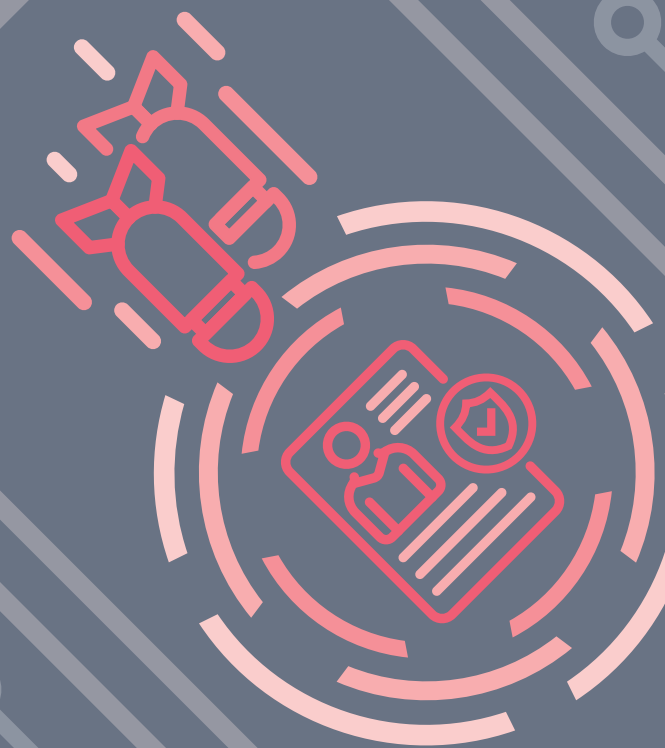
ARR-V-2020-②-199

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

요 약 본

금융보안원
FINANCIAL SECURITY INSTITUTE



FINANCIAL SECURITY INSTITUTE

Contents

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

I 개요

I 개요

스마트폰, 태블릿PC 등의 모바일 기기는 높은 AP(Application Processor) 성능과 고속 통신망(LTE, 5G) 및 무선 Wi-Fi 등에 24시간 연결된 밀접한 생활환경 속에 있어 사용자 PC 이상으로 공격자의 표적이 되고 있다.

2004년 이전에는 모바일 기기에서 위협이 되는 악성코드 및 공격이 발견되지 않았지만, 블루투스 방식을 이용하여 타 기기로 전파되는 특징을 갖는 Cabir.A 모바일 악성코드[1)]가 당시 점유율이 높았던 노키아 스마트폰(Symbian OS)에서 최초로 발견되었다.

국내 최초의 금융 모바일 악성코드는 2010년도에 발견된 윈도우 모바일 스마트폰에서 실행되는 WinCE/TerDial 악성코드로 인터넷 커뮤니티에서 공유되면서 유포되었고, 모바일 게임 설치파일에 국제전화 발신 기능이 포함되어 과금 피해가 발생하도록 구현되어 있었다. 국내에서는 일부 감염 사례가 있었으나 과금 피해는 없던 것으로 확인되었다.

사용자 PC가 널리 보급된 이후 다양한 보안 위협들이 출현한 것과 마찬가지로 스마트폰이 본격적으로 보급되기 시작한 2010년 이후부터 모바일 악성코드는 사용자 PC를 대상으로 개발된 악성코드의 구현된 기능과 형태들을 빠르게 흡수하여 그 수가 폭발적으로 증가하였다.

일반적으로 모바일 악성 앱은 정상 앱으로 위장하여 사회공학적 기법으로 다운로드를

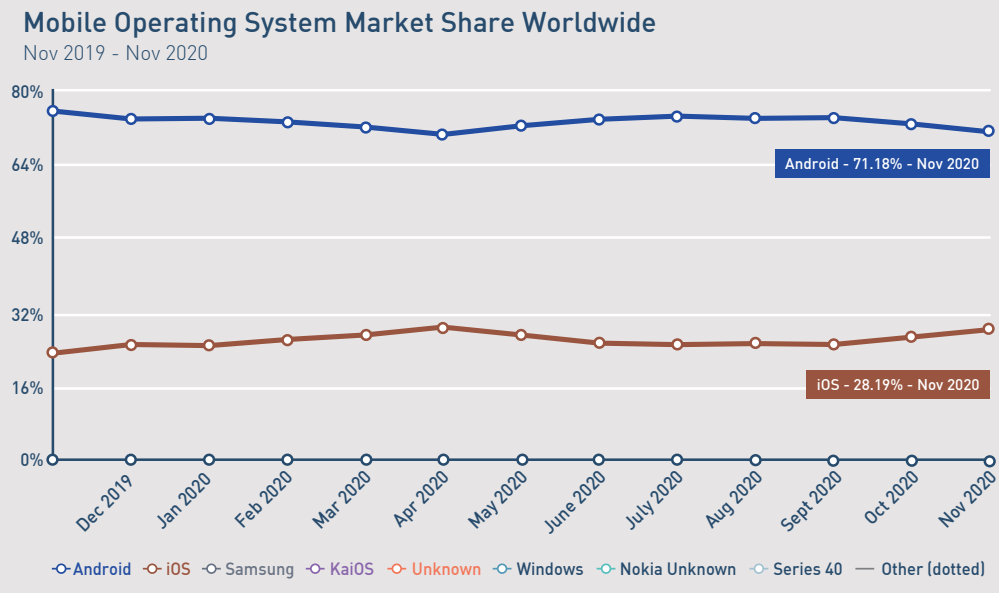
1) Kaspersky official blog | First smartphone virus, Cabir
http://kaspersky.com/blog/cabir-10/5107/

유도하고, 감염된 모바일 기기를 공격자가 원격에서 명령을 내리는 기능을 하고 있으며 금융 모바일 악성 앱은 주로 모바일 기기에 저장된 금융 데이터 및 사용자의 연락처, 문자 메시지, 중요 파일 등의 개인정보를 탈취하고, 피싱 페이지를 통해 아이디, 비밀번호, 카드 정보 등의 사용자 입력을 유도하거나 전화 수신 및 발신 번호를 변조하여 보이스피싱 피해를 발생시키는 등 다양한 악성 행위들을 포함하고 있다.

모바일 기기에는 금융 거래 및 결제 관련 데이터를 포함하여 다량의 개인 데이터가 저장되어 있으며 공격자는 이러한 정보를 탈취하기 위하여 노력하고 있다. 안드로이드 운영체제는 특히 악성 앱에 비교적 감염되기 쉬운 운영체제 구조와 악성 행위를 실행할 수 있는 환경을 갖고 있기 때문에 모바일 악성 앱 대부분이 안드로이드 모바일 기기(스마트폰, 태블릿PC)를 대상으로 개발되고 있다.

글로벌 모바일 기기 점유율 통계[2]에 의하면 2019년 11월부터 1년간을 기준으로 안드로이드 스마트폰 사용자는 71%, 아이폰 스마트폰 사용자는 28%이며, 국내 통계에서도 이와 비슷하게 발표되고 있다.

[그림] 글로벌 모바일 기기 점유율 통계



2) 글로벌 통계: Mobile Operating System Market Share Worldwide | StatCounter Global Stats
https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-201911-202011

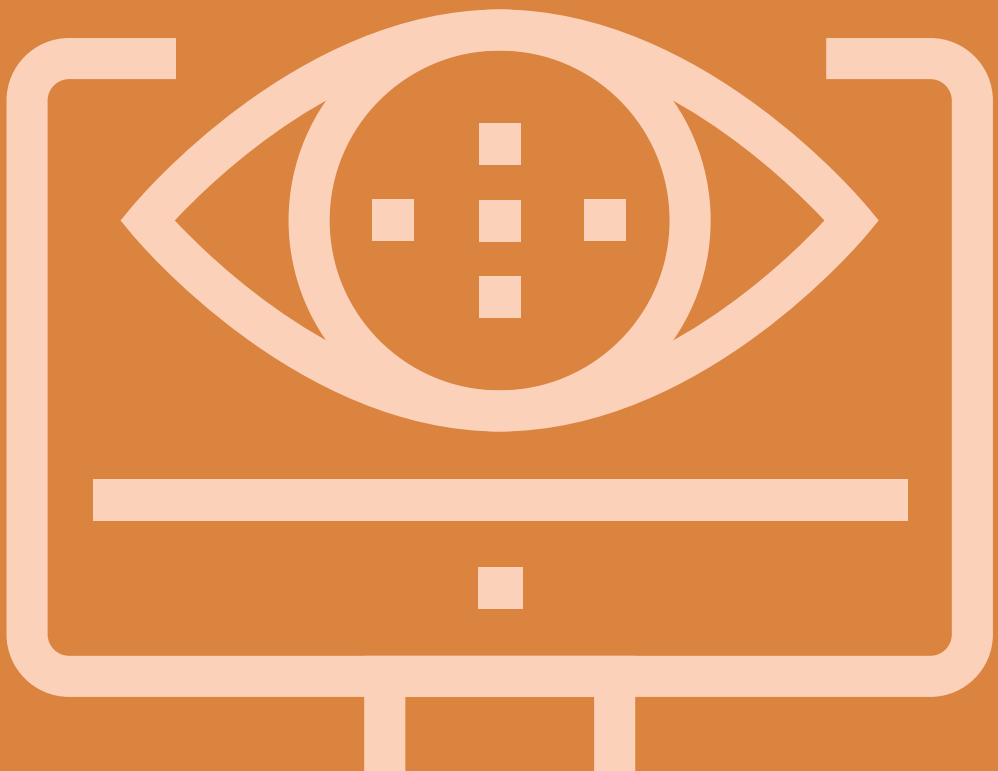
본 보고서에서는 해외 및 국내에서 발견된 Anubis, BlackRock, Cerberus, EventBot, KRBankBot, MysteryBot, RoamingMantis, Zitmo 등의 대표적인 안드로이드 금융 모바일 악성 앱 100여 개 샘플을 대상으로 바이너리 디컴파일 및 소스코드 분석을 하였다.

금융 악성 앱의 개별 분석 보고서가 아닌 전체적인 유포 방식과 기본 구조, 실행 흐름 및 주요 구현된 기능들을 소스코드 설명과 함께 종합적으로 분석하였고, 지난 10년간 모바일 악성코드의 주요 위협과 앞으로의 모바일 위협을 정리함으로써 악성 앱으로 인한 감염 예방에 도움이 되고자 한다.

FINANCIAL SECURITY INSTITUTE

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서



II

지금까지의 모바일 위협

II
지금까지의 모바일 위협

모바일 악성 앱은 다양한 유포 경로를 통해 사용자의 모바일 기기로 유입되고 있다. 금융 악성 앱이 유포되기 시작한 초기에는 문자 메시지, 메신저, 피싱 페이지 등이 주로 사용되었는데 최근에는 기존의 유포 방법을 사회적인 이슈와 결합하여 활용하는 한편, 광고 서버, 개발 관련 인증서 탈취, 공급망 및 개발사 등을 해킹하여 이 인프라를 통해 악성 앱을 유포하는 등 방법이 점차 진화하고 있다.

기본적으로 공식 마켓 이외에서 다운로드 받은 앱이나 악성 기능을 가진 앱들은 구글 플레이 프로텍트[3], 안티바이러스 탐지 기능을 탑재한 금융 앱에 의해 탐지 및 차단되고 있어서 최근 악성 앱들은 이러한 기술적 보호 조치를 우회하는데 집중하고 유포하는 방식을 다변화하고 있다.

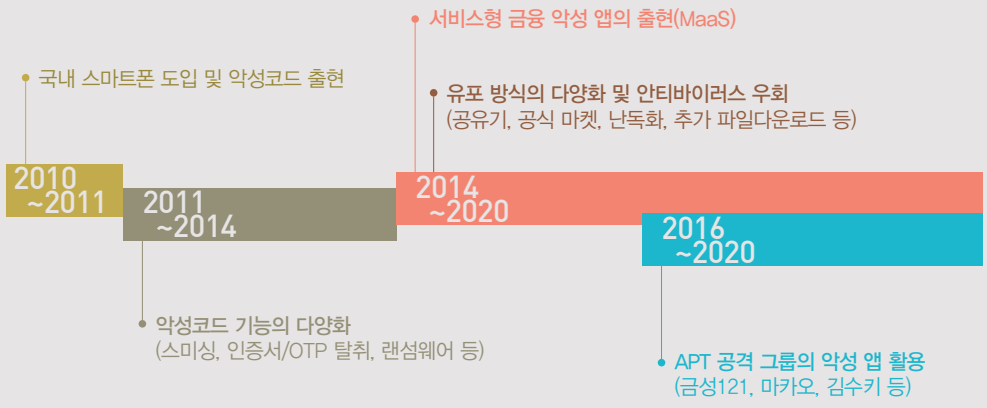
3) 구글 플레이 프로텍트: 구글에서 지원하는 악성 앱 탐지 기능으로 구글 플레이 스토어를 통해 다운받거나 APK 파일을 직접 설치했을 때, 설치된 앱들이 잠재적인 위험이 있는지 지속적으로 검사하여 악성 앱으로 의심되면 경고 메시지와 함께 제거 하도록 안내해주는 보호 기능이다.

1 모바일 악성코드 흐름

지난 10년간 모바일 악성코드의 주요 키워드와 위협을 살펴보면 다양한 특성이 보이는데 2010년 스마트폰 보급이 시작된 후 2012~2014년을 지나면서 모바일 악성코드가 폭발적으로 증가하였다.

이때 개인정보 유출, 랜섬웨어, DDoS봇, 몸캠피싱, 스미싱, 가상화폐 채굴 등 다양한 악성 기능들이 개발되었고, 현재 악성 앱 유포의 중심이라고 볼 수 있는 APT 공격 그룹과 서비스형 악성코드(MaaS: Malware-as-a-Service)에서 이러한 과거의 기능들을 계속 사용하고 있다는 것은 모바일 악성코드의 한계를 나타내는 의미라고 볼 수 있다. 다만, 최근의 모바일 악성코드는 안티바이러스 우회와 난독화, 유포 방식을 다양화하는데 더욱 초점을 맞추고 있다.

[그림] 지난 10년간의 모바일 악성코드 흐름



2012~2014년도에 이슈가 되었던 주요 악성코드를 살펴보기 위하여 뉴스 데이터 기반의 빅데이터 결과[4]를 참고하였고, 4,000개 이상의 뉴스 기사에서 모바일 악성코드와 관련된 키워드를 추출한 결과 스미싱 · 스파이앱 · 보이스피싱이 다수의 비율을 차지하였다. 또한 개체 수는 적지만 현재에도 이슈가 되고 있는 서비스형(금전 목적으로 판매한 도청 앱) 악성 앱, 무선랜 파밍, 몸캠 피싱, 다크웹을 이용한 악성 앱도 확인되었다.

4) 한국언론진흥재단 뉴스빅데이터 분석 서비스 – 빅카인즈
https://www.bigkinds.or.kr

이를 통해 알 수 있는 부분은 악성 앱 대부분이 새로운 변화 없이 과거에 이미 개발된 기능들과 유형들을 재사용하고 있고, 사용자가 악성 앱에 감염되는 주요 원인 또한 다르지 않다는 것을 알 수 있다. 과거부터 현재까지 지속해서 발생하고 있는 모바일 위협 중에서 악성 앱 감염에 근본적인 원인은 대부분 “신뢰할 수 없는 출처에서의 다운로드”, “정상 앱 사칭”, “탈옥 및 루팅” 등이 있다.

[그림] 뉴스 데이터 기반의 모바일 악성코드 키워드 통계

가. 전통적인 유포 방식 주의(신뢰할 수 없는 출처에서의 다운로드 및 정상 앱 사칭)

악성 앱 감염의 대부분은 사용자가 공식 마켓을 이용하지 않고 비공식 경로에서의 설치로 인해 감염되는 경우가 가장 많다. 문자 메시지 및 메신저로 유입되는 악성 앱 설치파일 링크를 다운로드 하고, 사용자가 직접 웹사이트, 블로그, 카페에 업로드된 설치파일을 다운로드 하거나 검색엔진 검색 결과를 통해 다운로드 하는 등 최초 스마트폰이 도입된 이후 현재까지도 신뢰할 수 없는 출처에서의 앱 설치가 문제의 원인으로 꼽힌다.

나. 탈옥 및 루팅으로 잠재적인 위협 환경 노출

안드로이드, 애플 모바일 기기에서 루팅 및 탈옥이 된 상태에서 비공식 마켓, 홈페이지 등에서 앱, 테마, 트윅을 설치하게 되면 악성코드에 감염될 확률이 높아진다. 공식 마켓은 앱 검수 시 악성 행위 포함 여부를 다양한 패턴으로 검사하여 차단하지만, 비공식 마켓은 이런 앱 검수가 미비하거나 관련 정책이 없기 때문에 악성코드에 감염될 수 있는 환경과 위협에 노출되게 된다.

만약 루팅 및 탈옥 된 모바일 기기에서 악성 앱에 감염이 되면 루트 권한으로 모바일 기기를 제어할 수 있으므로 저장된 중요 데이터 탈취를 포함하여 정상 앱을 악성 앱으로 임의 교체하거나 모바일 기기 설정을 임의 변경하는 등 루팅 및 탈옥되지 않은 상태에서의 피해보다 더욱 큰 피해가 발생할 수 있다.

다. 사회적 이슈를 이용한 문자 메시지 및 메신저

문자 메시지와 메신저는 대표적인 악성 앱 유포 수단이며, 주로 금융회사, 경찰, 법원, 택배 등으로 사칭하여 다운로드 및 설치를 유도한다. 정부의 추석 명절기간 스미싱, 보이스피싱 피해 주의 관련 보도자료[5]에 따르면, 추석 연휴를 앞두고 배송 확인, 코로나19 관련 긴급재난 지원 및 결제 등을 사칭한 스미싱 탐지 건수가 점차 증가 되었다고 한다.

라. 검색엔진 최적화 기법(SEO)를 통한 악성 앱 다운로드 유도

2016년 출시된 포켓몬Go 앱은 개인블로그, 커뮤니티 게시판 등 비 공식마켓에서 대량의 앱이 사용자 스마트폰으로 유입된 대표적인 사례이다. 당시 국내 공식마켓에서 포켓몬Go 앱이 배포되지 않은 시점에 이미 100만명[6] 이상의 국내 유저들이 설치한것으로 추산되었으며, 동시에 악성 행위를 추가한 리패키징 앱들이 발견되었다. 일반적으로 웹사이트를 이용한 악성 앱 배포는 이러한 트렌드를 반영함과 동시에 검색엔진 최상단에 노출되도록 SEO 기법[7]을 적용하며, 금융권에서도 이러한 기법을 이용한 악성코드들이 꾸준히 유입되고 있다.

5) 추석 명절기간 스미싱, 보이스피싱 피해 주의!! – 이통3사와 협업하여 스미싱 피해예방을 위한 문자 메시지 발송
https://www.korea.kr/news/pressReleaseView.do?newsId=156412329
6) 한국일보 – 포켓몬 잡으려다 스마트폰 해킹당할라
https://www.hankookilbo.com/News/Read/201607172096123994
7) SEO(Search Engine Optimization) 기법: 검색엔진에 노출되기 쉽도록 홈페이지 구조와 웹페이지에 필요한 정보들을 추가하여 검색엔진 상위에 노출되게 하는 방법

2 악성 앱 유포의 진화

가. 공식 마켓을 통한 유포

공식 마켓을 통한 악성 앱 유포는 지속적으로 발생하고 있는데 구글의 공식 플레이 스토어는 업로드되는 앱의 악성 여부를 기본적으로 판별하지만, 악성 앱들 또한 이 테스트를 통과하기 위한 방법으로 일정 시간이 지연된 이후에 악성 기능을 실행하거나, 앱이 실행될 때 구글 관련 IP에서 실행되는 경우 악성 기능 동작을 중지하거나 실제 악성 기능은 앱에 없지만, 추가로 악성 기능이 포함된 APK 파일을 다운받는 등 다양한 우회 기법을 사용하고 있다.

나. 인증서 탈취를 통한 앱 스토어 유포

인증서와 서명 정보가 탈취될 경우 동일 서명으로 악성 앱이 유포될 수 있으며 앱 개발 시 공개된 인증서를 사용하거나 다수의 앱을 한 개의 인증서로 사용할 경우 위협에 노출될 가능성이 증가한다.

다. 광고 라이브러리를 통한 악성코드 유입

앱 내부에 포함되는 광고 역시 공격벡터 중 하나가 될 수 있다. 앱 개발자는 모바일 광고 플랫폼 업체가 제공하는 SDK 및 소스코드 등을 이용하여 앱 내부에 광고를 포함할 수 있으며, 이에 따른 수익금을 얻을 수 있다. 이때 광고 플랫폼 업체가 해킹을 당하거나 의도적으로 개발자에 의해 소스코드에 악성코드가 삽입될 수 있다.

라. 공급망을 통한 악성 앱 선탑재

2017~18년도에는 스마트폰 공급단계에서 악성 앱이 선탑재된 사례도 발생하였는데 조사 결과 제조사에서 출고 시엔 문제가 없었으나, 특정 통신사나 기기 제조업체 등을 통해 유통된 기기라는 공통점이 발견되었다. 이러한 공급망 단계에서 악성 앱이 설치될 경우 사용자는 백신을 설치하기도 전에 위협에 노출되어 위험성이 높다.

마. 개발 및 유통사 홈페이지를 통한 유포

일반적으로 개발사의 홈페이지에서 제공되는 앱은 공식 마켓이 아니어도 사용자들이 의심 없이 설치하는 경향이 있는데, 해외에서 국내로 유통된 게임패드 전용 앱에서 스마트폰 정보를 사용자 동의 없이 수집하는 기능이 포함되어 이슈[8]가 되었다.

바. 인터넷 공유기를 통한 악성 앱 유포

보안이 취약한 공유기를 해킹하여 사용자의 스마트폰을 악성 페이지로 리다이렉트 시키는 DNS 파밍 공격은 국내에서도 지속적으로 발생해왔다. 대표적으로 아래와 같이 ID/PW가 취약하거나 기본 관리자 계정으로 설정된 인터넷 공유기의 관리자 페이지에 접근하여 DNS 서버 IP를 공격자의 DNS 서버 IP로 변조하는 공격이 많이 발생되었다.

사. PC 및 네트워크를 통한 모바일 기기 감염

2018년 다량의 안드로이드 기기와 TV셋톱박스가 가상화폐(모네로) 채굴을 위한 ADB.Miner 악성코드[9]에 감염된 정황이 발견되었는데 효과적인 확산을 위해 2016년도에 확산되었던 미라이(Mirai) 봇넷의 소스코드[10]를 참고하여 스스로 전파하는 기능과 포트스캔을 수행하도록 개발되었다.

아. 신규 취약점 이용

일반적으로 앱이 개발되어 유포된 이후 기능을 수정하기 위해서는 동일한 서명이 필요하지만 2017년도에는 이러한 앱 마켓의 업데이트 관리 시스템을 우회하여 서명이 일치하지 않더라도 임의의 기능을 앱에 추가하여 유포할 수 있는 야누스(CVE-2017-13156) 취약점[11]이 발견되었다.

8) 이스트시큐리티 알약 블로그 | Misc.Android.InfoStealer 악성코드 분석 보고서
https://blog.alyac.co.kr/1837
보안뉴스 | 안드로이드 모바일 사용자 정보를 훔쳐가는 악성앱 발견
https://www.boannews.com/media/view.asp?idx=72315
9) 긴급 경고 : ADB.Miner 안드로이드 ADB를 활용 한 마이닝 봇넷 빠르게 확산
https://www.trendmicro.com/ko_kr/about/newsroom/press-releases/2018/2018-02-05.html
10) ITWorld Korea | 미라이 소스코드를 이용한 IoT 봇넷 확산, 감염된 IoT 기기 49만 3,000개로 증가
https://www.itworld.co.kr/news/101662/
11) CVE - CVE-2017-13156
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13156

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

III

금융 모바일 악성코드 특성

III
금융 모바일 악성코드 특성

금융 악성 앱은 개인정보와 금융정보 탈취를 목적으로 개발되었고, 주로 모바일 기기에 저장된 개인정보(연락처, 문자메시지 등)를 탈취하거나 피싱 페이지를 통해 입력을 유도하여 금융정보(카드번호, 유효기간 등)를 탈취하고, 이를 보이스피싱 범죄에 활용하여 금융 소비자의 금전을 편취하는데 큰 역할을 하고 있다.

이러한 공격들이 가능하려면 모바일 운영체제에서 '백그라운드에서 실행되는 서비스', '현재 실행 중인 앱 정보 확인', '앱 화면 위에 오버레이 화면을 보여주기', '악성 행위를 가능하게 하는 권한과 API 지원' 기능들을 제공하여야 한다.

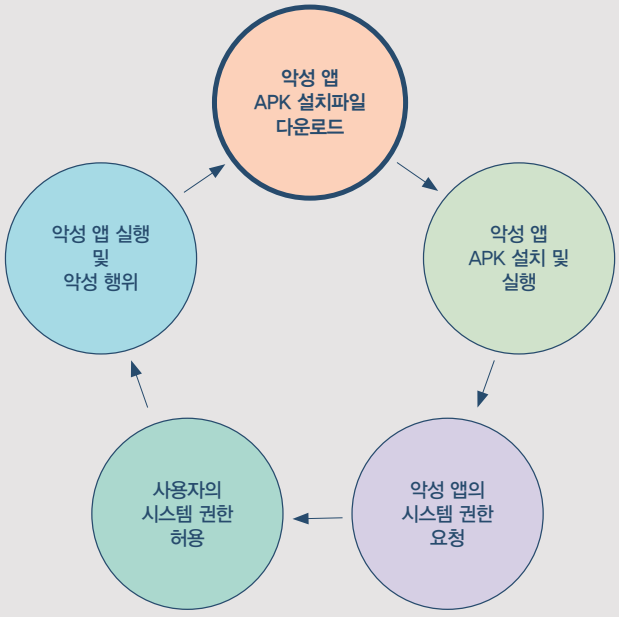
iOS 및 iPadOS(이하 iOS) 운영체제는 제한된 조건에서만 백그라운드 서비스 실행을 지원하고 있으나 안드로이드 운영체제는 악성 앱 감염에 필요한 기능을 모두 지원하고 감염되기 쉬운 환경 때문에 모바일 악성 앱 대부분이 안드로이드 모바일 기기를 대상으로 개발 및 유포되고 있다. 안드로이드는 공식 플레이 스토어 외에도 다양한 안드로이드 앱 마켓이 존재하며 삼성 갤럭시 스토어, 아마존 앱스토어, 국내 통신 3사와 네이버 앱스토어를 통합한 원스토어 등 사용자는 다양한 곳에서 앱 설치파일을 다운로드 받을 수 있는 특징이 있다.

안드로이드 사용자는 구글 플레이 스토어 및 다양한 앱 마켓과 웹사이트, 블로그, 커뮤니티 등에서 공유되는 설치파일을 다운로드하여 자유롭게 설치가 가능하지만 본인도 모르는 사이 악성코드가 포함된 앱이 설치되거나 문자, 메신저 등으로 전달된 악성 앱 설치파일 링크를 통해 감염되는 등 편의성에 따른 감염 위협이 높은 편이다.

안드로이드 운영체제에는 2020년 기준 160여 개의 시스템 권한[12]이 존재하며 마시멜로 v6.0 이전 버전에서는 앱 설치 시 최초 1회에 모든 시스템 권한이 허용되는 형태였지만 마시멜로 v6.0 이후에는 개인정보에 접근하는 연락처, 전화, 문자, 카메라 권한들을 위험(dangerous)으로 구분하여 개별 권한마다 사용자에게 허용 요청을 할 수 있도록 권한 정책이 강화되었다.

사용자의 모바일 기기에서 악성 앱이 다운로드 및 감염되면 사용자에게 시스템 권한 요청을 하게 된다. 권한이 허용되면 데이터 탈취 및 악성 행위를 하게 되는데 이 과정이 반복되어 여러 차례 악성 앱에 감염될 수 있다.

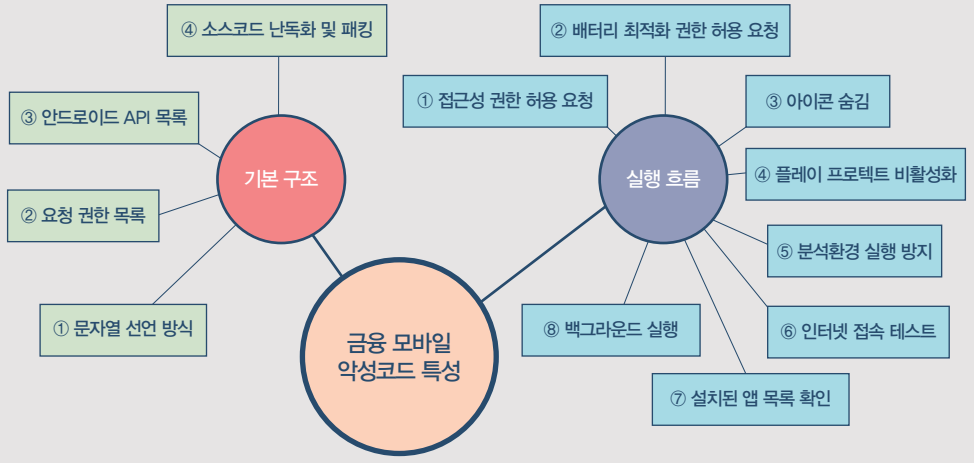
[그림] 악성 앱이 설치 및 실행되는 과정(1차 감염 이후에도 반복 감염)



본 보고서에서는 해외 및 국내에서 발견된 Anubis, BlackRock, Cerberus, EventBot, KRBankBot, MysteryBot, RoamingMantis, Zitmo 등의 대표적인 안드로이드 금융 모바일 악성 앱 100여 개 샘플을 대상으로 바이너리 디컴파일 및 소스코드 분석을 통해 전체적인 기본 구조, 실행 흐름 및 주요 구현된 기능들을 다음과 같이 종합적으로 분석하였다.

12) Android Developers | Manifest.permission
https://developer.android.com/reference/android/Manifest.permission?hl=ko

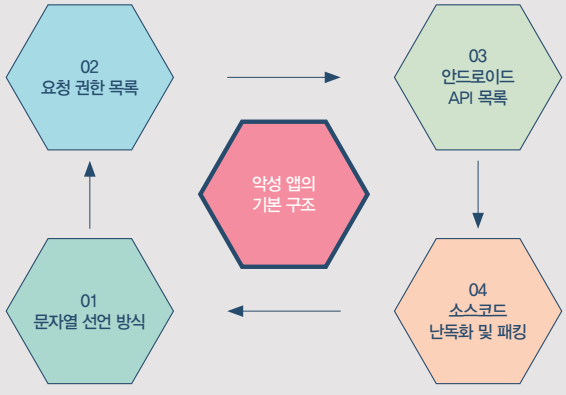
[그림] 금융 악성 앱 세부 분류



1 기본 구조

악성 앱은 사용자의 개인 및 금융정보 탈취 등의 악성 행위를 위하여 은행, 대출, 사회적인 이슈 등의 관심사를 이용하여 정상 앱의 이름과 아이콘으로 사칭하여 설치를 유도하고, 필요한 권한들을 사용자에게 요청하는 공통적인 특징을 갖고 있으며, 악성행위를 하는 앱들은 아이콘과 이름은 서로 다르지만 주요 악성 행위 및 기본 구조는 유사한 경우가 많다.

[그림] 악성 앱의 기본 구조



가. 문자열 선언 방식

앱을 분석하기 위해서는 정적 및 동적 분석 방법을 이용하여 사람이 이해 가능한 문자와 숫자로 구성된 코드의 작동 흐름으로 해당 함수가 어떤 기능들을 하는지 알 수 있지만, 악성 앱은 사용되는 문자열들을 별도 파일에 상수로 선언하거나 base64로 인코딩을 하는 형태를 하여 분석을 어렵게 한다.

나. 요청 권한 목록

국내외에서 발견된 대표적인 금융 악성 앱의 AndroidManifest.xml[13] 파일에서 공통적으로 요청하는 권한을 정리하면 모바일 기기 정보, 사용자의 위치정보, 전화 수발신 제어, 문자 메시지 제어, 연락처 및 카메라 제어 등 모바일 기기에 대한 정보와 사용자의 개인정보가 저장된 데이터에 접근하는 특징을 볼 수 있다.

다. 안드로이드 API 목록

악성 앱의 Manifest 파일에는 위치정보 확인, 문자 메시지 접근 등의 악성 행위를 위해 필요한 권한을 정의한다.

라. 소스코드 난독화 및 패킹

소스코드 난독화 솔루션으로는 안드로이드 개발 환경인 안드로이드 스튜디오에서 무료로 제공하는 ProGuard, 상용 솔루션으로는 Allatori, DexGuard, ProGuard 등이 있는데 ProGuard는 클래스, 함수 이름들을 의미 없는 문자열로 치환해주는 등 한정적인 기능만 제공하여 쉽게 복호화가 가능한 반면 Allatori, DexGuard 등의 상용 솔루션은 ProGuard에서 지원하는 기능과 문자열 정보 난독화, 실행 흐름 사이에 의미없는 함수를 넣거나 실행 파일을 다수 구성하여 앱 실행파일을 숨기는 멀티덱스를 적용하는 등 다양한 난독화 옵션들을 제공한다.

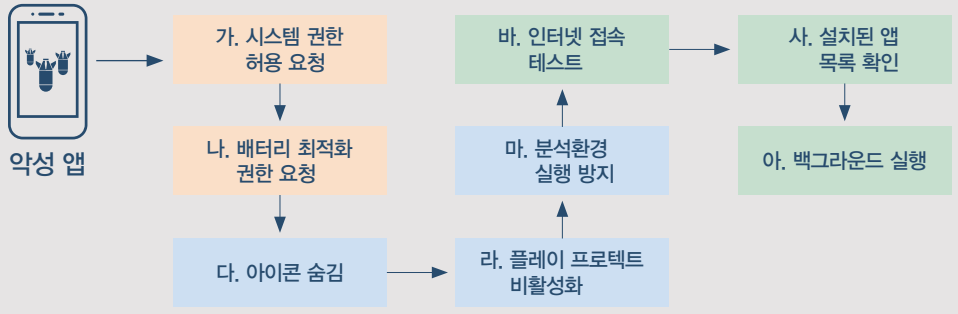
13) 안드로이드 모바일 앱의 패키지 이름, 고유 식별자, 앱의 구성요소(액티비티, 브로드캐스트 리시버, 컨텐츠 프로바이더, 서비스), 필요 권한 등의 정보들이 담겨있는 파일이며, 액티비티와 브로드캐스트 리시버, 서비스는 “AndroidManifest.xml” 파일에 등록이 되어야 한다.

2 실행 흐름

악성 앱의 종류, 세부 버전, 변종마다 실행 흐름은 조금씩 다르지만, 일반적으로 악성 앱은 최초 설치 및 실행 후 악성 행위를 위한 사용자의 권한을 얻기 위하여 접근성 권한을 허용하도록 유도하고, 구글에서 제공하는 안티바이러스 탐지 기능인 구글 플레이 프로텍트 보안 기능을 비활성화한다.

지속적인 악성 행위 및 모니터링을 위하여 백그라운드 서비스로 동작하도록 설정하고 공격자가 사전에 정의한 앱을 사용자가 실행하면 악성 앱의 화면 오버레이 기능이 실행되어 개인 및 금융정보가 탈취되고, 사용자의 모바일 기기를 원격에서 제어하여 스미싱 및 보이스피싱 등의 금전적인 피해를 입힌다.

[그림] 악성 앱의 일반적인 실행 흐름



가. 접근성 및 기기 관리자 권한 허용 요청

최초 악성 앱 설치 후 실행이 되면 사용자에게 접근성 권한(Accessibility Service)[14]과 기기 관리자 권한을 허용하도록 유도하는데 일부 사용자는 앱을 정상적으로 실행하는 데 필요한 과정으로 생각하여 허용하게 되고, 악성 앱은 허용된 권한을 이용하여 여러 가지 악성 행위를 할 수 있게 된다.

14) 접근성 서비스: 시각, 청각 등이 불편한 사용자들을 위해 만들어진 지원 기능으로 접근성 권한을 갖고 있는 앱은 다른 앱의 화면에 표시되는 텍스트에 접근할 수 있고, 다양한 설정 및 제어에 접근할 수 있다. 접근성 서비스 권한을 사용하려면 앱 개발 시 "BIND_ACCESSIBILITY_SERVICE" 시스템 권한을 추가하고, 사용자가 권한을 허용하면 되지만 악성 앱은 접근성 권한을 악용하기 위하여 사용자의 권한 허용을 유도하고, 권한이 허용되면 화면 오버레이 스크린 표시, 전화 및 문자 메시지 수발신, 연락처에 접근하여 악성 행위를 할 수 있다.

나. 배터리 최적화 권한 요청

악성 앱이 화면에 보이지 않고 백그라운드에서 항상 실행되기 위해서 사용자에게 “ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS”라는 “배터리 최적화 무시” 권한을 요청하게 된다.

다. 아이콘 숨김

일부 악성 앱은 백그라운드 서비스로만 동작하는데 이를 위해 최초 악성 앱이 실행 되면 악성 앱이 필요로 하는 접근성 권한 허용을 유도하고, 설치된 앱 목록에서 사용자가 삭제하지 못하도록 자신의 아이콘을 숨긴다.

라. 구글 플레이 프로텍트 기능 비활성화

악성 앱은 허용된 접근성 권한으로 사용자 개입 없이 구글 플레이 프로텍트 기능을 비활성화하고 설치된 악성 앱과 추가로 다운로드 및 설치하는 악성 앱 등을 탐지할 수 없게 한다.

마. 분석환경 실행 방지

악성코드 분석 에뮬레이터 및 분석 도구에서의 실행을 방지하기 위하여 실제와 같은 모바일 기기의 움직임을 모션 센서로 감지하여 일정 조건이 맞을 경우에만 동작하여 동적 분석이 되지 않도록 실행을 방지하는 경우도 있다.

바. 인터넷 접속 테스트

일부 악성 앱은 악성 행위를 실행하기 전에 인터넷 접속이 가능한 환경인지 확인하기 위하여 특정 홈페이지 접속 결과를 바탕으로 결과값을 확인한다.

사. 설치된 앱 목록 확인

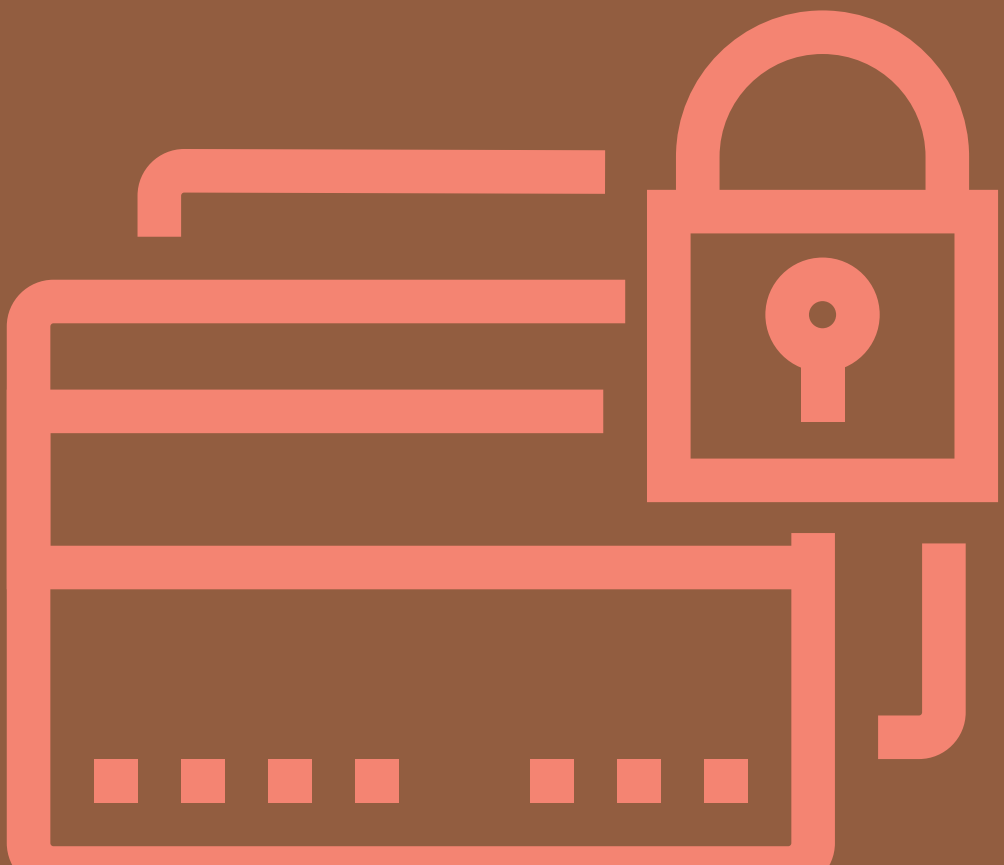
악성 앱의 공격 대상이 되는 앱이 설치되었는지 확인하기 위하여 설치된 앱 목록을 확인하고, 앱이 실행되면 화면 오버레이 공격을 통해 정상 앱 화면 위에 사용자의 개인 및 금융정보 입력을 유도하는 화면을 출력하여 입력된 정보를 탈취한다.

아. 백그라운드 실행

악성 앱은 백그라운드로 실행되어 공격자가 사전에 정의한 금융, 이메일 등의 앱과 전화 앱을 사용자가 실행하면 화면 오버레이 기능을 악용하여 개인 및 금융정보 입력을 유도하는 피싱 페이지를 화면에 띄우고 정보를 탈취하거나 보이스피싱으로 금전을 편취하는 등 악성 앱이 삭제되기 전까지 지속해서 피해를 입힌다.

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

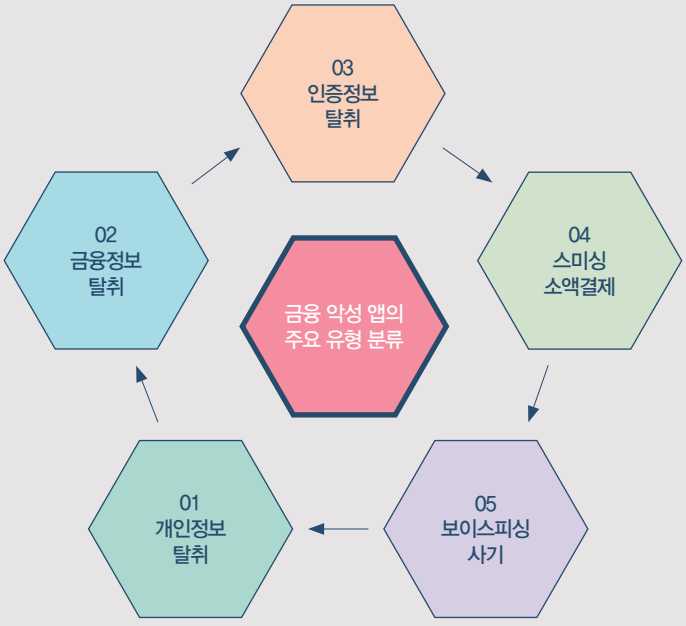


Ⅳ 금융 모바일 악성코드 유형 분류

Ⅳ 금융 모바일 악성코드 유형 분류

금융 악성 앱의 주요 기능들은 크게 개인정보, 금융정보 및 인증정보 탈취와 스미싱 소액결제 및 보이스피싱 사기로 나눠볼 수 있으며, 다수의 일반 악성 앱도 금융정보들을 탈취하는 기능이 일부 포함되어 있어 명확하게 금융 악성 앱을 구분할 수는 없다.

[그림] 금융 악성 앱의 주요 유형 분류



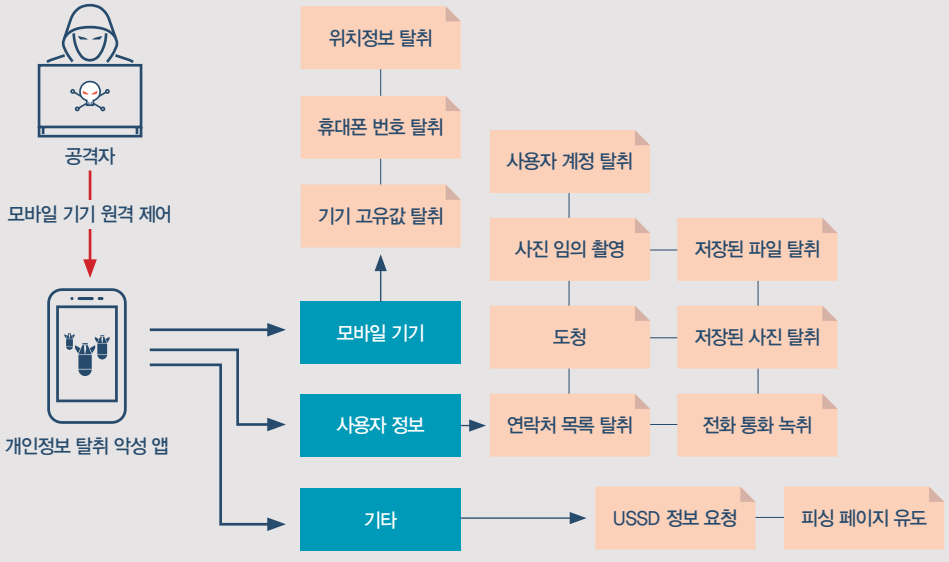
1 개인정보 탈취

모바일 기기에는 연락처 목록, 통화 목록, 문자 메시지 등 다양한 개인정보들이 저장되어 있고, 악성 앱은 이런 정보들을 탈취하기 위하여 문자 메시지, 메신저, 이메일에 악성 앱 설치 링크와 파일을 전달하는 등의 방법으로 악성 앱을 설치하도록 유도한다.

스미싱은 주로 지인과 검찰, 경찰, 우체국, 택배사 등을 사칭하여 악성 앱 설치파일 링크를 유포하고, 피싱 페이지 접속을 유도하는데 공격자는 발신자 번호 변조 및 문자 메시지 대량 발송의 편리함을 위하여 문자 전송 프로그램 및 문자 메시지 인터넷 서비스 등을 이용하여 스미싱 문자를 발송하고 있다.

인터넷으로 문자 메시지를 발송하게 되면 메시지 처음 부분에 "인터넷 발송 문자식별 표시제도"[15]에 의해 "[Web발신]" 문구가 추가되는데 휴대폰 발송 문자와 인터넷 발송 문자를 구분하기 위해서 정책적으로 도입된 것으로 "[Web발신]" 문구가 포함된 경우 주의가 필요하다는 의미이지만, 감염된 모바일 기기에서 직접 발송된 경우 정상 발송이므로 "[Web발신]" 문구 없이 수신된다.

[그림] 개인정보 탈취 흐름 및 악성 앱의 기능별 개요도



15) 대한민국 정책브리핑 | 인터넷발송 문자에 'Web 발신' 문구 표시 – 정책포커스
https://www.korea.kr/special/policyFocusView.do?newsId=148769172&pkgId=49500580

스미싱 악성 앱에 감염되면 모바일 기기 정보, 연락처 목록(저장된 이름, 전화번호, 주소 등), 문자 메시지 데이터 등을 탈취하고, 공격자는 탈취된 개인정보들을 모아 개인정보 판매, 보이스피싱 및 대출 사기 등에 활용한다.

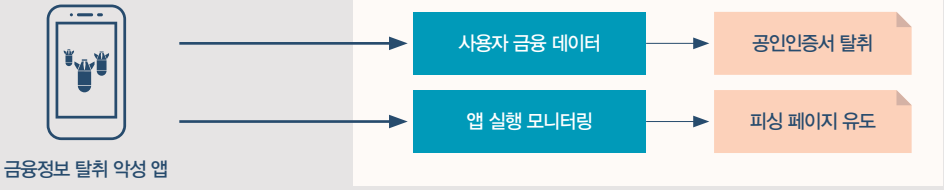
[표] 악성 앱의 주요 개인정보 탈취 데이터

구분	탈취 데이터
모바일 기기 정보	휴대폰 번호와 기기 고유값
	모바일 기기 위치정보
개인 데이터	연락처 목록에 저장된 이름, 휴대폰 번호, 주소, 이메일 정보
	전면과 후면 카메라를 이용하여 모바일 기기 사용자의 사진
	공격자가 원하는 시간에 카메라를 이용하여 사진 촬영
	모바일 기기와 연동 중인 사용자 계정 목록 확인
	마이크를 이용한 주변 소리 녹음 및 도청
	전화 수신 및 발신 통화 녹음/파일 저장
	저장된 사진 파일(모바일 기기 소유자, 신분증, 보안카드, 신용카드, 통장 사진들)
	저장된 문서, 압축 파일(다운로드 디렉터리 등)
기타	USSD를 이용한 정보를 요청

2 금융정보 탈취

금융정보 탈취를 위한 앱의 경우 개인정보 탈취와 마찬가지 형태로 검찰, 경찰, 우체국, 택배사 등을 사칭하거나 사용자가 검색엔진에서 대출, 저금리 등으로 검색했을 때 노출되는 피싱 페이지에서 악성 앱을 설치하는 경우가 일반적이며 기타 다양한 감염 경로로 사용자에게 설치를 유도하고 있다.

[그림] 금융정보 탈취 흐름 및 악성 앱의 기능별 개요도



악성 앱은 일반적으로 자주 사용되는 금융 앱들을 사전에 정의하고, 사용자의 모바일 기기에 정상적으로 설치된 앱을 사용자가 실행하면 시각적으로 유사한 피싱 페이지를 정상 앱 화면 위에 띄우는 화면 오버레이 공격을 주로 사용하며 금융정보를 입력하도록 유도하여 사용자의 계정 및 신용카드 등의 정보를 탈취한다.

[표] 악성 앱의 주요 금융정보 탈취 데이터

구분	탈취 데이터
개인 데이터	개인정보(이름, 주소, 전화번호, 생년월일)
금융 데이터	카드정보(카드번호, 유효기간, CVC/CVV)

3 인증정보 탈취

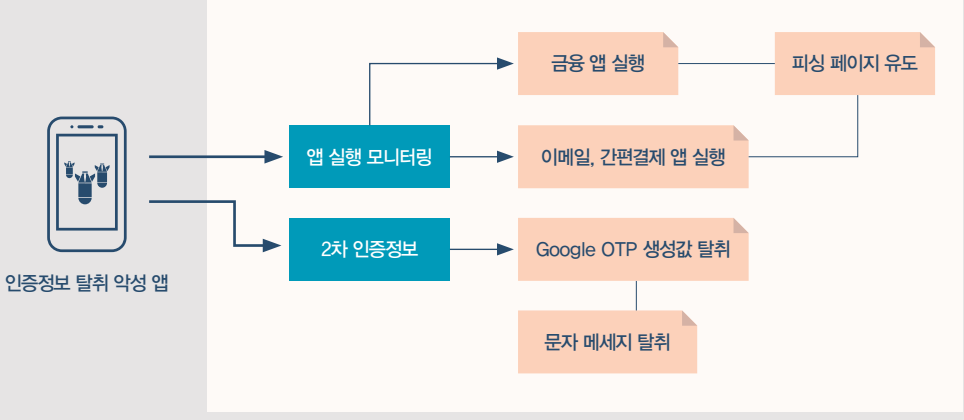
아이디, 비밀번호는 접근 권한을 얻기 위한 기본적인 인증 방식으로 이러한 인증정보는 PC 및 모바일 기기에서 악성코드 감염으로 유출되거나 가입한 홈페이지가 해킹되는 등 다양한 원인으로 유출되는데 사용자가 유출 사실을 인지할 수 없는 한계가 있다.

그래서 아이디, 비밀번호 인증 이후에 이메일, 전화, 문자 메시지, TOTP(Time-based One-time Password), 보안카드 등의 추가적인 인증 절차와 소유 기반의 인증 방식인 2단계 인증을 도입하여 아이디, 비밀번호가 유출되어도 접근 권한을 얻을 수 없도록 하고 있다.

국내 금융 앱은 2단계 인증으로 전화 인증, 문자 메시지를 주로 이용하지만, 일부 국가에서는 문자 메시지, TOTP 정보를 활용하고 있는데 문제는 2단계 인증정보 대부분이 사용자의 모바일 기기에 수신되는데 악성 앱에 감염된 상태인 경우 2단계 인증의 안전성을 보장할 수 없게 된다.

이를 통해 악성 앱에 감염되면 공격자는 모바일 기기를 제어하여 사용자가 홈페이지 로그인, 모바일 뱅킹 인증으로 2단계 인증정보를 수신받게 되면 정보를 탈취하여 권한을 획득할 수 있게 된다.

[그림] 인증정보 탈취 흐름 및 악성 앱의 기능별 개요도



[표] 악성 앱의 주요 인증정보 탈취 데이터

구분	탈취 데이터
개인 데이터	이메일 계정(아이디, 비밀번호)
금융 데이터	2차 인증정보(구글 OTP)
	금융회사 및 간편결제 계정(아이디, 비밀번호)

4 스미싱 소액결제

스미싱(Smishing)은 SMS(문자 메시지)와 Phishing(피싱)의 합성어로 문자 메시지로 수신되는 악성 앱 설치파일이 포함된 링크를 사용자가 접속 후 정상 앱으로 인지한 사용자가 다운로드 및 설치하면서 감염되는 형태로 개인정보 탈취 및 소액결제 피해까지 발생시키는 사기 범죄이다.

악성 앱은 감염된 모바일 기기에 저장된 문자 메시지 데이터와 가입한 통신사 및 휴대폰 번호 등의 개인정보를 탈취하며, 공격자는 탈취한 정보를 게임머니, 상품권 등의 결제 과정에서 입력하고 감염된 모바일 기기에 수신되는 본인인증에 필요한 인증 문자를 중간에서 가로채어 금전적인 피해를 준다. 또한, 모바일 기기에 저장된 연락처를 이용하여 스미싱 문자를 발송하여 공격을 전파한다.

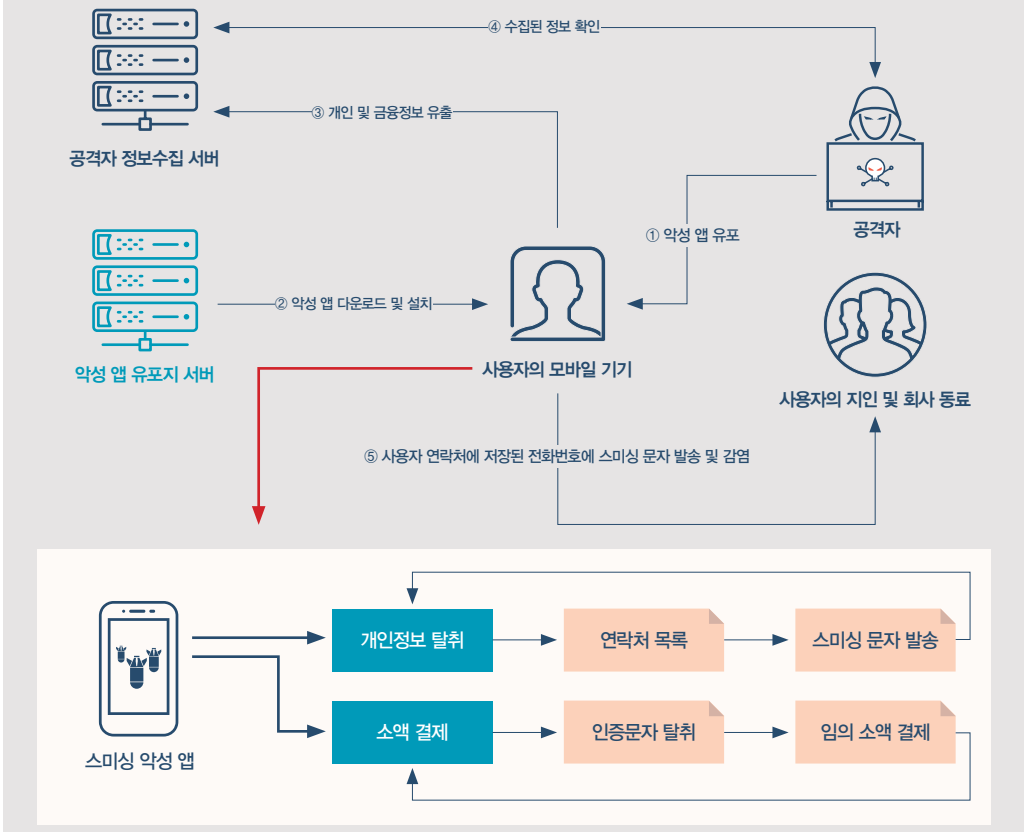
공격자는 사전에 이름, 주민등록번호, 휴대폰 번호 등의 개인정보를 홈페이지 및 데이터베이스 해킹, 다크웹 등에서 확보하고, 악성 앱이 포함된 링크를 개인정보가 유출된 사용자에게 문자 메시지로 전송하며 다운로드 및 설치를 유도한다.

공격자는 결제 사이트에서 사전에 확보한 이름, 주민등록번호, 휴대폰번호를 입력 후 인증번호를 요청하고, 감염된 모바일 기기에 수신되는 인증정보를 악성 앱에 의해 중간에 가로채어 공격자에게 전달한다. 이때 문자 메시지 전체를 실시간으로 전달 받는 방법과 특정 전화번호에서 수신되는 문자 메시지만 전달 받는 방법을 사용한다.

인증번호를 중간에 가로채어 전달받은 공격자는 결제 사이트에 입력함으로써 소액결제 피해가 발생되는데 소액결제가 가능하면서 현금화가 가능한 게임 아이템, 웹하드 포인트 등이 대상이다. 사용자는 보통 피해 사실을 나중에 모바일 청구서에서 확인을 할 수 밖에 없어 빠른 대처가 어려운 실정이다.

다음은 공격자의 악성 앱 유포부터 시작하여 모바일 기기에 저장된 개인 및 금융정보 유출과 연락처에 저장된 전화번호에 스미싱 문자 발송을 하여 2차 공격이 진행되는 일반적인 스미싱 범죄 흐름을 나타낸 것이며 이 중 사용자의 모바일 기기에서 실행되는 스미싱 악성 앱의 기능들을 분석하였다.

[그림] 일반적인 스미싱 범죄 흐름 및 악성 앱의 기능별 개요도



5 보이스피싱 사기

보이스피싱(Voice Phishing)은 음성(Voice) + 개인정보(Private Data) + 낚시(Fishing)의 합성어로 전화, 문자 메시지, 메신저 등을 이용하여 금융회사, 공공기관 등을 사칭하고 개인정보 유출, 범죄사건 연루, 해외 결제, 고액 결제, 계좌 검증 등의 거짓말로 피해자에게 심리적으로 압박하여 계좌이체 및 상품권 등으로 금전을 편취하는 범죄이다. 또한 단순히 피해자에게 전화하여 주민등록번호, 계좌번호 등의 정보를 요청하고 개인정보를 탈취하는 경우도 존재한다.

보이스피싱을 하기 위해서 범죄조직이 무작위로 전화를 발신하는 경우와 이미 피해자 가족들의 개인정보와 연락처를 알고 있는 상태에서 전화를 발신하는 경우가 있는데 범죄자는 이런 개인

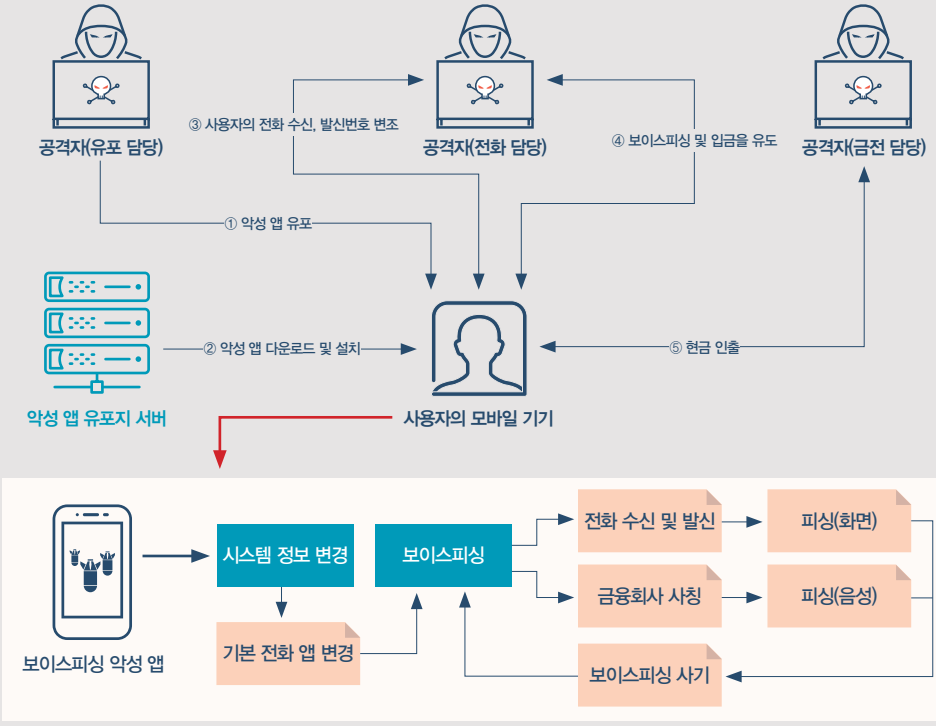
정보들을 홈페이지 데이터베이스 유출, 다크웹 등에서 획득했을 수 있지만, 사용자의 모바일 기기가 보이스피싱 악성 앱에 감염이 되어 모바일 기기에 저장된 연락처, 문자 메시지, 사진 등의 개인정보들이 탈취되면서 범죄에 이용되기도 한다.

사용자가 악성 앱에 의해 범죄조직에 전화 연결이 되면 사전에 녹음한 안내 음성을 재생하는 형태가 일반적이었지만 최근에는 경찰이나 금융회사 고객센터 전화 연결 시 나오는 안내 음성을 별도 녹음하여 파일로 저장하고 재생하는 형태도 발견되었다.

녹음된 66개 파일을 분석하면 공공기관 및 자산규모가 큰 은행, 카드, 저축은행, 대부업 등과 관련된 고객센터 및 지역 지점 전화번호 344개를 이용하여 구성된 것을 확인할 수 있다.

다음은 공격자의 악성 앱 유포부터 시작하여 사용자의 전화 수신 및 발신번호를 변조하여 보이스피싱을 통해 입금을 유도하고, 현금화를 하는 일반적인 보이스피싱 범죄 흐름을 나타낸것이며 이 중 사용자의 모바일 기기에서 실행되는 보이스피싱 악성 앱의 기능들을 분석하였다.

[그림] 일반적인 보이스피싱 범죄 흐름 및 악성 앱의 기능별 개요도



금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

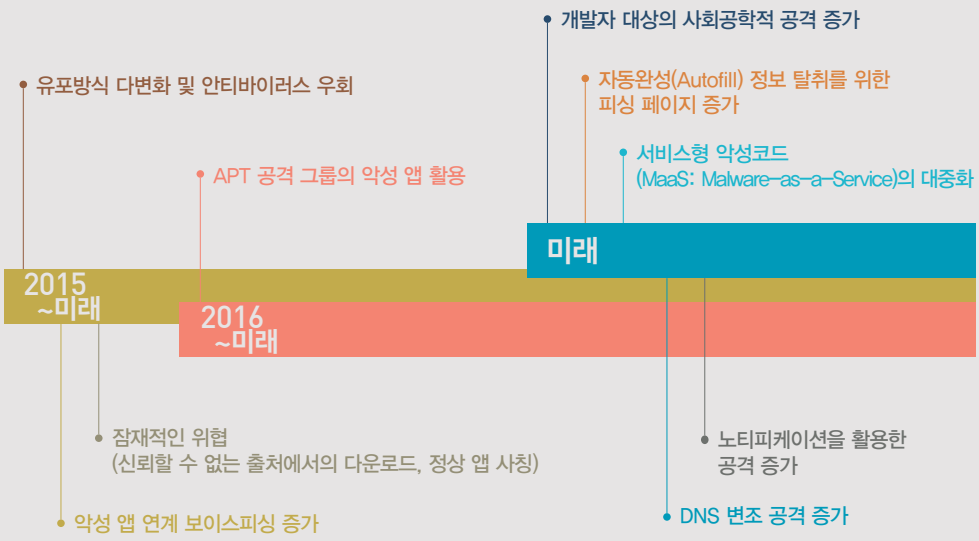
V

예상되는 모바일 위협

V
예상되는 모바일 위협

미래의 모바일 공격 위협을 예측하는 것은 상당히 포괄적인 연구이다. 따라서 기존에 없던 혁신적인 기술에 대한 예측보다는, 과거와 현재의 모바일 악성코드의 흐름을 통해 앞으로 확산 및 강화될 가능성이 있는 위협을 전망하였다.

[그림] 예상되는 미래의 모바일 보안 위협



1 개발자PC 및 사용자 모바일 기기 환경

가. 개발자 대상의 사회공학적 공격 증가

2019년 국내 안드로이드 앱 개발자의 PC가 해킹[16]되어 개발 중인 버스 알리미 앱의 소스 코드에 악성 앱을 다운로드하는 코드를 추가하여 공식 마켓에 업로드 되면서 많은 사용자가 해당 앱의 신규 설치 및 업데이트로 악성 앱이 설치되었다.

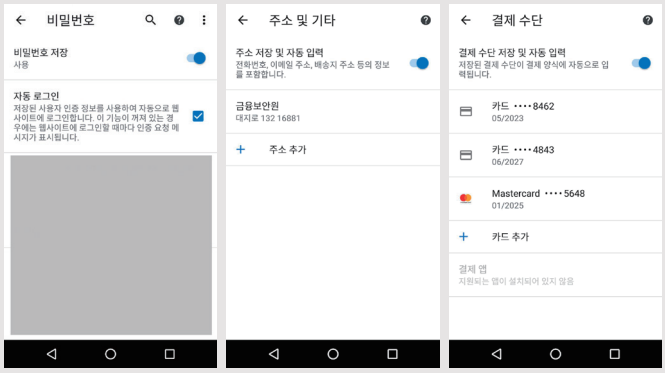
악성 앱은 특정 키워드의 파일을 검색하여 공격자의 서버에 업로드하고, 구글 피싱 로그인 페이지를 화면에 띄워 사용자의 구글 계정을 탈취하는 공격을 수행하였다.

나. 자동완성(Autofill) 정보 탈취를 위한 피싱 페이지 증가

자동완성 기능은 사파리, 엣지, 크롬 등의 웹브라우저에서 지원하고 있고, 안드로이드 운영체제에서는 v11에서 공식적으로 키보드와 자동완성 기능을 통합하여 지원 예정[17]이다. 사용자가 저장하는 개인 및 카드 정보는 보안 기술 및 정책으로 안전하게 저장될 수 있지만, 이 정보들을 사용하고 입력하는 것은 사용자의 선택이기 때문에 의심스러운 페이지에서의 정보 입력은 조심해야 하며 앞으로 자동완성 기능을 이용한 피싱 페이지 공격이 증가할 것으로 예상된다.

16) MalBus: Popular South Korean Bus App Series in Google Play Found Dropping Malware After 5 Years of Development | McAfee Blogs
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/malbus-popular-south-korean-bus-app-series-in-google-play-found-dropping-malware-after-5-years-of-development/
17) Android 개발자 | Android Developers | 키보드와 자동완성 통합
https://developer.android.com/preview/features/ime-autofill?hl=ko

[그림] 웹브라우저에서 지원하는 자동완성 기능



저장된 계정정보는 저장된 도메인과 접속하는 도메인의 인증서를 비교하기 때문에 피싱 사이트에서는 인증서 오류가 발생하여 자동완성 기능이 동작하지 않지만 개인 및 카드 정보 자동완성 기능은 사전에 약속된 입력 폼의 구조만 맞으면 반응하기 때문에 사용자가 부주의하면 피싱 사이트에서 자동완성으로 입력된 데이터가 유출될 수 있다.

2 공격자 환경

가. 서비스형 악성코드(MaaS: Malware-as-a-Service)의 대중화

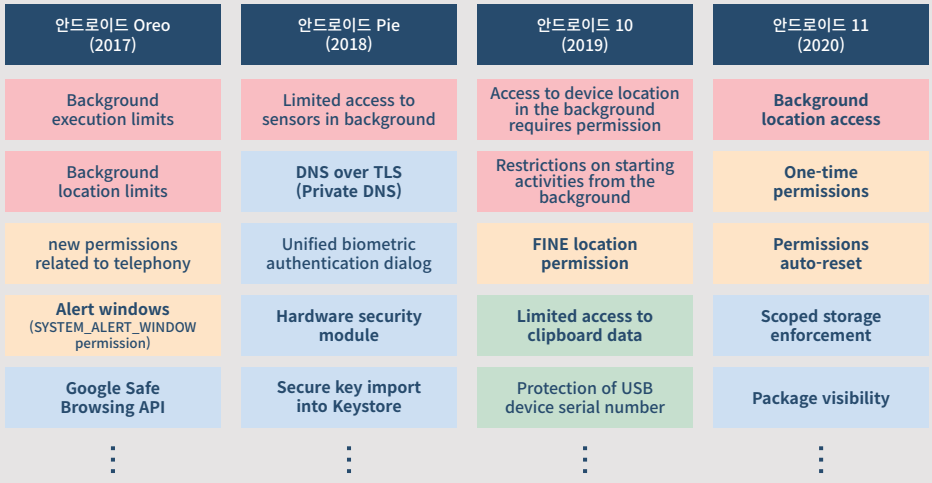
기존에는 공격자가 악성코드 개발부터 유포 및 운영까지 관련된 기술들을 모두 알아야 했지만, 공격 방법 및 기술적인 이해가 없어도 비용만 지불하면 맞춤형 악성코드 제작, DDoS 공격, 익스플로잇킷, 봇넷 등의 서비스를 이용할 수 있는 다크웹 비즈니스 모델인 MaaS(Malware-as-a-Service)가 생겨났다.

악성코드 제작자는 안티바이러스에 탐지되지 않도록 주기적으로 업데이트 버전을 제공하고, 디도스 공격자는 봇넷들을 관리하여 이를 사용할 수 있는 계정을 제공하는 등 공격자는 공격 도구와 서비스들을 유료로 임대하여 공격에 활용하고 있으며 앞으로 다크웹과 함께 지속적인 발전이 예상된다.

3 모바일 운영체제 환경

안드로이드는 새로운 버전을 출시할 때마다 다양한 보안 업데이트를 제공하고 있다. 2020년에 출시된 안드로이드 11을 포함하여 최근 4개 버전에서 보안과 관련된 주요 업데이트를 살펴보면, 사용자와 상호작용이 이루어지지 않은 상태에서 발생하는 악성 행위와 권한 획득을 막기 위한 패치가 다수 존재한다.

[그림] 안드로이드 운영체제 버전별 주요 업데이트 현황



또한 사용자가 일회성으로 권한을 승인하는 One-time permissions, 일정 시간 후 자동으로 권한이 취소되는 auto-reset, 민감 센서를 사용하는 앱이 노티피케이션에 표시되는 등의 업데이트는 백그라운드 제한과 더불어 악성 앱의 지속성 유지가 어려워 졌음을 의미한다.

가. 지속성을 위한 :: DNS 공격 증가

국내에서 DNS를 이용한 모바일 공격은 2장(지금까지의 모바일 위협)에서 살펴본 사례와 같이 공유기 환경에서 주로 발생해 왔다. 하지만 해외에서는 DNS를 이용한 공격 위협이 꾸준히 지적되고 있으며, 안드로이드 또한 Pie 버전부터 PrivateDNS[18] 기능을 도입하여 제 3자가

18) Google Developers | Public DNS
https://developers.google.com/speed/public-dns/docs/using

인터넷 트래픽을 도청하는 것을 방지하는 등 DNS 보안을 강화하고 있다. 이러한 점은 모바일 환경에서의 DNS 공격 파급력이 상당하기 때문이다.

현재까지는 별도로 Private DNS 설정을 변경할 수 있는 API가 제공되지 않으며 Private DNS가 사용 중인지 확인만 가능하다. 따라서 루팅된 환경에서 ADB 명령어를 사용할 수 있거나, 접근성 서비스 권한 획득을 통한 설정 변경 등의 선행 조건이 필요하다. 하지만 다수의 악성코드들이 접근성 서비스를 획득을 시도하고 있으므로 한번 설정이 변경되면 사용자가 인지하지 못한 상태에서 악성코드가 지속적으로 사용자의 스마트폰에서 악성 행위를 유지할 수 있다.

VPN Service 기능은 가상 네트워크 인터페이스를 생성하여 VPN 환경을 구성할 수 있는 기능이다. Private DNS 기능이 API로 제공되지 않으므로 다수의 DNS 변경 앱들이 이와 같은 기능으로 동작하고 있으며, 기능의 특성상 네트워크 트래픽에 접근이 가능하다. 따라서 DNS 서버를 공격자의 서버 IP로 설정하거나 임의의 페이지로 리다이렉션 시킬 수 있다.

나. 백그라운드 서비스 유지를 위한 :: 노티피케이션 공격 증가

노티피케이션은 지금까지 광고를 푸쉬 하거나 안티바이러스 앱의 경고를 제거하는 등 부가적인 공격 수단으로 사용되었고, 노티피케이션 없이도 화면 오버레이 공격 및 백그라운드 서비스를 유지할 수 있는 여러 방법들이 존재했기 때문에 주목 받지 못했다.

그러나 안드로이드 버전이 백그라운드 서비스 유지가 어려운 안드로이드 10, 11의 점유율이 올라갈수록 사용자 상호작용이나 노티피케이션 없이는 백그라운드 서비스를 유지하는 방법이 점차 어려워지고 있다. 따라서 이를 대체하는 기능이 도입되지 않는 이상 앞으로 노티피케이션을 활용한 포그라운드 서비스 형태의 악성 앱이 증가할 수 있다.

FINANCIAL SECURITY INSTITUTE

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

VI 맺음말

VI
맺음말

모바일 기기에는 다양한 개인 및 금융 데이터가 저장되고 있어 공격자의 주요 표적이 되고 있다. 앞으로도 꾸준히 특정 사회적인 이슈, 개인의 관심사 등을 역이용한 정교한 사회공학적 기법을 통해 정상 앱을 사칭하여 악성 앱에 감염되도록 하고, 저장된 데이터 탈취 및 원격 모바일 기기 제어 등 지속적인 위협과 피해 발생이 예상된다.

안드로이드 모바일 기기의 앱 설치를 위하여 공식 마켓이 아닌 구글 검색, 블로그, 커뮤니티 등에서 공유되는 설치파일은 악성 앱에 감염될 위험이 크다. 또한 문자 메시지, 메신저 등을 통해 악성 앱 설치파일 링크를 전송받는 경우는 악성 앱 배포 시 주로 사용되는 방법으로 앱 설치는 반드시 공식 마켓을 이용하고 평점, 비평 등을 확인하여 인지도 있는 앱 설치를 권장한다.

악성 앱의 다양한 감염 경로와 악성 행위들을 살펴봄으로써 감염 예방에 도움이 되었으면 하고, 앞으로 다가올 새로운 모바일 위협들은 계속되는 악성코드 실행 환경의 제한으로 모바일 운영체제 구분 없이 신규 지원하는 기능들을 악용하거나 과거와 현재에서 구현된 악성 행위들을 재사용하고, 사회공학적 기법과 결합하여 더욱 정교화된 새로운 이름의 악성 행위가 예상된다.

금융 악성 앱의 주요 목표는 모바일 기기에 저장된 금융정보 및 인증정보 탈취를 통한 부정 결제와 개인정보를 탈취하여 보이스피싱 범죄에 이용하는 것으로 스미싱, 보이스피싱 등의 악성 앱 차단과 금전적인 피해를 최소화하기 위하여 무엇보다 악성 앱을 가장 먼저 마주하는 사용자 스스로 방어하는 자세와 유추하기 어려운 비밀번호 설정, 2단계 인증 설정, 신뢰할 수 없는 출처에서의 앱 설치 금지 등의 기본적인 보안 설정과 데이터 보호가 선행되어야 하겠다.

FINANCIAL SECURITY INSTITUTE

금융 모바일 악성코드의 현재와 미래

2020 사이버위협 인텔리전스 보고서

요 약 본

발행일 2020년 12월

발행인 김영기

작성자 금융보안원 침해대응부 침해대응기획팀 (팀장 김신영)
이강석, 전희수, (윤석언, 조현호, 김흥섭, 서상헌)

발행처 금융보안원
경기도 용인시 수지구 대지로 132
TEL 02-3495-9000

금융보안원
FINANCIAL SECURITY INSTITUTE

금융미래를 열어가는
금융보안파트너

금융보안원 인텔리전스 보고서

금융권 대상의 다양한 사이버위협 데이터를 금융보안원 위협분석 전문가가 추적 · 분석하여,
유의미한 심층정보(Intelligence)로 이끌어낸 보고서입니다.

※ 문의: 침해대응부 (cert@fsec.or.kr)