스마트폰 백신의 동향 및 분석

홍준표*, 김혜인*, 김승환**, 임헌정**, 정태명***
*성균관대학교 컴퓨터공학과, **성균관대학교 전자전기컴퓨터공학과
***성균관대학교 정보통신공학부
e-mail : jphong.bsb@gmail.com,
{shkim, hjlim99}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

A Survey on Current Anti Virus for Smartphone

Jun-Pyo Hong*, Hye-In Kim*
Seung-Hwan Kim**, Hun-Jung Lim**, Tai-Myoung Chung***
*Dept of Computer Engineering, Sung-Kyun-Kwan University
**Dept. of Electrical and Computer Engineering, Sungkyunkwan Univ.
***School of Information Communication Engineering, Sungkyunkwan Univ

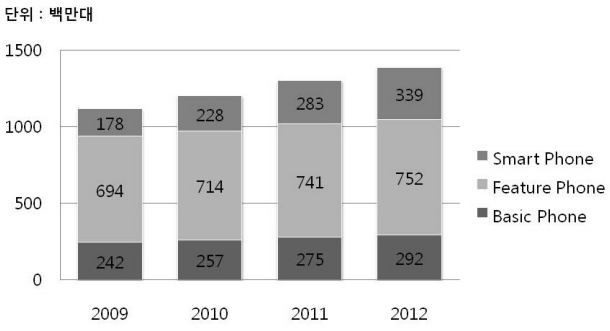
요 약

최근 스마트폰에 대한 관심이 고조되면서 스마트폰 시장 저변이 확대되고 있다. 이러한 환경 변화에 비례하여 기존에는 크게 대두되지 않았던 스마트폰 보안 위협 역시 증가하고 있는 실정이다. 이러한 보안 위협을 억제하기 위해 가장 손쉽게 취할 수 있는 대처방안이 스마트폰에 적합한 백신을 제작 및 배포하는 것이다. 이에 대해, 현재 스마트폰 보안 위협이 구체적으로 어떠하며, 출시되어 있는 백신들을 비교, 분석하여 향후 발전 방향을 모색해 보았다.

1. 서론

작년 국내에서 판매를 시작한 아이폰(iPhone)으로 일반 대중들에게 많은 관심을 얻고 있는 스마트폰은 일반 휴대전화의 통화 기능과 소형 컴퓨터의 이메일, 인터넷, e-book등의 기능을 이용할 수 있는 휴대용 단말기를 의미한다[1].

스마트폰의 성장세는 해가 지날수록 가파르게 성장하고 있다. 아래의 (그림 1)은 스마트폰의 점유율과 판매량의 추이를 나타내고 있다[2].



(그림 1) 스마트폰의 판매량과 시장 점유율 추이

(그림 1)과 같이 시장 점유율과 판매량이 급증하는 이유에는 <표 1>과 같이 휴대전화 서비스에 대한 인식이 기존 음성 서비스에서 모바일 데이터 서비스 중심으로 변화하는 것에 원인이 있다[3].

<표 1> 휴대전화 서비스에 대한 인식의 변화

기존 서비스	변화하는 서비스
데이터	애플리케이션
음성통화	데이터
	음성통화

주목해야 할 서비스의 변화는 모바일 단말기에 제공되는 애플리케이션 서비스이다. 기존의 공급자가 주도하여 서비스를 제공하는 폐쇄적인 구조를 탈피했다. 이러한 구조의 변화로 인하여 모바일 소프트웨어 플랫폼 개발이 일반 사용자들에게 공개 되었고, 사용자가 공급자의 역할을 할 수 있게 되었다. 이러한 결과로 인하여 모바일 서비스 상에서의 디지털 콘텐츠 거래량이 급증하게 되었다.

이와 같은 모바일 콘텐츠 시장 저변의 확대에 비례하여 이 분야에 관련된 보안 문제 역시 증가하고 있다. 통계에 따르면 2004년 15건에 그쳤던 스마트폰 악성코드 발견 건수가 5년 사이 612건으로 대략 40배 이상이 증가했으며[3], 최근에는 구글의 안드로이드(Android) 플랫폼에서 사용자의 개인 정보를 임의로 해커의 서버로 전송하는 악성 프로그램이 발견되기도 하였다[4]. 이와 같은 피해가 아직은 일반 데스크톱 컴퓨터에 유포되는 악성코드의 피해에 비하여 미비한 것이 사실이

나, 앞으로의 스마트폰 관련 모바일 콘텐츠 시장의 성장세를 감안할 때, 그 피해의 규모가 기하급수적으로 증가할 것이다.

보안상 직면한 문제에 대하여, 국·내외 다수의 보안 업체에서 스마트폰용 백신을 이미 출시하였거나 출시를 준비 중이다. 하지만 모바일 플랫폼 특성상 기존 PC의 백신에 적용되던 방법론을 그대로 모바일 백신에 적용할 수 없는 문제가 있다. 그리고 사용자 입장에서는, 어느 백신이 어떠한 기능을 가지고 있는지, 또 어느 백신이 자신의 플랫폼에 적절한지 아직 혼란스러운 상태이다.

언급한 문제에 관한 모바일 백신의 기본적인 성능 등을 비교하기 위하여 다음 2장에서는 스마트폰 상의 보안 위험 요소를 구체적으로 조사하였고, 3장에서는 국·내외 백신 4종을 선택하여 비교, 특성을 정리하였다. 마지막 4장에서는 3장에서 서술한 내용을 요약·정리하여 향후 모바일 백신의 방향을 예측해 보았다.

2. 스마트폰 상에서의 보안 위협 요소

스마트폰이 대중화되고 사용자가 확대되어감에 따라 기존의 보안 위협 요소가 적었던 모바일 환경 역시 보안 안전에 위협을 받고 있다. 이에 대해 모바일 환경에 대한 공격 유형에는 무엇이 있으며, 그에 대한 실제 사례를 살펴보고자 한다.

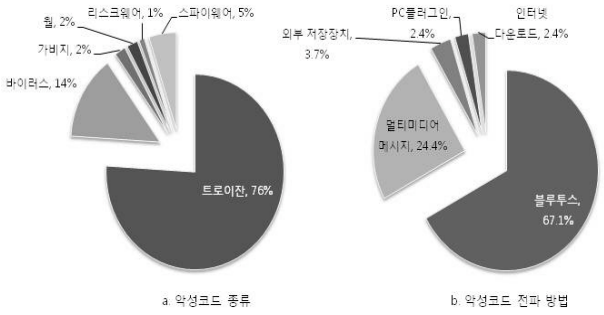
2.1. 모바일 환경에서의 공격 유형

모바일 환경에서 단말기에 가해질 수 있는 공격 유형은 아래 (그림 2)와 같다[5].

(그림 2) 모바일 공격 유형

위와 같이 다양한 공격 유형이 존재하지만, 그 중에서도 바이러스와 웜을 이용한 공격이 현재 대두되고 있다. 특히, 스마트폰의 애플리케이션 마켓이 활성화되면서 (그림 3)에서[6] 알 수 있듯이, 유용한 프로그램을 가장하여 사용자의 설치를 유도하는 트로이잔의 비율이 매우 높은 비율을 나타내고 있다.

또한 모바일 악성 코드는 유선 네트워크를 통한 전파보다는 사용자가 인지하기 힘든 무선 네트워크 환경을 통해 전파되는 성향이 강하다. 따라서 기존의 피해 양상과 비교해 봤을 때 피해의 규모가 훨씬 크고 범위 또한 광범위해질 것이라고 예상된다.



(그림 3) 악성코드의 종류와 전파경로

2.2. 모바일 악성 코드

모바일 악성코드는 사용자 단말기에 불법으로 설치되어 단말기의 기능을 마비시키거나, 배터리를 고갈시키거나, 개인정보의 유출 혹은 사용자에게 금전적인 손실을 끼치게 된다[7]. 모바일 악성코드에 의한 보고된 피해사례는 다음과 같다.

- 2004년 Mosquito라는 악성코드는 P2P 네트워크를 통하여 사용자 단말기에 저장되고 사용자가 알지 못하게 SMS를 발송하여 금전적인 손실을 끼침
- Skulls는 단말기의 시스템 애플리케이션에 침투, 사용자가 단말기를 사용하지 못하게 피해를 끼침.
- CommWarrior는 MMS를 통해 전파되는 최초의 모바일 웜으로 감염된 단말기의 주소록에 있는 모든 연락처에 웜의 복사본을 첨가한 MMS를 발송[8].

실제로 국내에서는 2009년 당시 스마트폰 가입자 160만명 중 약 150여명(0.01%)이 윈도모바일 운영체제를 탑재한 스마트폰 대상 모바일 악성코드(WinCE/Tredial)에 감염된 사례가 있다[9].

또한 최근에 애플의 앱스토어나 구글의 안드로이드 마켓을 통해 정상적인 애플리케이션으로 위장한 악성코드의 피해사례가 발생하고 있다.

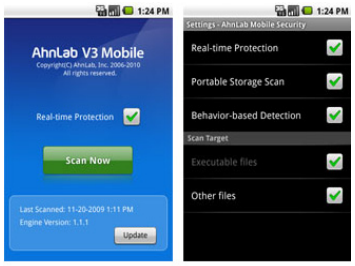
3. 모바일 백신의 동향 및 기능 분석

현재 스마트폰용 백신을 개발하였거나 개발 중인 회사는 국내의 안철수 연구소, 하우리, 잉카 인터넷, 국외의 카스퍼스키랩(Kaspersky Lab), 맥아피(McAfee), 시만텍(Symantec) 등이 있다. 실제로 기존 PC 백신 시장에서 꾸준히 제품을 출시하던 회사들은 대부분 스마트폰용 백신을 출시한 것으로 나타났다. 이러한 백신들 중에서 국내 제품 2개, 국외 제품 2개를 선택하여 제품들의 특징을 조사하였다. 또한 제품의 특징을 조사하는데 있어 주로 보안업체의 공식 홈페이지의 자료를 인

용하였다.

3.1. 안철수 연구소 - AhnLab V3 Mobile

V3 mobile은 안드로이드, 윈도우즈 모바일, 심비안 플랫폼을 지원한다. 각 플랫폼에 적절한 방식을 적용한 V3 mobile의 큰 특징으로는 안드로이드 플랫폼에서 행위기반[1]으로 위험 애플리케이션을 차단하는 것이다. Windows Mobile에서는 순수 C코드로 제작하여 작은 프로그램사이즈를 구현하였다. 플랫폼 공통적인 기능으로는 파일, 프로세스, 악성코드의 실시간검색, SD카드 영역 및 내장메모리를 검사한다. 유무선상에서 예약 및 수동업데이트를 제공한다. 사용자 편의를 위해 진단 및 치료의 옵션을 설정할 수 있고, 잘못 삭제된 파일을 복원할 수 있다. 진단된 악성코드에 대한 상세정보를 제공하고 있으며, 예약검사 기능이 있다.



(그림 4) V3 Mobile 화면

3.2. 하우리 - Virobot Mobile

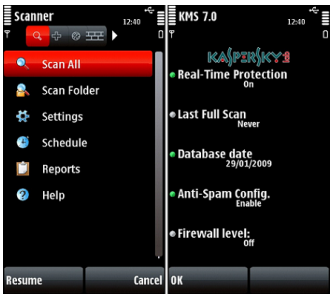
바이로봇 모마일은 안드로이드 플랫폼에서 지원된다. 3.1.의 V3 Mobile과 마찬가지로 행위기반 검색으로 위험 애플리케이션을 차단, 취약환경을 점검한다. 악성코드 진단 및 최신 패턴 업데이트가 실시간으로 이루어진다. 블랙리스트기반으로 전화와 SMS를 차단한다. Wi-Fi의 AP접근을 제어하며, 3G 망의 데이터 통신량을 감시 및 차단한다. 폰을 분실할 경우, 원격 잠금 및 삭제가 가능하고, SIM 카드 변경 시 잠금 기능이 설정된다. 파일 및 디렉터리 단위의 파일암호화를 지원하고, 프로그램 실행 시 인증기능을 넣을 수 있다.

(그림 5) Virobot mobile 화면

1) 특정 애플리케이션이 행하는 일련의 동작들(주소록 접근, SMS전송 등)을 점검, 애플리케이션의 목적과 부합하지 않을 경우 악성 코드로 간주 하는 검색 기법.

1.1. 카스퍼스키 -Kaspersky Mobile Security9

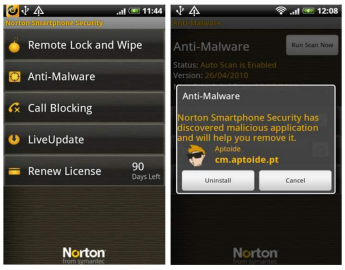
카스퍼스키사의 모바일백신은 윈도우즈 모바일과 심비안 플랫폼에 지원되며, 해외에서만 판매되고있다. 제공하는 기능 전반이 사생활 보호에 맞추어져있다. 눈에 띄는 특징이 있다면, 폰 분실 시 내장된 GPS Find 기능을 이용하여 폰의 위치를 확인할 수 있고, 원격으로 잠금 및 삭제기능을 지원하는 것이다. SIM 카드가 교체되면 SIM Watch가 작동, 잠금 기능이 설정된 후, 기존 주인의 주소로 새 번호가 전송된다. 그 밖의 보안기능으로는 실시간 멀웨어 스캔, 자동업데이트, 미리 정의된 보안레벨을 기반으로 위험한 네트워크 연결 차단 등이 있다.



(그림 6) Kaspersky Mobile Security 9 화면

3.3. 시만텍- Norton Smartphone Security

안드로이드 플랫폼에 지원되는 Smartphone Security는 악성 애플리케이션에 대한 데이터베이스(Norton Community Watch)를 구축하고, 이를 바탕으로 악성 코드를 검출하는 방식을 사용한다. 또한 사용자의 참여로 데이터베이스를 구축하게 된다. 부가서비스로는 SMS를 통한 잠금 기능을 지원한다. 이 때 잠금 해제번호를 잘못 입력한 경우, 내장된 데이터가 모두 삭제되므로 신중하게 입력해야한다. 또한 원격으로 애플리케이션 삭제도 할 수 있다. 멀웨어를 차단하는 방식으로 멀웨어 시그니처를 통한 애플리케이션 스캐닝, 블랙리스트 관리, 새로 다운받는 애플리케이션에 대한 검사를 수행한다. 전화번호 및 SMS 차단 역시 블랙리스트 기반으로 작동한다. 업데이트방식은 실시간과 주기설정이 가능하다.



(그림 7) Norton Smartphone Security 화면

<표 2> 제품별 지원 플랫폼 및 기능과 특징

구분	AhnLab V3 Mobile	하우리 브이로봇	Kaspersky Mobile Security9	Norton Smartphone Security
지원 플랫폼	Windows Mobile Android Symbian	Android	Symbian Windows Mobile	Android
악성 애플리케이션 검출 방식	행위기반(Android) 악성리스트 기반	행위기반 악성리스트 기반	Heuristic (계발 구동식)	악성리스트 기반
실시간 검색	파일 및 프로세스 검색	악성코드 검색	기능 기원	기능 지원
원격 삭제 및 도난 방지 기능	지원하지 않음	기능 지원	GPS Find, SIM Watch 등 다양한 기능 지원	SMS 전송을 이용한 휴대폰 잠금/삭제 기능제공

※ 조사 대상 플랫폼 중 iOS용 플랫폼의 특성상 조사 항목에서 제외하였다.

4. 결론

조사 결과 국내 제품의 경우 안드로이드 플랫폼인 경우 지원하는 악성 애플리케이션 검색 방식이 행위기반 방식이라는 공통점이 있었다. 그에 비해 외국 제품의 경우 기존의 해당 회사의 검색 방식을 사용함을 알 수 있었다. 또한 공통적으로 애플리케이션 스캔 기능 이외에 서비스 제공 범위의 차이는 존재하였으나, 개인정보 보호 기능들은 모든 백신 프로그램에서 제공되고 있었다. 노턴 각 백신별 자세한 지원 플랫폼 및 지원 기능은 다음의 <표 2>와 같다.

또한 현재 출시되어 있는 스마트폰용 백신의 지향점이 기존의 PC백신과는 확연히 다름을 알 수 있었다. 특히 악성 코드를 검출하는데 있어서는 행위기반 검출이라는 특이한 방법을 사용함을 알 수 있었다. 이는 스마트폰이라는 단말기의 특성상 악성코드가 취할 수 있는 행동 패턴이 제약되는 점에서 착안한 것이라 판단된다. 또한, 스마트폰이 민감한 개인정보를 다루는 디바이스이어서 백신에 악성 코드 검출 및 치료 기능 외에 개인정보를 관리해주는 기능을 추가한 제품이 대다수였다. 특히 카스퍼스키(Kaspersky)사 제품의 경우 타사의 제품과 비교했을 때 개인정보 보호 기능이 매우 강화되었음을 알 수 있었다.

따라서 향후 스마트폰 백신은 좀 더 개인정보 보호에 치중하게 될 것이며, 스마트폰이라는 디바이스 성격에 적합한 악성 코드 검출 방법이 새롭게 적용 될 것으로 예상된다.

참고문헌

[1] 김경진, 정지희, 김유진, 홍승필, “모바일 오픈 플랫폼 내 보안 API설계 방안”, 2010 한국인터넷정보학회 학술발표대회, pp. 375 - 380, 2010.

[2] 제갈병직, “스마트폰 시장과 모바일OS 동향”

[3] 김도형, 류철, 이재호, 김선자, “스마트폰용 모바일 소프트웨어 플랫폼 동향”, 전자통신동향분석 제25권 제3호, 2010.6

[4]“http://venturebeat.com/2010/07/28/android-wallpaper-app-that-steals-your-data-was-downloaded-by-millions/“, 2010. 9. 20일 검색

[5] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보보호학회지 제19권 제5호, 2009.10

[6] 임종훈, “이슈와 논좀”, 제22호, 2010.2.1

[7] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보보호학회지 제19권 제5호, 2009.10

[8] 김기영, 강동호, “개방형 모바일 환경에서 스마트폰 보안기술”, 정보보호학회지 제19권 제5호, 2009.10

[9] 임종훈, “2010 국정감사 정책자료 II”, 국회입법조사처, P.257