

2019 한국정보보호학회 하계학술대회

CISC-S'19

Conference on Information Security and Cryptography-Summer 2019

2019. 6. 20(목)~22(토)

부산 동명대학교 (제1정보통신관, 중앙도서관)

주최



한국정보보호학회
Korea Institute of Information Security & Cryptology

주관



동명대학교
TONGMYONG UNIVERSITY

후원



국가정보원
National Intelligence Service Korea



과학기술정보통신부



행정안전부



KISA 한국인터넷진흥원

ETRI

한국전자통신연구원
Electronic and Telecommunications
Research Institute

NSR

국가보안기술연구소
National Security Technology Research Institute

IITP

정보통신기획평가원

AhnLab

TRACK 6 - 305호 소강의실

세션	발표논문
6월 21일(금) 13:00 ~ 14:30	VR상의 편리한 PIN입력 방식 제안 김현준, 권혁동, 김경호, 서화정 (한성대학교)
A6	망혼용 프린터 기반 은닉채널에 대한 통신 프로토콜 천종희, 김용현, 안명길 (국방과학연구소)
암호 프로토콜1	WBAN 환경의 PUF 기반 경량 인증 프로토콜 설계 오정민*, 정익래*, 변진욱** (*고려대학교, **평택대학교)
좌장 : 이광수 교수 (세종대)	SSL/TLS 보안 및 취약점 동향 윤재용, 서화정 (한성대학교)
	블록체인을 활용한 클라우드 파일 권한 관리 시스템 김선형, 최규현, 정재열, 정익래 (고려대학교)

6월 21일(금) 14:40 ~ 16:10	OCRA 적용을 통한 적응형 인증 기법 연구 윤건*, 정재민*, 안효범**, 김원수***, 유일선* (*순천향대학교, **공주대학교, ***한국교육과정평가원)
B6	IoT DNS를 활용한 이중 IoT 플랫폼 식별체계 상호연동 및 보안 김현곤, 이스마일, 수란토 나우팔, 김호원 (부산대학교)
암호프로토콜2/ 블록암호/ 하드웨어보안	S-Box의 비선형 불변 도출 연구 김성겸*, 이상협*, 조은지*, 홍득조**, 성재철***, 홍석희* (*고려대학교, **전북대학교, ***서울시립대학교)
좌장 : 노건태 교수 (세종사이버대)	차분 및 선형 Branch 수가 모두 3인 8-bit S-box에 대한 연구 전용진, 김기윤, 김한기, 김종성 (국민대학교)
	멜트다운과 스펙터에 대한 기술 동향 연구 김베드로, 김형식 (성균관대학교)

6월 22일(토) 10:00 ~ 11:30	클라우드 기반 전화가로채기 앱 탐지 기법 정해선, 김득훈, 박진 (아주대학교)
C6	클라우드 컴퓨터 보안위협요소 최명길, 한기원, 김진배 (중앙대학교)
클라우드보안	클라우드 분산 컴퓨팅 서비스를 위한 블록체인 기술 동향 박승윤, 김민우, 오희국 (한양대학교)
좌장 : 김동민 박사 (NSR)	블록체인 기반의 클라우드 서비스를 이용한 안전한 OAuth 프레임워크 박진성, 이창훈 (서울과학기술대학교)
	M2M 통신을 위한 DAG 기반 키 관리 시스템 이정호, 최형기 (성균관대학교)

클라우드 기반 전화가로채기 앱 탐지 기법

정해선*, 김득훈**, 곽진***

*,***아주대학교 사이버보안학과

**아주대학교 컴퓨터공학과, 정보보호응용및보증연구실

Cloud based Detecting method for Phone call Intercept App

Hae-Seon Jeong*, Deuk-Hun Kim**, Jin Kwak***

*,***Department of Cyber Security, Ajou University.

**ISAA Lab., Department of Computer Engineering, Ajou University.

요 약

개인정보 유출과 금전적 손실을 주는 보이스피싱이 지속적으로 증가하고 있으며, 공격 기법 또한 고도화 및 지능화되고 있다. 신종 보이스피싱 중 전화가로채기 앱을 이용한 보이스피싱 피싱 문구를 통해 악성 앱의 설치를 유도하고 사용자가 금융 기관에 전화를 걸면 보이스피싱 조직이 전화를 가로채고 사용자를 속인다. 전화가로채기 앱으로 인한 피해 또한 매년 증가하고 있으며, 이러한 전화가로채기 앱을 실시간으로 탐지하여 피해를 줄이기 위해 본 논문에서는 전화가로채기 앱의 작동 과정을 분석하여 전화가로채기 앱을 탐지하기 위한 클라우드 기반 탐지 시스템을 제안한다.

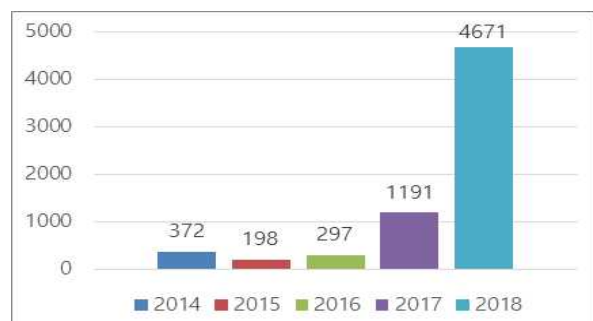
I. 서론

악성 앱을 통한 보이스피싱은 2014년부터 지속적으로 증가하고 있으며, 매년 그 피해가 점점 확대되고 있다. 그중 전화가로채기 앱은 스미싱 문자에 포함되어 있는 URL을 클릭하면 사용자 기기에 설치된다. 앱이 설치된 이후, 사용자가 금융 기관에 전화를 걸면 전화가 가로채어져서 공격자에게 전화가 연결되고 사용자는 금융기관으로 위장한 공격자를 신뢰하여서 공격자의 유도에 따라 입금하게 되는 방식이다[1].

스미싱 예방 및 대응 가이드라인에서는 의심되는 문구 및 URL을 포함하고 있으면 URL을 클릭하지 말 것을 권고하고 있지만 스미싱 기법이 나날이 발전함에 따라 보이스피싱 피해가 속출하고 있다[1]. 악성 앱을 사용한 보이스피싱의

발생빈도는 2016년과 대비하여 2018년에 약 16배 이상 증가하였다[2]. 따라서 이를 대응하기 위한 방안이 필요한 실정이다.

본 논문의 구성은 2장에서는 관련 연구로 전화가로채기 앱의 동작 방식 및 사용하는 권한과 API를 분석하고, 3장에서는 클라우드 기반 분석 시스템을 제안한다. 마지막으로 4장에서 추후 연구 방향을 제시한다.



(그림 1) 2014년 이후 보이스피싱 앱 증가 추이

이 논문은 2019년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1E1A1A01075110).

[표 1] 전화가로채기 앱의 요구 권한

권한명	권한 설명	악성 앱이 수행하는 기능
WRITE_CALL_LOG	통화 기록을 쓰기 위해 요구됨	통화 기록 조작
READ_CALL_LOG	통화 기록을 읽기 위해 요구됨	
READ_CONTACTS	전화번호부를 읽기 위해 요구됨	사용자 지인 번호 탈취 및 공격자 번호의 전화번호부 상 이름을 신빙성있는 기관 이름으로 저장
WRITE_CONTACTS	전화번호부를 쓰기 위해 요구됨	
READ_PHONE_STATE	단말기 정보를 얻기 위해 필요한 권한	전화번호, 사용자 기기 ID, 기기의 네트워크 상태 등 여러 핸드폰의 상태 정보를 탈취
PROCESS_OUTGOING_CALLS	전화 발신 시 발신 번호 참조, 리다이렉트, 통화 종료하는 경우 요구됨	발신 전화 리다이렉트
CALL_PHONE	사용자 조작 없이 앱 스스로 전화하기 위해 요구됨	사용자 조작 없이 앱 스스로 전화 및 발신 전화 종료
MODIFY_PHONE_STATE	핸드폰 상태 변화를 위해 요구됨	
SYSTEM_ALERT_WINDOW	다른 앱, 시스템 위(최상단)에 창을 띄우기 위해 요구됨	사용자 조작 없이 앱 스스로 전화 및 발신 전화 종료

II. 관련 연구

2.1 전화가로채기 앱 동작 방식

전화가로채기 앱은 피싱 문구를 통해 SMS 내에 있는 URL을 누르도록 유도한다. URL에는 악성 앱 설치 경로가 내포되어 있어 URL을 클릭하면 악성 앱이 설치된다[3].

전화가로채기 앱의 기능은 발신 전화를 공격자에게 리다이렉트하는 것과 공격자의 전화번호를 은닉하는 두 가지로 구성된다[2].

□ 발신 전화 리다이렉트

공격자는 발신 전화를 감지하면 endCall() API를 호출하여 전화를 끊고, 공격자의 번호로 전화를 건다.

- 탈취 대상 발신 번호는 국내 금융 기관, 수사 기관등의 전화번호로 앱 내에 하드코딩 되어있다.
- 공격자의 번호는 하드코딩되어 있거나, 보이스피싱 번호 차단을 우회하기 위해 C&C 서버에서 동적으로 가져온다.

□ 공격자 전화번호 은닉

공격자는 다양한 방식으로 자신의 번호를 은닉한다.

- 공격자와의 통화 기록은 삭제하고, 사용자가 기존에 발신한 번호의 기록을 삽입한다.
- 공격자는 사용자가 전화를 건 번호가 있는 가장 화면을 전화 통화 화면 가장 위에 표시한다.
- 공격자 번호의 전화번호부 이름을 탈취 대상

번호인 금융 기관 번호로 저장해서 정상 기관에 전화한 것처럼 보이게 한다.

- 기본 전화 앱을 악성 앱으로 변경하여 공격자에게 전화해도 금융 기관으로 전화한 화면이 표시된다.

2.2 전화가로채기 앱에서 사용하는 권한

전화가로채기 앱은 기능 수행을 위해서 [표 1]의 권한을 사용한다. 해당 권한들은 정상 앱보다 악성 앱에서 높은 빈도로 나타나기 때문에 악성 앱을 식별하는데 사용할 수 있다[2, 4].

2.3 전화가로채기 앱에서 사용하는 API

전화가로채기 앱은 기능 수행을 위해서 [표 2]와 같은 API를 호출한다. 해당 API들은 정상 앱보다 악성 앱에서 높은 빈도수로 나타나기 때문에 악성 앱을 식별하는데 사용할 수 있다[3, 5, 6].

[표 2] 전화가로채기 앱에서 사용되는 API

클래스	메소드	악성 앱이 수행하는 기능
android.telephony.	getLine1Number()	통화 기록 조작
TelephonyManager	getDeviceID()	단말기 고유 일련번호 탈취
android.telecom.	endCall()	앱 스스로 통화 종료
TelecomManager	registerPhoneAccount()	전화번호부에 번호 등록

III. 제안 기법

3.1 시스템 구조

개인정보 유출과 금전적인 피해를 일으킬 수 있는 전화 가로채기 앱은 사후처리 방식이 아닌 실시간 탐지 기법을 사용해서 대응한다면 피해를 최소화할 수 있다. 따라서 본 논문에서는 클라우드 환경에서 실시간으로 악성 앱을 탐지하는 시스템을 제안한다.

□ 클라이언트

사용자 기기에 사전에 설치된 앱으로, SMS에 포함된 URL을 모니터링한다. URL이 탐지되면 해당 URL을 클라우드 서버로 전송한다.

□ 클라우드 서버

클라우드 서버에서 악성 앱에 대한 정적 분석과 동적 분석을 수행한다. 정적 분석은 앱의 코드 수준에서 분석하는 방법이고, 동적 분석은 앱을 실행시키면서 분석하는 방법이다. 따라서 동적 분석은 난독화 및 암호화된 앱인 경우에도 분석이 가능하기 때문에 정적 분석과 동적 분석을 모두 수행한다. 이때 동적 분석과 정적 분석을 독립적인 VM에서 동시에 진행하여 분석 효율을 높인다. 분석이 완료되면 분석 결과를 클라이언트에게 전달한다.

□ 제안 시스템 동작 과정

Step 1. 공격자가 스미싱 문자 전송

공격자는 악성 앱의 설치 경로를 포함한 URL을 클릭하게 유도한다.

Step 2. URL을 클라우드에 전송

사용자 기기에 미리 설치되어 있는 앱은 SMS에 포함된 URL을 클라우드에 전송한다.

Step 3. 클라우드에 앱 설치 및 분석

사용자에게 할당된 클라우드 영역에서 URL에 내포된 앱을 설치하고, 정적 분석과 동적 분석을 각각 동시에 진행한다.

Step 4. 사용자에게 분석 결과 전송

클라우드에서 분석한 결과를 사용자에게 전송한다. 해당 결과를 통해 사용자는 앱 설치 여부를 결정할 수 있다[7].

3.2 정적 분석

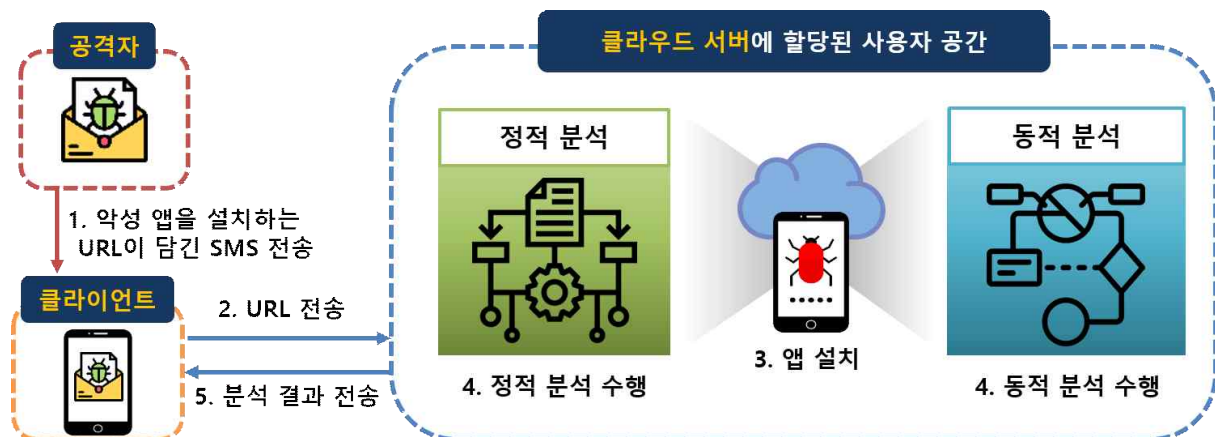
□ 악성 앱에서 사용하는 권한 확인

전화 가로채기 앱의 기능 수행을 위해 [표 1]의 권한이 요구된다. 해당 권한들은 악성 앱에서 높은 빈도로 나타난다. 또한 전체 권한 목록과의 일치율을 통해 악성 앱과의 행동이 유사함을 판단할 수 있기 때문에 [표 1]의 권한 목록을 통해 전화 가로채기 앱을 탐지할 수 있다.

3.3 동적 분석

□ 악성 앱의 행위 기반 분석

전화 가로채기 앱은 사용자가 금융 기관이나 수사 기관에 발신하는 것을 기다리다가 (그림 3)의 코드를 통해 발신을 탐지하면 전화를 즉시 끊고, 공격자에게 전화를 건다. 이를 탐지하기 위해 (그림 4)의 순서로 분석한다. 동적 분석 단계에서 악성 앱이 설치된 클라우드에서 임의의 금융 기관이나 수사 기관으로 전화를 건다. 전화가 강제로 끊기는 것이 탐지되면 악성 행위로 의심할 수 있다. 이때 전화가 끊긴



(그림 2) 제안하는 시스템 구조 및 절차

```

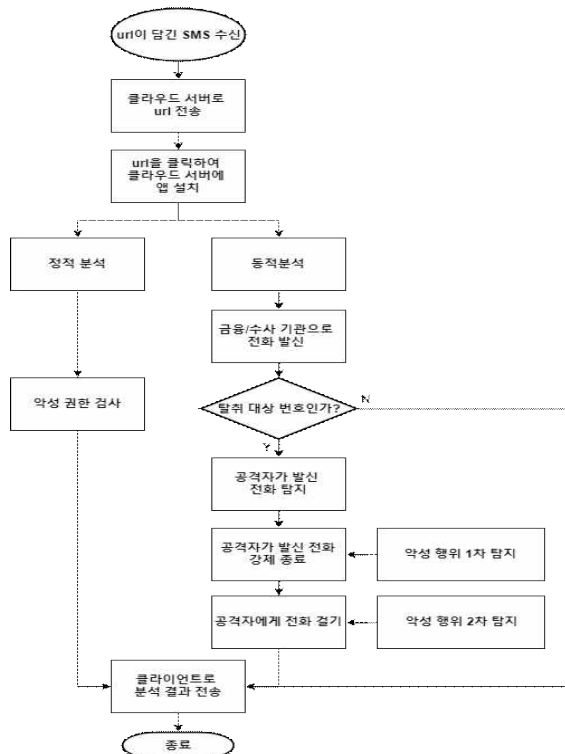
public class CallReceiver extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
        if(intent.getStringExtra(TelephonyManager.EXTRA_STATE).equals(TelephonyManager.EXTRA_STATE_OFFHOOK)){
            showToast(context, message: "Call started...");
        }
        else if(intent.getStringExtra(TelephonyManager.EXTRA_STATE).equals(TelephonyManager.EXTRA_STATE_IDLE)){
            showToast(context, message: "Call ended...");
        }
        else if(intent.getStringExtra(TelephonyManager.EXTRA_STATE).equals(TelephonyManager.EXTRA_STATE_RINGING))
            showToast(context, message: "Incoming call...");
    }
}

```

(그림 3) 전화 상태 변화를 탐지하는 코드

이후 빠르게 다른 번호로 발신되면 이는 공격자에게 전화를 건 것으로 탐지할 수 있다.

범위를 확장할 수 있고 제안하는 시스템의 안전성을 향상시킬 수 있으므로 추후 연구를 진행하고자 한다.



(그림 4) 제안하는 분석 순서도

IV. 결론

본 논문에서는 전화가로채기 앱의 동작 방식을 분석하여 실시간으로 전화가로채기 앱을 탐지하기 위한 클라우드 기반 정적 분석과 동적 분석 기법을 제시하였다.

최근에 발견된 앱 중에는 분석 환경을 탐지하여 동작을 중지시키는 앱도 있다. 이를 분석하기 위해 루팅 탐지 우회 기법을 적용할 필요가 있다[8]. 또한 사용자 기기와 클라우드 서버 사이에서 사용하는 안전한 프로토콜에 관한 연구도 필요하다. 이를 통해 탐지할 수 있는 악성 앱의

[참고문헌]

- [1] KISA, “스미싱 예방 및 대응 가이드”, <https://www.boho.or.kr/cyber/smishing.do>, Mar. 2015.
- [2] AhnLab, “악성 앱과 결합한 보이스피싱, 눈 뜨고 당한 이유 있다?”, <https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=28030>, Feb. 2019.
- [5] EST security Alyac blog, <https://blog.alaya.co.kr/92>, Jun. 2014.
- [4] J. Park, H. Chun and S. Jung, “API and permission-based classification system for Android malware analysis”, International Conference on Information Networking (ICOIN), IEEE, pp.930-935. Jan. 2018.
- [5] EST security Alyac blog, <https://blog.alaya.co.kr/1994>, Nov. 2018.
- [6] EST security Alyac blog, <https://blog.alaya.co.kr/1971>, Nov. 2018.
- [7] 제설아, 웅웁부렁, 정수환, “클라우드 플랫폼을 이용한 악성 URL 및 수정된 APK 파일 검증 시스템 설계 및 구현”, 정보보호학회논문지 제26권 제4호, Aug. 2016.
- [8] 강성은, 윤홍선, 정수환, “Xposed를 이용한 안드로이드 악성코드 분석을 위한 API 추출 기법 설계 및 구현에 관한 연구”, 정보보호학회논문지 제29권 제1호, Feb. 2019.