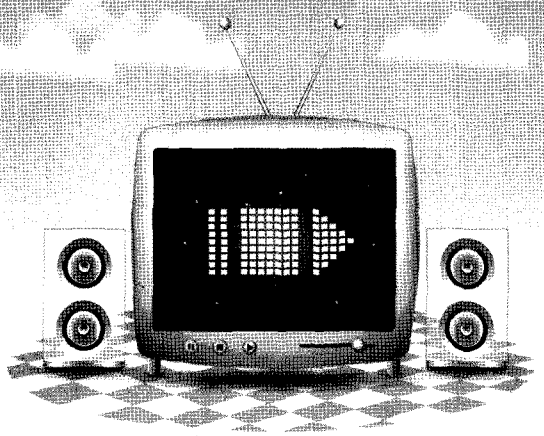
스마트폰 보안 위협 및 대응 전략



서승현 | KISA 코드분석팀 선임연구원
전길수 | TTA PG502 부의장, KISA 코드분석팀장

1. 머리말

2009년 4월, 방송통신위원회가 해외 스마트폰의 국내 도입장벽 역할을 했던 WIPI 탑재 의무화를 해제하면서, 애플사의 아이폰(iPhone), 구글사의 안드로이드폰 등 해외의 많은 스마트폰들이 국내에서 출시되었다. '손안의 PC' 라고 불리는 스마트폰은 언제 어디서든 인터넷접속이 가능해 SNS(소셜네트워크서비스), 증강현실, 내비게이션 등 생활 밀착형 콘텐츠를 통한 개인의 생활 편의성을 증대시켰다. 기업들은 스마트폰을 활용하여 모바일 오피스를 구축함으로써 업무 효율성 증대 및 비용 절감의 효과를 누리고 있다. 이에 국내 스마트폰 가입자는 2009년 12월 기준으로 100만 명을 돌파하였으며, 2010년 9월, 약 434.9만 명으로 4배 이상 증가했다. 그러나 개인의 중요 정보가 저장되어 있으면서 손안의 PC로서의 역할을 하는 스마트폰은 24시간 인터넷과 연결되어 있는 특성과 휴대성으로 인해 새로운 보안 위협에 노출되어 있다. 이미 해외에서는 600여 종의 스마트폰 악성코드가 발견된 것으로 추정되며, 최근 국내에서도 윈도우모바일 스마트폰을 대상으로 한 악성코드가 발생했다. 스마트폰이 활성화될수록 스마트폰의 보안 위협을 이용한 악성코드들의 제작 및 유포가 증가될 전망이라 사용자의 주의가 요구된다. 본 고에서는 스마트폰의 보안 위협 요소, 모바일 악성코드 유형, 국내에서 발생되었던 스마트폰 악성코드 및 구글 안드로이드폰을 겨냥한 악성코드를 살펴보고, 스마트폰 보안위협에 대한 대응현황 및 방향을 소개한다.

2. 스마트폰 보안 위협 요소

2.1 무선인터넷 접속 환경

스마트폰은 3G 이동통신망뿐만 아니라, 무선랜(Wi-Fi) 및 블루투스 기능이 기본적으로 탑재되어 있어 공중 무선랜이나 사설 무선랜의 이용 빈도가 높으며, 스마트폰 사용자들은 무선데이터 요금을 아끼기 위해 무작위로 검색되는 무선 AP를 이용하는 사례도 늘고 있다. 만약 해커가 악의적인 의도를 가지고 악성코드를 심어놓은 무선 AP를 제공한다면, 스마트폰 사용자는 이러한 무선 AP에 접속하는 것만으로도 악성코드에 감염될 수 있다. 따라서 스마트폰의 무선인터넷 접속환경은 유해한 사이트에 방문해야 악성코드에 감염되었던 기존 PC 환경보다 악성코드 유입이나 해킹 공격 등

이 용이한 환경이라 할 수 있다.

2.2 스마트폰의 개방성

스마트폰이 일반 휴대폰과 구분되는 가장 큰 특성은 개방성이다. 즉, 일반 휴대폰과 다르게 무선인터넷 및 외부 인터페이스를 개방하여 제공하고 있고, 애플리케이션 개발시 시스템 자원의 사용을 위한 API를 제공하고 있다. 스마트폰의 다양한 외부 인터페이스는 사용자가 손쉽게 네트워크 서비스를 이용할 수 있도록 지원하고, 내부 API 인터페이스 제공은 개발자가 편리하게 개발할 수 있는 환경을 제공한다. 하지만 다양한 외부 인터페이스 제공은 악성코드 전파경로가 다각화되어 악성코드가 쉽게 퍼지는 결과를 가져왔으며, 내부 인터페이스는 악의적인 개발자가 모바일 애플리케이션에 악성코드를 쉽게 은닉하여 제작할 수 있도록 만들었다.

2.3 개방형 스마트폰 애플리케이션 마켓

스마트폰은 구글 안드로이드 마켓 등 개방형 스마트폰 애플리케이션 마켓을 통해 누구든지 콘텐츠 제작과 유통, 사용이 가능하여 악성코드가 삽입된 애플리케이션 유통위협이 존재한다. 실제로 국외 스마트폰 애플리케이션 마켓(사이디아)에서 판매된 온라인 뱅킹 프로그램이 금융사기에 활용된 사례가 있었다. 현재 국내외 스마트폰 애플리케이션 마켓들의 보안성 검증 체계가 미흡한 상황으로 악성코드에 감염된 스마트폰 애플리케이션이 유통될 위협이 존재한다.

2.4 도난과 분실

스마트폰은 휴대 편의성으로 인해 분실 및 도난율이 높으며, 작년 한해 스마트폰을 포함한 휴대폰의 분실 및 도난 건수가 총 233만 5천 건으로 월평균 20만 대에 이르고 있다. 스마트폰은 개인 연락처, 문자전송 내역은 물론 위치정보, 이메일, 전자결재, 기밀정보 등 개인 사생활과 업무 관련 중요 정보를 가지고 있어, 이를 분실하거나 도난당할 경우 유출된 정보는 보안사고뿐만 아니라 심각한 사회문제를 야기할 수도 있다.

3. 스마트폰 악성코드 유형 및 사례 연구

3.1 스마트폰 악성코드 유형

스마트폰 악성코드란 스마트폰에서 동작하면서 시스템을 파괴하거나 저장된 개인정보 등을 유출하는 악의적 활동을 수행하는 코드이다. 스마트폰을 공격하는 악성코드는 대부분은 스마트폰 기기의 기능을 마비시키거나 스마트폰 내에 저장된 정보의 유출 및 금전적 이익을 취하는 것을 목적으로 하고 있다.

3.1.1 단말 장애 유발형 악성코드

스마트폰 기기에 장애를 불러일으키거나 심한 경우 사용자체를 불가능하게 하는 악성코드의 유형이다. 2004년에 발견된 스마트폰 악성코드 중의 하나인 해골(Skull)이 대표적인 단말장애 유발형 악성코드로 스마트폰의 모든 메뉴 아이콘을 해골로 변경시키고 통화 기능 외의 모든 기능을 마비시켰다.

3.1.2 배터리 소모형 악성코드

스마트폰의 전력 사용을 지속적으로 유발해 결국에는 배터리를 고갈시키는 목적을 가지는 악성코드들이다. 2004년에 블루투스를 통해 전파되었던 최초의 모바일 악성코드인 Cabir가 대표적인 배터리 소모형 악성코드이다. Cabir는 기기의 침해를 유발하기 보다는 지속적으로 근처 기기의 블루투스 장치를 스캐닝하고, 검색된 블루투스를 통해 악성코드를 전파하는 기능을 가지고 있었다. 결국 감염된 기기는 지속적인 스캐닝을 통해 배터리 고갈의 피해를 입게 된다.

3.1.3 과금유발형 악성코드

스마트폰의 SMS 서비스나 송신 서비스를 지속적으로 시도하여 과금을 발생시키는 악성코드유형이다. 2006년 러시아에서 제작된 J2ME 플랫폼용 RedBrowser가 대표적인 과금 유발형 악성코드이다. 감염된 기기는 사용자도 모르게 불특정 다수에게 SMS 및 송신을 함으로써 이용자에게 금전적으로 피해를 입히는 악성코드이다. 2010년 4월, 국내에서 최초로 발생한 스마트폰 악성코드인 WinCE/TerDial은 게임 내에 숨겨진 형태로 존재하면서 국제전화를 송신해 사용자에게 피해를 입히는 시도를 했다.

3.1.4 정보유출형 악성코드

악성코드에 감염된 스마트폰 기기의 정보나 사용자의 개인정보를 외부로 유출시키는 악성코드유형이다. 2008년 발견된 Infojack은 합법적으로 애플리케이션이 기기에 다운로드 될 때 설치파일과 함께 설치되고난 후, 외부의 특정 웹서버에 접속하여 악성코드의 나머지 부분을 다운로드하여 재설치하는 지능적인 수법을 썼다. 일단 악성코드가 설치되고 나면 기기의 보안설정을 변경하고 기기의 정보를 외부로 전송하여 추가적인 공격을 용이하게 하였다. 최근 구글 안드로이드폰을 겨냥한 AndroidOS.Tapsnake도 사용자의 위치정보를 빼가는 악성 스파이웨어이다.

3.1.5 크로스 플랫폼형 악성코드

스마트폰을 통해 PC를 감염시키는 악성코드유형으로 2005년에 발생된 Cardtrap.A가 최초의 크로스 플랫폼형 악성코드이다. Cardtrap은 기기의 메모리카드에 웜을 복사하여, 감염된 메모리카드를 PC에 장착했을 때 autorun 기능을 통해 PC를 자동으로 악성코드에 감염시키는 기능을 했다.

3.2 악성코드 사례연구

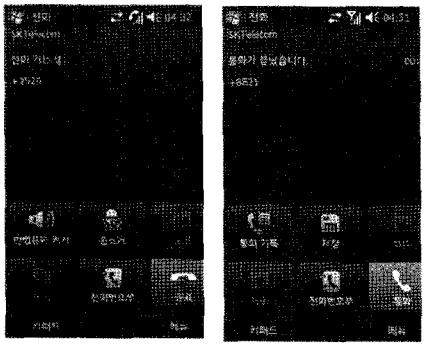
현재까지 보고된 스마트폰 악성코드는 대략 600여 종으로 90% 이상이 심비안 OS를 탑재한 스마트폰에서 발생하였다. 국내에서는 지난 4월, 윈도우 모바일 스마트폰 사용자를 대상으로 국제전화 무단발신을 유발시키는 악성코드 WinCE/TerDial이 최초로 발견된 바 있으며, 국외에서 구글사의 안드로이드 OS를 탑재한 스마트폰을 대상으로 한 악성코드 출현이 계속적으로 늘어는 추세이다. 본 장에서는 국내에서 최초로 발생한 스마트폰 악성코드 WinCE/TerDial과 안드로이드 대상 악성스파이웨어에 대한 분석내용을 소개한다.

3.2.1 WinCE/TerDial

WinCE/TerDial은 '3D Anti Terrorist Action' 이라는 게임에 트로이목마 형태로 악성코드가 숨겨져서, 게임이 설치되는 시점에 스마트폰을 감염시킨다. [그림 1]에서 보는 것처럼 사용자가 해당 게임을 설치하면 사용자도 모르게 악성코드 Smart32.exe파일과 Microsoft.WindowsMobile.Telephony.dll파일이 설치된다.

[그림 1] WinCE/TerDial 감염되어 악성코드가 설치된 상태

악성코드가 설치되고 나면 [그림 2]와 같이 자동으로 해외 premium-rate number(Quiz Show, 투표 등에 사용되는 번호로 분당 과금을 취하는 전화서비스)에 국제전화를 시도하여 과금을 부과시킨다.



[그림 2] 무단으로 국제전화 시도하는 화면

3.2.2 AndroidOS.Tapsnake

AndroidOS.Tapsnake는 'Tap snake' 게임으로 위장하여 GPS 위치정보를 빼가는 악성스파이웨어로 구글 안드로이드 OS가 탑재된 스마트폰에서 동작한다. GPS 정보를 전송하는 모듈이 Tap snake 안에 들어있으며 백그라운드 형태로 실행되면서 스마트폰 사용자의 위치정보를 특정 URL에 전송하여 'GPS Spy'를 설치한 사용자가 위치를 추적할 수 있도록 한다.

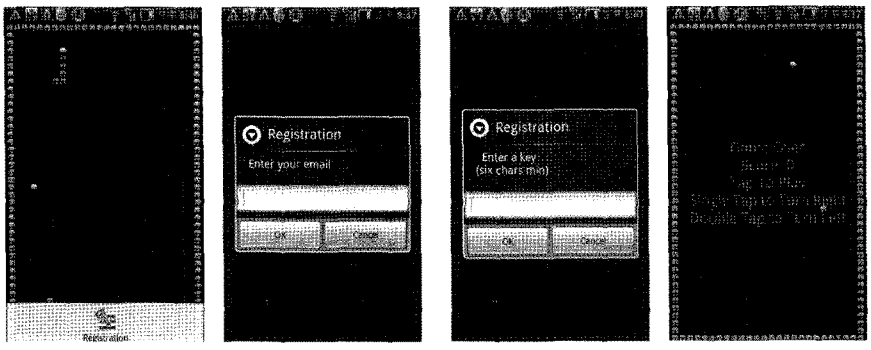
[그림 3]과 같이 사용자가 Registration 메뉴를 통해 이메일과 패스워드 키를 입력하면 사용자의 GPS 정보를 전송한다.

악의적인 의도로 상대방의 위치정보를 확인하기 위해, 유료 애플리케이션 'GPS Spy'를 설치한 사용자는 'Tap Snake' 사용자가 Registration 메뉴를 통해 입력한 이메일 정보를 입력하여 피해자의 위치정보를 확인할 수 있다.

[그림 4] 피해자 스마트폰의 GPS 정보가 노출되는 화면

4. 스마트폰 침해대응 현황 및 방향

스마트폰 침해사고에 신속하게 대응하고 보안위협을 완화하기 위해서는 유관기관 협력 체계 구축, 보안 기술 개발, 관련 제도 정비, 사용자 보안인식 제고 등의 노력이 필요하다. 현재 방송통신위원회와 KISA는 유관기관 및 관련업체와 함께 '스마트폰 정보보호 민·관 합동대응반'을 구성하여 스마트폰 침해사고 공동 대응 모의 훈련을 실시하고, 지속적으로 국내외 모바일 침해사고에 대한 모니터링을 수행하면서 사고 예방책과 대응방안을 마련 중에 있다. 또한 산·학·



[그림 3] Tap snake를 설치하여 이메일 및 패스워드 정보를 입력하는 화면

연 · 관 전문가를 중심으로 한 '모바일시큐리티포럼'을 구성해 스마트폰을 비롯한 모바일 보안 전반에 관련된 체계적인 연구 계획과 대책을 수립 중에 있다.

'스마트폰 정보보호 민 · 관 합동대응반'은 2010년 2월, 스마트폰 사용자의 보안인식 제고를 위해 '스마트폰 이용자 10대 안전수칙'을 발표했다. 2010년 6월, 스마트폰 이용자, 이통사, 제조사, 백신사 및 정부기관을 대상으로 한 정보보호 주체별 스마트폰 침해사고 대응 절차 안내서를 개발했다. 또한 침해사고 긴급대응체계를 상시 운영하여 2010년 4월, 국내 최초로 스마트폰 악성코드가 발생했을 때에도 신속히 대응하여 피해확산을 방지한 바 있다.

스마트폰 보안위협에 대응하기 위해서는 유관기관 공조체제 운영과 더불어 다음과 같은 제도적 방안과 기술적 방안들이 기본적으로 마련되어야 한다. 첫째, 무선랜 AP를 통해 스마트폰 악성코드가 감염되지 않도록, 안전한 무선랜 환경을 조성하기 위한 제도적 방안을 마련하고 무선랜 AP의 보안관리를 강화해야 한다. 둘째, 스마트폰 애플리케이션 마켓에서 악성 애플리케이션이 유통되지 않도록 마켓에서 판매되는 애플리케이션에 대한 보안성 검증을 강화할 수 있는 제도가 마련되어야 한다. 이를 위해서는, 스마트폰 애플리케이션 보안 검증 기술 개발 및 마켓 보안성 검증 체계 구축 등이 선행되어야 하며, 국내 스마트폰 애플리케이션 환경에 적합한 코드서명기술을 개발하여 개발자의 신원확인을 통한 애플리케이션의 신뢰성을 확보해야 한다. 셋째 위치 기반 서비스에 의한 GPS 노출 및 사생활 침해 예방을 위해서 불법적인 개인 위치정보 측위 방지, 수집된 위치 정보의 용도 외에 사용금지 및 파기방안이 마련되어야 한다. 넷째, 안티바이러스 및 스마트폰 전용 백신 등의 보안 솔루션 개발을 활성화하고 제조 단계부터 백신을 탑재하는 등의 스마트폰 사용자들의 백신 이용률을 높일 수 있는 방안들을 모색해야 한다. 마지막으로 분실 및 도난을 대비하여 원격제어 서비스, 폰잠금 장치, 중요 데이터 암호화를 위한 초경량 암호알고리즘 기술 등이 개발되어야 한다.

5. 맺음말

본 고에서는 스마트폰 보안위협의 주요 요인들, 모바일 악성코드 유형 및 최근 발생된 스마트폰 악성코드 사례 등을 살펴보고, 현재 정부에서 추진중인 스마트폰 보안위협 대응 방향에 대해서 소개했다. 언제 어디서나 인터넷에 접속하며 다양하고 편리한 기능들을 제공해주는 스마트폰은 유관기관 공조체제를 통한 신속한 사고대응, 이용자 보안 의식 제고, 정부의 보안정책, 유관기관들의 기술개발 노력들이 합쳐진다면 유비쿼터스 사회를 실현하는 주요한 도구로 우리 생활에 자리잡을 것이다.

[참고문헌]

[1] TTA(www.tta.or.kr), 표준화전략맵, '네트워크&시스템보안-4차-배포자료', 2010.09.03

[2] TTA(www.tta.or.kr), '응용보안 평가인증 보고서', 2010.11.01

[3] ITU-T, 'Security aspects of mobile phones', T09 SG17 100407 TD PLEN 1012, 2010.04.16

[4] ITU-T, T REC Y.Sup8-201001-1 , 'Supplement on a survey of global ICT forums and consortia', 2010.01

[5] Microsoft, http://msdn.microsoft.com/en-us/library/ms537361.aspx

[6] Apple, http://developer.apple.com/, 'code signing guide', 2009.10.13

[7] Google Android, http://developer.android.com/, http://developer.android.com/guide/publishing/app-signing.html

TTA