모바일 악성코드 분석 방법과 대응 방안

정회원 김 익 수*, 학생회원 정 진 혁*, 준회원 이 형 찬*, 종신회원 이 정 현*°

Analysis Method and Response Guide of Mobile Malwares

Ik Su Kim* *Regular Member*, Jin Hyuk Jung* *Student Member*,
Hyeong Chan Lee* *Associate Member*, Jeong Hyun Yi*° *Lifelong Member*

요 약

최근 휴대전화의 위피 탑재 의무 해제와 스마트 폰 시장의 개방 정책으로 많은 외산 제품들이 국내 시장에 유입되고 있어, 사용자는 다양한 제품을 저렴한 가격으로 구입할 수 있게 되었다. 하지만 이러한 변화로 인해 해외에서만 발생해왔던 모바일 악성코드 침해 사고가 곧 국내에서도 발생될 가능성이 매우 높아졌다. 현재 국내에서는 PC용 악성코드에 대한 정형화된 분석 기법과 대응 방안이 널리 알려져 있으나, 모바일 악성코드에 대해서는 대응 준비가 매우 부족한 상황이다. 이에 본 논문에서는 기존의 모바일 악성코드를 소개하고, 모바일 악성코드 분석에 활용 가능한 도구들을 살펴본다. 아울러 현재 모바일 악성코드에 대한 대응 준비가 부족한 국내 현실을 고려하여 모바일 악성코드 분석 방법과 대응 방안을 제시한다.

Key Words : Mobile Malware, Malicious Code, Smart Phone, Analysis Tool, Windows Mobile

ABSTRACT

Korean government has recently abrogated WIPI policy to open domestic mobile phone market to the world, which may result in the influx of foreign smart phones. This circumstance has given users more wide range of choices to buy a product and also has brought benefit to buy mobile phone cheaply. On the other hands, this change might have brought potential danger of mobile malware incidents which have only occurred in foreign countries. There are standardized analysis methods and response guides for computer malwares, not but for mobile malwares in our country. In this paper, we introduce existing mobile malwares and available tools for their analysis. Considering domestic circumstances which might not be properly protected against mobile malwares, we propose analysis methods and response guide of mobile malwares.

Ⅰ. 서 론

가트너 보고서에 따르면 2008년 스마트 폰 판매량은 이미 1.39억만대를 넘어섰으며, 이는 2007년과 비교하여 약 13.9%의 증가율을 나타낸다. 국내의 경우, 2009년 4월 1일을 기점으로 휴대전화의 위피(WIPI) 탑재 의무화 정책이 해제됨에 따라 많은 해외 스마트 폰들이 국내 시장에 유입되고 있으며, 국내 휴대폰 제조업체에서도 스마트 폰 개발과 모바일 컨텐츠 마켓 오픈에 많은 투자를 하고 있다.

현재 출시되고 있는 스마트 폰들은 PC 환경과 매우 유사하기 때문에 PC 환경에서 발생하는 악성코드에 의한 침해 사고들이 스마트 폰 환경에서도 유사하게 발생한다. 하루에도 수십 개의 악성코드가 출현하는 PC 환경의 경우, 이미 악성코드를 분석하기 위한 정형화된 기법과 도구들이 많이 알려져 있으며, 거의

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 20090089245)
* 숭실대학교 컴퓨터학부(iksuplorer@ssu.ac.kr, {nemojjh, iclear0708}@gmail.com, jhyi@ssu.ac.kr), (° : 교신저자)
논문번호 : KICS2009-12-597, 접수일자 : 2009년 12월 1일, 최종논문접수일자 : 2010년 3월 19일

표 1. 운영체제 시장 현황

운영체제	2008년 4분기 판매량(천 대)	2008년 4분기 시장 점유율(%)	2007년 4분기 판매량(천 대)	2007년 4분기 시장 점유율(%)	전년 대비 증가율(%)
Symbian	17,949.1	47.1	22,902.5	62.3	-21.6
RIM	7,442.6	19.5	4,024.7	10.9	84.9
MS Windows Mobile	4,713.9	12.4	4,374.4	11.9	7.8
Mac OS X	4,079.4	10.7	1,928.3	5.2	111.6
Linux	3,194.9	8.4	2,675.9	7.3	19.4
Palm OS	326.5	0.9	449.1	1.2	-27.3
Other OSs	436.9	1.1	411.3	1.1	6.2
Total	38,143.3	100.0	36,766.1	100.0	3.7

대부분의 악성코드가 윈도우즈 플랫폼을 기반으로 개발되었기 때문에 기존의 분석 기법 및 도구의 활용이 용이하다. 반면, 스마트 폰 상에서 동작하는 모바일 악성코드의 경우에는 분석 가능한 전용 도구들이 부재할 뿐만 아니라, 스마트 폰 자체가 수십 종의 플랫폼 상에서 구현되며 다양한 운영체제를 탑재하고 있기 때문에 체계적으로 악성코드를 분석하는데 어려움이 따른다. 2008년 6월까지 확인된 모바일 악성코드 수는 변종을 포함하여 총 400여개에 이르고 있으며, 그 중에서도 99%이상의 모바일 악성코드들이 스마트 폰 시장 현황을 반영하듯 심비안과 윈도우즈 모바일을 공격 대상으로 하고 있다. 현재까지 국내에서의 모바일 악성코드 피해보고 사례는 없었지만, 개방화 된 스마트 폰 시장에서의 외산 단말기 유입과 국내 제조사의 스마트 폰 생산, 해외 로밍 서비스 사용자에 의한 모바일 악성코드의 전파로 인해 국내 역시 모바일 악성코드에 의한 사고가 발생될 것으로 예상된다.

본 논문에서는 현재 모바일 악성코드에 대한 분석 및 대응 준비가 부족한 국내 상황을 고려하여 모바일 악성코드의 심각성을 알리고, 모바일 악성코드 분석에 이용 가능한 도구들을 파일 시스템, 프로세스, 네트워크 등과 같이 다양한 측면에서 살펴본다. 또한, 모바일 악성코드 분석 절차와 대응 방안을 제시함으로써 모바일 악성코드에 대한 정형화된 분석 방법론 확보를 위한 초석을 마련하고, 스마트 폰 사용자 및 관련 기관들이 모바일 악성코드에 효과적으로 대응할 수 있는 능력을 부여하고자 한다.

Ⅱ. 관련연구

2.1 스마트폰 및 운영체제 시장 현황

가트너 보고서에 따르면 2008년 전 세계 스마트 폰 판매량은 이미 1.39억만대에 이르렀으며 이는 2007년과 비교하면 약 13.9%의 증가율을 나타낸다. 제조사별 시장 점유율을 살펴보면, 2008년 4사분기를 기준으로 노키아(Nokia)사 제품이 전체 판매량의 40.8%, RIM사 제품이 19.5%, 애플(Apple)사가 10.7%를 차지하고 있으며, 국내 제품인 삼성 스마트 폰이 전체 시장에서 5위를 차지하고 있다[1].

스마트 폰에 탑재되는 운영체제 점유율을 살펴보면, 표 1과 같이 2008년 4사분기 기준으로 심비안이 47.1%, RIM가 19.5%, 윈도우즈 모바일이 12.4%를 차지하고 있다. 노키아 제품에 탑재되는 심비안의 경우, 노키아 제품의 시장 점유율 감소와 함께 21.6%의 감소율을 보이며, 반대로 RIM과 Mac OS는 RIM사의 블랙베리 폰과 애플사의 아이폰(iPhone) 판매량 증가와 함께 각각 84.9%, 111.6%의 증가율을 보이고 있다.

반면, 국내에서 출시되는 스마트 폰 운영체제의 대부분이 윈도우즈 모바일을 사용하는 것으로 보고되고 있으며, 심비안 플랫폼을 탑재한 노키아 제품은 국내 스마트 폰 시장에서 거의 영향력을 발휘하지 못하고 있는 현실이다[2].

2.2 모바일 악성코드

모바일 악성코드란 기존 PC 환경에서 발생하는 악성코드와 유사하게 모바일 단말기를 대상으로 개인정보 유출, 시스템 파괴, 원격지 접속 등의 악의적인 행위를 수행하기 위해 제작된 악성 프로그램을 의미한다[3]. 모바일 악성코드를 분류하면 대표적으로 전파를 목적으로 다른 파일을 감염시키는 바이러스, 유용한 프로그램을 가장한 트로이잔, 자신의 복사본을 생성하여 전파하는 웜이 있으며, 이중에서도 사회공학기법을 이용하여 사용자의 설치를 유도하는 트로이잔이 가장 많은 비율을 차지하고 있다[4]. 이들은 주로 PC와의 동기화, 메모리 카드, 블루투스, MMS(Multimedia Message Service), 모바일 인터넷을 통해 전파된다[5,6]. 모바일

악성코드에 의한 단말기 사용자의 피해 유형을 살펴보면 다음과 같다[4, 7, 8, 9, 10].

- 파일 조작 : 응용 프로그램 및 시스템 프로그램에 특정 내용을 덮어 쓰거나 다른 파일로 교체하여 프로그램의 실행 및 단말기 사용이 불가
- 정보 유출 : 전화번호부나 주소록, 사진 등의 개인정보 및 스마트 폰 사용자의 수신 메시지 내용과 통화 내역이 외부로 유출
- 서비스 과금 : 감염된 스마트 폰을 통해 SMS와 MMS 메시지를 무단으로 발송하게 하여 금전적인 피해 유발
- 장치 사용 불가 : 서비스 거부 공격을 통해 스마트 폰의 배터리를 방전시키거나, 메모리 카드의 패스워드를 임의로 변경하여 사용 불가

Ⅲ. 모바일 악성코드 분석 도구

본 장에서는 현재 국내 스마트 폰 시장의 대부분을 차지하는 윈도우즈 모바일 환경에서 모바일 악성코드를 분석하는 데 사용 가능한 도구들을 살펴본다. 특히, 분석 도구 활용에 대한 이해를 돕기 위해서 대표적인 모바일 악성코드인 Brador를 기반으로 도구 활용법을 기술한다.

3.1 파일 시스템 기반 분석 도구

일반적으로 악성코드가 실행되고 난 후 파일 시스템에는 파일복제, 파일변조, 레지스트리 수정, 삽입, 삭제, 시스템 로그 등의 다양한 공격 흔적이 남게 된다. 이들은 악성코드 행위 분석에 있어 매우 중요한 데이터가 될 수 있다. SSnap은 공개 소프트웨어로써 실제 단말기는 물론 에뮬레이터 상에서도 레지스트리와 파일 시스템 정보를 저장할 수 있다.

그림 1의 좌측부터 SSnap 로그파일에 포함될 내용을 설정하는 화면, 로그 작성을 수행하는 화면, 생성된 결과를 보여주는 화면이다. SSnap 로그파일의 분석을 통해 레지스트리의 삽입 및 삭제, 파일 시스템에서 행해지는 파일 복제, 변조, 갱신 여부를 확인함으로써 악성코드에 의한 악성행위를 파악할 수 있다. 악성코드의 실행 전후에 각각 수집된 레지스트리 및 파일 시스템 정보를 좀 더 효율적으로 분석하기 위해서는 WinMerge를 사용할 수 있다.

WinMerge는 공개 소프트웨어로써 파일간의 비교분석을 위해 사용할 수 있는 유용한 도구이다. 그림 2는 Brador 악성코드 실행 전후의 단말기 상태를 비교하기 위해서 SSnap을 이용하여 파일 시스템 로그파일

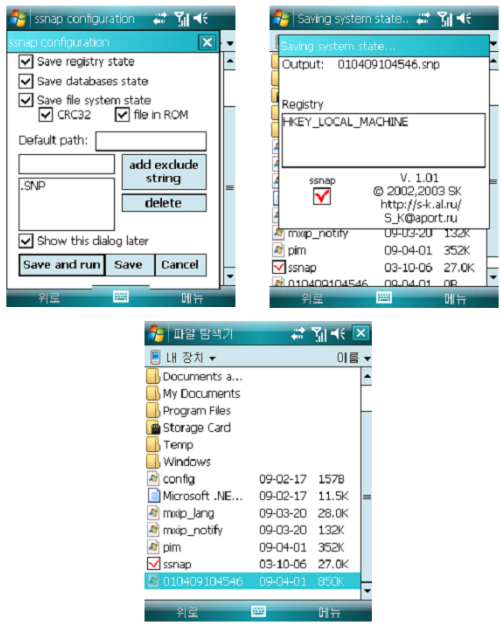

그림 1. SSnap 수행 화면

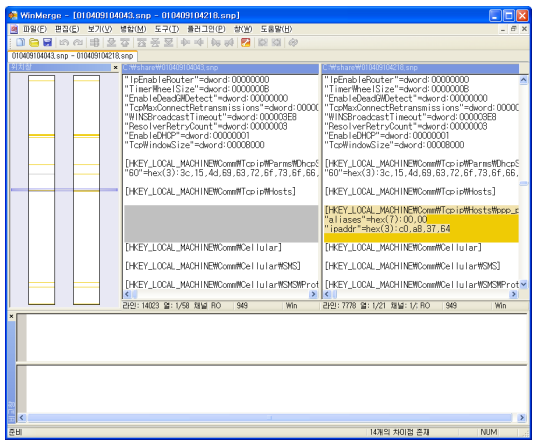

그림 2. WinMerge를 통한 SSnap 로그파일 분석

을 생성한 후, WinMerge를 이용하여 분석하는 모습이다. WinMerge는 서로 다른 파일의 내용을 동시에 비교하기 위한 두 개의 뷰(우측 두 영역)와 전체적인 파일 비교의 아웃라인을 표시하는 뷰(좌측 영역)를 제공한다, 그림 4에서 회색과 노란색으로 각각 구분되는 영역은 두 파일 간에 서로 다른 부분을 나타낸다. WinMerge는 파일 및 폴더 비교에 대한 가독성이 좋아 분석에 소요되는 시간이 크게 단축된다는 장점이 있다.

3.2 네트워크 기반 분석 도구

네트워크 기반 분석 도구를 이용하면 악성코드에

의해 사용된 포트에 관한 정보와 전송되는 패킷 정보 등을 분석할 수 있다. WireShark는 공개 소프트웨어로써 실제 단말기는 물론 에뮬레이터 상에서의 네트워크 스니핑이 가능한 도구이다. 이 도구를 이용하면 모바일 악성코드로부터 생성되는 TCP/IP 기반의 네트워크 패킷의 동적 분석이 가능하기 때문에 그림 3과 같이 네트워크를 통해 전송되는 패킷의 전송 시간, 송수신 IP 주소, 프로토콜, 포트번호에 관한 정보를 확인할 수 있다. 또한, 패킷 데이터를 16진수 값으로 제공하기 때문에 악성코드의 공격 패턴 분석에 유용하게 사용된다.

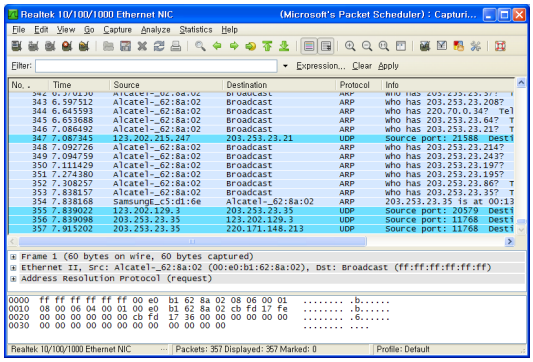

그림 3. WireShark를 이용한 패킷 스니핑

3.3 프로세스 기반 분석 도구

프로세스 기반 분석은 악성코드에 의해 생성된 프로세스와 쓰레드, 사용된 라이브러리 및 모듈에 관한 정보를 확인하는데 유용한 방법이다. Windows CE Remote Process Viewer는 윈도우즈 모바일 플랫폼에서 동작하는 상용 소프트웨어로써 에뮬레이터와 실제 단말기 상에서 실행중인 프로세스의 모니터링 및 제어가 가능하다.

그림 4는 Brador 악성코드에 감염된 단말기에서 Windows CE Remote Process Viewer를 실행한 모습을 나타낸다. 실행 결과를 살펴보면 Brador 악성코드의 프로세스 ID와 악성코드에 의해 사용된 dll 파일 목록 확인이 가능한 것을 알 수 있다. 특히, 사용된 dll 목록 중에서 dtpt_lsp.dll, ws2.dll, ssllsp.dll들은 네트워크와 관련된 dll로써 Brador 악성코드의 악성행위가 네트워크와 관련되어 있다는 것을 알 수 있다.

Windows CE Remote Heap Walker는 윈도우즈 모바일 플랫폼에서 동작하는 상용 소프트웨어로써 이 도구를 이용하면 에뮬레이터와 실제 단말기 상에서의 힙 메모리 영역 분석이 가능하여 악성코드의 악성행위를 추측할 수 있다. 그림 5는 Brador 악성코드를 실

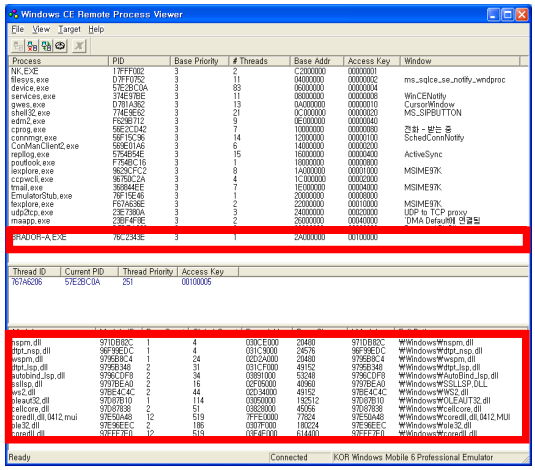

그림 4. Windows CE Remote Process Viewer를 이용한 프로세스 분석

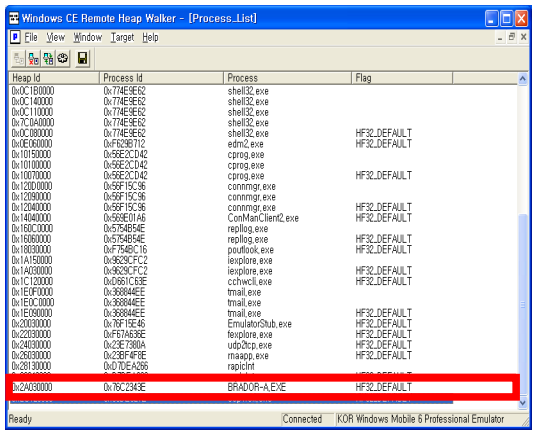

그림 5. Windows CE Remote Heap Walker를 이용한 힙 영역 분석

행시킨 상태에서의 힙 메모리 영역을 확인한 결과이다. 악성코드의 경우 레지스트리 변경, 수정, 삭제를 목적으로 특정 레지스트리의 주소를 메모리에 할당할 수 있다. 또한 악성행위를 수행하기 위해 쉘을 실행시키기도 하는데, 이를 위해 쉘 코드의 바이너리 데이터를 메모리에 할당하기도 한다. 이러한 데이터들이 동적 메모리 할당을 통해서 힙 메모리에 저장될 경우, 힙 메모리 영역 분석을 통해 악성행위에 대한 정보를 확보할 수 있다. 그림 6은 여러 힙 메모리 영역들 중 특정 힙 메모리 영역을 상세하게 확인한 결과이다.

3.4 패킹(Packing)/언패킹(Unpacking) 도구

대부분의 악성코드는 실행파일의 형태로 존재하지만 탐지를 회피하기 위해 실행압축 기법을 사용하기도 한다. 따라서 압축된 파일내의 목록 확인 및 각 파

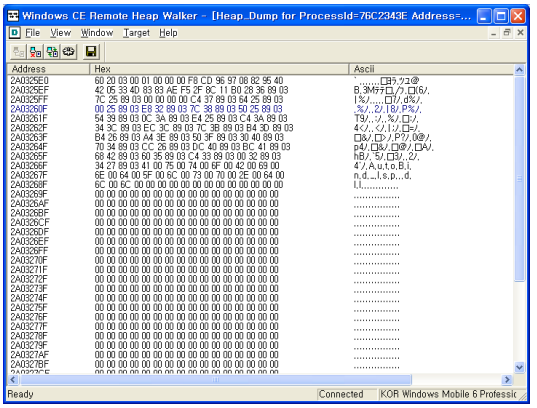

그림 6. Windows CE Remote Heap Walker를 이용한 특정 힙 상세 확인

일의 상세 분석을 위해서는 UPX Packer를 사용한다. UPX Packer는 그림 7과 같이 압축된 윈도우즈 모바일용 프로그램으로부터 파일을 추출하거나 파일들을 하나로 압축할 때 사용할 수 있는 공개 소프트웨어이다.

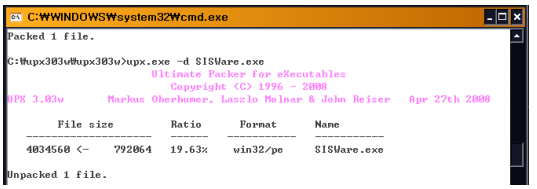

그림 7. UPX Packer를 통한 파일 언패킹

3.5 역공학 기반 분석 도구

악성코드를 분석하는 방법으로 역공학 기법인 디스어셈블링과 디버깅을 이용할 수 있다. 디스어셈블링의 경우에는 바이너리 데이터를 어셈블리 코드로 변환하여 분석하며, 디버깅은 악성코드를 실행한 후 브레이크 포인트를 적절히 설정하고 프로그램 실행루틴을 추적하면서 분석한다. 이 방법들은 상당한 숙련도와 시간이 요구되지만, 정확하고 정교한 분석이 가능하다는 장점이 있다. IDA Pro는 디스어셈블링과 디버깅 기능을 통한 파일 정밀 분석 기능을 제공하지만 상용 소프트웨어라는 단점이 있다.

Ⅳ. 모바일 악성코드 분석 절차와 샘플 분석

4.1 모바일 악성코드 분석 절차

4.1.1 모바일 악성코드 수집 단계

모바일 악성코드를 분석하기 위해서는 감염된 단말기로부터 실제 악성코드를 수집하는 것이 중요하지만 그와 함께 단말기 사용자로부터 악성코드 감염에 따른 단말기 증상에 관한 정보를 추가적으로 얻는 것이 매우 중요하다. 이는 단말기 내에 저장된 악성코드를 식별하고 관련 프로세스에 의한 악성행위를 분석하는데 소요되는 시간을 단축시킬 수 있다.

4.1.2 초기 검사 단계

초기 검사 단계에서는 악성코드에 의한 단말기의 증상, 악성코드의 압축상태, 이미 보고된 악성코드와의 유사성 정보를 수집하는데 목적이 있다. 디버깅 및 디스어셈블링과 같은 역공학 분석에서는 초기 검사 단계에서 수집된 정보가 유용하게 사용될 수 있다.

4.1.2.1 패커를 이용한 압축상태 검사

대부분의 악성코드는 실행파일의 형태로 존재하지만 탐지를 회피하기 위해 실행압축 기법을 사용하기 때문에 악성코드의 식별 및 분석을 어렵게 한다. 따라서 악성코드로 의심되는 파일들은 앞서 살펴본 언패킹 도구를 이용하여 압축을 해제한 후 정밀 검사가 이루어져야 한다.

악성코드로 의심되는 파일이 UPX로 패킹이 되어 있는지 검사하는 방법은 그림 8과 같이 PEiD를 통해 가능하다.

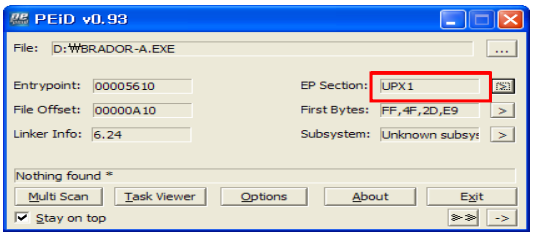

그림 8. PEiD를 통한 Packer 식별

4.1.2.2 안티바이러스를 이용한 악성코드 식별

최근 악성코드들의 특징을 살펴보면, 새로운 형태의 악성코드보다 기존의 악성코드와 유사한 변종 악성코드 형태로 나타나고 있다. 안티바이러스는 그림 9와 같이 기존의 악성코드를 식별할 수 있기 때문에 불필요한 분석 시간을 단축시키기 위한 목적으로 사용될 수 있다. 하지만 변종 악성코드가 기존의 악성코드와 매우 동일한 파일을 포함할 경우, 안티바이러스는 변종 악성코드가 아닌 기존에 알려진 악성코드로 인식할 수 있스는 변 경우헐할 기존 악성코드로 분류되어 악성코드 분석 작쇅코드누락될 수 있할 문제가 발생한다. 따라서 안티바이러스를 이용할 경우헐할 탐지기존에 알려진 단순히 필터링하기 위한 목적으로 사용간

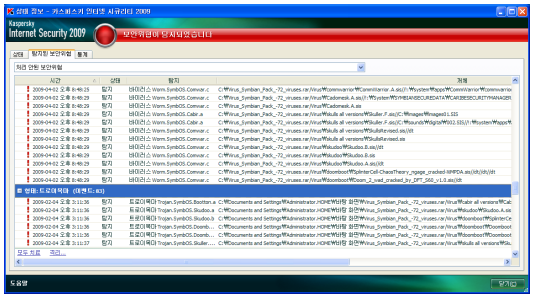

그림 9. 카스퍼스키 안티바이러스를 통한 악성코드 식별

을 단축시아니라 해당 악성코드의 동작과 증상 등의 정보를 참고하기 위한 목적으로 사용해야 한다.

4.1.2.3 정밀 검사 단계

초기 검사 단계에서 수집한 정보를 기반으로 분석을 위해 구성된 에뮬레이터나 실제 모바일 단말기 상에서 악성코드를 실제로 실행하면서 파일 시스템, 네트워크, 프로세스 기반의 분석 도구를 통해 정보를 수집한다. 수집된 정보를 통해 악성코드와 관련된 실행 파일을 식별한 후, IDA와 같은 디버깅 및 디스어셈블링 도구를 이용하여 악성코드에 대한 자세한 분석을 시도한다.

4.1.2.4 문서화 단계

이 단계는 이전의 각 단계에서 수집한 악성코드의 정보와 분석 자료를 문서화하는 단계이다. 악성코드는 변종의 수가 많기 때문에 특정 악성코드에 대한 문서화가 되어 있는 경우 변종 악성코드에 대해 좀 더 신속하고 효과적으로 분석하기 위한 참고자료로 사용될 수 있다.

4.2 악성코드 샘플 분석

본 절에서는 트로이잔의 일종인 Brador 악성코드에 대한 분석 과정을 기술한다.

Brador 악성코드는 감염된 단말기 상에 소켓을 생성하여 해커에게 감염 사실을 알리고 백도어를 통해 해커로부터 명령을 받는다. IDA를 이용하여 이를 분석할 때 먼저 소켓과 관련된 API에 중단점을 설정하고 디버깅을 시작한다. 그러면 그림 10에서와 같이 Brador가 소켓을 초기화하는 것을 확인할 수 있다.

소켓을 생성한 후, Brador는 그림 11에서와 같이 해커에게 감염된 단말기의 정보를 전송한다.

해커에게 정보를 전송하고 나면, 그림 12와 같이 단말기의 hostname인 Pocket PC를 통해 단말기 IP 주소를 식별한 후, 그림 13과 같이 해당 IP로 소켓을

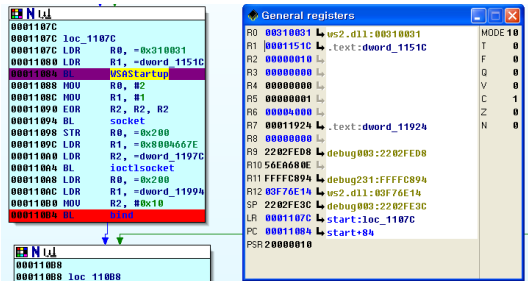

그림 10. 백도어 소켓 API 확인

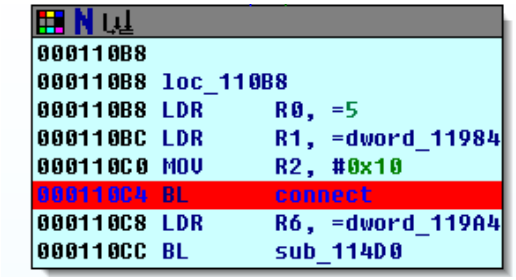

그림 11. 백도어 소켓 API 확인(connect)

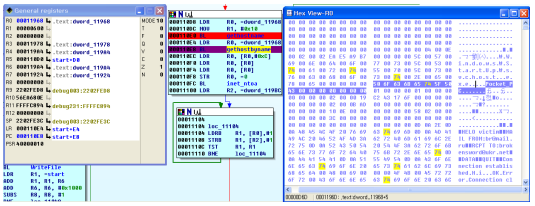

그림 12. 단말기 IP 정보 수집

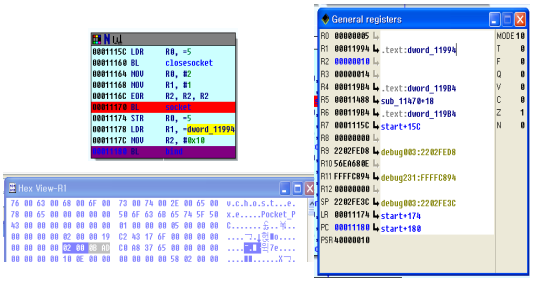

그림 13. 해커로부터 명령을 받을 소켓 바인딩

생성하여 2989(0x0BAD)번 포트로 바인딩 한다. 이후 Brador는 2989번 포트를 사용해 해커로부터 명령을 수신한다.

Windows Mobile은 시스템 구동 시 "\Windows\StartUP" 폴더에 있는 파일을 자동으로 실행한다. Brador는 그림 14와 같이 실행할 악성코드인 "svchost.exe" 파일을 복제하여 시스템이 구동될 때

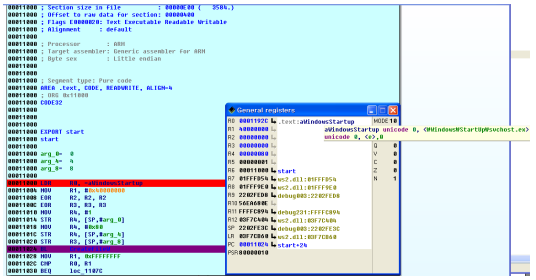

그림 14. 악성코드 파일 생성위치 확인

마다 자동으로 실행되게 한다.

V. 모바일 악성코드 대응 방안

본 장에서는 모바일 악성코드에 대한 대응 준비가 부족한 국내 상황을 고려하여 모바일 악성코드에 효과적으로 대응하기 위한 사용자, 기업체, 정부기관 측면에서의 대응 방안에 대해 기술한다.

5.1 사용자 측면 대응 방안

스마트 폰을 통해 발생하는 대부분의 피해는 사용자가 스마트 폰의 특성과 모바일 악성코드에 대한 이해가 부족하고 이에 따른 스마트 폰의 부주의한 사용으로 발생한다. 따라서 자신의 정보를 보호하고 금전적인 피해를 최소화하기 위해서는 다음과 같은 사항들을 준수해야 한다.

5.1.1 보안 소프트웨어 설치

국내의 지속적인 모바일 인프라 발전과 모바일 시장의 성장에 따른 모바일 악성코드의 확산 및 피해가 예상된다. 모바일 단말기를 통해 발생할 수 있는 개인적 피해로는 단말기 내의 정보 유출에 의한 프라이버시 침해와 금전적인 피해이며, 비즈니스 모델의 변화에 따라 스마트 폰을 통한 회사 업무로 회사 내 정보가 유출될 수 있다. 이에 스마트 폰 사용자들은 가능한 한 다음과 같은 보안 솔루션들을 활용하여 악성코드에 의한 피해를 줄여야 한다[4,5,11,12,13].

5.1.1.1 침입차단을 위한 방화벽

스마트 폰 상에서도 PC에서와 같이 외부로부터의 침입 가능성이 존재한다. 특히, 스마트 폰은 다양한 무선 인터페이스를 지원하기 때문에 모든 가능한 연결 지점을 감시하여 허가되지 않은 접근으로부터 스마트 폰을 보호할 수 있는 방화벽을 활용해야 한다.

5.1.1.2 백신 프로그램

앞서 기술했듯이 지금까지 발견된 400여개의 모바일 악성코드들은 전파 경로와 그 피해 증상이 매우 다양하기 때문에 사용자가 이를 식별하고 자신의 스마트 폰을 보호하기란 매우 어려운 일이다. 따라서 이들 악성코드로부터 스마트 폰이 감염되는 것을 예방하고 사용자 자신의 개인 정보 유출을 막기 위해서는 백신 프로그램 설치가 매우 중요하다.

5.1.1.3 데이터 암호화 프로그램

텍스트 형태로 저장된 데이터는 타인에 의해 쉽게 읽혀질 수 있기 때문에 외부로 유출된 민감한 개인 정보 및 중요 회사 정보는 기밀성 유지가 되어야 한다. 만일 스마트 폰에 데이터 암호화 프로그램이 포함되어 있을 경우에는 이를 적극 활용하며, 그렇지 않을 경우에는 별도의 데이터 암호화 프로그램을 설치하여 정보 유출에 의한 피해를 최소화 한다.

5.1.1.4 안티스팸

최근 들어 사용자의 심리를 이용한 사회공학기법이 큰 문제가 되고 있다. 대표적인 사회공학기법으로는 우체국, 국세청, 건강보험공단을 사칭하여 금전적인 피해를 유발하는 보이스 피싱을 들 수 있다. 이러한 사기 수법은 SMS 스팸을 통해서도 발생 가능하기 때문에 메시지 필터링을 통한 SMS 스팸 차단 프로그램을 설치할 경우, 피싱으로 인한 금전적 피해와 광고 스팸으로 인한 불필요한 시간적 낭비를 줄일 수 있다.

5.1.2 불필요한 무선 인터페이스 설정 해제

지금까지 해외에서 발생되고 있는 대부분의 모바일 악성코드 감염은 보안 수준이 낮게 설정된 블루투스 연결을 통해 발생하였다. 이 외에도 아직까지 발생하지는 않았지만 무선 인터페이스를 통한 악성코드의 감염경로로 Wi-Fi와 적외선 채널이 이용될 수 있다. 이와 같은 무선 인터페이스를 통해 감염되는 악성코드에 대응하는 간단한 방법은 그림 15와 같이 실제로 서비스가 필요하기 전까지 무선 인터페이스의 설정을

그림 15. 불필요한 무선 인터페이스 설정 해제

해제하는 것이다[14]. 무선 인터페이스 기능의 설정 해제는 악성코드의 감염으로부터 스마트 폰을 보호할 뿐만 아니라 스마트 폰의 불필요한 배터리 소모를 막을 수 있는 이점이 있다.

5.1.3 서명되지 않은 소프트웨어 설치 금지

많은 사용자들이 웹과 P2P를 통해 다양하고 유용한 소프트웨어들을 쉽게 구해서 사용한다. 하지만 인터넷 상에 존재하는 소프트웨어들이 모두 사용자에게 유용한 것은 아니다. 사용자는 자신도 모르게 바이러스에 감염된 프로그램과 유용한 프로그램을 가장한 트로이잔을 다운로드하여 설치할 수 있다. 그리고 모바일 악성코드 유포자들은 악성코드를 전파하기 위해 MMS와 E-mail의 첨부기능을 이용하기도 한다. 예를 들어, 게임이나 백신 프로그램을 가장하여 프로그램 설치 및 파일 실행을 유도한다.

이러한 모바일 악성코드로부터 스마트 폰이 감염되는 것을 막기 위해서 그림 16과 같이 서명되지 않은 프로그램 설치에 대한 경고 메시지를 확인할 경우 프로그램 설치를 중단해야 한다.

그림 16. 서명되지 않은 프로그램 설치 화면

5.1.4 무분별한 인터넷 다운로드 주의

많은 사용자들이 웹과 P2P를 통해 다양하고 유용한 소프트웨어들을 쉽게 구해서 사용한다. 하지만 인터넷 상에 존재하는 소프트웨어들이 모두 사용자에게 유용한 것은 아니다. 사용자는 자신도 모르게 바이러스에 감염된 프로그램과 유용한 프로그램을 사칭한 트로이잔을 다운로드 할 수 있다.

사용자는 인터넷을 통해 스마트 폰이 악성코드에 감염되는 것을 예방하기 위해 의심스럽거나 알려지지 않은 사이트로부터의 소프트웨어 다운로드를 자제해야 한다.

5.1.5 MMS와 E-mail 수신 시 주의

MMS와 E-mail은 첨부파일 기능을 제공하기 때문에 악성코드를 전파하기 위한 좋은 수단이 될 수 있다. 악성코드가 첨부된 대부분의 MMS와 E-mail은 사용자가 설치하도록 유도하기 위해 다양한 사회공학기법을 이용한다. 예를 들어, 게임이나 유틸리티, 혹은 특정 개인의 사생활에 대한 이야기가 담겨있는 파일을 가장하여 프로그램 설치 및 파일 실행을 유도한다. 따라서 알려지지 않은 전화번호나 E-mail 주소로부터 수신되는 첨부파일을 함부로 열어서는 안 된다. 또한 신뢰하는 전화번호나 E-mail 주소로부터 메시지를 수신할 지라도 백신 프로그램을 통해 첨부된 파일을 검사해야 한다.

5.1.6 모바일 악성코드 감염 및 의심 시 준수사항

스마트 폰 상의 프로그램 오작동이나 스마트 폰 자체의 작동이 불능상태에 이를 경우에는 모바일 악성코드에 의한 감염을 의심해야 한다. 사용자는 악성코드에 의한 감염이 의심되면 백신 프로그램을 통해 치료하거나, 서비스 업체에 신고하여 차후에 발생할 수 있는 더 큰 피해를 예방해야 한다.

5.2 기업체 측면 대응 방안

5.2.1 이동통신사 측면

지금까지 이동 통신사들은 사용자에게 원활한 통화와 데이터 전송 서비스에 초점을 맞추어 네트워크를 운영해 온 반면, 모바일 악성코드로부터 무선 네트워크와 사용자를 보호하는 데에는 큰 투자를 하지 않았다. 하지만 위피 탑재 의무화 해제에 따른 외산 스마트 폰의 국내 시장 유입, 개방형 운영체제 기반의 다양한 스마트 폰의 출시로 모바일 악성코드에 의한 피해가 예상되기 때문에 정보보호 측면의 네트워크 관리 및 보안 서비스 제공이 요구되고 있다.

보안 사고로 인한 피해는 사용자의 정보 유출은 물론 이동통신사의 일시적인 서비스 불가 상태에 이르게 된다. 이는 고객의 프라이버시 침해와 함께 원활한 서비스 이용을 저해하며, 이동통신사의 수익에 큰 지장을 초래한다. 다음은 모바일 악성코드로부터 발생할 수 있는 피해를 최소화하기 위한 이동통신사의 역할을 나타낸다.

- 정보보호관리체계 수립 및 이행 : 전사적이고 체계적인 보안 관리를 위한 보안정책을 수립하고 모든 부서가 이를 숙지 및 이행
- 네트워크 및 서버 관리 : 공격자로부터 네트워크 및 서버를 보호하여 사용자에게 지속적이고 안정적인 서비스를 제공하기 위한 보안 솔루션 구축

- 사고 접수 및 처리 업무 고도화 : 모바일 악성코드에 의한 침해 사고가 발생할 경우, 피해를 최소화하기 위해 사고 접수 및 처리를 위한 별도의 가이드 작성 및 숙지
- 악성코드 조기 경보 : 새로운 악성코드의 출현 및 악성코드에 의한 피해 접수 시, SMS 메시지를 통해 모든 서비스 가입자에게 통보하여 사용자의 보안 의식 강화
- 안티 스팸 서비스 : 메시지 트래픽 모니터링을 통해 과대한 SMS 메시지 발송 탐지 시 블랙리스트에 등록하여 관리

5.2.2 단말기 제조사 측면

과거의 휴대폰과 비교하여 데이터 저장 및 처리 능력에 월등한 성능을 제공하는 스마트 폰은 해커에 의한 공격과 모바일 악성코드에 의한 사용자 피해 가능성 및 피해 규모가 매우 커질 것으로 예상된다. 다음은 모바일 악성코드로부터 발생할 수 있는 피해를 최소화하기 위한 단말기 제조사의 역할을 나타낸다.

- 단말기 보안 매뉴얼 개발 : 스마트 폰에 내장된 다양한 보안 기능에 대한 상세한 설명과 함께 악성코드에 의한 피해 사례 및 침해 사고 탐지 및 대응 방안에 대한 내용을 포함하여 사용자의 보안 의식 강화
- 하드웨어 보안 메커니즘 구현 : 데이터 암호화, 백업 및 복구, 안티 스팸, 접근 제어 기능을 제공하여 사용자 정보를 보호
- 소프트웨어 패치 개발 : 스마트 폰에 탑재된 운영체제 및 응용 프로그램의 취약점에 대한 패치를 적시에 개발하여 단말기 및 사용자 정보보호
- A/S 센터 지원 : 악성코드에 감염된 스마트 폰에 대한 A/S 접수 시, 이를 판단하여 악성코드의 감염 증상 및 악성코드 샘플을 추출할 수 있는 기술을 확보

5.2.3 백신업체 측면

이미 국외 백신업체들은 모바일 악성코드 대응에 주력해왔으며, 국내 백신업체들도 악성코드에 대한 신속한 대응 능력을 갖추어야 한다. 다음은 모바일 악성코드로부터 발생할 수 있는 피해를 최소화하기 위한 백신업체의 역할을 나타낸다.

- 보안 솔루션 개발 : 시스템 자원 및 전원 공급 등의 많은 제약이 따르는 스마트 폰 환경에 적합한 백신, 방화벽, VPN 기술 및 제품 개발
- 신속한 악성코드 샘플 확보 : 단말기 제조사의 A/S 센터와 협력 관계를 유지하여 단말기 제조사에게 악성코드 치료 및 악성코드 샘플 추출 기술을 제공하고, A/S 센터는 감염 단말기로부터 추출된 악성코드 샘플을 백신업체에게 신속하게 제공
- 신속한 업데이트 지원 : 이동 통신사와의 협력 관계를 유지하고, 무선 업데이트 서비스를 통해 사용자에게 악성코드 탐지 시그너처를 신속히 제공함과 동시에 사용자의 데이터 전송 서비스 부담을 최소화
- 악성코드 상세 정보 제공 : 악성코드 탐지 및 치료뿐만 아니라 악성행위(정보유출, MMS 무단 전송 등)에 대한 상세한 정보를 제공하여 악성코드 피해에 따른 사용자의 효과적인 감사 활동을 지원

5.3 정부 기관 측면 대응 방안

모바일 악성코드에 효과적으로 대응하기 위해서는 정부가 국가적인 차원에서 모바일 악성코드에 대한 위험성을 알리며, 법제적, 관리적, 기술적인 지원을 제공해야 한다[15]. 아울러 스마트 폰 사용자와 모든 유관기관들의 역할을 할당하고 적극적인 참여를 유도하며, 이들을 효과적으로 조율할 수 있는 능력을 갖추어야 한다. 다음은 모바일 악성코드로부터 발생할 수 있는 피해를 최소화하기 위한 정부 기관 측면에서의 역할을 나타낸다.

- 관련법 제정 및 강화 : 급속히 발전하는 정보통신 기술을 이해하고 발생 가능한 새로운 범죄 활동에 대한 관련법을 제정하며, 위반에 대한 처벌 기준을 강화하여 정보보호 기반을 확립
- 교육을 통한 보안 인식 제고 : 인터넷을 포함한 각종 매체와 오프라인 세미나를 통해 모바일 악성코드에 대한 위험을 알리고, 사용자가 모바일 악성코드에 대응할 수 있는 가이드를 작성하여 배포
- 위협정보 및 분석 기술 상시 수집 관리 : 국내외 유관기관들과 정보를 공유함으로써 새로운 취약점과 악성코드에 관한 정보를 신속하게 수집 및 분석하며, 모바일 악성코드 조기 경보 시스템을 구축하여 사용자와 유관기관들에게 신속하게 통보
- 민관 협력 체계 구성 : 모바일 악성코드에 효과적으로 대응하기 위해 이동통신사, 단말기 제조사,

백신업체들로 구성된 민관 협력 체계를 구성
- 관련 기관의 협력 체계 지원 : 모바일 악성코드에 대비한 원활한 정보 공유를 위해 정기적인 협력 회의를 주최하며, 모바일 악성코드 테스트를 위한 망을 구축하여 제공

Ⅵ. 결 론

최근 트러스트 디지털사는 공격자가 스마트 폰을 통해 SMS 메시지를 전송하면, 메시지를 수신한 스마트 폰이 자동으로 웹페이지에 접속하여 모바일 악성코드를 다운로드하는 동영상을 공개하였으며[16-19], 가까운 미래에는 불법으로 스마트 폰에 내장된 멀티미디어 컴포넌트를 제어함으로써 사진 및 동영상을 촬영하고 외부로 전송하는 모바일 악성코드가 등장할 것으로 예상된다[4].

이에 본 논문에서는 국내의 모바일 악성코드의 등장 및 피해가 예상되는 현 시점에서, 그 심각성을 알리고자 모바일 악성코드를 소개하였으며, 이를 분석하기 위한 도구 및 분석 절차를 기술하였다. 그리고 마지막으로 모바일 악성코드에 의한 침해 사고를 조기에 예방하고 침해 사고 시 발생할 수 있는 피해를 최소화하기 위한 사용자, 이동 통신사, 단말기 제조사, 백신업체, 정부 기관 측면에서의 대응 방안을 제시하였다.

본 연구는 현재 모바일 악성코드에 대한 대응 준비가 부족한 국내 상황에 있어서 사용자들에게는 모바일 악성코드에 대한 효과적인 대응 능력을 제공하며, 관련 연구기관에게는 체계적인 악성코드 분류법 확립을 위한 초석을 마련한다는 점에서 큰 의미가 있다고 판단된다.

참 고 문 헌

〔1〕 Available at http://www.gartner.com/it/page.jsp?id=910112

〔2〕 Available at http://www.etimes.net/Service/etimes_2007/ShellView.asp?ArticleID=2009101513203001749&LinkID=6019&newsset=IT_juyo

〔3〕 정진혁, 이형찬, 김익수, 이정현, "모바일 악성코드 현황 및 대응 방안", *한국정보보호학회 동계학술대회*, 2009.

〔4〕 K. Dunham, S. Abu-Nimeh, M. Becher, S. Fogie, B. Hernacki, J. A. Morales, and C. Wright, *Mobile Malware Attacks and Defense*, Syngress, 2008.

〔5〕 W. Jansen and K. Scarfone, "Guidelines on Cell Phone and PDA Security," *NIST*, 2008.

〔6〕 A. Schmidt and S. Albayrak, "Malicious Software for Smartphones," Tech. Rep., *DAI-Labor*, 2008.

〔7〕 M. Khapra and N. Uchat, "Mobile Worms, Viruses and Threats," *Indian Institute of Technology*.

〔8〕 A. Gostev, "Mobile Malware Evolution: An Overview," 2006.

〔9〕 A. Gostev, "Kaspersky Security Bulletin 2006: Mobile Malware," 2007.

〔10〕 Available at http://www.f-secure.com

〔11〕 "The CIO's Guide to Mobile Security," *Research In Motion Limited*, 2006.

〔12〕 S. Sudan, S. Drake, and B, Burke, "Worldwide Mobile Device Security 2007-2011 Forecast," *IDC*, 2007.

〔13〕 "White Paper: Protecting mobile Data and Increasing Productivity," *Trend Micro*, 2007.

〔14〕 K. Scarfone and J. Padgette, "Guide to Bluetooth Security," *NIST*, 2008.

〔15〕 "Policy and Guidance for the Use of BlackBerry by the Australian Government," *Australian Government*, 2006.

〔16〕 "WAP Push Technology Overview," Openwave Systems, 2002.

〔17〕 "Comparison of WAP Push and Short Message Service(SMS)," *Openwave Systems*, 2002.

〔18〕 "WAP Push Architectural Overview," *Wireless Application Protocol Forum*, 2001.

〔19〕 Available at http://www.boannews.com/media/view.asp?idx=15635&kind=1

김 익 수 (Ik Su Kim) 정회원

2000년 2월 숭실대학교 컴퓨터학부
2002년 2월 숭실대학교 컴퓨터학과 석사
2008년 2월 숭실대학교 컴퓨터학과 박사
2009년 9월~현재 숭실대학교 컴퓨터학부 조교수
<관심분야> 시스템 보안, 네트워크 보안, 모바일 보안

이 형 찬 (Hyeong Chan Lee) 준회원

2010년 2월 숭실대학교 컴퓨터학부
2010년 3월~현재 숭실대학교 컴퓨터학과 석사과정
<관심분야> 모바일 보안, 시스템 보안

정 진 혁 (Jin Hyuk Jung) 학생회원

2004년 3월~현재 숭실대학교 컴퓨터학부
<관심분야> 모바일 보안, 시스템 보안

이 정 현 (Jeong Hyun Yi) 종신회원

1992년 2월 숭실대학교 전자계산학과
1995년 2월 숭실대학교 컴퓨터학과 석사
2005년 8월 University of California, Irvine 박사
1995년~2001년 한국전자통신연구원 연구원
2000년~2001년 Natinal Institute of Standards and Technology 객원연구원
2005년~2008년 삼성종합기술원 수석연구원
2008년~현재 숭실대학교 컴퓨터학부 조교수
<관심분야> 모바일 보안, 네트워크 보안, 응용보안