현재 안티 치트들의 작동방식

* 클라이언트가 보내는 정보를 감시  
  게임서버에서 클라이언트가 보내는 정보를 감시하여 핵을 사용하는지 적발하는 것 이다.   
  원래 규칙에는 없는 동작, 이를테면 게임 캐릭터가 하늘에 날아다닌다 거나 정상적으로는 불가능한 위치정보 변동을 서버에서 감시하는 것 이다.   
  에임 핵의 경우, 플레이어의 에임을 감시하는 방식으로 만은 에임 핵을 적발하진 않는데, 일반인이 보기에는 핵이라고 생각될 수 있는데 정말 에임이 말도 안될 정도로 뛰어난 사람도 존재하기 때문이다.   
  그래서 보통 게임 회사들은 기술적인 부분에서 다양한 검토를 걸쳐서 핵을 적발하고 밴을 한다.   
  이 안티치트는 서버사이드에서 작동하기 때문에 서버와 연결이 불안정하여 갑작스럽게 위치가 변하는 경우를 핵으로 판단할 소지가 있다.
* 게임 클라이언트 무결성 검사  
  플레이어가 실행중인 게임 클라이언트에 원래 클라이언트에는 존재하지 않는 부적절한 코드가 포함되어 있는지 패키지 검사를 하는 방식으로도 핵 적발이 이루어진다. 하지만 이런 방식은 클라이언트 프로그램 자체를 조작한 핵에만 해당하며, 클라이언트 자체는 조작하지 않았으나 그 게임 클라이언트에 간섭하는 프로세스를 수행하는 별도의 프로그램의 경우까진 적발할 수 없다. 따라서 이 경우엔 아래와 같은 방식이 사용된다.
* 실행중인 프로세스와 컴퓨터 사용기록 분석  
  컴퓨터 시스템의 정보, 실행중인 모든 앱과 백그라운드, windows 프로세스를 감시하여 그 중에서 게임 클라이언트에 부적절한 접근, 간섭을 하는 코드를 실행하는 프로그램을 적발하는 것 이다.  
  가장 강력하고 효과적인 방식이나, 몇가지 딜레마가 존재한다. 일단 프로세스 전부를 실시간으로 모니터링 하다보니 CPU 점유율이 있어서 사양이 낮은 컴퓨터에는 원활한 게임 진행에 방해가 될 수 있으며 너무 지나치게 사용자의 컴퓨터 정보에 접근하는 안티 치트는 개인정보침해논란으로도 번질 수 있기 때문이다.   
  이러한 논란은 EasyAntiCheat문서에서도 자세히 설명되어 있다.   
  예를 들어 VAC의 경우는 사용자의 DNS 캐시, 즉 인터넷 접속 기록을 밸브 서버에 보낸다는 사실이 밝혀진 뒤 개인정보 침해 논란이 있었는데, 단순히 핵 사이트에 들어간 기록이 있을지만 매칭할 뿐 이고 그 외 사용자가 어떤 페이지에 들어갔는지는 보지 않는다고 해명했다. 물론 그렇다고 개인정보 침해를 없던 일로 할 수는 없다. 핵 사이트에 들어간 기록도 엄연한 개인정보의 일부이다.
* 커널 모드 디바이스 드라이버  
  안티 치트는 컴퓨터의 모든 프로세스를 원활하게 검사하고 자가 보호를 위해 커널 모드 드라이버를 사용한다.   
  게임을 실행할 때 관리자 권한을 요구하는 이유는 안티 치트의 커널 드라이버를 실행하기 위해서다.
* 가상머신 감지  
  대부분의 안티 치트는 가상머신 환경 확인 기능이 들어있다.   
  가상머신 환경일 경우 게임이 종료된다.