모바일 게임에서 악성 프로그램 탐지에 관한 연구

김효남[O]
[O]청강문화산업대학교 게임콘텐츠
e-mail: hnkim@ck.ac.kr[O]

A Study on Malware Program Detection in Mobile Game

Hyo-Nam Kim[O]
[O]Dept. of Game Contents, ChungKang College of Culture Industries

● 요 약 ●

전 세계 모바일 게임 소비 시장의 증가와 사용자들이 지속적으로 증가하는 반면 랜섬웨어와 같은 악성 프로그램들이 악의적인 목적을 위하여 모바일게임 시장에 피해를 주는 사례들도 지속적으로 증가하는 것도 사실이다. 본 논문에서는 모바일 게임을 이용한 악성코드 위협으로부터 보호하기 위하여 4차 산업의 가장 핵심 기술인 인공지능의 학습기술에 악성코드 분석기술을 연계시켜 새로운 모바일 악성코드 탐지와 속도를 향상시키는 기술의 필요성을 제시한다.

키워드: Mobile Game, Malware Program, AI

I. Introduction

올해 글로벌 게임 시장은 연평균 8% 성장이 지속되며, 모바일 게임 시장의 비중은 46%로 추정하고 있다. 어느 국가를 막론하고 최근 가장 뜨거운 게임 시장은 역시 모바일 게임이다. 시장조사업체인 newzoo는 2020년까지 모바일 게임이 약 40%의 시장 점유율을 차지하며 가정용 게임기 시장을 압도할 것이라 예상했다[1].

이처럼 모바일게임 시장 규모의 증가와 사용자들이 지속적으로 증가하는 반면 랜섬웨어와 같은 악성 프로그램들이 악의적인 목적을 위하여 모바일게임 시장에 피해를 주는 사례들도 지속적으로 증가하는 것도 사실이다[2]. 최근 통계로 1년 사이 300배나 증가할 정도로 수없는 종류의 악성 응용프로그램과 방법들이 흘러넘치고 있다고 한다[3].

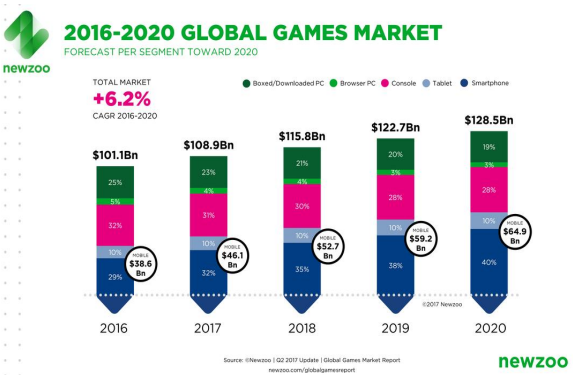

Fig. 1. Global Games Market
(출처 : www.newzoo.com)

본 논문에서는 모바일게임 시장 규모가 지속적으로 증가하는 반면에 비례해서 악의적인 목적으로 인한 피해사례도 증가하는 부분에 대해서 보안적인 측면에서 랜섬웨어와 같은 악성 프로그램들을 차단할 수 있는 모바일 플랫폼 기반의 AI와 연계한 모바일 게임 보안 대안을 제시하고자한다.

II. The Main Subject

최근에 중국의 바이두에서 만든 프로그램 안에 사용자의 스마트폰을 장악할 수 있는 백도어 등의 취약점이 발견되어 한때 세계적으로 문제가 되기도 하였다. 이처럼 안드로이드 랜섬웨어가 내년에도 모바일 플랫폼에서 선도적인 유형의 악성코드로 계속 증가하고 지배할 것으로 전망했다. 그리고 가장 문제가 되는 랜섬웨어만을 대상으로 탐지율을 테스트했을 때는 미탐지율이 17.0% 수준의 결과 자료를 제시한 것도 있다[4].

이와 관련하여 최근 4차 산업혁명이 ICT 분야에서 최고의 화두로 떠오르고 있고, 특히, 인공지능에 대한 기대감이 매우 커지고 있다. 전 세계적으로 앞으로 다가올 인공지능 시대에 대한 논의가 활발하게 이루어지고 있으며, 과학자들과 많은 업계에서 인공지능을 기반으로 다양한 분야에서 연계한 기술들이 개발되고 연구되어지고 있다. 현재 사이버공격 대부분은 악성코드에 의해 발생하고 있으며, 매달 1,000만개의 새로운 악성코드들이 나타나고 있다. 이처럼 수많은 악성코드들에 대한 분석을 인공지능 기반의 기술을 적용하며 악성코드의 변종형태의 공격이 발생하더라도 완벽할 순 없지만 기존 보안솔루

션의 약점을 보완할 수 있을 것으로 예상한다.

Table 1. Vaccine Detection Rate Testing
(출처 : 삼성 SDS)

파일종류	시그니처 백신	머신러닝 백신	시그니처와 머신러닝 결합
실행파일 미탐지율	10.1%	1.1%	0.5%
문서전체 미탐지율	14.4%	10.7%	2.7%
랜섬웨어 미탐지율	17.0%	0%	0%
변종악성코드 미탐지율	93.8%	0%	0%

표 1.의 삼성SDS가 제시한 자료에 의하면 머신러닝 기반 백신 프로그램으로 동일 테스트를 한 결과 변종 악성코드의 미탐지율은 93.8%에서 0%로 하락했다. 기존에 수집된 악성코드의 특성을 바탕으로 새로운 형태의 악성코드를 판별하기 때문에 변종 코드도 모두 찾아낼 수 있다는 설명이다. 파일 대상 악성코드 미탐지율도 9.9~24.6%에서 1.1~13.3% 수준까지 떨어졌다. 시그니처 백신과 머신러닝을 연동하면 0.5~2.7%로 더 낮아졌다[4].

이처럼 보안 업계에서는 인공지능을 이용해서 이전에 찾아볼 수 없었던 위협을 찾아내는데 많은 도움을 기대하고 있다. 최근에는 클라우드 자원을 활용하여 보안에 특화된 알고리즘 연구 개발이 진행되고 있어 각종 공격이 어떤 방식으로 들어오는지 학습하고, 이를 통해 적절한 방어를 하기 위한 툴이 개발되고 있다. 현재까지의 연구로 본다면 악성코드 분석, 소스코드 보안 분석, 인증, 사용자 행위 분석을 통한 이상 행위 탐지, 보안 관제 등의 분야에 적용할 수 있을 것이다[5]. 특히 대표적으로 인공지능을 적용할 수 있는 부분이 악성코드 분석에 있다. 현재 악성코드 분석에 대표적인 기술이 시그니처 기반의 진단 기술을 사용하고 있는데, 이때 인공지능의 학습기술에 모바일 앱에서 나타나는 보다 단순한 악성코드의 이상 행위와 활동들에 대한 분석과 위협 정보들을 데이터베이스에 연계하여 빅데이터 기반의 분석을 통해 자동으로 변종 혹은 알려지지 않은 악성코드 패턴들을 식별해내는데 보다 효과적으로 응용할 수 있을 것이다. 그리고 제로데이 공격에 대한 탐지와 방어 속도 역시 향상될 수 있으며, 특히 인공지능에 의해 분석된 새로운 모바일 악성코드 패턴들에 대한 정보를 공유함으로써 사전에 모바일 보안위협으로 벗어날 수 있을 것이다.

III. Conclusions

전 세계 모바일 게임 소비 시장의 규모는 5조 원에 육박하였고, 2021년에는 7조 원까지 성장할 것이라 많은 이들이 예측하고 있다. 어느 국가를 막론하고 최근 가장 뜨거운 게임 시장은 역시 모바일 게임이다. 모바일 게임 분야에서 중요한 것은 지속적인 성장과 발전에 가로막는 요인 중에 하나인 악의적인 목적의 랜섬웨어와 같은 악성코드를 유포하여 사용자들의 소중한 정보들을 탈취하고 손실을 가하는 행위를 차단하는 것이다.

본 논문에서는 모바일 게임을 이용한 악성코드 위협으로부터 보호하기 위하여 4차 산업의 가장 핵심 기술인 인공지능의 학습기술에 악성코드 분석기술을 연계시켜 새로운 모바일 악성코드 탐지와 속도를 향상시키는 기술의 필요성을 제시한다.

REFERENCES

[1] http://m.post.naver.com/viewer
[2] Hyo-Nam Kim, ”A Study on Obfuscation of the InGame Data for the Mobile Game Security“ Winter Conference of the Korea Society of Computer and Information. Vol. 25, No. 1, Jan 2017.
[3] https://byline.network/2017/11/1-921/
[4] http://news.hankyung.com/article/
[5] https://blog.naver.com/ibm_korea/