스마트폰 악성코드 동향 및 전망

김상수* · 최연성*
*국립군산대학교

Trends and Prospects of SmartPhone Malware

Sang-Su Kim* · Yeon-Sung Choi*
*Kunsan National University
E-mail : tosail@kunsan.ac.kr

요 약

애플의 아이폰이 출시된 이후 전 세계적으로 스마트폰 열풍이 불기 시작했다. 이후, 다양한 종류의 스마트폰이 출시되었고, 스마트폰의 편리함으로 인해 가입자 수가 폭발적으로 증가하였다. 스마트폰 사용자가 급증함에 따라 스마트폰을 대상으로 하는 악성코드 또한 폭발적으로 증가하였다. 스마트폰 악성코드는 2011년 하반기부터 본격적으로 발견되기 시작해 2012년 폭발적으로 증가하였고, 현재까지도 지속적으로 증가하고 있는 추세이다. 본 논문에서는 스마트폰 악성코드 발생 현황과 동향에 대해 살펴보고, 악성코드 동향 분석을 통해 악성코드의 향후 전망에 대해 기술한다.

ABSTRACT

Apple's iPhone was released and the SmartPhone craze started in the world. Then, Many kind of SmartPhone released on the market, the number of subscribers increased explosively for the convenience of SmartPhone. By SmartPhone users increases rapidly, the number of Malware targeting SmartPhones increased explosively. The SmartPhone Malware, tend to increase explosively in 2012 beginning to be discovered in earnest from the second half of 2011, and is continuously increasing even now. In this paper, describes the status and trends of SmartPhone Malware, through the analysis of trends in the SmartPhone Malware, we describe the future prospects of SmartPhone Malware.

키워드

스마트폰 악성코드, 안드로이드 악성코드, 악성코드 현황, 악성코드 전망

Ⅰ. 서 론

애플의 아이폰이 출시된 이후 전 세계적으로 스마트폰 열풍이 불기 시작했다. 2009년 WIPI 탑재 의무화 정책을 해제한 이후, 국내에는 아이폰, 안드로이드폰, 심비안, 블랙베리 등 해외의 많은 스마트폰들이 출시되었고, 스마트폰의 편리함으로 인해 가입자 수가 폭발적으로 증가하였다. [1] IT 리서치 업체인 가트너의 발표에 따르면 2013년 1분기 휴대폰 시장은 4억 2천 5백대 규모로, 전년 동기 대비 1% 상승에도 미치지 못했지만, 스마트폰 시장은 2억 1천만대 수준으로 전년 대비 30% 이상의 상승률을 기록하며, 전 세계적인 스마트폰 열풍이 지속되고 있음을 확인 할 수 있다. [2] 스마트폰 사용자가 증가함에 따라 스마트폰 데이터 트래픽 또한 폭발적으로 증가하였다.

에릭슨이 발표한 '모빌리티 보고서'에 따르면 세계 모바일 데이터 트래픽 규모가 5년 내 12배 늘어날 것이라고 전망했다.[3] 네트워크의 속도가 증가함에 따라 이 증가세는 더욱 커질 것으로 예상된다.

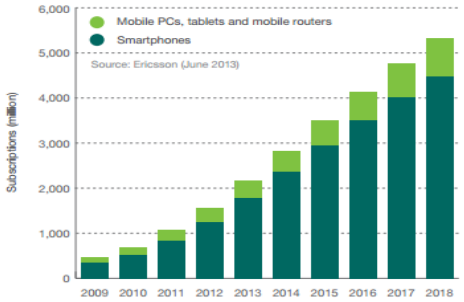

그림 1. 모바일 기기 데이터 트래픽

스마트폰 시장의 성장과 데이터 트래픽 증가와 더불어 사용자의 개인정보를 빼내거나 사용자 스마트폰 시스템을 공격하기 위한 악성코드 또한 폭발적으로 증가하였다.

본 논문에서는 스마트폰 악성코드 발생 현황과 동향에 대해 살펴보고, 스마트폰 악성코드 동향 분석을 통해 스마트폰 악성코드의 향후 전망에 대해 기술한다.

Ⅱ. 스마트폰 악성코드 발생 현황

2013년 1분기 세계 스마트폰 OS점유율은 안드로이드가 74.4%로 1위, 2위는 18.2%의 점유율로 iOS가 차지했다.[4]

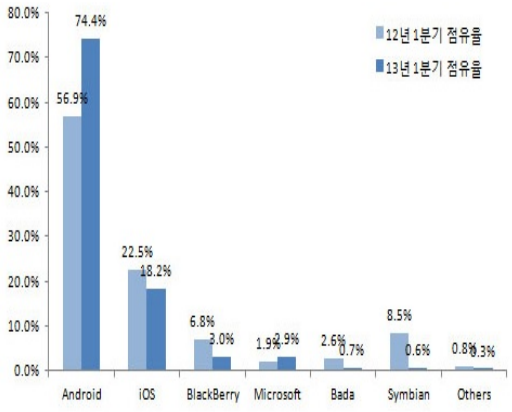

그림 2. 세계 스마트폰 OS 점유율

가장 높은 점유율을 보이는 안드로이드는 리눅스 2.6커널을 기반으로 하는 개방형 플랫폼이다. 안드로이드는 소스코드를 모두 공개함으로써 누구라도 이를 이용하여 소프트웨어와 기기를 만들어 판매 할 수 있도록 하였다.[5] 또한, 이 플랫폼에서 응용할 수 있는 애플리케이션을 거래하는 온라인 공간인 '안드로이드 마켓'을 통해 누구나 쉽게 보안 검증 절차나 심의 과정 없이 애플리케이션을 배포 할 수 있는 환경을 제공하고 있다. 이러한 장점 때문에 많은 회사들이 안드로이드 플랫폼을 기반으로 스마트폰을 출시하고 있다.

하지만, 안드로이드는 소스코드가 공개되어 있고 애플리케이션 등록 절차가 간단하고 애플리케이션 등록 시 보안 검증 절차나 심의 과정이 없기 때문에 많은 악성코드 제작자들이 안드로이드 플랫폼을 타겟으로 악성코드를 제작 유포하고 있다. 미국 국토안보부와 법무부가 공동으로 발표한 보고서에 따르면 지난해 발생한 모바일 악성코드 위협 중 안드로이드에서 발생한 비율이 전체 운영체제의 79%를 차지했다. [6]

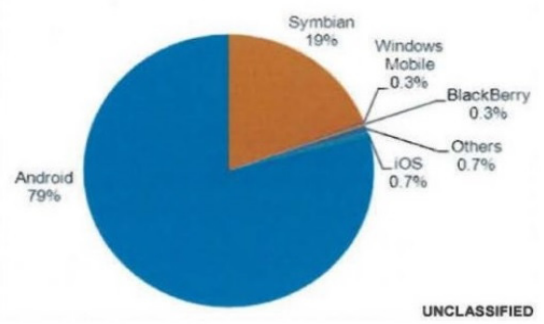

그림 3. 모바일 운영체제 별 악성코드 위협, 2012

안드로이드의 경우 공식 마켓 이외에도 비공식적인 서드파티 마켓을 통해 애플리케이션을 다운받을 수 있다. 이 곳 또한 별도의 보안 검증이나 심의 과정이 없기 때문에 악성코드에 쉽게 노출될 수 있다.

표 1. 스마트폰 악성코드 발견 건수

월	2011년	2012년	2013년
1월	5	2112	43109
2월	9	4578	83868
3월	21	5233	79651

안랩에서 발표한 1분기 스마트폰 악성코드 동향을 보면 1분기 동향 조사결과 총 206,628개의 안드로이드 기반 악성코드 샘플이 수집되었다고 밝혔다. 이는 지난 해 동기 11,923개의 약 17배 증가한 수치이다. 스마트폰 악성코드는 2011년 하반기부터 본격적으로 발견되기 시작해 2012년 폭발적으로 증가했고, 현재까지도 지속적으로 증가하고 있는 추세이다. [7] 이러한 증가세는 당분간 지속 될 것으로 보인다.

Ⅲ. 스마트폰 악성코드 동향

초창기 악성코드는 개인이 호기심 또는 자기과시를 목적으로 제작되었다. 하지만 최근의 악성코드는 금전적 이득, 개인정보 유출, 사용자 기기를 제어하기 위한 봇넷 등 다양한 목적을 위해 조직적으로 제작되고 다양한 방법으로 배포되고 있다.

표 2. 모바일 악성코드 사례

악성코드명	주요 악성행위	발생일자
WinCE/TerDial	국제전화 발신	2010.04.19
Jackeey Walpaper	정보 유출	2010.07.30
Geinimi	SMS 무단전송	2010.12.29
ADRD	음성 녹음	2011.02.15
HiddenSms	위치정보유출	2011.06.02
qqgame.lord	루팅, 악성앱 설치	2011.06.07
GoldDream	통화기록 유출	2011.07.07
WebLoic	Dos 공격수행	2012.02.18
Rootor.TC	자동루팅, C&C	2012.04.05
Zitmo.B/C/D	기기 정보 유출	2012.06.19
KRSpammer	SMS 정보 탈취	2012.10.26
KRFackerPK	SMS 정보 탈취	2013.01.14
KRSpammer.V	DDos 모듈	2013.01.14
Obad	관리자권한 탈취	2013.06

2010년 4월에 발생한 WinCE/TerDial 악성코드의 경우 3D Anti Terrorist Action 이라는 스마트폰 게임에 트로이 목마 형태로 숨어 있었으며, 설치되는 시점에 스마트폰을 감염시키고 국제전화를 무단으로 발신함으로써 사용자는 금전적 피해를 입게 된다. [8] 이러한 악성코드에 감염될 경우 사용자는 금전적 피해를 입게 되지만 악성코드 제작자가 얻는 금전적 이득은 없다. 악성코드 제작자들은 금전적 이득을 얻기 위해 다양한 종류의 악성코드를 제작하고 있다. 2012년 10월에 발생한 KRSpammer의 경우 악성코드 제작자에게 금전적 이득을 얻게 하는 악성코드이다. 이 악성코드는 잘 알려진 국내 업체의 할인, 무료쿠폰 등의 SMS 형식으로 전파되며, 문자에 포함되어 있는 URL에 접속을 유도한 후 사용자들로부터 악성 앱을 설치하도록 한다.[9] 악성 앱이 설치된 스마트폰을 이용해 각종 사이트에서 소액결제 서비스를 진행하고 인증용 SMS를 탈취하여 결제를 완료한다. 악성코드 제작자는 이를 현금화하여 부당이득을 취득한다. 하지만 금전적 피해를 유발하는 최근의 악성코드는 기존의 단순 소액결제를 노리던 것에서 금전 피해 규모가 커질 우려가 있는 금융정보(공인 인증서, 계좌번호, 보안카드 일련번호) 등을 훔치는 형태로 진화 하고 있다.[10]

금전적 이득을 위한 악성코드 이외에도 개인정보 유출을 목적으로 하는 악성코드 또한 꾸준히 발견되고 있다. 개인정보 유출 악성코드의 경우 주로 사용자의 위치 정보를 수집하는 형태였지만, 최근에는 사용자의 통화내용이나 통화기록, 사진, USIM 정보, 전화번호, 메모 등 다양한 정보를 수집하고 있다. 이러한 개인정보 유출은 2차 범죄에 악용될 가능성이 있다. 수집된 전화번호는 악성코드 유포에 사용될 가능성이 있다. 실제로 수집한 전화번호를 통해 모바일 청첩장을 전송해 악성코드를 유포하는 일이 발생했다. 지인의 번호로 청첩장이 전송되었기 때문에 의심 할 여지가 적었다. 이처럼 수집한 개인정보를 통해 악성코드 유포에 사용하거나 범죄에 악용하는 일이 점점 늘어나고 있다.

금전적 피해 또는 개인정보 유출을 위한 악성코드 뿐만 아니라 사용자 시스템을 점유하기 위한 악성 코드가 배포 되고 있다. 2013년 등장한 'Obad' 라고 하는 악성코드는 관리자권한까지 확보해 제거조차 할 수 없고, 기기에 저장된 모든 데이터를 훔칠 수 있다. 추가로 악성애플리케이션을 다운받아 설치하며, 블루투스나 와이파이를 통해 근처에 있는 다른 단말기 까지 악성코드를 전파하는 것으로 확인되었다. 또한 다양한 암호층과 코드 난독화 기법을 사용하여 자신의 작업을 숨기고 있으며 SMS를 통해 명령을 받을 수도 있다. [11] 이러한 방법으로 관리자 권한을 획득한 스마트폰은 DDoS 공격, 웹 하드 그리드 컴퓨팅 등 악의적인 목적으로 사용될 가능성이 있다.

Ⅳ. 스마트폰 악성코드 전망

3장에서 살펴본 바와 같이 사용자에게는 금전적 피해를 입히고, 악성코드 제작자에게는 금전적 이득을 얻게 하는 악성코드가 점차 지능화 되고 있다. 금전적 피해를 입게 하는 악성코드는 개인정보유출을 목적으로 하는 악성코드와 함께 사용되어 점차 지능화 될 것으로 예상된다. 스마트폰에 저장된 지인들의 생일, 기념일등에 축하 메시지와 함께 쿠폰으로 위장한 악성코드 URL을 전송한다면 사용자가 악성 앱을 설치할 확률이 높아질 것이다. 이러한 악성코드는 구글이 애플리케이션 설치 시 외부 링크를 허용하는 한 지속 적으로 발생 할 것으로 예상된다.

3장에서 살펴본 악성코드는 서드파티 마켓 또는 쿠폰이나 가짜 어플리케이션으로 위장한 악성코드를 사용자가 직접 다운 받아 악성코드에 감염 되는 형태였다. 하지만 최근의 악성코드 감염 경로는 점차 다양해지고 있다. 최근 웹페이지 접속 만으로 악성코드에 감염되는 취약점이 발견되었다. 이외에도 다양한 취약점을 통해 악성코드에 감염되는 사례가 늘고 있다. 이러한 취약점은 대부분 낮은 버전의 스마트폰 OS에서 발생한 문제로 버전이 올라가면서 취약점을 보완하고 있다.

표 3. 안드로이드 버전별 점유율

Codename	API	Distribution
Froyo	8	2.4%
Gingerbread	10	30.7%
Honeycomb	13	0.1%
Ice Cream Sanwich	15	21.7%
Jelly Bean	16	45.1%

하지만 많은 수의 안드로이드 사용자들이 구버전 OS를 사용하고 있다. 때문에 이러한 취약점을 통한 악성코드 감염 피해는 지속적으로 발생할 것으로 예상된다.

최신 OS를 사용한다고 해서 항상 악성코드로부터 안전 한 것은 아니다. 최근 커널 레벨에서 동작하는 악성코드가 속속 등장하고 있다. 커널에 악성코드가 설치되면, 문자를 통해 원격 제어를 할 수 있고, 원하는 모든 정보를 훔칠 수 있게 된다. 이러한 커널 레벨 악성코드는 현재의 스마트폰 백신으로는 전혀 탐지가 안되며 네트워크 상태 정보도 숨김이 가능하다.[12] 커널 레벨 악성코드는 현재의 스마트폰 백신으로 탐지가 안되고 사용자 스마트폰을 자유자재로 제어할 수 있기 때문에 꾸준히 증가할 것으로 예상된다.

Ⅴ. 결 론

스마트폰의 등장과 함께 우리 생활의 많은 부분이 바뀌었다. 스마트폰은 언제 어디서나 웹에 접근 할 수 있고, 다양한 종류의 어플리케이션을 통해 유용한 정보를 실시간 확인과 같은 다양한 장점을 가지고 있다. 하지만 유용한 정보로 위장한 악성코드들이 등장하고 있고, 이로 인한 피해가 점점 증가하고 있다. 이러한 악성코드는 금전적 피해, 개인정보 유출, 스마트폰 강제 제어 등 다양한 형태로 발생하고 있다. 앞서 언급한 악성코드로 인한 피해는 사용자가 조금만 주의를 기울인다면 피해를 방지 할 수 있다. 대부분의 악성코드가 비공식 서드파티 마켓에서 배포가 되고 있기 때문에 정식 마켓을 이용한다면 어느 정도 피해를 줄일 수 있다. 또한, SMS 나 공식 마켓이 아닌 외부 링크를 통한 어플리케이션 설치를 자제한다면 피해를 줄일 수 있다. 더욱 확실한 방법은 마켓에 등록 할 때 어플리케이션을 검증하는 방법이 있다. 마켓에 어플리케이션을 등록할 때 검증 과정이 없는 안드로이드를 대상으로 악성코드가 주로 발생하고 있다. 어플리케이션 등록 시 검증 과정을 실시하는 앱 스토어의 경우 악성코드 발생 비율이 현저하게 낮은 것을 확인 할 수 있다. 마켓에 어플리케이션 등록 시 검증 과정을 만들거나 광고, SNS 등을 통해 사용자의 보안 의식을 향상 시킨다면 악성코드로 인한 피해를 상당 부분 줄일 수 있을 것으로 예상된다.

본 연구는 군산대학교 정보통신기술연구소의 부분적인 지원으로 수행되었음

참고문헌

[1] 서승현, 김종명, 전길수, 2010년 모바일 악성코드 동향 분석 및 전망 한국정보보보학회 2011
[2] http://www.connectinglab.net/wordpress/?p=5664
[3] Ericson Mobility Report, Jun 2013
[4] http://www.connectinglab.net/wordpress/?p=5850
[5] http://terms.naver.com/entry.nhn?docId=1348050&cid=200000000&categoryId=200003371
[6] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=21449
[7] http://blog.ahnlab.com/ahnlab/1754
[8] 전길수, 모바일 보안 한국인터넷진흥원, 2013
[9] http://www.datanet.co.kr/news/articleView.html?idxno=64691
[10] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNews View.do?menu_dist=1&seq=21502
[11] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130610062814
[12] http://dailysecu.com/news_view.php?article_id=102