메모리 변조를 사용하는 AimBot의 분석과 탐지에 관한 연구

임지성[1], 홍영우[2], 유동영[3]
홍익대학교 소프트웨어융합학과 [1]학부생, [2]석사과정, [3]교수
jsleem0400@g.hongik.ac.kr, hyw1021@g.hongik.ac.kr, ydy@hongik.ac.kr

A Study on the Analysis and Detection of AimBot Using Memory Modulation

Ji-Sung Lim[1], Young-Woo Hong[2], Dong-Young Yoo[3]
Dept. of Software and Communications Engineering, Hongik University

요 약

글로벌 게임 시장 규모가 2023년까지 2,000억 달러를 넘게 성장할 것이라는 전망과 대중적인 온라인 FPS(First Person Shooter) 게임들이 출시되면서 게임 내 치팅(Cheating) 도구들을 배포, 판매하는 사례가 등장하고 있다. 이러한 사례들은 게임 이용에 불편을 초래하고 게임 매출액 감소로 이어질 수 있다. 따라서 본 논문에서는 과거 FPS 게임들에 사용되었던 AimBot들의 사례와 악성코드 탐지에 사용되었던 연구 사례들을 분석해 메모리 변조를 사용하는 AimBot의 탐지 방안을 연구하였다.

1. 서론

글로벌 시장 통계 분석 매체 “Newzoo”[1]에 따르면 2023년까지 글로벌 게임 시장 규모가 2,000억 달러를 넘어설 유망한 시장이라 평가하였다.

게임 전문 리서치 ‘게임트릭스’[2]의 2023년 4월 1주차 주간 게임 동향에 의하면, 넥슨의 ‘서든어택(SuddenAttack)’, 라이엇 게임즈의 ‘발로란트(Valorant)’, 블리자드 엔터테인먼트의 ‘오버워치2(OverWatch2)’, 블루홀의 ‘배틀그라운드(BattleGround)’ 순으로 게임 점유율 순위 3위부터 6위까지 FPS(First Person Shooter) 게임들이 차지하였다. 이는 FPS 게임이 대중적으로 큰 인기를 얻고 있음을 보여준다. 하지만, 이러한 인기와 더불어 FPS 게임 내에서 AimBot들이 빠르게 등장하고 있다. AimBot이란, FPS 게임에서 조준을 자동으로 수행하는 매크로의 일종이다.

본 논문에서는 Aimbot들에 대응할 수 있도록 과거 FPS 게임들에 등장한 메모리 변조를 사용하는 AimBot 사례들과 악성코드 탐지 방법들을 분석해 메모리 변조를 사용하는 AimBot을 탐지할 방안을 연구하였다.

2. 관련 사례 분석

2.1 “AssaultCube”의 Aimbot 분석

AssaultCube는 Cube 게임 엔진 기반으로 만들어진 오픈 소스 FPS 게임이다. 주로 사용된 라이브러리는 _.pId, _.hWnd, _.moduleBase, _.health, _.armor, _.xPos, _.yPos, _.zPos이 있으며 상대방의 위치정보와 자신의 위치정보 사이의 각도를 계산하여 나온 계산값을 자신의 마우스 위치값에 적용시켜 상대방에게 자동으로 조준할 수 있도록 해준다.

2.2 강화학습이 적용된 AimBot 분석

강화학습을 사용하여 목표물을 조준하고 발사하는 봇을 훈련시킨다. Unity의 공식 리포지토리에서 MLAgent를 복제하고 Python 및 Tensorflow와 같은 필요한 종속성을 설치한 다음 MLAgents SDK 라이브러리를 사용했다. 학습에 사용된 봇은 x축과 y축에서 회전할 수 있는 카메라이고 봇은 위-아래, 왼쪽-오른쪽 및 발사 3가지 작업을 수행한다. 환경은 벽이 서 있는 방에 배치되며 목표물이 무작위로 나타나며 회전, 자신과 타겟 사이의 dispalcement 벡터, 전방 벡터와 변위 벡터 사이의 각도를 공급받는다.

<표 1> 강화 학습 AimBot의 보상방식

보상	설명
+100	목표물을 정확하게 조준한다.
+0.1	십자선을 목표물 쪽으로 이동한다.
-0.001	십자선을 대상에서 멀어지게 한다.
-10	십자선을 벽 밖으로 이동한다.
-0.001	모든 프레임, 더 빠른 조준을 장려한다.
-0.5	시간 제한으로 인해 환경이 재설정될 때마다.

봇의 조준/십자선이 벽을 떠나거나 목표물에 적중할 경우, 이 두 가지 일이 발생하지 않고 일정 시간이 지난 경우 환경을 재설정한다. 환경을 재설정할 때 대상은 벽의 새로운 임의 위치로 이동되고 봇의 회전은 초기 회전으로 설정된다.

2.3 API 호출 중심 악성코드 분석

Mamoun Alazab 외 3인이 연구한 Towards Understanding Malware Behaviour by the Extraction of API calls[3]에 의하면 모든 실행 프로그램은 API 호출을 사용하여 작업을 수행한다. 악성코드는 다른 코드들과 비교적 다른 동작을 수행하기에 프로그램 바이너리에서 API 호출을 추출하여 가장 일반적인 악성코드 동작 패턴을 분석하고 프로그램 실행 파일을 악성 또는 양성으로 분류했다.

2.4 OpCode 패턴 분류기법 적용 악성코드 탐지

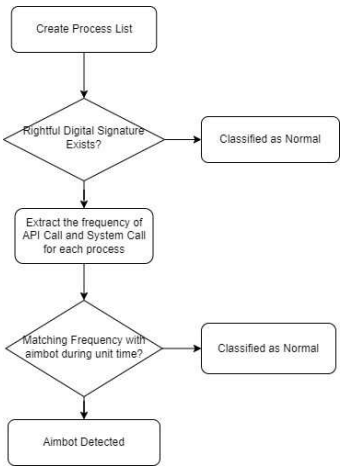
Asaf Shabtai 외 4인이 연구한 Detecting unknown malicious code by applying classification techniques on OpCode patterns[4]에 의하면 검사된 실행 파일을 분해하여 생성된 OpCode n-gram 패턴을 사용하여 검사된 파일에서 기능을 추출한다. 이 추출된 OpCode n-gram 패턴은 알려지지 않은 악성코드를 식별하기 위해 분류 프로세서에서 사용된다.

2.5 특정 랜섬웨어(Cerber)의 탐지방법 분석

이계혁 외 4인이 연구한 Opcode와 API의 빈도수와 상관계수를 활용한 Cerber형 랜섬웨어 탐지모델에 관한 연구[5]에 따르면 특정 랜섬웨어(Cerber)를 탐지할 때 RandomForest 알고리즘을 사용한 탐지모델에서는 는 N_estimators/depth 값이 96/2일 때, SVM 알고리즘을 사용한 탐지모델에서는 Cost 값이 138일 때 각 97.4%, 94.8%로 나타났다.

3. 연구 방법

연구를 진행할 환경은 Unity3D 2019.4.36f1을 통해 생성한 Micro FPS 게임 프로젝트를 대상으로 한다. 디지털 서명이 되지 않은 프로그램들에 대해 AimBot들이 자주 사용하는 API와 System Call의 단위 시간 동안 빈도수를 측정해 탐지하는 연구를 진행한다.



(그림 1) 연구 Flow-Chart

4. 결론

AimBot들을 분석했을 때 사용자와 상대방의 위치정보를 계산해서 나온 yaw, pitch값을 게임내 자신의 yaw, pitch 값으로 게임 프로세스의 메모리를 변조하기위한 WIN API인 ReadProcessMemory()와 SendInput() 같은 사용자의 마우스 제어 API를 공통적으로 사용하는 것을 확인하였다 향후 연구에서는 위치 정보와 마우스 정보를 지속적으로 요청하는 행위가 패턴화 되어있기에 이 패턴을 학습시켜 AimBot을 탐지하도록 연구를 진행할 예정이다.

참고문헌

[1] Newzoo, “2021 Global Games Market”, May 6 2021

[2] Gametrics, “2023년 4월 1주차 주간게임동향”, 2023.04.10.

[3] Mamoun Alazab, Robert Layton, Sitalakshmi Venkataraman, Paul Watters, Towards Understanding Malware Behaviour by the Extraction of API Calls Conference Paper · July 2010

[4] Asaf Shabtai, Robert Moskovitch, Clint Feher, Shlomi Dolev, Yuval Elovici Detecting unknown malicious code by applying classification techniques on OpCode patterns Shabtai et al. Security Informatics 2012

[5] 이계혁, 황민채, 현동엽, 구영인, 유동영 정보처리학회논문지. 컴퓨터 및 통신시스템 / KIPS Transactions on Computer and Communication Systems. Oct 31, 2022 11(10):363