Operation BlackEcho

:Voice Phishing using Fake Financial and Vaccine Apps

Speakers : Hyeji Heo, Sungchan Jang

Contributors : Kuyju Kim, Jinyong Byun, Byungwoo Hwang

Speakers

Hyeji Heo

- Security researcher at Financial Security Institute (2017~)
- Master’s degree from Chungnam National University (2015~2016)
- Responsible for analyzing and responding to Android malicious apps

Sungchan Jang

- Security researcher at Financial Security Institute (2019~)
- Security engineer at NCSOFT (2016~2019)
- Responsible for detecting and responding to phishing sites

Contributors

Kuyju Kim

- Security researcher at Financial Security Institute
- Author of the report “Voice Phishing App Distribution Group Profiling”, published by FSI in 2022.

Jinyong Byun

- Security researcher at Financial Security Institute

Byungwoo Hwang

- Security researcher
  & Malware analyst at Financial Security Institute

Outline

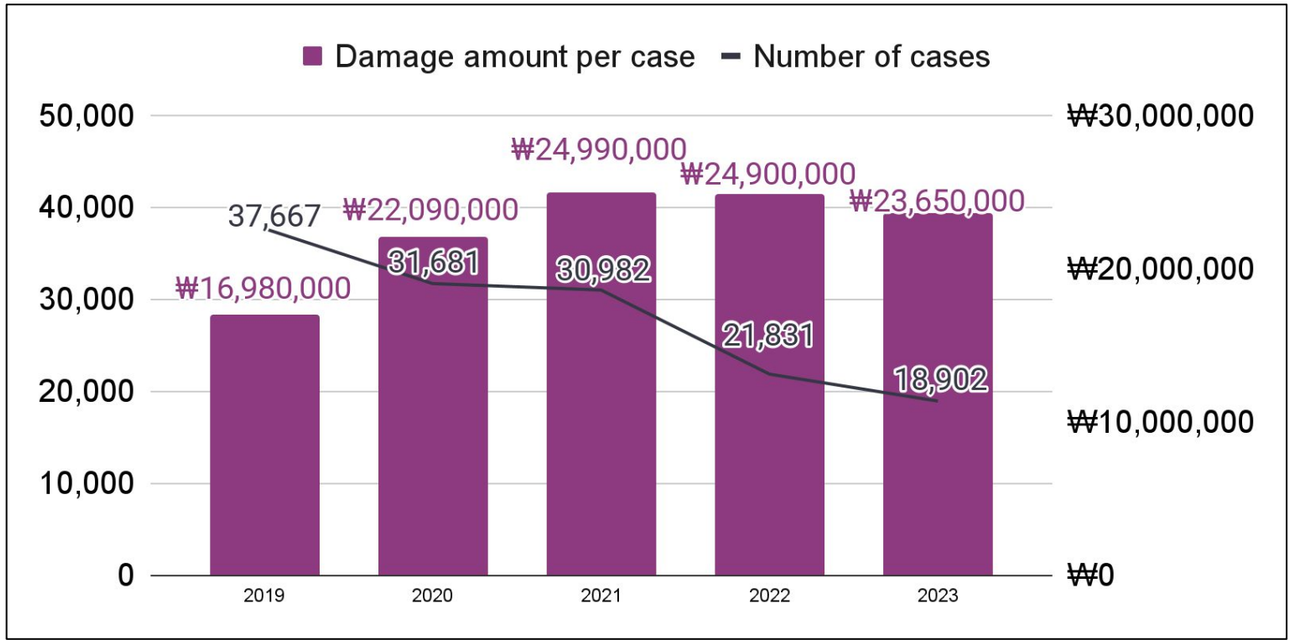
1. Background
2. Attack Flow
3. Malicious Apps
4. Infrastructure
5. Voice Phishing Scenario
6. Countermeasure
7. Trend
8. Conclusion

1. Background

Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

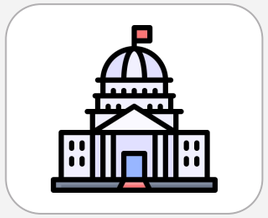
Understanding Voice Phishing

- Voice Phishing (a.k.a. Vishing)
  - A crime where scammers trick people over the phone to get money or personal information.
- Voice Phishing in South Korea (last 5 years)



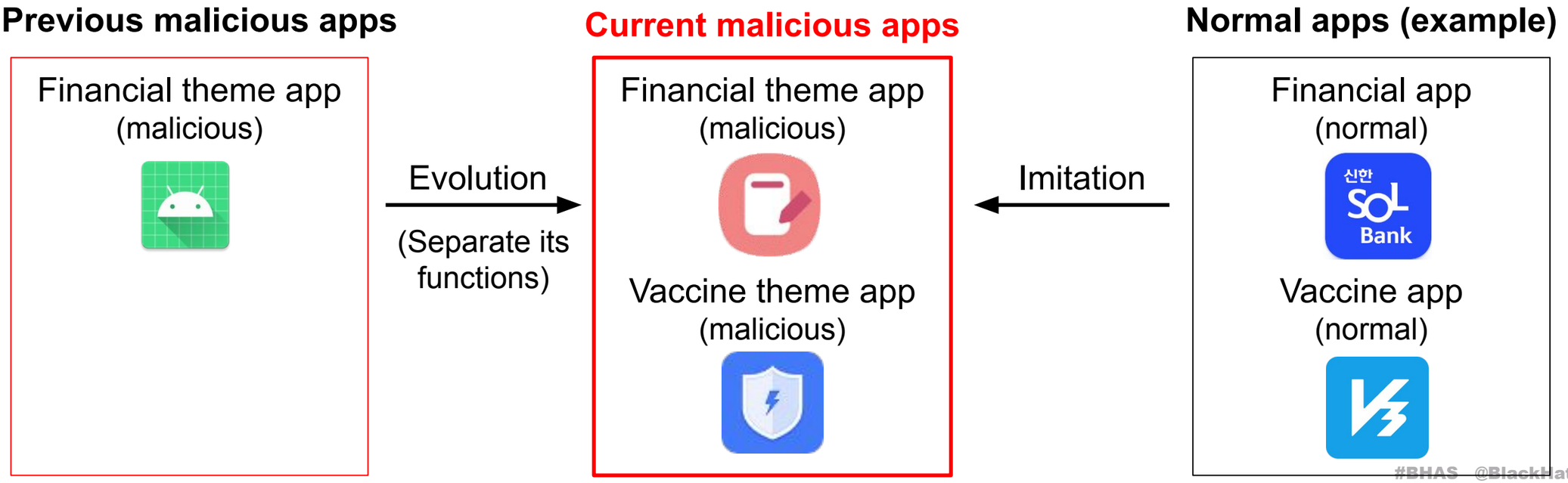
※ [Reference] Korean National Police Agency

※ High-value damage cases

Financial theme	Government theme
	

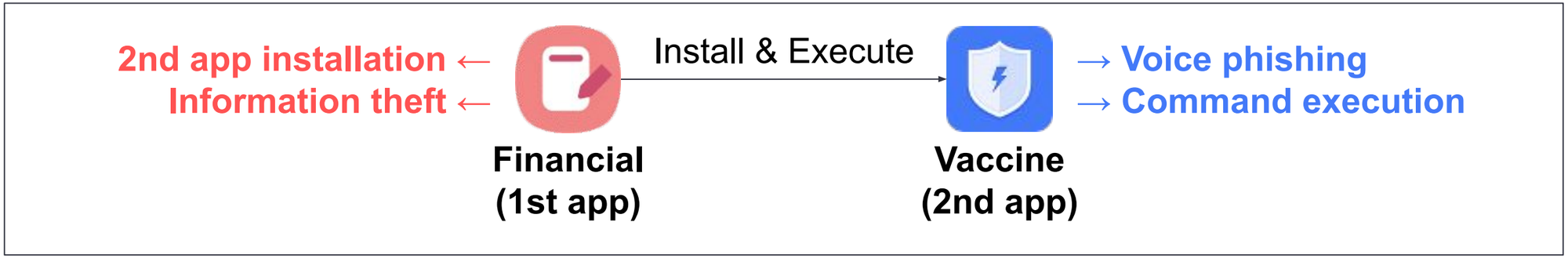
Why we did research

- Malicious Apps
  - **Malicious apps play a crucial role** in voice phishing attacks on smartphone users.
  - These apps **intercept and block phone calls**, **tamper with call screens and call logs**.
- New Type of Malicious Apps



Introducing Operation BlackEcho

- The criminal organization uses malicious apps **impersonating** financial and **vaccine** apps for voice phishing

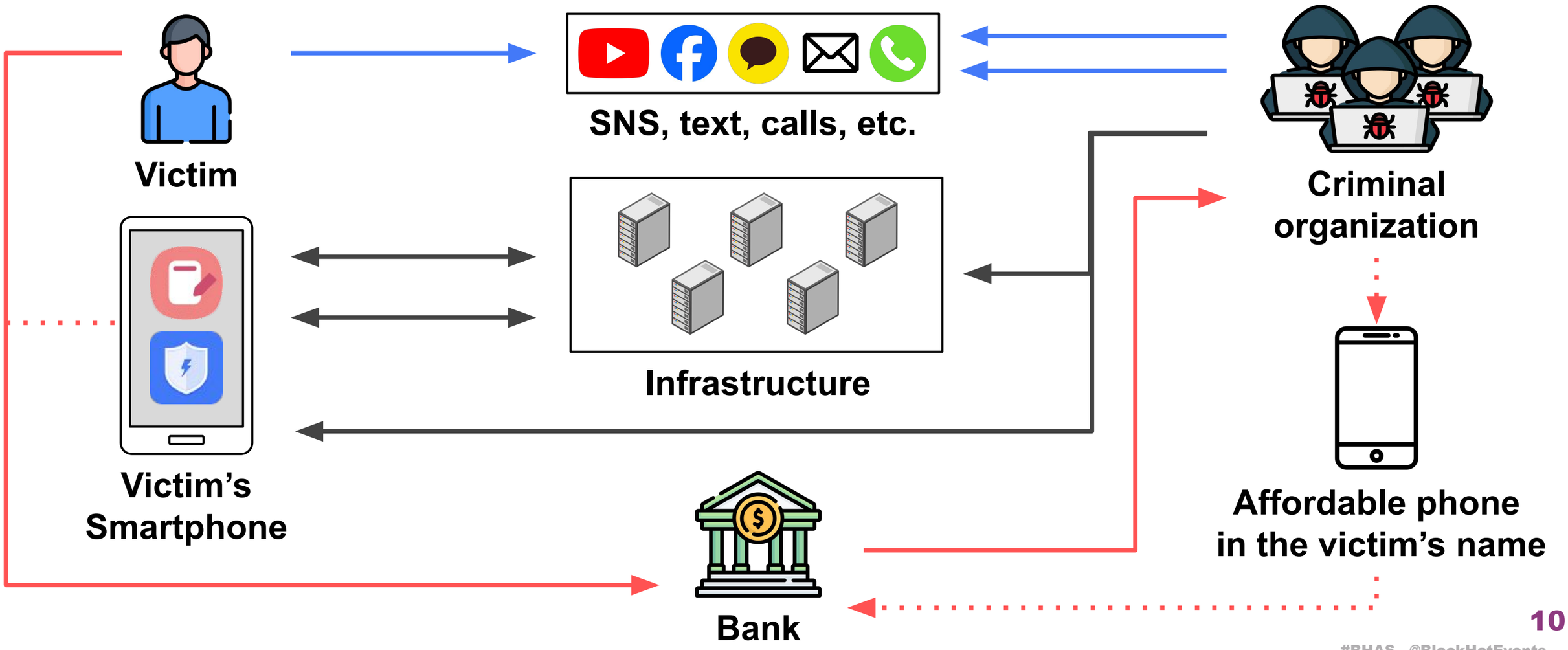


- It also uses apps **impersonating** **government agencies** for voice phishing, and creates **smishing** apps.

2. Attack Flow

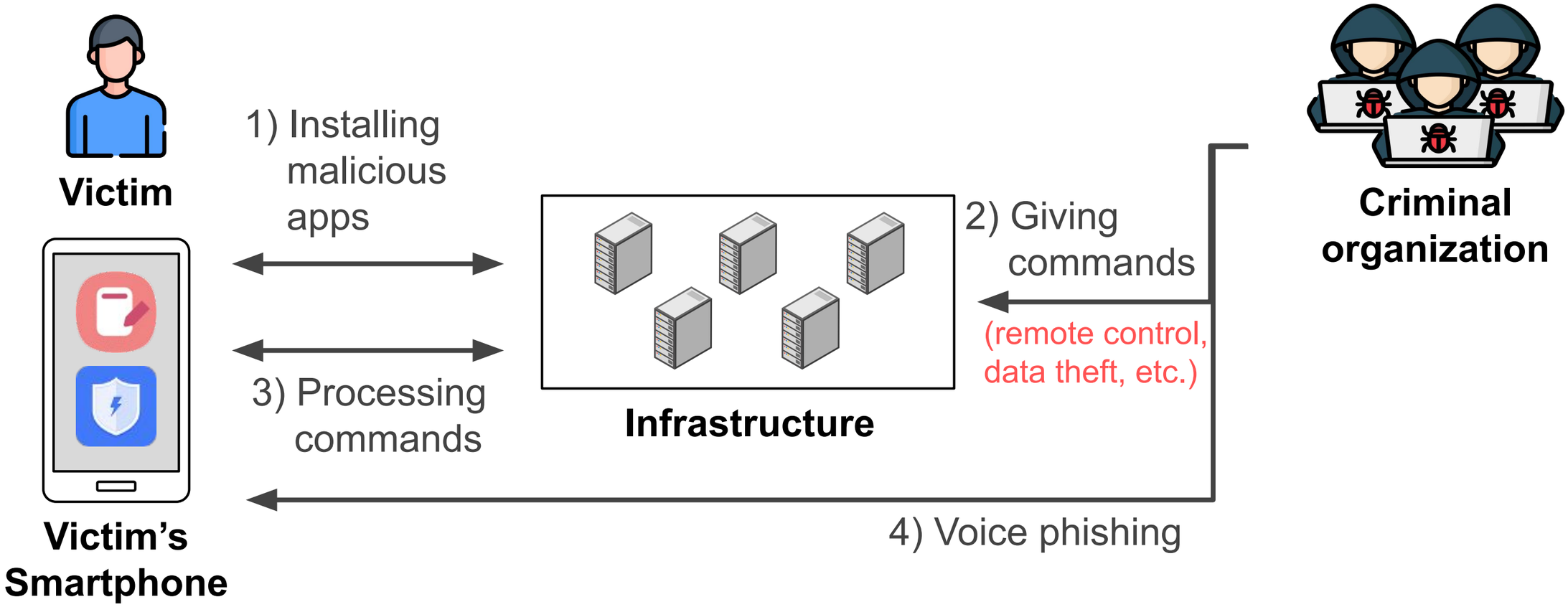
Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

Attack Flow

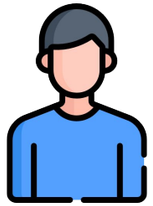

Victim
SNS, text, calls, etc.
Criminal organization
Infrastructure
Victim's Smartphone
Affordable phone in the victim's name
Bank

① Malicious App Distribution

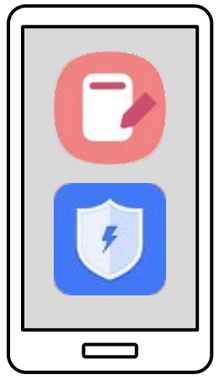
② Attacks


Victim
1) Installing malicious apps
3) Processing commands
Infrastructure
2) Giving commands
(remote control, data theft, etc.)
Criminal organization
Victim's Smartphone
4) Voice phishing

③ Financial fraud



Victim



Victim's Smartphone

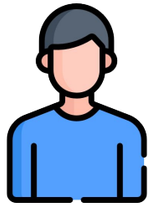
1) Transferring /Withdrawing money

Bank

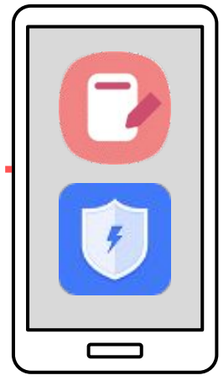
2) Swindling money

Criminal organization

③ Financial fraud



Victim



Victim's Smartphone

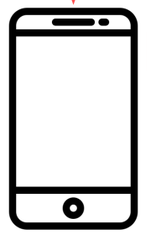
1-2) Making transactions (remote control)

Bank

2) Swindling money

Criminal organization

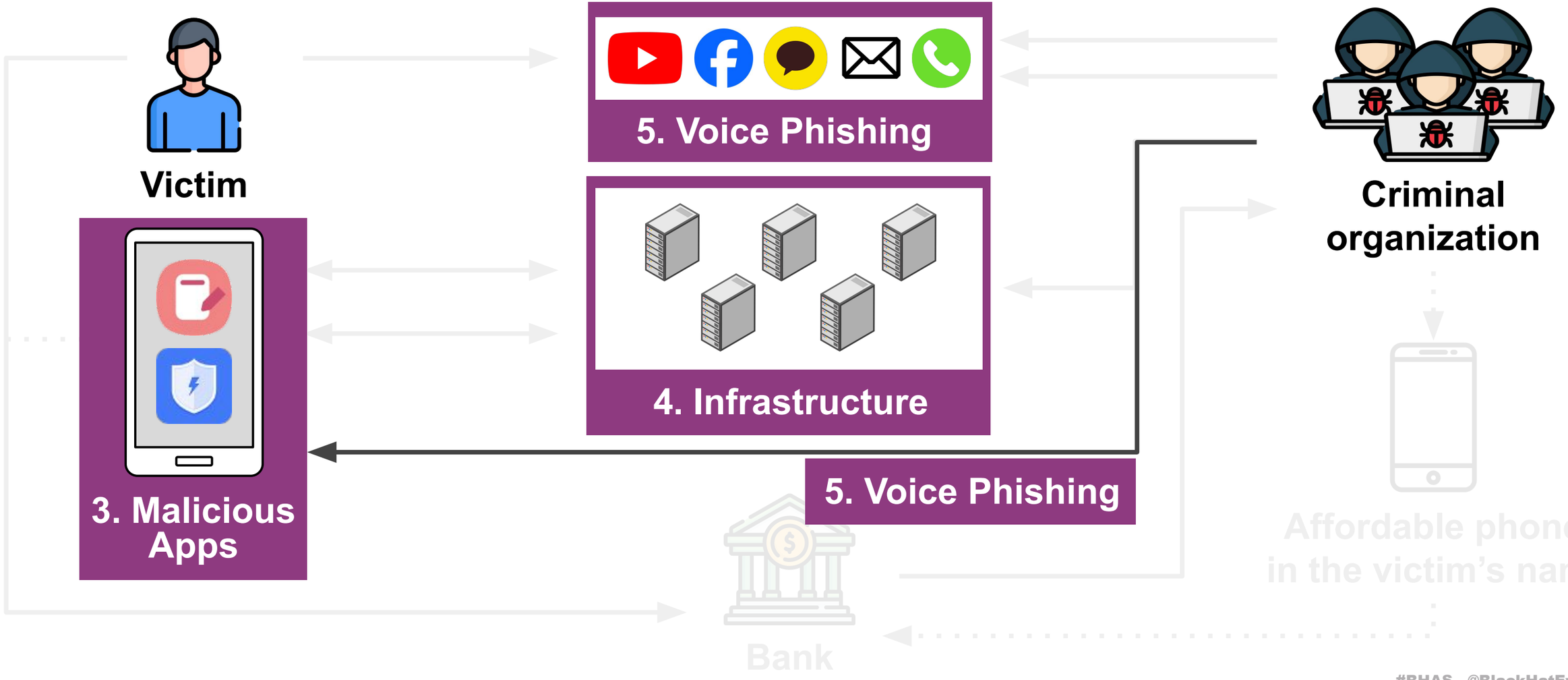
1-3) Activating phone



Affordable phone in the victim's name

1-3) Making transactions

What is next?


Victim
5. Voice Phishing
Criminal organization
4. Infrastructure
3. Malicious Apps
5. Voice Phishing
Affordable phone in the victim's name
Bank

3. Malicious Apps

Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

History

❖ Malicious apps are implemented separately based on their functionality.

December 2021
Started (estimated)

2022 ~ July 2023
Separated (1st + 2nd)

July 2023 ~
Separated (1st + 2nd_main + 2nd_call)

1st app (Financial or Government theme, dropper/downloader + data theft)

2nd app (Vaccine theme, Voice Phishing + a)

2nd_main app (Vaccine theme, control + data theft)

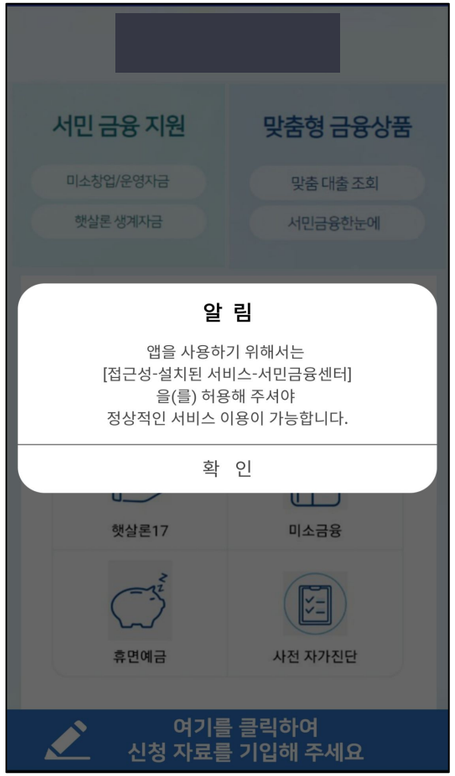
2nd_call app (Call theme, Voice Phishing)

※ These malicious apps copied official apps' icons.

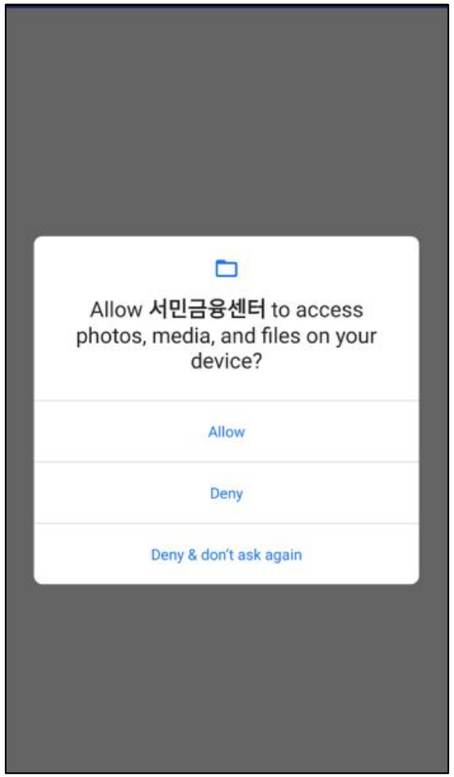
1st app

- Installing additional apps & stealing personal information

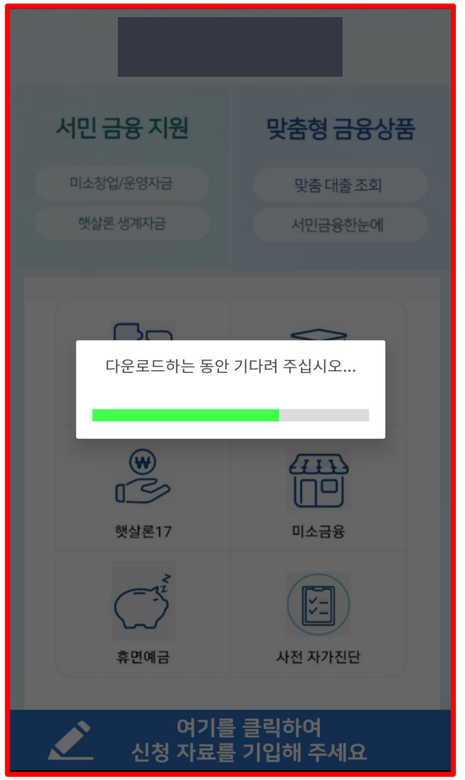
Main screen



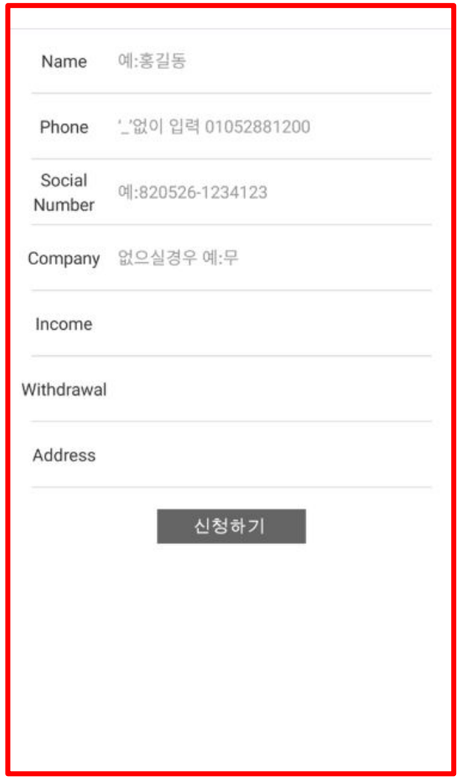
Requesting Accessibility permission



Requesting permission



Installing app



Loan application screen (data theft)

1st app - Screen Display

- The 1st app displays screens disguised as financial companies.
- And the screen display method has changed in three ways.

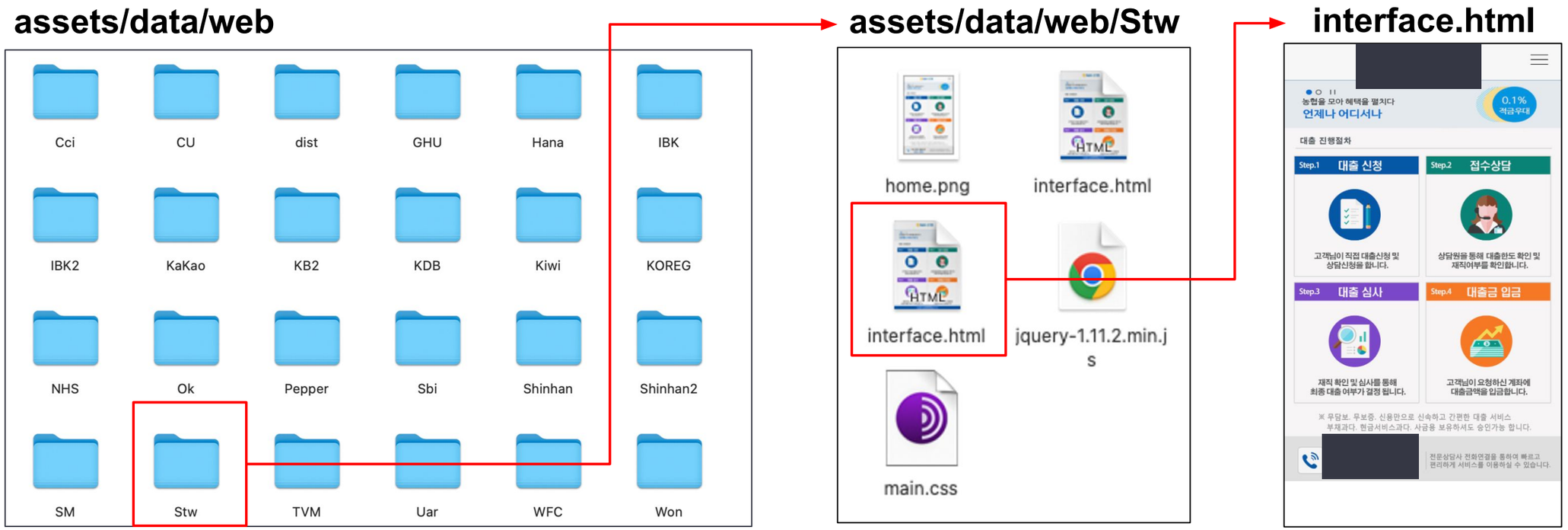
① Local html (~ June 2022)

② Layout (June 2022 ~)

③ Phishing page (April 2023 ~)

1st app - Screen Display

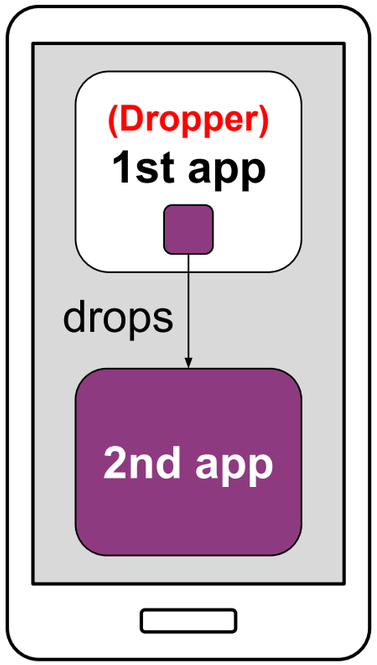
- The 1st app displays screens disguised as financial companies.
- And the screen display method has changed in three ways.
  - In the case of Local HTML, the app contains all the files to disguise.



1st app - Additional app Installation

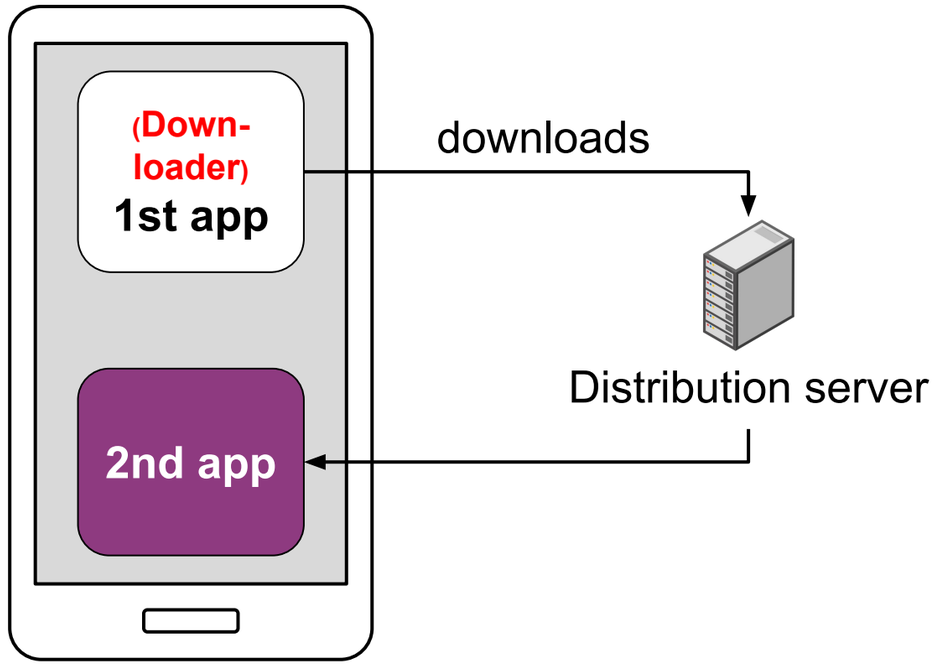
- The 1st app installs 2nd, 2nd_main and 2nd_call apps.
- And the app installation method has changed from ‘drop’ to ‘download’.

① Drop (Before September 2022)



file name	unzip result
assets/mobilev3.apk	-
assets/huhu.apk	-
assets/apk.zip	huhu.apk
assets/apk.zip	plus.apk
assets/asdf/apk.zip	huhu.apk

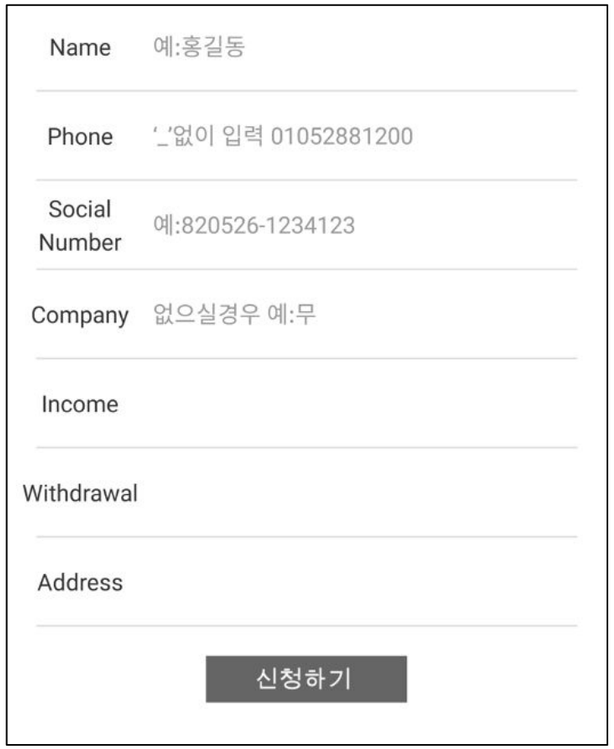
② Download (After September 2022)



1st app - Personal Information Theft

- The 1st app steals personal information by pretending to offer loan applications.

  → Name, Phone number, Social number, Company, Address, ID card, …



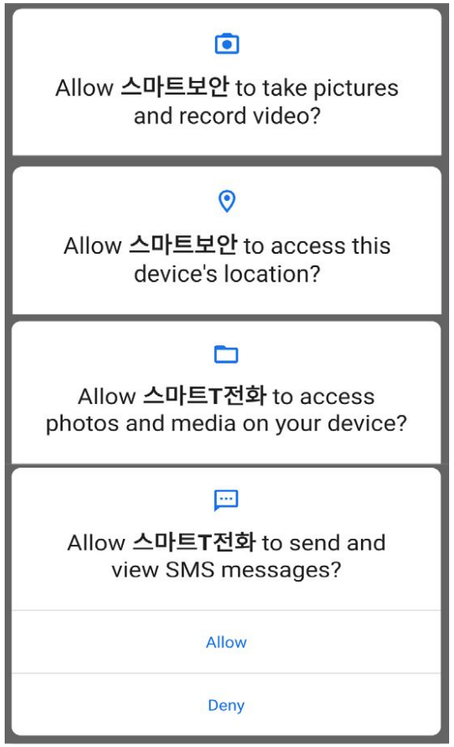
Default Value in the loan applications

Key	Value
Name	Hong Gildong
Phone number	01052881200
Social number	820526-1234123

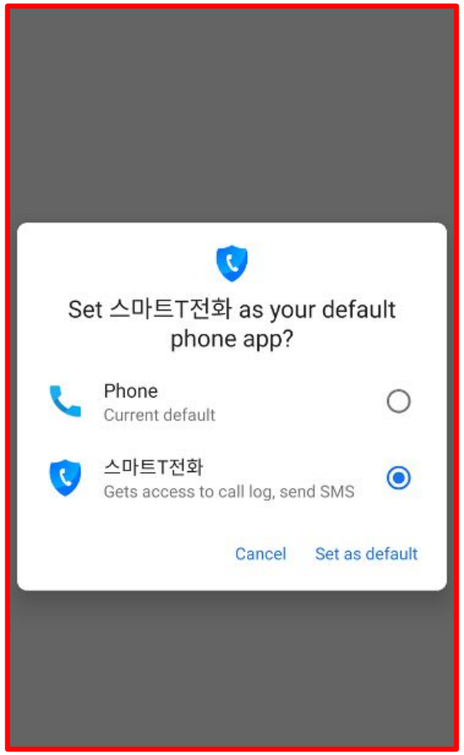
2nd app

- Processing commands & Voice Phishing

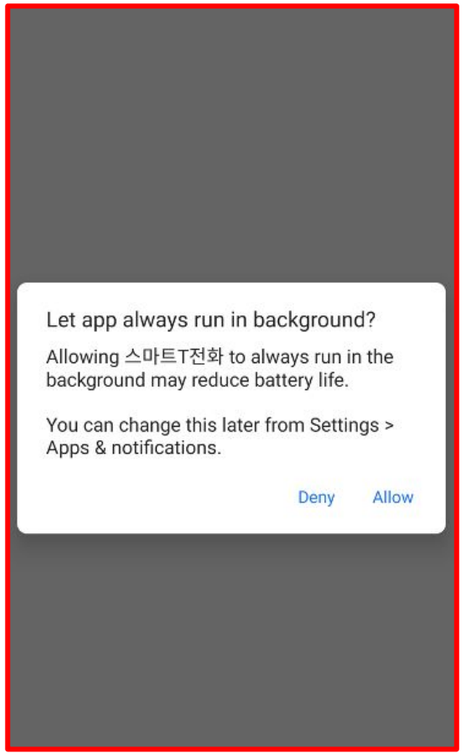
Requesting Accessibility permission



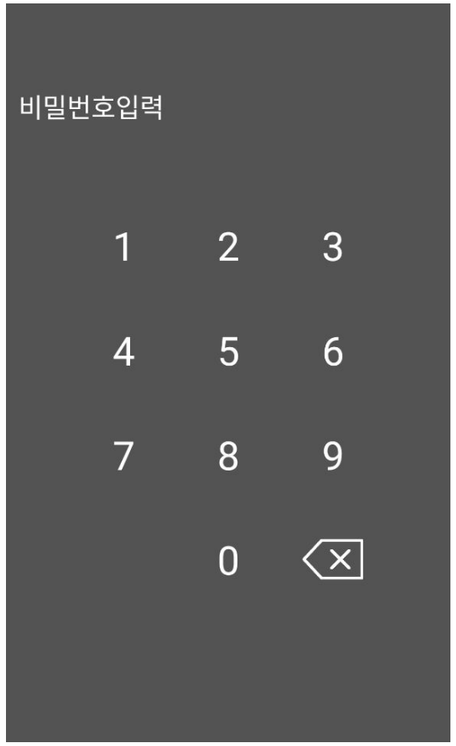
Requesting permission



Setting a default app



Maintaining persistence



Processing a cmd. (get PIN)

2nd app - Command Processing

- Command list

streaming
control
screen record
location
app
file
Accessibility
record
bluetooth
album

```
this.mSocket.on("stream_camera", this.onStreamCamera);
this.mSocket.on("stream_switch_camera", this.onStreamSwitchCamera);
this.mSocket.on("stream_mic", this.onStreamMic);
this.mSocket.on("stream_display", this.onStreamDisplay);
this.mSocket.on("action", this.onAction);
this.mSocket.on("capturing_on", this.onStartCaptureScreen);
this.mSocket.on("capturing_off", this.onStopCaptureScreen);
this.mSocket.on("upload_location", this.onUploadLocation);
this.mSocket.on("upload_apks", this.onUploadApks);
this.mSocket.on("delete_apk", this.onDeleteApk);
this.mSocket.on("upload_filelist", this.onUploadFileList);
this.mSocket.on("download_file", this.onDowndloadFile);
this.mSocket.on("upload_file", this.onUploadFile);
this.mSocket.on("request_rac", this.onRequestRAC);
this.mSocket.on("mic_record", this.onMicRecord);
this.mSocket.on("mic_record_duration", this.onMicRecordDuration);
this.mSocket.on("call_record", this.onCallRecord);
this.mSocket.on("enable_record", this.onEnableRecord);
this.mSocket.on("bluetooth_on", this.onBluetoothOn);
this.mSocket.on("bluetooth_off", this.onBluetoothOff);
this.mSocket.on("upload_album", this.onUploadAlbum);
```

```
this.mSocket.on("monitoring_on", this.onMonitoringOn);
this.mSocket.on("monitoring_off", this.onMonitoringOff);
this.mSocket.on("update_numbers", this.onUpdateNumbers);
this.mSocket.on("update_number_real", this.onUpdateNumberReal);
this.mSocket.on("block_update", this.onBlockUpdate);
this.mSocket.on("block_delete", this.onBlockDelete);
this.mSocket.on("block_create_one", this.onBlockCreateOne);
this.mSocket.on("incoming_update", this.onIncomingUpdate);
this.mSocket.on("incoming_delete", this.onIncomingDelete);
this.mSocket.on("incoming_create_one", this.onIncomingCreateOne);
this.mSocket.on("outgoing_update", this.onOutgoingUpdate);
this.mSocket.on("outgoing_delete", this.onOutgoingDelete);
this.mSocket.on("outgoing_create_one", this.onOutgoingCreateOne);
this.mSocket.on("update_private_numbers", this.onUpdatePrivateNumbers);
this.mSocket.on("hangup", this.onHangup);
this.mSocket.on("upload_contacts", this.onUploadContacts);
this.mSocket.on("add_contact", this.onAddContact);
this.mSocket.on("delete_contact", this.onDeleteContact);
this.mSocket.on("set_default_message", this.onSetDefaultMessage);
this.mSocket.on("unset_default_message", this.onUnSetDefaultMessage);
this.mSocket.on("upload_sms", this.onUploadSms);
this.mSocket.on("send_sms", this.onSendSms);
this.mSocket.on("delete_sms", this.onDeleteSms);
this.mSocket.on("upload_calllog", this.onUploadCallLog);
this.mSocket.on("delete_calllog", this.onDeleteCallLog);
```

voice phishing (enable, update phone numbers, end calls)

contact

sms

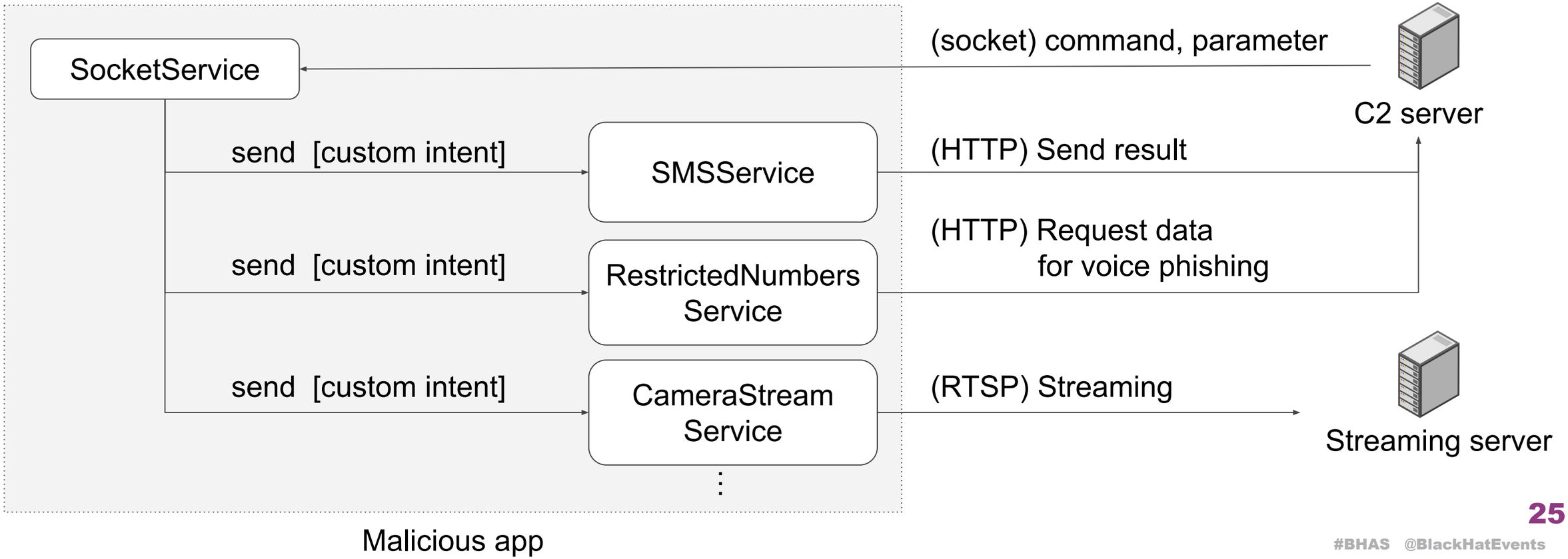
call log

2nd_main app

2nd_call app

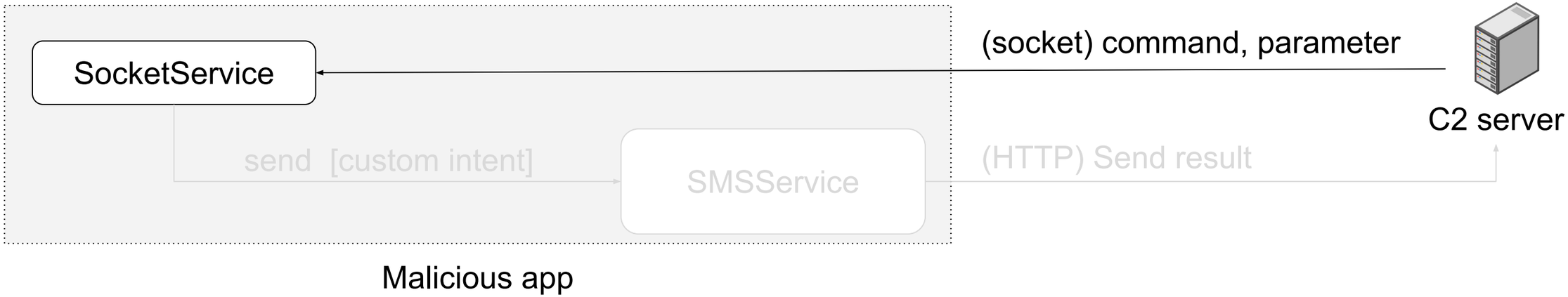
2nd app - Command Processing

- Custom Intent
  - The 2nd, 2nd_main, 2nd_call apps handle commands through ‘custom intent’.



2nd app - Command Processing

- Custom Intent
  - The 2nd, 2nd_main, 2nd_call apps handle commands through ‘custom intent’.

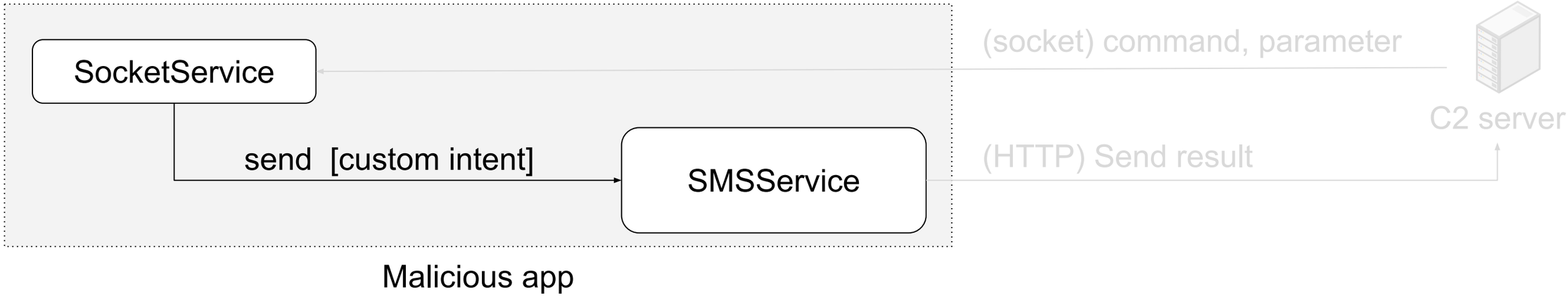


SocketService
Receive commands
“send_sms”

```
this.mSocket.on("set_default_message", this.onSetDefaultMessage);
this.mSocket.on("unset_default_message", this.onUnSetDefaultMessage);
this.mSocket.on("upload_sms", this.onUploadSms);
this.mSocket.on("send_sms", this.onSendSms);
this.mSocket.on("delete_sms", this.onDeleteSms);
```

2nd app - Command Processing

- Custom Intent
  - The 2nd, 2nd_main, 2nd_call apps handle commands through ‘custom intent’.



SocketService
Send [custom intent]
“com.dagger.rmc.intents.SEND_SMS”

```
this.onSendSms = (Object[] arr_object) -> {
    Timber.d("msg: send_sms", new Object[0]);
    if(arr_object.length > 0 && arr_object[0] != null) {
        JSONObject jSONObject0 = (JSONObject)arr_object[0];
        String s = jSONObject0.optString("number");
        String s1 = jSONObject0.optString("body");
        if(!TextUtils.isEmpty(s) && !TextUtils.isEmpty(s1)) {
            this.sendBroadcast(new Intent("com.dagger.rmc.intents.SEND_SMS").putExtra("number", s).putExtra("body", s1));
        }
    }
};
```

2nd app - Command Processing

- Custom Intent
  - The 2nd, 2nd_main, 2nd_call apps handle commands through ‘custom intent’.

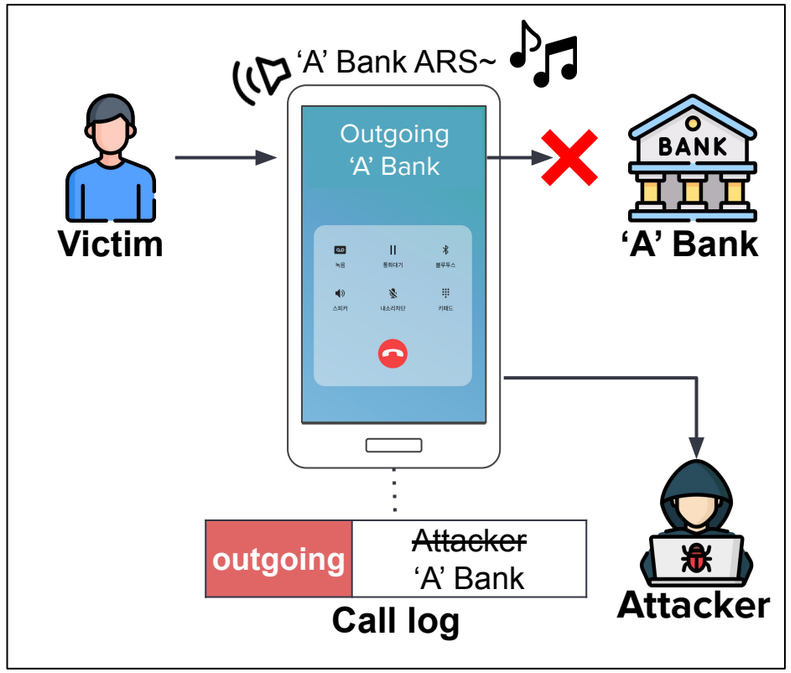
SMSService
Receive and handle [custom inten])
sendMessage()

```
case "com.dagger.rmc.intents.SEND_SMS": {
    this.sendMessage(intent0.getStringExtra("number"), intent0.getStringExtra("body"));
    return;
}
```

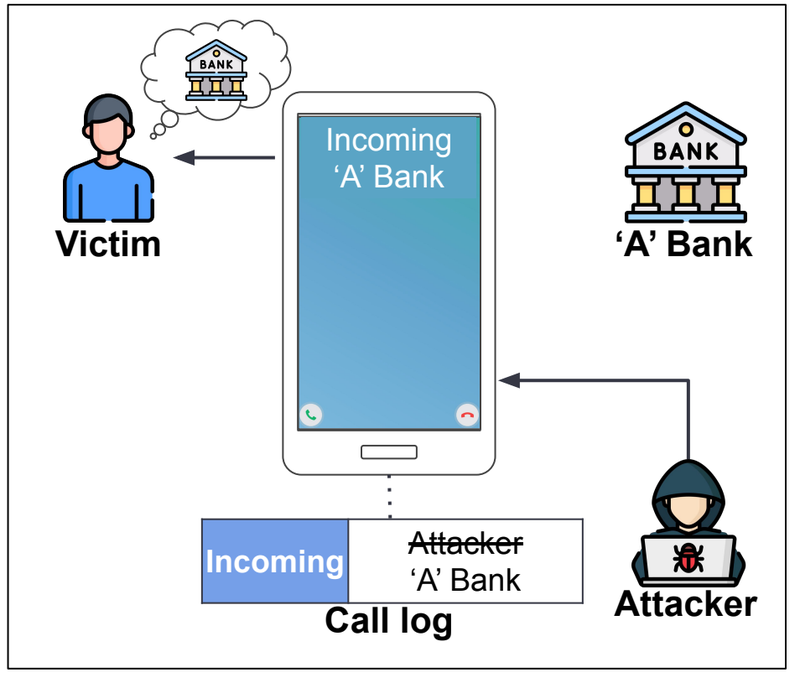
2nd app - Voice Phishing

- Malicious apps(2nd, 2nd_call) intercept or block calls

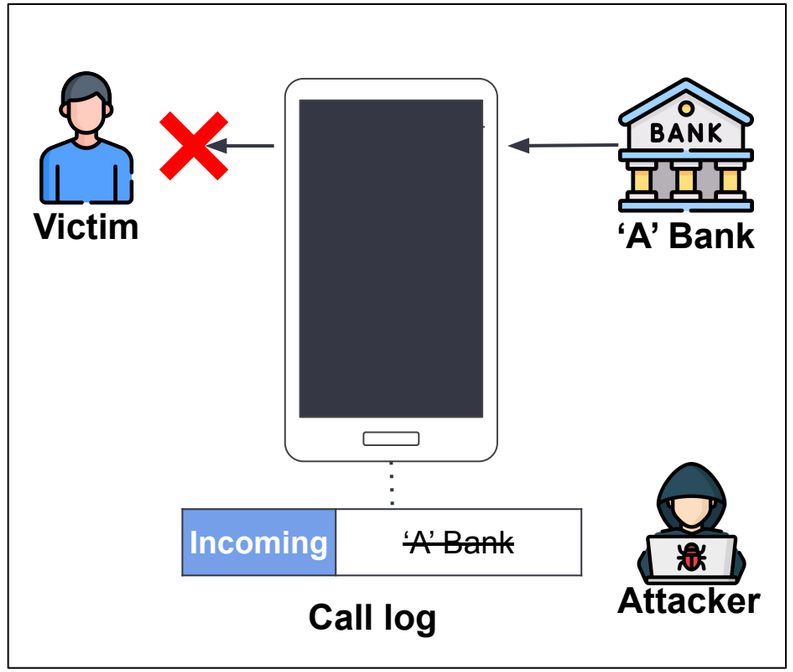
Forced outgoing calls (‘Gangbal’)



Forced incoming calls (‘Gangsu’)

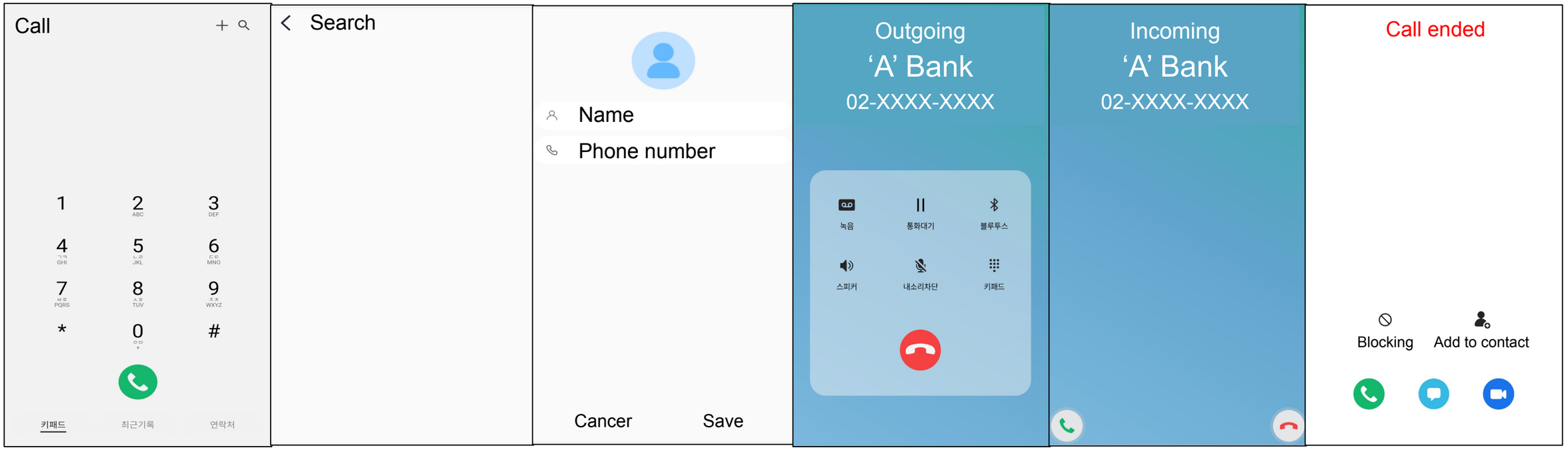


Blocking incoming calls (blacklist)



2nd app - Voice Phishing

- Screens
  - Malicious apps(2nd, 2nd_call) have their custom screens for voice phishing.

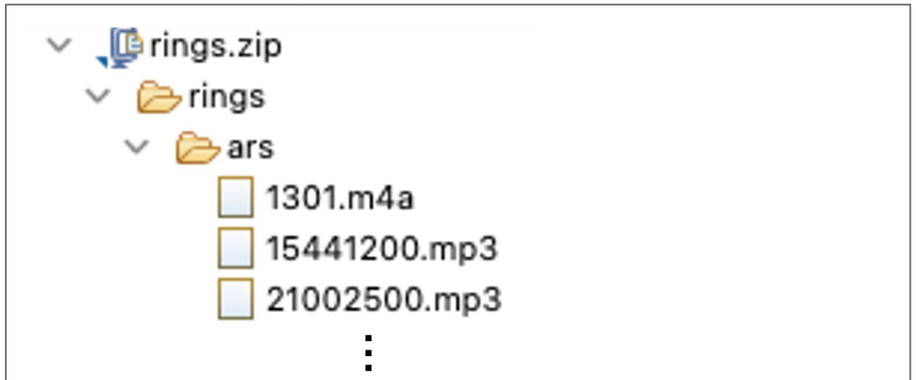


CustomDialerActivity | DialerSearchActivity | ContactActivity | CallActivity (outgoing call) | CallActivity (incoming call) | CallActivity (call ended)

2nd app - Voice Phishing

- ARS files
  - ➢ Malicious apps(2nd, 2nd_call) play files when they intercept victims' outgoing calls.

ARS files (93)



zip file name	unzip result
website.zip	website/ars/*.mp3
nackvlaitje.zip	nackvlaitje/ars/*.mp3
menu_sound.zip	nackvlaitje/ars/*.mp3
123123.zip	nackvlaitje/ars/*.mp3

Phone numbers (368) - ARS files (93)

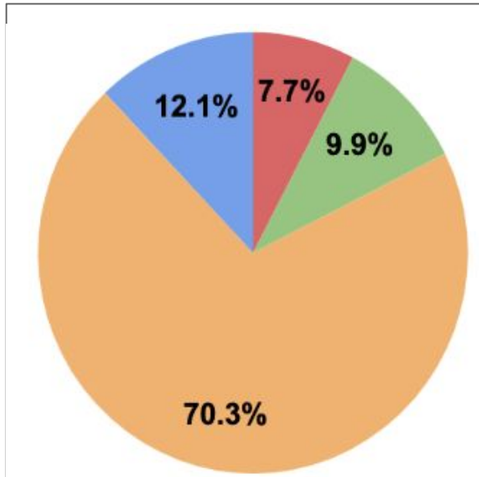
```
list0.add(new Ring(1, "1301", "1301.m4a"));
list0.add(new Ring(2, "021301", "1301.m4a"));
list0.add(new Ring(3, "15448600", "ajucap.mp3"));
list0.add(new Ring(4, "0215448600", "ajucap.mp3"));
list0.add(new Ring(5, "16880070", "ajucap.mp3"));
list0.add(new Ring(6, "0216880070", "ajucap.mp3"));
list0.add(new Ring(7, "18999911", "aqueoncap.mp3"));
list0.add(new Ring(8, "0218999911", "aqueoncap.mp3"))
list0.add(new Ring(9, "15775511", "aqueoncap.mp3"));
                    ⋮
list0.add(new Ring(364, "16700001", "welcomeloan.mp3"));
list0.add(new Ring(365, "0216700001", "welcomeloan.mp3"));
list0.add(new Ring(366, "0221002500", "21002500.mp3"));
list0.add(new Ring(0x16F, "15441200", "15441200.mp3"));
list0.add(new Ring(0x170, "0215441200", "15441200.mp3"));
```

→ save them to the database ("rings" table)

2nd app - Voice Phishing

- ARS files
  - Malicious apps(2nd, 2nd_call) play files when they intercept victims' outgoing calls.

Phone number classification

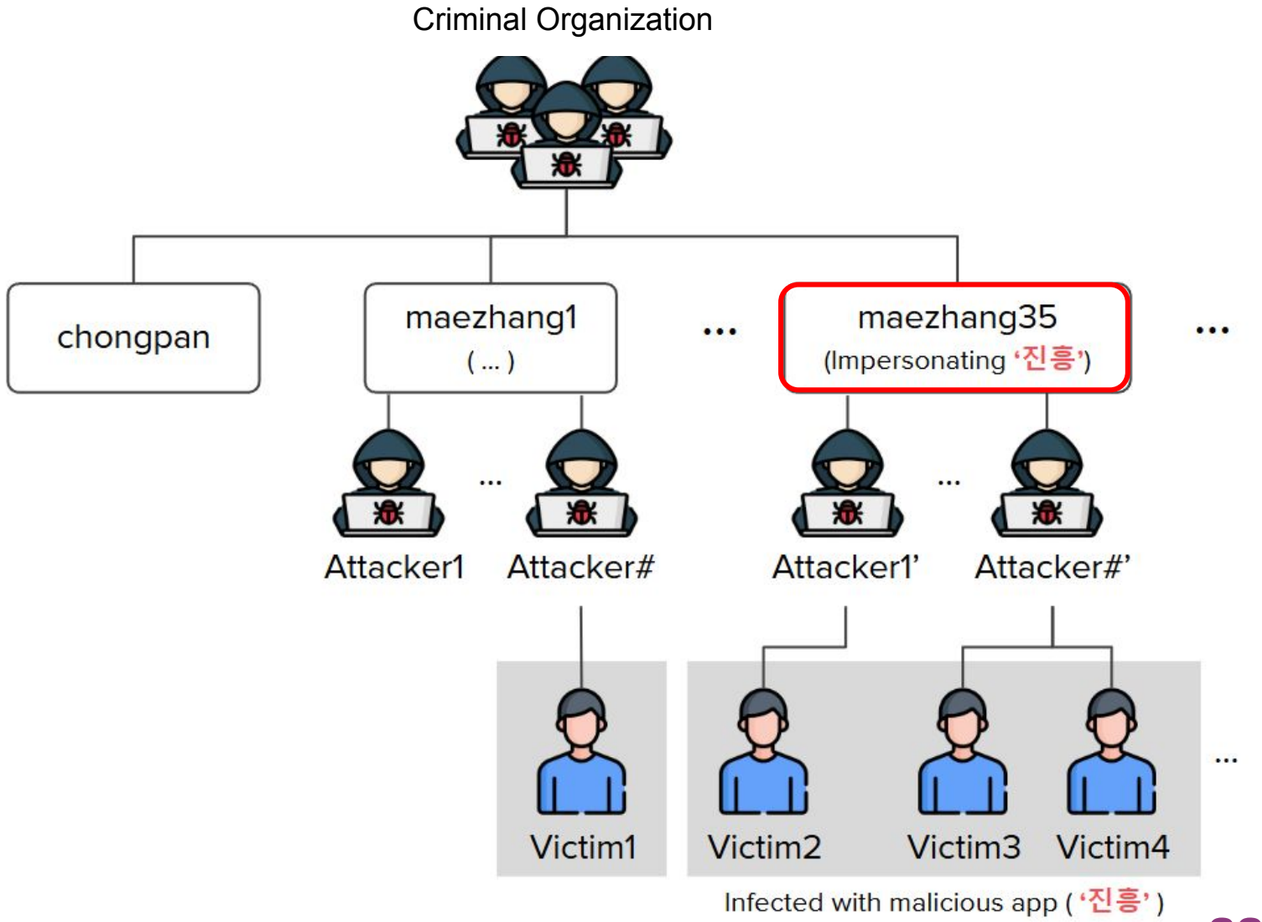


Category		Details
●	Government agency	Financial, Investigative, Tax, and Other related agencies (FSC, FSS, SPO, NTS, KODIT, KINFA, KAMCO)
●	1st financial sector	Banks
●	2nd financial sector	Saving Banks, Insurance companies, Capital firms, Credit card companies and Cooperative federations
●	3rd financial sector	Other lending companies

2nd app - Voice Phishing

- The victim is mapped with the attacker.
- AndroidManifest.xml in 1st app
  - app_id : App identifier
  - app_name : Keyword of financial companies or government agencies

```
<meta-data
  android:name="app_id"
  android:value="maezhang35"/>
<meta-data
  android:name="app_name"
  android:value="진흥"/>
```



2nd app - Voice Phishing

- Phone numbers
  - The malicious apps(2nd, 2nd_call) send the ‘app_id’ and request phone numbers to the C2 server.
    - ex) Visa card : The attacker pretends to be a Visa card employee.
    - ex) Financial Supervisory Service : The attacker blocks the victim from reporting voice phishing

ex) Intercepting outgoing calls

```
{
  "id": 11879,
  "mobile_id": "",
  "name": "비자카드",
  "number": "18992364",
  "number_real": "070[redacted]6142",
  "enabled": true,
  "is_special": false,
  "updated_at": "2023-11-29T02:57:46.000Z"
},
```

Visa card

→ number : Outgoing call made by the victim
→ number_real : The app actually makes a call to the attacker

ex) intercepting incoming calls

```
{
  "id": 2,
  "mobile_id": "",
  "name": "비자카드",
  "number": "0263970114",
  "number_real": "07045[redacted]30",
  "enabled": false,
  "updated_at": "2024-02-19T03:22:24.000Z"
},
```

Visa card

→ number : The app displays it to the victim
→ number_real : Incoming call to the victim

ex) blocking incoming calls

```
{
  "id": 11801,
  "mobile_id": "",
  "number": "1332",
  "name": "",
  "enabled": true,
  "updated_at": "2024-06-17T02:46:58.000Z"
},
```

Financial Supervisory Service

→ number : The app blocks the incoming call

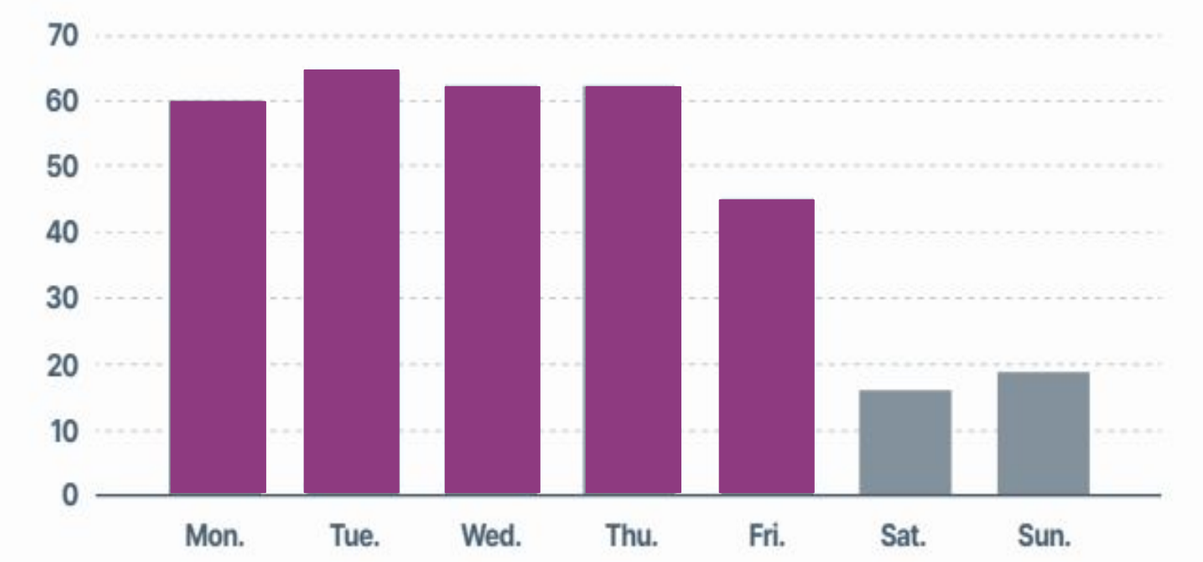
The attacker’s phone number

```
{"number_real":"070[redacted]6142"}
```

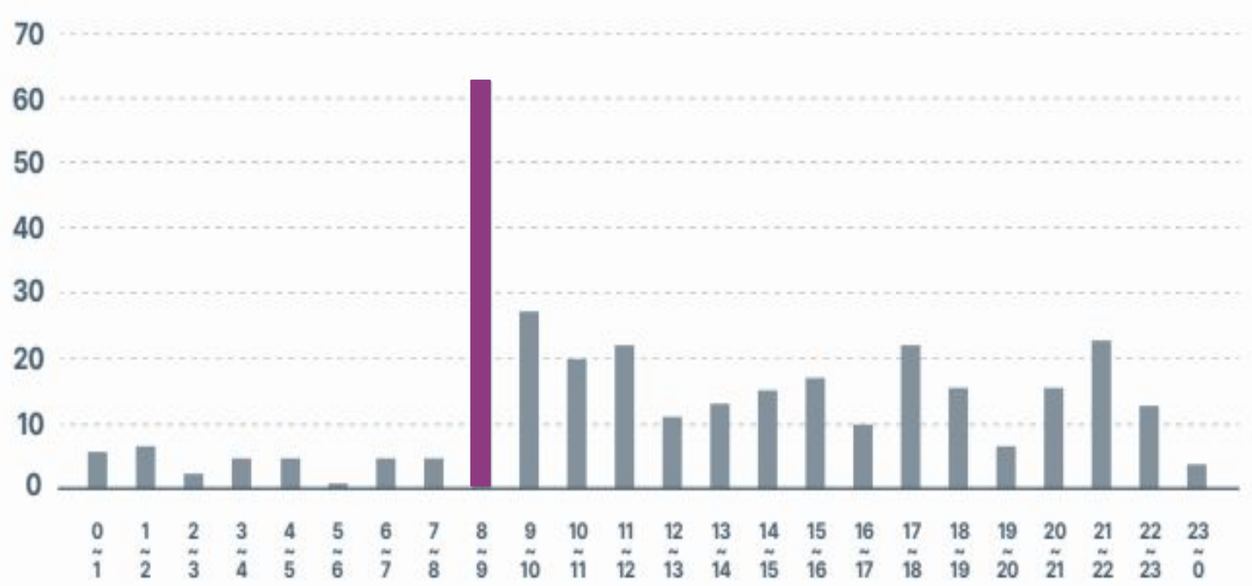
Common Features

- Update statistics
  - Malicious app updates were frequently updated made on weekdays between 8:00 and 9:00 AM

Number of malicious apps updates by day of the week



Number of malicious apps updates by time



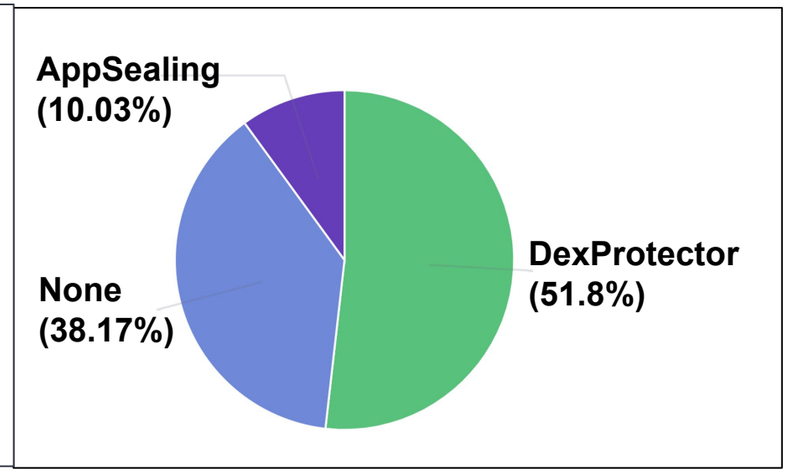
Common Features

- Packer
  - Packers(DexProtector, AppSealing) are applied to malicious apps to hinder analysis.
    - DexProtector (Lical) : Over 50%, applied to the entire period
    - AppSealing (INKA Entworks) : About 10%, applied from 2024.1. to 2024.5.

```
private File createImageFile() throws IOException {
    String s = new SimpleDateFormat(ProtectedAppStart.s("吞")).format(new Date());
    String s1 = ProtectedAppStart.s("吮") + s + ProtectedAppStart.s("吃");
    File file0 = new File(this.getFilesDir() + ProtectedAppStart.s("呔"));
    if(!file0.exists()) {
        file0.mkdir();
    }

    File file1 = File.createTempFile(s1, ProtectedAppStart.s("呕"), file0);
    this.mCurrentPhotoPath = ProtectedAppStart.s("吩") + file1.getAbsolutePath();
    return file1;
}
```

Code example



Statistic

Common Features

❖ Keyword

Huhu / whowho / 후후

- **Code**

```
<string name="alert_message">Please Install 후후</string>
<string name="alert_update_message">Please Update 후후</string>
<string name="app_main">huhu.apk</string>
<string name="app_name">비대면 신청서</string>
<string name="app_package">com.p615.b1003</string>
```

- **Api**

ghdlwejkg30582.freemall-kr.top/api/mobile/huhu_info


```
{
  "appVersion": "4.0.4",
  "url": "https://store1.gofile.io/download/direct/b730025f-1d2a-4ae
  "url2": "https://bit.ly/3pPuXwP",
  "url3": "",
  "packageName": "com.nkninini.bhbhbb",
  "appName": "SecurityProgram",
```


Paekjo / dagger

- **Certificate**

Subject	CN=paekjo, OU=Unknown, O=paekjo, L=Unknown, ST=Unknown, C=Unknown
Type	X.509
Validity	
From	Thu Dec 09 13:57:26 KST 2021
To	Mon Apr 26 13:57:26 KST 2049
Version	3

- **Custom Intent**

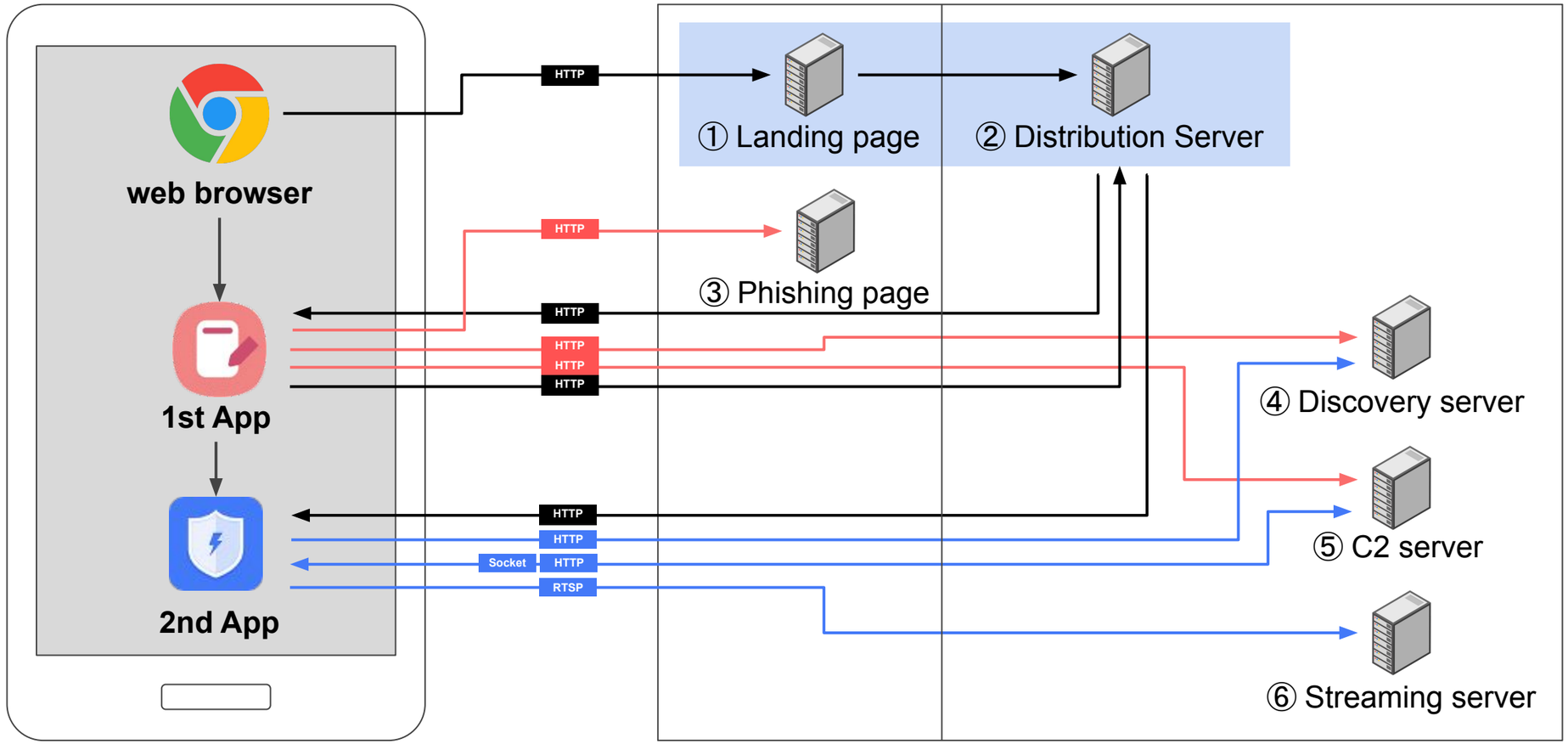
```
this.onStreamMic = (Object[] arr_object) -> {
    Timber.d("msg: stream_mic", new Object[0]);
    this.sendBroadcast(new Intent("com.paekjo.rmc.intents.STREAM_MIC"));
};
this.onStreamDisplay = (Object[] arr_object) -> {
    Timber.d("msg: stream_display", new Object[0]);
    this.sendBroadcast(new Intent("com.paekjo.rmc.intents.STREAM_DISPLAY"));
};
this.onUploadContacts = (Object[] arr_object) -> {
    Timber.d("msg: upload_contacts", new Object[0]);
    this.sendBroadcast(new Intent("com.paekjo.rmc.intents.UPLOAD_CONTACTS"))
```

4. Infrastructure

Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

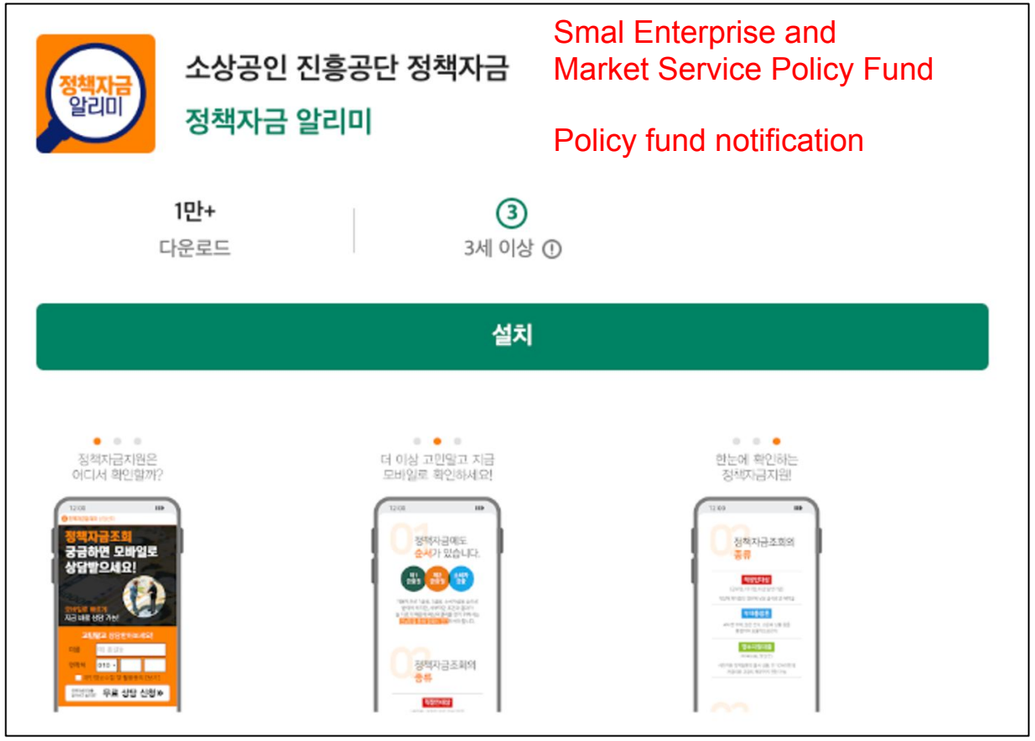
Infrastructure

- Diagram



① Landing page

- Role : Tricking victims into download the 1st app
- Features : It looks identical to the Google Play(Android's official app store)



Landing page (kmso)

Landing page (somin)

② Distribution server

- Role : Distribution of malicious apps
- History : C2 server → File share & Hosting services → Distribution server

History	Date	Type	File name	
C2 server	2022.9.	① C2 server	huhu.apk	2nd_app
File-sharing services	2023.1.	② catbox	[a-zA-Z0-9]{6}.apk	
	2.	② gofile	huhu_[version].apk	
	6.		Security[version].apk	
File-sharing, hosting services (2nd → 2nd_main & 2nd_call)	7.	② gofile	Call.apk, Main.apk	2nd_call & 2nd_main
	12.	③ dothome	Call.apk, Main.apk	
	2024.3.	② gofile	Call.apk, Main.apk	
Distribution server	7.	④ Distribution server	Call.apk, Main.apk	

③ Phishing page server

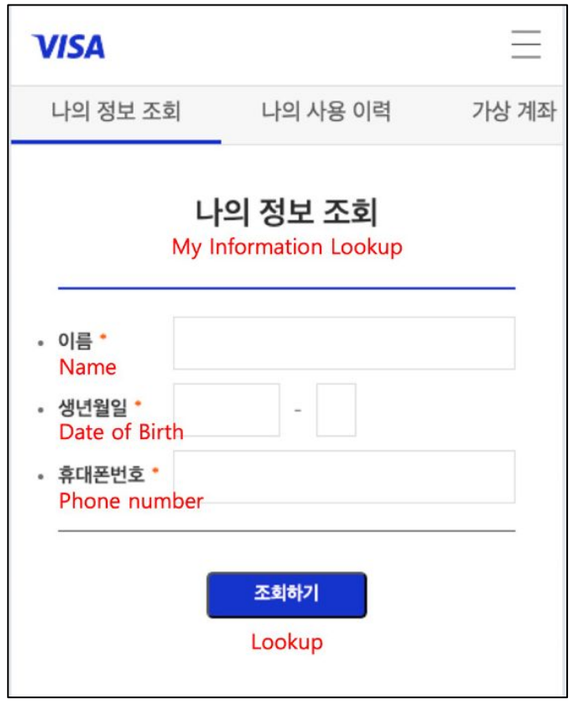
- Role : Personal information theft
- Features : Pretending to be a financial companies or government agencies.

Official homepage

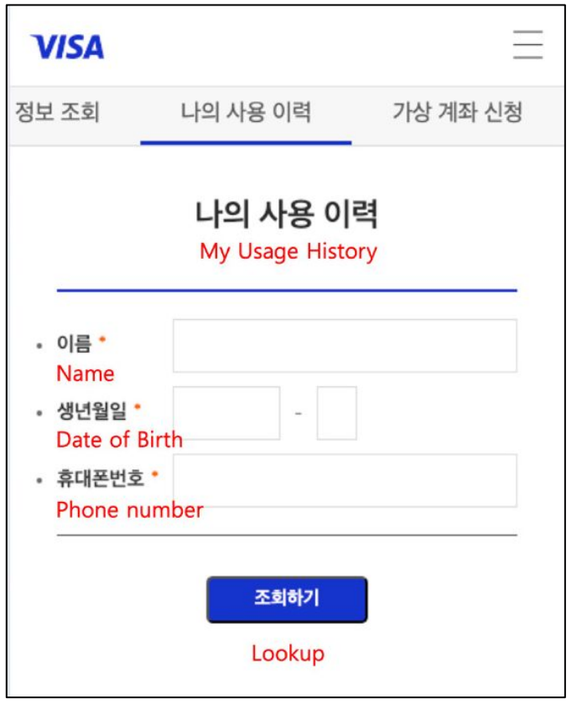
Phishing page

③ Phishing page server

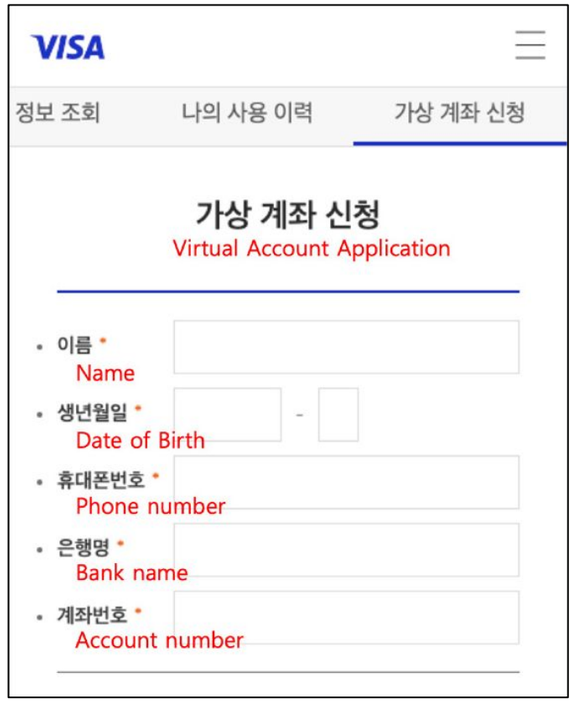
- Role : Personal information theft
- Features : Pretending to be a financial companies or government agencies.



Phishing page
(‘My Information Lookup’)



Phishing page
(‘My Usage History’)



Phishing page
(‘Virtual Account Application’)

④ Discovery, ⑤ C2, ⑥ Streaming server

- Role :
  - Discovery server : Providing addresses of C2 server & Streaming server
  - C2 server : Issuing commands, providing voice phishing data, and more.
  - Streaming server : Streaming camera / mic. / screen

Server address

- Server address found in plaintext
  - ① Landing page server, ② Distribution server, ③ Phishing page server

Landing page server address

The attacker send it directly to the victim.

Distribution server address

The Landing page
or the C2 server provides it.

```
"url": "https://store0.2024tec.top/1721776631177/Call.apk",
"url2": "https://store0.2024tec.top/1721776631421/Main.apk",
"appVersion": "4.5.0",
"packageName": "kr.or.knfa.nfcs.ci",
"packageName2": "kr.or.knfa.nfcs.gi",
"appName": "스마트T전화",
"appName2": "스마트보안",
```

Phishing page server address

It is hard-coded in the 1st app.

```
this.e.a.s.loadUrl("https://site111.mallmaster.top/ibk/index.html");
this.e.a.s(1, b.d);
```

```
this.e.a.s.loadUrl("https://site111.mallmaster.top/ibk/order.html");
return;
```

Server address

- Server address found in plaintext
  - Keywords and epoch time are used

Landing page server address

The attacker send it directly to the victim.

Distribution server address

The Landing page
or the C2 server provides it.

```
"url": "https://store0.2024tec.top/1721776631177/Call.apk",
"url2": "https://store0.2024tec.top/1721776631421/Main.apk",
"appVersion": "4.5.0",
"packageName": "kr.or.knfa.nfcs.ci",
"packageName2": "kr.or.knfa.nfcs.gi",
"appName": "스마트T전화",
"appName2": "스마트보안",
```

→ epoch time
(2024.7.24. 08:17:11.421 (KST))

Phishing page server address

It is hard-coded in the 1st app.

```
this.e.a.s.loadUrl("https://site111.mallmaster.top/ibk/index.html");
this.e.a.s(1, b.d);
```

```
this.e.a.s.loadUrl("https://site111.mallmaster.top/ibk/order.html");
return;
```

→ Keyword of the financial company (**I**ndustrial **B**ank of **K**orea)

Server address

- Server address found in encoded-text
  - ④ Discovery server, ⑤ C2 server, ⑥ Streaming server

Discovery server address

It is encoded and hard-coded in the apps

```
static {
    ServerInfoService.SERVER_URLS = new String[]{"eWVlYWIrPj51fmZ_P2J4f3lwfzxzcH96P3J-fD55ZHlk",
            "eWVlYWIrPj51fmZ_P356PGJkcnJ0YmI_cn58PnlkeWQ="};
}
```

C2, Streaming server

The discovery server provides them

```
{
  "a01": "eWVlYWIrPj52eXV9ZnR7enYiISQpIz93Y3R0fHB9fTx6Yz9lfmE=",
  "b05": "Y2ViYWIrPj4jICI_ICIoPyMiIj8gIiArKSIjIz59eGd0",
  "a07": "eWVlYWIrPj5mZmY_f3k8Znh_P3J-fA=="
}
```

Decoding algorithm

Base64 + XOR (key : 17)

```
public static String decode(String s) {
    byte[] arr_b = Base64.decode(s, 8);
    for(int v = 0; v < arr_b.length; ++v) {
        arr_b[v] = (byte)(arr_b[v] ^ 17);
    }

    return new String(arr_b, StandardCharsets.UTF_8);
}
```

Server address

- Server address found in encoded-text
  - Decoding with Base64 & XOR (key : 17)

Discovery server address

It is encoded and hard-coded in the apps

```
static {
    ServerInfoService.SERVER_URLS = new String[]{ https://down.sinhan-bank.com/huhu ,
                https://down.ok-success.com/huhu };
}
```

C2, Streaming server

The discovery server provides them

```
{
  "a01":  (      C2 server      ) https://ghdlwejkg30582.freemall-kr.top
  "b05":  (Streaming server) rtsps://213.139.233.131:8322/live
  "a07":  (Alternative server) https://www.nh-win.com
}
```

Decoding algorithm

Base64 + XOR (key : 17)

```
public static String decode(String s) {
    byte[] arr_b = Base64.decode(s, 8);
    for(int v = 0; v < arr_b.length; ++v) {
        arr_b[v] = (byte)(arr_b[v] ^ 17);
    }

    return new String(arr_b, StandardCharsets.UTF_8);
}
```

Cloudflare

- The criminal organization uses Cloudflare
  - They can hide the IP and location of their servers.
  - Therefore, they can prepare for blocking and continue their malicious behavior.

Server	Example of server address	IP	Nation	Note
Phishing page	site111.mallmaster[.]top	172.67.168[.]51, 104.21.26[.]2	-	Cloudflare
Phishing page	visakor[.]info, visakor[.]asia	8.217.194[.]83	HK	Alibaba US Technology Co., Ltd.
Discovery	down.sinhan-bank[.]com	172.67.134[.]184, 104.21.6[.]104	-	Cloudflare
Discovery	down.ok-success[.]com	172.67.170[.]125, 104.21.87[.]177	-	Cloudflare
C2	jhjdlkjeifhsl989.na333[.]top	172.67.168[.]210, 104.21.38[.]238	-	Cloudflare
Streaming	213.139.233[.]131	213.139.233[.]131	JP	Net Innovation LLC
Distribution	*.2024tec[.]top	172.67.141.[.]157, 104.21.94[.]238	-	Cloudflare

5. Voice Phishing Scenario

Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

Scenario

- Voice Phishing Crime Phases

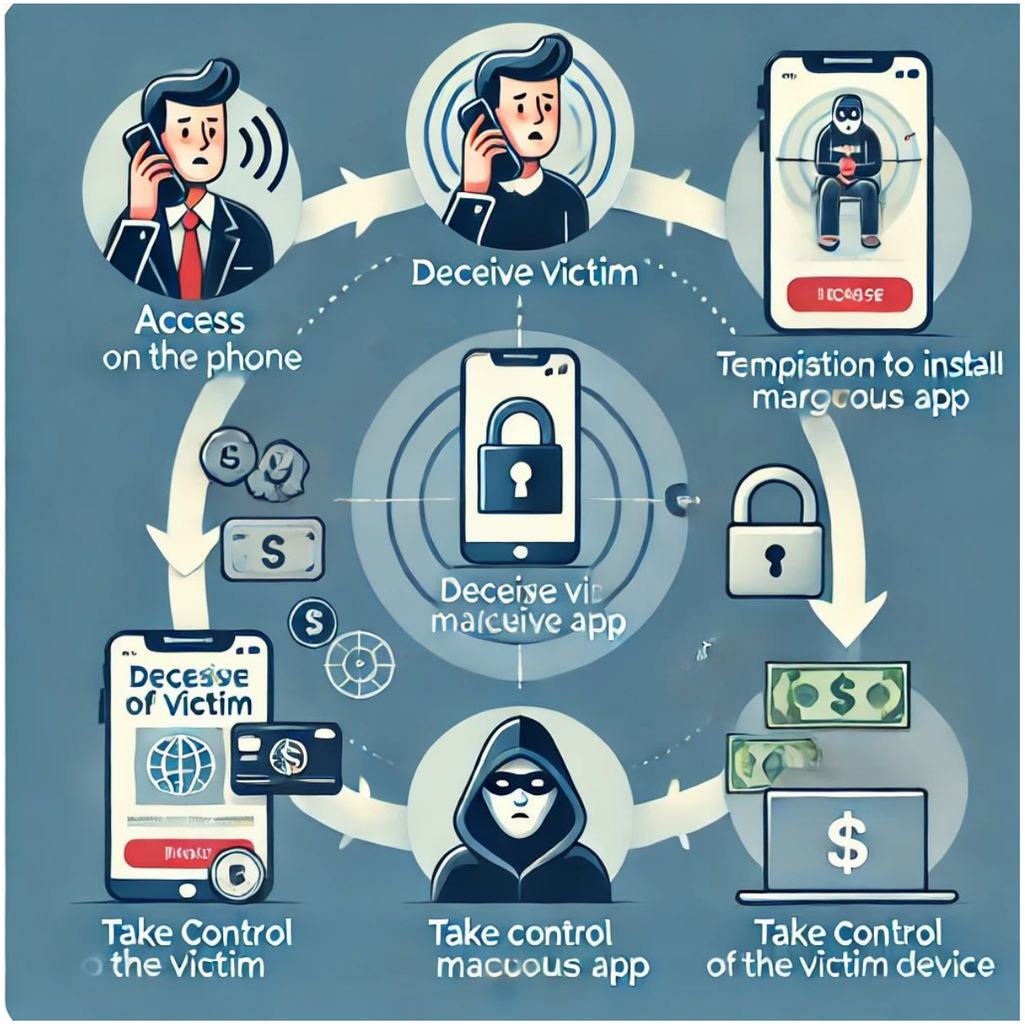
① Access to victim

② Deceive victim

③ Temptation to install malicious app

④ Take control of the victim device

⑤ Take the victim's money

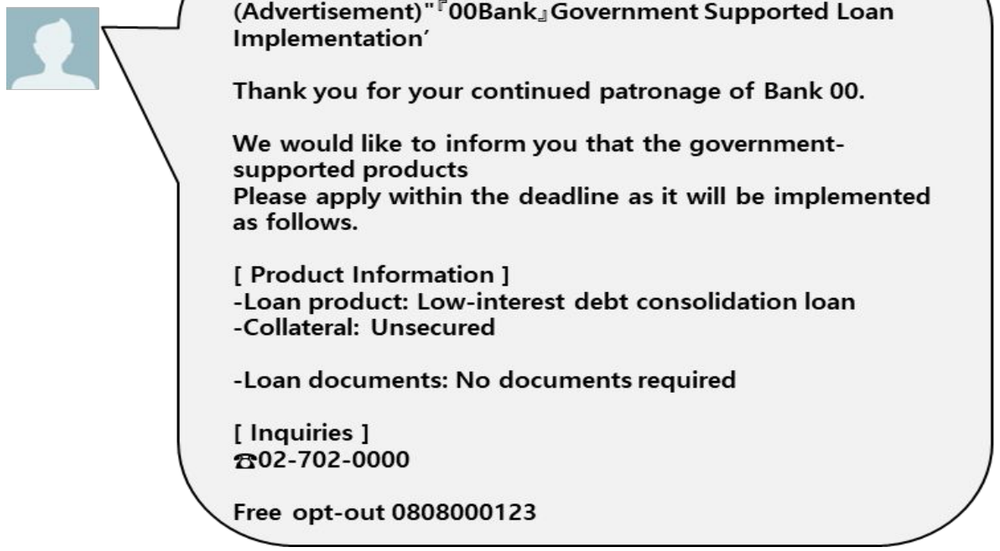


※ Scenario covering all voice-phishing malware, not just Operation BlackEcho

① Access to victim

- Attackers use various means to lure victims, for example, SMS, Facebook, instagram, etc
  - ➢ They usually offer **unusually good terms on loans** or **threaten victims by posing as prosecutors.**

Spam Message



SNS Advertisement

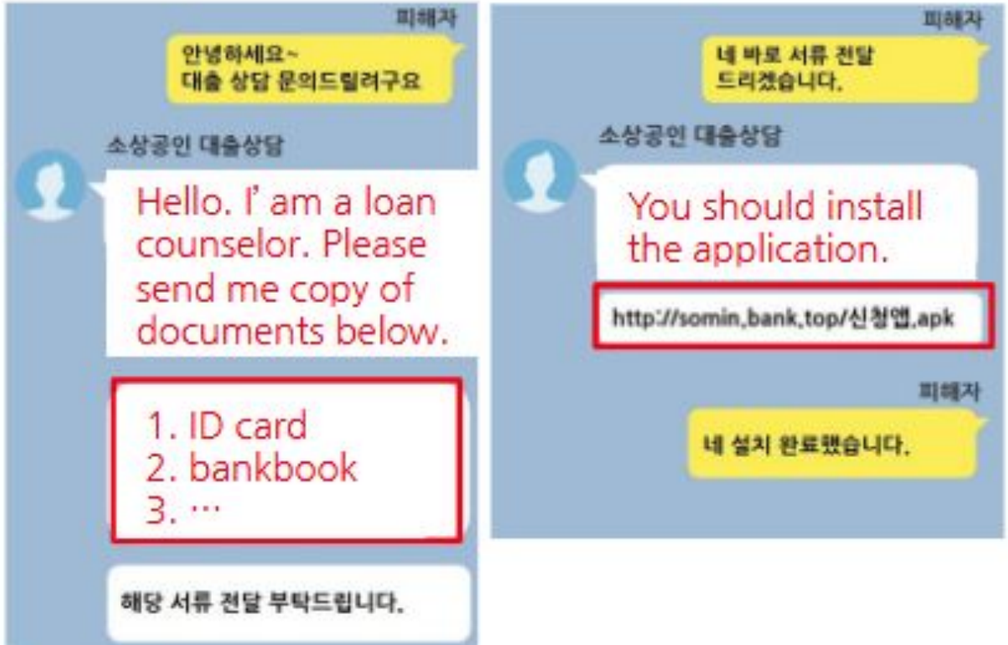
② Deceive victim (1/2)

❖ Attacker disguises the process as a legitimate financial loan, and the **victim in need of money follows the attacker's instructions.**

➢ The attacker asks the victim for sensitive documents containing personal information.

Fake business card or ID card

Request Document & Deliver Malicious App



② Deceive victim (2/2)

❖ Attackers use a variety of methods to disable the victim's cognitive abilities by pressuring the victim's mind.

1) **Impersonating the social status of prosecutors, financial institutions to pressure victim**

- In particular, ‘criminal involvement’ and ‘economic disadvantage’ are used to frighten victims.

1) **Pressuring victims with time pressure and legal penalties**

- Pressure victim to make a quick decision (ex : withdraw cash) in a short amount of time

1) **Isolating the victim psychologically**

- When installing the malicious app, the victim believes they are speaking to the police, financial institutions, etc. The victim is unable to speak to their family.

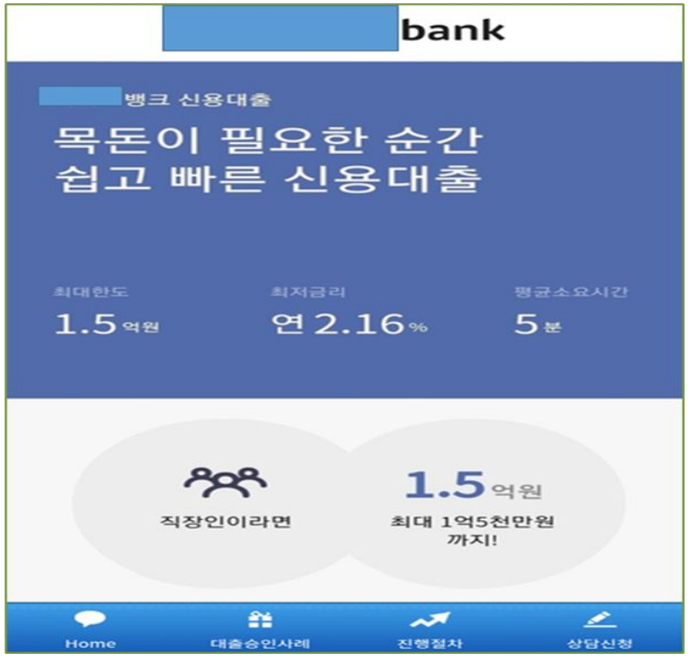
※ **Reference :** "A Study on the Process of Voice Phishing Crime in Korea" by Choi Kwan, Korean Police Studies Review, September 24, 2015
"Analysis of Institutional Impersonation Voice Phishing Scenarios: Focusing on Victims' Psychological Factors" by Lee Yong-soo, Korean Police Studies Review, June 2024

③ Temptation to install malicious app (1/2)

- Victim accesses a download page and installs a malicious app to apply for a loan.
  - **South korea has a very developed mobile banking service** and many financial companies offer mobile apps.

Malicious App download page

Malicious App display

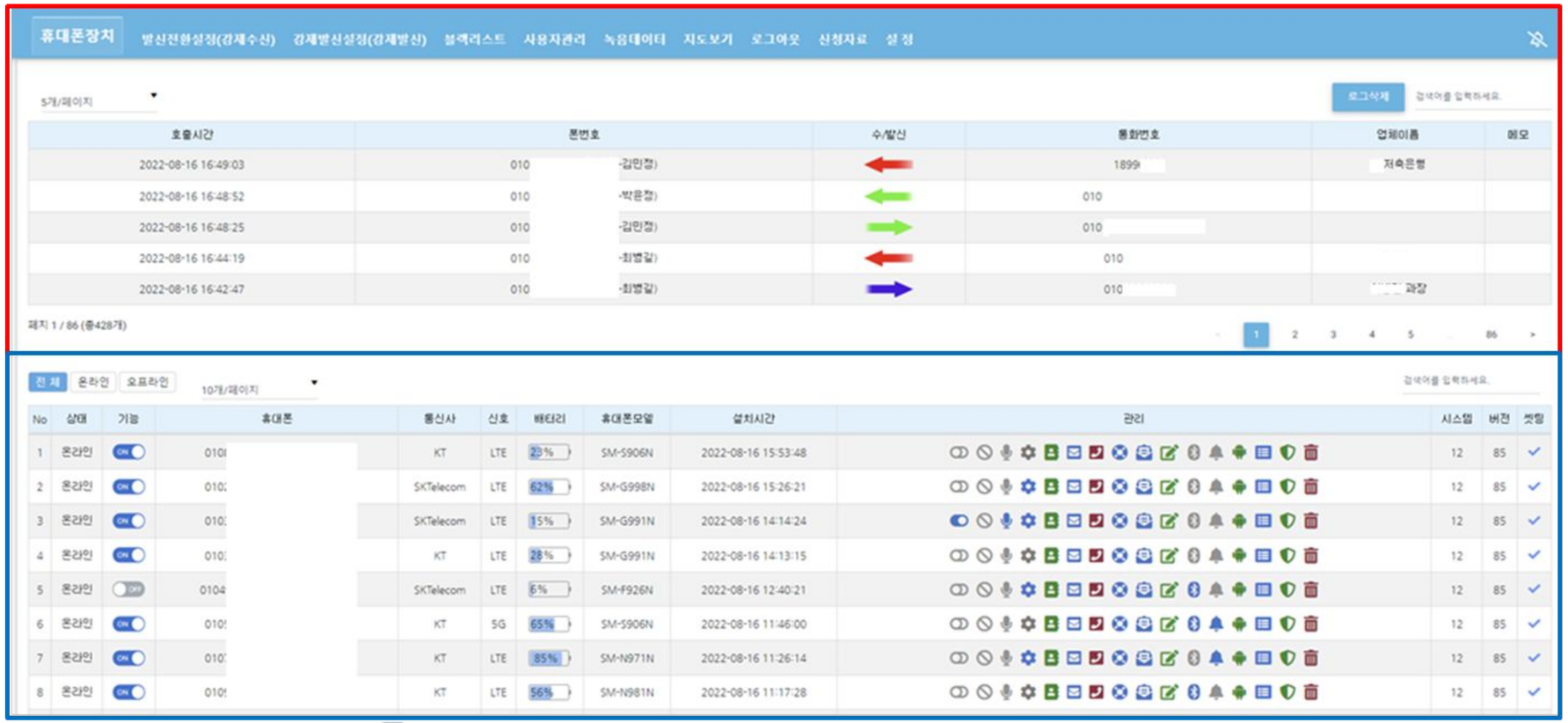


③ Temptation to install malicious app (2/2)

- If a malicious app is installed on phone, it can **steal phone history, contacts, and other information and control calling's functions.**
  - **Control examples: block specific calls, manipulate outgoing calls, change contact information**

④ Take control of the victim device (1/2)

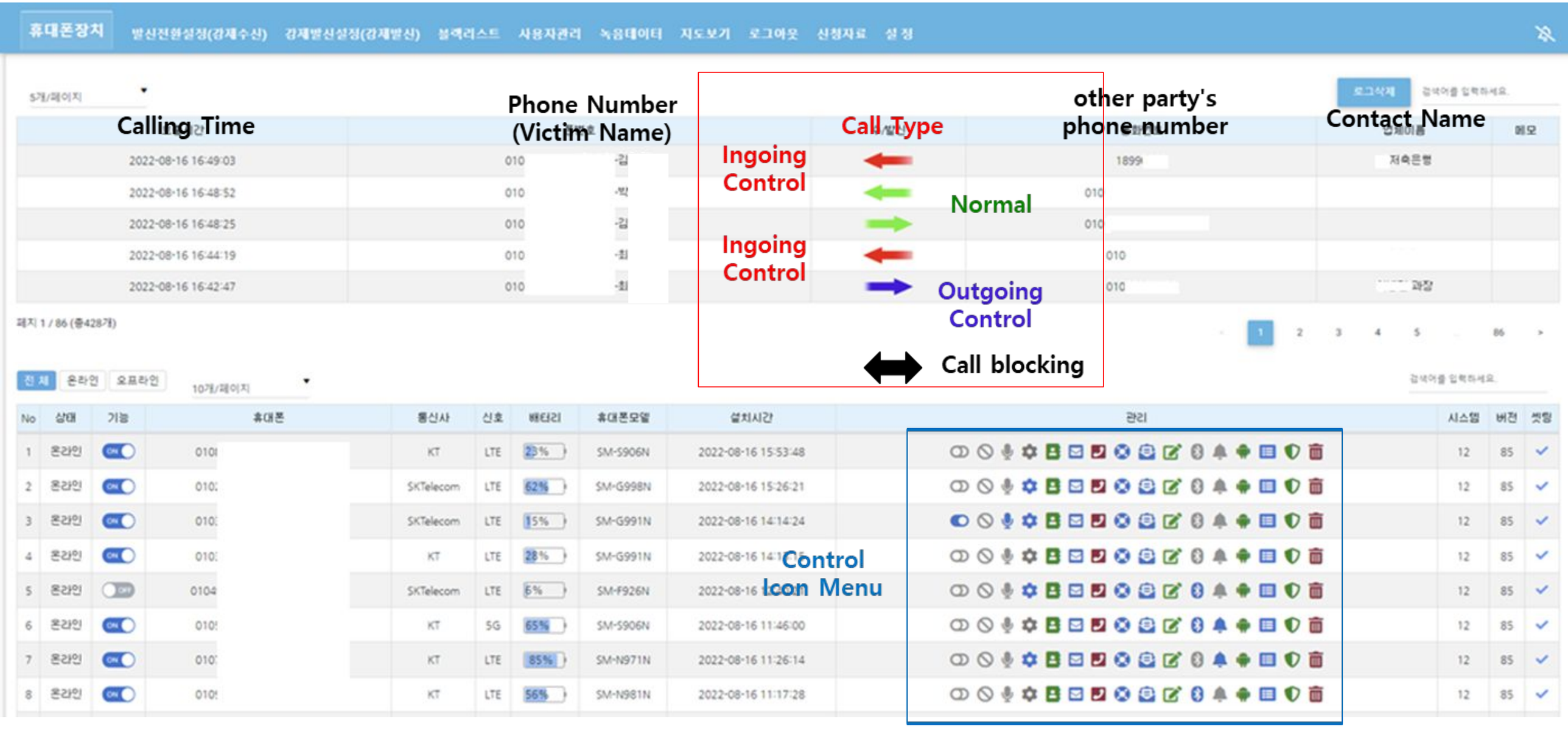
❖ Attacker monitors everything about victim, **All calls are routed to the criminal organization.**



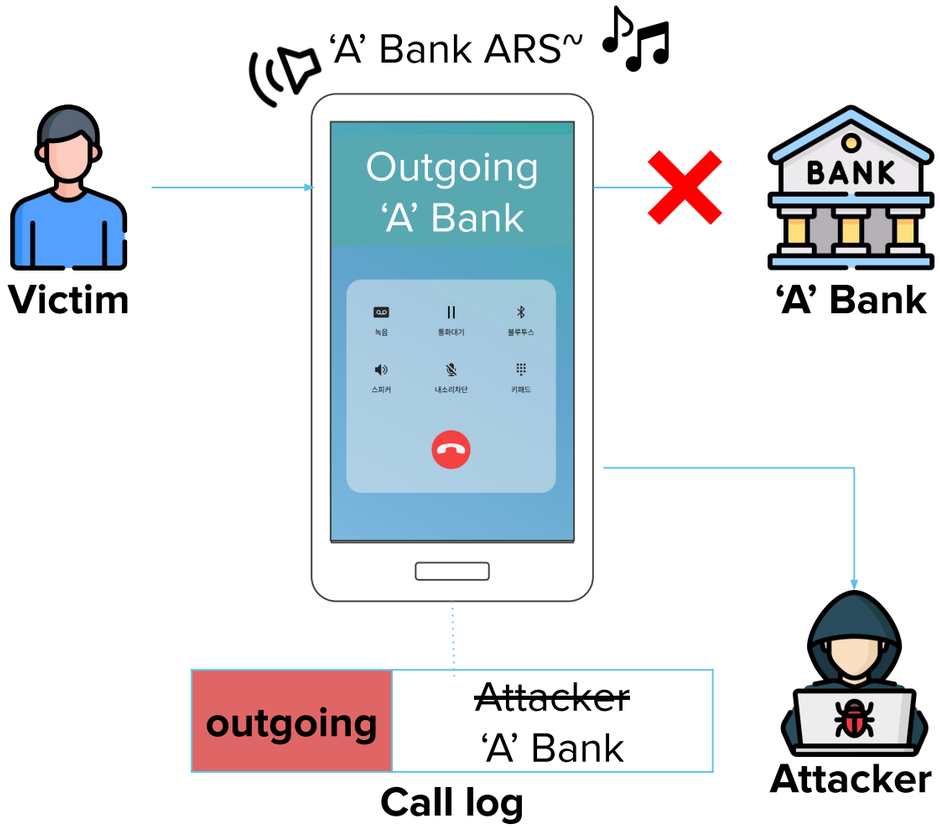
Infected Phone Call History (Real-time Monitoring)

Infected Phone List (Phone Comand/Control)

[Control Server – Manage Phone Menu]


휴대폰장치
발신전원설정(강제수신)
강제발신설정(강제발신)
블랙리스트
사용자관리
녹음데이터
지도보기
로그아웃
신청자료
설정
Calling Time
Phone Number
(Victim Name)
Call Type
other party's
phone number
Contact Name
Ingoing
Control
Normal
Ingoing
Control
Outgoing
Control
Call blocking
Control
Icon Menu

Call Control Type - Forced outgoing calls



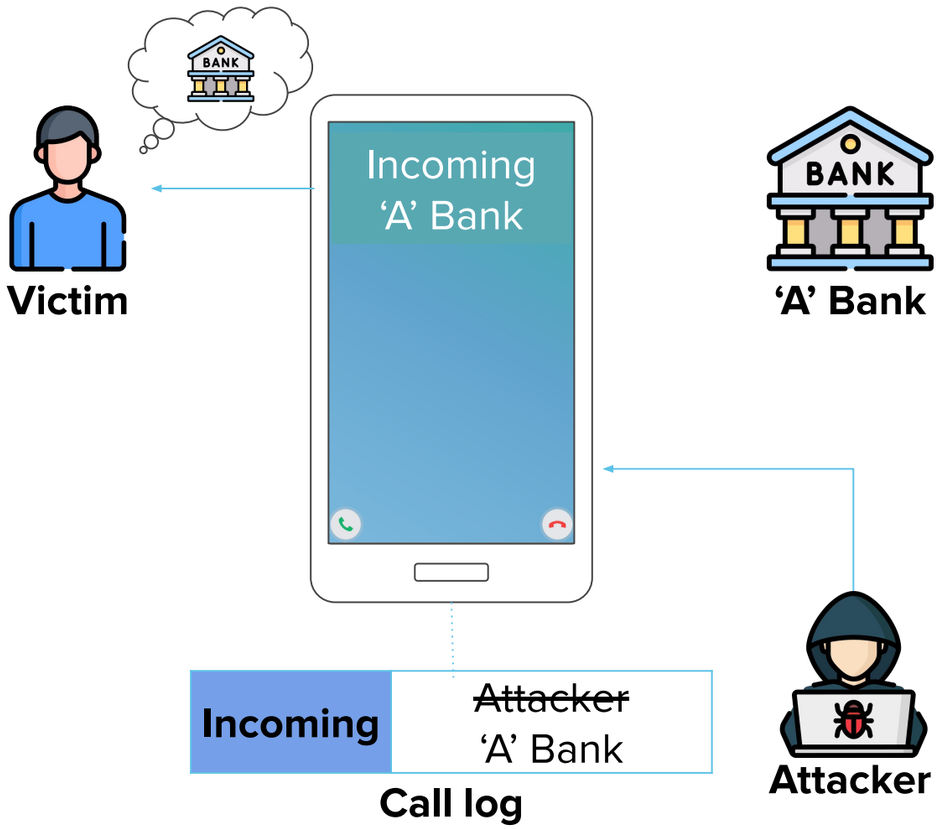
① The victim makes a call to 'A' bank.

② The malicious app plays an ARS file for 'A' bank, ends the outgoing call.

③ The malicious app initiates new call to the attacker, and changes the call screen.

④ After the victim finishes the call, the malicious app modifies the outgoing call log, from the attacker to 'A' bank.

Call Control Type - Forced incoming calls

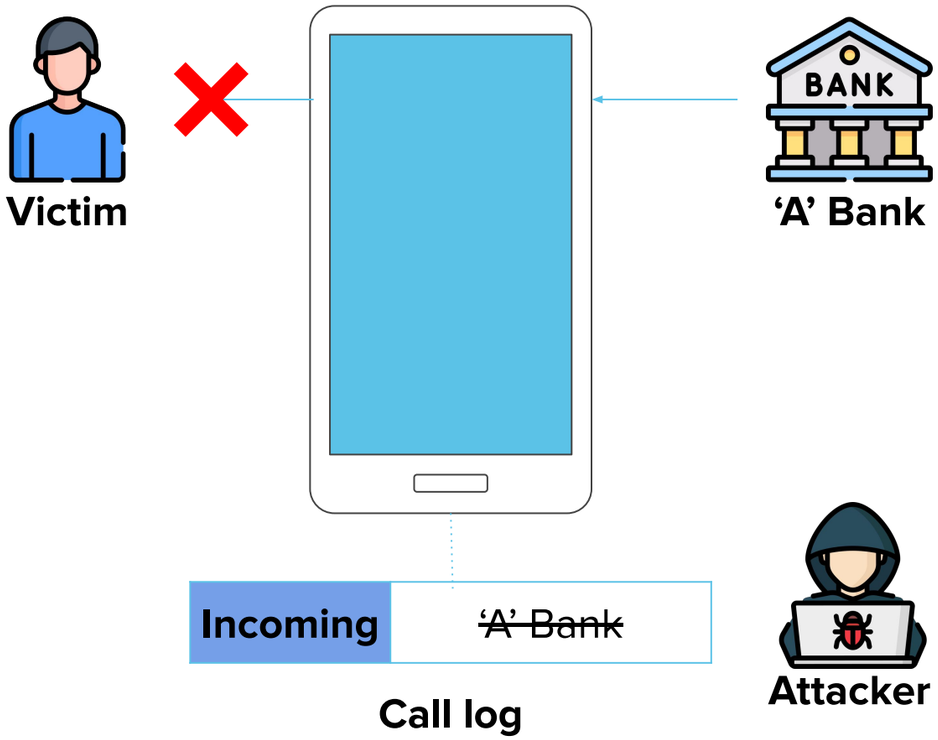


① The attacker makes a call to the victim.

② The malicious app changes the call screen to trick the victim into believing that the call is from 'A' bank rather than from the attacker.

③ After the call ends, the malicious app modifies the incoming call log, from the attacker to 'A' bank.

Call Control Type - Forced incoming calls blocking



① 'A' bank makes a call to the victim.

② The malicious app ends the call from 'A' bank.

③ The malicious app deletes the incoming call log.

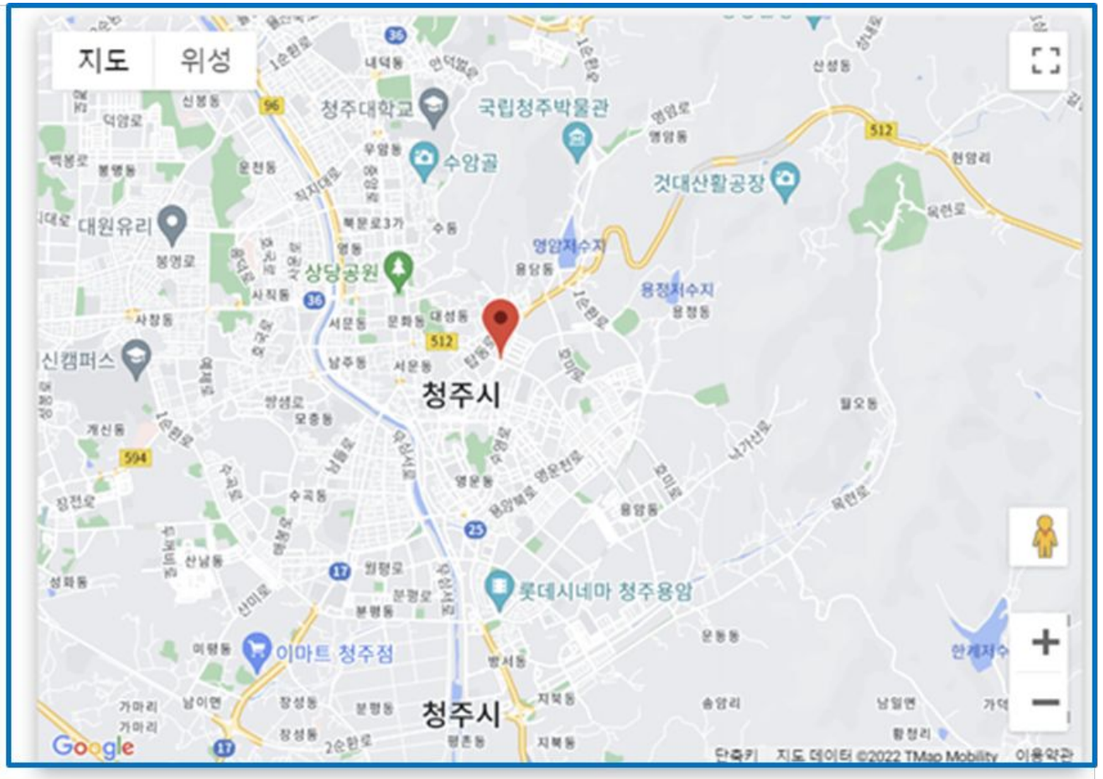
④ Take control of the victim device (2/2)

- Attacker monitors everything about victim, **All calls are routed to the criminal organization.**

⑤ Take the victim's money

❖ Finally, attacker sends a **cash collector to collect the victim's money.**

Infected Phone List



Infected phone location on Google Maps

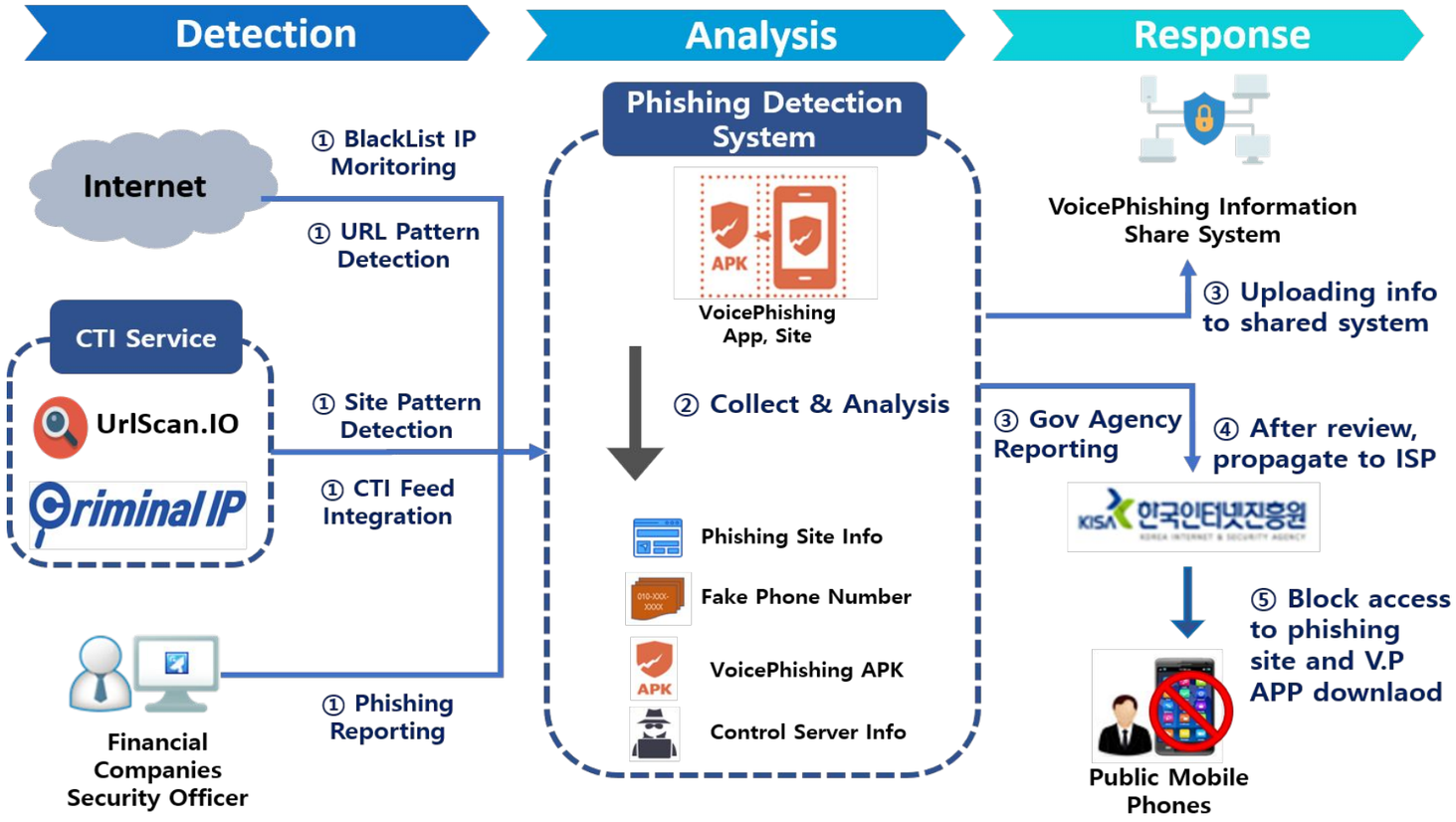
[Control Server – Show Map Menu]

6. Countermeasure

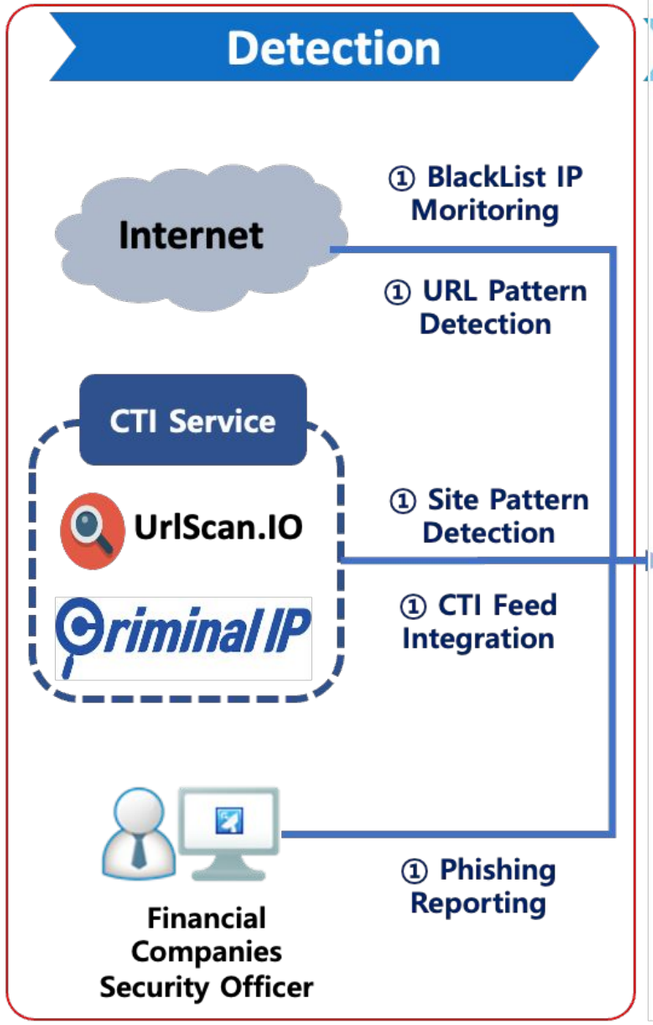
Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

Phishing Kill Chain - Introduction

❖ To combat phishing crimes, including voice phishing, **we proactively take down phishing sites and voice phishing app download sites.**



Phishing Kill Chain - Detection

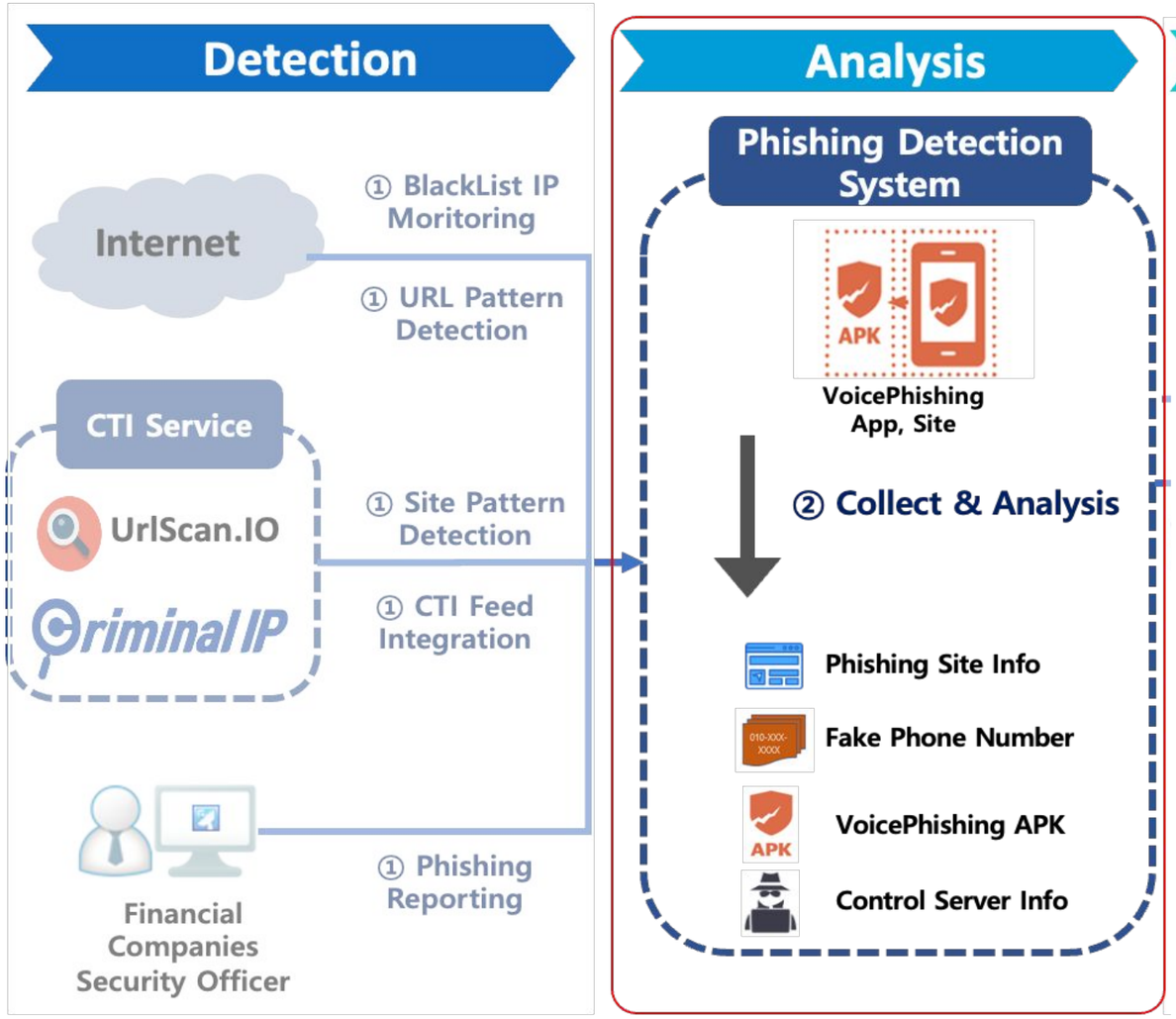


Analysis | Response

Detection method

- ❖ Phishing detection system
  - ➢ Blacklist IP Monitoring
  - ➢ URL pattern detection
- ❖ Use of external intelligence
  - ➢ Site pattern detection (Using API)
  - ➢ CTI Feed Integration
- ❖ Report from security officer

Phishing Kill Chain - Analysis



- **Collect**
  - Phishing Site html, Screenshot
  - Site info (ip, url, asn, country,.. etc)
- **Analysis**
  - APK info (Hash, Package name, App name)
  - App's Control Server info (URL)
  - App's Fake Phone Number (from hardcoding or Control Server communication)

Phishing Kill Chain - Response

Detection → Analysis → Response

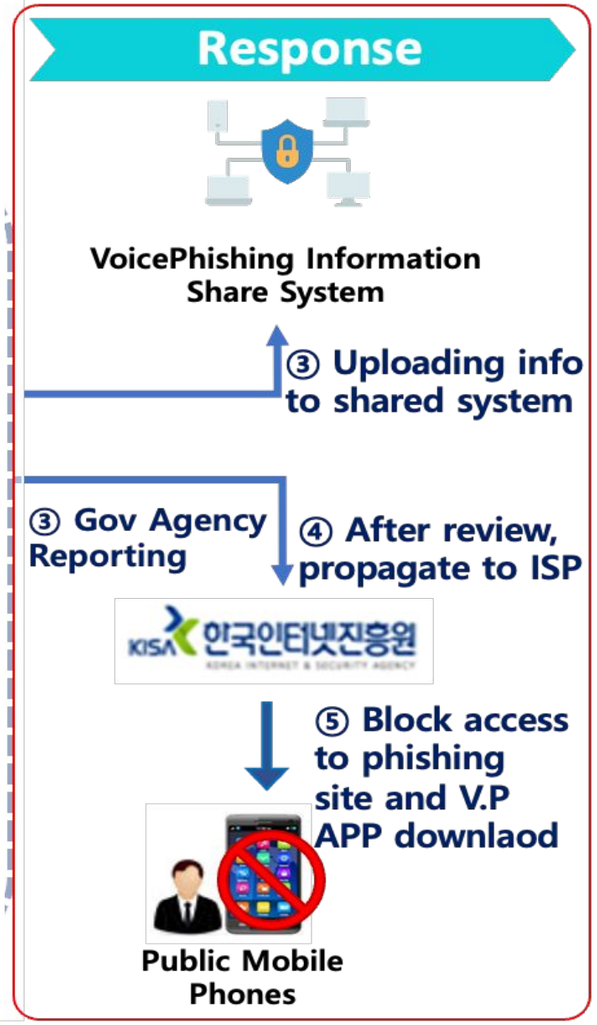
❖ Share

➢ Sharing information with financial and security companies through a sharing system called VFISS
(VoicePhishing Information Sharing System)

❖ Report

➢ Report phishing sites to KISA
(Korea Internet & Security Agency)

➢ KISA asks South Korean ISPs to block



Sharing Info List

- Financial and security companies use this information to prevent voice phishing.
  - Malware app: App hash information, control server information, impersonation agency
  - Phishing Site : IP, URL, Impersonation agency, Screenshot
  - Therefore, they can prepare for blocking and continue their malicious behavior.

Malware APP

DATA	
id	208105
datetime	2024-03-11 16:17:28
c2_ip	http://154.19.69.122
c2_nation	
distribution_ip	61.223.153.22
apk_name	typing works
pkg_name	com.huNhpw.jYanzF
apk_md5	c66753ea78593fc65d77e7d3f6bca473
apk_link	http://61.223.153.22/3adQsmsXph.end
company	인피니그루
origin_phonenum	
Attachment	다운로드

Phishing Site

DATA	
id	208553
datetime	2024-03-20 04:53:09
company	검찰청
distribution_ip	61.223.129.152
distribution_url	http://61.223.129.152
Attachment	다운로드

Fake Phone Number

DATA	
id	208550
datetime	2024-03-20 02:30:37
c2_ip	172.67.196.50
c2_nation	
fake_phonenum	07047844169
origin_phonenum	
Attachment	다운로드

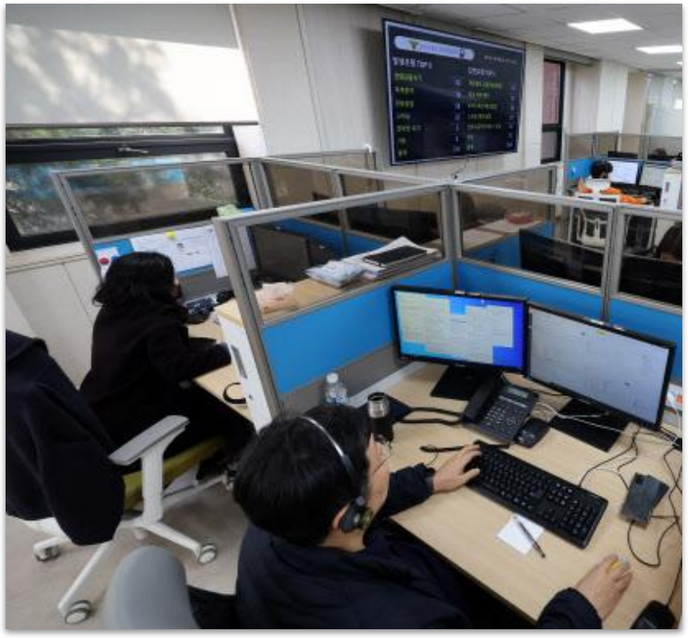
Korean Gov., Police, Financial Response

- With the rise in the prevalence of voice phishing crimes, **many industries are working to combat the crime.**

Goverment

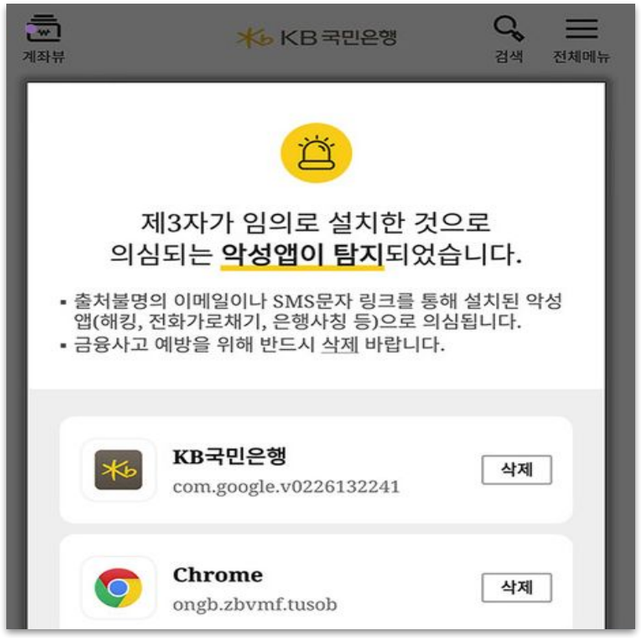
Voice Phishing Crime Task Force

Police



V.P Integrated Reporting Centre

Financial industry



Detecting malicious apps in financial apps

7. Trend

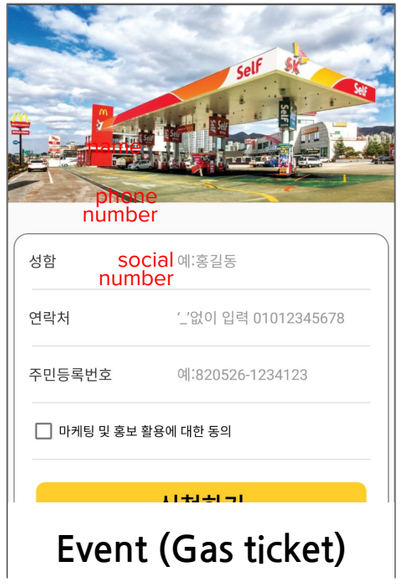
Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

Trends

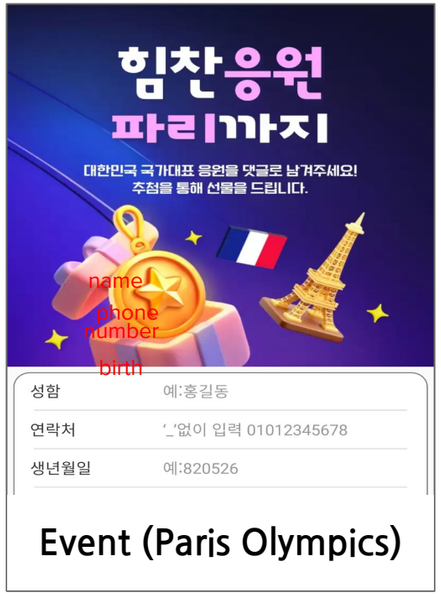
- As the pressure on voice phishing grows, **criminal organizations are moving to other phishing businesses.**
  - ➢ **The “balloon effect” is a situation where solving one problem creates another.**

Balloon Effect

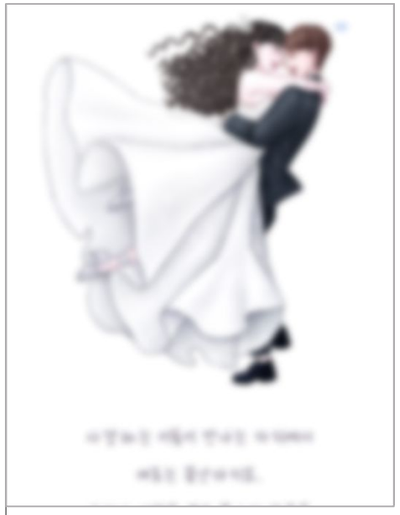
BlackEcho Smishing



Event (Gas ticket)



Event (Paris Olympics)



Wedding Invitation

Trends

- **South Korea has a very high smartphone penetration rate of 98%**, and mobile apps are used to make payments, buy and sell goods, and conduct various financial activities.
  - ➢ Compared to voice phishing, Smishing and second-hand fraud are low-value and require relatively little time and labor.

Smishing

Second-hand Phishing

당근

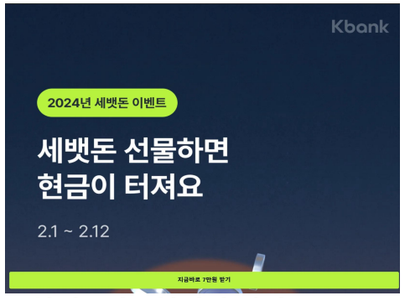
번개장터

Joonggonara

Trends - Smishing(1/2)

- While early smishing in South Korea was mostly about impersonating **delivery services and National Health Insurance**, there are now many different themes.
  - ➢ Criminal organizations spread smishing texts to **match holidays or social issues.**

Holiday pocket money

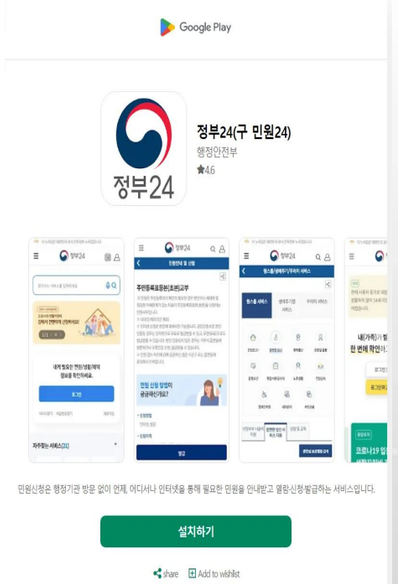


최대 1만 5천원이 터져요

2.1 ~ 2.12

Obituary / wedding invitation

Administrative Fines



Trends - Smishing(2/2)

- Recently, smishing in South Korea is basically using **shortened URLs** and creating phishing sites with **modern UIs that are specialized for mobile.**
  - The main purpose of a smishing app is **to spread to the masses.**
    (The Smishing app is lighter in function than the VoicePhishing app.)

Using the Shortened URL Service

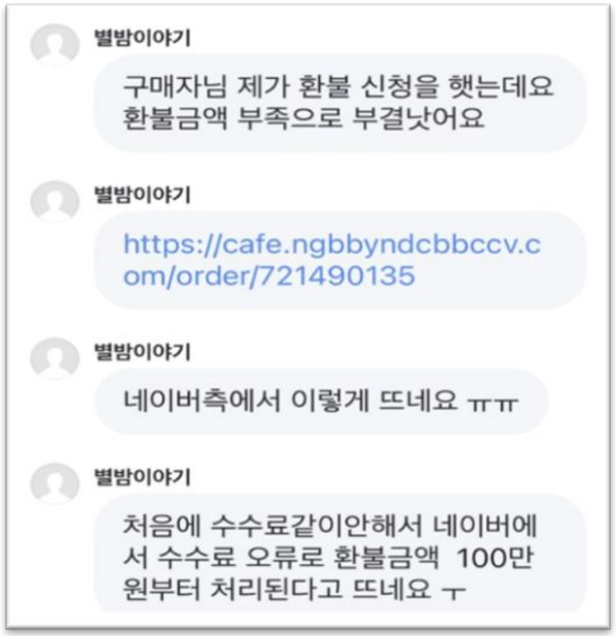
Domain addresses consisting of commonly used keywords, such as KOR, GOV, etc.

Mobile-friendly Web UI

Trends - Second-hand Phishing

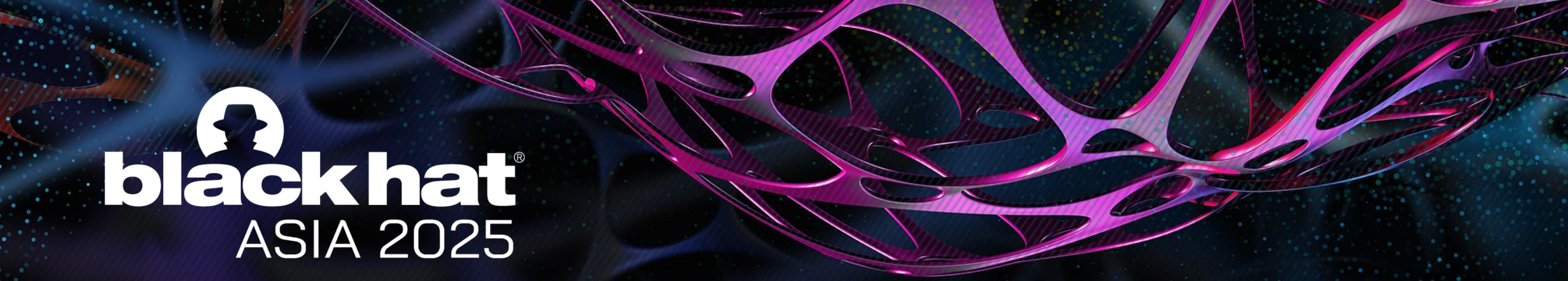
- Korea has a number of active second-hand trading platforms such as “Joonggonara” and “Carrot”.
  - They trick you into depositing cash by pretending to be a secure payment.

1. Encourage customers to enter personal information and pay for goods



2. Deposit errors, non-payment of fees, drive additional deposits

3. Deposit additional funds for the victim



8. Conclusion

Operation BlackEcho
:Voice Phishing using Fake Financial and Vaccine Apps

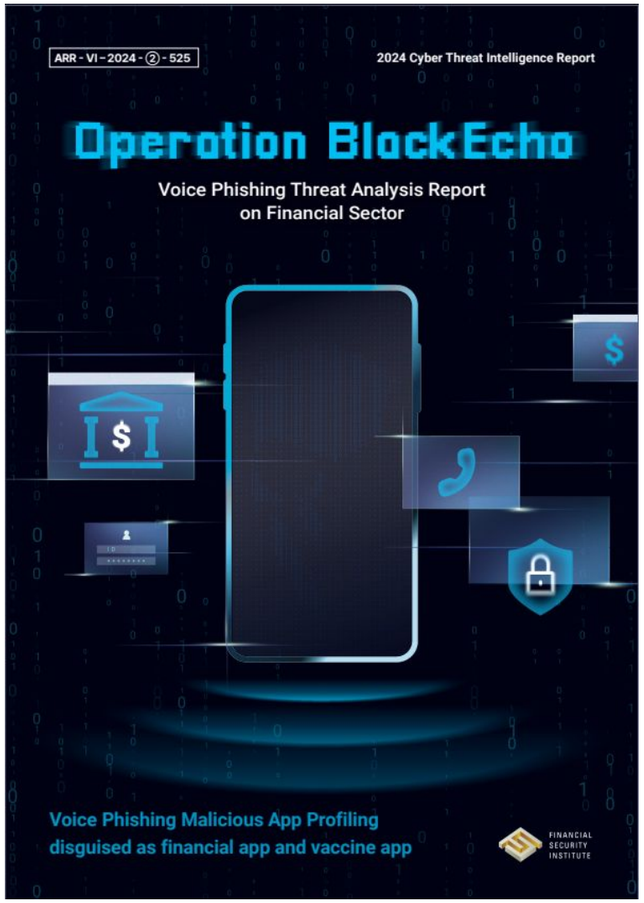
What can we do?

- People
  - Install mobile antivirus apps and **don't download apps** from unknown sources
  - **Be careful about providing personal information**, ID images, and credit information
- Investigative Agencies, Financial companies
  - **Share information** related to voice phishing with each other.
  - Analyze infrastructure related to malicious apps and work to prevent them in advance
  - Financial firms should operate a system that immediately **alerts or blocks suspicious transactions** on customer accounts. (FDS).

Intelligence Report

- This report provides details about Operation BlackEcho
  - Crime Scenario
  - Malicious App Analysis
  - Network Analysis
  - Voice Phishing Analysis
- Additionally, it includes IoC and various artifacts to identify and respond to Operation BlackEcho.
  - IoC (Indicator Of Compromise)
  - Files / SharedPreferences / Database / …

You can download the report here.



Black Hat Asia Sound Bytes

- Malicious apps are becoming increasingly sophisticated.

  Security researchers must enhance their skills to analyze and respond to these apps.
- **Companies** and **agencies** should identify potential threats and respond accordingly.

  Collaboration between them can be beneficial.
- **Financial consumers** should learn how to protect themselves from financial fraud, including voice phishing.

  Understanding the attack process and real-life cases can help strengthen their defenses.

black hat ASIA 2025

Thank you

Financial Security Institute

Hyeji Heo : heohj@fsec.or.kr

Sungchan Jang : bsstudent23@fsec.or.kr