스마트폰 상에서의 개인정보 유출 탐지 모니터링 연구

김웅준 · 박상휘 · 박상노 · 김창수 · 정회경

배재대학교 컴퓨터공학과

A study to detect and leaked personal information on the smartphone.

Wung-Jun Kim · Sang-Hwi Park · Sang-No Park · Chang-Su Kim · Hoe-Kyung Jung

Department of Computer Engineering, PaiChai University

E-mail : y199073@naver.com, shpark0618@hanmail.net, psn@hankisul.com, MIE-ddoja@pcu.ac.kr, hkjung@pcu.ac.kr

요 약

최근 스마트폰의 사용자가 지속적으로 증가함에 따라 스마트폰의 악성 어플리케이션들이 증가하고 무분별한 배포를 통해 단말 내에 존재하는 개인정보 유출, 스미싱 등의 피해 또한 증가하고 있다. 대표적인 개인정보 유출방법은 정상적인 어플리케이션으로 가장한 악성코드를 단말 내에 설치하여 문자메시지나 개인적인 메모, 전화번호부, 공인인증서 등의 개인정보를 유출시키는 방식이다. 따라서 단말의 루트권한을 획득하려는 공격 이벤트를 수집하여 악성코드 감염여부를 판별하고 대응하기 위한 기법이 필요하다.

본 논문에서는 실시간으로 스마트폰 시스템의 점검 기능을 수행하는 어플리케이션에 관한 연구를 통하여 단말 내 공격 이벤트를 분석, 수집하여 악성코드 감염여부를 판별할 수 있는 모바일 보안 모니터링 시스템을 제안한다. 이는 사용자의 개인정보 유출탐지 및 방지 분야에 활용될 것으로 예상된다.

ABSTRACT

Recent smartphone users constantly increases, an increase in malicious applications smartphones indiscretions exists within the Terminal, through the deployment of privacy disclosure, Singh and other victims also are on the rise. A typical personal way to malicious code masquerading as a normal application and install it on the handset of my text message or a personal note, such as personal information, the certificate directory, is the way that leaked. Therefore, to obtain permission to attack the root Terminal event by collecting malware infections and respond to determine whether it is necessary for the technique.

In this paper, check the features of a Smartphone in real time systems, to carry out a study on the application throughout the Terminal to collect my attack event analysis, malware infection can determine whether or not the mobile security monitoring system. This prevents a user's personal information and take advantage of the top and spill are expected to be on the field.

키워드

악성코드, 모바일, 이벤트, 개인정보

Ⅰ. 서 론

최근 스마트폰 사용자의 증가로 스마트폰의 악성 어플리케이션들의 무분별한 배포를 통해 단말 내에 존재하는 개인정보 유출, 스미싱 등의 피해 또한 증가하고 있다. 폐쇄적인 정책을 사용하는 애플의 앱스토어 보다 개방적인 정책을 사용하는 안드로이드 계열의 마켓에서는 상대적으로 악성코드 감염률이 높다. 악성코드에 감염된 스마트폰은 개인 정보 유출, 스마트폰 위치 추적, 과금을 유발하는 SMS 발송 등이 있다. 특히 공격자가 악성 어플리케이션에 악성코드를 삽입하여 루팅(Ro

oting) 공격을 수행한 후 단말에 저장된 사용자의 공인인증서, SMS, 전화번호부 등과 같은 개인 정보나 금융 정보를 외부 서버로 유출시키는 공격이 있다. 이러한 악성코드들은 어플리케이션 다운로드뿐만 아니라 웹브라우저를 통해서도 설치할 수 있어 악성코드 차단이 어렵다. 이런 악성코드 중 대표적으로 PUP(Potentially Unwanted Program)와 트로이목마 악성코드가 있으며, 이 두 가지 악성코드는 악성코드 전체의 약 93%를 차지한다. 이에, 일반 스마트폰 사용자들이 손쉽게 사용할 수 있는 악성코드에 대한 대응 방안이 필요하다.

본 논문에서는 스마트폰의 악성코드로 인한 피해를 줄이고 확산을 방지하기 위해 모바일 단말 루팅 과정을 분석하고, 대표적인 악성코드들의 기능과 특징을 분석하여 공격이 수행되는 과정에서 발생하는 이벤트를 수집하고 감염여부를 판별할 수 있는 모바일 보안 모니터링 시스템을 제안한다.

Ⅱ. 악성코드 현황

본 절에서는 모바일 악성코드의 유형에 대해 살펴본다.

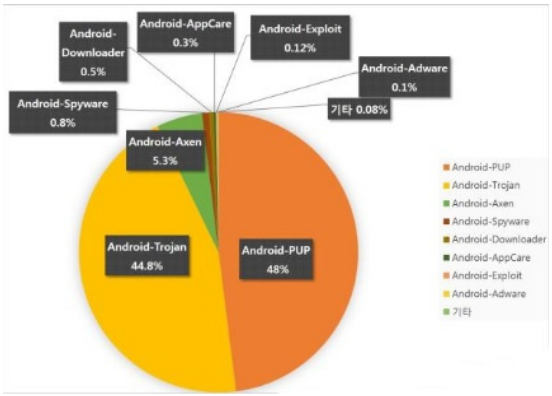

그림 1. 모바일 악성코드 진단 건수 기준 분류

악성코드 유형에는 여러 종류가 있다. 그림 1은 국내 보안 연구소인 AhnLab에서 2014년 1분기 안드로이드 기반 모바일 악성코드 진단 건수를 표로 나타낸 것이다. 통계 결과에 따르면 PUP가 48%로 가장 많았고, 그다음으로 Trojan이 44.8%를 차지했다.

PUP는 형식적으로 사용자의 동의를 받고 설치되지만 사용자가 인지한 프로그램들과는 관계가 없거나 필요하지 않은 프로그램을 설치하여 시스템에 문제를 일으키거나 사용자의 불편을 초래하는 프로그램이다.

트로이목마 유형은 사용자의 스마트폰에 은닉하여 정보유출, 과금 등의 악성 행위를 하는 악성코드이다. 이외에 사용자 몰래 정보를 수집하는 스파이웨어, 다른 악성코드를 추가로 설치하는 다운로더, 향후 악의적인 목적으로 활용 될 수 있는 앱케어 등이 있다.

Ⅲ. 시스템 제안

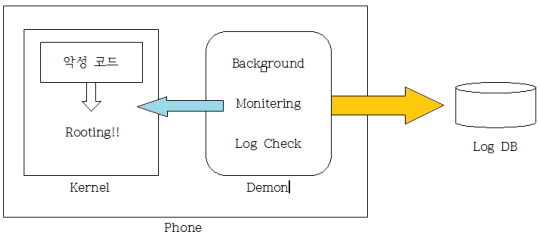

그림 2. 제안 기법 구조도

그림 2는 제안하는 기법의 구조도로 악성코드가 단말을 루팅하면 단말 내 중요 개인정보 등을 외부로 유출하는 과정에 악용될 수 있다. 플랫폼 내에 탑재되어있는 데몬은 이 이벤트들을 모니터링하고, 공격 이벤트들을 탐지하는 기능을 제공할 수 있다. 기록 된 로그(log)들은 외부 DB서버에 전송하고 기록하여 특정 악성코드의 공격방법에 대한 정보를 얻을 수 있다.

기존의 탐지 방법은 프로그램을 실행시켜 기록된 로그를 분석하고 악성코드를 탐지한다. 이러한 탐지 방법은 유출행위가 발생한 후에 탐지가 가능한 단점이 존재한다. 단점을 보완하기 위해서는 모바일 단말에 대한 효율적인 공격탐지 및 대응 기법이 개발되어야 한다. 이를 위해서는 단말 내의 프로세스, 메모리, 스토리지 등에 대한 변화를 실시간으로 모니터링 하여 악성코드에 대한 변화를 알 수 있어야 한다. 그림 3은 본 논문에서 제시하는 방법을 나타낸 절차이다.

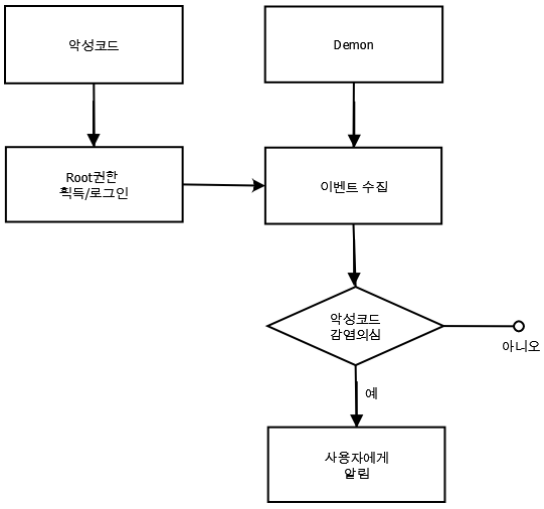

그림 3. 악성코드 감지 절차

사용자가 데몬을 설치하면 안드로이드 리눅스 커널 내 데몬이 실행이 되어 주요 프로세스의 이

벤트를 확인할 수 있다. 악성코드가 단말 내 루트 권한을 획득하기 위해 루팅 과정을 수행하면 이 벤트가 발생한다. 안드로이드 운영체제의 기반이 된 리눅스 환경에서는 모든 파일과 프로그램에 접근할 수 있는 권한을 가진 계정을 루트(root)라 하고, 이 루트 계정을 획득하는 것이 루팅이다. 루팅 방식은 사용자가 단말기를 직접 루팅하는 방식과 공격자가 악성코드를 심어 루팅하는 방식이 있다.

IV. 결 론

본 논문에서는 최근 부각되고 있는 안드로이드 악성 어플리케이션들의 현황에 대해 분석하고, 악성코드의 공격 방법 중 하나인 루팅 공격을 분석하고 탐지하여 차단할 수 있는 방법에 대해 연구하였다.

먼저, 알려진 악성 어플리케이션과 불법적으로 단말에 대한 루트 권한을 획득하기 위한 루팅 공격에 대해 살펴보았다. 악성코드가 루팅 공격 시 안드로이드 커널 상에 이벤트들이 기록되고, 이벤트들을 데몬이 모니터링 하여 전송하는 방식이다. 커널에서 탐지를 하기 때문에 모든 파일의 접근과 이벤트를 모니터링 할 수 있으며, 기존의 탐지 방법에서 탐지가 어려웠던 유출행위를 실시간으로 탐지와 차단이 가능하다.

향후과제로는 이러한 로그들을 분석하여 기존의 악성코드에 대한 대응책을 만들고 오탐율을 최소화할 수 있는 연구가 진행 되어야 하며, 다른 방식에 대한 공격에 대해 능동적으로 대응할 수 있는 방법에 대한 연구가 필요하다.

참고문헌

[1] 이형우, “안드로이드 기반 모바일 단말 루팅 공격에 대한 이벤트 추출 기반 대응 기법”, 한국정보보호학회 제23권 제3호, pp.479-490, 2013.6

[2] 이형우, “안드로이드 기반 모바일 단말 루팅 공격 검출 및 악성 앱 이벤트 모니터링”, 한국정보보호학회 제13권 제1호, pp.30-38, 2012.3

[3] 최영석, 김성훈, 이동훈, “개인정보 유출 탐지 및 차단에 관한 연구”, 한국정보보호학회, 제23권 제4호, pp.757-766, 2013.8

[4] 천우봉, 이정희, 박원형, 정태명, “스마트폰 악성코드 대응을 위한 모바일 보안 진단 시스템”, 한국정보보호학회논문지 제22권 제3호, pp.537-544, 2012.5

[5] http://blog.ahnlab.com/ahnlab/1912, 2014.4