좀비 스마트폰 특징 추출에 관한 연구

이대성*

*부산가톨릭대학교

A Study on Feature Extraction of Zombie Smartphone

Daesung Lee*

*Catholic University of Pusan

E-mail : dslee@cup.ac.kr

요 약

DDoS와 같은 악성 네트워크 공격은 뚜렷한 대비책이 없으며, 그 피해 또한 막대하다. 특히, 스마트폰이 감염되어 좀비화 될 경우 통신요금 과금 및 개인정보 유출 등 네트워크 장애와 더불어 다양한 사용자 피해가 예상된다. 본 연구에서는 좀비 PC에서 나타나는 특징들을 바탕으로 스마트폰이 악성코드에 감염되어 좀비 서비스가 실행되는 동안 나타나는 현상 및 특징들을 추출한다.

ABSTRACT

Malicious network attacks such as DDoS is no clear preparedness, the damage is also a bar. In particular, when a smartphone is infected to the zombies, the damage such as communication fee billing and leakage of personal information with numerous network failures are expected. In this study, with reference of the features that appear in a zombie PC we extract the zombie smartphone's phenomena and features that appear while the zombie service is running

키워드

좀비 스마트폰, 좀비PC, 분산 서비스 거부 공격, 특징 추출

Ⅰ. 서 론

스마트폰은 지난 2004년 미국 내 사무직 종사자를 중심으로 열풍이 시작되어 미국 전역으로 확대 된 것에 이어 국내에도 2009년 4월부터 방송통신위원회의 WIFI 탑재 의무화 제도 폐지가 확정되면서 표준화된 개발 환경을 제공하는 범용 OS 기반의 스마트폰 시장이 확산되고 있다. PC수준의 기능을 제공하는 스마트폰의 경우 PC와 유사한 보안 취약점이 발생할 수 있다고 보안 전문가들은 우려하고 있는데, 이는 스마트폰이 단순한 휴대폰이 아닌 다양한 네트워크 인터페이스를 가진 컴퓨터로 현재 인터넷 환경에서 발생할 수 있는 모든 보안 위협이 스마트폰 환경에서 동일하게 적용되기 때문이다. 개인 중요 정보가 저장되고 오픈 개발 환경의 제공으로 자유로운 프로그램 개발 및 설치가 가능하다는 점에서 악성코드에 감염될 가능성이 크고, 이른바 좀비스마트폰이라 불리는 악성코드에 감염된 스마트폰은 해커에게 제어권이 넘어간 경우 디도스(DDoS) 공격, 악성 스팸 유포, 스파이웨어 설치, 개인정보 유출 등에 악용될 수 있다.

해커는 좀비스마트폰을 만들기 위해서 다양한 방법을 시도하고 있다. 육안으로 보이는 증상의 악성 어플리케이션을 활용한 방법, 루트(root)권한을 획득한 후 스마트폰 사용자의 개인정보 탈취 및 요금을 과금 시키는 현상 그리고 지능형 좀비 서비스를 사용하여 사용자의 스마트폰을 지배하는 등의 방법으로 좀비 서비스를 개발하고 유포시킨다[1,2,3,4,5]. 본 연구에서는 스마트폰의 영역별 위협과 스마트폰 DDoS 공격의 특징을 알아봄으로써 좀비스마트폰의 특징을 확인하고 안드로이드 APK구성 요소에 대한 분석과 주요 클래스 및 안드로이드 어플리케이션 프로그래밍 절차에 대한 취약점 조사를 통해 안드로이드 스마트폰의

좀비화가 어떻게 진행되는지 파악할 것이다.

본 연구에서는 실제 100여개의 샘플 악성 어플리케이션을 순정상태의 스마트폰과 루팅된 스마트폰에서의 직접 설치 및 실행을 통해서 어떤 증상이 나타나는지 대표적으로 증상을 분류해 보고, 나아가, 샘플 악성 어플리케이션을 설치 및 실행을 통해 겉으로 드러나는 것들만으로는 분석이 어렵다 판단될 경우, 디컴파일을 통해 악성 어플리케이션의 클래스파일 내부의 소스코드를 분석, 좀 더 깊이 있는 연구를 진행하였다.

II. 본 론

본 연구에서는 100개의 악성 어플리케이션 샘플을 실행하고 그 수행결과를 분석하였으며, 경우에 따라서는 소스코드 분석을 통해 분석에 대한 정확도를 높였다. 분석결과는 [그림 1]과 같이 동적 서비스 등록 61%, 정적 서비스 등록 39%로 나타났으며, 동적 서비스 등록과 정적 서비스 등록 방식을 사용한 어플리케이션들을 각각 분류하였을 때, 각 서비스 내에서는 비슷한 수치를 보이고 있었다.

어플리케이션을 실행 시켰을 경우 눈에 보이는 증상과 코드 상에서의 특이사항이 없는 경우가 동적 서비스 등록이 61%, 정적 서비스 등록이 72%로 소폭 차이를 보이고 있었다. 그 외에도 악성 광고를 실행시키는 어플리케이션은 비슷한 수치로 각각 12%, 11%를 나타내고 있다. 홈 화면 실행 어플리케이션 생성은 동적 서비스 등록이 20%, 정적 서비스 등록이 11%로 차이를 보이고 있었는데, 이 차이는 생성된 실행 어플리케이션이 불법 사이트나 공식적이지 않은 사이트가 링크되어 있어서 그에 해당하는 서비스, URL을 감추기 위해서 서비스를 동적으로 등록한 것이 많다고 볼 수 있다. 이어서 SMS Service에 해당하는 부분은 동적 서비스 등록과 정적 서비스 등록은 각각 5%, 3%, Alarm Service 등록은 동적 서비스 등록과 정적 서비스 등록이 각각 2%, 3%를 차지하고 있었다.

동적 서비스 등록과 정적 서비스 등록의 목적은 같지만 그 방법적인 면에서 큰 차이를 보여주고 있다. 은폐 엄폐시키기 좋은 동적 서비스 할당 방식이 악성코드 활용 면에서 빈도수가 높다고 판단할 수 있다. 그 이유는 동적 서비스 등록 방식은 Manifest.xml 이외에도 기타 MainActivity, onReceiver, onCreate, onDestroy, onStart, onStop 등 다양한 함수에서 백그라운드 서비스 등록이 가능하며, 추가로 호출되는 다른 많은 함수들에서 좀비 프로세스가 실행되는 서비스를 호출해서 사용할 수 있기 때문인 것으로 분석되었다.

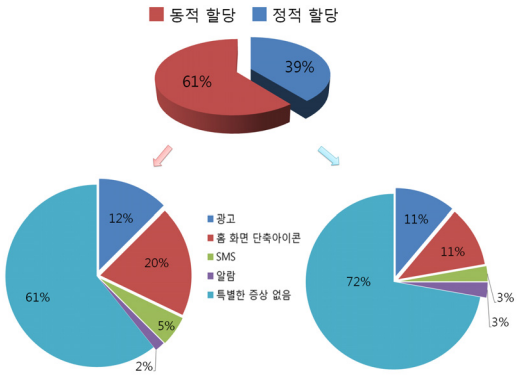

그림 1. 100개의 악성 앱 분석 결과

III. 결 론

PC의 DDoS 공격으로부터 시작되어 좀비PC가 생긴 이후로 DDoS 공격은 금융, 방송국, 공공기관 사이트 등을 공격하여 대규모 피해를 일으키고 있다. PC 사용자보다 스마트폰 사용자가 점차 늘어나고 있는 이 시점에서 스마트폰의 보안대책은 아직까지 미비한 상태이다. 스마트폰 상에서도 DDoS 공격뿐만 아니라 악성 어플리케이션을 통해서 사용자에게 피해를 발생 시키는 사고사례가 계속 늘어나고 있다.

본 연구에서는 100개의 보고된 악성 어플리케이션 샘플을 가지고 스마트폰에 직접 설치해서 실행하고, 실행의 경과를 지켜보고, 디컴파일을 통해서 코드분석을 해본 결과, 소스코드의 다양한 함수에서 좀비 서비스가 백그라운드 서비스로 다시 재실행 되는 구조를 구성하고 있는 것으로 분석하였다.

참고문헌

[1] 장기헌, “Source-End 기반의 패킷 모니터링을 통한 스마트폰 DDoS 공격 탐지 및 대응 체계 연구”, 순천향대학교 석사학위논문, 2012

[2] 맹호규, 오태원, “스마트폰 동기화의 개인정보 유출방지 모델”, 한국컴퓨터종합학술대회 논문집, Vol38, No.1(D). pp 44~47, 2011

[3] 장기헌, 최상명, 염흥열, “스마트폰 DDoS 공격 동향”, 한국정보보호학회 논문지, 제21권 5호, pp 65~70, 2011

[4] 최상명, “좀비스마트폰과 DDoS 공격”, ㈜하우리 선행기술팀, 배포자료, 2012

[5] 한국정보화진흥원, “스마트폰과 모바일 오피스의 보안 이슈 및 대응 전략”, CIO Report, 2010