안드로이드 환경에서의 스미싱 및 몸캠피싱 분석과 대응 방안

서동훈* 전유민* 김민수**

*중부대학교 정보보호학전공 (대학생, okko2929@gmail.com, yumin3404@gmail.com)

**중부대학교 정보보호학전공 (교수, mskim@joongbu.ac.kr)

Analysis of Smishing and Body Cam Phishing in Android Environment and Countermeasure

DongHun Seo* Yumin Jeon* MinSu Kim**

*Department of Information Security, Joongbu University (Undergraduate student, okko2929@gmail.com, yumin3404@gmail.com)

**Department of Information Security, Joongbu University (Professor, mskim@joongbu.ac.kr)

요 약

2021년도 최근 들어 가장 많이 급증하고 있는 사이버 금융범죄 중에서 스마트폰을 이용한 범죄로는 스미싱과 몸캠피싱이 대표적이다. 이러한 금융범죄는 2017년도부터 현재까지 범죄 발생률이 증가함에 따라 관련 악성 파일 분석은 필수적인 요소로 자리 잡아 가고 있으며, 모바일 금융범죄 피해가 주로 발생한 운영체제는 안드로이드인 것으로 나타났다. 본 논문에서는 스미싱과 몸캠피싱 피해가 주로 발생한 안드로이드 APK 악성 파일 분석을 수행한 뒤, 분석 내용을 토대로 한 결과를 제시하여 모바일 금융범죄 피해를 막기 위한 대응 방안과 결론을 제시한다.

I. 서론

본 논문은 2021년도 최근 들어 가장 많이 급증하고 있는 사이버 금융범죄 중에서 스마트폰을 이용한 범죄로 대표적인 스미싱과 몸캠피싱의 APK 파일을 분석하여, 모바일 금융범죄에 대하여 안전한 보안 설정 방법에 대한 대응 방안을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 2017년도부터 2020년도까지 사이버 금융범죄가 발생했던 현황과 사이버 금융범죄 피해를 주로 입은 연령대 분포도 그리고 피해가 발생한 스마트폰 브랜드 통계와 스미싱, 몸캠피싱과 관련된 사칭 방법 등과 관련된 통계를 분석한 뒤, 결과를 정리한다. 3장에서는 2장에서 정리한 통계 결과를 토대로 스미싱, 몸캠피싱 피해가 주로 발생한 안드로이드 APK 악성 파일 분석을 수행한 뒤 분석 내용을 토대로 방법론을 제시한다. 4장에서는 안드로이드 환경에서의 스미싱과 몸캠피싱 피해를 막기 위한 대응 방안을 내며 본 논문을 마무리한다.

II. 자료 분석

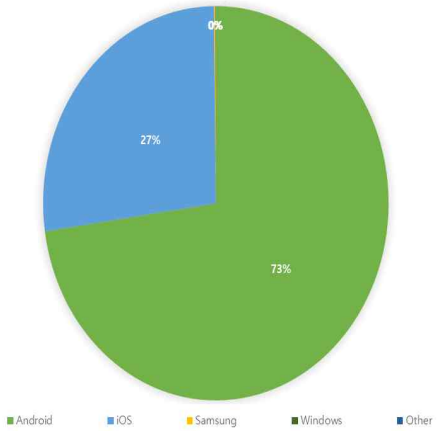
스마트폰 사용량이 계속해서 증가하고 있음에 따라 이에 대한 피해도 점점 증가하고 있다. 실제 경찰청에서 조사한 정보에 따르면 2017년도 이후로 피싱, 스미싱, 몸캠피싱과 같은 범죄 발생 건수가 [그림 1]처럼 매년 증가하고 있음을 알 수 있다.

연도	피싱	스미싱	몸캠피싱
2017	545	667	1234
2018	1978	293	1406
2019	2874	207	1824
2020	1519	822	2583

[그림 1] 모바일 금융범죄 피해 증가량

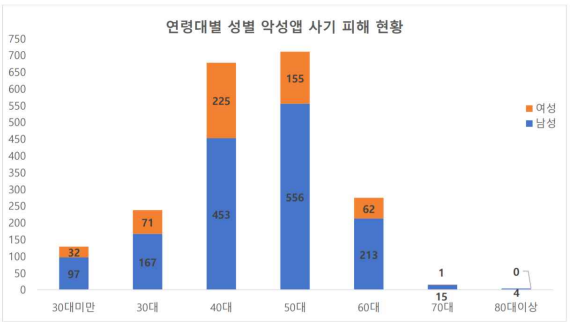
이처럼 증가하고 있는 피해를 막고자 관련된

연구를 시작하게 되었으며, 분석할 기반이 될 운영체제를 선정할 필요가 있었다. 이는 [그림 2]와 같이 단순히 한국에서 사용하는 운영체제 점유율을 통해 안드로이드를 선택할 수 있었지만, 단순 점유율이 아닌 실제 피해 사례를 통해 이를 찾고자 노력하였다.



[그림 2] 대한민국 운영체제 시장 점유율

다음 [그림 3]은 (주)인피니그루의 '피싱아이즈' 앱에서 수집한 보이스피싱, 스미싱, 악성 앱 사기와 같은 모바일 금융범죄 피해를 본 피해자의 연령대를 표현한 것이다. [그림 3]을 확인해보면 피해자의 80% 이상이 40대에서 60대인 것을 확인할 수 있다. 이는 디지털과 친숙한 10대부터 30대와는 달리 아직 디지털에 적응하지 못한 세대는 금융기관을 사칭하거나 자녀를 사칭하는 사기와 같은 범죄에 대한 대응 능력이 부족하므로 이에 대한 피해가 많이 발생하는 것을 알 수 있다.



[그림 3] 연령대별 성별 악성 앱 사기 피해 현황

또한, 주요 피해 연령대인 40대에서 60대의 스마트폰 사용 브랜드를 확인해보면 [그림 4]와 같이 각 연령대에서 85% 이상이 삼성 혹은 LG사의 스마트폰을 사용하고 있다는 것을 알 수 있는데 이는 곧 주요 피해자의 85% 이상이 안드로이드 운영체제를 사용한다는 것을 알 수 있다.

나이	삼성	애플	LG
40대	79%	11%	9%
50대	77%	5%	15%
60대 이상	65%	1%	25%

[그림 4] 연령대별 스마트폰 브랜드 사용량

최종적으로 피싱, 스미싱, 몸캠피싱과 같은 악성 APK에서 사용하는 운영체제가 안드로이드라는 것을 단순 점유율이 아닌 실제 피해 사례와 자료 조사를 통해 피해자 대부분이 안드로이드 운영체제를 사용한다는 것을 알 수 있다.

III. 악성 APK 분석

악성 APK 분석은 정적 분석과 동적 분석을 이용하여 진행한다.

3.1 정적 분석

APK는 리소스, 라이브러리, 서명, 메니페스트, Dex, 등 여러 파일을 ZIP 형식으로 압축한 파일을 의미한다. 정적 분석은 APK의 구성 중 Java 코드를 컴파일하여 바이트 코드로 변환한 Dex 파일이나 C/C++ 코드를 컴파일한 so 파일을 디컴파일러(IDA, JEB, jadx-gui)로 분석하여 코드의 흐름을 읽거나, C&C 서버의 주소와 같은 시그니처 정보를 얻는 것과 같은 과정을 의미한다.

3.2 동적 분석

공격자의 C&C 서버로 보내는 패킷을 분석하거나 실시간으로 APK의 동작을 확인하거나 변조를 할 때 사용한다. 동적 분석 방법 중 하나인 프록시를 사용한 방법은 안드로이드 분석 환경에 Burp suite 인증서 등록과 네트워크 고급 설정 관리에서 프록시 설정 후 윈도우 내 Burp suite에서 이에 대한 Listner를 생성하면 SSL Pinning이 설정되어 있지 않은 이상 모든

통신을 확인, 변조 혹은 제거할 수 있다. 다음으로 후킹을 사용한 방법은 Frida server를 안드로이드 환경에 설정한 후 윈도우 환경에서 이를 활용하여 실시간으로 APK 내 함수로 넘어오는 인자의 값을 확인하거나 반환 값을 변경할 수 있으며, 라이브러리나 메모리 또한 접근과 변조를 할 수 있다. 다음으로 디버깅은 JEB, IDA를 이용해 동적으로 변수나 인자 값을 확인하며 코드 흐름에 대해 분석할 수 있다.

IV. 모바일 금융범죄 대응 방안

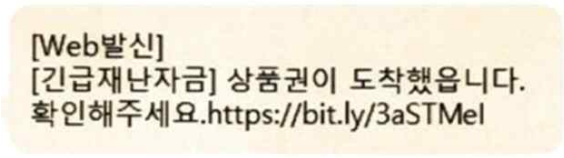
앞 장에서 APK 파일을 분석한 내용을 토대로 스미싱과 몸캠피싱과 같은 모바일 금융범죄 피해를 막기 위해서 안드로이드 환경에서의 대응 방안을 정리해보면 다음과 같다.

4.1 출처를 알 수 없는 앱 설치 거부

[그림 5] 출처를 알 수 없는 앱 허용 안 됨

기본적으로 스미싱이나 몸캠피싱과 관련된 모바일 금융범죄의 APK 파일은 출처를 알 수 없는 앱 설치를 허용하게 되면 범죄가 발생한다. 따라서 안드로이드 환경에서 APK 파일을 설치할 때는 해당 업체의 운영체제에서 제공하는 공식 스토어나 또는 검증되거나 신뢰할 수 있는 APK 파일만을 사용해야 한다.

4.2 의심되는 이메일 혹은 메시지 열람 금지



[그림 6] 출처가 불분명한 인터넷 주소(URL)

위 [그림 6]과 같이 코로나19 긴급재난지원금, 택배 배송확인 등을 사칭한 사이버 공격이 활발히 전개되고 있다. 따라서 문자 메시지의 출처를 반드시 확인하고 메시지 내 URL과 첨부파일을 꼼꼼히 확인해봐야 할 필요가 있다.

[참고문헌]

[1] 경찰청, “경찰청_사이버 금융범죄 현황_20201231”, 공공데이터포털, 2020.

[2] “Mobile Operating System Market Share Republic Of Korea 2018-2021”, statcounter GlobalStats, 2021.

[3] ㈜인피니그루, “피싱아이즈 보이스피싱 통계 보고서”, 스마트 치안 빅데이터 플랫폼, 2021.

[4] 한국갤럽 데일리 오피니언, “2012-2021 스마트폰 사용률 & 브랜드, 스마트워치, 무선이어폰에 대한 조사”, 한국갤럽조사연구소, 2021.

[5] 신희강, “설 연휴 보안수칙, 코로나19 스미미싱·해킹 주의”, 뉴데일리경제, 2021.