情 報 保 護 學 會 誌
第19卷 第 6號, 2009. 12

모바일 인터넷 정보보호를 위한 모바일 악성코드 동향 분석

심 재 홍*, 이 석 래**

요 약

최근 국내는 물론 전 세계적으로 스마트폰을 이용한 인터넷 이용인구의 증가에 따라 스마트폰과 모바일 악성코드에 대한 관심이 높아지고 있으며, 해외에서는 심비안, 윈도우 모바일이 탑재된 스마트폰을 대상으로 600여종의 모바일 악성코드가 발생하고 있어 이에 대한 대응이 필요하다. 따라서 본 고에서는 국내 모바일 악성코드의 발생에 대비하기 위하여 해외 현황 및 주요 침해사고 유형에 대해서 분석하고자 한다.

Ⅰ. 서 론

스마트폰은 음성통화 및 메시지 송·수신 기능만을 제공하던 휴대폰과 달리 모바일 결제, MP3, 카메라, DMB, GPS, 인터넷 등을 포함한 다양한 기능을 제공한다. 특히, 블루투스, 무선랜(Wi-Fi) 및 무선네트워크(HSDPA, Wibro 등)를 통한 접속이 언제든지 가능하기 때문에 미래 유비쿼터스(Ubiquitous) 환경에서의 유용한 인터넷 접속도구가 될 것이다.

2008년 12월 10일 방송통신위원회는 2009년 4월 1일을 기점으로 해외 스마트폰의 국내 도입장벽 역할을 했던 위피(WIPI)의 휴대전화 탑재 의무화를 해제하기로 결정했다. 이로 인해 MS社 윈도우모바일폰, Nokia社 Symbian폰, Apple社 iPhone, RIM社 Blackberry폰, 구글社 안드로이드폰을 포함한 많은 해외 스마트폰이 국내 휴대폰 시장에 도입되고, 특히, 개방형 플랫폼 기반의 다양한 스마트폰이 출시되어 시장 경쟁이 치열해 질 것으로 예상할 수 있으나, 이는 해외에서만 발생해 왔던 모바일 악성코드에 의한 피해가 곧 국내에서도 발생할 수 있다는 것을 의미한다.

Ⅱ. 스마트폰 현황

스마트폰은 글자 그대로 똑똑한(Smart) 휴대폰(Phone)이라는 의미를 내포하고 있다. 전 세계적으로 휴대폰 생산량은 감소하는 반면 스마트폰은 증가하고 있는데 이러한 추세는 가속화 될 것으로 전망하고 있다. 이러한 현상은 통신서비스 이용자들이 스마트폰을 이용하여 기본적인 통신서비스를 이용함은 물론 모바일 인터넷을 이용하여 장소에 구애받지 않고 인터넷을 접속하고자 하는 욕구가 반영된 것으로 볼 수 있다.

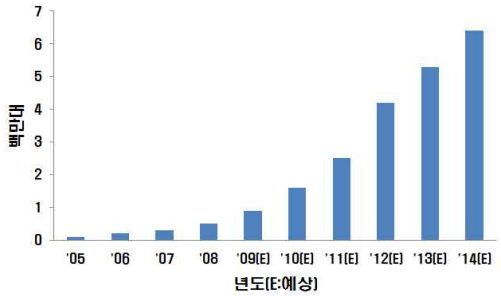
[표 1] 스마트 폰 판매 현황 (출처:가트너 '09.2Q)

제조사	판매대수 (천대)	시장 점유율 (%)
Nokia	18,441.0	45.0%
RIM	7,678.9	18.7%
Apple	5,434.7	13.3%
HTC	2,471.0	6.0%
후지쯔	1,249.0	3.0%
Others	5,688.2	13.9%
Total	40,962.8	100%

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT R&D 사업의 일환으로 수행하였음. [2009-F-054-01, 유해 멀티미디어 콘텐츠 분석/차단 기술 개발]

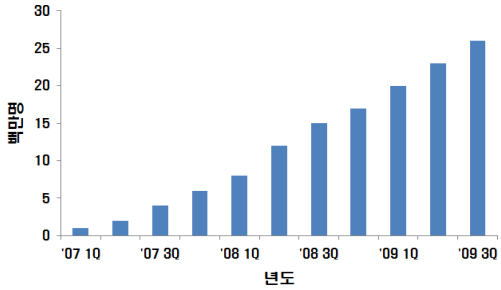
* 한국인터넷진흥원(KISA) 코드분석팀
** 한국인터넷진흥원(KISA) 코드분석팀

해외 시장조사 전문기관 Gartner의 자료에 의하면 전 세계적으로 개방형 플랫폼 기반 스마트폰 시장의 규모는 '08년 12.9%에서 '10년까지 26.5%로 성장할 것으로 예상하고 있다. 현재('09.10) 국내 스마트폰 이용자 수는 약 50만명으로 추산되고 있으며 이는 전체 이동통신서비스 이용자의 1% 정도에 불과하다. 이 수치는 미국의 스마트폰 보급현황이 약 20% 수준임을 감안할 때 국내 스마트폰 시장의 성장 가능성은 매우 높은 것으로 분석되고 있다.



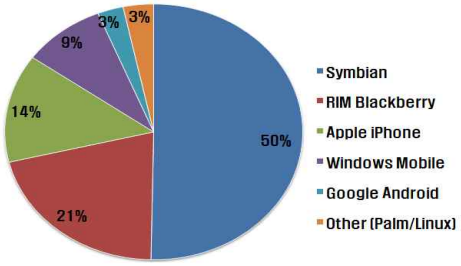
[그림 1] 국내 스마트폰 판매량 추이
(출처:미래에셋 보고서)

국내 3G환경에서의 무선인터넷 가입자 수는 약 2,564만명('09.9)에 이르며 이는 전체 이동통신 가입자의 54%에 해당하는 것으로 보고되고 있다.



[그림 2] 국내 무선인터넷 가입자 수 추이(3G)
(출처:미래에셋 보고서)

또한, 스마트폰에 탑재되는 운영체제(플랫폼) 시장도 지속적으로 증가하고 있어 새로운 고부가가치 사업으로 주목받고 있다.



[그림 3] 개방형 운영체제 시장현황
(출처:Wikipedia)

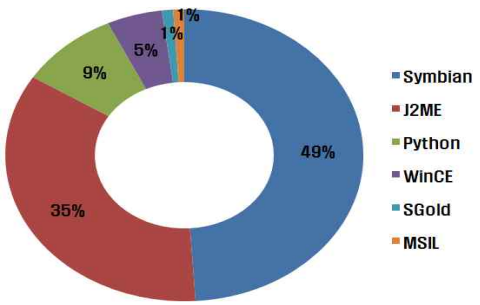
하지만, 모바일 컨텐츠 부족, 무선인터넷 서비스 요금제 부담 등이 시장 확대의 걸림돌로 작용하고 있는 상황이라서 정부에서는 요금제 개선과 스마트폰 보급 확대, 망 개방제도 개선, 컨텐츠 시장 활성화 등의 제도적인 장치를 통하여 무선 인터넷 시장을 선진국 수준까지 활성화시킬 계획이다.

Ⅲ. 모바일 악성코드 현황

국내에서는 아직까지 모바일 악성코드가 발생하지 않았지만, 해외에서는 이미 600여종의 모바일 악성코드가 발생하여 피해를 유발하고 있다.

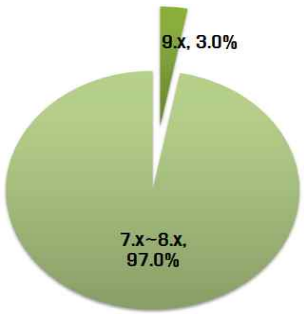
1. 국내 · 외 현황

모바일 악성코드는 주로 심비안 플랫폼이 탑재된 스마트폰을 대상으로 동작하였다. 이는 초기에 심비안이 탑재된 단말기의 수요가 많았고 또한 심비안에 대한 정보를 쉽게 획득할 수 있었다. 그러나, 최근 윈도우모바일폰, 아이폰, 블랙베리폰 등의 시장이 확대되면서 해커의 주요 관심대상이 변화하고 있는 것으로 분석되고 있다.



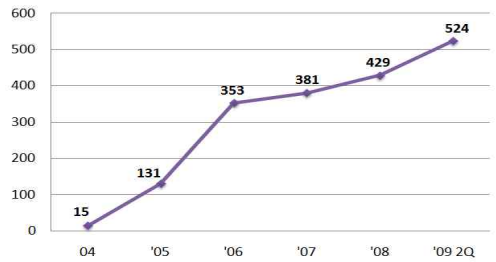
[그림 4] 플랫폼별 모바일 악성코드
(출처:Kaspersky)

또한, 심비안 악성코드는 주로 구버전(7.x, 8.x)에서 약 97%가 발견되었으며 신버전(9.x) 플랫폼에서는 3%를 차지하는 등 크게 다른 양상을 보이고 있다.



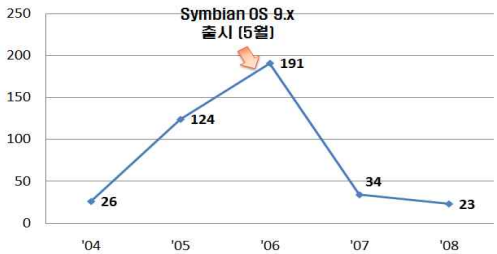
[그림 5] 심비안 악성코드 분포
(출처:s60tips)

특이할 점은 2004년도 최초의 모바일 악성코드 Cabir 발생 이후 2005년도 가파른 증가세를 보이다가 2006년도부터 증가세가 둔화되기 시작했다.



[그림 6] 모바일 악성코드 발생추이
(출처:SMobile Systems)

또한, 심비안에서 9.x 버전부터 인증체계(Code Signing)를 도입한 이 후 심비안을 대상으로 동작하는 모바일 악성코드 발생비율이 현저히 감소했다.

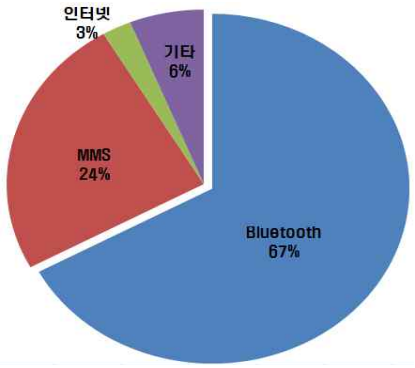


[그림 7] 심비안 악성코드 발생추이
(출처:Wikipedia)

심비안에서 인증체계(Code Signing) 도입 후 감소한 악성코드 발생비율에서도 알 수 있듯이, 국내에서도 온라인 모바일 콘텐츠 시장을 기획하거나 또는 관련 사업을 운영 중인 서비스 사업자가 향후 모바일 악성코드의 발생에 대비하여 주목해야 할 부분이다.

2. 전파방법

모바일 악성코드는 주로 블루투스(Bluetooth)나 멀티미디어메시지(MMS) 첨부파일 및 원격지 다운로드 등을 통하여 감염된다. 비록, 악성코드의 전파수단이 저장매체, 첨부파일 또는 다운로드 방식을 이용하더라도 사용자가 해당 악성코드를 직접 실행시켜야 감염되는 사회공학적인 기법을 이용하고 있어, 사용자의 스마트폰에 대한 보안인식 제고가 스마트폰 보안에서 중요한 요소로 작용하고 있다.



[그림 8] 모바일 악성코드 감염경로별 분포
(출처:F-Secure, '08)

Ⅳ. 모바일 악성코드 유형

모바일 악성코드란 PC 환경에서와 같이 개인정보 유출, 시스템 손상 등의 행위를 유발시켜 스마트폰 사용자에게 피해를 끼치는 악성코드이다.

1. 시스템 파괴 및 변경

감염된 스마트폰 내부의 시스템 파일을 삭제하거나 변형시켜 정상동작을 방해하며 일부 종류에서는 개인정보를 삭제하기도 한다. 또한, 단말기에 중대한 영향을

끼치지는 않지만 화면에 표시된 모든 아이콘을 변경시키는 단순한 행위를 하는 경우도 있다. 한 예로 2004년도에 발생한 Skulls의 경우 심비안 플랫폼이 탑재된 스마트폰을 대상으로 동작하며 감염 후 화면에 있는 모든 아이콘을 해골모양으로 변경시켜 사용에 불편을 초래한 경우도 발생한 바 있다.

2. 배터리 소모를 통한 가용성 저하

대부분의 모바일 기기의 전력공급은 전적으로 배터리에 의존하고 있다. 점차 배터리 제작 기술의 발전에 따라 가용성이 증가하고 있으나, 주변장치(예를 들어, Wi-Fi, 블루투스, IrDA 등)를 자주 사용하는 경우는 배터리 소모가 빠르게 진행된다. 이렇듯 모바일 악성코드에서는 고의적이든 또는 자신을 전파하기 위한 목적으로 주변장치를 접근할 수 있다. 이는 스마트폰의 가용시간을 줄이기도 하지만 긴급한 상황에서 스마트폰을 사용하지 못하도록 만들 수 있다. 2004년도에 발생한 카비르('Cabir') 악성코드는 블루투스를 이용하여 전파를 시도한 결과 배터리 소모가 많아졌다.

3. 금전적 피해유발

스마트폰 이용자에게 금전적인 손해를 유발시키기 위한 목적으로 제작된 악성코드이며 다량의 문자메시지 및 전화발송, 금융정보 갈취 등이 있다. 2007년 러시아에서 발생한 RedBrowser는 자바(J2ME)기반으로 작성된 모바일 악성코드이며 감염 된 스마트폰에서 일반 메시지보다 비싼 프리미엄 요금으로 문자메시지를 발생시켜 사용자에게 과금을 유발시키기도 했다. 이와 같은 금전적 피해유발의 경우 스마트폰 이용자에게는 모바일 환경에 대한 불신감을 심어줄 수 있어 산업 활성화에 저해 요소로 작용할 수 있다.

4. 시스템 및 개인정보 유출

PC 환경에서의 봇 계열의 악성코드와 같이 감염된 스마트폰으로부터 사진, 메시지 및 기타 개인정보를 원격지로 유출하는 형태이다. 이는 수집된 정보를 메시지 및 e메일 전송, 원격지 송신 등의 방법으로 유출한다. 지난 2008년 2월에 중국에서 발생한 모바일 악성코드(InfoJack)는 협박성(Ransom) 유형이며 감염된 스마트폰 정보를 유출시키고 사용자에게 악성코드 치료를 위한 송금을 요청하였다.

Ⅴ. 사례연구

현재까지 발견된 모바일 악성코드를 분석하는 것은 향후 발생 가능한 유형을 파악하기 위한 기초자료로 활용될 수 있다.

1. WinCE/Brador-A

윈도우즈CE 기반에서 동작하는 최초의 악성코드는 Dust로 알려져 있으나 버그로 인해 루트 폴더에 있는 일정크기 이상의 실행파일만 감염시킨다. 그 외, 스마트폰 화면에 팝업으로 감염사실을 알리는 점, 특별한 한 행위를 유발하지 않는 점 등으로 인해 실제 전파목적보다는 개념증명코드로 알려져 있다.

[그림 9] WinCE/Dust 악성코드

이 후 등장한 악성코드는 WinCE/Brador로서 재부팅 후에도 동작할 수 있도록 시작프로그램에 등록하고 스마트폰 감염사실을 메일을 통해 악성코드 제작자에게 통보하는 Backdoor 개념을 도입하였다.

```
.text:000119D1 aHeloVictimMail DCB "HELO victim",0xD,0xA
.text:000119D1                                        ;
.text:000119D1 DCB "MAIL FROM:br@mail.ru",0xD,0xA
.text:000119D1 DCB "RCPT TO:brokensword@ukr.net",0xD,0xA
```

[그림 10] WinCE/Brador 악성코드 내부

2. SymbOS/Mosquito

Mosquito는 2004년에 등장한 심비안에서 동작하는 악성코드로서 Mosquitos라는 유명한 게임의 해적판을 가장하여 P2P 네트워크를 통해 다운로드하는 사용자의 단말기에 저장되었다. 이 악성코드 내에는 고액의 비용을 청구하는 서비스 전화번호 리스트를 포함하고 있으며, 단말기 사용자 몰래 SMS 메시지를 해당 전화번호로 보냄으로써 고액의 서비스 이용료를 부과하게 했다.

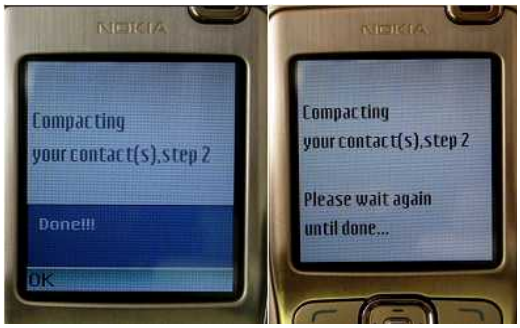
[그림 11] Mosquito 악성코드

3. SymbOS/CommWarrior

CommWarrior는 MMS를 통해 전파되는 모바일 악성코드이며, 2005년 러시아에서 제작되었다. 이 웜은 MMS 메시지에 자신의 복사본을 첨부하고 단말기 주소록에 있는 모든 연락처에 발송함으로써 단말기 소유자에게 고액의 서비스 이용료를 부과하게 했다. CommWarrior는 Skull과 함께 심비안 플랫폼 단말기를 공격 대상으로 했기 때문에 Nokia 폰 사용자들에게 많은 피해를 주었다. 지난 2007년 2월 스페인 경찰에서는 CommWarrior, Cabir 모바일 폰 바이러스 변종을 제작한 혐의로 28세의 한 남자(스페인 남동부 발렌시아)를 구속했으며, 해당 악성코드는 약 115,000 대의 전화를 감염시켰으나, 특별히 심각한 위협은 되지 않는 것으로 분석되었다.

4. SymbOS/PBStealer

2005년에 등장한 PBStealer는 전화번호부 압축 유틸리티를 사칭한 악성코드로서 단말기에 저장된 전화번호를 외부 단말기로 유출시켰다. PBStealer에 감염된 단말기는 [그림 12]와 같은 메시지를 확인하게 되는데 이 과정에서 단말기에 저장된 전화번호부는 텍스트 파일로 유출된다.



[그림 12] PBStealer 악성코드에 감염된 단말기

[그림 13]은 감염 단말기로부터 전화번호부 파일을 수신한 단말기에 뜨는 메시지이다. 메시지는 블루투스를 통해 인접 단말기에 메시지를 전송하기 때문에 일반 단말기 사용자도 해당 파일을 읽을 수 있다.

[그림 13] 전화번호 정보

5. SymbOS/Skull

Skull은 2004년에 등장한 악성코드로 심비안 플랫폼 단말기를 공격 대상으로 하였다. 감염된 단말기의 시스템 애플리케이션을 다른 파일로 교체함으로써 단말기를 사용할 수 없게 하며, 이 악성코드에 감염되었을 때 단말기 내의 모든 애플리케이션 아이콘은 [그림 14]과 같이 해골 이미지로 변경되거나 전체 화면에 해골 이미지

의 애니메이션이 출력되기도 한다.

[그림 14] Skull 악성코드에 감염된 단말기 화면

6. SymbOS/YXE

YXE 악성코드는 기존의 블루투스나 멀티미디어메시지(MMS)를 이용하지 않고 문자메시지(SMS)를 이용하여 전파한다. 감염된 단말기의 전화번호부에 등록된 모든 번호에 게임을 가장한 웹사이트 링크를 포함한 메시지(Callback SMS)를 전송하여 사용자로 하여금 실행시키도록 유도한다. 해당 악성코드는 심비안 Code Signing이 적용된 3rd Edition을 대상으로 동작하며 이는 인증체계를 우회하여 전파되는 악성코드로 평가받고 있다.

[그림 15] 심비안 인증체계를 우회한 악성코드

7. iPhone Malware

최근 국내의 한 이동통신사에서 Apple社와 협약을 체결하여 아이폰의 국내 도입 및 판매를 담당하고 있다. 이러한 아이폰의 인기를 반영하듯 11월에 3종류의 아이폰 악성코드가 발생하였다. 이들 악성코드의 공통적인 특징은 소위 JailBreak된 아이폰의 SSH를 통하여 접근하고 설정된 기본 패스워드를 이용하여 루트권한을 획득하게 된다. 이렇듯 아이폰 내부로 접근이 가능하게 되면 정보유출, 악성코드 삽입 등의 행위가 가능하게 된다.

[그림 16] Ikee 아이폰 악성코드

[표 2] 아이폰 악성코드

악성코드 명칭	주요특징
Ikee (‘09.11.09)	감염된 아이폰의 바탕화면을 80년대 팝가수 릭 애슬리의 사진으로 변경
iPhone/Privacy (‘09.11.10)	감염된 아이폰에서 무선랜을 접속하는 경우 개인정보를 원격지로 전달함
Duh Worm (‘09.11.24)	아이폰 사용자의 은행사이트 이용 시 비밀번호를 유출하며 인터넷을 통한 원격제어 가능

VI. 결 론

스마트폰 시대의 도래는 비단 새로운 고가의 휴대폰을 이용할 수 있는 환경이 조성되어 이에 따른 신규 서비스 시장형성 및 산업 활성화의 기반이 되지만 한편, 새로운 보안위협의 등장을 예고하고 있다. 신규 서비스가 보안위협에 노출될 경우 서비스 전반에 대한 불신으로 인하여 시장 성장을 저해할 수 있다. 따라서 향후 발생 가능한 보안위협에 대해 보다 선제적으로 예방 및 대응할 수 있는 체계를 구축하는 것은 급속도로 변화하고 있는 환경에 신속하게 대처할 수 있는 최적화된 해결책이 될 것으로 예상된다. 요컨대, 아직 국내에서 발생하지 않은 모바일 악성코드를 대비한다는 것이 시기

상조일 수도 있으나, 해외에서 발생한 사례들을 타산지석(他山之石)으로 삼아 선제적 대응기반 마련 및 민·관 협력체계를 강화하는 기회를 가져야 할 것이다.

참고문헌

[1] “IT 산업분석: 개화기를 앞둔 스마트폰 시장 전망”, 정보통신연구진흥원, 2008.

[2] 채송화, “Web 2.0 시대 인터넷 보안 위협”, 2007.

[3] 배근태, 김기영, “모바일 단말 보안 운영체제 기술 동향”, 전자통신동향분석, 제 23권, 제 4호, 2008.

[4] 정우철, 김성훈, “스마트폰 시장확대에 따른 영향”, Mirae Asset TIMES No.104, 2009

[5] Ken Dunham, Mobile Malware Attacks and Defense, Syngress, 2008.

[6] Stacy K. Sudan, Stephen D. Drake, and Brian E. Burke, "Worldwide Mobile Device Security 2007-2011 Forecast", IDC, 2007.

[7] Wayne Jansen and Karen Scarfone, "Guidelines on Cell Phone and PDA Security", NIST, 2008.

[8] Mitesh M. Khapra and Nirav S. Uchat, "Mobile Worms, Viruses and Threats".

[9] “WAP Push Technology Overview”, Openwave Systems Inc., 2002.

[10] “Comparison of WAP Push and Short Message Service(SMS)”, Openwave Systems Inc., 2002.

[11] “WAP Push Architectural Overview”, Wireless Application Protocal Forum, Ltd., 2001.

[12] Aubrey-Derrick Schmidt and Sahin Albayrak, “Malicious Software for Smartphones”, DAI-Labor, 2008.

[13] Jon Collins and Dale Vile, “Mobile Security: A primer on the security of mobile devices and the implications for enterprise IT”, Freeform Dynamics, Ltd., 2007.

[14] “The CIO's Guide to Mobile Security”, Research In Motion Limited, 2006.

[15] “Guide to Bluetooth Security”, NIST, 2008

[16] "White Paper: 3G Mobile Network Security", iGillottResearch, Inc., 2007.

[17] Thomas M. Chen and Cyrus Peikari, “Malicious Software in Mobile Devices”, IGI Global, 2008.

[18] Mikko Hypponen, “Malware Goes Mobile”, Scientific American, Inc., 2006.

[19] “White Paper: Protecting Mobile Data and Increasing Productivity”, Trend Micro, Inc., 2007.

[20] Shane Coursen, “The future of mobile malware”, Kaspersky Lab, Inc., Network Security Magazine, 2007.

[21] Alexander Gostev, “Mobile Malware Evolution: An Overview”, 2006.

[22] Ingo Naumann and Giles Hogben, “Security Issues of Authentication Using Mobile Devices”, European Network and Information Security Agency, 2008.

[23] Tim Kridel and Dennis Mendyk, “Mobile Malware: The Enterprise at Risk”, 2006.

[24] Neal Leavitt, “Will Proposed Standard Make Mobile Phones More Secure?”, IEEE Computer Society, 2009.

[25] Zhu Cheng, “Mobile Malware: Threats and Prevention”.

[26] Dancho Danchev, “New mobile malware silently transfers account credit”, 2009.

[27] “2006: Year of the mobile malware”, Dawn Kawamoto, 2005.

[28] Liam Tung, "Cell phone security has at least one flaw: People", 2007.

[29] Gemma Simpson, “F-Secure: Low threat from mobile malware”, 2007.

[30] Vlad Constandes, “Mobile Users - Ransomware Trojan Victims”, 2008.

[31] Matthew Hines, “More Mobile Malware Models Evolving”, 2008.

[32] Natasha Lomas, “Mobile malware: The threat exists”, 2008.

[33] Jimmy Shah, “Crimeware goes Mobile”, McAfee, 2008.

[34] “Windows Mobile”, Wikipedia, 2009.

[35] Pu Wang, Marta C. Gonzalez, Cesar A. Hidalgo and Albert-Laszlo Barabasi, “Understanding the Spreading Patterns of Mobile Phone Viruses”, Science Magazine, 2009

[36] http://www.vnunet.com/
[37] http://www.viruslist.com/
[38] http://secure.smobilesystems.com
[39] http://en.wikipedia.org/wiki/Smartphone
[40] http://www.f-secure.com
[41] http://www.s60tips.com

<著者紹介>

심 재 홍 (沈載弘)
비회원
2000년 2월 : 충북대학교 컴퓨터과학과 졸업
2002년 2월 : 서울대학교 컴퓨터공학부 석사
2003년 1월 ~ 2006년 6월 : (주)팬택앤큐리텔
2006년 9월 ~ 현재 : 한국인터넷진흥원

이 석 래 (이석래)
회원
1992년 2월 : 한양대학교 전자통신공학과 졸업
1994년 2월 : 한양대학교 전자통신공학과 석사졸업
1994년 1월~1999년 6월 : (주)LG전자
1999년 7월 ~ 현재 : 한국인터넷진흥원