

게임 커뮤니티를 오래 지켜보면, 무료 체험을 내세우는 배그핵 광고가 공기처럼 떠다니는 시기가 있다. 큰 업데이트 직후, 시즌 초기, 혹은 핵 탐지 시스템의 공백이 소문으로 번질 때가 그렇다. 당장은 호기심과 편의가 앞선다. 설치만 하면 헤드샷률이 오르고, 승률이 올라간다고 말한다. 비용도 없으며 살살 달란다. 하지만 무료라 여긴 순간 시작된 비용이 조용히 쌓인다. 시스템 보안의 구멍, 계정 정지 이력, 도용된 스킨과 화폐, 그리고 무엇보다 남는 불신. 몇 해 동안 여러 사건을 옆에서 겪고, 포렌식으로 실마리를 찾으며 내가 배운 점은 단순하다. 배그핵의 무료 체험에는 공짜가 없다.

## 왜 무료 체험이 늘 문제를 부르는가

유료 핵은 거래 기록이 남고, 결제가 취소되면 자금이 역추적될 가능성이 높다. 그래서 일부 유포자는 진입장벽을 낮추려고 무료 체험판을 미끼로 쓴다. 눈에 띄지 않는 목적은 트래픽을 모으는 것이다. 실행 파일 배포, 관리자 권한 요청, 보안 예외 추가, 디스코드나 텔레그램 챗방로 유도, 이 과정 전부가 신뢰를 깎는다. 그리고 이 신뢰의 틈으로 악성 모듈이 들어온다. 표면적으로는 배그핵이지만, 안쪽에 붙어 있는 것은 계정 탈취기, 브라우저 암호 덤프, 장치 지문 수집기, 가상통화 지갑 스니퍼가 섞인다. 유포자는 이렇게 채집한 데이터로 더 많은 돈을 번다.

무료 체험을 둘러싼 심리는 단순하다. 남들보다 먼저 써본다는 선점 욕구, 지금만 반짝 써보고 버리자는 안전 착각, 그리고 비용이 0이면 리스크도 낮다는 오류. 실제로는 반대다. 유료의 경우라도 위험하지만, 무료는 그 자체로 공격자가 리스크를 전가하는 신호다.

## 숨은 비용 1, 계정 정지와 기록이 남기는 그림자

게임사는 사업의 핵심을 공정성으로 지킨다. 치팅 탐지 시스템은 완벽하지 않지만, 로그와 패턴을 축적한다. 무료 체험판조차 실행 파일이 메모리를 패치하고, 드라이버를 로드하고, 렌더링 체인을 건드리면 흔적이 남을 수밖에 없다. 한 번 정지되면 끝이라는 말은 과장이 아니다. 하드웨어 뱅까지 걸리면 장비 교체가 필요하고, 지문 마스킹을 하려다 또 다른 도구를 깔게 된다. 고작 몇 판의 우위를 위해 수십 시간, 수백 시간 쌓아둔 기록을 한순간에 잃는다.

문제는 정지가 과거형으로 끝나지 않는다는 점이다. 최근 몇 년간 로스터 검증이 강화되면서, 프로 아마추어 대회, 랭크 상위권 출신 지원 과정에서 정지 이력 제출 요구가 잦아졌다. 몇 달, 몇 년 전 무료 체험으로 남긴 잡음이 커리어의 발목을 잡는다. 취미 수준이라도 친구들이 바라보는 눈빛이 변한다. 커뮤니티는 기억력이 좋다.

## 숨은 비용 2, 스킨과 화폐가 사라지는 방식

배그는 총기 스킨과 크레이트, 배틀패스를 통해 경제가 돈다. 계정의 가치가 단순하게 금액으로만 환산되진 않지만, 거래 시세로 따지면 수십만 원에서 수백만 원까지도 간다. 무료 핵 배포 파일에 붙은 정보 탈취기는 이 가치부터 노린다. 가장 흔한 경로는 브라우저와 런처의 세션 토큰 탈취다. 공격자는 계정이 활성화된 상태에서 세션을 복제해 2차 인증을 건너뛰고, 스킨을 제3자 계정으로 옮긴다. 전송 중 잠깐의 공백조차 보이지 않게 작업한다. 피해자는 다음 로그인 시점에서야 눈치챈다.

탈취 방식이 점점 정교해진 것도 함정이다. 예전에는 키로거가 주류였다면, 지금은 암호 관리자 확장 프로그램 데이터와 쿠키 저장소를 툴다. 브라우저가 크로미움 계열이면 구조가 비슷하다. 공격자가 OS 레벨의 데이터 보호 API를 우회해 복호화한 사례도 봤다. 가끔은 자산만 노리지 않는다. 디스코드나 이메일 계정 접속 토큰까지 가져가 주변인 계정으로 확산을 시도한다. 한 번의 무료 체험으로 피해의 범위가 게임을 넘는다.

## 숨은 비용 3, 시스템의 무게와 기회비용

치트 로더는 시스템 코어에 가까울수록 무겁다. 커널 드라이버를 로드하려면 서명이 필요하고, 이를 우회하려면 보안 기능을 꺼야 한다. 보안 부팅 비활성화, 드라이버 서명 강제 해제, 안티치트 예외 등록, 이 조치가 겹친 PC는 더 취약해진다. 그렇게 손 본 시스템을 다시 원상복구하는 데 드는 시간은 생각보다 길다. 포맷까지 가는 경우도 적지 않다. 데이터 백업, 재설치, 인증, 튜닝, 이 며칠은 게임은커녕 일을 미뤄야 한다. 공짜는 없다, 이 말이 여기서 또 유효하다.

또 한 가지 비용은 학습 기회의 상실이다. 핵에 기대는 동안 예임, 포지셔닝, 사운드 리딩, 팀 소통이 느려진다. 한 시즌, 두 시즌 지나면 실력의 근육이 퇴화한다. 나중에 정상 플레이로 돌아와도 몸이 반응하지 않는다. 실력이 줄어든 공백을 다시 메우는 데 몇 배의 시간이 든다.



## 내가 본 실제 사례

작년 여름, 장비 최적화 상담을 하던 대학생 A가 이틀 만에 다시 연락했다. 배그핵 무료 체험을 깔았다가 게임이 꺼지고, 계정에 접속이 튕긴다고 했다. 원격으로 들어가 보니 이상한 점이 여러 개였다. 시작 프로그램에 이름을 바꾼 서비스가 둘, 이전에 없던 루트 인증서가 하나, 브라우저의 로그인 세션 수가 급증해 있었다. 포렌식 툴로 훑어 보니 특정 도메인과 비정상 통신 흔적이 있었고, 그 시간대에 스팀 마켓 기록이 비어 있었다. 이 계정에서만 보유한 스킨 몇 개가 자취를 감췄다.

우리는 OS를 재설치하고, 모든 비밀번호를 바꾸고, 2차 인증을 새로 걸었다. 그런데 문제는 거기서 끝나지 않았다. A는 트위터와 디스코드에서도 비정상 로그인 경고를 받았다. 공격자가 브라우저에서 같이 탈취한 토큰을 돌려 쓴 것이다. 사건이 수습되기까지 5일 정도 걸렸다. A는 무료 체험을 다운받는 데 5분을 썼고, 잃은 시간은 수십 시간이었다. 남은 건 찝찝함과 대체 불가 스킨의 빈 자리뿐이었다.

## 기술적으로 무슨 일이 일어나는지

배그핵의 로더는 보통 두 단계로 동작한다. 먼저 외부에서 암호화된 페이로드를 내려받고, 메모리 상에서 복호화해 주입한다. 이 과정에서 관리자 권한을 요구하는 이유는 커널 또는 드라이버 레벨 접근 때문이다. 윈도우의 사용자 계정 컨트롤을 우회하는 기법도 붙는다. 이때 공격자가 추가로 엮기 쉬운 기능이 정보 수집이다. 시스템의 하드웨어 ID, MAC 주소, 설치된 보안 프로그램 목록, 실행 중인 프로세스를 모아서 전송한다. 이 데이터는 나중에 하드웨어 밴을 피하는 데 쓰이기도 하고, 반대로 장비 지문을 묶어 피해자를 특정하는 데도 쓰인다.

정보 탈취기는 브라우저의 로그인 데이터베이스와 쿠키 저장소를 노린다. 크롬 기반 브라우저는 로컬 상태 키와 DPAPI를 조합해 민감 데이터를 보호한다. 공격자는 로컬 키를 가져와 메모리 내에서 복호화하고, 크로스 세션으로 토큰을 재사용한다. 2단계 인증이 걸려 있어도 이미 로그인된 세션이면 무용지물이다. 게다가 클립보드 모니터링, 암호 관리자 데이터 훔치기, 디스코드 레벨DB 접근 등은 추가 코드 몇 줄이면 된다. 무료 체험이라고 달라지지 않는다. 오히려 무료에서 이런 모듈이 섞일 확률이 높다.

한편, 커널 드라이버를 통한 렌더링 오버레이는 그래픽 파이프라인을 건드린다. 안티치트가 메모리 스캔과 행위 기반 탐지를 병행하기 때문에, 로더는 은폐에 더 많은 신경을 쓴다. 이때 루트킷적 기법이 곁들여지는데, 이런 은폐가 시스템 안정성을 크게 떨어뜨린다. 블루 스크린, 랜덤 프리징, 장치 인식 오류로 이어지는 경우를 자주 본다.

# 통계가 말해 주는 현실

정확한 숫자는 공격자의 영역이라 공개되지 않는다. 다만 업계 전반을 보면 대략적인 범위는 있다. 자격 증명 채우기 공격의 성공률은 보통 0.1퍼센트에서 2퍼센트 사이다. 하지만 게임 커뮤니티처럼 동일 비밀번호 재사용률이 높은 곳에선 상한선이 더 올라간다. 탈취된 게이밍 계정의 암시장은 가격이 천차만별인데, 레벨, 스킨, 결제 이력, 지역, 락 상태에 따라 수천 원에서 수십만 원까지 매겨진다. 공격자가 무료 체험으로 유입된 1,000명 중 10명만 털어도 이득이 남는 구조다. 무료를 미끼로 쓰는 동기가 여기에 있다.

## 법적 리스크와 책임

치팅 프로그램 사용은 이용약관 위반이다. 여기서 끝나지 [배그핵](#) 않는다. 유포, 판매, 제작은 국내법상 업무방해, 정보통신망 침해 관련 규정에 저촉될 여지가 있다. 일부 판례에서는 게임사의 서비스 제공을 방해하는 행위로 처벌이 내려졌다. 사용자가 단순 이용자라 해도, 계정 도용과 결합되면 피해 규모가 커진다. 본인 계정이 해킹의 소스가 되어 주변인에게 피해가 확산되면 도의적 책임을 피하기 어렵다. 해외 서버를 경유했다고 안전하다는 믿음은 신기루에 가깝다. 로그는 남는다.

## 가짜 안전장치의 유혹

일부는 가상 머신, 샌드박스, 테스트용 서브 계정을 쓰니 괜찮다고 말한다. 직접 검증해 보면 이런 방어는 구멍이 많다. 커널 드라이버를 요구하는 치트는 가상 머신에서 제대로 동작하지 않거나, 동작하게 만들려다 호스트에 영향을 미친다. 샌드박스는 사용자 공간에서 제한을 걸 뿐이라, 관리자 권한을 얻은 악성 모듈에는 무력하다. 서브 계정도 안전망이 아니다. 같은 PC에서 로그인하면 세션과 쿠키, 런처 데이터가 공유될 수 있다. 하드웨어 밴은 장비 지문을 따른다. 안전하다는 말은 보통 유포자가 믿게 만들려고 하는 소리다.

## 무료 체험 홍보 문구를 보는 눈

초보가 보기엔 그럴듯한 진술이 많다. 오래 보다 보면 책임을 회피하는 문장, 기술적으로 불가능에 가까운 문구가 눈에 들어온다. 빠르게 거를 수 있도록, 홍보 문구에서 특히 주의할 표현을 정리한다.

- 안티치트 100퍼센트 우회, 평생 안전 보장
- 설치 필요 없음, 클릭 한 번으로 적용
- 관리자가 직접 지원, 환불 100퍼센트
- 정품 드라이버 서명 사용, 시스템에 무해
- 인증된 유저 10만 명, 검증 완료

표현만 보면 든든해 보이지만, 보안에서 100퍼센트는 금기다. 설치가 없다면 메모리 인젝션인데, 이런 방식은 오히려 탐지에 취약하다. 정품 서명은 도난된 인증서일 가능성이 있고, 이 경우 더 위험하다. 사용자 숫자는 확인할 길이 없다. 영수증이나 제3자 감사를 내놓지 못하면 믿지 않는 편이 낫다.

## 이미 설치했다면, 무엇을 해야 하나

실수는 누구나 한다. 핵심은 빠르게 범위를 좁히고, 두 번째 피해를 막는 일이다. 당장 할 수 있는 조치를 간결하게 정리한다.

- 네트워크를 끊고, 게임과 런처를 포함한 모든 프로세스를 종료한다.
- 오프라인 상태에서 중요한 파일을 외장 저장장치에 백업한다.
- 다른 기기에서 비밀번호를 모두 변경하고, 가능한 서비스에 2차 인증을 켜고.
- 포렌식 도구가 없다면, 초기화와 재설치를 고려한다. 재설치 후 복원은 신중히 진행한다.
- 게임사 고객센터에 접속 이력과 자산 변동 내역을 문의한다.

이 다섯 가지면 초기 대응은 충분하다. 추가로, 은행, 이메일, 디스코드 같은 주요 계정의 로그인 내역을 전부 훑어보자. 예상치 못한 지역, 새 기기 표기가 보이면 세션을 전부 강제 로그아웃하고, 복구 이메일과 전화번호를 다

시 확인한다. 공격자는 보조 채널을 바꿔두는 경우가 많다.

## 계정을 지키는 습관에 관해

예방은 도구보다 습관이 만든다. 비밀번호는 서비스마다 다르게, 길게 만든다. 비밀번호 관리자를 쓰면 유지가 쉽다. 2차 인증은 앱 기반으로 설정한다. SMS는 편하지만, 교환 사거나 SIM 스와핑에 취약하다. 스팀가드 모바일 인증기를 켜면 계정 회수에 큰 도움이 된다. 브라우저의 비밀번호 저장 기능을 꺼두라는 조언을 종종 듣지만, 현실적으로 어렵다. 대신 장치 자체의 잠금, 암호화, 최신 업데이트를 유지하는 편이 낫다.

관리자 계정으로 평소 작업하지 않는 것도 도움이 된다. 표준 사용자 계정을 만들고, 필요할 때만 승격하는 습관이 악성코드의 자리 잡기를 늦춘다. 이메일 필터는 과소평가되지만, 피싱 링크의 첫 관문을 막아준다. 디스코드, 텔레그램의 링크 미리보기 차단도 효과적이다. 특히 친구가 보낸 링크라도 맥락이 이상하면 의심하자. 공격자는 먼저 주변인을 뚫고 신뢰를 훔쳐낸다.

## 성능 최적화로 얻는 실질적 이득

핵 없이 성적을 올리는 방법은 생각보다 많다. 그래픽 설정을 낮춰 가시성을 확보하는 것만으로 교전에서 반 템포 앞서간다. 프레임 타겟을 144 혹은 165으로 고정하고, 입력 지연을 줄이는 세팅을 병행하면 체감이 크다. 엔비디아 리플렉스, AMD 안티-래그 같은 기능은 이름값을 한다. 네트워크 측면에서는 공유기의 큐오스 설정, 이중 NAT 제거, 유선 연결 전환이 안정성을 높인다. 헤드셋의 좌우 밸런스를 상황에 맞게 조절하고, 발소리 주파수대를 살짝 올리면 방향 파악이 빨라진다.

에임 트레이너를 하루 10분만 해도 추적, 미세 조정, 클릭 타이밍이 달라진다. VOD를 보며 자신이 죽은 장면을 세 번씩 돌리는 습관을 들이면 원인을 구체적으로 본다. 상대가 잘해서 졌는지, 내가 잘못 섰는지, 이동 루트가 들켰는지, 이런 구분이 쌓이면 다음 선택이 바뀐다. 듀오나 스쿼드에서는 콜아웃을 합의하고, 노이즈를 줄이자. 간단한 규칙 하나, 예를 들면 교전 중엔 좌표 먼저 말하고 감상은 나중에, 이런 합의도 승률을 끌어올린다.

## 경제적 계산, 냉정하게 따져 보기

한 계정에 들어간 시간과 돈을 적어 보자. 시즌 패스 몇 번, 스킨 몇 개, 랭크를 올리기 위한 시간, 친구들과 보낸 밤, 합치면 적지 않다. 가치를 돈으로 환산하기 어렵다면, 잃었을 때 다시 만들 수 있는지 스스로에게 물어보면 된다. 다시 만들 수 없다면 그 가치는 크다. 무료 체험이 부르는 손실은 대개 이 가치를 정면으로 친다. 계정이 잠깐 정지됐다가 풀리는 행운을 믿기보다, 아예 그런 상황을 만들지 않는 편이 낫다.

## 커뮤니티와 신뢰의 구조

게임은 기본적으로 사회적 활동이다. 스쿼드의 한 명이 치트로 이긴 승리는 아무도 자랑하지 못한다. 커뮤니티의 암묵지는 생각보다 촘촘하다. 특정 시간대 특정 매치에서 말없이 이상하게 잘한 플레이어는 금방 표적이 된다. 신고와 의심이 겹치면, 진짜 실력자도 엮인다. 그래서 핵은 개인의 편의가 아니라 공동의 신뢰를 부순다. 무료 체험을 덤씩 받은 순간, 그 균열은 시작된다.

## 소프트웨어 배포의 표면과 이면

무료 체험을 배포하는 채널을 보면 패턴이 있다. 신생 웹사이트, 무료 파일 호스팅 링크, 광고가 과도하게 많은 블로그, 우리끼리만 안다는 디스코드 방. 파일 형식은 압축 파일로 위장하고, 내부에 스크립트와 실행 파일을 섞는다. 압축 비밀번호를 알려준다면 DM을 유도하고, 채팅 창 밖에서 소통하자고 한다. 이 일련의 과정이 전부 흔적을 지우기 위한 장치다. 깔끔하게 만들어진 제품처럼 보이게 포장하지만, 계약, 환불, 책임은 어디에도 없다.

## 가끔 듣는 반론에 대해

누군가는 무료 체험으로 장난삼아 한두 판 했고, 아무 일 없이 넘어갔다고 말한다. 그런 사례가 존재하는 것은 사실이다. 하지만 보안은 확률의 게임이다. 탐지도 확률, 감염도 확률, 회수도 확률이다. 오늘은 운이 좋았다 해도, 내일 업데이트가 들어가면 로그가 뒤늦게 매칭될 수 있다. 이 주의 업데이트 노트에 잡히지 않아도, 수집된 데이터셋 위에서 패턴이 바뀌면 과거의 행위가 새 기준에 걸린다. 도둑이 한 번 들어오고 아무것도 안 훔쳤다고 해서 문단속을 그만둘 이유는 없다.

## 개발자의 관점에서 본 손익

게임사가 안티치트에 쓰는 예산은 연간 수익에서 수십억 원 사이다. 이 예산은 핵 유저 몇 명을 쫓기 위해서가 아니라, 대다수의 몰입을 지키기 위해 쓰인다. 핵 유저가 몰려오는 주기에 따라 신규 가입자가 이탈하고, 스트리머가 게임을 내려놓는다. 지표는 민감하다. 신규 유입 대비 2주차 잔존율이 몇 퍼센트포인트만 떨어져도 손실이 크다. 그러니 게임사는 정지 정책을 강하게 가져간다. 한 유저의 치팅이 공동 자산을 해치기 때문이다. 개발자 입장에서는 설계 선택이 무거울수록 정상 유저에게도 불편이 간다. 이 불편을 줄이기 위한 노력과 핵과의 싸움 사이에서 균형을 잡는다. 무료 체험을 고리로 들어온 핵이 커질수록, 그 균형점은 정상 유저에게 불리하게 이동한다.

## 스스로 묻기

배그핵 무료 체험을 누르기 전, 간단히 자문해 보자. 지금의 실력 부족을 인정하기 어려워서인가, 짧은 만족을 얻고 싶은가, 팀원과의 약속을 가볍게 여겼나. 내가 잃을 수 있는 것을 명확히 적어 보면 답은 대개 선명하다. 시스템의 구멍은 언제나 있다. 하지만 그 구멍을 통과하는 데 따르는 대가를 감당하는 사람은 드물다. 도전은 어렵고, 지름길은 매력적이지만, 게임에서의 성취는 지름길에서 나오지 않는다.

## 정리, 빗장과 습관

핵은 기술의 문제가 아니다. 유혹과 선택의 문제다. 무료 체험이라는 단어가 갖는 달콤함 뒤에 숨어 있는 비용을 이해하면, 선택은 쉬워진다. 계정을 지키는 습관을 들이고, 장비를 정돈하고, 팀과의 약속을 단단히 하면 된다. 만약 실수를 했다면 빠르게 끊고, 범위를 좁히고, 기록을 남겨 복구하자. 배그핵은 잠깐의 승리를 줄 수 있다. 그러나 그 승리를 기념할 자리는 소실점처럼 멀어진다. 게임을 오래 즐길수록 알게 된다. 진짜 재미는 불안이 아니라 확신에서 나온다.