게임 사이트 보안을 위한 사이버 보안 테스트에 관한 연구

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

A Study on Cyber Security Test for The Game Site Security

Hyo-Nam KimO
ODept. of Game Contents, ChungKang College of Culture Industries

● 요 약 ●

글로벌 게임 시장 규모가 전년 대비 13.3% 늘어나고 국내 게임 시장 규모도 전년 대비 6.2%로 증가되고 있는 것이 현재 게임 산업의 현황이다. 그러나 이에 반해 게임을 향한 해킹 공격도 지금 이 순간에도 지능화되고 횟수 역시 기하급수적으로 늘어가는 것도 현 게임 산업의 실태이다. 본 논문에서는 게임을 기반으로 게임 사용자들의 중요한 데이터를 탈취하고 피해를 막기 위해서 좀 더 다른 시각에서 게임 해킹을 방어할 수 있는 방법으로 사이버 보안 테스트를 이용하여 현재 게임 사이트의 보안상태를 점검하고 개선할 수 있는 방법을 제시한다.

키워드: Game Security, Cyber Security Test, Hacking

I. Introduction

올해 글로벌 게임 시장 규모가 전년 대비 13.3% 늘어난 1,379억 달러를 기록할 것으로 내다봤다. 한국콘텐츠진흥원에 따르면 2018년 국내 게임 시장 규모는 전년 대비 6.2% 늘어난 11조5703억원이다[1]. 이처럼 게임시장의 규모가 지속적으로 증가하고 있는 추세에 반해 게임 시장에서는 여러 가지 문제점들을 가지고 있다. 특히 보안과 관련해서 가장 중요한 문제는 해킹으로 인한 피해 사례가 증가하고 있다는 것이다. (그림 1)은 라임라이트 네트워스, '2018 전세계 온라인 게임 현황' 보고서에서 게임 사용자의 절반 이상(57 %)이 이전에 보안 침해 사고를 당한 게임 사이트에서 온라인 게임이나 구매를 하지 않겠다고 답변한 만큼, 보안은 중요한 고려 사항으로 생각하고 있다. 그리고 한국과 프랑스에서 보안에 대한 우려를 가장 많이 나타냈는데, 보안 문제가 발생한 게임 사이트를 방문하지 않겠다고 응답한 비율은 한국이 71.2%로 가장 높았고, 프랑스가 68%로 그 뒤를 보여주고 있다[2].

Country	Never	Less than 1 hour each week	1-3 hours each week	3-7 hours each week	7-15 hours each week	More than 15 hours each week
France	64.8%	13.2%	10.8%	5.8%	2.4%	3.0%
Germany	55.0%	21.8%	10.8%	7.0%	4.2%	1.2%
Japan	44.6%	22.8%	17.4%	7.2%	4.6%	3.4%
South Korea	21.4%	30.8%	24.2%	14.4%	6.2%	3.0%
U.K.	52.0%	18.8%	14.2%	7.4%	5.6%	2.0%
U.S.	52.0%	21.0%	13.4%	8.2%	3.4%	2.0%
Global	**48.3%**	**21.4%**	**15.1%**	**8.3%**	**4.4%**	**2.4%**

Fig 1. Will you continue to play online games that has previously experienced a security breach or been hacked?[2]

본 논문에서는 게임을 기반으로 게임 사용자들의 중요한 데이터를 탈취하고 피해를 막기 위해서 좀 더 다른 시각에서 게임 해킹을 방어할 수 있는 방법으로 사이버 보안 테스트를 이용하여 현재 게임 사이트 기반에서 조직의 인식, 취약성 평가, 빌드 평가, 침투 테스트 등 4가지 항목의 보안상태를 점검하고 보안 정책 개선에 참고할 수 있는 방법을 소개하고자 한다.

II. The Main Subject

게임시장의 규모가 지속적으로 증가하고 있는 추세에 반해 게임을 향한 해킹 공격은 지금 이 순간에도 지능화되고 횟수 역시 기하급수적으로 늘어가고 있다. 지난해 국내의 가장 대표적인 게임으로 떠올랐던 '배틀그라운드'는 중국발 핵 프로그램이 기승을 부려 골머리를 앓고 있으며, 기존의 대작 MMORPG였던 '아이온'이나 '블레이드&소울'도 비슷한 공격을 받은 바 있다.

배틀그라운드 게임 사례에서처럼 비인가 프로그램을 이용하여 해킹하는 과정이 다음과 같다. 첫 번째 단계로 비인가 프로그램(exe)과 게임(exe)이 구동되면 이와 동시에 관련 데이터가 메모리(RAM)에 로딩 된다. 두 번째 단계에서는 게임 프로세스 영역의 자체 구현된 보호 기술 혹은 제 3자 게임 안티 치트 솔루션의 보호 장치가 작동한다. 여기서 해당 프로세스 영역을 타 프로세스가 접근하지 못하도록 1차적으로 보호하는 단계이다. 세 번째 단계는 불법프로그램 프로세스

가 두 번째 단계에서의 보호기술을 무력화하고 게임 프로세스 메모리에 접근하는데 성공한다. 접근이 가능해졌다는 것은 게임과 관련된 정보를 임의로 바꿀 수 있다는 것을 의미한다. 네 번째 단계에서는 게임 프로세스 메모리에 접근권한을 획득한 비인가 프로그램은 게임 내 각종 정보들을 수집하여 변조 또는 복제 후 게임에서 제공하지 않는 불법적인 기능(DLL인젝션과 Code인젝션 기법 사용)을 제공하게 된다. 마지막으로 다섯 번째 단계에서는 획득한 메모리공간을 마음대로 읽어오거나, 위조/변조하여 게임에서 제공하지 않는 비정상적인 기능을 제공하는데 성공하게 된다[3].

이처럼 다양하고 신종 방법을 이용하여 지속적으로 게임을 기반으로 게임 사용자들의 중요한 데이터를 탈취하는 것을 막기 위해서 탐지와 방어기술들에 대한 연구가 활발하게 진행되고 있다. 본 논문에서는 좀 더 다른 시각에서 게임 해킹을 방어할 수 있는 방법으로 게임 사이트에서 사이버 보안 테스트를 이용하여 현재 게임 사이트의 보안상태를 점검하고 개선할 수 있는 방법을 제시한다. 사이트 문이 닫히면 해커는 열려있는 문을 찾는다. 해커들은 게임 사이트에 들어가는 큰 도전으로 생각하고 약점의 위치를 파악하기 위해 위협 관리 및 서비스 관리와 같은 서비스를 사용할 수 있다. 첫 번째 사이버 보안 테스트의 범위는 미리 동의하여 조직의 모든 부분 (내부 또는 외부)을 포함 할 수 있다. 특히 네트워크 및 응용 프로그램 계층뿐만 아니라 실제 계층에 대한 액세스도 살펴봐야 한다. 두 번째로 취약성 평가는 게임사의 디지털 인프라에서 시스템, 네트워크 및 응용 프로그램의 취약점을 확인하려고 시도한다. 이러한 사이버 보안 테스트는 심각도 및 위험도에 따라 각 문제를 설명하는 포괄적인 보고서와 이러한 문제를 해결할 수 있는 방법을 제공한다. 취약성 평가는 네트워크 인프라, 웹 응용 프로그램, 모바일 앱, 피싱 방어, 네트워크 장치, 시스템 빌드 등과 같은 자산을 평가하는데 사용할 수 있다. 다음은 세 번째는 빌드 검토에 대한 부분으로 디지털 환경의 약점을 식별하기 위해 수행되는 테스트이며, 지속적인 평가와 강화기술 사용을 통해 해커가 네트워크에서 성공할 수 있는 기회를 크게 줄일 수 있다. 빌드 평가는 디지털 및 물리적 사이버 보안 전략의 워크 스테이션(데스크톱, 랩톱 등), 활성 디렉토리, 데이터베이스 서버 요소를 다룬다. 마지막 네 번째는 침투 테스트로 평가하는 방법으로 가장 논란이 되고 있는 사이버 보안 테스트이다. 테스터들은 사이버 보안 조치가 어떻게 반응하는지 평가하기 위해 해커의 공격을 모방한다. 침투 테스트는 다른 테스트보다 시스템 및 네트워크 평가에 더 깊이 관여하며 발견 된 취약점을 회사의 유형 위험으로 변환하기위한 것이다. 예를 들어, 수백 개의 다른 서버 사이에 있는 서버상의 패치 되지 않은 응용 프로그램은 사소한 것처럼 보인다. 그러나 침투 테스트를 통해 이러한 취약성을 사용하여 장치에 대한 관리자 권한을 얻는 방법을 명확히 알 수 있고 이 액세스는 다른 시스템에 대한 추가 공격을 개발하여 전체 네트워크를 손상시키는 데 사용될 수 있다. 위에서 제시한 네 가지 요소들에 대해서 보안 테스트 결과를 통해 게임 사이트의 안정성을 검증하고 향후 보안 정책을 수립하는데 중요한 정보가 될 것이다.

III. Conclusions

국내 게임 시장 규모가 전년 대비 6.2% 늘어나고 있는데 비해 게임을 향한 해킹 공격은 지금 이 순간에도 자능화되고 횟수 역시 기하급수적으로 늘어가고 있다는 것이 가장 큰 문제이다.

본 논문에서는 게임을 기반으로 게임 사용자들의 중요한 데이터를 탈취하고 피해를 막기 위해서 좀 더 다른 시각에서 게임 해킹을 방어할 수 있는 방법으로 게임 사이트를 대상으로 사이버 보안 테스트를 진행하여 현재 게임 사이트의 보안상태를 점검하고 개선할 수 있는 방법을 제시한다.

REFERENCES

[1] http://www.upinews.kr/news
[2] https://kr.limelight.com
[3] https://cafe.naver.com/playbattlegrounds/