모바일 악성 코드 현황 및 대책

최아빈*, 류수미*, 이훈재*
*동서대학교 정보통신공학과

Mobile Malicious code Trends and Consideration

A-bin Choi*, Su-mi Ryu*, HoonJae Lee*
*Dept. of Information and Communication Engineering, Dongseo University

E-mail : abin9163@nate.com, qururu@nate.com, hjlee@dongseo.ac.kr

요 약

최근 다양한 기능을 지원하는 애플리케이션이 개발됨에 따라 스마트 폰의 보급률이 증가하고, 애플리케이션 시장이 급속도로 커지면서 사용자가 급증하는 추세이다. 스마트 폰이 실생활에 밀접해져 기기 안에 중요한 데이터가 저장된다. 이러한 점을 악용하여 생긴 다양한 목적을 가진 악성코드로 인해 스마트 폰의 안전은 위협 받고 있다. 이에 본 논문에서는 최근에 유포된 각각 모바일 OS의 악성코드로 인해 발생한 원인 및 문제점에 대해서 분석하고 대책을 알아보고자 한다.

ABSTRACT

Recently, as application that support a various functions is developing, through the smart phones penetration rate and applications market is increasing quickly, the user has been growing rapidly. An important data is stored in the smart phone because smart phone is closely connected to real life. Due to the malicious code caused by abuse with diversity purpose, the safety of the smart phone is being threatened.Accordingly in this paper, we will grasp about malicious code such as incidence, cause and attack type. Through this, it will be considered that problems is caused by malicious code each mobile OS spreaded lately.

키워드
악성코드, 모바일, 현황, iOS, 안드로이드

Ⅰ. 서 론

현대사회는 과학기술의 발전으로 우리 일상생활에 있어 많은 변화를 가져왔다. 이 중 가장 두드러지게 발전된 분야는 휴대용 단말기 분야라 해도 과언이 아니다. 초기 휴대용 단말기의 경우 간단한 전화나 메시지 전송만 가능 했으나 현재에는 스마트 폰이라는 변화된 이름을 가지고 여러 가지 작업을 할 수 있게 되었다. 스마트 폰을 통하여 사용자가 원하는 여러 가지 작업을 할 수 있다. 예를 들어, 웹 서핑, 문서작업, 물품 구매 및 결제, 은행업무까지 다양한 작업들을 스마트 폰 하나로 해결할 수 있게 되었다. 이로 인해 점차적으로 스마트 폰 사용량이 증가함에 따라 스마트 폰은 현대인들의 생활에 없어선 알 될 필수품으로 자리 잡게 되었다. 이로 인해 스마트 폰은 많은 정보들이 저장하는데 이 정보들의 상당수는 개인정보이다. 이러한 점을 악용하여 이익을 얻으려는 사람들이 생기기 시작하였고, 현재에 이르러서는 그 수가 많이 증가하였다. 이러한 사람들이 다른 스마트 폰 사용자들의 개인정보를 얻거나 금전적 이익을 얻기 위해 사용하는 방법 중 하나가 악성코드를 유포하는 것이다. 이들은 스마트 폰 모바일 OS의 취약점을 이용해서 악성코드를 애플리케이션에 삽입하여 개인정보를 탈취하거나 사용자 몰래 일정 금액의 이용대금을 부과하는 등의 피해를 일으키고 있다. 이런 악성코드 중 대표적인 유형에는 PUP(Potentially Unwanted Progr

am)이나 Trojan이 있다. PUP은 trojan의 종류 중 하나로 스마트 폰에서 광고를 알림 바에 띄워 악성 애플리케이션을 다운 할 수 있도록 유도한다. 이로 인해 2차 피해를 일어 날 수 있으며 수시로 광고를 띄어주기 때문에 스마트 폰 사용을 방해한다. Trojan은 감염되면 원격지에서 사용자의 스마트 폰 내의 여러 정보를 수집하여 서버에 전달하거나 특정사이트에 대한 접속하는 작업등을 수행한다. 이에 본 논문에서는 이러한 악성코드들에 대해서 자세히 알아보고자 한다.

Ⅱ. OS별 악성코드 분포 현황 및 발생경로

스마트 폰이 국내에서 주목받은 것은 몇 년 되지 않았다. 그러나 스마트 폰이 고가의 기기임에도 불구하고 상당히 많이 판매됨에 따라 국내의 기업들도 구글 안드로이드 운영체제를 탑재한 스마트 폰을 내놓기 시작하였다. 이를 시작으로 스마트 폰 시장이 급격히 성장하였다. 시장이 커질수록 스마트 폰 보급률은 급속도로 증가하여 세계기준 2012년 3분기에 10억 명을 넘어섰다[1]. 아래의 [그림1]은 국내 스마트 폰 OS 점유율을 나타낸다.

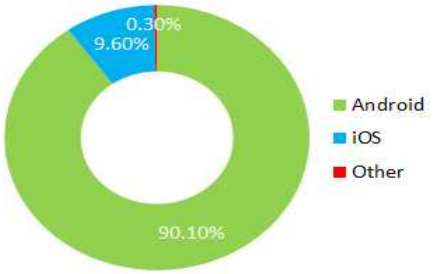

그림 1. Korea Smartphone Market, OS Share

하지만 가장 많이 보급된 OS인 안드로이드와 iOS이지만 악성코드의 위협에서는 상반된 특성을 보이고 있다. 2010년, 국내 최초의 스마트 폰 악성코드인 'TredDial'가 발견된 이래 악성코드의 발생률은 매우 급증하였다[2]. 그 중 OS별 악성코드 발생률은 급격한 차이를 보였는데 이는 [그림2]의 OS별 악성코드 발견률에서 알 수 있다.

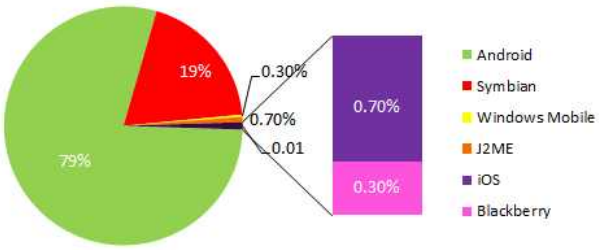

그림 2. Threat Families and Variants by Platform, 2012

가장 많이 보급된 OS임에도 불구하고 안드로이드는 가장 높은 발생률을 보였지만 이에 반해 iOS는 단, 0.7%의 발생률로 극명한 차이를 보였다. 이러한 이유는 안드로이드가 사용자가 많다는 것도 이에 속하지만 본질적으로 각 OS의 정책이 다르기 때문이다. 안드로이드의 경우 리눅스 기반의 개방형 플랫폼으로 쉽게 취약점에 노출되었으나 iOS는 애플사에서 개발한 비공개형 플랫폼으로 공격자들이 쉽게 취약점을 찾을 수 없기 때문에 악성코드 발생률이 안드로이드에 비해 매우 낮았다. 그리고 iOS는 자사 Appstore에 애플리케이션 등록 시 사전 신청을 통해 애플사에 애플리케이션을 검열 받는다. 이때 적합하지 않은 애플리케이션은 Appstore에 등록되지 않는다. 하지만 안드로이드는 iOS와 달리 별도의 검열 없이 애플리케이션 등록이 가능하기 때문에 손쉽게 악성코드가 심어진 애플리케이션을 구글 play에 올려 사용자가 쉽게 내려 받을 수 있게 되었다. 안드로이드가 이렇게 검열 없이 무분별하게 애플리케이션을 올리는 것이 가능하다는 것이 하나의 약점이 될 수도 있지만 애플리케이션 등록 시 검열하는 iOS도 안전하지만은 않다. 왜냐하면 이런 철저한 검열에도 불구하고 Appstore에 악성 애플리케이션이 등록되었기 때문이다. 이는 Find and Call이란 이름을 가진 애플리케이션으로 겉으로는 연락처를 찾는 기능을 가지고 있지만 실제는 사용자의 연락처를 수집하여 스팸메일을 발송하는 악성코드를 담고 있다[3]. 현재 해당 애플리케이션은 삭제되었지만 단단한 검열체계를 자랑하는 애플 또한 더 이상 악성코드에 대해 안전하지 않다는 것이다.

이외에 안드로이드는 iOS와 달리 사용자가 시스템으로부터 최고 관리자 권한을 가져오는 루팅을 하지 않아도 apk 파일로 손쉽게 애플리케이션 설치가 가능하기 때문에 공격자가 애플리케이션에 악성코드를 심어 리패키징하여 배포하는 경우 사용자는 설치하려는 해당 애플리케이션이 악성 애플리케이션인지 모르고 감염 될 수 있다. 그리고 안드로이드에는 공식 마켓인 구글play 말고도 사설 애플리케이션 시장이 있다는 것도 악성코드가 유포될 수 있는 또 하나의 경로가 된다. iOS는 안드로이드의 루킹과 비슷한 탈옥을 통하면 악성코드의 위협에서 안전하지 못한다. 탈옥이란 아이폰의 여러 잠금장치를 풀게 되는 것으로 이 작업을 통해 사용자는 인증되지 않은 불법 애플리케이션을 내려 받아 사용할 수 있다. 이외에 이증되지 않은 다른 사설 애플리케이션 장터를 통해 Appstore에서는 볼 수 없는 검증되지 않는 애플리케이션을 사용가능 하다. 이 과정에서 사용자들은 악성코드의 위협에 쉽게 노출된다.

Ⅲ. 악성코드 유형별 현황 및 최근 악성코드 유형

모바일 악성코드는 스마트 폰 사용자들이 편의를 위해 스마트 폰을 매우 오랜 시간동안 이용한다는 점과 무선인터넷을 이용한다는 점을 악용하여 다양한 유형들로 유포 되었다. [그림3]은 12년도에 발견된 악성코드의 유형을 나타낸다.

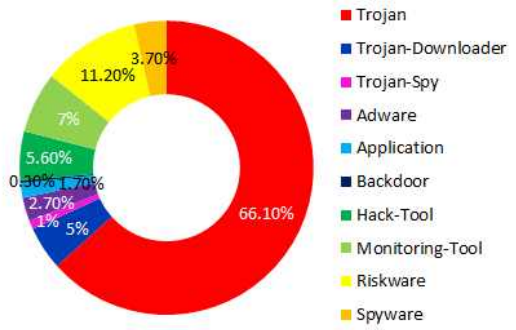

그림 3. Mobile Threats by Type, 2012

작년 한 해 가장 많이 발생한 악성코드는 trojan, spyware 순으로 많았다. 가장 많이 발생한 trojan은 주로 자기 복제 기능은 없지만, 유용한 프로그램으로 가장, 침투해 여러 가지 정보를 유출하는 등의 방식으로 이루어진다. 이외에 사용자의 동의 없이 설치하여 사용자 정보를 수집하는 Spyware, 스마트 폰의 보안 취약점을 이용해 폰 내의 보안을 해제하고 권한을 얻어 특정 애플리케이션 설치 및 삭제 등의 특정한 작업을 하게 하는 Exploit 등이 있다. 이 장에서는 대표적으로 발견된 악성코드에 대해 자세히 설명하고자 한다.

3.1 trojan

trojan은 자기 복제 기능은 없지만 유용한 프로그램으로 가장하여 침투해 여러 가지 피해를 일으키는 악성코드 유형이다. 자기 복제 기능이 없지만, 정상적인 프로그램으로 가장하여 그 안에는 어떤 숨겨진 기능이 있을지 몰라 주의가 필요하다. 또한 스마트 폰의 정보를 외부로 유출하는 악의적 기능을 포함하고 있는 경우가 많다. 최근에는 위와 같은 악성코드가 담긴 애플리케이션을 유포하기 위해 해당 애플리케이션으로 유도하는 URL을 포함한 스팸 문자가 사용자들에게 가는 경우가 많아졌다. 이렇게 설치된 악성 애플리케이션은 휴대전화 번호를 빼돌려 서버로 유출하거나, 해당 전화번호로 소액 결제를 유도하는 방식으로 이어지고 있다. 그렇기 때문에 사용자들은 문자에 포함된 URL에 접속하지 않는 것이 좋다.

3.2 spyware

spyware란 사용자의 사전 동의 없이 특정한 작업을 수행하는 프로그램이다. 특정 프로그램 설치 시 별도의 프로그램 설치나 다른 악성 애플리케이션 설치를 유도하고 SMS나 통화기록과 사용자 스마트 폰 모니터링 등의 경우로 이어져 사생활 침해라는 큰 피해가 생기므로 주의가 필요하다. spyware은 리패키징을 통해 변형된 애플리케이션에 삽입된 경우가 있으며, 몇몇 악의적인 목적을 가진 애플리케이션에 포함된 채로 유포되고 있다. 이외에 백도어 설치로 이어지거나 스마트 폰 정보 수집, 루팅이 되어 있는 폰이라면 통화 녹음 까지 악의적인 행위도 가능하다.

3.3 그 외 악성코드 유형

위의 2가지 유형 이외에도 많은 여러 가지 악성코드 유형들이 있지만 일부만 다뤄보고자 한다. 우선 Adware에 대해 살펴보자면 특정 애플리케이션 설치 시 수시로 특정 광고를 띄우거나 애플리케이션 실행 시 인터넷 팝업창을 띄우게 만든다. 또 사용자 의사와 상관없이 광고를 표시하여 부당이익을 창출해 내는 방법이다. 사용자가 만일 이 광고를 누르게 된다면 또 다른 Adware나 악성 애플리케이션 설치 유도가 불가피 하기 때문에 2차 피해가 일어날 수가 있다. Backdoor는 시스템 접근에 대한 사용자 인증 등 정상적인 절차를 거치지 않고 응용프로그램 또는 시스템에 접근 할 수 있도록 도와준다. Backdoor가 삽입된 애플리케이션을 설치할 시 스마트 폰 모니터링, gps를 통한 위치수집 등의 피해가 일어나게 된다. 이는 곧 공격자들이 개인정보를 이용하여 2, 3차 적으로 피해를 발생시키는 방법이 된다.

최근에는 이러한 정보수집만을 위한 악성코드만이 아닌 스마트 폰을 DDOS 공격에 이용되는 일종의 좀비 폰으로 만드는 악성코드가 발견되었다[4]. 실제로 스마트 폰을 통해 이동통신사 망의 특정 대역폭에 할당된 자원을 고갈 시키는 등의 DDOS공격이 가능하다는 전문가의 의견도 나오고 있다 시간이 갈수록 스마트 폰 악성코드의 종류가 일반 컴퓨터만큼 다양해지며, 교묘해지고 있다.

Ⅳ. 스마트 폰 악성코드 대책 및 방안

본 논문에서는 앞서 언급한 악성코드에 대해 분석한 내용을 토대로 피해 감소 및 대처 방안에 대해 언급하고자 한다.

안드로이드, iOS는 일반적으로 악성 애플리케이션이 설치되어 기기가 악성코드에 감염된다. 이로 인해 개인정보가 유출되는 등의 피해가 발생한다

는 사실을 알 수 있었다. 이러한 피해를 막기 위해서 우선 악성코드가 심어진 악성 애플리케이션의 배포를 차단하는 것이 가장 확실한 방법이다. 구글 안드로이드의 경우 마켓 내에서 악성 애플리케이션을 탐지하는 바운서(Bouncer) 시스템을 시작하였지만[5] 작년 6월 보안 컨퍼런스에서 바운서를 우회하는 과정이 공개되었다. 그로 인해 악성코드가 들어있는 악성 애플리케이션의 탐지가 무용지물 되어 악성코드가 스마트 폰에 유입할 수 있게 되었다. 때문에 바운서의 탐지 기능에 위의 우회과정까지 포함하고 그 외에 생길 수 있는 과정에 대해서도 미리 예측하여 보안할 수 있어야한다. 그리고 바운서를 보좌할 수 있는 새로운 시스템 개발로 더욱더 안전한 시스템의 구축이 필요하다. 더하여 구글 사 내에서도 좀 더 강력하고 효율성 높은 보안 정책을 통해 사용자 이용환경이 안전하게 유지 되어야 한다. 그리고 안드로이드 정책 특성상 안전하지 못한 안드로이드 OS를 보안하기 위해 마켓 내에 수많은 백신들이 존재한다. 이 중 Kaspersky 사의 Mobile Security Lite는 실시간 검사가 아닌 애플리케이션 설치 시 자사의 클라우드 기반의 통신하여 애플리케이션 내에 위험이 존재하는가에 대해서만 확인하며 국내의 Ahnlab사에서 만든 V3 Mobile 2.0은 행위기반 검사와 패턴 기반 검사를 이용하여 실시간 검사와 악성코드 탐지를 한다. 하지만 위와 같은 백신들은 먼저 악성코드가 발견되고 나서 후에 백신을 만들기 때문에 매우 비효율적이다. 백신이 만들어지기 이전에 이미 사용자가 해당 악성코드에 감염되었다면 이미 피해가 일어난 후 치료되는 것이나 마찬가지이기 때문이다. 그렇기에 이를 보완하기 위한 휴리스틱 탐지 기법의 안정성을 고려하고 좀 더 발전시켜 이를 백신에 적용해야 한다. 그리하여 발견되지 않은 악성코드라도 피해가 일어나기 전에 치료할 수 있도록 하여야 한다.

iOS는 보안정책 특성상 검열을 통과한 애플리케이션만을 설치가능하기 때문에 백신이 거의 존재하지 않지만 Intego사의 'VirusBarrier'은 iOS전용 백신으로 Appstore내 등록되었다. 이는'Virus Barrier'의 주 목적이 iOS전용 바이러스를 탐지하는 것만이 아니라 iOS를 탑재하고 있는 스마트폰을 경유해 PC용 악성코드가 개인 및 기업 컴퓨터로 흘러 갈 수 있음을 예측하고 windows 악성코드나 MAC OS 악성코드를 차단하기위해 만들어진 애플리케이션이기 때문이다. 하지만 이와 같은 백신이 iOS의 보안을 안전하게 지켜주는 것이 아니다. 그렇기에 안전성을 보장하기 위하여 애플사는 더욱더 엄격하고 강력한 검열 방식 재구축과 이를 보완할 수 있는 안전한 보안정책이 필요하다. 그리고 운영체제의 취약점이 드러나기 이전에 이를 미리 파악하여 iOS 자체의 안정성을 높여야 한다. 이외에 취약점을 보안한 신속한 iOS 업데이트를 통해 사용자들에게 악성코드가 유포되기 전에 사전 차단이 필요하다.

사용자들은 안전한 애플리케이션 이용을 위해 좀 더 신경을 기울여 애플리케이션의 출처나 서명인증이 제대로 되어있는지 확인하고 올바르지 않는 출처나 인증이 되어있지 않은 경우에는 설치하지 말아야한다. 또한 제조사가 제한 지어 놓은 시스템 부분을 루팅이나 탈옥을 통해 해제 시켜 보안을 위협하기 때문에 이를 하지 않는 것을 권장한다. 그리고 믿을 수 있는 경로로 설치된 애플리케이션이라도 해당 애플리케이션의 최신버전을 유지하여 안전하게 스마트 폰 이용하는 것을 제시한다.

Ⅴ. 결론

본 논문에서는 스마트 폰의 발생경로, 분포 현황, 대책 및 방안에 대해 살펴보았다. 스마트 폰 악성코드는 사용자 수의 증가와 각 OS의 취약점으로 인해 수가 매우 증가했으며, 이 중 악성코드는 공격자의 목표에 따라 매우 다양한 종류로 나누어진다. 이에 따라 개인정보 유출, 소액 결제 등의 피해가 발생 이를 막기 위하여 각 안드로이드와 iOS의 취약점과 보안정책을 보완하여 보다 더 안전한 스마트 폰의 이용을 위해 필요하다. 이에 따라 사용자는 믿을 수 있는 출처에서만 애플리케이션을 설치하는 등의 스마트 폰을 안전하게 이용할 수 있는 대책 및 방안을 따라야 한다. 이외에 더욱더 안전한 스마트 폰 이용이 할 수 있도록 보안성을 높이기 위한 연구가 필요하다.

참고문헌

[1]ZDNet Korea from : http://www.zdnet.co.kr/news/news_view.asp?artice_id=20121017183235
[2]지식정보보안연구부“스마트 단말 보안 위협 및 대응 기술”, 한국전자통신연구원, p.17, 2011
[3]SECURELIST - Denis(Kaspersky Lab Expert) from : http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam
[4]박용규, “사이버대피소를 통해 본 ‘12년도 DDoS 공격 동향 분석’, ”, Internet&Security Focus 2013 2월호, 2012
[5]임정관, 심재화, 강승구, 이훈재, “안드로이드 해킹 사례 및 향후 보안 대책”, 정보통신학회, 제19권 제1호, p689, 2012