모바일 악성코드 감염과 보안취약성에 대한 학부생의 인식조사 연구

김명오*, 강경혁*, 김태양*, 박건우*, 김석민*, 장영수*
*한국폴리텍대학 안성캠퍼스 스마트소프트웨어과
email : auddh0601@hanmail.net, {bestkkha,rjsehflsha12}@gmail.com,
{5jeeeeek,tjrals0704,jyskkh}@naver.com

A Study on the Awareness of Mobile Manifesto Infestions and Security Vulnerabilities

MyeongOh Kim*, KyeongHyeok Kang*, TaeYang Kim*,
GunWoo Park*, SeokMin Kim*, YoungSu Jang*
*Dept. of Smart Software, Korea Polytechnic Ansung College

요 약

모바일 기기를 이용하는 인터넷 서비스가 증가하고 있다. 반면 응용소프트웨어의 보안 허점을 노린 바이러스, 웜, 악성코드는 나날이 증가하여 개인은 물론 기업, 국가차원의 대책이 요구되고 있다. 악성코드는 악의적인 목적을 위해 작성된 코드를 통칭하며 시스템 성능저하, 개인정보 유출, 파일 감염 및 손상을 입힌다. 본 논문에서는 모바일 기기의 악성코드 종류, 증상, 감염경로를 알아보고, 보안 취약성에 대한 학부생의 인식도를 조사하여 예방하는데 그 목적을 둔다. 이러한 인식도 조사를 통해 모바일 악성코드에 대한 학부생의 인식을 향상시키고, 기초 예방만으로도 쉽게 감염률을 낮출 수 있도록 백신을 설치하고 수시로 업데이트하여 이용자들에게 악성코드 감염 증상과 사례의 심각함을 알려줌으로써 예방 인식도를 함양 시킬 수 있다.

1. 서론

인터넷의 보급과 모바일 기기를 활용하여 금융, 업무정보 등 개인정보나 가치 높은 자료를 다루면서 개인정보 유출, 프로그램 손상을 초례하는 악성코드가 증가하고 있다. 또한 모바일 응용프로그램의 보급이 활성화 되면서 이러한 악성코드의 악용 사례는 증가 추세이다. 본 논문에서는 이러한 악성코드의 종류, 증상, 경로, 인식을 살펴보고 이에 대한 학부생들의 인식도를 연구 하였다.

2. 모바일 악성코드의 종류

악성코드의 대표적인 종류로는 바이러스, 웜, 트로이목마가 있다. 바이러스는 스스로를 복제해서 악의적인 목적을 수행하는 악성 소프트웨어이며 운영체제의 부트(Boot) 영역을 감염시켜 숙주 프로그램에 감염된다. 바이러스는 만들어진 목적과 의도에 따라 그 종류가 크게 세분화 되지만 대표적으로 감염된 후 바로 기능을 수행하는 바이러스, 일정 기간의 잠복기를 거쳐 수행되는 바이러스, 공격자가 프로그래밍 한 특정 일자에 실행되는 바이러스 등이 있다[1]. 웜은 스스로를 복제하는 시스템 프로그램으로 독자적으로 실행된다. 또한, 웜은 어떠한 중재 작업 없이도 네트워크를 통해 자신의 복사본을 전송할 수 있으며 네트워크를 손상시키고 대역폭을 잠식한다[2,3]. 트로이 목마는 시작부터 끝까지 메모리에 상주하며 시스템의 내부 정보를 공격자에게 빼돌린다. 이러한 트로이 목마의 감염 비율은 전체 악성코드의 35%를 넘으며 바이러스나 웜과는 달리 스스로 전파되지 않고 다른 파일에 삽입되어 감염한다[4].

3. 대표적인 감염 증상과 사례

3-1. 바이러스 증상

바이러스 증상은 크게 네 가지 유형으로 나눌 수 있다.

- 시스템이 느려진다. 이유 없이 시스템의 속도가 느려진다는 것은 사용자가 지시하지 않은 다른 동작들이 시스템 내부에서 수행되고 있다는 것이다.
- 바이러스에 감염된 프로그램이라면 대부분 정상적으로 실행되지 않고 실행 오류가 발생한다.
- 메모리 용량이 이유 없이 줄어드는 현상이 발생한다. 바이러스에 감염된 코드의 수행으로 인해 임시 파일들의 용량이 커지는 현상이 발생한다.
- 시스템이 이유 없이 다운된다. 시스템 이상이나 운영체제의 이상인 경우도 있으나 대게는 바이러스의 감염으로 인한 증상이다[5].

사례) 2017년 모바일 기기로 문자메시지 전송 시 감염 파일을 최우선으로 읽어 자동 실행하는 기능을 중국에서

변조하여 바이러스를 확산시켰다. 이 결과 전 세계 스마트폰 141만 대가 감염됐고 공격자는 감염당한 스마트폰 사용자에게 텍스트 문서를 띄워 겁을 주며 협박하고 금품을 요구했다[6,7].

3-2. 웜 증상

웜 증상으로는 시스템 속도가 느려지고 자동으로 특정 프로그램이 열리며 웹 브라우저의 성능이 불규칙 해지고 시스템에 비정상적인 동작이 발생하며 운영 체제 오류가 발생한다.

사례) 2015년 STPAX 웜의 등장으로 모바일 기기 사용자의 시스템 속도를 저해시키고 시스템을 비정상적으로 동작시켜 안드로이드 운영체제의 오류를 발생시켰다[8].

3-3. 트로이 목마 증상

트로이 목마 증상으로는 시스템 내 임의의 파일을 수정하거나 데이터를 삭제시킨다. 이렇게 함으로써 모바일 시스템의 하드웨어를 작동하지 않도록 만든다.

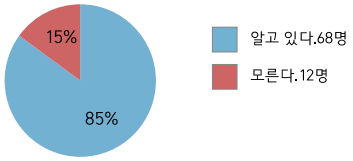
사례) 2010년 안드로이드 폰 사용자의 개인정보를 노리는 트로이목마가 발견되고, 2015년 메르스 정보로 위장한 트로이 목마 파일이 발견되었다[9].

4. 악성코드에 대한 이공계 학부생의 인식도 조사

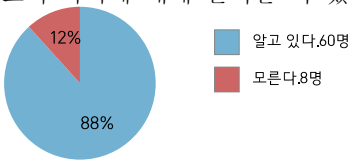
• 조사대상 : 한국 폴리텍대학 안성캠퍼스 학부생 80명

• 조사방법 : 설문지를 통한 문답형 조사

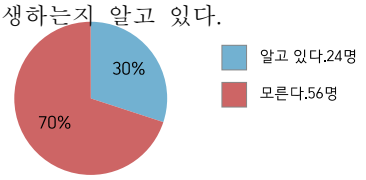
ⓐ. 악성코드가 무엇인지 알고 있다.



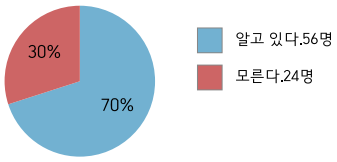
ⓑ. "ⓐ에 알고 있다"를 체크한 사람 중 바이러스, 웜, 트로이 목마에 대해 들어본 적 있다.



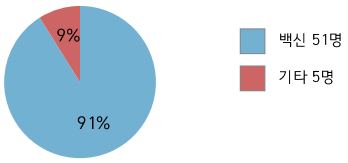
ⓒ. 바이러스, 웜, 트로이 목마 등의 악성코드가 왜 발생하는지 알고 있다.



ⓓ. 악성코드의 예방방법을 알고 있다.



ⓔ. "ⓓ에 알고 있다"를 체크한 사람 중 예방방법에는 어떤 것이 있는가?



• 조사결과: 설문에 참여한 학부생 대다수는 모바일 악성코드에 대해 알고는 있으나 감염 경로, 이유는 잘 모르는 학생들이 전체 조사대상의 70% 이었으며, 예방방법 으로는 전체 조사대상 학부생 80명 중 남학생 58명, 여학생 16명의 학생이 백신 이라고 대답하였다

5. 결론

본 논문에서는 모바일 악성코드의 종류와 증상 그리고 이에 대한 학부생의 인식도 조사를 수행 하였다. 현재 우리가 사용하는 V3 Mobile, 알약M 등 대부분의 바이러스 백신은 악성코드로부터 시스템을 지킬 수 있도록 잘 설계되어있다. 백신을 설치하고 수시로 업데이트하는 것은 물론, 이용자들에게 악성코드 감염 증상과 사례의 심각함을 알려줌으로써 예방 인식도를 함양 시키는 것이 중요하다.

참고문헌

[1] Namuwiki(https://namu.wiki/w) - Computer Virus
[2] Namuwiki(https://namu.wiki/w) - Worm
[3] Graynews(http://news.grayhash.com) - "최초의 웜, 모리스 웜" - 2016년
[4] Namuwiki(https://namu.wiki/w) - Malware
[5] WonKwang University Computer Center (https://cc.wku.ac.kr) - "보안100문100답" - 감염 증상과 사례 - 2014년
[6] Namuwiki(https://namu.wiki/w) - Autorun Virus
[7] Boannews(http://www.boannews.com) - "中 트로이 목마·웜 바이러스, 모바일 141만대 감염" - 2017년
[8] Veracode(http://www.hankookilbo.com) - Computer Wrom "What is a computer worm?"
[9] Korea Times(http://www.hankookilbo.com) - "메르스 사칭 악성코드, 알고 보니 '트로이 목마'" - 2015년