한국컴퓨터정보학회 하계학술대회 논문집 제26권 제2호 (2018. 7)

모바일 게임에서 지능형 공격 차단에 관한 연구

김효남O
O청강문화산업대학교 게임콘텐츠
e-mail: hnkim@ck.ac.krO

A Study on Intelligence Threat Firewall in Mobile Games

Hyo-Nam Kim*
*Dept. of Game Contents, ChungKang College of Culture Industries

● 요 약 ●

모바일 게임 시장의 성장과 함께 보안 위협도 함께 증가하고 있는 것이 현재 상황이다. 게임 앱을 해킹하여 결제를 우회한 뒤 금전적 이익을 가로채거나, 원작 게임의 복제 앱을 만들어 부당이득을 취하는 일이 빈번하게 발생하고 있다. 본 논문에서는 모바일 게임 보안을 위하여 위협 인텔리전스와 같은 기술을 기반으로 모바일 게임에서 악용되고 있는 단순한 공격 유형들을 대상으로 사전에 수집 분석하여 지능형 공격을 차단할 수 있는 방안을 제시한다.

키워드: Mobile Game, Threat Intelligence, Mobile Security

I. Introduction

4차 산업혁명 시대에 접어들면서 모바일 기기의 수가 컴퓨터를 넘어섰고 개인 스마트폰을 이용하여 회사 및 개인 업무를 보는 것이 일반화되면서 그 어떤 분야보다 보안이 중요해졌다. 모바일 보안과 관련해서 가장 중요한 문제는 해킹으로 인한 피해 사례가 증가하고 있다는 것이다. 그리고 해킹 침해 사례 중에서도 모바일 게임 해킹이 대표적이며, 모바일 게임을 향한 해킹 공격은 지금 이 순간에도 지능화되고 횟수 역시 기하급수적으로 늘어가고 있다.

본 논문에서는 모바일 게임을 대상으로 공격자가 내부 침투 후, 악성코드를 심고, 악성 행위를 실행하는 전 과정을 재구성할 수 있는 능력을 갖추는 것이 지능형 공격을 막을 수 있는 유일한 방법인데 이것을 가능토록 해주는 것이 바로 위협 인텔리전스 개념이며, 모바일 게임 보안을 위하여 위협 인텔리전스와 같은 기술을 접목하여 지능형 공격을 차단할 수 있는 방안을 제시해 본다.

II. The Main Subject

현재 스마트 폰을 사용하는 것이 일상생활화 되면서 이면에 가장 큰 문제가 되고 있는 것이 해킹으로 인한 개인정보 누출과 금전적 피해이다. 모바일 보안 위협으로 인한 대표적인 피해 사례는 악성 앱 또는 SMS를 이용한 모바일 스미싱 등을 들 수 있으며, 이외에도 악성코드를 심은 가짜 앱 등을 통해 해커의 공격을 받을 수도 있다. 이런 모바일 보안 위협에서 가장 대표적으로 악용되고 있고 해커들이 가장 많이 사용되고 있는 앱이 모바일 게임이다. 라임라이트 네트웍스의 '2018 전세계 온라인 게임 현황(State of Online Gaming)' 보고서에 따르면 게임 사용자의 절반 이상 57%가 이전에 보안 침해 사고를 당한 게임 사이트에서 온라인 게임이나 구매를 하지 않겠다고 답변하여, 보안은 중요한 고려 사항으로 지목하고 있다. 특히, 한국에서 보안에 대한 우려를 가장 많이 나타냈는데, 보안 문제가 발생한 게임 사이트를 방문하지 않겠다고 응답한 비율은 71.2%로 가장 높은 결과를 보였다[1].

모바일 게임을 향한 해킹 공격은 지금 이 순간에도 지능화되고 횟수 역시 기하급수적으로 늘어가고 있다. 이처럼 다양한 방법들을 사용하면서 모바일 게임을 해킹하려는 이유는 게임 앱 해킹이 쉽고 개발 시간을 많이 투자하는 것에 비해 앱을 보호하기 위한 보안기술 개발에는 소홀히 할 수밖에 없는 상황이 있기 때문이다. 그리고 게임 특성상 게임 플레이어들은 강한 캐릭터를 성장 시키고 더욱 빠르고 쉽게 게임을 즐기려는 욕구들을 충족시켜줄 수 있는 행위들이 해킹하는 목적으로 연관지울 수 있다고 본다.

게임 플레이어들이 즐기는 모바일 게임을 위협하는 대표적인 해킹의 첫 번째 유형은 스마트 폰에서 게임 앱을 추출하고 APK 파일을 다시 제작 작업을 거쳐 코드를 변조하고 다시 패킹해 배포하는 방법으로 사용자들은 어떠한 지불 없이 해킹된 상태로 서비스를 이용할 수 있음으로 서비스에 가장 파급력이 강력한 종류라 할 수 있다. 두 번째 유형은 인앱 결재를 우회하여 해커들이 부당한 이익을 챙기는 공격 방법으로 해킹 툴을 이용하거나 결제 과정을 변경 혹은 인증을 우회하여 공격하는 방법이다. 세 번째 유형으로는 게임 내 아이템이나 점수 등 주요 데이터를 찾아 위 변조하는 방법으로 해커들이 게임의

메모리를 해킹하여 인 게임의 점수나 혹은 아이템의 능력치 등을 수정하는 유형이다. 이처럼 다양한 방법들을 이용하여 모바일 게임 사용자들에게 극심한 피해를 가하고 있으며 해커들의 욕구를 충족시키기 위한 행위들을 진행하고 있다. 그래서 정보보호 분야에서도 모바일 보안에 대한 새로운 방어 기술들을 제시하고 있으며 4차 산업과 연계한 새로운 보안기술들도 연구되고 있다.

최근에 많은 연구에서 모바일 보안과 관련하여 모바일 게임을 이용하여 진행되고 있는 해킹과 악성코드 유포와 같은 악의적인 공격을 방어하기 위한 방안으로 4차 산업의 핵심 기술인 AI 기술과 연계하여 보안과 불법 유저 관리에 AI를 도입하여 기존 시스템보다 빠른 대응과 업무 처리가 이뤄지게 하는 보안기술을 제시하고 있다[2]. 그러나 인공지능, 클라우드, 사물인터넷 등이 보안 기술에 접목되면서 자동화된 대응이 새로운 기술인데 반해, 역이용에 대한 우려의 목소리 또한 끊이지 않는 것도 사실이다. 공격자의 다양한 행동에 따른 대응을 자동화시키다 보면 공격에 대한 사후적 조치로서의 방어밖에 할 수 없기 때문이다.

최근에 보안 업계에서는 새로운 기술의 하나인 위협 인텔리전스(Threat Intelligence) 개념에 대해서 중요성을 강조하고 적용하려는 시도가 여러 기업이나 연구소에서 연구되고 있다. 시장조사업체 가트너는 위협 인텔리전스를 기존에 있었거나 새롭게 부상하는 위협에 대해 알려주는 증거 기반의 지식으로서, 해당 위협에 대해 반응하는 의사결정에 활용되는 요소라 정의하고 있다. 가트너 정의를 세밀하게 살펴보면, 첫째 '현재 또는 임박한 위협'은 알려진 위협과 알려지지 않은 위협을 탐지하는 것으로 분류해 살펴볼 수 있다. 알려진 위협은 방화벽, IPS , 안티바이러스 등 기존 보안장비도 탐지, 차단, 치료가 가능하다. 알려지지 않은 신종 위협정보를 탐지하는 것이 더 중요하며 이를 수집, 분석하는 것이 위협 인텔리전스의 핵심이라고 할 수 있다[3].

모바일 게임을 이용한 해커들의 공격이 상존하고 지속 진화되고 있는 시점에 게임 서비스 기업들은 어느 곳에 위협이 도사리고 있는지 반드시 알고 있어야 한다. 잠복해 있는 적을 파악해야 그들이 어디서 어떻게 공격할지 예상할 수 있고, 해킹 당할 가능성이 있는지 확인할 수 있기 때문이다. 이뿐만 아니라 공격 대상이 됐을 때 대응 방안도 준비할 수 있다. 간단히 말하면 진화하는 위협을 주의 깊게 살펴보고 대응하기 위해서는 모바일 게임 보안 측면에서도 '위협 인텔리전스'가 필요하다. 본 논문에서는 모바일 게임 보안을 위하여 최근에 제시되고 있는 위협 인텔리전스와 같은 기술을 기반으로 모바일 게임에서 악용되고 있는 단순한 공격 유형들을 대상으로 사전에 수집 분석하여 지능형 공격을 차단할 수 있는 방안을 제시해 본다.

III. Conclusions

2021년에 모바일 게임 소비 시장의 규모가 7조원까지 성장할 것이라고 예측하고 있다. 성장과 함께 모바일 게임 해킹으로 모바일 게임을 향한 해킹 공격은 지금 이 순간에도 지능화되고 횟수 역시 기하급수적으로 늘어가고 있는 것이 현실이다.

본 논문에서는 모바일 게임 보안을 위하여 위협 인텔리전스와 같은 기술을 기반으로 모바일 게임에서 악용되고 있는 단순한 공격 유형들을 대상으로 사전에 수집 분석하여 지능형 공격을 차단할 수 있는 기술의 필요성을 제시한다.

REFERENCES

[1] https://kr.limelight.com/gaming

[2] Hyo-Nam Kim, "A Study on Malware Program Detection in Mobile Game" Winter Conference of the Korea Society of Computer and Information. Vol. 26, No. 1, Jan 2018.

[3] https://www.secui.com/information/press?id=269