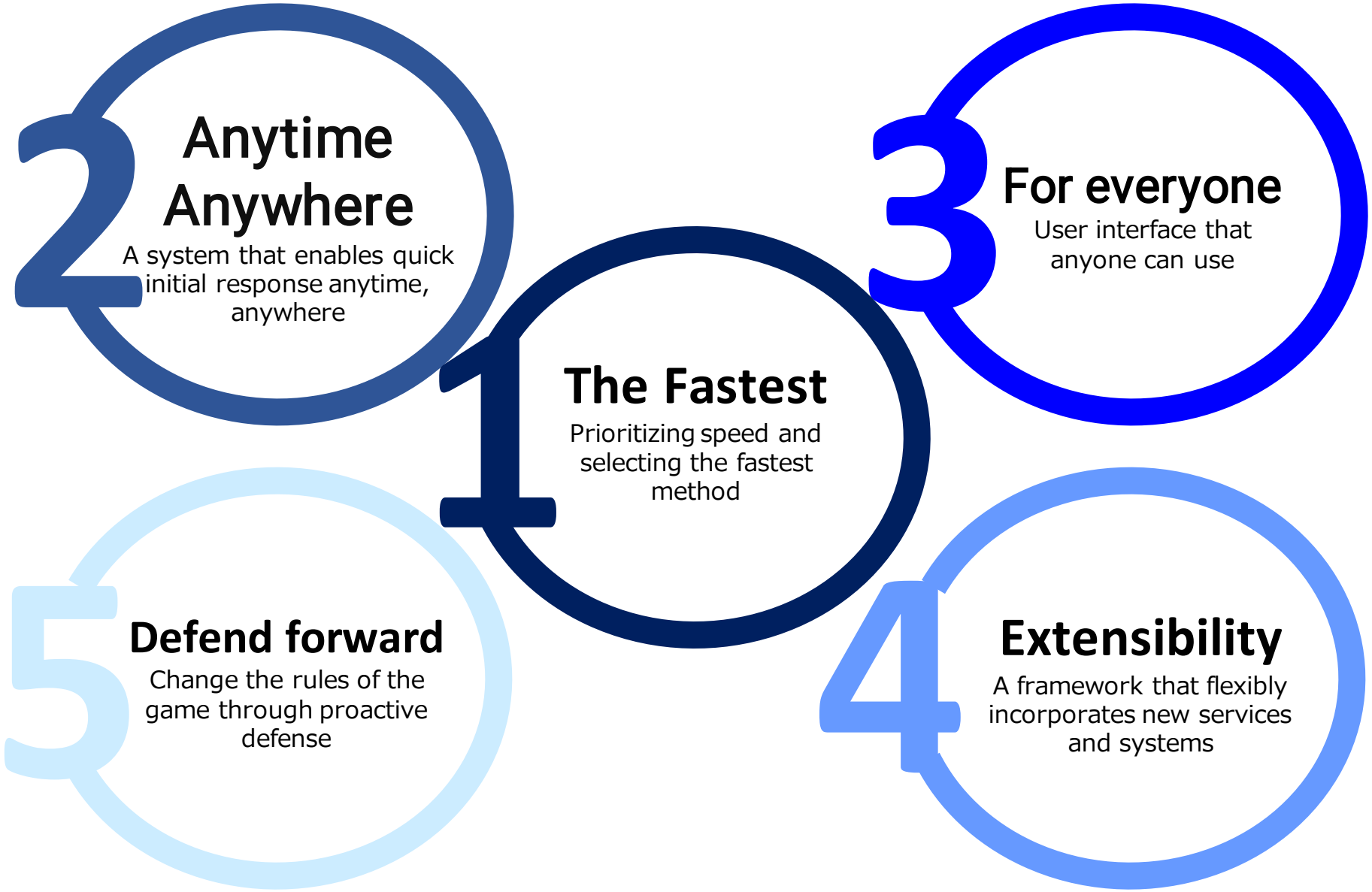
- We analyzed KeepSpy and investigated the content of the communications.
- By establishing an Observation platform, it is possible to observe SMS spam commands, enabling early detection of phishing sites and taking them down.
- Provide mutual assistance by sharing SMS dissemination information (target bank and phishing site URL) with other banks.

Chapter 5_Summary

- Counting the number of phishing sites per month
- Count the number of server certificates issued each month
- DuckDNS is frequently used during the period from April to August 2024, and multiple FQDNs are registered in the SAN of the issued server certificate.
- Using this feature, it was possible to detect phishing sites early from CT logs.
- The number of duckdns.org domains will decrease in the September-October 2024 period.

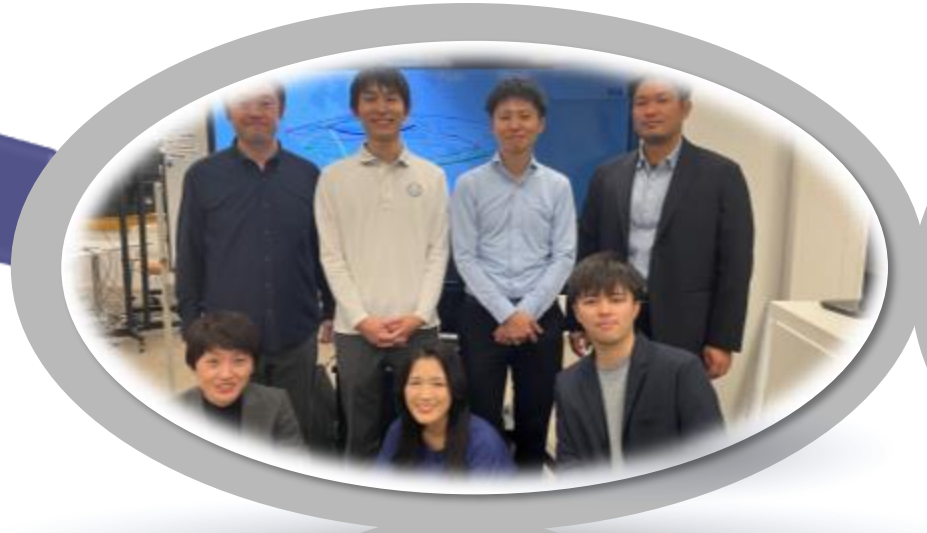
6. Mizuho's Automation Initiatives and Future Direction

Our Approach Concepts



The Fastest - Long-Term Monitoring Implementation in Private Companies

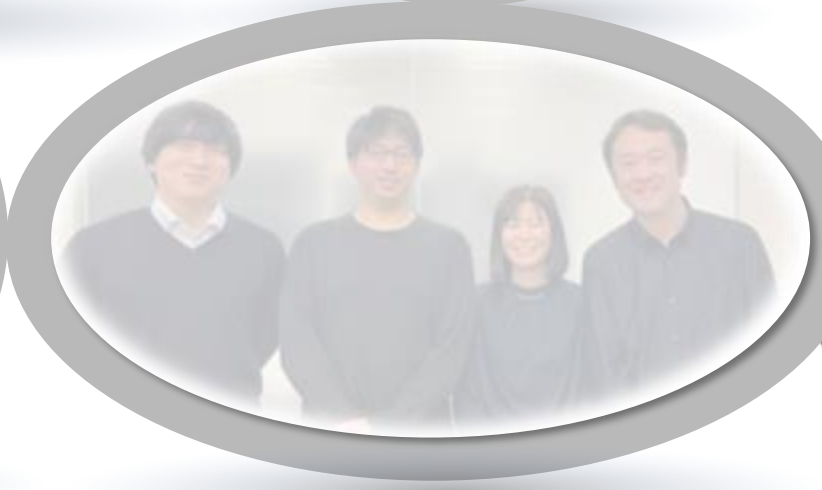
01 Cybercrime Investigation squad



02 Technical squad (Malware Analysis)

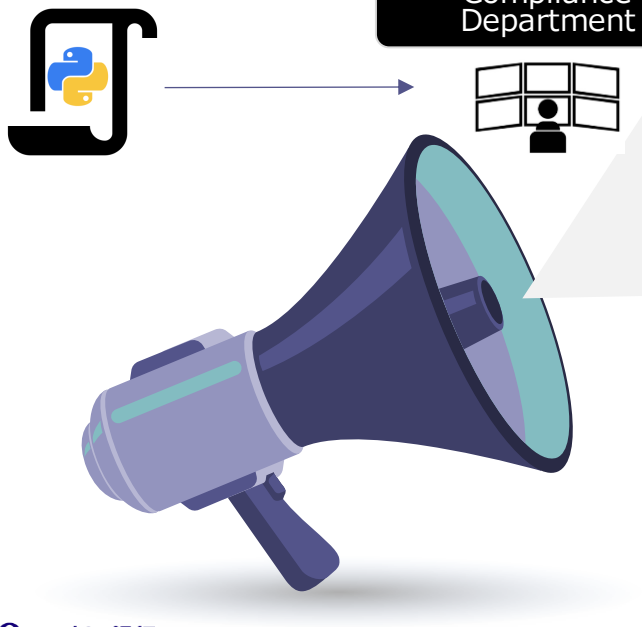
03 Development squad

04 Automation Promotion squad



The Fastest - Long-Term Monitoring Implementation in Private Companies

Long-Term Monitoring Implementation in Private Companies - Send out alerts as fast as possible.



Compliance Department

Direct Banking Center

Preparation for mass inquiries from customers due to receipt of suspicious SMS, customer hearings

Internet Banking Department

Preparation for strengthening monitoring rules in internet banking

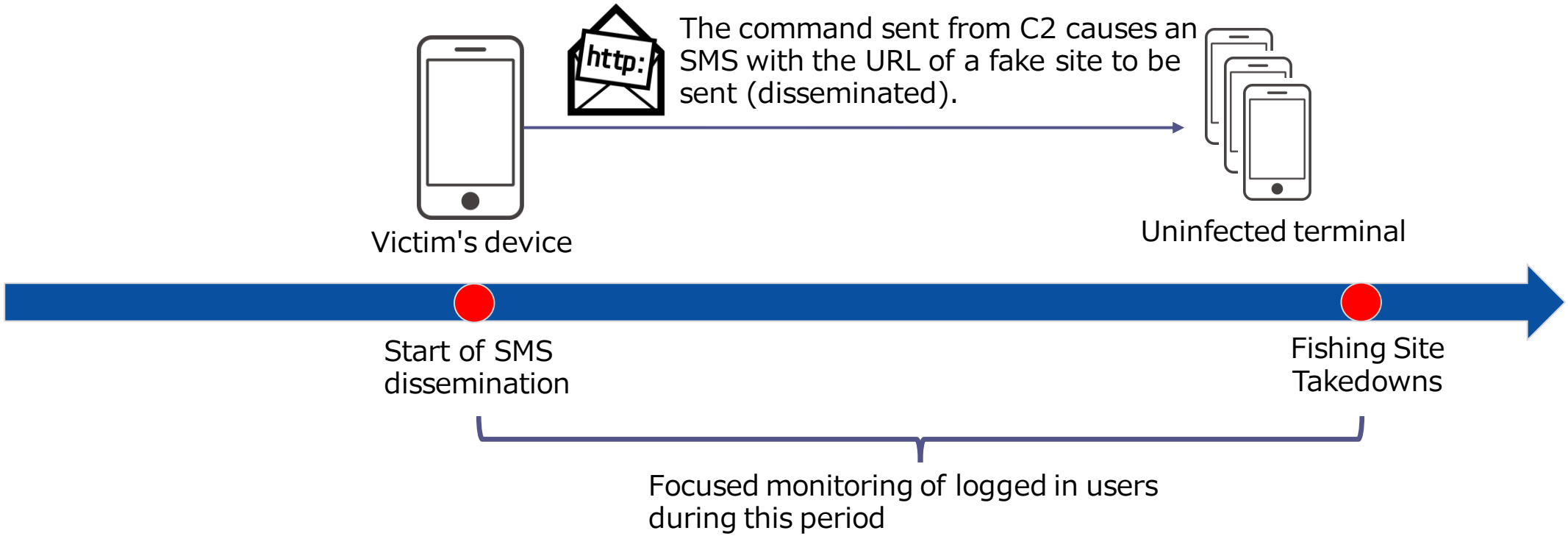
Compliance Department

Preparation for uploading contents of alerts for customers on the website.

Compliance Department

Takedown work of phishing sites.
Analysis of phishing sites.
Dummy account submission.

The Fastest - Long-Term Monitoring Implementation in Private Companies



Triage of impacted users with down-to-the-minute accuracy and enhanced monitoring

Anytime Anywhere - Phishing is sudden

- Phishing response challenges include the need to be prepared for phishing sites 24/7
- Delays in initial response to phishing sites targeted on holidays and at night when resources are scarce

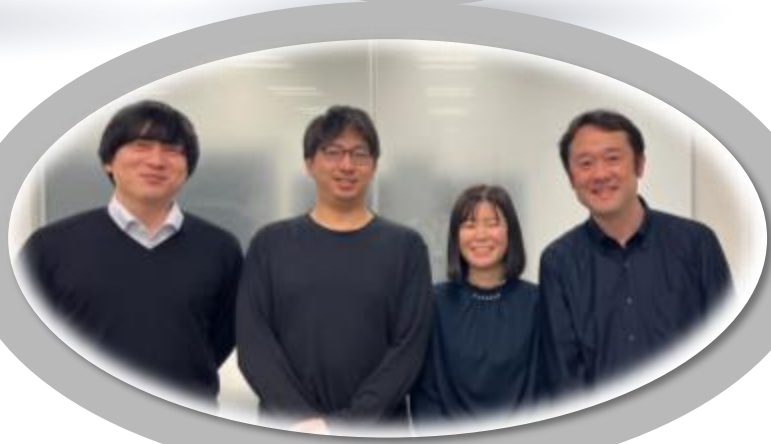
Anytime Anywhere - Automation is not easy

01 不正送金班

02 Tech班(マルウェア解析)

03 開発実装担当

04 自動化推進担当



Projection Only

Projection Only

大迫 結花

When do you use the current free version of urlscan.io?
I heard that it will be changed to the Pro version with API access...

森 三千代

We have a budget in place. !

竹内 司

I use urlscan.io after submitting a takedown request
I feel that the GSB will be effective faster if the takedown is judged as malicious by urlscan.io.

土井 優大

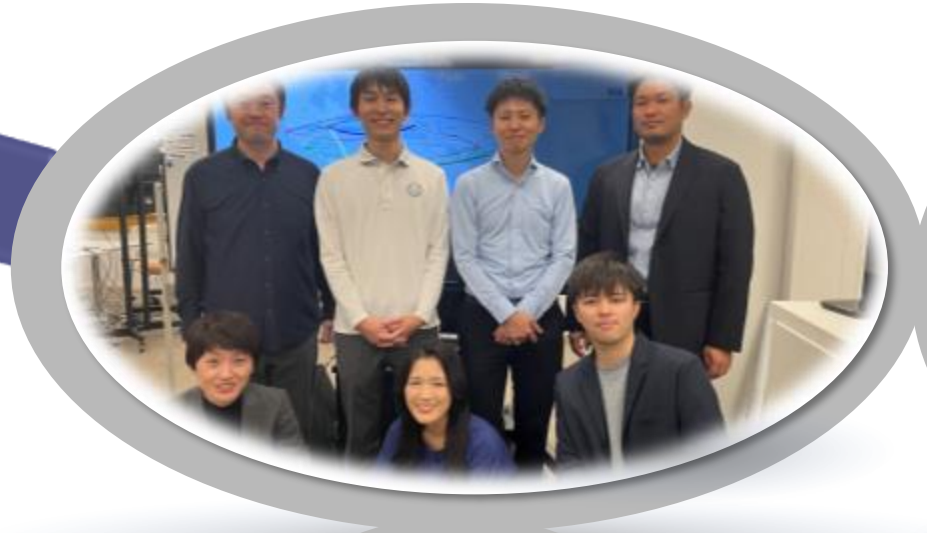
There is a possibility that the urlscan.io API can get images of phishing sites. I'm thinking it would be useful to get an image of the site before the takedown, what do you think?

竹内 司

That's right!
Let's take another look at the workflow for automation.

Anytime Anywhere – Detailed Flow

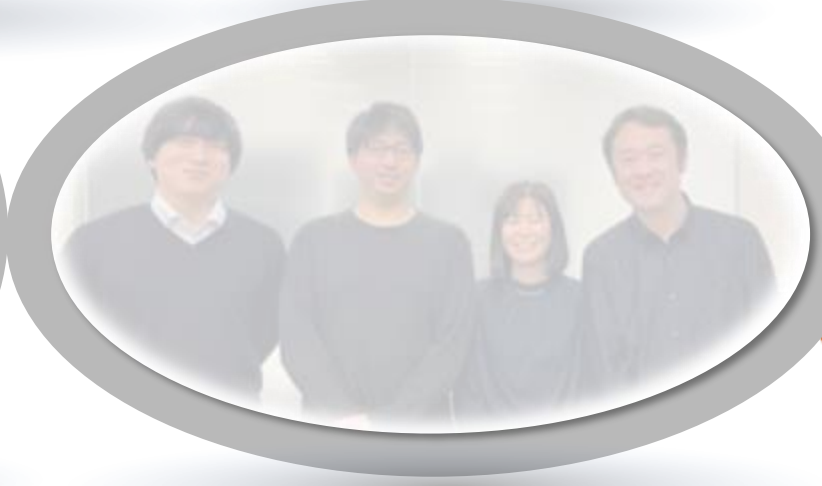
01 Cybercrime Investigation squad



02 Technical squad (Malware Analysis)

03 Development squad

04 Automation Promotion squad



西川 昌広

I'd like to organize the conditions that will be the first input to automate the process.
Can I just get an email from the detection service?

竹内 司

I use two services and receive mail from both. There is a pattern of manually submitting detected URLs. Classification conditions for phishing detection are complex.

西川 昌広

森 三千代

I would like to separate the number of investment fraud websites.

竹内 司

The conditions are too complex, so once you have them,
could you please write down everything you just said?

西川 昌広

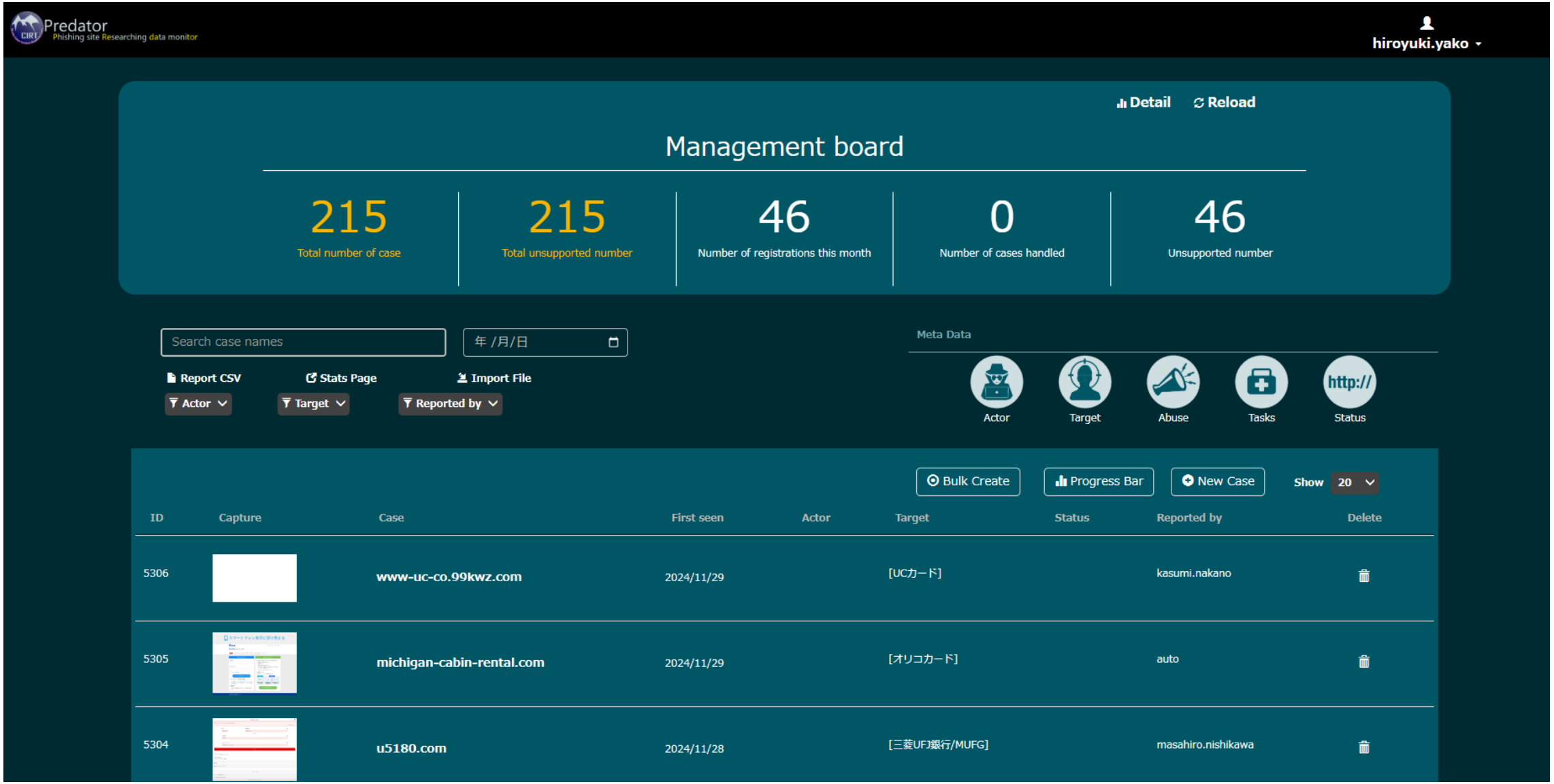
Projection Only

Projection Only

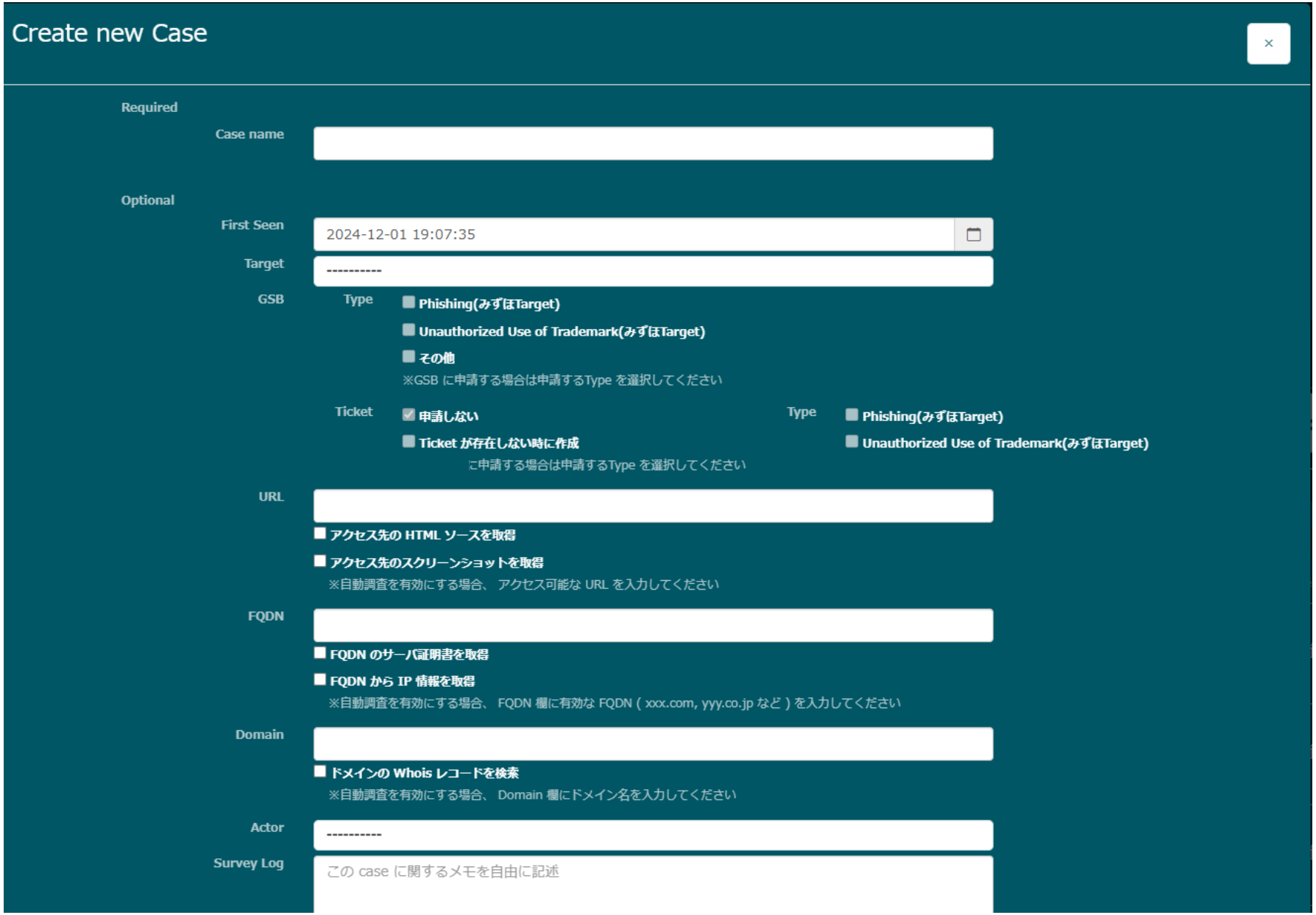
Projection Only

Projection Only

For everyone – Update takedown support tools



For everyone – Update takedown support tools

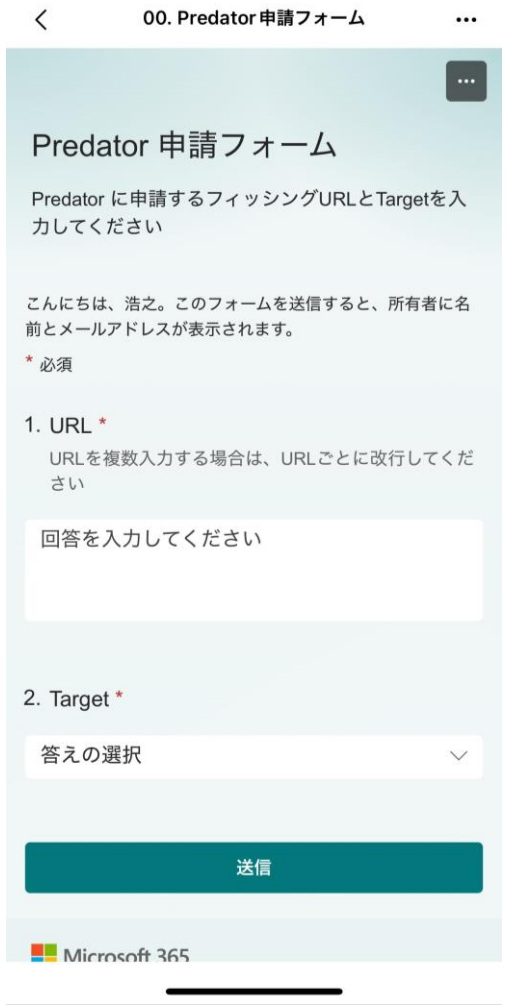


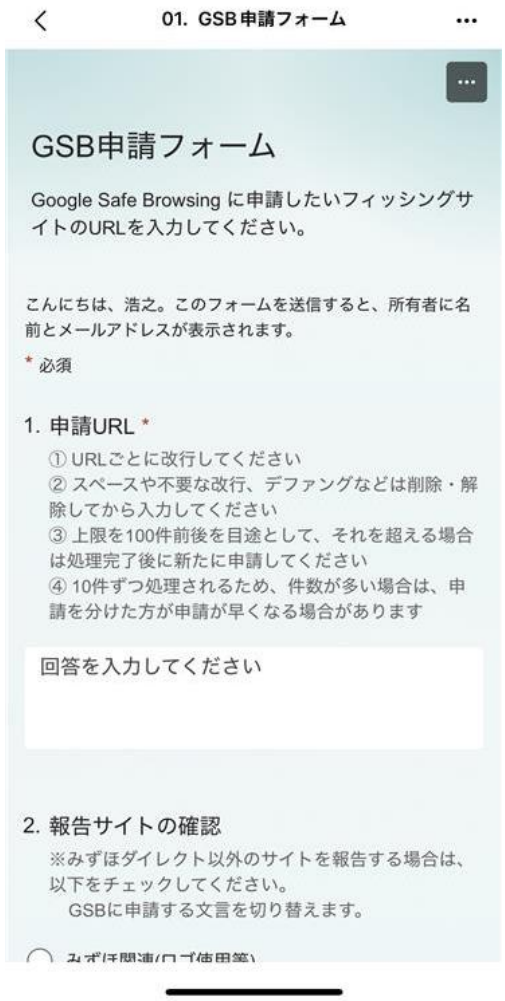
A air3_apps 9/30 10:04 編集済み

README

各種フォーム

00. Predator申請フォーム
01. GSB申請フォーム
02. URLScan申請フォーム
03. 申請フォーム





Extensibility – Expansion is flexible

Projection Only

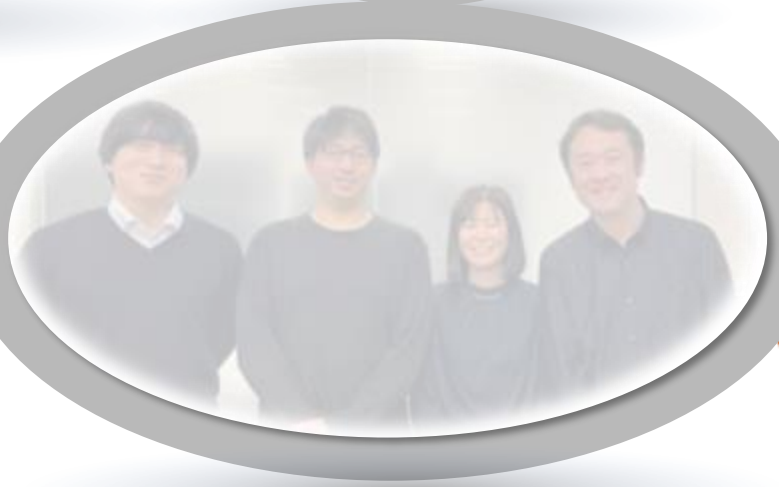
Defend forward – Deception approach

01 Cybercrime Investigation squad

02 Technical squad (Malware Analysis)

03 Development squad

04 Automation Promotion squad



Defend forward - Deception approach

フィッシングサイトに対する Deceptionアプローチ

Abstract

近年、フィッシングサイトの数が急増しており、状況が悪くなる一方である。彼らの主な目的はクレジットカード情報やオンライン口座の認証情報など「金の種」を狙うことがわかっている。

フィッシング攻撃に対する対応として、一般的には
1. テイクダウン
2. 一般ユーザーへの啓蒙
の２つ手段がある。しかし、ABUSEによるサイトのテイクダウンは報告先の対応に依存し、攻撃者のインフラの選択により大きな制限を受けることになる。一般ユーザーへの啓蒙も一朝一夕には進まない。

延々とテイクダウンを継続する対応は心が病んでいくため、上記以外の対応として何ができるか調査し、Deceptionのアプローチを試してみた。本講演では、２つの攻撃グループが作成したフィッシングサイトに対して行なったアプローチについて説明する。また、一連の作業において発生してきた問題と対策を共有する。

Speaker

猪野 裕司

吉川 允樹

Projection Only

Projection Only

In the future, we are planning a system to classify target groups as soon as phishing sites are discovered and automatically submit dummy accounts.

Further promotion of automation

- Due to the high burden of management tasks (managing the number and status of phishing sites) during mass outbreaks, improve the efficiency of phishing status monitoring and its aggregation, and organize it into a dashboard that can be viewed by management as well.
- Pursue enhancement of mechanisms to automatically collect information from phishing site information collection sources as input and expansion of linkage to services necessary for takedown.
- can take AI, the system is expected to be used for automatic classification of phishing site attack actor groups, analysis of phishing site characteristics, and other applications. In the future, the foundation for executing a “pretend to be fooled” strategy that is more can take that of human beings will be developed.

Promotion of joint defense (≠ information sharing)

- We would like to encourage companies struggling with phishing to make their know-how available at JSAC to the extent possible, and to collaborate with each other to share and improve on features that have been mutually effective.
- We would like to develop this into personnel exchanges through training programs and mutual training, sharing of phishing defense techniques and joint research, and mutual observation and takedown of phishing sites. We would like to actively promote public-private partnerships, as this is a particularly important area.
- We have received tremendous support from communities such as JC3 and the financial ISAC, and we will actively contribute to their development. We would like to participate actively as an organization that can take an action, not just an information-sharing organization.

Conclusion

・Monitoring fraudulent remittances is essential, but there are limitations, so it is also necessary to detect and take down phishing sites early.
・When dealing with this, there are limitations to human resources, so combine it with partial automation of the response.
・It is not a solo effort, but an all-out effort.

・By acquiring expertise in areas such as malware analysis, client companies can develop systems for early detection of phishing sites.

- Automation requires knowledge and expertise across multiple business areas. Beyond your own specialty, you need the courage and teamwork to delve into other teams' domains.
- To fight against phishing, we want to actively work towards taking "action" together with organizations and companies that share the same mission.

Appendix

IoC

value	type
66b118b5c63a3c8e30941b2e620211d04febbb21e3c90feb1f283b0b598fb46c	SHA256 hash value of Keepspy
siltsb6.duckdns[.]org	Keepspy C2 Server A Domain
104.255.152[.]61	Keepspy C2 Server B IP Address
104.255.152[.]62	Keepspy C2 server B IP address (other C2 servers)
104.255.152[.]85	Keepspy C2 server B IP address (other C2 servers)
104.255.152[.]86	Keepspy C2 server B IP address (other C2 servers)
104.255.152[.]100	Keepspy C2 server B IP address (other C2 servers)