情報保護學會論文誌
第 22 卷 第 3 號, 2012. 6

스마트폰 악성코드 대응을 위한 모바일 보안 진단 시스템

천 우 봉,[1†] 이 정 희,[2‡] 박 원 형[3], 정 태 명[4]
[1]성균관대학교, [2]한국전자통신연구원 부설연구소, [3]극동대학교, [4]성균관대학교

The Mobile Security Diagnostic System against Smart-phone Threat

Woo Bong Cheon,[1†] Jung Hee Lee,[2‡] Won Hyung Park,[3] Tai Myoung Chung[4]
[1]Sungkyunkwan University, [2]The Attached Institute of ETRI, [3]Far East University,
[4]Sungkyunkwan University

요 약

최근 무선 전산망 인프라를 발판으로 스마트폰의 사용자가 크게 증가하고 있다. 이와 함께 스마트폰의 악성코드도 함께 급증하여 개인정보 유출, 과금 부과 등의 피해가 속출하고 있다. 무선전산망 환경의 보안 위협에 대처하기 위해 WIPS, MDM과 같은 무선 전산망 및 무선 단말 기기를 관리하기 위한 솔루션이 시판되고 있으나 이는 기업이나 대규모 사업자를 위한 솔루션으로 일반 스마트폰 사용자에게는 제한적이며 다양한 경로로 유포되는 알려지지 않은 악성코드를 탐지하는데 어려움이 있다. 본 논문에서는 악성코드 유형에 따른 행위 분석을 바탕으로 스마트폰 시스템 점검을 수행하여 악성 코드 감염 여부를 판별할 수 있는 기초 자료를 제공하며, 악성 코드 확산을 방지하기 위한 블랙리스트 관리 기능, 악성코드 채증 기능이 포함된 모바일 보안 진단 시스템을 제안한다.

ABSTRACT

With wireless network infrastructure, the number of smart-phone users is remarkably increasing in the world and the amounts of damage due to the smart-phone malwares are also raised. Many security solutions for wireless network have come into the market but these solutions are for companies or large enterprises, therefore, the public users of smart-phone don't feel easy to select as their solutions and it is difficult to detect unknown malwares. In this paper, we propose the mobile security diagnostic system for public smart-phone users, which provides functions like smart-phone system check, comparison with blacklist of applications and collecting malwares.

Keywords: Security, Smartphone, Mobile

I. 서 론

스마트폰 사용자가 급증함에 따라 스마트폰 악성코드 감염 피해도 급격히 증가하고 있다. 스마트폰 악성코드에 대비하기 위한 다양한 보안 솔루션들이 제공되고 있으나 기업이나 대규모 사업자를 위한 솔루션으로 일반 사용자에게는 쉽게 채택할 수 있는 방안이 아니다. MDM(Mobile Device Management) 제품의 경우는 무선단말기 관리, 엑세스관리, 응용 관리 등의 기능들을 제공하지만 완성도에 있어 아직 초기단계의 서비스를 제공하는 제품들이 많고 서서히 진화되고 있다[1]. 이외에도 안티바이러스(Anti-virus) 를 이용한 접근방법으로, 통신사에서 무료로 안티바이러스 앱을 배포하여 스마트폰 악성코드 감염 피해를 감소시키고자 한다. 그러나 대부분의 안티바이러스 업체에서는 이미 유포된 악성코드를 분석하여 대응 방안을 마련하

접수일(2011년 10월 31일), 수정일(2011년 10월 21일), 게재확정일(2011년 10월 21일)
† 주저자, cwb3242@naver.com
‡ 교신저자, lake@ensec.re.kr

기 때문에 알려지지 않은 취약점에 대해서는 역시 차단이 어렵다. 더구나 안드로이드폰의 경우 사설 앱 마켓에서의 앱 다운로드 및 설치가 손쉬울 뿐만 아니라 웹브라우저를 통해서도 쉽게 설치할 수 있어 악성코드 차단이 특히 어렵다. 이에, 일반 스마트폰 사용자들이 손쉽게 사용할 수 있는 악성코드에 대한 대응 방안이 필요하다.

본 논문에서는 스마트폰의 악성코드로 인한 피해를 줄이고 악성코드 확산을 방지하기 위해 스마트폰 시스템 점검 도구, 블랙리스트 관리 도구, 악성코드 채증 기능이 포함된 모바일 보안 진단 시스템을 제안한다. II 장에서는 스마트폰 보안 동향을 살펴보며, III 장에서는 스마트폰 악성코드를 분석하여 스마트폰 시스템 점검 도구에서 사용할 점검 항목을 정의하는 자료로 사용한다. IV 장은 본 논문에서 제안하는 모바일 보안 진단 시스템의 기능 및 기대 효과에 대하여 기술한다.

II. 스마트폰 보안 동향

2009년 3월까지 국내에서 사용하는 휴대전화에 대해 WIPI(Wireless Internet Platform for Interoperability) 플랫폼 탑재 의무화라는 폐쇄적인 정책을 사용한 시기에는 다른 나라보다 상대적으로 악성코드 감염률이 낮았다. 하지만, 2009년 4월 WIPI 사용 의무화가 폐지되어 애플 아이폰, 구글 안드로이드 계열의 스마트폰이 국내 사용이 허용되었다. 이와 함께 다양한 악성코드가 유입되어 스마트폰 악성코드 감염 피해가 발생하고 있다. 국내에 최초로 발생한 피해 사례는 2009년 4월, 윈도우 모바일 OS의 취약점을 이용한 트레드다이얼(TredDial)로 모바일 게임과 코덱 유틸리티에 포함되어 배포, 50초 단위로 국제전화를 걸어 사용자에게 과다 요금을 징수하도록 하였다[2]. 현재 국내 스마트폰 가입자는 2011년 7월 기준 1500만 명 이상으로 급증하였고, 스마트폰 악성코드도 2010년 3월 기준 500여개에서 2011년 3월 기준 1,200여종으로 1년 사이에 2배 이상 증가한 것으로 나타났다[3].

본 장에서는 무선전산망을 통한 악성코드 유포 탐지 및 차단하기 위한 방법들과 앱 유통 경로인 앱 마켓에서의 앱 관리 현황을 살펴본다.

2.1 무선전산망 접근 단말기기 관리

대부분의 스마트폰에는 무선랜칩이 기본 탑재되어 있어 3G 뿐만 아니라 무선랜을 이용한 인터넷 접근이 가능하다. 이로 인해 무선랜의 보안 취약점을 이용한 공격으로부터 스마트폰도 자유로울 수 없다. 비인가 AP 사용, 보안정책 위반 AP, Ad-hoc 네트워크, AP MAC 복제 등의 위협에 대응하기 위해 전파 신호를 감시하는 다양한 무선 IPS(WIPS, Wireless Intrusion Prevention System) 제품들이 있다. 대표적인 제품으로는 모토롤라의 AirDefense와 AirTight의 SpectraGuard이며, AirDefense Enterprise는 무선랜은 물론, 3G, 블루투스, 와이브로까지 감시 대상을 확대하여 모니터링하고 위협에 대한 보호 기능을 제공한다.

무선 단말기 관리, 엑세스 관리, 응용 관리, 메시지 푸쉬 기능을 특징으로 하는 MDM(Mobile Device Management) 솔루션이 있다. 일반적인 MDM의 구조는 무선 단말기를 관리하는 명령어를 전송하는 서버 컴포넌트와 무선 단말기에 설치되어 서버로부터 명령어를 수신하고 해당 명령을 수행하는 클라이언트 컴포넌트로 구성되어 있다. MDM 솔루션은 제품마다 제공하는 기능에는 차이가 있을 수 있지만, 소프트웨어 업데이트, 원격 설정, 백업 및 복구, 카메라 또는 wifi 차단과 같은 장치 제어, 화면캡쳐 방지, 스마트폰 위치 추적, 원격 데이터 삭제 등의 기능을 제공한다. 대표적인 제품으로는 Mobile Iron의 MDM과 Sybase의 Afaria 등이 있다.

2.2 스마트폰 앱 마켓 보안 정책

폐쇄적인 정책을 사용하는 애플은 앱 개발을 위해서 다운로드하는 SDK도 개발자 등록 후 다운로드 가능하도록 하며 앱스토어에 앱 등록 절차도 개발자가 앱 등록을 신청하면 해당 앱의 악성코드 유무를 판별해 등록 여부를 결정한다[5].

개방성을 표방한 안드로이드 계열의 스마트폰에서 상대적으로 악성코드 감염률이 높게 나타난다. 구글 마켓은 악성코드에 대한 필터링 장치가 존재하지 않으며 사용자의 신고 누적 시 악성 앱을 제거하는 정책을 사용하고 있다. 또한 앱 설치를 위한 인터페이스도 설치 전용 소프트웨어 없이 웹브라우저로만으로도 앱을 설치할 수 있어 악성코드 유포가 용이하다[5].

국내외 통신사들도 스마트폰 악성코드 차단을 위해 [표 1]과 같이 자사 스마트폰 가입자를 대상으로 자사 마켓에서 안티바이러스 앱을 무료로 배포하고 있다.

〔표 1〕 각국 통신사 앱 마켓에서 제공하는 안티바이러스

국가	통신사	앱마켓	안티바이러스
미국	AT&T	AppCenter	Internet Security Suite
	Verizon	MediaStore	Internet Security Suite
중국	China mobile	Mobilemarket	NetQin Anti-virus
일본	Docomo	Docomo market	VirusScanMobile
한국	SKT	T-스토어	바이러스스캔모바일 알약 안드로이드 바이로봇 모바일
	KT	Olleh마켓	KT 모바일 보안 알약 안드로이드
	LG U+	OZ 스토어	알약 안드로이드

2.3 스마트폰 보안 점검 도구

방송통신위원회와 한국인터넷진흥원에서 스마트폰 보안 자가점검 앱 Self Security Checker(S.S. Checker)를 개발하여 2011년 9월 배포하였다. 주요 기능은 스마트폰의 비밀번호 패턴 설정, 안티바이러스 설치 여부, 사용 프로그램에 대한 악성코드 감염 여부 등을 점검하여 취약한 부분에 대해 안티바이러스 설치, 악성 앱 삭제 등의 조치 방법을 사용자에게 안내한다〔6〕.

III. 스마트폰 공격 유형

3.1 악성코드 감염 경로

악성코드는 다양한 경로를 통해 스마트폰에 설치된다. 주로 인터넷 접근을 통한 경우가 많다. 이외에도 PC와 동기화 시 PC나 스마트폰으로 악성코드 유입이 가능하며, 블루투스 스캐닝 등의 방법으로 감염된 스마트폰이 타 스마트폰에 악성코드를 감염시키기도 한다〔7〕.

3.1.1 인터넷 접속을 통한 감염

스마트폰은 PC처럼 인터넷 사용이 가능한 단말기로, 웹브라우징, SNS, 이메일, 앱 마켓 등을 통해 각종 바이러스, 웜, 트로이목마와 같은 악성코드 감염이 가능하다. SNS 사용 중에 단축 URL 등 악성 링크 판단이 직관적으로 어려운 사이트에 접근하여 악성코드에 감염되기도 한다.

3.1.2 PC와 연결 시 감염

스마트폰 사용자는 ActiveSync, iTunes와 같은 프로그램을 이용하여 앱 다운로드, 이메일, 일정 등의 정보를 동기화하기 위해 PC와 연결을 한다. 공격자는 동기화에 사용하는 PC를 감염시킨 후 스마트폰에 연결 시 악성코드가 감염시킬 수 있다. 반대로, 악성코드를 보유한 스마트폰 또는 메모리카드를 PC에 장착할 때 PC를 감염시킬 수 있다.

3.1.3 타 스마트폰을 통한 감염

블루투스, UWB(Ultra Wideband)와 같은 WPAN을 사용하여 스마트폰은 다른 스마트폰을 스캔할 수 있으며 악성코드도 감염시킬 수 있다. 심비안 OS를 탑재한 S60 플랫폼을 타겟으로 한 카비르(Cabir)의 경우, 블루투스로 주변 스마트폰을 지속적으로 스캔하여 악성코드를 전파시킨 악성코드이다.

3.2 스마트폰 악성코드 유형

악성코드를 사용자에게 피해를 주는 형태에 따라 시스템 변경, 서비스 거부 공격, 과금 피해 유발, 개인정보유출 유형으로 구분하여 살펴본다.

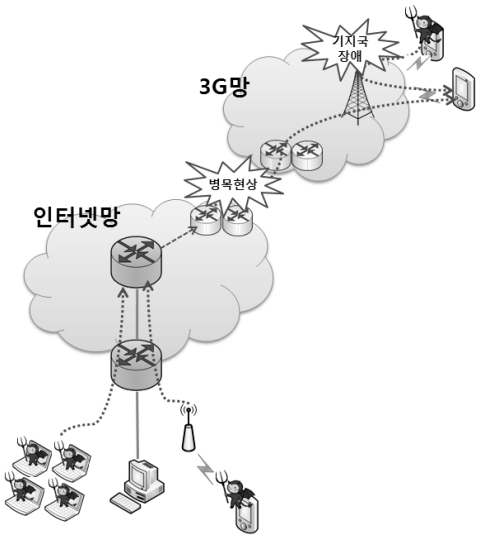
3.2.1 시스템 변경 유형

스마트폰에 침투하여 시스템의 주요 파일을 삭제하거나 변형하여 스마트폰 사용에 문제를 일으키는 유형이다〔8〕.

루트킷이라 불리는 악성코드를 이용하여 시스템 파일들을 변경할 수 있으며 이 악성코드는 스마트폰에 침입한 사실을 은폐하기 위해 침입 흔적을 지우고 루트 권한을 획득한다. 스마트폰 OS 취약점을 이용해 OS 영역에 악성코드를 삽입하는 방법 등으로 루트권한 획득할 수 있다. 루트권한을 획득한 후 전체 혹은 일부 주요 파일을 삭제하여 시스템의 오동작을 일으킨다. 특히 안드로이드 계열 스마트폰에 침입한 루트킷은 리눅스 커널모듈로 실행되어 매우 강력한 공격 도구가 될 수 있으므로 각별한 주의가 필요하다.

3.2.2 분산 서비스 거부 공격

공격자가 악성코드에 감염된 스마트폰을 이용해 불



〔그림 1〕 분산 서비스 거부 공격

특정 다수의 번호로 전화통화를 시도할 수 있다. 이 경우 기지국에 부하를 주어 통화 장애가 발생할 수 있다. 좀비 스마트폰들이 다량의 음성전화 또는 SMS를 발신하여 기지국에 부하를 발생시켜 기지국에 장애를 초래하는 서비스 거부 공격 방법이 있다. 또 외부 인터넷망에서 대규모 네트워크 트래픽을 발생시켜 인터넷망과 3G망 사이에 병목현상을 발생시킬 수 있다. 이로 인해 최대 사용가능한 회선 용량을 초과해 휴대단말기가 3G망을 통해 외부 인터넷 사용을 못하게 하는 분산 서비스 거부 공격 방법이 있다〔7〕.

3.2.3 과금 피해 유발 유형

사용자 모르게 SMS, MMS 등의 스팸 문자를 발송하거나 휴대전화 소액결제, 국제전화 발신 등의 방법으로 과금 부과를 유발하는 유형이다.

안드로이드 OS가 탑재된 스마트폰에서 발생한 TrojanSMS.AndroidOS.FakePlayer.a는 동영상 플레이어인 MoviePlayer로 위장하여 UI 없이 사용자 모르게 SMS를 전송하여 과금 피해를 발생시킨 트로이목마이다〔8〕.

3.2.4 개인 정보 유출 유형

연락처 정보, 통화내역, 위치 정보 등의 개인 신상정보를 전송한다거나 IMEI, 은행계좌정보 등 기밀정보를 유출하는 유형이다.

개인정보유출형 악성코드 사례로는 2010년 7월 Blackhat USA 2010에서 발표된 Jackey Wallpaper가 있다. 스마트폰의 배경화면을 변경해주는 이 무료앱은 약 400만 명의 사용자가 다운로드하였으며 전화번호, 가입자 식별번호, 음성메일함 비밀번호 등을 사용자 모르게 수집하였다〔8〕.

이 외에도 파일을 대량 복사하거나 전파 송수신을 발생시켜 스마트폰의 성능을 저하시키거나 배터리를 소모시키는 공격 유형이 있다〔9〕.

3.3 스마트폰 악성코드 감염 사례

최근에 탐지된 악성코드들은 기존의 악성코드의 변종 형태가 많았다. 악성코드들의 행위를 분석하여 스마트폰 시스템 점검 시 주의깊게 살펴볼 항목들을 선별할 수 있다.

3.3.1 DroidDeluxe

DroidDeluxe〔10〕는 루트권한을 획득하는 악성코드로, 실행 시 제조사, 모델명 등 스마트폰에 설정된 다양한 정보를 수집한다. 이 정보는 특정 구글 계정(UA-19670793-1)을 사용하여 업로드된다. DroidDeluxe 패키지에 포함된 루트 익스플로잇 코드가 사용자 모르게 백그라운드로 실행되어 루트 권한 획득을 시도한다. 루트권한 획득이 성공하면 DroidDeluxe에 포함된 special이라는 이름의 실행코드가 스마트폰의 계정 관련 파일들의 모드를 읽기쓰기 가능하도록(world-readable, world-writable) 변경하여 계정 정보, 연락처 등의 주요 정보를 유출한다.

3.3.2 DroidOS/Spitmo 트로이목마

공격자는 일차적으로 은행 웹페이지에 악성코드를 삽입하여 온라인뱅킹 서비스를 이용하기 위한 필수 보안 모듈인 것으로 가장하여 사용자로 하여금 스마트폰에 다운로드하도록 유도한다. 2단계로 사용자가 설치 버튼 클릭 시 악성코드 유포 사이트에서 앱을 다운로드하여 스마트폰에 설치하게 되고 설치 완료를 위해 특정 숫자로 전화를 걸게 한다. 이 때부터 악성코드가 활성화된다. 3단계로, 트로이목마가 성공적으로 설치 완료되어 모든 SMS를 가로채어 C&C 서버로 전송이 가능해진다. 4단계는 SMS를 감시하고 C&C 서

버와 통신하는 단계이다. 이 트로이목마가 접근을 시도하는 URL를 분석한 결과, 124ff42.com, 124ff-dfsaf.com, 124sfafsaffa.com, 124ffsaf.com 4개의 도메인을 사용하는 것으로 나타났다[11].

잉카인터넷 대응팀에 따르면, DroidOS/Spitmo 트로이목마는 Spyeye 봇 계열의 악성코드로 의심이 되지만 아직까지 특별한 연관성을 찾지 못했다고 발표했다[12].

3.3.3 Basebridge

안드로이드 2.3 이전의 버전에 존재하는 취약점을 이용한 악성코드로, 추가 악성 페이로드를 사용자가 모르게 설치한다. 이 악성 페이로드는 원격 서버에 접속하여 스마트폰의 IMSI(International Mobile Subscriber Identity), OS 정보와 같은 개인 정보를 전송한다. 또, SMS를 전송하거나 수신함에 있는 특정 SMS 메시지를 삭제한다. AdSmsService, BridgeProvider와 같이 사용자가 모르는 서비스가 스마트폰에 설치된 경우 이 악성코드 감염을 의심할 수 있으며, 인터넷 접속으로 인한 과금 피해가 발생할 수 있다[13].

3.3.4 Cruisewind

SMS 릴레이하는 안드로이드용 악성코드로, 감염된 스마트폰이 메시지 송수신을 위한 프록시 장치가 되도록 한다. 처음 설치 후 빈 화면을 띄운 후 몇 초 후 바로 사라진다. FlashService가 설치되며 이 서비스는 스마트폰이 원격 서버와 통신을 허용하도록 한다. 원격서버로부터 XML 설정 파일을 다운로드한 후, 이 파일에 인코딩되어 저장되어 있는 특정 번호로 메시지를 지속적으로 전송하여 과다 요금 부과를 유도하며 사용자가 인지못하도록 메시지 송신 후 보낸문자함에서 제거한다. FlashService 서비스나 com.flashp 프로세스가 실행되는 경우 이 악성코드 감염을 의심할 수 있다[14].

IV. 모바일 보안 진단 시스템 제안

WIPS나 MDM은 강력한 보안 기능을 제공하지만, 이는 기업이나 대규모 사업자를 위한 솔루션으로 일반 스마트폰 사용자들은 안티바이러스를 설치하여 모바일 공격에 대비하고 있다. 하지만, 안티바이러스의 경우도 알려진 공격에 대해서는 탐지 및 차단이 되지만 알려지지 않은 공격에 대한 차단이 어렵다. 안드로이드폰의 경우 상대적으로 관리가 되는 통신사 앱 마켓 이외에도 자유롭게 오픈한 사설 앱 마켓에서 다운로드 및 설치가 가능해 악성코드에 쉽게 감염될 수 있다.

스마트폰 보안 점검 도구인 S.S. Checker는 안티바이러스 설치 유무, 악성앱 설치 유무, 사용하는 비밀번호의 안전 여부, 무선 장치 등의 보안설정 상태를 점검해 취약한 보안 설정을 점검한다. 하지만 안티바이러스에 의한 점검에 의존하여 안티바이러스에서 제공하지 않은 악성코드에 대해서는 탐지가 불가능하며 보안 설정 점검만으로는 과도한 통신시도, 주요 파일 변경 등의 이상징후를 판단하기 어렵다.

이 장에서는 일반 스마트폰 사용자가 손쉽게 자신의 스마트폰의 악성코드 감염 여부를 진단하고 이상징후를 발견할 경우 신고할 수 있는 경로를 제공함으로써, 스마트폰 악성코드에 신속히 대처할 수 있는 프레임워크를 제시한다.

[그림 2] 모바일 보안 진단 시스템

4.1 스마트폰 시스템 점검 도구

스마트폰 악성코드들은 악성 프로세스를 실행하거나 주요 파일들의 권한을 변경하는 등의 행위를 한다. 스마트폰 시스템 점검 도구는 이러한 행위들을 탐지하기 위한 기초 자료들을 수집한다.

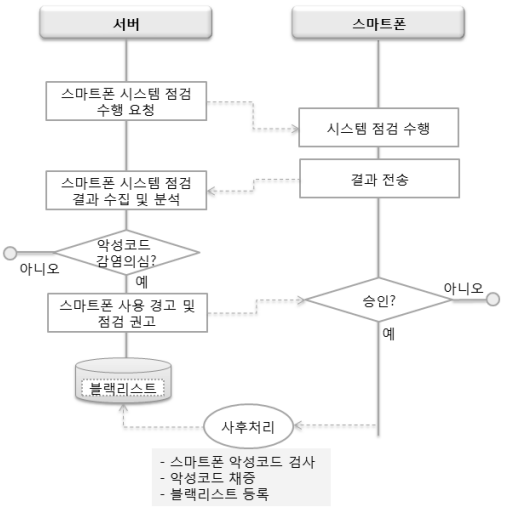
[표 2]는 스마트폰 시스템 점검 도구에서 점검할 항목들을 나타낸다. 악성코드마다 실행 프로세스명이나 수정한 파일들이 다를 수 있지만 아직 알려지지 않은 악성코드이더라도 이상 징후를 발견할 수 있다.

[그림 3]은 점검 도구 실행 절차를 나타낸다. 점검 도구 실행은 서버에서 점검 요청을 보낼 수도 있으며

〔표 2〕 스마트폰 시스템 점검 항목

수집항목	점검사항
시스템 정보 (OS 버전, 모델명 등)	점검 기초 정보
앱 설치 목록 (이름, 설치일시, 해쉬값 등)	악성의심 또는 악성 앱 식별
실행 중인 앱 목록	악성 프로세스 점검
SMS 전송 및 통화 발신 횟수	과다 요금 부과 악성 코드 존재 여부
주요파일들의 목록 (권한, 수정일시 등)	루트 권한 획득 여부
앱 다운로드 이력	신뢰할 수 없는 앱 마켓에서의 다운로드 여부
쉘 실행 현황 및 이력	악성으로 의심되는 불필요한 쉘 실행 여부
접속한 URL 목록	악성 URL 접속 여부
블루투스 장비 등 연결 이력	과도한 무선 연결 시도 점검 (배터리 소모형 공격)
Wifi, 3G데이터 접속 이력	과도한 데이터 연결 점검 (DDoS 공격, 과다 요금 부과 공격)

사용자의 필요에 의해 직접 실행 가능하다. 점검 도구 수행 결과는 파일로 저장되어 사용자가 확인이 가능하고, 사용자가 요청할 경우 서버에 결과 파일을 전송하여 담당자에게 분석을 요청할 수 있다. 점검 요청을 위해 서버에 파일을 전송할 때는 점검 결과 파일을 암호화하여 보호하고, 압축하여 데이터 전송량을 감소시킨다. 서버는 수신 후 결과파일을 압축 해제하고 설정



〔그림 3〕 시스템 점검 도구 수행 절차

〔표 3〕 안드로이드 계정관련 파일

/data/system/accounts.db /data/data/com.android.email/databases/EmailProvider.db /data/data/com.android.providers.contacts/databases/contacts2.db /data/data/com.android.providers.telephony/databases/mmssms.db

된 암호키를 사용하여 복호화한다.

악성코드 확산 속도가 빠른 구글 안드로이드 계열 스마트폰에서의 몇 가지 점검항목을 예로 들어보면, system/packages.xml 파일을 이용해 스마트폰에 설치된 앱 목록을 조회할 수 있다. 이 파일 안에 포함된 〈perms〉 태그 항목에 설정된 값으로 앱의 사용 권한을 확인할 수 있다. 안드로이드폰의 계정 관련 정보는 〔표 3〕에 명시된 파일들에서 확인이 가능하다. 이 파일들의 권한이 world-readable, world-writable로 설정되어 누구나 읽기, 쓰기 가능한 모드일 경우 감염이 의심된다.

윈도우모바일폰의 경우 레지스트리 점검을 통해 설치된 응용의 정보를 확인할 수 있으며 tasks 명령어로 실행되고 있는 프로세스 목록을 확인할 수 있다.

4.2 블랙리스트 관리

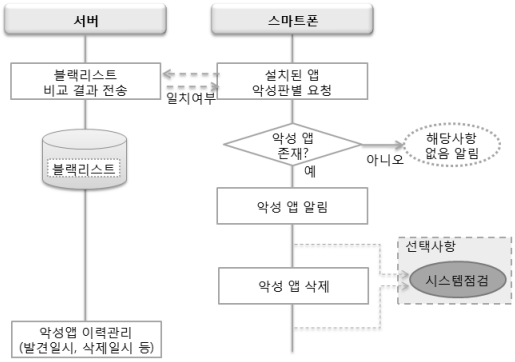
블랙리스트 관리는 이미 악성코드로 식별된 앱과 사용자의 스마트폰에 설치된 앱을 비교하여 악성 앱이 설치된 경우 경고 및 해당 앱의 실행을 차단하는 기능이다.

4.2.1 스마트폰용 블랙리스트 앱 DB

블랙리스트 앱 DB는 기존의 악성 앱 뿐만 신규로 발생한 악성 앱에 대해 신속히 추가되는 것이 관건이다. 안티바이러스 업체와 같은 상용 DB, Androguard〔15〕와 같은 공개된 DB, 사용자가 수집한 블랙리스트 DB와 연결하여 최신 악성코드 정보 제공이 가능하다. 또한 개발자 인지도나 앱의 사용 평가도 악성 의심 앱을 판단하기 위한 자료로 사용할 수 있다. 다양한 경로를 통해 블랙리스트 DB를 마련한다.

4.2.2 악성 앱 설치 확인

블랙리스트에 해당하는 악성 앱이 설치된 것이 확

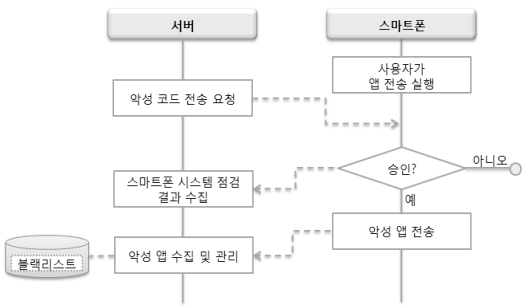


〔그림 4〕 블랙리스트 비교 절차

인되면 스마트폰을 변경한 내역을 확인하기 위해 시스템 점검을 선택 실행할 수 있다. SMS, 국제전화 발신 등의 과금이 부과되는 공격 유형인 경우 해당 앱을 신속히 삭제하거나 프로세스 실행을 중단시켜야 한다. 삭제 후 시스템 검검을 수행하여 시스템 변경 사항 및 통신 이력을 확인할 수 있다. 앱 삭제 전에 시스템 점검을 수행하게 되면 좀더 많은 악성코드의 행위 분석 자료 수집이 가능하다. 〔그림 4〕는 블랙리스트에 포함된 앱과 스마트폰에 설치된 앱을 비교하는 절차를 나타낸다.

4.3 악성코드 채증

〔그림 5〕는 악성코드 채증 절차를 나타낸다. 이상징후 확인 후 다른 스마트폰으로의 악성코드 확산을 방지하기 위해 서버 혹은 담당자에게 악성코드를 전달하여 상세 분석을 요청할 수 있다. 상세 분석은 모바일 가상 시뮬레이션 기능을 제공하는 HoneyM〔16〕과 같은 다양한 방법을 이용하여 분석이 가능하다. 악성코드 설치 유무를 가장 빨리 확인할 수 있는 방법이 안티바이러스에서 사용하는 시그니처 기반의 패턴 검색 방법이다. 악성코드 채증 절차를 통해 스마트폰용 악성코드 수집 및 분석에 활용되어 악성코드로 판별될 경우 블랙리스트 데이터베이스에 추가되어 스마트폰에 설치된 악성코드를 빠르게 탐지할 수 있다.



〔그림 5〕 악성코드 채증 절차

V. 결 론

모바일 보안 진단 시스템은 스마트폰 시스템 점검을 통해 스마트폰의 이상징후를 발견할 수 있는 방법을 제공한다. 사용자가 스마트폰에 설치된 이상징후를 확인할 수도 있으며 보안담당자에게 점검 요청을 할 수도 있다. 블랙리스트 DB와 연동, 스마트폰에 설치된 악성코드를 탐지해 악성코드로 인한 피해를 막을 수 있다. 악성코드 채증 기능은 알려지지 않은 악성코드들의 수집경로로 활용할 수 있으며 수집된 앱이 악성으로 판별될 경우 블랙리스트로 등록되어 악성코드 확산을 방지할 수 있을 것으로 기대한다.

참고문헌

〔1〕 IT World Korea, "기업 내 모바일 기기 관리, 포레스터의 10가지 팁", http://www.itworld.co.kr/news/71870, 2011.9.27.
〔2〕 전남대학교 산학협력단, "스마트폰 기반 악성코드 수집/분석 플랫폼 개발을 위한 연구", 한국인터넷진흥원, 연구보고서 KISA-WP-2010-0076, 2010.12.
〔3〕 김동우, "스마트폰 보안 앱 서비스 동향", 주간기술동향, pp. 18-20, 정보통신산업진흥원, 2011.10.
〔4〕 Wikipedia MDM, http://en.wikipedia.org/wiki/Mobile_device_management
〔5〕 Dino A. Dai Zovi and Alexander Sotirov, "Mobile Attacks and Defense", Securiy & Privacy, vol. 9, pp. 68-70, IEEE, 2011.
〔6〕 S.S. Checker 앱, https://market.android.com/details?id=com.kisa.secheck.android&feature=search_result
〔7〕 Chuanxiong Guo, Helen J. Wang, Wenwu Zhu, "Smart-Phone Attacks and Defenses", Proceedings of the 3rd Workshop on Hot Topics in Networks (HotNets), 2004.
〔8〕 서승현, 김종명, 전길수, "2010년 모바일 악성코드 동향 분석 및 전망," 정보보호학회지, 21(1), pp.

11-18, 2011년 2월.
〔9〕 강동호, 한진희 외, "스마트폰 보안 위협 및 대응 기술", ETRI 전자통신동향분석, 25(3), pp. 72-80, 2010.6.
〔10〕 DroidDeluxe, http://www.csc.ncsc.edu/faculty/jang/DroidDeluxe
〔11〕 SymbOS/Spitmo 트로이목마, http://droidsecurity.appspot.com/securitycenter/securitypost_20110601.html,
〔12〕 잉카인터넷대응팀, http://erteam.nprotect.com/tag/spyeye
〔13〕 Basebridge, http://www.fortiguard,.com/encyclopedia/virus/android_basebridge.a!tr.html
〔14〕 CruiseWind, http://blog.trendmicro.com/android-malware-acts-as-an-sms-relay
〔15〕 Androguard, http://code.google.com/p/androguard
〔16〕 T.J. O'cornor, Ben Sanster, "honeyM: a framework for implementing virtual honeyclients for mobile devices", WiSec '10 Proceedings of the third ACM conference on Wireless network security, pp.129-138, USA, 2010.3.

〈著者紹介〉

천 우 봉 (Woobong Cheon) 종신회원
2009년~현재: 성균관대학교 전자전기컴퓨터공학과 박사과정
〈관심분야〉 보안관제, 보안정책, 침해사고대응

사 진

이 정 희 (Junghee Lee) 정회원
1999년: 서강대학교 컴퓨터학과 학사
2004년: 한국과학기술원 전산과 석사
현재: ETRI 부설 연구소 연구원
〈관심분야〉 보안관제, 사이버보안

박 원 형 (WonHyung Park) 종신회원
2009년~2011년: 서울과학기술대학교 산업정보시스템공학과 겸임교수
2012년~현재: 극동대학교 정보경영학과 전임교수
〈관심분야〉 스마트폰 취약점, 보안관제, 윈도우포렌식

정 태 명 (Taimyoung Chung) 종신회원
1984년: 미국 일리노이 주립대학교 전산학과 졸업
1987년: 미국 일리노이 주립대학교 컴퓨터공학과 석사
1995년: 미국 퍼듀대학교 컴퓨터공학과 박사
현재: 성균관대학교 정보통신공학부 교수
〈관심분야〉 사이버보안, 소프트웨어공학