# 보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

## 피해자의 심리를 교묘하게 파고드는 모바일 스미싱

AhnLab 2023-12-04

모바일 스미싱(smishing) 공격은 과거 1차원적으로 공격 대상을 속였던 방식에서, 다양한 공격 기법을 활용하고 피해자들의 심리를 파고드는 형태로 진화했다. 특히, 이들이 제작하는 악성 앱은 쉽게 판단하기 어려울 정도로 교묘하게 설계되어 있어 더욱 주의가 필요하다.

최근 안랩은 모바일 스미싱과 악성 앱 공격 기법을 심층 분석한 보고서를 발간했다. 보고서의 주요 내용을 살펴본다.


### 1. 개요

스마트폰이 대중화되고 널리 보급되면서 이를 노린 공격이 점점 증가하고 있다. 안드로이드 단말기의 경우 외부에서 다운로드 한 앱을 간단한 과정을 거쳐 쉽게 설치할 수 있다. 이로 인해 단말기에 악성 앱이 설치될 가능성이 더욱 높아진다.

최근 뉴스에서 악성 앱 설치만으로 피해자의 자금이 유출되었다는 사례가 꾸준히 보도되고 있다. 이는 악성 앱이 2FA(2 Factor Authentication) 인증 우회 기법을 사용하면서 발생했다. 2FA 인증이란 사용자가 접근하고자 하는 서비스에 로그인할 때, 기존에 등록된 전화번호에 보안코드를 전송하고, 보안코드를 입력하면 본인 인증이 완료되어 서비스 로그인이 정상적으로 이뤄지는 인증 방법이다. 인증이 간편하다는 장점으로 온라인 뱅킹 계좌 변경 및 다양한 글로벌 서비스를 통해 널리 사용되고 있지만, 악성 앱에 의해 인증코드가 노출되어 악용될 수 있다.

이번 보고서에서는 국내를 대상으로 유포 중인 스미싱 메시지의 유형을 분류하고 각 유형별 사례를 정리
그리고, 피해자가 실제 악성 앱을 다운로드 하는 악성 앱 유포 사이트의 유형을 분류하고 각 사이트별 특징에

대해 설명한다. 보이스피싱 공격 시 구글 플레이 스토어에 존재하는 원격 제어 앱, 금융 자산 조회 앱에 대해 각 앱에 대한 특징과 함께, 실제 유포 사이트 주소를 숨기기 위해 사용되는 단축 URL에 대한 설명과 최근 3개월 동안 공격 시 활용한 단축 URL 주소 목록을 소개한다. 이어서, Infostealer(정보탈취), Kaishi(은행 및 백신 사칭), Infostealer(몸캠피싱), SMSstealer(2FA 인증 우회) 등 악성 앱의 특징과 악성 앱 종류, 실행 화면, 주요 기능을 설명한다.

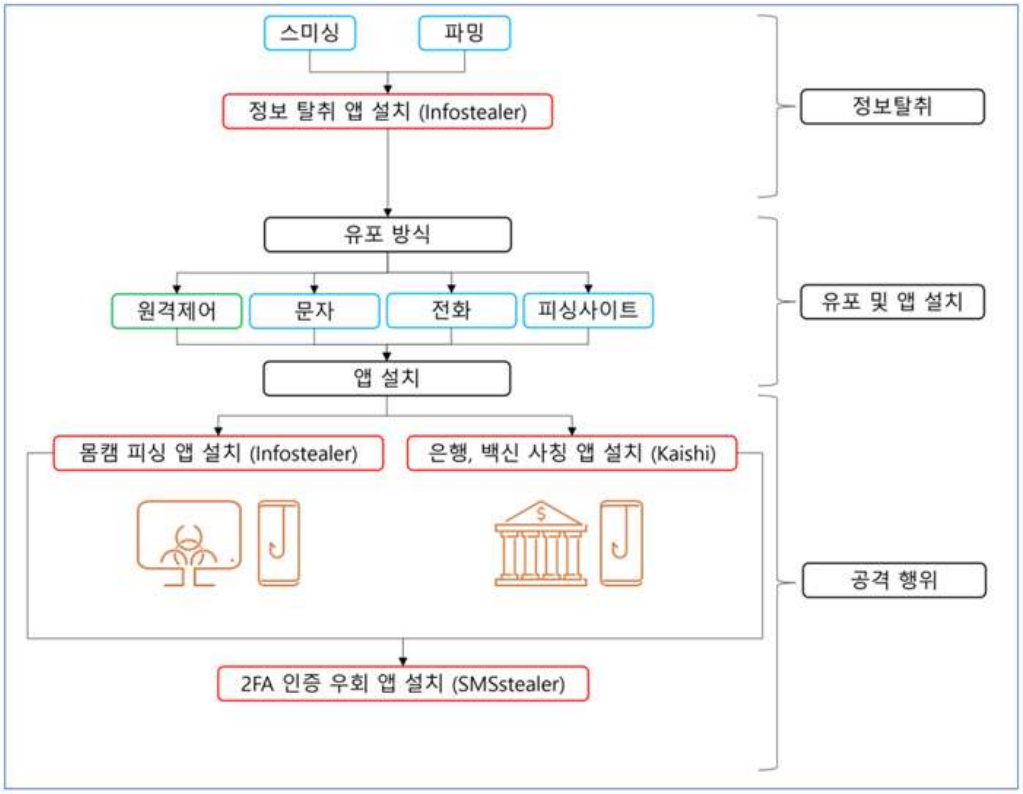
또한 각 앱의 관계를 통해 악성 앱이 설치되고 사용자의 제약 없이 자산이 유출되는 시나리오에 대해 소개한다.

## 2. 공격 시나리오

유포자는 타겟으로 설정할 피해자를 물색하기 위한 사전 작업으로 스미싱 또는 파밍 공격을 통해 악성 콘텐츠를 무차별적으로 유포한다. 피해자가 유포된 문자에 포함된 주소로 접속하면 정보 탈취 앱(이하 Infostealer)을 설치하고 실행하면 개인정보(연락처, 메시지 등)와 같은 민감한 정보가 유포자의 C2 서버로 전송된다.

정보탈취가 성공적으로 이루어지면 유포자는 감염된 사용자 뿐만 아니라 주변 지인들에게도 스미싱 문자 전송을 통한 피싱 사이트(악성 앱 유포사이트) 접속을 유도한다. 혹은 '범죄행위에 연루', '해외결제' 등 피해자의 불안감을 조성할 수 있는 말로 피해자를 현혹해 원격제어 앱 설치를 유도 후 '단말기 검사' 등의 명목으로 은행 및 백신 사칭 앱(이하 Kaishi)를 설치하고 실행한다. 이 밖에, 성인채팅 및 만남 앱을 가장해 더 많은 정보를 보고 싶어 하도록 몸캠 피싱 앱(이하 Infostealer)을 설치하도록 유혹한다.

유포자의 목적은 피해자의 자금을 탈취하는 것으로, 2FA 인증 프로세스를 우회하기 위해 메시지를 가로채는 악성 앱(SMSstealer)를 추가 설치하도록 유도한다. 이는 Infostealer와 Kaishi를 설치한 피해자 단말기로부터 인증 코드를 탈취해 자금을 훔치는 방식으로 진화하고 있다. 공격자가 활용하는 공격 기법과 악성 앱 정보 및 공격 시나리오를 정리하면 [그림 1]과 같다.




[그림 1] 공격 시나리오

[그림 1]에서 파란색으로 표시된 부분은 공격 기법으로, 각 기법에 대한 설명은 다음과 같다.
≫ **스미싱:** 메시지를 통해 피싱 사이트 접속을 유도하고 악성코드를 유포하는 공격 기법이다.
≫ **파밍:** 정상 사이트의 도메인 주소(DNS)를 중간에서 탈취해 사용자가 정상 사이트에 접속한 것처럼 착각하게 만들어 개인정보를 탈취하는 공격 기법이다.
≫ **피싱:** 불특정 다수에게 가짜 홈페이지로 접속하도록 해 개인정보를 탈취하는 공격기법이다.

[그림 1]에서 초록색으로 표시된 부분은 공격 시 활용하는 정상 앱으로 공격에 활용되는 방법은 다음과 같다.
≫ **원격 제어:** 공격자가 원격 제어 앱이 설치된 피해자 단말기를 제어한다. 원격 제어를 통해 앱 설치, 단말기 감시 등의 행위를 수행한다.

[그림 1]에서 빨강색으로 표시된 부분은 공격 시 사용한 악성 앱으로 각 앱의 특징은 다음과 같다.
≫ **정보 탈취 Infostealer 악성 앱:** 개인정보를 탈취한 악성 앱으로 주로 택배, 쇼핑몰 등으로 위장한다.
≫ **몸캠 피싱 Infostealer 악성 앱:** 단말기 및 개인정보를 탈취하고 실시간 녹음과 화면 녹화 등의 행위를 수행하는 악성 앱으로 주로 성인 앱으로 위장한다.
≫ **은행 및 백신 사칭 Kaishi 악성 앱:** 단말기 및 개인정보 등을 탈취하고 기본 전화 앱을 악성 앱으로 바꿔 전화 상태를 감시한다. 전화번호를 감시하는 목록이 존재하며, 유포자가 원치 않는 번호로 연락하거나 전화 미수신, 전화 연결 등 전화와 관련된 행위를 제어하는 강수강발(강제수신, 강제발신) 기능을 포함한다. 주로 은행 앱으로 위장한다.
≫ **2FA 인증 우회 SMSstealer 악성 앱:** 기본 메시지 앱을 악성 앱으로 바꿔 단말기에서 수발신되는 메시지 상태를 감시한다. 감염된 단말기의 모든 수발신되는 메시지를 탈취하기 때문에 메시지 이력이 존재하지 않으며, 모든 메시지의 내용을 유출한다. 주로 택배, 청첩장 등의 앱으로 위장한다.

## 3. 공격 기법

공격자가 악성 앱을 유포해 설치 후 실행하기까지 사용하는 공격 기법을 소개하고 공격 시 활용하는 정상 앱과 서비스에 대해 소개한다.

### 3.1. 스미싱

스미싱 문자 메시지는 피해자의 불안한 심리를 노려 사회적 이슈, 개인 생활과 밀접하게 관련된 내용을 유포하고 악성 앱 설치를 유도하는 형태로 진화하고 있다. 스미싱 메시지는 주로 내용과 악성 URL 링크가 포함된 주소 형태로 주로 유포되고 있으며, 최근에는 보안 앱 탐지를 우회하기 위해 URL 주소를 제외하고 공격자의 전화번호를 기입해 피해자에게 전화를 유도하는 형태로 진화하고 있다.

문자 내용 대부분은 '국외발신', 'Web발신' 등의 내용이 포함되어 있으며, 백신 앱 등으로 인해 탐지되는 것을 피하기 위해 정상 단어 내 불필요한 문자 삽입, 띄어쓰기 제거, 비정상적인 문자 사용 등의 방법을 사용한다. 악성 앱을 다운로드 하는 주소의 경우 피해자의 의심을 피하기 위해 단축 URL 사이트에서 제공하는 서비스를 활용한다. 각 스미싱 메시지 유형 별 내용과 특징 정보는 다음과 같다.

#### 3.1.1. 택배 사칭

국내에서 대다수 유포중인 택배 유형 스미싱 메시지는 주로 국내 택배 회사를 사칭한다. 사칭 메시지는 '국외발신', '국제발신', '송장번호'와 같은 정보로 시작되며 '도로명불일치로 인한 주소변경', '배송지연으로 인한 배송일정 확인', '미수취 택배 확인' 등과 같은 단어로 피해자에게 불안감을 조성한다. 메시지 내 안내되어 있는 주소로 접속하면 사칭한 회사를 가장한 피싱 사이트가 표시된다. 이로 인해 피해자는 의심을 하지 않고 정보를 확

인하기 위해 전화번호와 이름, 생년월일과 같은 정보를 입력한 후 악성행위가 포함된 앱을 다운로드 후 설치한다.

최근에는 국내 택배사들이 문자로 택배 운송 알림을 보내는 방식을 사용하지 않고 자체적으로 개발한 앱 또는 포털 사이트 내 알림 서비스를 활용하기 때문에 이를 꼭 유념해야 한다. 택배 사칭 스미싱 메시지 수신 시 택배 회사에서 제공하는 운송조회 서비스를 통해 직접 확인하는 절차를 거쳐 사전에 피해를 예방해야 한다. 택배 사칭 스미싱 메시지 유형은 [표 1]과 같다.

| **택배 사칭 유형** |
|---|
| 002-10**** [국외발신]9월15일 택배.미배달 도로명불일치 변경요망. http://xxx.xxxxx.xxx |
| [국외발신]9월15일 택배.미배달 도로명불일치 변경요망. http://xxx.xxxxx.xxx |
| [국제발신](A 택배회사)9월14일 택배.미배달 도로명불일치 변경요망 https://zrr.kr/xxxxx |
| 002-40**** [국외발신]9월15일 택배.미배달 도로명불일치 변경요망.http://xxx.xxxxx.xxx |
| [Web발신]운송장번호(5919********19): 물품지연 확인하시기바랍니다. http://xxx.xxxxx.xxx |
| [국외발신][B 택배회사]주소 정보 변경요망간단 변경하기https://tuney.kr/xxxxx |
| [국제발신]C 택배회사-잘못된 주소 정보로 인해 택배 배송이 일시 중단되었습니다. xxx.xxxxx.xxx |
| [D 택배회사]고객님의국제택배가 7,18 배송예정,본인구매아닐시 취소바람.http://xxx.xxxxx.xxx |
| [E 택배회사] 도착햇습니다 운송장번호 [5149****3326] 물품확인 하세요 xxxxx.xxx |

[표 1] 택배 사칭 스미싱 메시지 유형 - 기업명은 가칭으로 처리

3.1.2. 공공기관 사칭

공공기관 사칭 스미싱 메시지는 주로 최근 사회적 이슈 또는 경찰 및 공단 등을 사칭해 유포한다. 사칭 메시지는 '교통민원24', '국민보험공단', '질병관리청'와 같은 정보로 시작되며 '교통위반', '벌점보고서', '과태료', '통지서' 등과 같은 단어로 피해자에게 불안감을 조성한다. 메시지 내 안내되어 있는 주소로 접속하면 기관을 가장한 피싱 사이트가 표시된다. 이로 인해 피해자는 별다른 의심 없이 정보를 확인하기 위해 전화번호와 이름, 생년월일과 같은 정보를 입력한 후 악성 행위가 발현되는 앱을 다운로드 후 설치한다.

공공기관의 경우 공식 앱 스토어가 아닌 다른 곳에서는 앱 설치를 유도하지 않기 때문에 이를 꼭 유념해야 한다. 공공기관 사칭 스미싱 메시지 수신 시 발신 기관의 민원실에 확인하는 절차를 통해 사전에 피해를 예방해야 한다. 공공기관 사칭 스미싱 메시지 유형은 [표 2]와 같다.

| **공공기관 사칭 유형** |
|---|
| [A 기관]교통위반 벌점 15점 처벌 고지쳐 발송 완료 xxx.xxxxx.xxx/xxxxx |
| [A 기관]법규위반과속운전자동차벌점보고서 xxx.xxxxx.xxx/xxxxx |
| [Web발신][A 기관]과속운전(속도측정카메라 촬영) 처벌 안내 발송되었습니다 https://me2.do/xxxxx |
| [Web발신][A 기관]도로 교통 위반 소환장이 발송되었습니다. http://xxx.xxxxx.xxx |
| [Web발신][A 기관] 운행위반 감점 미처리 http://xxx.xxxxx.xxx:xxxx |
| [Web발신][B-기-관]신체검사 통지서 발송완료.상세확인 http://xxx.xxxxx.xxx |
| [Web발신]고객님 건강검진 통지서 발송완료. 상세보기 http://xxx.xxxxx.xxx |
| [Web발신][C 기관]국민연금기준소득월액변경통지서 https://vo.la/xxxxx |
| {D 기관}고객님신체검사 통지서 발송완료.내용확인 https://xxx.xxxxx.xxx |
| [국제발신](E 기관) 2차 재난지원금 신속지급 즉시확인▼ko.gl/xxxxx |

[표 2] 공공기관 사칭 스미싱 메시지 유형 - 기관명은 가명으로 표기

3.1.3. 지인 사칭

지인 사칭 스미싱 메시지는 "청첩장", "결혼식", "부고", "인증" 등과 같은 단어를 포함해 피해자의 실제 지인이 보낸 것처럼 보이도록 유포한다. 메시지 내 주소가 포함되어 있는 경우 피해자의 접속을 유도하지만, 포함이 안된 경우 메시지 또는 전화를 통해 본인인증을 명목으로 신분증 사진과 같은 개인정보를 요구하거나 특정 SNS 계정 추가를 유도한다. 지인 사칭 스미싱 메시지 수신 시 지인과의 연락을 통해 메시지를 직접 보냈는지 확인하는 절차를 통해 피해를 예방해야 한다. 지인 사칭 스미싱 메시지 유형은 [표 3]과 같다.

| **지인 사칭 유형** |
|---|
| (모바일초대장)♡결혼식♡일시: 09/30 (토) 12:00  많이많이와주세요: xxx.xxxxx.xxx/xxxxx |
| [모바일초대]♡결혼식♡일시: 09/02(토)  11:00많이많이와주 세요. xxx.xxxxx.xxx |
| *모바일 초대장♡결혼식♡일시: 09/30 (토) AM 12:00많이많이와주세요 xxx.xxxxx.xxx/xxxxx |
| 010-7717-**** *모바일초대장♡결혼식♡일시: 9/9 (토) 11:00 많이많이와주세요< xxx.xxxxx.xxx > |
| 저희 9월3일 결혼식 입니다.축하해 주세요^^ https://bit.ly/xxxxx |
| 엄마 나 폰화면이 나가서 as보냈어ㅠ이번호로 카톡추가해서 톡줘 |
| [국외발신] 나야 아빠 갑자기 급한일이 생겨서 010-xxxx-xxxx 이번호로 카톡친구추가해줘 문자답장하지말고 카톡으로얘기해줘 |
| 액정보험때문에 통신사 인증받아야 되는데. 본인인증이 안돼서 신청이 안되고 있어.아빠 폰으로 인증만 받아줄수 있어? |
| 부모님 마지막 가시는 길 외롭지 않게 부디 오셔서 참석하여주세요 me2.kr/xxxxx |
| 부모님께서 별세 하셨기에 아래와 같이 부고를 전해 드립니다.장례식장 https://zrr.kr/xxxxx |

[표 3] 지인 사칭 스미싱 메시지 유형

3.1.4. 결제 사칭

결제 사칭 스미싱 메시지는 다른 유형과 다르게 피싱 사이트 주소가 존재하지 않는다. 주소가 포함된 경우 의심을 받을 수 있기 때문에 피해자로부터 전화를 하도록 유도하기 위해 주로 큰 금액이 결제되었다는 내용으로 피해자에게 불안감을 조성해 전화를 연결하도록 유도한다. 메시지 내 기입된 전화번호로 연결하면 실제 고객센터가 아닌 가짜 고객센터로 연결되며 피해 접수를 명목으로 전화번호, 이름, 생년월일 등의 정보를 요구한다. 단순히 개인정보를 수집하는 용도가 아닌 해당 문자를 유포한 공격자가 실제 피해자에게 전달되었는지 확인하기 위한 작업의 일부이다.

공격자는 이미 기존에 확보한 개인정보를 기반으로 스미싱 메시지를 유포한다. 피해자가 전화를 걸면 실제 자신들이 유포한 대상인지 확인하고 일치하면 원격 제어 앱 설치 또는 휴대폰 검사를 명목으로 추가 앱 설치를 유도한다. 공격자가 사용하는 전화번호의 경우 평균 몇 시간이 지나면 비활성화되고, 시간이 경과되면 정상번호로 사용될 수 있기 때문에 단순히 번호 조회 결과로 스미싱 여부를 확인하는 것 보다는 의심되는 문자를 삭제하는 것이 중요하다. 결제 사칭 스미싱 메시지 수신 시 카드 고객센터에 연락해 결제 유무를 확인하고 결제한 항목이 아닌 경우 메시지를 삭제해 피해를 예방해야 한다. 결제 사칭 스미싱 메시지 유형은 [표 4]와 같다.

| **결제 사칭 유형** |
|---|
| [국제발신][해외승인]KRW:820,300원 간편결제 사용가능 해외거래 소비자보호센터:1533-2168 |
| [A 카드] 09/11일시불:961,870원 정상처리완료 추가 피해방지 본인 아닌경우(1533-1664)즉시연락바랍니다. |

| |
|---|
| [국외발신][이용내역]고객님 승인금액 549,800원 코드 6581 정상처리되었습니다 고객센터 02)532-990 |
| [국외발신][A 카드] 09/01 일시불: 989,470원 결제완료 추가 피해방지 본인 아닐경우(1551-9951) 즉시신고바랍니다 |
| [국제발신][B 카드](9647카드)개통안내드립니다.본인요청 아닐경우 신고접수-1551-8304 |
| [C 카드]08/31 일시불:724,220원 정상처리완료 추가 피해방지 본인 아닐시 즉시(1551-7720) 연락바랍니다 |
| [국외발신][D 카드]09/04 ****-****-****-***9647 카드 접수신청 고객님 신청 아닐경우 사고접수:1533-2615 |
| [Web발신]승인번호[0598] 385,150원 처리완료 [E 페이] 고객센터:052-227-6491 |

[표 4] 결제 사칭 스미싱 메시지 유형 - 카드명은 가명 처리

3.1.5. 금융기관 사칭

금융기관 사칭 스미싱 메시지는 대출, 사회적 이슈 등의 요소를 반영해 유포한다. 일전에는 코로나 19 재난지원금을 가장한 메시지가 유행했으며, 일반적으로는 대출에 관한 내용이 많다. 금융기관 사칭 스미싱의 경우 과거에는 'OO캐피탈' 내용과 함께 악성 앱을 다운로드할 수 있는 캐피탈 사칭 피싱 사이트 접속을 유도했다.

최근에는 피해자가 직접 공격자에게 전화하도록 문자 내 전화번호가 포함되어 있으며, 실제 은행 고객센터 전화번호와 '직통전화', '상담문의', '무료거부' 등의 내용과 가짜 번호가 함께 존재한다. 가짜 전화번호(공격자)로 연결하면 음성으로 은행 사칭 피싱 사이트 주소를 알려주고 피해자가 직접 접속 후 앱 설치를 하도록 유도한다. 금융기관 사칭 스미싱 메시지 수신 시 금융기관 고객센터로 연락해 피해 사실을 알리고, 피해 유무를 확인해야 한다. 금융 사칭 스미싱 메시지 유형은 [표 5]와 같다.

| **금융 사칭 유형** |
|---|
| A 은행입니다.고객님 개인뱅킹해외접속 결제시도 IP 로그인수집으로 고객정보 유출을 추정되오니 금융안전을위해 본인확인 인증절차 진행하오니 본인인증번호 정확히 입력하세요 |
| B 기관 OOOO팀 이동수과장입니다. 본인앞으로 해킹유출 연락드렸으나 부재중으로 연결안됩니다.빠른 보안강화하세요. 1588-9999 직통전화(07080183650) |
| [Web발신] 긴급생할비 지원사업이 집수되었습니다 다시한번 확인부탁드립니다 xxx.xxxxx.xxx |

[표 5] 금융 사칭 스미싱 메시지 유형 - 기관명은 가칭 처리

3.1.6. 기타 유형

기타 유형 스미싱의 경우 몸캠 피싱, 사회적 이슈 등의 요소에 따라 유포한다. 몸캠 피싱의 경우 가짜 회원과 연락하면서 피해자에게 더 많은 정보를 보기 위해서는 앱 설치를 해야 한다고 밝히며 악성 앱을 직접 보내거나 설치할 수 있는 사이트로 이동시킨다. 이 외에도, 사회적 이슈 또는 피해자가 불안한 부분을 악용해 스미싱 메시지를 유포하곤 한다. 이 역시, 불필요한 메시지를 수신하면 삭제해 사전에 피해를 예방해야 한다. 기타 스미싱 메시지 유형은 [표 6]과 같다.

| **기타 사칭 유형** |
|---|
| http://xxx.xxx.xxx.xxx 접속해서 apk 설치해서 영상통화해요 |
| 제가하는 요가 영상 있는데 보실래요? <apk> v3 잇으면 이상한문구뜨긴뜨는데 무시하고 설정에서 압축허용하면 바로나와요 |
| [국외발신][A 기업] 고객님계정이 해외IP에서 로그인되였습니다.해외IP차단해주세요. xxx.xxxxx.xxxxx |
| [Web발신] TTN (속보 ) N번방 전체회원 신상공개 https://bit.ly/xxxxx |

| |
|---|
| [국제발신]안녕하세요. 귀하의 프로필이 채용 추천을 받았으니 최대한 빨리 연락주세요.카카오톡ID:xxxxxxxxxx 문의바랍니다 |

[표 6] 기타 스미싱 메시지 유형 - 기업명은 가명 처리

**3.2. 악성 앱 유포 사이트**

악성 앱 유포 사이트의 경우, 사용자가 직접 앱을 설치하도록 하거나 사이트 접속 즉시 악성 APK가 다운로드 되는 형태 등 다양한 공격 형태가 있다. 유포사이트의 공통적인 특징으로는 특정 기관 또는 업체를 사칭하거나 성인 사이트 등을 가장해 활성화되어 있다는 것이다. 또한, 정상 사이트처럼 보이기 위해 피해자로부터 전화번호, 송장번호 등과 같은 정보를 입력하면 원하는 정보를 확인할 수 있게 설계되었다.

대부분의 유포 사이트는 모바일이 아닌 다른 환경(윈도우PC 등)에서 접속하는 경우 정상 사이트로 이동하도록 설계되어 있다. 공격자가 사이트를 직접 개설하고 접속을 유도하는 형태도 존재하지만 정상 사이트의 기능을 악용해 피해자의 접근을 유도하는 사례도 발견되고 있기 때문에 주의가 필요하다.

다음은 여러 악성 앱 유포 사이트들의 형태를 정리한 것이다.

3.2.1. 전화번호 입력

전화번호 입력을 유도하는 피싱 사이트의 경우 가장 일반적인 악성 앱 유포 사이트 유형 중 하나이다. 택배, 건강검진, 교통단속 등 다양한 유형으로 유포된 스미싱 메시지에서 전화번호, 송장번호를 입력하는 사이트로 이동한다. 과거에는 유포 사이트에서 입력한 정보(전화번호, 송장번호 등)의 경우 검사를 별도로 진행하지 않았지만, 최근에는 공격자가 유포한 대상의 전화번호, 송장번호, 이름, 생년월일 등이 아닌 경우 실제 악성 앱을 다운로드하지 못하게 진화했다.

3.2.2. 버튼 클릭

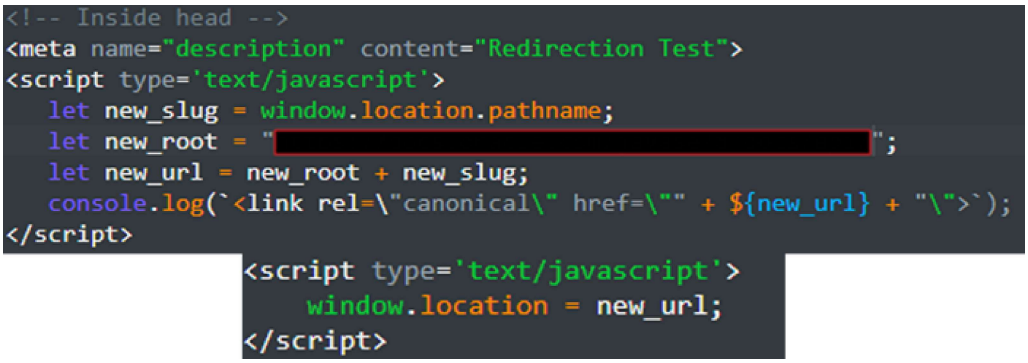
버튼을 클릭하는 유포 사이트의 경우 사용자가 직접 앱을 설치할 수 있도록 하기 위해 주로 '열기', '다운로드', '공식 스토어' 등의 버튼으로 표시된다. 공식 스토어 버튼 클릭 시, 실제 스토어에서 운영하고 있는 것처럼 보이기 위해 가짜 페이지로 이동되는 사례도 존재한다. 버튼을 클릭해 악성 앱을 유포하는 사이트의 경우 별다른 인증 없이 단말기 내 악성 앱을 다운로드 한다.

3.2.3. 직접 다운로드

다운로드를 유도하는 유형의 유포 사이트의 경우 유포자가 보낸 주소로 접속 시 악성 앱을 단말기에서 바로 다운로드 한다. 피해자는 다운로드 유무를 결정하지 못하며, 공격자는 원격 제어를 통해 다운로드 한 APK 파일을 단말기에 설치할 수 있다.

3.2.4. 리다이렉트

리다이렉트 유형의 경우 일부 SNS에서 허용하는 리다이렉트 기능을 통해 정상 사이트 주소로 접속 시 악성 앱 유포 사이트로 이동하도록 구현된다. 공격자는 정상 링크 주소가 포함된 메시지를 피해자에게 전송하고 피해자가 링크로 접속하면 악성 앱 유포 사이트로 리다이렉트 된다. 정상 사이트 주소에 숨어서 사용하는 기능이기 때문에 피해자는 해당 링크가 악성 링크인지 확인이 어려워 피해를 입을 가능성이 크다.




[그림 2] 리다이렉트 사이트 유형

### 3.3. 공격에 활용되는 정상 앱과 서비스

과거에는 공격자가 단순히 스미싱 메시지 내 주소를 통해 피해자가 악성 앱 유포 사이트에 접속하도록 유도했다. 하지만, 백신 앱 탐지, 스마트폰 사용자의 보안 인식 강화 등으로 인해 공격 성공에 어려움이 생겼다.

이 가운데, 공격자는 공격을 성공시키기 위해 기존 악성 앱 유포 사이트 주소를 직접 보내는 방식이 아닌, 단축 URL 서비스를 활용하거나 공식 스토어의 정상 앱을 먼저 설치하도록 하는 방식으로 사용자의 의심을 피하기 시작했다. 그리고, 공격자가 직접 피해자 단말기와 원격 연결 후 악성 앱 유포 사이트에 접속한 후 악성 앱을 다운로드 하는 형태로 진화했다. 또한, 자산 현황을 쉽게 파악하기 위해 국내에서 서비스 중인 자산 조회 앱을 통해 피해자의 자산 현황을 빠르게 파악해 탈취할 자산 규모를 확인하기도 한다.

다음으로 공격자가 주로 사용하는 원격 제어 앱과 금융자산 조회 앱 종류와 각 앱의 특징에 대해 소개한다.

#### 3.3.1. 원격제어 앱

공격자는 두 가지 측면을 악용해 원격 제어 앱 공격을 수행한다. 첫째는 앱이 공식 스토어에서 다운로드 된다는 점이다. 공격자는 피해자에게 공식 스토어에서 원격제어 앱을 설치하도록 유도하는데, 피해자는 공식 스토어에서 다운로드 하는 앱인 만큼 별다른 의심을 하지 않고 원격제어 앱을 다운로드 한다.

둘째는 피해자의 상황을 파악하기 위해 직접 단말기를 확인한다는 명목으로 원격제어 앱을 설치하도록 유도한다는 것이다. 피해자들은 어떻게 해야할 지 모르는 일이 발생했을 때 누군가가 호의를 베풀어 직접 단말기를 검사해준다고 하면 안도감을 느끼고 공격자의 요청에 따라 원격제어 앱을 설치한다. 공격자는 피해자 단말기에 직접 접근해 악성 앱을 쉽게 설치하고 금융 정보와 같은 개인정보, 백신 프로그램 설치 유무도 쉽게 확인할 수 있다.

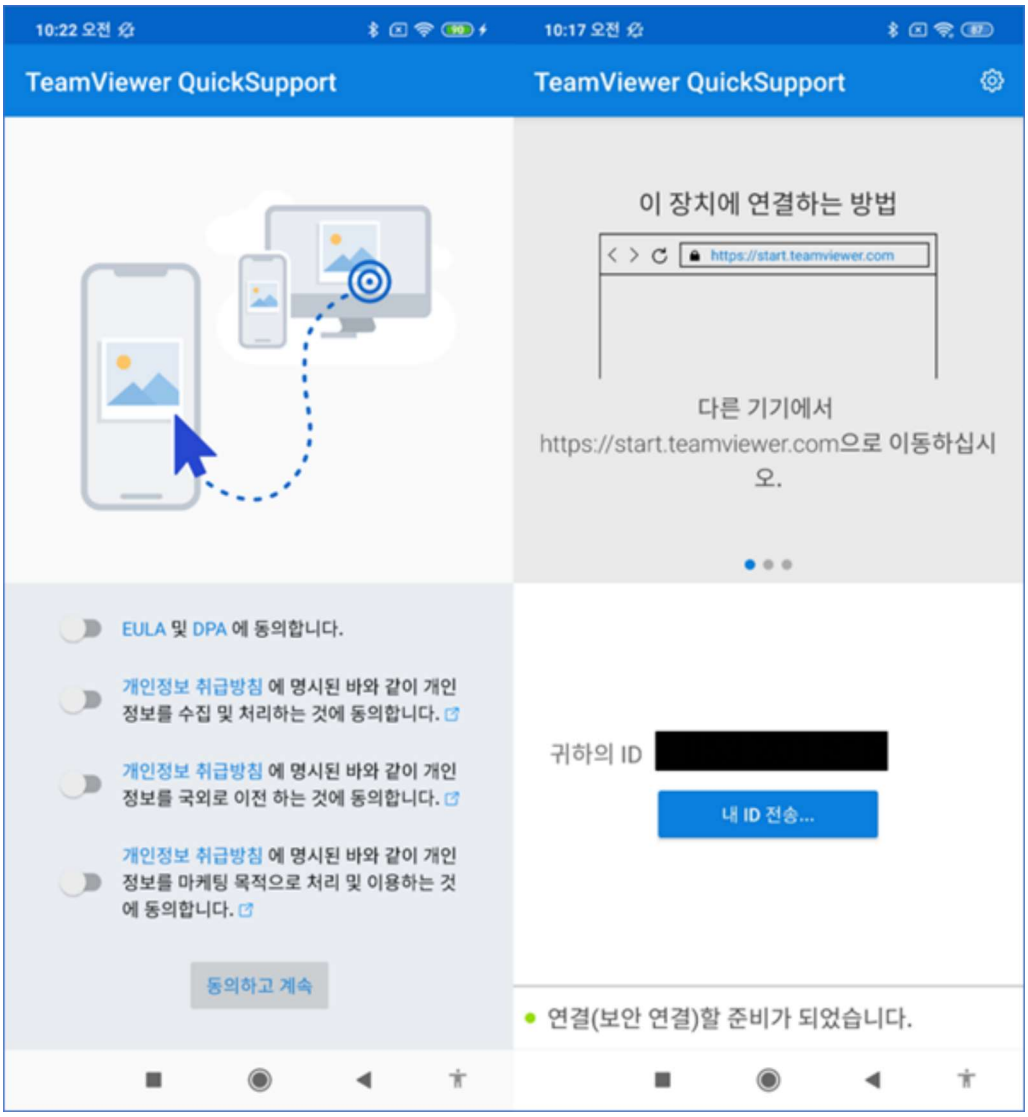
다음은 공격에 많이 활용되는 원격 제어 앱들이다.

##### 3.3.1.1. TeamViewer QuickSupport

TeamViewer QuickSupport의 경우 구글 공식 스토어에서 5000만 회 다운로드 될 정도로 인기가 높은 원격 제어 앱이다. QuickSupport의 경우 설치 후 간단한 사용 동의 절차를 거치면 단말기를 제어 가능한 고유 ID 정보가 할당되고 해당 ID 정보를 가지고 웹 또는 팀뷰어가 설치된 다른 단말기를 통해 제어가 가능하다.

공격자는 피해자와 전화를 연결한 상태에서 QuickSupport 앱을 구글 공식 스토어에서 설치하도록 유도하고 실행 후 고유 ID 정보를 요구한다. ID를 통해 원격제어 환경이 설정되면 피해자 단말기에는 "원격지원 허용", "알림창과 화면 내 모든 정보의 캡처" 창이 표시되는데 공격자는 피해자에게 허용 버튼을 클릭하도록 유도한

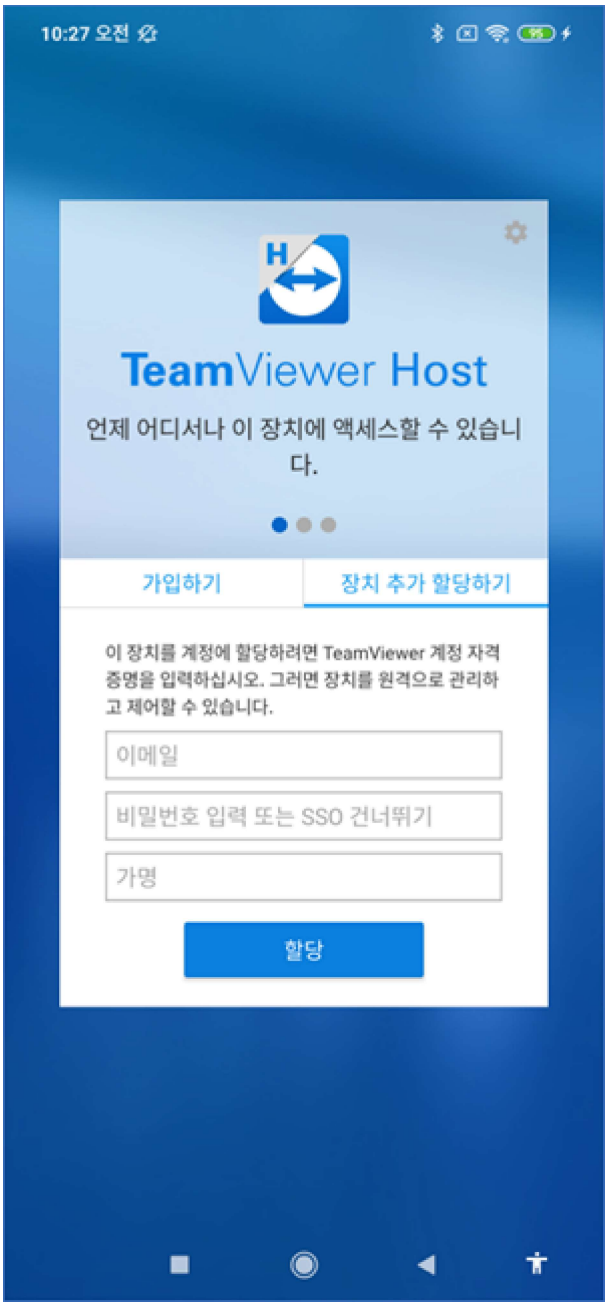
다. 원격 연결이 정상적으로 이루어지면 단말기 내 어떤 화면 부분을 클릭하는지 표시되는 기능이 존재하며, 실시간으로 단말기 화면 상태를 확인할 수 있다.




[그림 3] TeamViewer QuickSupport 실행화면

3.3.1.2. TeamViewer Host

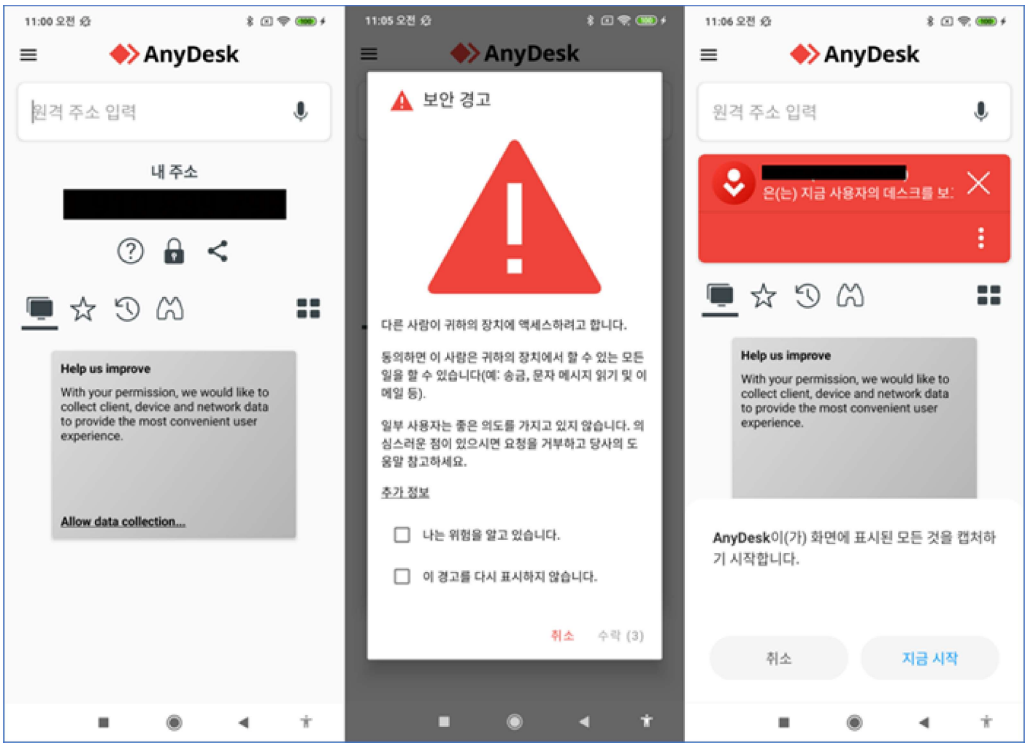
TeamViewer Host의 경우 구글 공식 스토어에서 500만 회 이상 다운로드 된 앱으로 다른 팀뷰어 앱에 비해 다운로드 수는 적지만 공격자들은 활발하게 사용하고 있다. 앞서 소개한 QuickSupport 앱과 다르게 앱 실행 시 장치 추가 할당을 명목으로 TeamViewer 계정 로그인을 요구한다. 공격자는 자신들이 사용하는 계정으로 앱에 로그인하고 피해자의 단말기를 공격자 계정에서 신뢰할 수 있는 기기로 등록한다. 로그인이 완료되면 공격자가 사용하는 단말기에 설치된 TeamViewer 앱을 통해 원격제어를 시작한다. 원격제어 시작 시 QuickSupport와 다르게 "원격지원 허용" 창만 표시되고 이를 허용하는 버튼을 클릭하면 원격제어를 수행한다.



[그림 4] TeamViewer Host 실행화면

3.3.1.3. AnyDesk

AnyDesk의 경우 구글 공식 스토어에서 5000만 회 이상 다운로드 되었으며, TeamViewer QuickSupport만큼이나 인기가 높은 원격제어 앱이다. 앱 실행 시 단말기에 따라 추가 플러그인 설치를 요청하며, 해당 플러그인은 원격제어를 보다 원활하게 하기 위해 접근성 권한 허용을 요청한다. 권한이 정상적으로 부여되면 사용 동의서와 단말기에 연결 가능한 고유 주소가 표시된다. 웹 또는 모바일에서 원격제어 연결 요청이 들어오면 보안 경고창이 표시되며 캡처 허용을 클릭하면 원격제어를 수행한다.



[그림 5] AnyDesk 실행화면

3.3.2. 금융자산 조회 앱

공격자의 최종 목적은 피해자의 자금이다. 그렇기 때문에 공격자가 선정한 대상이 어느 정도의 현금을 보유하고 있는지 확인이 필요하다. 과거에는 피해자에게 어느 은행을 사용하는지, 각 은행에 계좌 정보와 보유 금액 등을 일일이 물어봤지만, 최근 들어서는 개인 자산을 보다 쉽고 빠르게 확인할 수 있는 자산 조회 앱이 등장했기 때문에 이를 활용해 피해자의 자산 정보를 확인한다.

3.3.3. 단축 URL

단축 URL이란 '도메인 축약 서비스'라고 불리며, 기존 도메인 주소를 축소해 제공하는 서비스다. 기존 도메인 주소가 길고 복잡하기 때문에 메시지나 일부 SNS에서 글자 제한 등으로 인해 주소 정보를 전송하지 못할 때 주로 사용한다. 스미싱 메시지 유포자들은 악성 앱 유포사이트 주소를 단축 URL을 통해 숨겨 피해자가 단축 URL 주소만으로 어떤 링크인지 알기 어렵게 만든다. 최근 3개월 동안 수집된 스미싱 메시지 유포 시 사용한 단축 URL 목록은 다음과 같다.

**최근 활용 단축 URL 목록**

≫ me2.do
≫ abit.ly
≫ ko.gl
≫ urlzs.com
≫ snip.ly
≫ dokdo.in
≫ xgo.kr
≫ t.ly
≫ bit.ly
≫ han.gl
≫ zrr.kr
≫ vvd.bz

≫ surl.li
≫ bitly.com
≫ s.id

이처럼 공격자들은 고도화된 공격 기법을 바탕으로 피해자들의 심리를 교묘하게 악용하여 다양한 공격들을 전개해오고 있다. 모바일 스미싱과 악성 앱으로 인한 피해를 예방하기 위해서는 먼저 모바일 백신을 설치하고 최신 상태를 유지해야 한다. 또한, 의심스러운 웹사이트 방문을 지양하고 출처가 불분명한 문자는 삭제하는 습관이 필요하다.

이번 보고서의 보다 상세한 내용은 자사 위협 인텔리전스 플랫폼 'AhnLab TIP' 구독 서비스를 통해 확인할 수 있다.
►**TIP 포털 바로가기**

---

AhnLab 엔진개발팀 장연철 주임연구원