한국컴퓨터정보학회지
제22권 제1호, 2014. 6.

모바일 악성코드 유포 동향과 대응방안

• 최상용 (한국과학기술원 사이버보안연구센터)

I. 서론

최근 모바일 사용환경의 발전은 상시적으로 네트워크에 연결되어 있는 다양한 기능으로 인해 생활의 편리성을 가져다 준 반면 모바일 기기에 저장된 개인정보, 모바일 서비스를 이용한 소액결재 등을 노린 공격자의 주요 공격 대상이 되고 있는 것이 현실이다. 본 연구에서는 모바일 환경에서 늘어나고 있는 모바일 악성코드의 유포 동향과 사례에 대해 살펴보고 모바일 악성코드에 능동적으로 대응하기 위한 대응체계를 제안하고자 한다.

본 연구의 구성은 2장 관련연구에서 최근 증가하고 있는 모바일 악성코드 동향과 유형, 대응을 위한 연구내용을 살펴보고, 3장에서 모바일 악성코드의 현 대응체계의 한계점 및 능동적인 대응을 위한 대응체계를 제안하며 4장에서 결론을 맺는다.

II. 관련 연구

1. 모바일 환경의 특성과 공격

모바일 컴퓨팅 환경은 PC컴퓨팅 환경과 비교하여 그림 1과 같이 크게 3가지의 특성을 갖는다. 첫 번째 특성은 휴대성이다. 모바일 컴퓨팅 환경은 휴대전화와 연결되어 있기 때문에 항상 휴대하는 기기이며, 다양한 데이터 교류와 주체간의 상호작용의 기반이 된다. 두 번째 특성은 네트워크 상시연결이다. 모바일 기기는 대부분의 경우 인터넷에 상시 연결되어 사용자는 인지하지 못하지만 애플리케이션 및 콘텐츠의 업데이트가 이루어진다. 모바일 환경의 세 번째 특징은 다기능화이다. 과거 휴대전화 환경과는 달리 최근에는 모바일 단말기를 이용한 뱅킹, 쇼핑, SNS(Social Network Service), 문서작업 등 PC에서 제공하는 기능의 대부분을 모바일 단말을 통해서 할 수 있다.

이와 같은 3가지의 특성은 PC를 활용하여 인터넷상의 서비스를 제공받던 환경에서 모바일 단말기를 사용하게 됨으로 궁극적으로 생활의 편리함을 가져다 준 반면, 다양한 서비스를 사용하기 위해 모바일 단말에 저장되는 개인정보, 금융정보 등은 공격자들이 탈취하고자 하는 대상이 되며, 공격자들은 모바일 단말 사용자들에게 금전적인 피해를 입히기 위해 모바일 단말을 대상으로 국제전화 발신, 단문메시지 과다 발신, 소액결제 등의 비정상 동작을 유도한다. 즉, 모바일 단말 및 모바일 서비스는 그 환경적 특성으로 인해 점차 해킹의 대상이 되고 있다.

그림 1. 모바일 환경의 특성

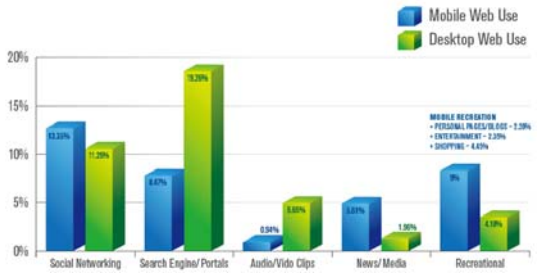

그림 2. 분야별 사용환경

웹보안 기업인 블루코트사에서 발표한 자료에는 특정 서비스에 대해서는 PC환경보다 모바일 환경을 더 많이 사용하는, 즉 PC환경에서 모바일 환경으로 변화되고 있는 증상을 더욱 잘 보여준다[1].

블루코트사에서 발표한 자료에 따르면 평균적으로 사용자는 애플리케이션을 사용함에 따라 연결되는 인터넷을 제외한 순수한 웹브라우징 시간이 하루 중 72분 정도로 확인된다. 이는 반대로 말하면 하루 중 72분 동안 위협이 존재하는 취약한 환경에 노출되어 있다는 것으로 간주할 수 있다. 특히 그림 2에 나타난 것과 같이 사용분야별 분포를 보면 소셜 네트워킹과 뉴스, 오락 등의 분야에서는 PC를 활용하는 시간보다 모바일 단말을 사용하는 시간이 월등이 많음을 알 수 있다.

이러한 사용특성의 변화로 인해 모바일 환경에서 동작하는 악성코드의 수 또한 급격히 증가하고 있다. 표 1에 보이는 것처럼 최근 3년간 월 평균 모바일 악성코드의 증가 추이는 가파른 상승세를 보여주고 있다[2].

표 1. 모바일 악성코드 탐지 수

연도	악성코드 탐지 수(월평균)
2011년	691건
2012년	21,892건
2013년	104,299건
2014년	145,041건

2. 모바일 악성코드 유형

모바일 악성코드는 2004년 심비안용 악성코드가 처음 등장한 이후 모바일 환경이 활성화되기 시작한 2006년 심비안 OS와 블랙베리 OS에서 동시에 동작하는 크로스 플랫폼(Cross Flatform) 악성코드가 증장하였으며, 애플의 iOS, 구글의 안드로이드 OS등이 등장한 2007년 이후 더욱 다양한 형태로 발전하고 있다[3].

이와 같은 모바일 악성코드는 대표적으로 기능적으로는 표 2와 같이 분류할 수 있다[4].

표 2. 모바일 악성코드 기능별 분류

유형	설명
Backdoor	공격자의 명령을 받아 모바일 기기에서 악의적인 행위를 하는 형태
Trojan	공격자가 원하는 데이터를 탈취하는 형태
Exploit	모바일 기기의 권한 상승을 획득하고자 하는 유형
HackTool	모바일 기기를 악의적으로 사용할 수 있도록 한 해킹 툴
Spyware	사용자 동의 없이 개인정보를 수집하고 탈취하는 유형

또한 모바일 악성코드는 PC용 악성코드와는 다르게 표 3과 같은 행위를 한다.

표 3. 모바일 악성코드의 행위

유형	설명
BOOT	부팅 완료 후 악의적인 행위
SMS	사용자 동의 없이 SMS문자 수발신, 가로채기
INTERNET	인터넷 모니터링 및 공격자 명령 수신 사용자 개인정보 유출
CALL	사용자 동의 없이 전화 수발신
USB	PC와 연결 후 악의적인 행위
PACKAGE	앱의 추가/삭제/수정/조회
BATTERY	배터리 과다소모 유발
SYSTEM	사용자 입력이나 화면의 좌표 가로채기
STORAGE	저장소의 데이터 추가/수정/삭제
GPS	사용자 동의 없이 위치정보 수집

3. 모바일 악상코드 유포 방법

모바일 단말기에 애플리케이션을 설치 할 때, 애플사의 IOS의 경우 애플사에서 운영하는 앱스토어를 통해서만 애플

리케이션 설치가 가능하다. 반면 안드로이드 단말기의 경우 구글사에서 운영하는 플레이스토어 외에도 각 통신사의 애플리케이션 마켓, 인터넷, Wi-fi, Bluetooth 등과 같은 파일직접 공유를 통해서도 애플리케이션 설치가 가능하다. 이러한 이유로 최근의 모바일 악성코드는 애플리케이션의 설치경로가 다양한 안드로이드 단말을 중심으로 유포되고 있다.

실제 모바일 악성코드 유포에 사용되는 방법은 크게 두 가지로 구분된다. 첫 번째는 애플리케이션 위변조이다. 즉 정상 애플리케이션으로 가장한 악성코드를 사용자로 하여금 다운로드 받을 수 있도록 유도하는 것이다[4][5]. Arxan사의 보고자료[6]에 따르면 2012년 안드로이드 마켓 상위 100개 유료 앱에 대한 위변조 애플리케이션이 모두 존재하는 것으로 확인된다. 모바일 악성코드 유포의 두 번째 방법은 PC상에서 가장 큰 위협이 되고 있는 Drive-by download공격[5]과 유사한 형태의 모바일 Drive-by download이다. Drive-by download 공격은 그림 3과 같이 공격자는 취약한 웹서버를 해킹하여 악성코드 경유지로 연결되는 링크를 삽입한다. 각 경유지에서는 Hidden iframe, JavaScript등을 이용하여 경유지들 사이에 링크를 형성하고, 최종적으로 악성코드 유포지로 연결된다. 만약 취약한 PC가 해킹당한 웹사이트에 접속한다면 사용자의 추가적인 행위 없이 자동으로 유포지로 연결되어 악성코드에 감염된다.

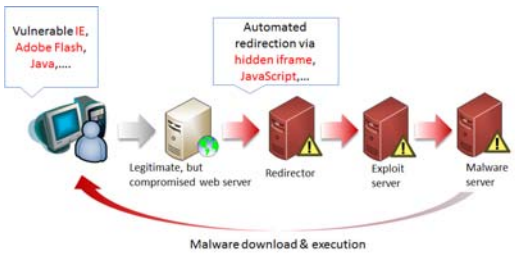

그림 3. Drive-by download 절차

모바일 환경에서 Drive-by download가 일어나는 과정 또한 그림 3과 유사하다. 다만 모바일 환경에서는 사용자를 적극적으로 유도한다. 그 첫 번째 예시는 QR코드(Quick Response Code)를 활용하는 것이다[5]. QR코드는 격자무늬의 패턴 내에 많은 정보를 담고 있고, 웹사이트로 연결시키기 위한 링크가 포함되어 있다. 공격자는 QR코드를 사용자에게 MMS등을 이용하여 전송한다. 사용자가 만약 QR코드를 클릭하면 모바일 브라우저가 실행되면서 QR코드 내에 포함되어 있는 링크가 실행된다. 사용자는 단순히 QR코드를 실행했을 뿐이지만 QR코드 내에 포함된 악성링크로 인해 안드로이드 단말의 권한이 공격자에게 탈취된다.

그림 4. 단축URL

두 번째 예로는 단축URL을 사용하는 방법이 있다[5]. 단축 URL은 긴 URL을 짧게 줄여주는 것으로 대표적으로 그림 4에 보이는 것처럼 단축URL이 실제 어디로 연결되는지 URL상으로는 알 수 없다. 이러한 특성을 공격자들이 악용하여 QR코드와 마찬가지로 사용자에게 클릭을 유도하고, 악성코드를 감염시킨다.

세 번째 예는 PC용 악성코드를 유포하는 사이트에서 모바일용 악성코드를 같이 유포하는 방법이다[7]. 이는 최근 모바일 단말기의 풀브라우징 기능 등 기능이 확장됨에 따라 PC용 웹 화면을 모바일로도 접속이 가능하기 때문인 것으로 분석된다. 그림 5는 KAIST사이버보안연구센터에서 2014년 4월 탐지된 내용으로 PC용 악성코드를 유포하는 사이트에서 안드로이드용 악성코드를 같이 유포하고 있는 것이 확인되었다.

그림 5. PC용 악성코드와 모바일용 악성코드 동시 유포

4. 모바일 악성코드 탐지 기술

모바일 악성코드를 탐지하고 차단하기 위해 연구되고 있는

기술은 대표적으로 애플리케이션 자체의 위변조 및 행위를 분석하는 방향으로 진행되고 있다.

대표적인 애플리케이션 위변조 탐지기술은 기존 공식 마켓에 등록되어 있는 애플리케이션과의 유사도를 분석하는 기술이다[8]. 이는 위변조된 애플리케이션은 공식 마켓보다 제3의 경로를 통해 유통될 확률이 높다는 것과 원래의 애플리케이션과 위변조 애플리케이션은 일부 소스코드를 공유한다는 가정에 기반하고 있으며, 애플리케이션을 소스코드 레벨에서 분석하지 않고 opcode를 비교하는 방식으로 수행된다. 애플리케이션 위변조 탐지기술의 구성은 그림 6과 같다.

모바일 악성코드에 대응하기 위한 또 다른 접근 방법은 애플리케이션의 무결성을 검증하는 방법이다[9]. 이는 애플리케이션 실행 시점에 위변조 여부를 탐지하는 방법으로 이를 위해 애플리케이션 내부에 위변조 여부를 탐지하기 위한 특별한 코드를 포함한다. 이후 실행 시점에 애플리케이션의 해시값을 측정하고 외부 서버에 존재하는 올바른 해시값과 비교하여 무결성을 체크하는 접근을 사용한다. 이와 같은 접근은 최근 모바일 뱅킹, 보험증권 등 금융 애플리케이션에 주로 사용되고 있다.

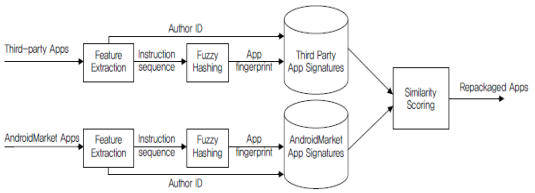

그림 6. 애플리케이션 위변조 탐지 기술

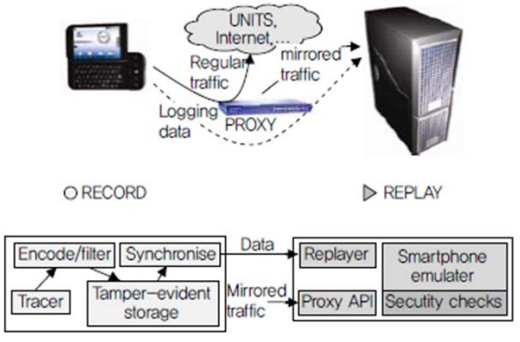

그림 7. Paranoid Android 시스템

위 두 가지 방법이 정적분석 방법이라면, 모바일 악성코드 탐지를 위한 또 다른 접근 방법은 악성코드 파일을 모바일 단말기 디버거나 에뮬레이터를 이용하여 실행 한 후 행동분석을 하는 동적 분석 방법이다. 이는 주로 안드로이드 기반 가상머신을 활용하여 실제 애플리케이션을 실행하고 실행 시 애플리케이션이 비정상적인 행위를 하는지를 분석하는 방법으로 정적분석의 한계점인 코드난독화가 적용된 악성코드에 대해 자동적으로 분석이 가능하지만 모든 가능한 실행패스를 다 분석하지 못한다. 예를 들어, 특정 취약점을 악용하는 악성코드일 경우 공교롭게도 실행환경이 해당 취약점을 가지고 있지 못한다면 악성코드를 탐지하지 못할 가능성이 있으며, 또 다른 경우로 두 개 이상의 취약점을 동시에 사용하는 악성코드를 둘 중 하나의 취약점만을 보유한 실행환경에서 실행할 경우 다른 하나의 취약점을 발견하지 못할 가능성이 있다. 대표적인 실행기반의 탐지기술은 Paranoid Android[10]라 불리는 시스템이다. 이는 그림 7과 같이 사용자 단말과 외부 서비스 사이에 프락시를 구축하고, 사용자로부터 발생되는 모든 트래픽을 프락시 서버에서 재실행 하는 방법을 사용한다.

하지만 이와 같은 방법은 사용자 단말의 모든 정보를 수집하기 때문에 개인정보보호 이슈 등으로 인해 현실적으로 적용이 쉽지 않은 것이 사실이다.

III. 모바일 악성코드 대응방안

이번 장에서는 기존 모바일 악성코드 대응의 한계점을 살펴보고 이를 해결하기 위한 접근방향을 제시하고자 한다.

1. 모바일 악성코드 대응의 한계점

앞 장에서 설명한 것처럼 최근 모바일 악성코드는 급격히 증가하고 있다. 이에 대응하기 위한 여러 가지 방법들이 나오고 있지만 알려진 방법들을 공통적으로 바이러스 백신과 같이 이미 악성코드가 감염된 단말에서 악성코드의 특징을 추출하여 분석하는 접근방법을 사용하고 있다. 하지만 악성코드가 단말기에 설치된다는 것은 단말기가 감염되었다는 것과 동일한 의미이기 때문에 어떤 의미에서는 사후 대응이다. 따라서 모바일 악성코드에 대응하기 위해서는 보다 능동적이고 사전적인 대응이 필요하다.

현재 모바일 악성코드 대응의 한계점은 크게 세 가지로 분석된다. 그 첫 번째는 보안패치 업데이트의 지연이다. 이는 PC와 비교해 볼 때, PC의 보안 취약점이 발견되면 OS제조사 또는 애플리케이션 제조사에서 즉시 보안패치를 발표하고, 사용자는 이를 쉽게 적용할 수 있다. 하지만 모바일 단말기, 특히 안드로이드 단말기의 경우 구글사에서 공급한 안드로이드 OS를 단말기 제조사 또는 통신사가 필요에 맞게 수정하여 사용한다. 따라서 안드로이드 OS의 보안패치를 적용하기 위해서는 OS제조사에서 발표한 보안패치를 단말기 제조사 또는 통신사에서 다시 수정하고 시험 한 후 적용이 가능하다. 이와 같은 단계는 그림 8에서 PC용 보안패치가 A,B,C 3단계로 적용되는 반면, 모바일 단말기용 보안패치는 E,F,G 3단계를 더 거쳐야 한다[5]. 일반적으로 이 단계는 수개월 이상 소요된다. 이러한 한계점으로 인해 발견된 보안 취약점을 공격자는 계속적으로 악용하게 되고, 결국 모바일 악성코드이 유포를 차단하기가 어렵게 된다.

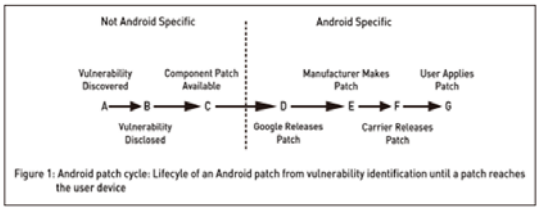

그림 8. 모바일 단말기 보안업데이트 절차

모바일 악성코드의 능동적인 대응의 두 번째 한계점은 유선환경과 상이한 네트워크 환경이다. QR코드, 단축 URL등은 육안으로 해당 링크가 악성인지 아닌지를 판단하기가 쉽지 않다. 또한 QR코드와 단축 URL과 같은 방법은 기존 PC 환경의 Drive-by download 탐지 기술에 그대로 적용하기에 한계가 있다.

마지막으로 세 번째 한계점은 PC악성코드 유포에도 많이 사용되지만 모바일 악성코드 유포에는 사회공학적 방법이 더욱 많이 사용된다는 것이다. 사회공학 공격은 신뢰관계를 기반으로 하는 “사기”이기 때문에 기술적으로 차단하는데 한계가 존재하고, SMS, 메신저 등과 같이 모바일 악성코드 유포에 주로 사용되는 애플리케이션은 대부분 개인정보를 다루고 있기 때문에 불특정 다수의 정보를 함부로 수집하거나 분석할 수 없는 한계점이 존재한다.

2. 모바일 악성코드 대응 방안

모바일 악성코드에 대해 보다 능동적으로 대응하기 위해서는 3가지의 요소가 결합된 적극적인 대응체계의 구축이 필요하다.

대응체계의 첫 번째는 업데이트 서비스의 신속화이다. 즉 단말기 제조사와 통신사에서 OS제조사에서 발표되는 보안패치를 가능한 빠르게 적용하기 위한 적극적인 노력과 체계가 필요하다. OS보안 패치의 경우 항상 최신 OS를 사용자에게 제공하는 방법을 사용할 수도 있고, 최신 OS가 아니더라도 배포된 OS에 해당하는 보안패치가 있다면 해당 패치를 적용하기 위한 개발, 시험이 적극적으로 실시되어 사용자에게 빠르게 최종 보안 업데이트가 제공되어야 한다.

두 번째는 사용자의 보안 인식 교육이다. 최근 PC악성코드의 위험이 높아지면서 많은 사용자들이 보안의 중요성을 인지하고 백신프로그램을 설치하고, 패스워드를 철저히 관리하며, 불분명한 웹사이트를 방문하지 않는 등 보안에 노력하고 있다. 이와 같이 모바일 단말에서 발생될 수 있는 위험의 중요성을 사용자에게 부각시키기 위해 지속적인 교육 프로그램을 개발하고 실시하여야 한다.

세 번째로 모바일 악성코드 대응을 위한 연구개발의 활성화이다. 유선 인터넷의 경우 Drive-by download 공격을 탐지하기 위한 다양한 기술이 개발되고 있으나, 현재 모바일 환경에서는 이에 대한 연구가 부족하며, 모바일 플랫폼의 취약점 및 모바일 악성코드 치료 백신의 보급 등 모바일 악성코드를 예방하기 위한 기술개발이 필요하다.

IV. 결론

최근 인터넷 사용 환경의 발전은 모바일 환경에서도 편리성을 가중시켰다. 하지만 살펴본 바와 같이 모바일 환경에서의 해킹의 위험 또한 증가하고 있으며, 특히 모바일 악성코드로 인한 피해는 사용자에게 금전적인 피해를 직접적으로 주는 만큼 더욱 빠르고 능동적인 대응이 필요하다.

하지만 기존의 대응방안은 지능적으로 발전하고 있는 모바일 악성코드에 능동적으로 대응하기에는 한계가 있다. 본 연구에서는 모바일 악성코드에 대응하기 위한 체계의 개선을 제안하였다.

모바일 악성코드에 대한 능동적인 대응을 위해서는 모바일 단말기 제조사와 통신사의 적극적인 보안 업데이트 서비스, 사용자에 대한 모바일 보안인식 프로그램 교육, 모바일 악성코드 예방, 탐지를 위한 연구개발 등이 체계적으로 개선되어야 하며, 이러한 체계 개선이 범국가적인 방향에서 추진될 필요가 있다.

참고문헌

[1] Blue Coat Systems, “Blue Coat Systems 2013 Mobile Malware report-How Users Drive the Mobile Threat Landscape”, 2014

[2] 2011~2014년 월별 스마트폰 악성코드 발견 건수, http://www.ahanlab.com

[3] The Tenth Anniversary of Mobile Malware, http://www.symantec.com

[4] 장상근, “모바일 악성코드의 전략과 사례 분석을 통한 모바일 악성코드 진단법,” 정보보호학회지, 제 23권, 제 2호, 14-20쪽, 2013년 4월.

[5] 김병익, “웹 페이지 취약점을 통한 모바일 악성코드 유포 방식 분석,” Internet & security focus, 통권, 제 1호, 63-85쪽, 2013년 1월.

[6] Arxan, “State of Security in the App Economy: Mobile Apps Under Attack” pp.5, 2012.

[7] KAIST 주간보안동향 보고서, http://csrc.kaist.ac.kr

[8] ZHOU, Wu, et al. “Detecting repackaged smartphone applications in third-party android marketplaces” the second ACM conference on Data and Application Security and Privacy, pp.317-326, 2012

[9] CIOCISO Articles, “앱 위변조 방지 솔루션,” 2012년 7월

[10] G. Portokalidis et al., “Paranoid Android: Versatile Protection for Smartphones,” Proc. 26th Annual Comput. Security Appl. Conf. (ACSAC), pp.347-356, 2010.

저자소개

최 상 용

2000: 한남대학교 수학과 이학사.
2003: 한남대학교 컴퓨터공학과 공학석사.
2014: 전남대학교 정보보안협동과정 이학박사
현 재: 한국과학기술원 사이버보안연구센터 차세대보안연구실장
관심분야: 네트워크보안, 웹보안