정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

Apple의 사이드로딩 허용이 사이버 보안에 미치는 영향

최 원 석*, 이 동 훈**

요 약

스마트폰 환경에서 사이드로딩 이란, 플랫폼 사업자의 심사 및 승인없이 앱을 스마트폰에 설치하는 것을 의미한다. 즉, 공식적인 앱 마켓을 통하지 않고 제3의 앱마켓 또는 인터넷에서 설치파일을 직접 다운로드하여 설치하는 과정을 말한다. 여기서 제3의 앱마켓이란 플랫폼 사업자가 공식적으로 관리하는 앱 스토어를 제외한 모든 앱 마켓을 의미한다. 본고에서는 사이버 보안 관점에서 제3의 앱마켓 및 사이드로딩 허용여부로 인해 발생하는 사회적 문제점을 고찰 하고자 한다. 특히, 제3의 앱마켓 및 사이드로딩을 제도적으로 허용하고 있는 안드로이드 환경에서 발생하고 있는 사회적 문제점들을 바탕으로 iOS 환경에서도 제3의 앱마켓 및 사이드로딩이 허용되는 경우, 사이버 보안 관점에서 예상되는 사회적 문제점들을 알아보고자 한다.

Ⅰ. 서 론

스마트폰 환경에서 사이드로딩 이란, 플랫폼 사업자의 심사 및 승인없이 앱을 스마트폰에 설치하는 것을 의미한다. 즉, 공식적인 앱 마켓을 이용하지 않고 제3의 앱마켓 또는 인터넷에서 설치파일을 직접 다운로드하여 설치하는 과정을 말한다. 여기서 제3의 앱마켓이란 플랫폼 사업자가 공식적으로 관리하는 앱 스토어를 제외한 모든 앱 마켓을 의미한다. 안드로이드 환경에서는 사이드로딩 및 제3의 앱마켓이 공식적으로 허용되고 있으나, Apple은 iOS 환경에서 사이드로딩 및 제3의 앱마켓을 허용하지 않고 있다. Apple은 이러한 정책을 통해 안드로이드 환경과 비교하여 사용자의 보안과 개인정보 보호 측면에서 안전한 앱스토어 생태계를 구축하고 있다. 만약 Apple이 사이드로딩을 허용하게 되면 생태계는 iOS 환경 또한 안드로이드 환경이 지니고 있는 다양한 부작용들에 노출될 것으로 예상된다.

본고에서는 사이버 보안 관점에서 제3의 앱마켓 및 사이드로딩이 허용될 경우, 현재의 iOS 생태계에 미치는 영향에 대해 고찰한다. 먼저 현재 Apple의 공식 App Store에서 앱 업로드 및 리뷰 프로세스에 대해 설명한다. 다음으로, 사이드로딩의 개념 및 방법에 대해 설명한다. 마지막으로 iOS 환경에서 제3의 앱마켓 및 사이드로딩이 허용될 경우 예상되는 사회적 문제점을 현재까지 안드로이드 환경에서 사이드로딩을 허용함으로 인해 발생하고 있는 피해 사례들을 예로 들어 제시하고자 한다.

Ⅱ. Apple App Store Review Process

Apple은 App Store라 불리는 iOS용 앱마켓을 운용하고 있다. Google의 경우에는 안드로이드용 앱을 다운로드 및 설치할 수 있도록 하는 앱마켓이 여러개 존재하는 것과 비교하여, Apple의 경우에는 단일 앱 마켓인 App Store만이 존재한다. 따라서, iOS용 앱을 개발한 개발자가 해당 앱을 배포하기 위해서는 App Store의 심사과정을 거쳐 승인을 받아야만 한다. 만약, 심사과정에서 승인이 거절되는 경우에는 해당 사유를 반영하여 수정된 앱으로 재심사를 받아야 한다. 기본적으로 Apple의 Review Process를 통과하기 위해 개발자들은 앱 제출 전에 i) 앱에 Crash나 Bug가 있는지 확인하고, ii) 모든 앱 정보와 메타데이터가 정확한지 확인하고, iii) 앱 심사팀이 연락할 경우를 대비하여 연락처 정보를 최신화 하고, iv) 실제 시연 계정과 로그인 정보, 기타 하드웨어 또는 앱을 심사하는 데 필요한 리소스를 제공하고, v) 심사 중에 바로 사용하고 접근할 수 있도록 백엔드 서비스를 활성화 시켜놓아야 하며, vi) 명확하지 않은 기능이나 앱 내 구입에 관한 자

* 한성대학교 IT융합공학부 (교수, wonsuk@hansung.ac.kr)
** 고려대학교 정보보호대학원 (교수, donghlee@korea.ac.kr)

세한 설명과 지원 문서를 앱 심사 메모에 기록하고, vii) 마지막으로 Apple이 제공하는 지침 문서를 준수하여 앱이 개발되어야 한다. 이와 같은 기본적인 내용을 충족하였을 때, 개발자들은 자신이 개발한 iOS용 앱을 App Store 심사를 위하여 제출할 수 있다. Apple은 안전성, 성능, 비지니스, 디자인, 법적 요구사항 측면에서 중점적으로 심사를 진행하여 승인 또는 거절 여부를 판단한다. Apple에서 심사하는 많은 항목들 중에서 보안이슈가 발생할 수 있는 항목들은 다음과 같다.

(1) 불필요한 리소스 사용: 전원을 효율적으로 관리하기 위해서 불필요한 리소스 사용(e.g., 배터리, Read/Write 등) 여부를 확인한다. 또한, 제 3자 광고에서 암호 화폐 채굴과 같이 관련 없는 백그라운드 프로세스 실행여부를 확인한다. 이를 통하여, 사용자 몰래 스마트폰의 리소스를 이용하여 악성행위를 하는 앱들을 사전에 차단할 수 있다.

(2) 불필요한 시스템 설정 요구: 앱에서 기기를 재시동하거나 앱의 핵심 기능과 직접적인 관련 없이 시스템 설정(e.g., 보안기능 비활성화)을 변경하도록 제안 또는 요구하는지 여부를 확인한다. 스마트폰의 시스템 설정이 변경된 이후에는 악성앱이 실행되는 것이 용이해지기 때문에, 시스템 설정 변경 여부는 반드시 사전에 점검되어야 하는 요소이다.

(3) 다른앱의 사용자 데이터 수정: 기본적으로 iOS에 설치되는 앱들은 각각 적절하게 샌드박스되어야 한다. 또한, 다른 앱에 저장된 사용자 데이터(e.g., 책갈피, 주소록, 캘린더 항목 등)를 수정하는 경우 macOS API만을 사용해야 한다. 악성앱의 경우에는 사용자의 민감한 정보를 다루는 앱에 저장되어 있는 데이터 탈취를 목표로 할 수 있다. 따라서, 하나의 앱이 다른 앱에 저장되어 있는 데이터의 접근 여부를 반드시 사전에 점검하여야 한다.

(4) 자동실행 여부 체크: iOS 부팅 또는 로그인 시 사용자 동의 없이 앱이 자동 실행되거나 자동으로 실행하는 다른 코드가 있어서는 안되며, 사용자가 앱을 종료한 후에도 동의없이 계속 실행하는 프로세스를 생성하면 안된다. 악성앱이 설치된 이후에는 사용자 해당 앱을 직접 실행하지 않더라도 자동으로 실행되게 하는 것이 일반적이다. 따라서, 특정 앱의 자동실행 여부는 반드시 사전에 점검되어야 할 요소이다.

(5) 추가 코드 다운로드 여부 체크: 심사 과정 중에 확인된 내용과 다르게 앱에 기능이 추가되거나 크게 변경되는 독립형 앱, 추가 코드나 리소스를 다운로드하거나 설치하면 안된다. 일부 악성앱의 경우에는 스캐닝 도구의 검사를 우회하기 위하여, 앱이 설치된 이후에 외부에서 악성행위를 하는 코드를 다운로드 받는 경우가 있다. 따라서, 특정 앱의 추가 코드 다운로드 여부는 반드시 사전에 점검되어야 할 요소이다.

(6) 루트 권한 요청 또는 setuid 속성 사용 여부: 루트 권한을 요청하거나 setuid 속성을 사용하면 안된다. 루트 권한을 갖는 앱은 다른 앱과 비교하여 스마트폰의 많은 기능들을 제어할 수 있다. 예로, 특정 앱이 루트권한을 갖게 있다면 스마트폰에 저장되어 있는 사용자의 개인정보 데이터를 모두 접근할 수 있다. 따라서, 특정 앱이 루트 권한을 요청하거나 setuid 속성을 이용하여 권한을 높이는 행위를 하는지 여부는 사전에 점검되어야 한다.

(7) 개인정보 처리 방침에 대한 준수여부: 모든 앱은 앱 내부에 쉽게 볼 수 있는 개인정보 처리방침 관련 링크가 포함되어야 한다. 또한, 개인정보 처리방침은 분명하고 명시적이어야 한다. 예를 들어, 앱과 서비스가 수집하는 대상 정보, 정보 수집 방법, 수집한 정보의 사용 목적을 명확하게 정의하여야 한다.

(8) VPN 앱: VPN 서비스를 제공하는 앱은 기관(organization)으로 등록된 개발자가 제공하고 NEVPNManager API를 사용해야 한다. 사용자가 서비스를 구입하거나 사용하기 전에 앱 화면에 어떤 사용자 데이터를 수집할 것이며 수집한 사용자 데이터를 어떻게 사용할 것인지를 명확하게 설명해야 한다.

(9) 모바일기기관리 (Mobile Device Management, MDM): MDM 서비스를 제공하는 앱은 Apple에 해당 기능을 사전에 요청해야만 한다. 모바일 기기 관리 앱은 민영 기업, 교육 기관 또는 정부 기관에서만 제공할 수 있지만, 제한적으로 유해 콘텐츠 차단 서비스 또는 기기 보안을 위해 MDM을 사용하는 기업에서도 제공할 수 있다. MDM 서비스를 제공하는 앱은 그 어떤 데이터도 제 3자에게 여하한 목적으로 판매, 사용 또는 공개해서는 안되며 이를 앱의 개인정보 처리방침에서 반드시 언급해야 한다.

Apple은 중앙집중화된 앱 유통시스템을 운영하면서 위와 같은 항목들을 철저하게 심사하고, 높은 기준을 통과한 앱들만 유통될 수 있도록 관리하고 있으므로, 높은 보안성과 안전한 앱스토어 생태계를 구축하고 있

다. 특히, 모바일 환경에서 악성코드가 정상적인 앱으로 위장하여 제3의 앱마켓을 통해 배포되는 이유는 이와 같은 중앙집중화된 검증과정을 회피하려는데 그 목적이 있다고 할 수 있다. 기술적인 측면에서는 안드로이드 OS와 iOS 여부와 무관하게 악성앱 제작이 가능하지만, iOS에서는 Apple의 앱 검증과정을 통과하는 것이 쉽지 않기 때문에 대부분의 악성앱 제작자들은 제3의 앱마켓을 통한 유통과 사이드로딩이 가능한 안드로이드 OS를 타겟으로 악성앱을 제작하고 있다. 만약 Apple이 사이드 로딩을 허용할 경우에는, iOS를 타겟으로 하는 악성앱의 수가 폭발적으로 증가할것으로 예상되며 iPhone의 전반적인 보안, 개인정보보호 수준이 약화될 수 있다.

Ⅲ. 제3의 앱마켓 (Third-party App Store)이란?

Google은 Google Play Store를, Apple은 App Store를 공식적인 앱마켓으로 운영하고 있다. Google은 Google Play Store 외에 다른 앱 마켓(즉 제3의 앱마켓)에서 앱의 다운로드 및 설치를 허용하고 있다. 반면에 Apple은 App Store 외에 제3의 앱마켓에서 앱의 다운로드 및 설치를 허용하지 않고 있다. 일반적으로 앱 마켓에 앱을 등록하는 경우에는 앱 마켓 자체적인 심사 프로세스가 존재한다. 경우에 따라서는 간소화된 심사절차를 갖고 있거나 심사절차 자체가 없는 앱 마켓도 존재한다. 따라서, 개발자 입장에서 공식 앱 마켓의 심사기준을 만족시키기 어려운 경우에는 제3의 앱마켓에 앱을 등록하는 경우도 있을 수 있다.

Google은 제3의 앱마켓을 허용하는 정책을 유지하고 있기 때문에, Google Play Store 외에도 다양한 앱마켓들이 존재한다. 하지만, Apple은 제3의 앱마켓을 엄격하게 규제하는 정책을 유지하고 있다. 따라서 기술적으로 Apple iOS를 위한 제3의 앱마켓은 존재할 수 없으며, 존재한다 하더라도 정상적으로 아이폰에 iOS 앱을 설치할 수 없다.

Ⅳ. 사이드로딩이란?

스마트폰에서 사이드로딩 (Sideloading)이란 공식적인 앱 마켓을 통하지 않고 앱을 설치하는 것을 말한다. 안드로이드 OS용 앱의 경우, 공식적인 앱 마켓인 Google Play Store가 아닌 제3의 앱마켓에서 다운로드 받은 APK 파일[1]을 안드로이드 스마트폰에 설치하는 것을 사이드로딩이라 말한다. 안드로이드에서 제3의 앱마켓을 통하여 APK 파일을 다운로드 받아 설치하는 경우, "Unknown Sources"로 부터 다운로드 받은 앱 설치에 대한 환경설정을 스마트폰 사용자가 변경해야 한다. iOS용 앱의 경우, 공식적인 앱 마켓인 App Store가 아닌 제3의 앱마켓에서 다운로드 받은 IPA 파일을 아이폰에 설치하는 것을 사이드로딩이라 말한다. Apple은 사이드로딩을 엄격하게 제한하고 있다.

Ⅴ. 제3의 앱마켓 및 사이드로딩의 문제점

5.1. 제3의 앱마켓의 관리부실

현재 악성코드를 포함하여 보안 및 개인정보 보호에 위협을 초래하는 많은 수의 앱들이 제3의 앱마켓을 통해 유통되고 있다. 이는 제3의 앱마켓이 악성코드가 포함된 앱의 유통을 허용하고 있으며, 사용자의 프라이버시를 침해하거나, 아동을 대상으로한 불법 또는 유해 컨텐츠가 포함된 앱들을 사전에 막지 못함을 보여준다. 결과적으로, 제3의 앱마켓의 관리부실은 사용자로 하여금 설치된 앱의 안전성을 스스로 판단해야하는 상황을 초래하고 있다. 최근 4년간 안드로이드 환경에서 악성코드에 감염된 기기가 아이폰에 비해 최소 15배에서 최대 47배 많은 것으로 조사된 결과는 사이드로딩을 공식적으로 허용하는 안드로이드 생태계에서 제3의 앱마켓의 관리가 부실한 현재의 상황을 뒷받침 한다 [19, 22].

하지만 Apple의 App Store 경우, 앞서 언급한 업격한 앱 심사 절차를 통해 악성앱이 유통되는것을 사전에 방지할 수 있다. 또한, 악의적인 사용자가 앱 심사 절차를 우회하여 App Store에 악성앱을 업로드 하더라도 Apple은 해당 앱을 삭제하는 조치를 통해 다른 사용자들의 피해를 최소화 할 수 있다. 만약 제3의 앱마켓이 허용될 경우, 공격자(또는 범죄조직)는 App Store가 아닌 제3의 앱마켓으로 이동하여 지속적인 악성행위를 할 수 있다.

5.2. 사용자의 알 권리 침해

Apple의 App Store와 달리 제3의 앱마켓은 앱 제

1) 안드로이드 OS와 iOS는 앱 설치 파일의 파일 포맷이 다르게 구성되어 있는데, 안드로이드 OS의 경우에는 APK 파일 포맷으로 Apple의 경우에는 IPA 파일 포맷으로 구성되어 있다.

작자로 하여금 앱에 대한 상세 정보를 제공하도록 강제하지 않고 있다. 이로 인해 사용자가 앱을 설치하기 전에 앱의 기능 및 동작에 대한 충분한 정보를 제공받지 못할 가능성이 있다. 다음은 사이드로딩이 허용될 경우 사용자의 알 권리가 침해될 수 있는 주요 항목들이다.

(1) 접근권한: Apple의 앱 심사 절차는 앱이 동작하는데 필요하지 않은 접근권한 또는 데이터에 대한 접근 요청을 요구하는지 심사한다. 또한, 사용자에게 접근권한을 요청할 때 오해의 소지가 있거나 잘못된 주장을 하지 않는지 확인한다. 예를 들어, 날씨 앱이 마이크 또는 건강 정보에 대한 접근을 요청한다면 이는 앱 심사 과정에서 반려사유에 해당한다. 사용자는 사이드로딩이 허용되면 이러한 권한관리를 보장받지 못한다.

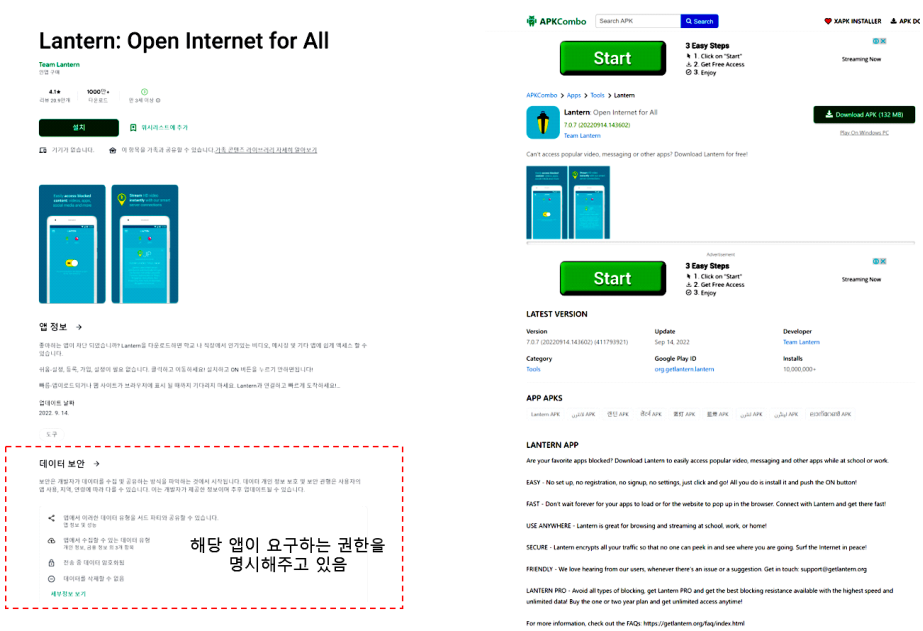
(2) 신뢰성 있는 정보: Apple의 앱 심사를 위해 앱 개발자는 앱과 해당 기능에 대한 설명, 앱 스크린샷, 어떤 종류의 데이터를 수집하는지 여부를 설명하는 개인정보보호 정보를 제출해야 한다. 이를 통해 사용자는 앱 다운로드 여부를 결정할 때 앱의 기능 및 동작을 예상할 수 있으며 신뢰할 수 있는 개발자를 사칭하는 악의적인 행위자로부터 보호 받을 수 있다. 만약 사이드로딩이 허용되면 사용자는 제3의 앱마켓에서 다운로드한 앱이 공식 앱인지 여부를 확인할 수 없으며 앱의 개인정보 보호 정책에 대한 정보를 신뢰할 수 없다.

(3) 프라이버시 보호: App Store의 모든 앱은 앱 추적 투명성 (App Tracking Transparency) 기능을 통해 타사 앱 또는 웹사이트에서 사용자를 추적하기 전에 사용자의 허가를 받아야 한다. 하지만 사이드로딩을 허용하면 개발자는 앱 추적 금지 기능을 활성화 하지 않도록 앱을 설계할 수 있다. 이를 통해 앱은 다른 기기 또는 사용자 데이터에 액세스하여 앱 추적 투명성 기능을 비효율적으로 만들 수 있다.

실제로, [그림 1]와 같이 현재 사이드로딩을 허용하고 있는 Android OS의 경우에 제3의 앱마켓에서 앱을 다운로드 받기위한 페이지에서는 요구되는 권한에 대하여 어떠한 명시도 하고 있지 않다.

5.3. 사용자의 범죄환경 노출

출처불명의 실행파일을 다운로드하여 피해자의 스마트폰에 설치되는 과정은 사이드로딩에 해당한다. 보이스피싱, 몸캠피싱, 스미싱 등 사이버 범죄수법은 계



<Google Play> <3rd Party Store, APKCombo>

〔그림 1〕 요구하고 있는 권한의 명시 여부 (좌 : Google Play, 우 : 제3의 앱마켓)

속해서 교묘해지고 있으며, 범죄수법의 진화에는 스마트폰에 설치되는 악성앱이 결정적인 역할을 하고 있다. 이러한 사이버 범죄수법과 이로인한 피해사례는 6장에서 상세히 기술한다. 만약 iOS 환경에서 사이드로딩을 허용할 경우, 사기범들의 범행대상이 안드로이드 사용자 뿐만 아니라, iOS 사용자로 확대되어 사이버 범죄피해가 급격히 증가할 것으로 예상된다.

Ⅵ. 제3의 앱마켓과 사이드로딩 피해 사례

본 장에서는 먼저 금융보안원에서 발간한 `금융 모바일 악성코드의 현재와 미래' 보고서를 기반으로 국내에서 발생한 모바일 악성코드의 흐름 및 유포방식의 변화에 대해 살펴본다. 이를 통해 악성코드의 대규모 유포과정에서 사이드로딩이 직접적인 원인으로 작용함을 설명한다. 다음으로 제3의 앱마켓 및 사이드로딩을 공식적으로 허용하는 안드로이드 환경에서 발생한 실제 피해 사례에 대해 기술한다.

6.1. 모바일 악성코드의 흐름 및 유포방식의 진화

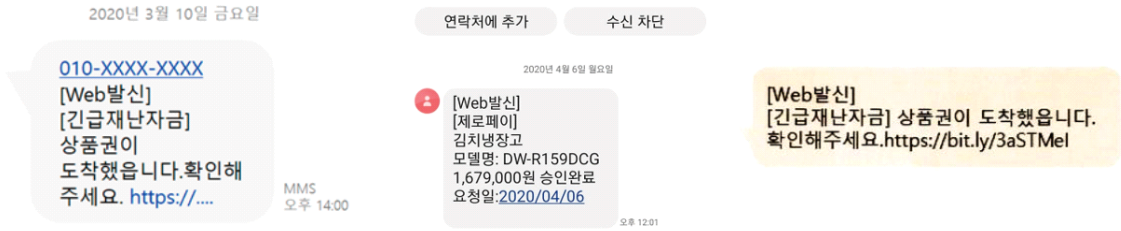
2010년 스마트폰 보급이 시작된 후 2012-2014년을 지나면서 국내 모바일 악성코드가 폭발적으로 증가하였다. 초기에는 문자 메시지, 메신저, 피싱 페이지 등이 주로 사용되었는데 최근에는 기존의 유포 방법을 사회적인 이슈와 결합하여 활용하는 한편, 광고 서버, 개발 관련 인증서 탈취, 공급망 및 개발사 등을 해킹하여 이 인프라를 통해 악성 앱을 유포하는 등 방법이 점차 진화하고 있다. 과거부터 현재까지 지속해서 발생하고 있는 모바일 위협 중에서 악성 앱 감염에 근본적인 원인은 대부분 **(1) 신뢰할 수 없는 출처에서의 다운로드**, **(2) 정상 앱 사칭 등이 있다**. iOS의 경우, 앱 설치를 위해서는 공식 App Store에서 설치파일을 다운받거나 테스트앱 형태로만 설치가 가능하기 때문에 이와 같은 악성앱 유포로 부터 안전하다.

(1) 신뢰할 수 없는 출처에서의 다운로드: 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 악성코드 유포의 원인으로 꼽힌다.

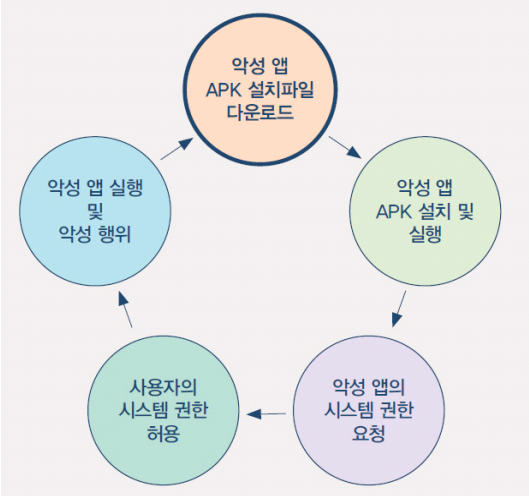
(2) 정상 앱 사칭: 정상 앱을 사칭하기 위한 방법의 하나로 정치 및 특정 이슈를 이용하기도 하는데 2015년 중동 호흡기증후군(MERS), 2020년 코로나19 등 사회적인 이슈와 혼란이 집중되었을 때 사용자는 관련된 이슈를 검색하는 과정에서 유포된 악성 앱에 감염되기도 한다. 서울특별시 코로나19 지원금 관련 스미싱 보도자료에 의하면 긴급재난지원금 지급이 본격화된 2020년 4월 중순 이후 스미싱 문자가 증가하고 있고, 출처가 불분명한 링크는 접속하지 않도록 안내하고 있다(그림 2)[29].

6.2. 모바일 악성코드 특성

모바일 악성코드에 의한 공격을 성공시키기 위해서는 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(그림 3). 악성 앱이 실행되려면 악성 행위에 필요한 접근성 서비스(Accessibility Service), 배터리 최적화 등의 권한들을 사용자가 허용해야 하며



〔그림 2〕 악성 앱 설치파일 URL이 포함된 단축 URL을 문자 메시지로 유포 (출처 : 금융보안원)



〔그림 3〕 악성 앱이 설치 및 실행되는 과정(1차 감염 이후에도 반복 감염) (출처 : 금융보안원)

악성 앱이 설치되었다고 해도 사용자가 권한 허용을 하지 않으면 개인정보에 접근하는 악성 행위가 실행될 수 없으므로 권한 허용 여부는 매우 중요하다.

6.2.1 악성코드 종류와 모바일에 미치는 피해

사이드로딩을 통해 발생한 보안 및 프라이버시 침해 사례는 매우 다양하며, 대표적으로 Adware, Ransomware, Spyware, Banking and credential-stealing trojans로 구분할 수 있다.

6.2.1.1 Adware

Adware는 사용자의 기기에 매우 많은 수의 팝업 또는 리디렉션 링크를 생성하여 기기의 성능을 떨어뜨리며 기기의 사용성(usability)를 저해한다. 대표적으로는 안드로이드 환경에 존재하는 HiddenAds [5], FakeAdsBlock [4], CopyCat [14] 등이 있다.

6.2.1.2 Ransomware

Ransomware는 디바이스에 저장된 데이터를 암호화 하여 사용자로 하여금 이를 복호화하는데 필요한 비밀키를 제공받는 대신 막대한 비용을 지불하도록 유도하는 사이버 공격 방법이다. 특히, 암호화폐의 발달로 인해 공격자들은 피해 사용자들로 부터 자금 추적이 어려운 암호화폐로 해당 비용을 지불하도록 유도하고 있다. 대표적인 ransomware는 CryCryptor [8], Fusob [12], MalLocker.B [3] 등이 있다.

6.2.1.3 Spyware

Spyware는 기기 사용자를 모니터링 하며, 문자 메시지, 사진, 비디오와 같은 민감 정보들을 탈취한다. Spyware는 개인 뿐만 아니라, 비즈니스 조직을 대상으로도 정보를 탈 취할 수 있다. 2020년 안드로이드 환경에서 발생한 멀웨어 공격중 1/3이 spyware를 사용하였다. 대표적인 spyware는 FluBot [11], FakeSpy [9], SpyNote [20], HelloSpy [13] 등이 있다.

6.2.1.4 Banking and credential-stealing trojan

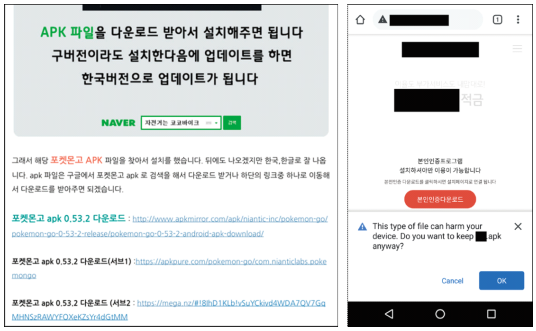
Banking and credential-stealing trojan은 대표적인 모바일 멀웨어의 타입이며, 기기에 접근하여 사용자의 금융정보를 탈취한다. 일부 악성 앱들의 경우 two-factor 인증을 우회하기도 한다 [17]. 대표적으로는 BlackRock [23], Banker.Br [18], TeaBot [21] 등이 있다.

6.3. 제3의 앱마켓으로 인한 피해사례

제3의 앱마켓은 적절한 앱 심사과정이 없기 때문에 많은 보안 취약점들에 노출될 수 있다. 만약 제3의 앱마켓 공식앱 또는 해당 서버가 취약점에 노출된다면, 해당 앱마켓에서 앱을 업로드한 제작자 뿐만 아니라, 유통되는 앱을 다운로드 받은 사용자들에게 막대한 피해가 발생할 수 있다. 실제로, Slash gear의 보고서 [6]에 따르면, 대표적인 제3의 안드로이드 앱마켓인 APKPure의 공식 앱이 악성 코드를 포함하고 있는 것으로 Kaspersky에 의해 밝혀졌다. Kaspersky는 해당 사실을 APKPure에 통보하였으며, 해당 취약점은 패치하여 3.17.19 버전을 배포하였다 [15]. 제3의 앱마켓의 적절한 앱 심사과정 부재로 인한 구체적인 사례로는 모바일 게임 앱인 포켓몬 GO와 넷플릭스 무료 시청을 가장한 플릭스온라인(FlixOnline) 앱의 경우가 있다.

6.3.1 포켓몬GO

증감현실 기반 게임인 포켓몬GO 앱은 2016년 미국, 호주, 뉴질래드에서 정식 출시되었다. 당시 국내 공식 앱마켓에 포켓몬GO 앱이 배포 되지 않은 시점에서 국내 이용자들은 비공식적인 제3의 앱마켓에서 포



〔그림 4〕 제3의 앱마켓에서 앱을 다운로드하는 예시 (포켓몬고) (출처 : 금융보안원)

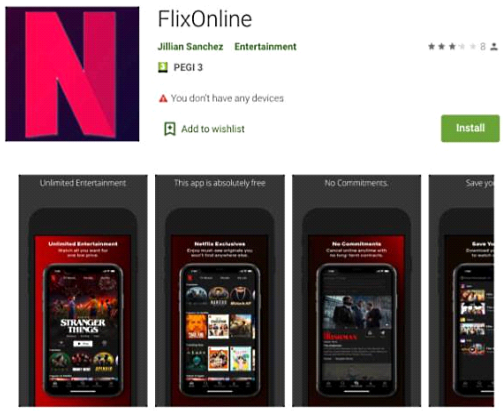
켓몬GO 앱을 다운로드 받아야 했다. 하지만 공식 출시 3일이 지나기도 전에 악성 코드[2]를 추가하여 리패키징한 앱들이 이미 제3의 앱마켓에서 발견되었다(그림 4) [16]. 모바일 시장조사 업체 와이즈앱에 따르면 당시 국내 공식마켓에 포켓몬GO 앱이 배포 되지 않은 시점에 이미 100만명 이상의 국내 사용자들이 제3의 앱마켓 등 공식 앱마켓을 통하지 않고 앱을 설치한것으로 추산되었다 [33].

6.3.2 플릭스온라인(FlixOnline)

코로나 팬데믹 기간동안 자가격리되는 인원들이 늘어남에 따라, 넷플릭스 서비스가 폭증하게 되었다. 이러한 현상을 악용하여, 2개월 동안 무료로 Netflix Premium 멤버쉽을 이용할 수 있다고 광고하는 FlixOnline이라는 악성앱이 등장하였다. 그러나 FlixOnline은 사용자의 스마트폰에서 과도한 Permission을 요구하여 메신저 앱들의 대화내용을 도청하거나 신용카드번호와 같은 주요 정보를 탈취한다 (그림 5)[7].

글로벌 사이버 보안 전문회사인 체크포인트리서치(CPR)의 분석에 따르면 플릭스온라인은 "넷플릭스 프리미엄 2개월 무료이용 https://bit[.]ly/3bDmzUw"이란 공지를 올려 사용자가 앱을 설치하도록 유도했다. 설치된 플릭스온라인은 사용자에게 개인 정보를 포함해 모든 알림을 읽을 수 있도록 허용할 수 있는 권한을

2) 추가된 악성 코드는 DroidJack (글로벌 사이버 보안 회사인 Trend Micro사는 AndroidOS SANRAT.A라고 밝힘)이라 불리는 원격제어 트로이 목마 바이러스로 밝혀졌으며, 설치된 스마트폰의 완전한 제어권을 획득하여 모든 기능을 수행할 수 있다.



〔그림 5〕 FlixOnline 악성앱 다운로드

요청하고 사용자가 동의를 누르면 플릭스온라인은 메신저인 왓츠앱(WhatsApp) 알림이나 내용을 모니터링 할 수 있게된다. 예로 왓츠앱에 메시지가 오면 자동응답 기능을 통해 상대방에게 피해자가 받은 '넷플릭스 프리미엄 2개월 무료이용 https://bit[.]ly/3bDmzUw' 메시지를 보내게 된다. 상대방이 링크를 클릭하면 역시 악성코드가 상대방의 스마트폰을 장악하게 된다. FlixOnline 앱은 주로 제3의 앱마켓을 중심으로 배포되었다. 게다가, 일부 제3의 앱마켓에서는 아직까지 FlixOnline을 여전히 다운로드 받을 수 있다 [10].

6.4. 사이드로딩 허용으로 인한 피해사례

사이드로딩을 통해 발생한 사이버 범죄 피해사례는 매우 다양하며, 대표적으로 보이스피싱, 몸캠피싱, 스미싱 등이 있다.

6.4.1 보이스피싱

국내에서 심각한 사회문제로 부각되고 있는 보이스피싱은 매년 수천억원의 피해를 입히고 있다. 경찰청 통계에 따르면 보이스피싱 범죄는 2019년 37,667건, 2020년 31,681건, 2021년 30,982건으로 코로나 발생으로 잠시 주춤하고 있다. 하지만 피해액 규모는 2019년 6,398억, 2020년 7,000억, 2021년 7,744억으로 증가하고 있다 (그림 6, 그림 7) [25]. 보이스피싱 수법은 정보통신의 발달로 그 수법이 날로 진화하고 있으며 최근에는 사이드로딩의 헛점을 이용해 전화 통화로 피해자의 스마트폰에 악성앱이 설치되도록 유도하여 보

1-1. 최근 5년간 보이스피싱 발생현황(기망수법별)

구분	합 계		기관사칭형		대출사기형	
	발생건수	피해(억원)	발생건수	피해(억원)	발생건수	피해(억원)
2017년	24,259	2,470	5,685	967	18,574	1,503
2018년	34,132	4,040	6,221	1,430	27,911	2,610
2019년	37,667	6,398	7,219	2,506	30,448	3,892
2020년	31,681	7,000	7,844	2,144	23,837	4,856
2021년	30,982	7,744	7,017	1,741	23,965	6,003

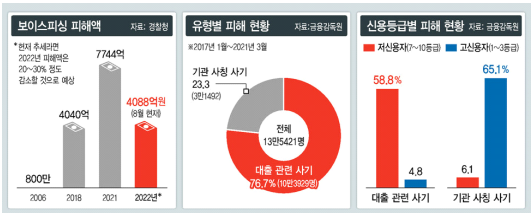
자료 : 경찰청

1-2. 최근 5년간 보이스피싱 발생현황(연령별)

구분	2017년		2018년		2019년		2020년		2021년	
	명	%	명	%	명	%	명	%	명	%
20대	5,273	21.7	4,480	13.1	3,855	10.2	5,323	16.8	5,459	17.6
30대	4,887	20.1	6,483	19.0	6,041	16.0	4,406	13.9	3,299	10.6
40대	**6,473**	**26.7**	**9,842**	**28.8**	**10,264**	**27.3**	7,704	24.3	6,755	21.8
50대	5,412	22.3	9,313	27.3	11,825	31.4	**9,217**	**29.1**	**9,564**	**30.9**
60대	1,807	7.4	3,389	9.9	4,617	12.3	4,188	13.2	4,778	15.4
70대	407	1.7	625	1.8	1,065	2.8	843	2.7	1,127	3.6
합계	24,259	100.0	34,132	100.0	37,667	100.0	31,681	100.0	30,982	100.0

자료 : 경찰청

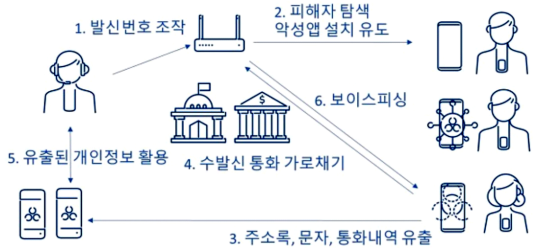
〔그림 6〕 최근 5년간 국내 보이스피싱 통계 현황 (출처: 경찰청)



〔그림 7〕 국내 보이스피싱 피해현황 (출처: 경찰청, 금융감독원)

이스피싱의 성공률을 높이고 있다. 안랩의 통계에 따르면 2021년 1월부터 3월까지 안드로이드 기반의 스마트폰 백신인 V3 mobile을 통해 진단한 보이스피싱 악성앱은 20,720건이다 [2].

구체적으로, 사기범은 금융기관 또는 수사기관 등을 사칭하여 대출, 수사절차 진행 등을 위해 관련 앱을 설치해야 한다고 속인다. URL, 도메인, IP 주소 등을 알려주면서 관련 앱을 다운로드 받으라고 하거나, 카카오톡과 같은 모바일 메신저를 이용해 앱 스토어를 거치지 않고 앱을 깔 수 있는 앱 설치파일을 전송한다. 이렇게 앱을 내려 받는 경우 "보낸 파일이 안전하지 않을 수 있습니다"라는 창이 뜨고 "출처를 알 수 없는 앱 설치"라는 경고도 올라오지만 대부분 무시하고 진행하게 된다. 심지어 원격제어 앱을 설치하도록 한 뒤 사기범이 직접 피해자 스마트폰에 악성앱을 설치하는 경우도 있다. 설치된 악성앱은 피해자의 스마트폰에서 정보를 수집하거나 문자를 감시하고, 수신과 발신 통화를 가로채는 것을 가능하게 한다. 예를 들어, 피해자



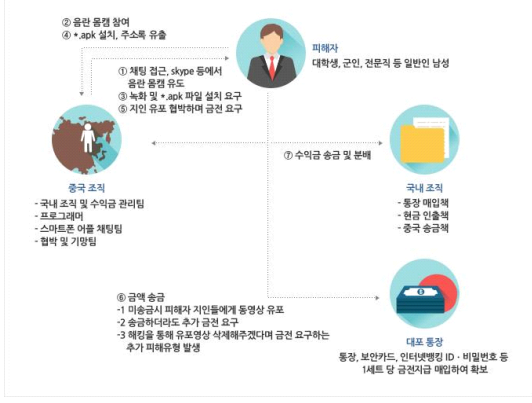
〔그림 8〕 보이스피싱 악성앱 공격 구조도 (출처 : 안랩)

가 보이스피싱을 의심하여 경찰, 금감원, 금융기관 등에 확인전화를 하더라도, 설치되어 있는 악성앱으로 인하여 다시 보이스피싱 사기범에게 연결 된다 (그림 8] [28, 30, 31].

6.4.2 몸캠피싱

스마트폰 사용자 모르게 악성앱을 설치하는 사기범죄의 또 다른 예로는 몸캠피싱이 있다. 몸캠피싱은 몸캠(body cam)과 피싱(fishing)의 합성어로 랜덤채팅이나 sns, 온라인 커뮤니티 등에서 사기 조직원들이 범행 대상자에게 접근하여 몸캠 (영상통화로 음란한 행위를 하는 것)을 빌미로 영상을 불법 촬영한 후 지인들에게 유포하겠다고 협박하며 금품을 갈취하는 사기를 의미한다 (그림 9)[27]. 이러한 몸캠피싱은 2년 전 N번방 사건의 시발점이 되었으며 지난해 만들어진 `N번방 방지법'도 올해 발생한 제2의 N번방사건을 방지하지 못했다.

구체적으로, 몸캠피싱은 타인의 사진을 도용한 범죄자가 랜덤 채팅 또는 모바일 메신저 등을 통해 피해자에게 접근한다. 접속에 성공하면 협박에 필요한 피해



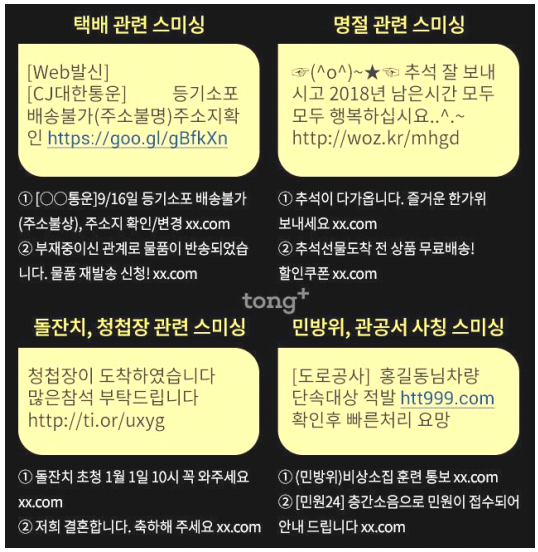
〔그림 9〕 몸캠피싱 범죄 흐름 (출처 : 경찰청 사이버수사국)

자의 음란 동영상을 확보하기 위해 화상채팅이 가능한 skype 등으로 이동하여 채팅할 것을 피해자에게 제의한다. 그리고 화상채팅에 필요한 앱이라거나, 상대방의 목소리가 들리지 않아 음성지원용으로 필요하다며 별도의 앱 (즉 APK 파일 포맷)을 설치할 것을 피해자에게 요구한다. (앱을 다운로드 받을 수 있는 URL을 전달한다.) 이러한 과정으로 해당 앱이 설치되면 주소록, 앨범 사진등과 같이 사용자의 개인정보가 범죄자의 서버로 옮겨지고 협박에 사용된다. 공식 앱 마켓을 이용하지 않고 다운로드 URL을 이용하여 앱을 설치하는 것은 사이드로딩을 의미하며, 이 처럼 사이로딩이 계속 가능한 환경에서는 제3, 제4의 N번방이 발생할 수도 있다. 경찰청 통계에 따르면 몸캠피싱 범죄는 2019년 1,824건, 2020년 2,583건, 2021년 3,026건으로 해마다 20% 이상 증가하고 있다. 몸캠피싱으로 인한 피해액 규모도 2019년 55억, 2020년 72억, 2021년 119억으로 해마다 40% 이상 증가하고 있다 [24, 26, 32].

6.4.3 스미싱

스미싱(smishing)이란 문자메시지(SMS)와 피싱(Phising)의 합성어이다. 사기범은 클라우드 스토리지, 서버 등에 앱 설치파일을 업로드 하고, 단문 메시지 입력 제한(80byte, 한글 40글자)과 설치파일 형태를 숨기기 위하여 URL을 단축 URL로 변환한다. 사용자의 접속을 유도하기 위하여 청첩장, 재난지원금 수령, 택배 안내, 경찰청 출석, 쇼핑몰 결제내역 등의 내용으로 발송하는 전통적인 유포 방식을 사용한다. 특히 코로나 상황을 이용하여 택배 배송이나 연말정산 환급금 결과 조회, 코로나19 관련 지원금 안내 문자 등 다양하다 (그림 10). 경찰청에 따르면 스미싱 발생건수는 2019년 207건으로 주춤하다가, 2020년 822건으로 늘더니 2021년 1,336건으로 2년 전보다 약 6배 이상 증가하고 있다. 스미싱으로 인한 피해액 규모도 2019년 4.1억, 2020년 11억원, 2021년 49억으로 2년 전과 비교해 10배 이상 증가했다 [26].

구체적인 방식은 스미싱에 사용된 메시지 내용에 따라 조금씩 상이하다. 최근 급증한 건강검진 스미싱의 경우 "[건강보험공단] 종합건강검진 보고서 발송완료. 내용확인[xxxx.xxxx[.]xyz]"와 같은 문자를 사용한다. 피해자가 건강검진 관련 문서를 받은 것으로 오인하여 링크를 클릭하게 되고 건강검진 문서가 아닌 악



〔그림 10〕 스미싱 주요 사례 (출처 : tong+)

성 앱을 다운로드받게 된다. 택배 스미싱의 경우 "[대한통운] 송장번호 (5901******90)주소불일치로 물품보관중입니다. 아래문의 hxxps://han[.]gl/xxxxx"와 같은 문자를 사용한다. 피해자는 실제 택배로 오인하여 링크를 클릭하면 역시 악성앱을 다운로드받게 된다. 보이스피싱을 유도하는 스미싱의 경우는 악성앱을 유포하는 url대신 공격자의 전화번호를 포함하고 있다. 피해자는 "[국제발신] 해외직구 승인번호 (89**) 2,064,000원 결제완료 [EN JAPAN]쇼핑 문의:070-xxxx-xxxx"와 같은 문자를 받고 사기범에게 전화를 하면 사기법은 악성앱 설치를 통한 보이스피싱 단계로 넘어간다. 수사관 사칭 스미싱은 경찰, 검찰 등의 수사기관을 사칭하여 "[Web발신] [교통민원24 (이파인)]차량 법규 위반 벌점 처분 통지서 발송 완료 hxxps://bit[.]ly/xxxxxxx"와 같은 메시지를 사용한다.

Ⅶ. 결 론

본고에서는 제3의 앱마켓과 사이드로딩이 허용되는 상황에서 발생할 수 있는 보안문제와 이로 인한 피해사례를 기술하였다. 대표적인 스마트폰 OS인 안드로이드의 경우에는 현재 제3의 앱마켓과 사이드로딩을 허용하고 있지만, Apple의 iOS의 경우에는 철저히 금지하고 있다. 이로 인해, **제3의 앱마켓과 사이드로딩으로 인한 보안문제와 피해사례들은 현재 안드로이드 스마트폰에서만 발생하고 있는 상황이다**. Apple

은 제3의 앱마켓 및 사이드로딩을 금지하는 정책을 통해 안드로이드 환경에 비해 높은 보안성과 안전한 앱 스토어 생태계를 구축하고 있다. 만약 Apple이 사이드로딩을 허용하면 다음과 보안 문제가 발생할 수 있을 것이라 예상할 수 있다.

(1) iOS 악성코드 증가: iOS와 안드로이드 OS 모두 악성코드로 부터 피해를 받고 있다. 일반적으로 스마트폰용 악성코드는 정상적인 앱으로 위장하여 제3의 앱마켓에서 다운로드 및 설치할 수 있도록 배포되거나 실행 파일을 직접 설치하도록 하는 사이드로딩 방식으로 배포된다. 하지만, Open source 정책을 유지하고 있는 안드로이드 OS임에도 불구하고 대부분의 스마트폰용 악성코드들은 안드로이드 OS를 타겟으로 하고 있다. 이는 사이드로딩과 제3의 앱마켓을 허용하고 있는 안드로이드 OS에서 악성코드 배포가 매우 용이하기 때문이다. 스텟카운터[3]의 통계에 의하면 애플의 국내 시장점유율은 올해 6월 27.28%, 7월 29.45%, 8월 32.97%, 9월 34.1%로 급격히 상승하고 있다 [1]. 결과적으로 Apple의 iOS에서 제3의 앱마켓과 사이드로딩이 허용 된다면, 현재 배포되고 있는 스마트폰용 악성코드의 수가 폭발적으로 증가할 것으로 예상된다.

(2) 범죄 증가: 범죄 피해자에게 악성앱 설치를 유도하는 보이스피싱, 몸캠피싱 및 스미싱의 경우, 사이드로딩을 허용하고 있는 안드로이드 OS 사용자들만이 범죄의 타겟이 되고 있다. 해당 범죄에 활용되는 악성앱은 기술적인 측면에서는 안드로이드 OS와 iOS 여부와 무관하게 제작이 가능하지만, iOS에서는 사이드로딩 방식으로 앱을 설치하는 것이 허용되지 않기 때문에 해당 악성앱이 설치되지 않는다. 만약 Apple의 iOS에서도 사이드로딩 방식으로 앱을 설치하는 것이 허용된다면, 6장에서 기술한 범죄의 타겟이 급격히 늘어나게 된다. 특히 이러한 범죄들은 스마트폰이 생활의 필수품이 됨에 따라 최근 몇년간 전국민, 특히 사회적으로 보호받아야 할 노인층과 청소년 층을 대상으로 심각한 사회문제를 야기시키는 사이버 범죄의 주류를 이루고 있다. 지난해 말 "N번방 방지법"의 제정 이후에도 몸캠피싱 악성 앱의 사이드로딩으로 인한 제2의 N번방 사건이 일어났다는 사실은 사이버 범죄를 방지하기 위해서는 법 제정이나 범죄 검거 등의 사후적 조치와 함께 사이드로딩 방지 등의 기술적 조치가 반드시 뒷바침되어야 한다.

(3) 패치 및 최신화 어려움: 사이드로딩 방식이 허용되고 제3의 앱마켓이 가능해지면, iOS 사용자들은 여러 마켓에서 앱을 다운로드하고 이를 설치할 수 있게 된다. 하지만, 다양한 마켓에서 앱을 다운로드 받게 되면, 해당 앱에 대한 최신 버전 유지가 어려워진다는 문제점이 존재한다. 앱에 대한 패치 및 최신버전 유지 관점에서는 단일화된 앱 마켓 환경이 매우 유리하다. 게다가, Apple의 App Store와 같이 앱 등록 전 심사단계를 거쳐 보안취약점 존재 유무나 사용자의 개인정보 침해 여부를 앱 배포이전에 식별할 수 있게 된다. 앱 배포 이후, 특정 앱에서 심각한 보안취약점이 발견되었다고 하면 Apple과 같이 단일 앱마켓 환경에서는 이에 대한 패치를 즉각적으로 진행할 수 있으며 패치가 어려운 경우에는 앱을 즉각적으로 삭제하는 것 까지 가능하다. 하지만, 다양한 앱마켓이 존재하는 안드로이드 경우에는 해당 보안취약점에 대하여 모든 앱마켓이 각각 대응해야 하기 때문에 더 많은 시간이 소요되고 이는 해당 앱이 설치되어 있는 스마트폰의 해킹 가능성을 높이게 된다. 6.3.2에서 기술한 바와 같이, 플릭스온라인 악성앱의 경우 Google의 공식 앱마켓이 Play Store에서는 삭제되었지만 18개월이 지난 현재에도 제3의 앱마켓에서는 여전히 다운로드 받을 수 있다. 따라서, Apple의 iOS에서 사이드로딩과 제3의 앱마켓이 허용 된다면 앱 배포이후에 계속해서 발견되고 있는 보안취약점에 대하여 효과적으로 대응하기 어려워지게 되고, 스마트폰이 악의적인 해커에 노출될 가능성이 높아질 것이라 예상된다.

Apple은 제3의 앱마켓 및 사이드로딩을 금지하는 정책을 통해 안드로이드 환경에 비해 높은 보안성과 안전한 앱스토어 생태계를 구축하고 있다. 만약 Apple이 사이드로딩을 허용하면 iOS 생태계는 기존 안드로이드 환경이 가지고 있는 다양한 부작용들에 노출될 것으로 예상된다. 특히, 사이버 보안 관점에서는 제3의 앱마켓의 관리 부실로 인한 악성코드의 유통, 사용자의 알권리 침해, Apple 기기의 보안성 약화가 예상된다. 현재 Apple의 정책이 iOS 앱 생태계의 높은 보안성과 안전성을 유지시키고 있는 만큼 제3의 앱마켓 및 사이드로딩 허용에 대해 보다 신중한 접근이 필요하다.

3) 스탯카운터는 인터넷 트래픽을 기반으로 운영체제(OS)의 점유율을 측정하는 업체다.

참 고 문 헌

[1] 3명 중 1명은 아이폰. . .삼성 텃밭 한국서 반전 쓴 애플 배성수의 다다it선 | 한경닷컴. https://www.hankyung.com/it/article/202210032036i. (Accessed on 10/15/2022).

[2] [ahnlab]진화하는 보이스피싱, 악성앱이 사용자를 노린다 뉴스/이벤트 - (주)소프트정보서비스. https://softinfo.co.kr/article/%EB%89%B4%EC%8A%A4%EC%9D%B4%EB%B2%A4%ED%8A%B8/2/932/. (Accessed on 10/13/2022).

[3] Androidos/mallocker.b, software s0524 | mitre att &ckR. https://attack.mitre.org/softw are/S0524/. (Accessed on 08/06/2022).

[4] Android/trojan.fakeadsblock | malwarebytes labs | detections. https://blog.malwarebytes,com/detections/android-trojan-fakeadsblock/. (Accessed on 08/06/2022).

[5] Android/trojan.hiddenads | malwarebytes labs | detections. https://blog.malwarebytes.com/detections/android-trojan-hiddenads/. (Accessed on 08/06/2022).

[6] Apkpure app store app infected withmalware - slashgear. https://www.slashgear.com/apkpure-app-store-app-infected-with-malware-12667869. (Accessed on 08/06/2022).

[7] Autoreply attack! new android malware found in google play store spreads via malicious autoreplies to whatsapp messages - check point software. https://blog.checkpoint.com/2021/04/07/autoreply-attack-new-android-malware-found-in-google-play-store-spreads-via-malicious-auto-replies-to-whatsapp-messages/. (Accessed on 10/13/2022).

[8] Crycryptor ransomware - nhs digital. https://digital.nhs.uk/cyber-alerts/2020/cc-3523. (Accessed on 08/06/2022).

[9] Fakespy, software s0509 | mitre att&ckR. https://attack.mitre.org/software/S0509/.(Accessed on 08/06/2022).

[10] Flixonline download at apkcombo. https://apkcombo.com/ko/flixonline/com.fab.wflixonline/. (Accessed on 12/10/2022).

[11] Flubot - wikipedia. https://en.wikipedia.org/wiki/FluBot. (Accessed on 08/06/2022).

[12] Fusob - malware wiki. https://malwiki.org/index.php?title=Fusob. (Accessed on08/06/2022)

[13] Hellokitty, software s0617 | mitre att&ckR. https://attack.mitre.org/software/S0617/.(Accessed on 08/06/2022).

[14] How the copycat malware infected android devices around the world - check point software. https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world/. (Accessed on 08/06/2022).

[15] Malicious code in apkpure app | securelist. https://securelist.com/apkpure-android-app-store-infected/101845/. (Accessed on 08/06/2022).

[16] Malicious version of popular mobile game pokemon go app spotted - nouvelles de securite -trend micro fr. https://www.trendmicro.com/vinfo/fr/security/news/mobile-safety/malicious-version-of-popular-mobile-game-pokemon-go-app-spotted. (Accessedon 10/13/2022).

[17] Mobile banking trojans: what they are and how to protect against them | kaspersky official blog. https://www.kaspersky.com/blog/mobile-banking-trojans-faq/13243/. (Accessed on 08/06/2022).

[18] New android banking trojan targets spanish, portuguese speaking users. https://securityintelligence.com/posts/new-android-banking-trojan-targets-spanish-portuguese-speaking-users/. (Accessed on 08/06/2022).

[19] Nokia’s threat intelligence report 2019warns on the fast-growing and evolving threat of maliciouss oftware targeting internet of things (iot) devices | nokia. https://www.nokia.com/about-us/news/releases/2018/12/04/nokias-threat-intelligence-report-2019-warns-onthe-fast-growing-and-evolving-threat-of-malicious-software-targeting-internet-of-things-iot-devices/. (Accessed on 08/05/2022).

[20] Spynote rat, software s0305 | mitre att&ckR. https://attack.mitre.org/software/S0305/.(Accessed on 08/06/2022).

[21] Teabot trojan haunts google play store, again | thr

eatpost. https://threatpost.com/teabottrojan-haunts-google-play-store/178738/. (Accessed on 08/06/2022).
[22] Threat intelligence report 2020 | nokia. https://www.nokia.com/networks/portfolio/cyber-security/threat-intelligence-report-2020/. (Accessed on 08/05/2022).
[23] What is blackrock android malware and how can you avoid it? https://www.makeuseof.com/blackrock-android-malware/. (Accessed on 08/06/2022).
[24] 늘어나는'메신저피싱'피해,작년피해액1200억원기록. . .몸캠피싱"E메모리해킹도급증:네이트뉴스. https://news.nate.com/view/20220914n28400. (Accessed on 10/15/2022).
[25] 데이터 상세 | 공공데이터포털. https://www.data.go.kr/data/15063815/fileData.do.(Accessed on 10/15/2022).
[26] 데이터 상세 | 공공데이터포털. https://www.data.go.kr/data/15064566/fileData.do.(Accessed on 10/13/2022).
[27] 몸캠피싱. https://ko.wikipedia.org/wiki/%EB%AA%B8%EC%BA%A0%ED%94%BC%EC%8B%B1.(Accessed on 12/10/2022).
[28] 보이스피싱앱, 악성앱중가장활개쳐. https://www.donga.com/news/Economy/article/all/20220515/113410302/1. (Accessed on 09/26/2022).
[29] 서울시, '코로나19지원금도착'빙자한스미싱증가. . .주의당부>보도자료|서울특별시. https://www.seoul.go.kr/news/news_report.do#view/313101. (Accessed on 10/13/2022).
[30] 앱(악성코드) 설치 유도형 보이스피싱 주의 - 보도자료 | 브리핑룸 | 뉴스 | 대한민국 정책브리핑.https://www.korea.kr/news/pressReleaseView.do?newsId=156309308. (Accessed on 09/26/2022).
[31] '이앱'깔리면속수무책....보이스피싱앱깔아봤습니다-youtube. https://www.youtube.com/watch?v=SYwXOAcYCXg. (Accessed on 09/26/2022).
[32] "지난해'메신저피싱'피해액1200억원. . . '몸캠피싱'도급증세"-헤럴드경제. http://news.heraldcorp.com/view.php?ud=20220911000015. (Accessed on 10/15/2022).
[33] '포켓몬 고' 국내 우회 설치 100만 돌파 - 디지털타임스. http://www.dt.co.kr/contents.html?article_no=2016071702100031033001. (Accessed on 10/13/2022).

〈저 자 소 개〉

최 원 석 (Wonsuk Choi)
종신회원
2008년 2월 : 서울시립대학교 수학과 졸업
2013년 2월 : 고려대학교 정보보호대학원 정보보호학과 석사
2018년 8월 : 고려대학교 정보보호대학원 정보보호학과 박사
2018년 9월~2020년 2월 : 고려대학교 정보보호연구원 연구교수
2020년 3월~현재 : 한성대학교 IT융합공학부 조교수
<관심분야> 자동차 보안, IoT 보안, 암호학

이 동 훈 (Dong Hoon Lee)
종신회원
1983년 8월 : 고려대학교 경제학과 졸업
1987년 12월 : Oklahoma University 전산학과 석사 졸업
1992년 5월 : Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월~2001년 2월 : 고려대학교 전산학과 부교수
2001년 3월~현재 : 고려대학교 정보보호대학원 교수
<관심분야> 암호 프로토콜, 암호이론, USN이론, 키 교환, 익명성 연구, PET 기술