# 스마트 폰 보안의 위협과 실태

손영수*, 황선호*, 조성환*, 이광우*, 김종성*
*경남대학교 e-Business학부
e-mail:neche123@naver.com

# Smartphone Security Threats and Reality

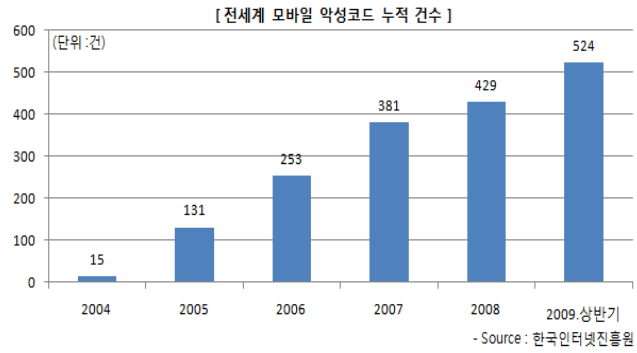
Young-Su Son*, Seon-Ho Hwang*, Seong-Hwan Cho*,
Gwang-Woo Lee*,Jong-Sung Kim*
*Division of e-Business, Kyungnam University

요 약

21세기 초부터 휴대폰으로 인터넷에 접속하는 다양한 서비스가 제공되었으며 스마트폰 사용량은 급증하였고 위협요소 또한 많아졌다. 본 논문은 스마트 폰을 위협하는 악성코드의 종류와 감염경로를 파악하고 그 사례를 통해 문제점을 제시한다.

## 1. 서론

정보기술(IT)의 출현 이래로 바이러스, 해킹, 정보유출 등의 보안 문제는 여전히 해결해야 될 숙제이다. 최근 유비쿼터스에 의해 단독적으로 활용하던 정보자원들을 네트워크를 통해 공유하고, 과거의 데스크톱과 서버 환경이 강력한 유무선 통신기술로 인해 다양한 장치 기반의 모바일 환경으로 확대됐다. 때문에 보안 이슈는 그 범위가 걷잡을 수 없이 커져가고 있다. 이제는 휴대폰에서조차 바이러스를 걱정해야 하는 시대가 된 것이다. 현재 인터넷 환경은 다양한 미디어 콘텐츠를 양방향으로 자유롭게 소비, 활용, 생산하는 이용자 참여 중심이다. 이에 따라 단순한 데이터뿐만 아니라 애플리케이션, 사용자 컨텍스트 정보, 단말상황 정보 등이 고수준(서비스 수준)에서 사용자가 인지하지 못하는 사이에 전파돼 정보가 유출, 침해될 확률이 높아지고 있다.




(그림 1) 모바일 악성코드 누적 건수 [1]

## 2. 본론

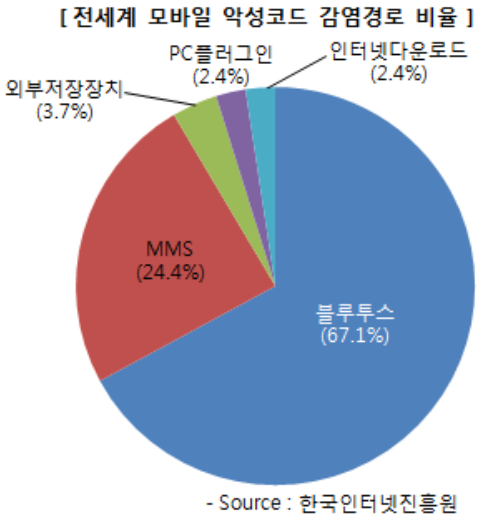
스마트 폰의 대표적 위험 요소로는 분실(Lost), 악성코드 감염(Infect Malware), 정보 유출(Data Steal), 금전적 손실(Monetary Loss), 공격지 활용(Attack Others)가 있으며, 그 중 악성코드 감염이 가장 문제가 되고 있다.

스마트 폰은 플랫폼마다 다른 악성코드가 존재한다. 첫 번째로 노키아의 심비아는 3가지 유형으로 나누어 진다. 단말 장애형 악성코드인 Skulls, Cardblock, 와 정보유출형 PBstealer 그리고 과금 유발형인 Commwarriar, RedBrowser가 있다. 두 번째로는 MS의 윈도우 모바일의 Infojack과 TredDial이 있는데 그 중 TredDial은 국내 최초의 스마트 폰 악성코드 이다. 세 번째론 아이폰 OS의 ikee, Privacy A, iBotNet이 있고, 마지막으로 구글의 안드로이드는 악성코드 은닉 애플리케이션(Royal Bank of Canada)이 있다.

<표 1> 각 플랫폼의 악성코드 종류와 특징 [2]

| 악성코드 | | 특징 |
|---|---|---|
| 노키아 심비아 | Skulls | • 단말 장애형 악성코드<br>• 에플리케이션 삭제 및 재부팅 시도 |
| | Cardblock | • 단말 장애형 악성코드<br>• 애플리케이션 및 데이터 삭제 시도 |
| | PBstealer | • 정보 유출형 악성코드<br>• Phonebook Stealer<br>• 전화번호 유출 시도 |
| | Commwarriar | • 과금 유발형 악성코드<br>• 주소록 연락처를 이용한 MMS 메시지 전송 시도 |
| | RedBrowser | • 과금 유발형 악성코드<br>• 프리미엄 메시지 전송 시도 |
| MS 윈도우 모바일 | Infojack | • 정보 유출형 악성코드<br>• 단말 보안설정 변경 및 단말 정보 전송 시도 |
| | TredDial | • 과금 유발형 악성코드<br>• 국내 최초의 스마트 폰 악성코드<br>• 50초마다 국제 전화 시도 |
| 아이폰OS | ikee | • 탈옥(Jailbroken) 단말<br>• 배경 화면을 유명 가수 사진으로 변경 |
| | Privacy.A | • 정보 유출형 악성코드<br>• 탈옥(Jailbroken) 단말<br>• 개인정보(문자메시지, 이메일 등) 유출 시도 |
| | iBotNet | • 단말 장애형 악성코드<br>• 탈옥(Jailbroken) 단말<br>• DDOS공격을 위한 좀비 단말에 활용 |
| 구글 안드로이드 | Royal Bank of Canada | • 정보 유출형 악성코드<br>• 모바일 뱅킹 프로그램으로 가장하여 정보 유출 |

이러한 악성코드들은 다양한 경로를 통하여 유입이 되는데 대부분 블루투스를 통해 유입되는 것으로 보고되고 있다. MMS에 의한 감염도 24.4%나 차지하고 있다.




(그림 2) 모바일 악성코드의 감염경로 비율 [3]

MS Windows Mobile 운영체제에 기반한 악성코드 'TredDial'은 지난해 4월 발견된, 금전적 피해를 입힌 국내 최초의 악성코드다. 'TredDial'은 모바일 게임과 동영상 관련 유틸리티 등에 포함되어 퍼지며, 원격으로 외국 전화번호로 음성전화와 데이터 서비스를 걸게 만드는 특징을 가진다. 이로 인하여 피해자는 50초마다 국제전화가 걸리는 이상 현상을 겪었다. 또한 악성코드가 발견된 6일 후, 변종이 추가로 발견되어 불편을 주는 등 변종으로 인한 피해가 발생했다.

Google Android 경우 Application을 통한 악성코드 유포가 활발히 이루어지고 있다. 'sexy girls' 나 'sexy legs' 같은 선정적 제목으로 다운로드를 유발하여 "통화 상태" 등의 휴대폰 이벤트 상태가 변경될 경우, IMEI[1]/IMSI[2] 값과 단말기에 설치되어 있는 OS버전, 설치된 모든 Application 정보 등과 같은 스마트폰 단말기 정보를 취득한다. 이러한 Application은 안드로이드 마켓을 통해 유포되고 있었으나 현재는 다운로드 및 설치가 불가능하도록 조치해두었다. 하지만 Application 배포의 특성상 블랙마켓, 3rd party 마켓 등을 통해서 여전히 유포가 되고 있는 실정이다.

## 3. 결론

개인의 보안수준은 기업에 비해 낮을뿐더러 보안시장조차 활성화 되지 않고 있다. 또한 개인을 대상으로 한 모바일 보안 시장이 활성화되려면 시간이 걸릴 것이다. 그러므로 개인적인 차원의 예방이 시급하다.

기업의 모바일 보안 대책으로는 현재 모바일 통합 보안 솔루션을 이용하여 위험 요소로부터 보안을 할 수 있다. 현재는 OS에 따라 제공된 보안기능에는 차이가 있지만, Enterprise Mobility가 활성화 되면서 구글과 애플이 기업의 다양한 요구사항을 수용하기 위해 API를 개방하고 라이센스를 확대하는 등 발 빠른 움직임을 보이고 있어 이러한 문제는 곧 해결될 것으로 보인다.

사용자가 컴퓨터나 네트워크를 의식하지 않고 장소에 상관없이 자유롭게 네트워크에 접속할 수 있는 환경이 도래했다. 기업은 각 플랫폼에 따른 악성코드의 종류와 특징을 잘 분석하여 피해를 줄이고, 개인은 스마트폰의 보안에 대해 많은 관심과 노력이 필요하다.

1) IMEI(International Mobile Equipment Identity : 국제 모바일 단말기 인증번호)

2) IMSI(International Mobile Subscriber Identity : 국제 모바일 가입자 인증번호)

### <참고문헌>

[1]한국인터넷진흥원

[2]유효선, "모바일 보안 위협과 대응방안", 정보과학회지 제28권 제6호 통권 제253호

[3]한국인터넷진흥원

[4]강동호 외 3명"모바일 보안 및 보안서비스 기술동향" 2010.06

[5]성연광 외 1명 "머니투데이 IT과학" 2011.09

[6]허종오, "모바일 보안",안철수 연구소 ASEC

[7]전자통신동향분석 제 23권 제 4호 2008.8