情 報 保 護 學 會 誌
第21卷 第1號, 2011. 2

2010년 모바일 악성코드 동향 분석 및 전망

서 승 현*, 김 종 명*, 전 길 수*

요 약

국내외 스마트폰 가입자 수의 폭발적인 증가는 스마트폰을 활용한 소셜미디어 산업, 생활 밀착형 어플리케이션 개발 산업, 모바일 광고 및 미디어 산업 등 관련 산업의 활성화를 이끌고 있으며, 정부 및 민간 기업에서도 스마트폰을 활용한 모바일 오피스 도입에 관심을 기울이고 있다.

그러나 '손안의 PC'로 불리는 스마트폰은 기존 PC가 가지고 있던 보안 위협 문제들도 내재하고 있으면서 무선인터넷 환경, OS 플랫폼의 개방성, 오픈마켓의 위험성, 도난 및 분실, 위치정보 노출 등의 신규 보안 위협도 존재하기 때문에 이런 취약성들을 활용한 새로운 모바일 악성코드들의 출현될 가능성이 더욱 커졌다. 따라서 본 논문에서는 현재까지 발생한 국내외 모바일 악성코드의 현황을 살펴보고, 2010년에 출현하였던 모바일 악성코드들의 주요 사례를 분석함으로써, 최근 악성코드들의 동향과 향후 전망에 대하여 기술하고자 한다.

Ⅰ. 서 론

방송통신위원회가 2009년 4월 WIPI 탑재 의무화 정책을 해제한 이후, 국내에는 iPhone, 안드로이드폰, 심비안, 블랙베리 등 해외의 많은 스마트폰 들이 출시되고, 스마트폰의 편리함으로 인해 가입자 수가 급격히 증가하여, 2010년 12월 말 기준으로 700만명을 넘어섰다. 특히, 올해는 국내 이통3사와 스마트폰 단말 제조사에서 저가의 보급형 스마트폰을 다수 출시할 계획으로 있어 국내에 스마트폰의 대중화시대가 도래했음을 알리고 있다.

그러나 스마트폰은 3G망, 무선 Wi-Fi, 블루투스 등을 통해 24시간 인터넷에 연결할 수 있기 때문에 편리한 반면, 무작위로 검색되는 보안이 취약한 무선 AP를 이용할 경우 악성코드에 감염될 위험이 있다. 또한 휴대 편의성으로 인해 분실 및 도난율이 높아 스마트폰에 저장되어 있는 개인정보 등이 유출될 수 있으며, 개방형 스마트폰 어플리케이션 마켓을 통해 악성코드가 감염된 스마트폰 어플리케이션이 다운로드될 위협도 존재한다.

지금까지 보고된 국내외 모바일 악성코드는 600여종으로, 국내에서는 2010년 4월 윈도우모바일 스마트폰을 대상으로 한 악성코드가 최초로 발생하였으며, 2011년 스마트폰 대중화 시점과 맞물려 모바일 악성코드의 출현은 더욱 빈번해질 것으로 예상된다.

본 논문에서는 지금까지 발생된 국내외 모바일 악성코드 발생현황을 살펴보고, 2010년 발생되었던 모바일 악성코드 주요 사례 분석을 통해 모바일 악성코드의 최근 동향과 향후 전망을 기술하도록 한다.

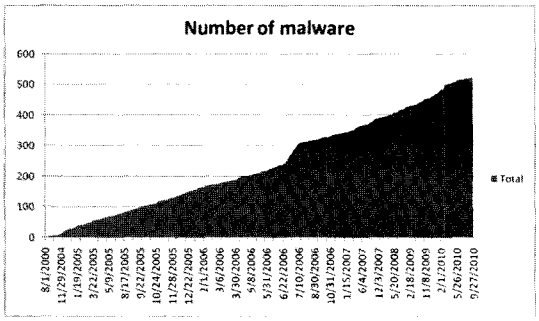
Ⅱ. 국내외 모바일 악성코드 발생현황

모바일 악성코드란 스마트폰 및 모바일 기기 등에서 동작하면서 PC 환경에서와 같이 개인정보 유출, 시스템 손상 등의 악의적인 행위를 유발시켜 사용자에게 피해를 끼치는 악성코드를 말한다.

최초의 모바일 악성코드로 알려진 Cabir가 2004년 8월에 필리핀에서 발견된 이후, 2010년 9월까지 발견된 모바일 악성코드는 총 524종이며, 국내외 보고된 자료들과 악성코드 발생 증가추세로 봤을 때 모바일 악성코드의 수는 2010년 말 기준으로 약 600여종으로 추정된다.

그동안 발생되었던 모바일 악성코드의 유형을 살펴보면, 감염된 스마트폰 내부의 시스템 파일을 삭제하거나 변형시켜 정상동작을 방해하는 시스템 파괴 및 변경 유형, 배터리 소모를 통한 가용성 저하 유형, 과금 피해

* 한국인터넷진흥원 코드분석팀({seosh, jmkim, kschun} @kisa.or.kr)



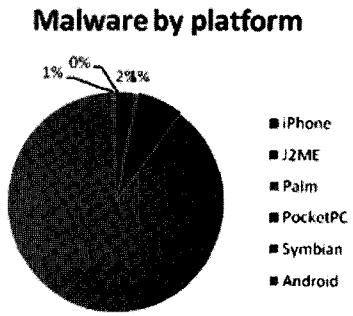
〔그림 1〕 전세계 스마트폰 악성코드 발견 수(누적)
출처: F-Secure

를 유발시키는 악성코드 유형, 스마트폰 기기 정보 및 개인정보 등을 유출하는 유형 등이 있었다.

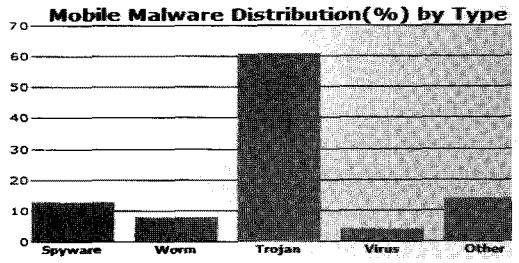
모바일 OS 플랫폼별 악성코드 현황을 살펴보면, 약 89% 이상이 국내 보급률이 미미한 심비안 OS에서 발생하였다.

이는 그동안 전 세계적으로 모바일 OS플랫폼을 주도한 것이 노키아사의 심비안 OS 플랫폼이었기 때문에, 상대적으로 다른 플랫폼들에 비해 악성코드 피해가 많이 발생한 것이라 볼 수 있다. 현재는 아이폰 및 안드로이드 폰 출시로 인해 과거 심비안, RIM, 윈도 모바일이 주도하였던 모바일 OS 플랫폼 시장이 다각화되었으며, 국내에서도 삼성이 신규 스마트폰 OS 플랫폼으로 '바다 OS'를 개발하는 등 계속해서 스마트폰 OS 플랫폼 시장의 경쟁이 심화될 전망이다. 이에 따라 신규 모바일 OS 플랫폼을 겨냥한 악성코드들도 등장하고 있으며, 2010년에 발생하였던 대다수의 모바일 악성코드들이 안드로이드 OS 플랫폼을 겨냥한 것이었다.

그밖에도 발생된 악성코드의 유형을 볼 때 약 60%가 트로이 목마(Trojan)형태이며, 그다음으로 스파이웨어,



〔그림 2〕 OS 플랫폼별 모바일 악성코드
출처: F-Secure



〔그림 3〕 모바일 악성코드 분류, 출처: SMobile Systems

웜, 바이러스 순으로 나타났음을 알 수 있다.

국내의 모바일 악성코드 발생현황을 살펴보면, 2010년 4월 MS 윈도우모바일 플랫폼을 탑재한 스마트폰을 대상으로 국제전화 무단발신을 유발시키는 악성코드가 (WinCE/TerDial) 최초로 발생하였다. WinCE/TerDial로 인해 2010년 3월말 기준, 국내 스마트폰 가입자 수 163만 명 중 155명의 단말기에서 국제전화 발신이 이루어 졌으나 과금 피해는 발생하지 않았다. 그러나 국내 스마트폰 가입자 수가 폭발적으로 증가하고 있기 때문에 해외 모바일 악성코드의 국내 유입 가능성이 증가할 전망이며 이에 따른 모바일 악성코드 침해 사고위협도 커지고 있다.

Ⅲ. 2010년 모바일 악성코드 주요 사례 분석

본 장에서는 2010년에 발생하였던 모바일 악성코드의 주요 사례들을 분석한다.

3.1 WinCE/Terdial

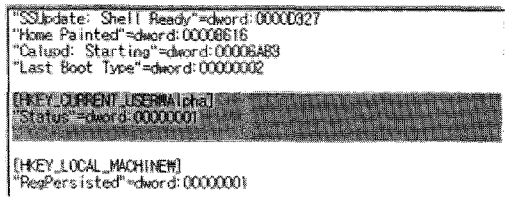
국내에서 최초로 발생하였던 스마트폰 악성코드인 WinCE/Terdial은 러시아 해커가 '3D 안티 테러리스트 액션'이라는 모바일 게임에 악성코드를 은닉하여 유포한 것으로 추정된다. WinCE/Terdial은 윈도우 플랫폼이 탑재된 스마트폰을 타겟으로 하며, 국내에서는 윈도우모바일 이용자 카페 등의 커뮤니티에서 무료 게임으로 유포되었다. '3D 안티 테러리스트 액션' 게임이 설치되면 아래와 같은 위치에 악성코드 파일이 이용자 몰래 설치되며,

\Windows\smart32.exe \Windows\Microsoft.WindowsMobile.Telephony.dll

다음과 같은 레지스트리가 생성된다.

```
키: HKEY_CURRENT_USER\Alpha "Status"
값: 1
```

〔그림 4〕 WinCE/TerDial 악성코드 smart32가 설치된 화면

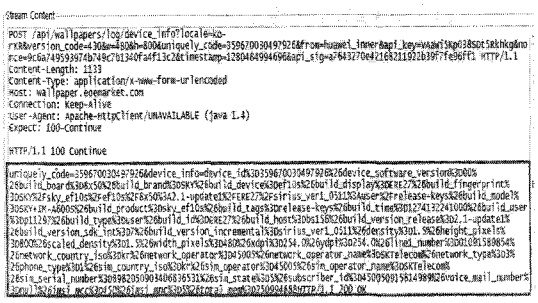


〔그림 5〕 WinCE/TerDial 로 인해 변경된 레지스트리 상태값

악성코드 'smart32.exe'는 레지스트리값(HKEY_CU R RENT_USER\Alpha "Status")을 확인하여, 'Status' 값이 1인 경우 국제전화 발신 루틴을 호출한다. 값이 1이 아닌 경우에는 값을 1로 변경하고 운영체제의 Notification에 'smart32.exe'를 등록하여 약 2일 뒤에 4개의 번호로 50초 간격으로 국제전화를 발신하게 한다. 최초 발신이 끝나면 다시 한달 후에 국제전화를 발신하도록 설정한다. 'Status' 값을 설정하는 이유는 악성코드 최초 감염시 바로 국제전화 발신하지 않음으로써 이용자의 의심을 피하기 위해서 이다.

3.2 개인정보 유출 월페이퍼

2010년 7월 Blackhat USA 2010에서 미국보안업체가 스마트폰의 배경화면을 바꿔주는 무료 월페이퍼 어플리케이션이 400만명에 이르는 이용자의 개인정보를



〔그림 6〕 Jackeey Wallpaper가 전송하는 개인 정보

유출했다고 발표하였다.

문제가 되었던 월페이퍼는 jackeey와 IceskYsl@1sters라는 두 개발자가 개발하여 안드로이드 마켓 및 앱브레인 앱 마켓(AppBrain App Market, 사설마켓 연결용 앱)에 무료로 올렸던 앱으로 앱을 통해 스마트폰 이용자의 휴대전화번호 및 가입자 식별번호, 음성메일함 비밀번호 등을 수집하였다. 해당 월페이퍼는 POST 요청을 통해 아래 [그림 6]과 같이 개인정보를 평문형태로 전송하며, 단말기 하드웨어(디스플레이) 정보 및 소프트웨어 정보, Network Operator, USIM 정보, Voice Mail Number, 가입자 정보 등의 개인정보들이 전송되었음을 알 수 있다.

3.3 Trojan-SMS.AndroidOS

2010년 8월, 구글 안드로이드 OS가 탑재된 스마트폰을 대상으로 하는 SMS 트로이목마 악성코드 Trojan-SMS.AndroidOS.FakePlayer.a가 최초로 등장했다. 해당 악성코드는 org.me.androidapplication1 이라는 패키지명을 가지고 있는데 동영상 플레이어인 "Movie Player"로 위장하였으며 어플리케이션 내에 "Подожди те, запрашивается доступ к видеотеке(잠깐 비디오 라이브러리에 대한 액세스를 요청)"이 포함되어 있는 것으로 보아 러시아 언어권을 목표로 한 것으로 추정된다.

어플리케이션 실행시에는 UI가 보이지 않지만 동작중임은 아래 그림과 같이 확인 할 수 있다.

악성코드가 설치되면 MoviePlayer 클래스가 실행되면서 '3353', '3354', '798657' 등으로 SMS를 전송하여 과금을 유발한다. 이중 '3353'과 '3354'번은 해외 프리미엄 서비스 요금 번호로 알려져 있다.

〔그림 7〕 동영상 플레이어로 위장되어 설치된 Trojan-SMS.AndroidOS

```
local_9 = SmsManager.getDefault();
local_10 = "3353";
local_6 = "90657";
local_8 = null;
local_3 = null;
local_2 = null;
}
try
{
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);
label99: local_10 = "3354";
local_8 = null;
local_3 = null;
label153: local_2 = null;
}
catch (Exception localException2)
{
try
{
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);
local_10 = "3353";
local_8 = null;
local_3 = null;
local_2 = null;
}
catch (Exception localException2)
{
try
{
local_9.sendTextMessage(local_10, local_8, local_6, local_3, local_2);
```

〔그림 8〕 Movie Player 클래스 화면

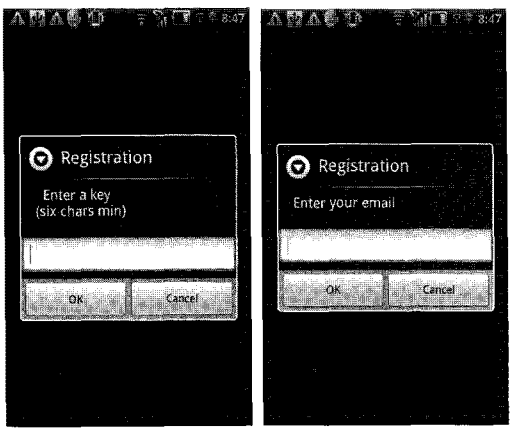
3.4 안드로이드 Tap Snake GPS Spy

2010년 8월, 1970년대 인기를 끌었던 'Tap snake' 게임으로 위장하여 구글 안드로이드 OS가 탑재된 스마트폰을 대상으로 GPS 정보를 유출하는 악성 코드 AndroidOS.Tapsnake가 등장하였다.

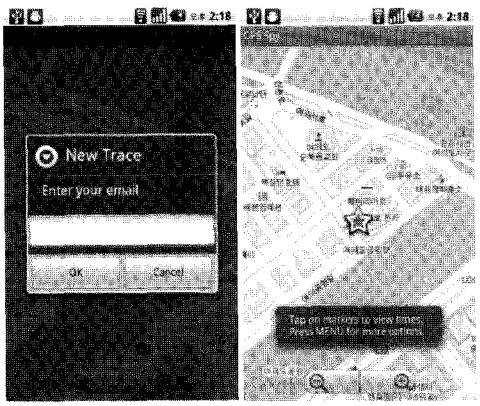
Tap snake 위장 악성어플리케이션은 net.maxicom.android.snake라는 패키지 명을 가지고 있으며, 어플리케이션이 설치시 GPS 정보 사용에 관한 문구가 보여지며, 어플리케이션 종료 후에도 서비스에 등록되어 동작중임을 확인할 수 있다.

해당 악성어플리케이션이 설치되어 실행되면 Registration 메뉴를 통해 이메일과 패스워드 키를 입력하면 사용자의 초기 GPS 정보를 전송하고, 주기적으로 스마트폰 사용자 위치정보 GPS를 업데이트하여 특정 URL (분석을 통해 밝혀진 URL 주소:http://gpsdatapoints.appspot.com/addPoint)에 전송함으로써 사용자의 위치를 추적할 수 있다.

〔그림 9〕 Tap Snake 동작 화면



〔그림 10〕 초기 GPS 정보 전송 화면



〔그림 11〕 위치정보를 이메일로 전송

그러면, 유료 어플리케이션이 'GPS Spy'를 통해 'Tap snake' 악성 어플리케이션에서 입력한 이메일 정보를 통해 위치를 확인할 수 있다.

3.5 Secret SMS Replicator

Secret SMS Replicator는 안드로이드 마켓에서 DLP_Mobile이라는 제작자에 의해서 $9.9에 판매되었던 SMS 감시용 어플리케이션이다. 해당 어플리케이션을 사용하면 스마트폰 문자메시지를 몰래 감시할 수 있어, 미국에서 사생활 침해 논란을 일으키면 2010년 11월에 안드로이드 마켓에서 삭제되었다.

SMS Secret Replicator가 설치되면 안드로이드 스마트폰에 수신되는 SMS를 사전에 설정된 휴대전화 번호로 전송한다. 이때 수신되는 문자메시지를 사용자가 열람하지 못하도록 삭제하는 것은 아니며 단순히 문자메시지를 포워딩하는 형태이다.

Secret SMS Replicator가 설치될 경우 아이콘이 생성되지 않아 스마트폰 사용자는 설치 여부를 인지하기 어렵다.

(그림 12) Secret SMS Replicator가 설치된 화면

Ⅳ. 최근 모바일 악성코드 동향 및 전망

2010년에는 안드로이드 OS 플랫폼을 탑재한 스마트폰을 대상으로 한 악성코드 및 악성 어플리케이션들이 다수 등장하였다. 애플사의 앱스토어와 달리 안드로이드 마켓은 어플리케이션 보안성 검증 절차가 존재하지 않기 때문에, 상대적으로 보안에 취약하며 악성코드들이 일반적인 어플리케이션으로 가장하여 손쉽게 마켓에서 유통될 수 있다.

본 장에서는 2010년에 등장한 모바일 악성코드들의 동향 및 향후 전망에 대하여 기술한다.

4.1 2010년 모바일 악성코드 동향

초창기 모바일 악성코드는 해커의 실력 과시를 위한 개념증명코드(POC: Proof Of Concept)가 대부분이었다.

2008년도부터 금전적 이득을 목적으로 하는 스마트폰 악성코드가 증가하기 시작하여, 2010년에 발생한 스마트폰 대상 모바일 악성코드들의 유형은 큰 범위에서 볼 때 금전적 이득을 목적으로 하는 유형과, 개인 정보 유출을 목적으로 하는 유형으로 나눌 수 있다.

4.1.1 금전적 이득

2010년 4월에, 국내 최초로 발생하였던 스마트폰 악성코드 WinCE/TerDial의 경우가 금전적 이득을 노린 대표적인 악성코드로, 게임으로 위장된 악성코드를 사용자가 다운로드 받아 실행하면 해외 프리미엄 서비스 번호(전화 연결 성공시 일정 금액 결제)로 국제전화를 발신하였다.

또한 안드로이드 스마트폰을 대상으로 한 최초의 트로이 목마 형태의 악성코드 TrojanSMS.AndroidOS.FakePlayer.a 역시, 요금이 결제되는 특정번호로 SMS를 전송하여 피해를 입힌 바 있으며 계속해서 이의 변종 악성코드 TrojanSMS.AndroidOS.FakePlayer.b, TrojanSMS.AndroidOS.FakePlayer.c 들이 출현하였다.

이러한 유형의 모바일 악성코드가 이용자 스마트폰의 SMS를 통해 전파를 시도하거나 요금이 부과되는 3G 네트워크를 이용하여 C&C 서버와 통신할 경우, 이용자에게는 부당한 과금이 부과된다.

4.1.2 개인 정보 유출

SMS 등을 무단으로 발신하여 과금 피해를 직접적으로 입히는 악성코드 이외에도, 인터넷뱅킹, 휴대전화 소액결제, 불법광고, 스토킹 등의 추가적인 범죄를 목적으로 스마트폰에 저장된 개인정보를 유출하는 모바일 악성코드 역시 작년한해 기승을 부렸다.

대표적인 사례로 안드로이드 OS 플랫폼을 탑재한 스

마트폰을 대상으로 한 Jackeey wallpaper(개인정보 유출 월페이퍼)와 AndroidOS.Tapsnake, Secret SMS Replicator 등을 들 수 있다. 이들 악성코드들은 피해자 모르게 피해자 단말기의 정보, 보이스메일 정보, 위치정보, 문자메시지 등을 유출하였다.

24시간 인터넷에 연결되어 있어 언제어디서나 개인 업무를 볼 수 있는 스마트폰은 PC보다 더욱 더 개인화된 정보들(USIM 정보, 전화번호부, 개인일정, SMS, 통화기록, 사진, 이메일, GPS, 회사 기밀, 공인인증서 등)을 저장하고 있기 때문에 정보 유출형 악성코드의 피해를 입었을 때 그 파급효과가 더욱 크다고 할 수 있다.

4.2 모바일 악성코드 향후 전망

앞장에서 살펴본 바와 같이 과금 유도 및 국제전화 무단 발신 등 해커가 금전적인 이득을 노리고 제작·유포한 모바일 악성코드와 개인정보 등을 유출하여 2차적인 범죄에 악용하기 위한 모바일 악성코드 출현이 증가하고 있음을 알 수 있다. 앞으로는 좀 더 지능화된 형태로 스마트폰 뱅킹을 겨냥하여 금전적 이득을 취하고자 하거나 기업정보 유출을 시도하는 악성코드들이 출현될 것으로 예상된다.

4.2.1 스마트폰 뱅킹 공격으로 확산

현재 스마트폰이 인터넷뱅킹 등 금융결제 수단으로 활용되면서 스마트폰 뱅킹 이용자수가 급증하고 있다. 한국은행에 따르면 2009년말 4분기 1만 3천명에 불과했던 스마트폰뱅킹 사용자가 2010년 3분기(9월말 기준)에는 136만 명으로 폭발적으로 증가하였다고 한다.

이에 따라 과거 금전적 이득을 노린 악성코드들이 국제전화 무단발신이나 과금 유도 형이었다면, 앞으로는 본격적으로 스마트폰 뱅킹을 대상으로 한 모바일 악성코드로 진화하여 출현할 것으로 예상된다.

4.2.2 기업정보 유출 시도

2010년 7월, 정부가 스마트워크 활성화를 위해 "스마트워크[1] 인프라 고도화 및 민간 활성화 기반 조성(안)"을 발표하였고 민간업계에서도 스마트폰을 이용한 모바일 오피스 도입을 적극적으로 검토하는 등, 스마트폰을 업무용으로 사용하기 위한 분위기가 확산되고 있다.

그러나 스마트워크는 스마트폰의 개방성과 이용자의 이동성, GPS 등 신규 서비스의 연계로 다양한 보안 취약점에 노출되어 있으며, 현재까지 스마트워크 도입시 가장 큰 위협 요인으로 분류되고 있는 점은 다음과 같다. 첫째, 회사 내부망과 모바일 단말 사이의 통신시 트래픽을 도청하거나 해킹 등을 통해 권한 없는 접근 및 정보 유출이 발생 가능한 문제, 둘째, 스마트폰 단말기 분실로 기업 내부정보 유출 및 내부 업무망 접근이 가능하다는 문제이다.

충분한 보안대책을 고려하지 않고 스마트워크가 도입된다면, 위에서 언급한 취약점을 악용하여 기업의 기밀을 유출하기 위한 악성코드 제작도 늘어날 것으로 예상된다.

4.2.3 악성코드 감염 경로의 다양화

지금까지 보고된 모바일 악성코드는 사회 공학적인 기법을 이용하여 감염된 것이 대다수 였으나 점차적으로 감염경로가 취약점 및 USB 감염 등으로 다양해질 전망이다.

2010년에 발생하였던 WinCE/TerDial, Tapsnake, Jackeey wall paper 등 모두 유용한 어플리케이션으로 위장하여 악성코드들을 유포한 사회공학적 기법에 의한 감염에 해당된다. 이밖에도 이메일이나 MMS의 첨부 파일, SMS이나 SNS 등을 이용한 악성 URL 전송, 공공장소에 악성 URL이 포함된 QR 코드 유포 등 모두 사회공학적인 기법에 의한 악성코드 감염 경로가 될 수 있다.

취약점 이용 기법은 안드로이드 및 아이폰 등 모바일 OS 플랫폼에 존재하는 취약점 뿐만 아니라 웹브라우저, 플래쉬, PDF 등의 어플리케이션 취약점을 활용하여 악성코드를 감염시키는 방법을 말한다. 대표적인 사례로 2009년 11월에 발생한 Ikee 악성코드를 들 수 있는데, Jailbreak된 아이폰을 SSH를 통해 접근하여 설정된 기본 패스워드를 이용해 루트권한을 획득한 후 아래 그림과 같이 바탕화면을 바꾸거나, 악성코드 들을 삽입하는 행위를 할 수 있다.

---

1) 종래의 사무실 개념을 탈피하여 언제 어디서나 편리하게 효율적으로 업무에 종사할 수 있도록 하는 미래지향적 업무환경 개념으로 모바일 오피스, 스마트워크 센터, 재택근무 형태가 있음.

〔그림 13〕 Ikee에 감염된 스마트폰 바탕 화면

마지막으로 스마트폰이 데이터 백업 및 음악, 동영상 등의 이동을 위해 PC와 USB로 연결될 때, PC에서 스마트폰으로 악성코드를 설치하여 실행할 수 있는 USB 감염 기법이다. 지금까지 USB 감염을 통한 모바일 악성코드 출현은 보고된 바가 없으나, 모바일 악성코드 제작의 진화와 감염경로의 다양화 시도 등으로 비추어 볼 때 발생 가능성이 높다고 할 수 있다.

V. 결 론

스마트폰은 생활밀착형 컨텐츠 등을 통한 개인 생활의 편이성을 증대시켰고, 언제어디서나 인터넷이나 이메일 서비스, SNS 및 블로그 등을 이용할 수 있어 실시간 소통 채널을 다양하게 만드는 등 개인 이용자 생활에 큰 변화를 가져왔다. 기업에서도 스마트폰과 연계한 모바일 오피스 도입을 통해 업무 효율성 및 비용절감의 효과를 누리고 있다.

그러나 스마트폰은 다양한 무선인터넷 접속 환경, 개방형 스마트폰 어플리케이션 마켓을 통한 악성 어플리케이션의 유통 위협, 도난과 분실 등 기존 PC와는 다른 새로운 보안 위협요소들이 존재하며, 이로 인한 모바일 악성코드의 피해사례도 점차 증가될 전망이다. 또한 악성코드 감염 경로가 다양해지고, 스마트폰 뱅킹 및 기업 정보 유출을 노린 모바일 악성코드들도 등장할 것으로 예상된다. 따라서 스마트폰 보안 위협에 대응하기 위해서는 민·관 합동의 유관기관 공조체제를 운영하면서 모바일 악성코드 감염경로를 모니터링하여 조기탐지 하고, 침해사고 피해 유형별 대응방법을 마련하여 체계적으로 대응할 수 있는 방안을 마련 해야한다. 이와 더불어 무선랜 AP의 보안관리 강화, 불법적인 위치정보 측위 방지, 스마트폰 전용 백신 등 보안솔루션 개발 활성화, 분실 및 도난을 대비한 원격제어 서비스 및 잠금장치 등의 방안 마련 등 제도적·기술적 방안들이 마련되어야 한다. 이러한 노력들이 스마트폰 대중화 시대를 맞아 안전하고 편리한 스마트폰 이용환경을 만들기 위한 초석이 될 것이다.

참고문헌

[1] 심재홍, 이석래, "모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석," *한국정보보호학회지*, 19권 6호, pp. 41-48, 2009년 12월

[2] 서승현, 전길수, "스마트폰 보안 위협 및 대응 전략," *TTA 저널, 132호, pp 44-48*, 2010.

[3] http://www.f-secure.com/weblog/archives/0000 1930.html

[4] http://www.kaspersky.com/news?id-207576152

[5] http://www.symantec.com/business/security_response/writeup.jsp?docid=2010-081214-2657-99

[6] http://www.securelist.com/en/blog/2286/Android _SMS_Trojan_Now_Being_Delivered_via_SEO_Techniques

[7] http://www.securelist.com/en/blog/329/FakePlayer_take_3

[8] http://www.flexispy.com/spyphone-flexispy-android.htm

[9] http://news.donga.com/3/all/20110116/33983014/1

〈著者紹介〉

서 승 현 (Seung-Hyun, Seo)
종신회원

2000년 2월 : 이화여자대학교 수학과 이학사
2002년 2월 : 이화여자대학교 과학기술대학원 컴퓨터학과 석사
2006년 2월 : 이화여자대학교 과학기술대학원 컴퓨터학과 박사
2006년 5월 ~ 2006년 11월 : 고려대학교 정보보호대학원 연구전임강사
2006년 12월 ~ 2010년 2월 : 금융보안연구원 주임 연구원
2010년 2월 ~ 현재 : 한국인터넷진흥원 코드분석팀 선임연구원
관심분야 : 모바일 보안, 악성코드 분석, 금융 보안

김 종 명 (Jong-Myoung Kim)
정회원

2007년 2월 : 성균관대학교 정보통신공학과 공학사
2009년 2월 : 성균관대학교 전자 전기컴퓨터공학과 석사
2009년 1월 ~ 현재 : 한국인터넷진흥원 코드분석팀 주임연구원
관심분야 : 모바일 악성코드 분석, 스마트폰 보안, 모바일 포렌식

전 길 수 (Kilsoo Chun)
종신회원

1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 수학과 이학석사
1998년 2월 : 서강대학교 수학과 이학박사
1998년 10월 ~ 1999년 9월 : 서강대학교 기초과학연구소 박사후연구원
2001년 3월 ~ 2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월 ~ 2009년 7월 : 한국정보보호진흥원 팀장
2009년 7월 ~ 현재 : 한국인터넷진흥원 팀장
관심분야 : 암호학, ID관리, 모바일 보안