지능형 모바일 악성코드 감염 경로에 관한 연구

최요한*, 서희석*, 백의칠*, 김성준**

요약

국내외로 스마트폰에 대한 관심이 높아지고 사용자층이 확대되면서 스마트폰을 활용한 다양한 연구가 여러 분야에서 진행 중이다. 스마트폰의 사용자가 늘어난 만큼 사용자의 개인정보를 탈취를 목적으로 하는 악성어플리케이션 또한 크게 증가하고 있다. 과거에는 단순한 유형의 악성코드가 주를 이룬 반면 최근에는 APT등과 같은 다양한 방법의 악성코드가 등장하고 있다. 이러한 악성코드를 탐지하고 예방하기 위해서는 스마트폰이 어떠한 경로를 통해 감염되는지에 대한 연구가 선행 되어야 한다.

본 논문에서는 지금까지 발견된 악성코드 대해서 살펴보고 APT등과 같은 다양한 방법과 접목된 모바일 악성코드 감염 시나리오를 통해 미래에 발생할 수 있는 지능형 모바일 악성코드 감염 경로를 살펴보고자 한다.

A Study on Intelligent Mobile Malware Infection Paths

Yo-Han Choi*, Hee-Suk Seo*, Eui-Chil Baek*, Seong-Jun Kim**

ABSTRACT

Interest in smart phones is increasing. Using the expanding user base, a variety of smart phones is underway in many areas of research. Now, the smartphone is very closely connected with our everyday lives. Because an increase in smart phone users, malicious code has increased The purpose of the malicious code to steal the personal information. In the past, was the most simple types of malicious code. The other hand, recently a variety of ways, such as APT has emerged of malicious code. The malicious code in order to detect and respond Should be followed for the study to Smartphone is infected by any route. In this paper, we look for malicious code found so far, Grafted with a variety of ways, such as APT and mobile malicious code infection scenarios are recognized. That may occur in the future intelligent mobile malware infection paths will be discussed.

Keywords : mobile, malware, scenario, wi-fi, add-on application

* 한국기술교육대학교 컴퓨터공학부(✉crlayh@kut.ac.kr)

** 동국대학교 법학과

· 제1저자(First Author) : 최요한 · 교신저자(Correspondent Author) : 서희석

· 접수일(2012년 4월 17일), 수정일(1차 : 2012년 5월 14일), 게재확정일(2012년 5월 17일)

Ⅰ. 서 론

최근 국내·외에 다양한 종류의 스마트폰이 출시되면서 일반 사용자들까지 스마트폰에 대한 관심을 가지게 되었고 시간이 지날수록 스마트폰에 대한 관심은 높아지고 있다. 이러한 소비자들의 요구를 반영하여 경제, 문화 등 사회 전반적으로 스마트폰에 대한 의존도가 높아지고 있으며, 이제 스마트폰은 우리 생활에 없어서는 안 될 필수적인 요소로 자리 잡고 있다.

스마트폰에서 데이터통신을 위해 사용하는 3G망은 기존의 전화망을 사용하기 때문에 통신 속도가 느릴 수밖에 없다. 이러한 3G망의 느린 속도를 해결하기 위해서 각 통신사는 경쟁적으로 전국에 자사의 고객이 사용할 수 있는 Wi-Fi망을 구축하였다. 현재는 지하철, 버스 등과 같은 곳에도 Wi-Fi망을 이용할 수 있다. 하지만 이러한 Wi-Fi망의 관리 소홀 및 사용자의 주의 부족으로 인해 개인정보가 유출되는 통로로 사용될 수 있다.

다른 예로, 많은 스마트 폰 사용자들은 자신의 스마트 폰을 꾸미는데 돈과 시간을 아끼지 않는다. 특히나 요즘 많은 사람들은 폰 꾸미기 어플리케이션을 이용해 자신만의 개성적인 인터페이스와 배경, 폰트를 꾸미는데 적지 않은 투자를 한다. 사회적 상호작용 과정에서 사람들은 종종 말이나 행동을 통해서 뿐 아니라, 사회적 정체성을 표현하는 사물을 소유하거나 사용함으로써 타인들로 하여금 자신에 대한 분류를 단순화할 수 있도록 돕는다. 일반적으로, 특정한 물건들은 특정한 정체성의 상징으로 사용된다[1]. 즉, 개성 있는 자기표현을 위한 방식 중 한 방법으로 자신만의 특별한 스마트폰을 가지고자 꾸미는 것이다.

이러한 폰 꾸미기 어플리케이션은 기본프로그램을 스마트 폰에 설치하고 난 후 각종 테마, 폰트, 인터페이스를 추가로 다운받아 사용한다. 이 때 공격자의 악성코드가 심겨진 추가 인터페이스를 받을 경우 사용자의 각종 개인정보가 유출 될 가능성이 있다.

이처럼 우리의 실생활에 밀접하게 연관되어 있는 스마트폰에 대한 보안의식이 늦을 경우 개인정보 유출과 같은 치명적인 보안위협을 가질 수 있다[2]. 최근 일본에서 스마트폰 어플리케이션을 통해 대규모의 개인정보가 유출된 사건이 발생했으며, 유출된 개인정보유출 규모는 약 100만여 명에 달하는 것으로 추산된다. 이 어플리케이션은 실행되면서 전화번호부에 등록되어 있는 이름과 전화번호가 외부로 전송되는 것으로 밝혀졌고 최대 27만여 명이 다운로드 한 것으로 집계됐다. 일본의 사례와 같이 정상적인 어플리케이션을 가장한 악성코드가 사용자의 개인정보를 노리고 있다.

본 논문에서는 관련연구를 통해 스마트폰을 공격대상으로 하는 악성코드의 유형을 분석하고, 과거와 현재의 공격 동향을 분석하였다. 분석한 공격 동향을 토대로 앞으로 발생 가능한 악성코드 감염 경로를 제시하였으며, 제시한 악성코드 감염 방법에 대한 탐지 방법에 대해 알아보고자 한다.

Ⅱ. 관련연구

최초의 모바일 악성코드로 알려진 Cabir가 2004년 8월에 필리핀에서 발견된 이후, 꾸준한 증가세를 보이고 있다. 국내에서도 2010년 4월 윈도우 모바일 스마트폰을 대상으로 한 악성코드가 최초로 발생한 후로 스마트폰 대중화로 인해 역시 꾸준한 증가세를 보이고 있다.

그동안 발생되었던 모바일 악성코드의 유형을 살펴보면 감염된 스마트폰 내부의 시스템 파일을 삭제하거나 변형시켜 정상적인 동작을 방해하는 시스템 파괴 및 변경 유형, 배터리 소모를 통한 가용성 저하 유형, 과금 피해를 유발시키는 악성코드 유형, 스마트폰 기기 정보 및 개인 정보를 유출하는 유형 등이 있다[3].

2.1 단말 장애 유발형 악성코드

스마트폰 단말기에 장애를 유발시켜 사용자가 단말기를 사용하기 못하게 하는 공격 유형이다. 일부 부가기능을 마비시키거나 메뉴를 임의로 변경시키고 특정키가 눌리지 않게 만든다[4].

2.2 배터리 소모형 악성코드

스마트폰 단말기의 전력을 지속적으로 소모시켜 배터리를 고갈시키는 공격 유형이다. 2004년에 블루투스를 통해 전파되는 최초의 모바일 악성코드인 Cabir가 대표적이다. Cabir는 단말의 침해를 유발하지 않는 대신 지속적으로 인근 단말의 블루투스를 스캐닝하고, 블루투스를 통해 악성코드를 전파하는 특징을 가지고 있다[5].

2.3 과금 유발형 악성코드

스마트폰 단말기의 문자 서비스나 지속적인 통화연결을 시도하여 요금을 부과하는 유형이다. 이 악성코드에 감염된 단말기는 사용자 모르게 불특정 다수에게 문자 메시지를 보내 사용자에게 과금을 유발한다[6]. 스마트폰의 경우 사용하는 요금제에 따라서 3G사용 요금이 달라지는데 악성코드로 인해 통신사에서 무료로 제공되는 3G사용량을 모두 소모하고도 지속적으로 3G망에 접속해 사용자에게 과도한 요금부담을 주게 된다.

2.4 정보유출형 악성코드

스마트폰 기기 정보나 사용자 정보를 공격자에게 유출시키는 유형이다. 이 악성코드에 감염된 스마트폰은 단말기의 기기의 시리얼번호나 운영체제, 그리고 해당 스마트폰에 설치된 어플리케이션의 종류를 외부로 전송한다. 이 외에도 스마트폰의 통화기록이나 문자메시지 또한 외부로 전송한다. 최근 발견되는 악성코드들은 대부분 이러한 정보 유출형 악성코드로 스마트폰 기기 정보뿐만 아니라 연락처에 저장된 개인정보의 유출로 인해 2차적인 피해를 입을 수 있는 유형의 악성코드 이다.

2..5 크로스 플랫폼형 악성코드

모바일 단말을 통해 PC를 감염시키는 공격 유형이다. 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드로써 폰의 메모리 카드에 윈도우 웜을 복사하여, 감염된 폰 메모리 카드를 PC에 장착했을 때 autorun를 통해 PC를 자동으로 감염시켜 데이터를 삭제하거나 성능을 저하시키게 만든다. 모바일 기기간의 확산이 아닌 모바일 기기에서 PC를 감염시킨다는 점에 서 새로운 형태의 공격 유형을 가지고 있다[7].

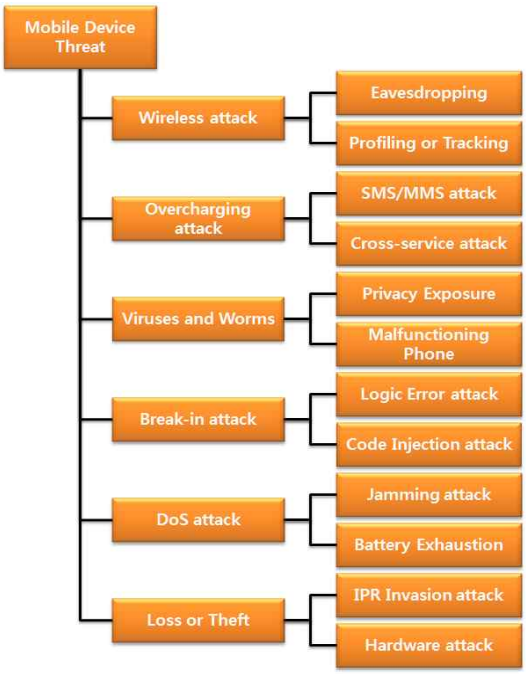

그림 1. 모바일 공격 유형 분류
Fig. 1 Mobile Device attack threat

이러한 여러 악성코드에 대응 하기위한 보안 기술이 계속적으로 등장하고 있지만, 단말기의 발전과 서비스에 따라 모바일 악성코드로 인한 스마트폰의 보안 위협 또한 증가하고 있다[8].

그림 1는 모바일 환경에서 스마트폰이 공격을 받을 수 있는 여러 유형을 분류하고 있다.

스마트폰을 공격하는 유형은 침해방법과 그 목적이 다양하기 때문에 하나의 방법으로 정의하기 힘들지만 주요 공격을 기반으로 분류했다.

최근 발견되고 있는 악성코드들은 대부분 안드로이드 운영체제기반의 악성코드이다. 오픈소스라는 특징으로 인해 안드로이드OS의 구조를 파악하기 쉽기 때문에 안드로이드 악성코드 제작이 다른 모바일OS를 대상으로 하는 악성코드에 비해 월등이 많은 추세이다. 또한 단기간에 안드로이드 사용자가 폭발적으로 증가하면서 안드로이드 계열 스마트폰의 악성코드가 급증한 것이다. 무엇보다 정보 탈취형 악성코드보다 소비자의 직접적인 피해가 우려되는 과금발생형 악성코드가 80% 이상을 차지하고 있다. 최근에 중국의 안드로이드 마켓에서 새로운 악성코드 루트스마트(RootSmart)가 유포되어 10만대의 스마트 폰이 감염되어 봇넷을 형성하고 있었다. 안드로이드 2.3.3과 3.0 이전 버전의 단말기로부터 정보를 훔쳐내고 프리미엄 요금제 문자메시지 서비스와 전화 사기로 수익을 얻었다. 중국으로 제한된 이 봇넷은 모바일 봇넷 중 최대 규모이다. 2011년 9월부터 감염시키기 시작해 지난 2월까지 1만 1천여 대의 봇넷 디바이스가 활성화 되어 있었다. 이 봇넷을 통해 하루에 1,600 ~ 9,000달러의 피해가 생기는 것으로 추정되며, 앞으로도 이러한 봇넷이 계속 출현할 것으로 예상된다.

이제 국내 스마트폰사용자도 2500만여 명으로 앞으로도 꾸준히 늘어날 것으로 전망된다. 이에 따른 모바일 악성코드로 인한 피해도 늘어날 것이다.

III. 지능형 모바일 악성코드 감염 경로

3.1 무선 AP접속으로 인한 악성코드 감염

최근 스마트폰을 활용한 다양한 어플리케이션이 등장하면서 3G 전화망을 이용한 데이터 통신 또한 많아졌다. 하지만 3G 전화망은 기존의 인터넷망에 비해 전송 속도가 느리고 높은 비용으로 인해 스마트폰 사용자들은 개인이 구축한 Wi-Fi(Wireless Fidelity)망을 이용하거나, 카페, 통신사에서 제공해 주는 Wi-Fi망을 사용하는 빈도가 높아지고 있다.

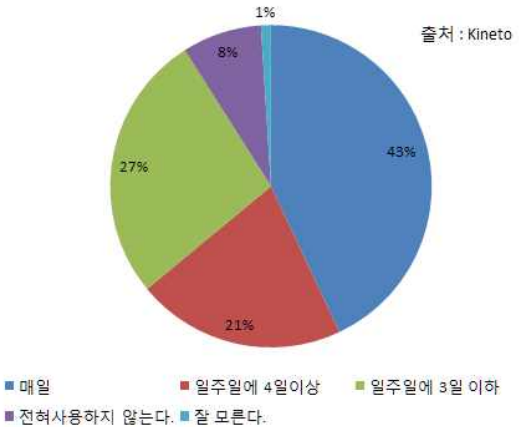

그림 2. 미국 Wi-Fi 이용 현황
Fig. 2 Wi-Fi Usage Status in U.S.

많은 스마트폰 사용자가 이용하는 Wi-Fi망에 대한 보안의식은 상대적으로 낮은 경향이 있다[9]. 이러한 점을 이용하여 공격자는 Wi-Fi망을 이용하여 악성코드를 유포할 수 도 있을 것이다.

본 논문에서 말하는 Wi-Fi망을 이용한 악성코드 감염시나리오는 공격자가 현재 통신사 혹은 기업에서 무상으로 제공하는 AP(Access Point)와 유사한 이름을 가지는 AP를 제공함으로써 사용자를 자신이 제공하고 있는 AP로 유도한다.

공격자는 자신의 AP로 사용자를 유도하고 일정시간동안 인터넷사용을 할 수 있도록 제공한다. 사용자가 공격자의 AP를 통해 인터넷을 일정시간 사용하면

인터넷 사용을 중지시키면서 공격자가 사전에 제작한 어플리케이션을 기업의 홍보어플리케이션으로 가장해 사용자의 스마트폰에 설치하도록 유도한다. 사용자가 해당 어플리케이션을 설치할 경우 인터넷을 사용할 수 있도록 허가를 하여, 악성코드가 포함된 어플리케이션을 의심하지 않도록 한다.

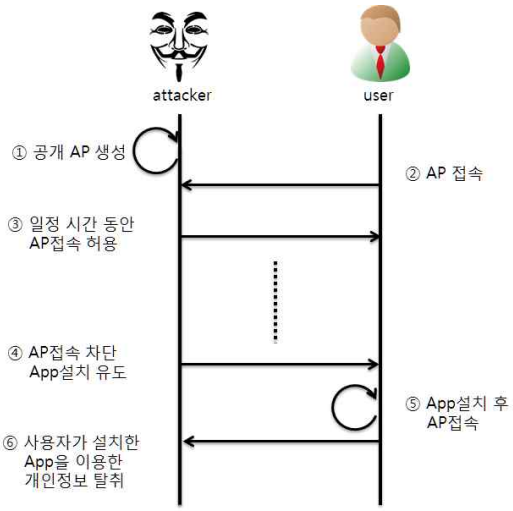

그림 3. Wi-Fi를 이용한 악성코드 유포 개요
Fig. 3 Application to Wi-Fi Malware Spread Overview

이렇게 불특정 다수의 사용자에게 공격자는 악성코드가 포함된 어플리케이션을 배포할 수 있다. 이러한 악성코드 유포는 안드로이드 어플리케이션 설치 파일인 apk파일만 있으면 마켓을 통하지 않더라고 어플리케이션을 설치 할 수 있어 안드로이드OS를 사용하는 스마트폰에 치명적이다.

그림 3은 가짜AP를 이용한 악성코드 유포 과정을 보여주고 있다. 공격자가 사용자에게 어플리케이션을 설치하도록 유도하고 설치된 어플리케이션을 이용하여 개인정보를 유출하는 과정에 대해서 자세히 살펴보면 다음과 같다.

각 통신사에서 사용자들의 과도한 3G망사용으로 3G망에 부하가 걸리는 것을 방지하는 대책으로 최근 도시 주요 시설 AP를 설치하여 3G보다 빠른 인터넷 속도를 제공해 주는 Wi-Fi망을 사용하도록 유도하고 있다. 공격자는 이러한 AP와 유사한 이름을 가진 공개 AP를 생성하여 사용자에게 각 통신사에서 제공하고 있는 AP로 속이고 사용자의 접속을 기다린다. 공격자는 자신이 생성한 AP로 많은 사용자들이 접속하도록 유도하기 위해 AP이름 앞에 fast, new등과 같은 키워드를 이용하여 기존에 통신사에서 제공하고 있는 AP보다 빠른 속도를 제공해 하는 것처럼 사용자를 속여 접속을 유도한다.

사용자는 빠른 데이터통신을 위해 공격자가 생성한 AP에 접속을 요청한다. 사용자의 AP접속 요청을 받으면 공격자는 자신이 생성한 AP를 통해 사용자가 인터넷을 이용할 수 있도록 제공해 준다. 이렇게 사용자가 공격자의 AP를 이용하는 동안 공격자는 자신의 AP를 통과하는 패킷정보를 수집하여 사용자가 접속하는 웹사이트의 주소, ID/PW등을 수집 시작한다.

사용자가 공격자에 AP를 통해 일정시간 이상 인터넷을 이용할 경우, 공격자는 사용자의 AP사용을 차단하고, 계속 인터넷을 이용하기 위해서는 어플리케이션을 설치하도록 유도한다. 공격자는 사용자가 어플리케이션을 설치하는 것에 대한 거부감을 줄이기 위해서 기업의 홍보용 어플리케이션 혹은 보안성을 향상시키기 위한 어플리케이션으로 가장한다. 또한 안드로이드OS를 이용하는 스마트폰의 경우 정상적인 마켓을 이용하지 않아도 apk파일만을 이용하여 어플리케이션을 설치 할 수 있어 마켓의 검열을 공격자는 손쉽게 회피할 수 있다.

공격자는 사용자의 스마트폰에 설치된 어플리케이션을 이용하여 연락처, 메일 등과 같은 개인정보에 접근할 수 있는 권한을 획득할 수 있다. 공격자는 이렇게

획득한 사용자의 개인정보를 불법적으로 이용할 수 있으며, 이러한 공격이 장기간에 걸쳐 이루어질 경우에는 공격자는 많은 수의 스마트폰을 좀비화 시킬 수 있다. 공격자는 상당수의 좀비스마트폰을 확보하고 이러한 좀비스마트폰을 이용하여 동시다발적으로 3G망을 사용하면 3G망 마비와 같은 현상을 초래할 수 있을 것이다.

3.2 추가 인터페이스 다운로드를 통한 감염

시대의 흐름에 맞추어 개성 있는 모습을 추구하는 사람들이 늘어가고 있다. 스마트폰 또한 각자의 개성에 맞추어 꾸며 사용하는 사람들이 꾸준히 증가 하고 있다.[10] 이에 따라 손쉽게 스마트폰을 꾸며주는 어플리케이션을 다운받아 사용하는 사람들이 많이 늘어가고 있다. 본 장에서는 이러한 폰꾸미기 앱을 통한 악성코드 유포과정을 설명하고자 한다.

런처를 쓰게 되면 스마트폰 사용자 누구나 쉽게 자신이 원하는 테마로 스마트폰 환경을 바꿀 수 있다. 하지만 런처를 쓴다고 해서 바로 자신이 원하는 테마를 쓸 수 있는 것이 아니다. 런처 프로그램을 베이스로 스마트폰에 설치한 후 사용자는 자신이 원하는 테마를 선택해 추가로 다운을 받아 설치해야 한다.

그림 4를 보면 Go 런처의 점유율이 다른 런처보다 많은 것을 확인할 수 있다.

그림 4 런처별 총 다운로드 현황
Fig. 4 Launcher Download Figure

Go 런처는 타 런처와 다르게 테마 뿐 아니라 widget 이나 locker도 지원을 하는데 이 역시 추가로 다운을 받아야만 사용할 수 있다.

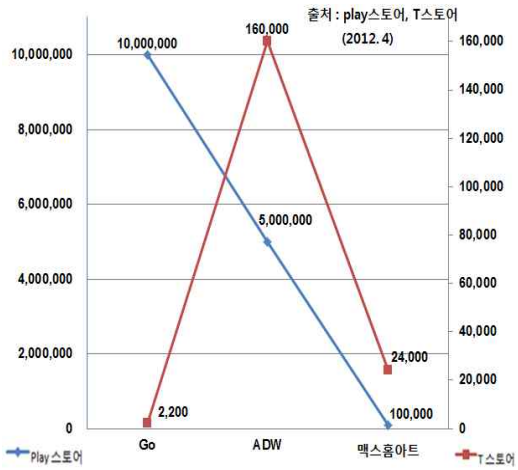

그림 5. Play스토어와 T스토어의 런처 다운로드 횟수
Fig. 5 Play store and T-store Launcher Downloads

그림 5는 최근 각 스토어의 런처 다운로드 현황을 나타낸 것이다. 가장 많은 사람들이 이용하는 Play스토어에서 Go런처가, 그리고 T 스토어에서는 ADW 런처를 가장 많이 다운받아 사용하고 있는 것으로 나타났다. 특히나 Go 런처의 다운로드 현황은 1천만 건 이상으로 많은 스마트폰 사용자들이 이용하는 것으로 확인된다.

또한 현재 4,400만이 이용하는 카카오톡 같은 경우에도 어플리케이션 그대로 사용하기 보다는 독특하고 개성 있게 꾸며주는 테마를 이용하는 사용자들이 많은 것으로 나타났다.

특히 Go 런처의 경우 런처 고유의 스토어가 존재한다. 그래서 테마 제작자는 마켓이 아닌 런처 고유 스토어에 자신이 제작한 테마를 스마트폰 사용자들이 다운받아 사용할 수 있도록 업로드 할 수 있다.

이러한 점을 이용해 공격자는 테마 제작 시 악성코

드를 심어 스토어에 등록해서 테마를 다운받은 사용자들의 정보를 불법적으로 획득할 수 있다.

추가적인 앱을 이용한 악성코드 감염 경로는 그림6과 같은 과정을 통해 유포된다. 유포되는 과정을 각 단계마다 자세히 분석해 보면 다음과 같다.

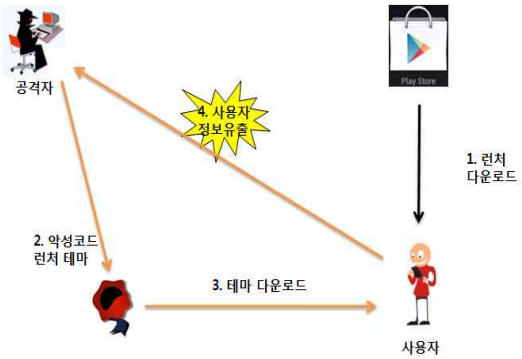

그림 6 앱 다운로드를 통한 악성코드 유포 개요
Fig. 6 Application to Download Malware Spread Overview

첫 번째, 사용자가 자신의 스마트폰을 꾸미기위해 런처 프로그램을 다운받는다. 이때 받은 런처 프로그램은 기본적인 테마만 제공하므로 사용자가 자신의 스마트폰을 꾸미기에는 부족하다 느끼게 되고, 원하는 테마를 찾게 된다. 이처럼 공격자의 타겟은 기본적인 런처 프로그램을 다운받아 쓰는 사용자들이 된다.

두 번째, 공격자는 사전에 런처 테마를 제작해둔다. 이렇게 제작된 런처 테마에 악성코드를 심어서 사용자들이 해당 런처 테마를 다운로드 하도록 런처 스토어에 업로드 한다.

세 번째, 사용자는 기본적인 런처 테마를 바꾸기 위해 런처 스토어에서 자신이 원하는 테마를 찾아보게 되고, 이 때 공격자가 제작한 악성코드가 포함된 테마를 다운받게 된다.

마지막으로, 악성코드가 심겨진 테마를 다운 받아 사용하게 되면 사용자 스마트폰에 저장된 전화번호부, 매일 같은 개인 정보에 접근할 수 있는 권한을 공격자가 획득할 수 있게 된다. 공격자는 이렇게 얻은 사용자 개인 정보를 불법적으로 이용하거나 금전적인 이득을 취할 수 있다.

대부분의 런처가 오픈소스로 공개되어 공격자가 테마 제작 시 악성코드를 심어 둔다면 사용자는 자신의 정보가 빠져나가는지 조차 모른 채로 자신의 개인정보를 공격자에게 유출하게 되는 것이다.

추가적인 앱을 통한 악성코드의 경우 사용자가 테마의 겉모습만 보고 무의식적으로 다운을 받기 때문에 자신의 스마트폰이 악성코드에 감염이 되었는지 인지하기조차 어렵다.

3.3 백신 삭제를 유도한 악성코드 감염

최근 모바일 악성코드가 많이 유포되면서 모바일 악성코드로 인한 피해가 심각하다. 모바일 악성코드로 인한 사용자의 피해를 최소화하기 위해서 PC 백신을 만들고 있는 업체에서는 모바일 환경에서 사용할 수 있는 백신 어플리케이션을 제공해 주고 있다. 한국의 대표적인 PC 보안 업체인 이스트 소프트에는 안드로이드OS에서 사용할 수 있는 백신 프로그램인 "ALYac Android" 어플리케이션을 제작해 사용자의 스마트폰에 설치되어 있는 악성코드가 포함된 어플리케이션 검사를 통해 사용자의 개인정보를 보호하고 있다.

모바일 환경에 최적화된 보안어플리케이션은 대표적인 악성코드 유형인 과금 부과형에 대한 검사와 현재 스마트폰에 설치되어 있는 어플리케이션에 부여된 권한을 검사하여 사용자의 개인정보에 불법적으로 접근하는 어플리케이션을 감지해 낸다.

현재 안드로이드 어플리케이션 마켓인 play 스토어에 모바일 보안 어플리케이션은 ALYac, 터보백신 모바일, Lookout 보안 바이러스 백신 등 10여개 이상이 등록되어 있다. ALYac의 경우 세계 55개국에서 700만

건 이상의 다운로드를 기록할 정도로 많은 스마트폰 사용자들이 사용하는 것으로 나타났다.

그림 7 모바일 알약

Fig. 7 Moblie ALYac

이처럼 백신 어플리케이션이 설치되어 있는 경우 악성코드가 포함된 어플리케이션을 설치하지 못하거나 악성코드가 포함된 어플리케이션이라는 경고 알람이 발생해 공격자는 사용자의 스마트폰에 악성코드가 포함된 어플리케이션 설치를 유도할 수 없다.

백신을 우회하기 위해서 공격자는 사용자 스스로 백신프로그램을 삭제하도록 유도할 수 있다. 백신 프로그램 제작사의 실수로 사용자가 다운받아 설치하려는 어플리케이션이 악성코드로 분류되었다는 메시지를 사용자에게 보여준다. 또한 사용자에게 해당 어플리케이션을 사용하려면 백신 프로그램을 삭제하고 재설치하기를 권한다는 메시지도 같이 보여준다.

공격자는 백신프로그램이 해당 어플리케이션을 실행하기 위해 필요한 기능에 대해서 백신 프로그램의 오류로 인해 사용할 수 없다는 경고메시지를 어플리케이션 마켓에 개재하고, 백신 프로그램 제작사와 연락하여 수정될 것이라고 사용자에게 알려서 사용자 스스로 백신 프로그램을 삭제하도록 유도한다. 실제로 마켓에 등록되어 있는 일부 게임 어플리케이션은 사용자의 연락처에 접근하여 자동적으로 사용자의 연락처에 저장된 사람 중 해당 게임을 하고 있는 사람을 추가한다거나, 다른 사람과의 대전을 위해서 인터넷 접속을 시도하는 경우가 많이 있다.

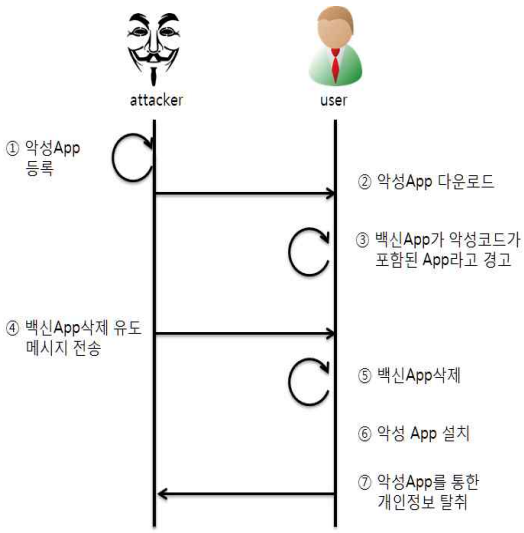

그림 8 백신 삭제를 유도하는 악성코드

Fig. 8 Delete vaccines Induction malignant code

사용자가 스스로 백신 프로그램을 삭제하고 공격자가 등록한 어플리케이션을 설치하면 공격자가 등록한 어플리케이션은 사용자의 스마트폰에 저장된 연락처, 단말기 정보, 이메일 등을 공격자에게 전송하게 되고, 공격자는 이 정보들을 불법적으로 이용할 수 있다. 또한 백신 프로그램을 사용자가 삭제한다면 스마트폰의 보안 수준이 낮아지게 되면 다른 악성코드에 감염될 가능성도 높아져 추후 2차, 3차적인 피해를 입을 수도 있다. 보안의식이 낮은 스마트폰 사용자들은 애초에 백신프로그램을 설치하지 않는 경우도 있기 때문에, 이러한 사용자들은 공격자의 좋은 타겟이 될 수 있다.

Ⅳ. 결 론

스마트폰이 일반 사용자에게 많이 보급되면서 실생활 곳곳에서 스마트폰이 활용되고 있다. 특히 과거에는 PC상으로만 가능했던 인터넷뱅킹이 스마트폰을 통하여 가능해졌으며, 기업의 중요한 사항이 포함된 메일을 즉시 확인하고 처리할 수 있게 되었다.

스마트폰이 실생활에 밀접하게 연관되면서 스마트폰에 대한 보안 또한 중요해 졌다. 과거에는 단순히 스마트폰에 장애를 일으키거나 배터리를 소모하는 등이 단순한 기능을 수행하는 악성코드가 주를 이루었지만, 최근 들어 스마트폰에 저장되어 있는 개인의 연락처, 스마트폰의 내부기기정보 등을 노리는 악성코드가 등장하였다. 이러한 스마트폰에 저장된 개인의 정보를 노리는 악성코드는 사용자의 개인정보에 위협을 가하고 있다. 최근 일본에서 발견된 악성코드는 어플리케이션을 통한 사용자의 개인정보를 외부로 유출하였고, 유출된 개인정보의 량은 100만 건에 달하는 것으로 파악되었다.

이처럼 점점 지능화 되고 있는 스마트폰의 악성코드에 대응하기 위해서 본 논문에서는 앞으로 발생 가능성이 높은 악성코드 유포 시나리오에 대해서 살펴보았다. 살펴본 악성코드 유포시나리오는 공격자가 생성한 공개 AP를 통한 악성코드 감염과 추가 인터페이스를 필요로 하는 어플리케이션으로 인한 악성코드 감염 시나리오를 살펴보았다.

우선 무선 AP를 통한 악성코드 감염 시나리오는 공격자가 악의적인 목적을 가지고 생성한 무선 AP망에 사용자가 접근을 요청하고, 공격자는 사용자의 AP접속을 허용해 주면서 사용자의 패킷을 도청하거나 악성코드가 포함된 어플리케이션설치를 유도하여 사용자의 스마트폰을 좀비화 시켜 모바일 DoS와 같은 공격을 위해 사용하는 시나리오를 살펴보았다.

그리고 추가 인터페이스 다운로드로 인한 악성코드 감염 시나리오는 안드로이드OS의 아이콘 혹은 UI변경을 위해서 설치한 어플리케이션은 기본적인 UI변경 이외에 사용자의 기호에 맞게 변경하기 위한 추가 인터페이스를 다운로드하는 과정에서 공격자가 악성코드를 포함시킨 인터페이스를 다운로드 함으로써 악성코드에 감염되는 시나리오였다.

본 논문에서 살펴본 모바일 악성코드 감염 경로는 사용자의 개인정보를 탈취하는 것뿐만 아니라 현재까지 해당 악성코드를 삽입하여 유포하는 공격에 대해서는 뚜렷한 대응 방법을 찾기가 어렵다. 추가적인 인터페이스를 이용한 악성코드와 정식적인 마켓을 통한 어플리케이션설치가 아니면 악성코드를 탐지하는데 있어 여러 어려운 점이 많기 때문에 사용자들의 피해가 빠른 속도로 확산될 가능성이 있다. 또한 대부분의 사용자는 악성코드 감염 사실조차 모른 채로 개인정보가 공격자에게 유출되는 심각한 상황이 우려된다.

향후 모바일 백신에 대한 연구를 통해 다양한 악성코드 유포에 대해 대응할 수 있도록 지속적인 연구가 필요할 것이다. 추후 본 논문에서 살펴본 악성코드 유포 시나리오에 대한 실험을 통해서 지능화 되고 있는 악성코드 탐지 방법 및 해결 방안에 대한 연구하자고 한다.

참고문헌

[1] Eugene Park, “A Study on Minihompy Users'" cyber item using Motivation and Benavior”, Cyber communication Academic Society, Vol 25 No3, 2008.

[2] Namje Park, “Analysis of Privacy Weakness and Protective Countermeasures in Smart Grid Environment”, Korea Institute of Information Technology, Vol 8 No 9, 2010

[3] Ik Su Kim, Jin Hyuk Jung , Hyeong Chan Lee, Jeong Hyun Yi, “Analysis Method and Response Guide of Mobile Malwares”, korea information and communication society, vol 35 no 4, 2010

[4] Park Yeonhee, Kim Jonguk, Lee Seong-uck, Kim Cholmin, Usman Tariq, Hong Manpyo, “A Scalable

Distributed Worm Detection and Prevention Model using Lightweight Agent", The korean institute of Information Scientists and Engineers, vol 14 no 5, 2008

[5] Kang Dong Ho, Kim Jeong Nyeo, Cho Hyun Sook, "Trends of Mobile Threats and Security Service Technology", The korean institute of Information Scientists and Engineers, Vol 28 No 6, 2010

[6] Giyoun kim, Seongij Cho, "Security Vulnerability Trends in Smartphones", The korean institute of Information Scientists and Engineers, Vol 37 No 2, 2011

[7] Kyu Won Lee, Jae Won Ji, Hyun Woo Chun, Sang-jo Youk, Geuk Lee, "Traffic Analysis Technique for Intrusion Detectionin in Wireless Network", Journal of Security Engineering, Vol 7 No 6, 2101

[8] Eun-Young Jang, Hyung-Jong Kim, Choon-Sik Park, Joo-Young Kim, Jae-il Lee, "The study on a threat countermeasure of mobile cloud services", Korea Institute of information Security & Cryptology, Vol 21 No 1, 2011

[9] Dipankar Dasgupta, Hal Brian, "Mobile Security Agents for Network Traffic Analysis", DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, Vol 2, 2001

[10] Ilyoung Yang, Sooyoung Lee, "Exploring smartphone early adopters categories on the basis of motivations", Korean Journal of Journalism & Communication Studies, Vol 55 No 1, 2011

감사의 글

이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2010-0021951).

저자소개

최요한 (Yo-Han Choi)

2012년 한국기술교육대학교 컴퓨터공학부 학사

2012년~현재 한국기술교육대학교 컴퓨터공학부 석사과정

※ 관심분야 : 악성코드, 네트워크, 모바일 보안

서희석 (Hee-Suk Seo)

2000년 성균관대학교 산업공학과 학사
2002년 성균관대학교대학원 전기전자 및 컴퓨터공학과 석사
2005년 성균관대학교대학원 전기전자 및 컴퓨터공학과 박사
2005년～현재 한국기술교육대학교 컴퓨터공학부 교수
※ 관심분야 : 모델링&시뮬레이션, 네트워크보안, 보안 시뮬레이션, USN

백의칠 (Eui-Chil Baek)

2006년 ~ 현재한국기술교육대학교 컴퓨터공학부 학사

※ 관심분야 : 악성코드, 네트워크, 모바일 보안

김성준 (Seong-jun Kim)

2003년 동국대학교 법학학사
2006년 동국대학교 법학석사
2009년 동국대학교 법학박사
2009년～현재 동국대학교 법학과 겸임교수
연세대학교 정보대학원 박사과정
※ 관심분야 : 개인정보보호, 산업보안, 네트워크 보안