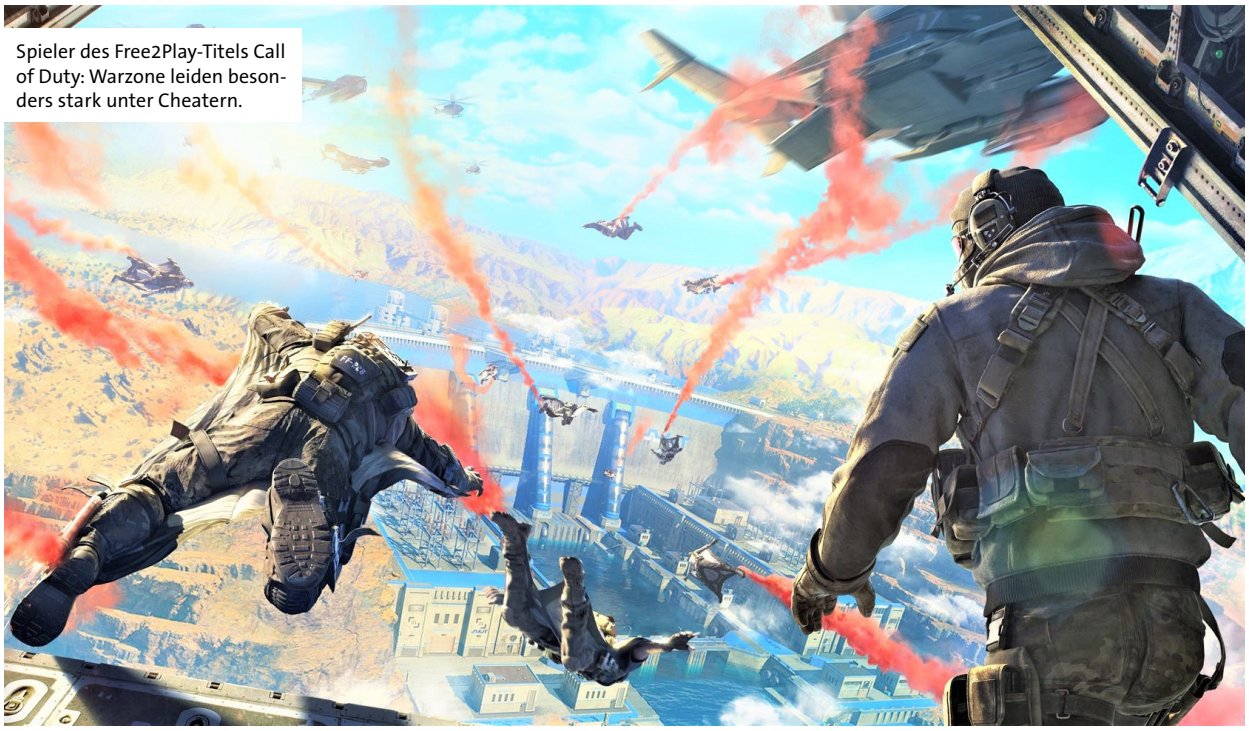
Die nächste Generation

CHEATS MIT KI

Ein KI-Cheat namens User Vision Pro könnte das Betrügen revolutionieren. Zwar wurde das Programm von Activision schnell abgeschossen, beunruhigende Fragen bleiben aber. Von Christian Just



Spieler des Free2Play-Titels Call of Duty: Warzone leiden besonders stark unter Cheatern.

Wie viel Skynet steckt im Gaming der Zukunft? Laufen bald nur noch virtuelle Terminatoren, ausgerüstet mit KI-Cheats, durch unsere liebsten Mehrspielertitel? Allzu fern scheint so eine Zukunft nicht mehr zu sein. Ein KI-Cheat namens User Vision Pro (Userviz) wollte nicht nachweisbar sein, live das Gameplay des Schummlers analysieren und die Controller-Eingaben so manipulieren, dass ein Shooter-Spieler immer trifft. Zumindest in der Theorie, denn noch vor dem Release erklärte der Entwickler – ein ominöser »USER101« – das Projekt nicht weiter zu verfolgen. Activision Blizzards Anwälte hatten zugeschlagen und dem Treiben ein jähes Ende bereitet, um das Cheater-Problemkind Call of Duty: Warzone zu beschützen. Dennoch bleiben von dem »Abenteuer« hochbrisante Implikationen übrig.

Bedrohen künftig mächtige, für Otto Normalnutzer unerkennbare KI-Cheats die Integrität von Multiplayer-Partien? Sind wir als ehrliche Spieler bald in der Minderheit? Wir haben mit Anticheat-Experten, Cheat-Entwicklern und natürlich auch Cheat-Nutzern gesprochen. Während Entwickler euch technisch ins Bild setzen, gewähren die Cheater einen seltenen Einblick in die Gedankenwelt der Szene. Kurz vorab: Ganz so schlimm wie befürchtet wird es vermutlich nicht, aber es bleibt doch noch Grund zur Sorge.

Eine bunte Tüte Cheats

Cheats dürften den meisten Spielern ein gängiger Begriff sein. Wer gerne online zockt, ist bestimmt bereits mit dem ein oder anderen unfairen Spieler in Kontakt gekommen, sei es in aktuellen Blockbustern wie Call of Duty: Warzone oder uralten Klassikern wie Counter-Strike 1.6. Jeder Schuss ein Treffer, auch über Kilometer Entfernung, ohne dass man die Maus überhaupt anrühren muss? Kein Problem mit Aim- und Trig-

GTA Online ist ein beliebtes Ziel von Hackern und Cheatern. Die Community ist verärgert: Tut Rockstar genug gegen die Spielverderber?

gerbot. Die Position aller Spieler auf der ganzen Map durch Wände hindurch erkennen? Wallhacks machen es möglich.

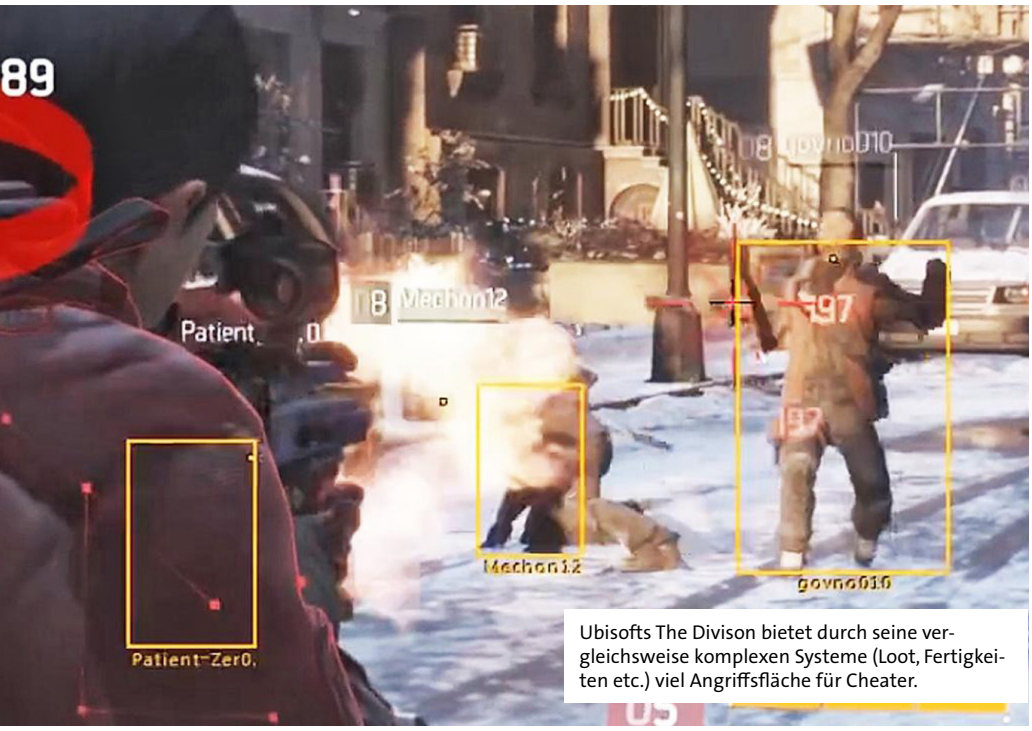
Dabei handelt es sich nur um zwei bekannte Beispiele. Heutzutage decken Cheats schließlich ein sehr breites Spektrum ab, fast kein Spielelement ist vor unerlaubten Manipulationen sicher. Die Methoden reichen von Scripting/Modding (oft gesehen in GTA Online) über unerlaubte Makronutzung (zum Beispiel um in Shootern Schnellfeuer zu erzwingen) bis hin zu World Hacking (um in einem Echtzeitstrategiespiel den Fog of War zu entfernen).

Aber auch unsportliches Verhalten, etwa das Ausnutzen von im Spiel enthaltenen Fehlern (Exploits) oder das in MMOs vorkommende Character Sharing, können von Entwicklern und der Community mit dem Prädikat Cheating versehen werden. Was erlaubt ist und was nicht, beruht zum einen auf dem allgemeinen Konsens und wird zum anderen explizit in den Nutzungsbedingungen von Spielen definiert.

Was sind diese Machine Learning Cheats eigentlich?

Die Verwendung von Machine Learning, also lernender künstlicher Intelligenz, stellt eine Art moderne Weiterentwicklung bekannter Cheat-Konzepte dar. Mitunter kommt es unterstützend schon seit Jahren bei klassischen Cheats zum Einsatz. User Vision Pro beziehungsweise Userviz wollte das Konzept auf die nächste Stufe heben. Userviz soll analysieren, was auf dem Monitor des Nutzers geschieht, indem es die Frames direkt an der Grafikkarte ausliest. Das soll für minimale Verzögerung sorgen. Mit Hilfe von Machine Learning erkennt das Programm menschliche Silhouetten von Spielfiguren und unterscheidet zwischen Freund und Feind. Taucht nun ein Feind im Blickfeld des Cheat-Nutzers auf, sendet Userviz Controller-Eingaben an den Computer.

Wer sich besonders sicher fühlen will, dabei nicht erwischt zu werden, kann zusätzliche, sozusagen externe Hardware nutzen. Dann kommen die Eingaben nicht von User-

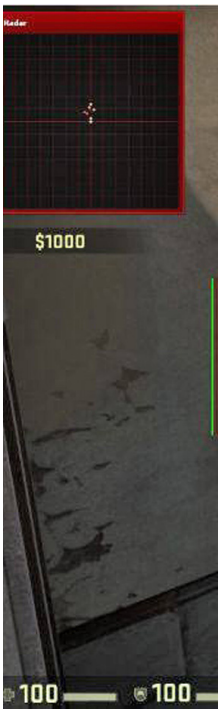


Ubisofts The Divison bietet durch seine vergleichsweise komplexen Systeme (Loot, Fertigkeiten etc.) viel Angriffsfläche für Cheater.

UNSER EXPERTE

Paul Chamberlain ist ein seit vielen Jahren erfahrener Spieleentwickler und Software-Ingenieur, der an Fortnite, Valorant und League of Legends mitgearbeitet hat. Er hat Anti-Cheat-Teams bei Riot Games und Epic Games geleitet und zu Anti-Cheat-Systemen wie Vanguard und dem »Fog of War«-System von Valorant beigetragen. Vor seiner Tätigkeit in der Spielebranche arbeitete er im technischen Bereich für Google und die australische Regierung.

Eine der schwierigsten Aufgaben der Macher von Battlefield 2042 wird es sein, Cheater im Zaum zu halten.



In Age of Empires haben die Entwickler selbst Cheats eingebaut, die Autos als Einheiten erzeugen. (Bild: SergiuHellDragoonHQ/YouTube)

viz auf dem eigenen PC, sondern eben extern von einer Videoaufnahmekarte. Jetzt passiert die (schwarze) Magie: Die KI bewegt die Waffe auf den richtigen Punkt für einen Treffer und drückt ab. Peng, Gegner besiegt – ohne dass der Mensch vor dem Monitor viel beitragen müsste.

Das Ganze geschieht natürlich, ohne die eigentlichen Spieldateien zu manipulieren, wodurch es für Anti-Cheat-Organisationen und -Abteilungen schwierig werden soll, die Nutzung von Userviz nachzuweisen. Was wie eine Kampfansage an Gegenmaßnahmen klingt, ist aber vermutlich nicht viel mehr als PR, wie uns der renommierte Anti-Cheat-Entwickler Paul Chamberlain (siehe Kasten) erklärt: »Cheats, die nicht auf dem Gerät arbeiten, auf dem das Spiel gespielt wird, können einige Arten von Anti-Cheat-Erkennungssystemen umgehen, sind aber nicht von Natur aus unauffindbar. Das Verhalten eines Spielers, der einen solchen Cheat verwendet, wird sich stark von dem eines Spielers unterscheiden, der das Spiel sauber spielt – und dieser Unterschied kann zur Erkennung des Cheats genutzt werden. Es kann auch nicht-behaviorale Methoden geben, um solche Cheats zu erkennen, aber das hängt ganz von der Implementierung des Cheats und der spezifischen Plattform ab, auf die der Cheat abzielt.«

Erster Vorstoß gescheitert

User Vision Pro sorgte weit über einschlägige Szenekreise hinaus für Aufsehen: Der Entwickler des Cheats, im Internet bekannt unter dem Pseudonym »USER101«, hatte mit einem Video den Release von User Vision Pro angekündigt. Auch eine entsprechende Website war bereits in Stellung gebracht, einem Vertrieb des KI-Cheats stand also fast nichts mehr im Weg. Der Entwickler versprach Unentdeckbarkeit, die Einsatzmöglichkeit auf allen Plattformen und in allen Spielen. Komplette Unabhängigkeit also, um in jedem Spiel cheaten zu können!

Der Traum ist aber vorerst geplatzt: Bevor sich das Tool in der Praxis beweisen konnte, trat CoD-Warzone-Publisher Activision auf den Plan. Im Video ist immerhin Gameplay von Call of Duty: Cold War zu sehen, der Gedankenschritt zum arg von Cheatern gebeutelten CoD: Warzone war also nicht weit. Activision ließ die Werbevideos für den Cheat auf YouTube entfernen, was wegen des Strike-Systems für Rechteinhaber gezeigter Spiele eine Sache von Minuten ist. Aber das

Valorant nutzt eine Anti-Cheat-Software namens Vanguard, die durch ihren Kernel-Zugang auch andere, nicht verdächtige Software blocken kann.

Wallhack und Aimbot in Aktion – so wird das Siegen leicht gemacht. (Bild: Kaspersky)

war nicht alles: Auch kontaktierten offenbar Anwälte von Activision den Cheat-Entwickler, woraufhin dieser schnell reagierte und die Entwicklung von User Vision Pro laut eigenen Angaben komplett einstellte.

Er wollte nur spielen

Zudem veröffentlichte die Person auf der Website eine Stellungnahme und beteuerte, »keine illegalen Absichten« gehabt zu haben. Inzwischen ist die Website nicht mehr zu erreichen. Das Statement konnten die Kollegen von Eurogamer allerdings festhalten: »Diese Erklärung war nicht erforderlich. Auf Wunsch von Activision Publishing, Inc. (›Activision‹) werde ich jedoch keine Software mehr entwickeln oder zur Verfügung stellen, die zur Ausnutzung ihrer Spiele verwendet werden könnte. Es war nie meine Absicht, etwas Illegales zu tun. Am Ende des Videos, das so viel Aufmerksamkeit auf dieses Projekt lenkte, hieß es ›kommt bald‹. Die Software wurde nie veröffentlicht. Diese Art von Technologie hat auch andere Vorteile, zum Beispiel könnte man mit einer Webcam, die man auf sich selbst richtet, Bewegungen ohne den Einsatz von Gliedmaßen steuern. Leider werde ich sie wegen ihrer möglichen negativen Auswirkungen nicht weiterentwickeln.«

Ein Durchbruch?

Was sich wie eine gute Nachricht für ehrliche Spieler liest, hinterlässt einen Beigeschmack. Einen minzigen, denn man kriegt die sprichwörtliche Zahnpasta bekanntlich nicht zurück in die Tube. Vermutlich ist es nur eine Frage der Zeit, bis ein inspirierter Entwickler die Scherben aufsammelt und versucht, eine neue Cheat-Vase zusammenzukitten, um in der bunten Bildersprache zu bleiben. Wie gut sich die dann aber ins Cheater-Feng-Shui einfügt, wird von Cheat- und Anti-Cheat-Entwicklern gleichermaßen in Frage gestellt. Einer der Hacker, den wir hier mit dem Pseudonym »Niedrigfrittiert« ansprechen, sieht die Einsatzgebiete für Cheats wie Userviz sehr eingeschränkt: »Machine Learning ist hauptsächlich für Anwendungen gedacht, bei welchen man die Daten nicht in ›Rohform‹ hat. Auf einem PC gibt es jedoch zig Möglichkeiten, an diese relevanten Daten zu kommen. Auf einem geschlossenen System wie einer Spielekonsole ist das dagegen schwieriger.«

Deshalb könnten Konsolen einen Markt für moderne Cheats wie Userviz darstellen. Da die Geräte von Natur aus sicherer sind als PCs, haben es Cheat-Entwickler dort schwerer, zuverlässige Cheat-Software zu entwickeln. Ähnlich sieht das »Toothless«, eine Moderatorin in einem großen Cheat-Forum, die »hunderte Cheats reverse engineert« hat, um Nutzer vor Malware und Viren zu schützen: »An sich finde ich das Konzept sehr interessant. Jedoch bin ich skeptisch, da die meisten Machine Learning Cheats, die ich bisher live gesehen habe, eher mäßig zuverlässig waren. Im Vergleich zum PC sind Konsolen aber um einiges schwieriger zu ›hacken‹, da sie meistens nicht dokumentiert und stark spezialisiert sind. Hinzu kommen eingebaute Schutzmechanismen gegen Cracking/Jailbreaking, die Cheaten auf der vom PC bekannten Memory-Ebene sehr viel schwerer machen.«

KI kann nicht alles

Auch Anti-Cheat-Experte Paul Chamberlain sieht auf dem PC, zumindest in naher Zukunft, keine große Gefahr durch KI-Cheats: »Ein maschinelles Bildverarbeitungssystem kann zum Beispiel keinen Wallhack erstellen oder Fehler in der Spiellogik ausnutzen. Die Leistung dieser KI-Cheats ist im Allgemeinen schlechter als die herkömmlicher Cheats, da die Bildverarbeitung im Vergleich zu Methoden, die den Speicher des Spiels direkt auslesen, weniger Kontext hat. Solche Cheats könnten eine Nische in sehr gut geschützten Spielen oder auf Plattformen finden, auf denen es ansonsten schwierig ist, willkürliche Software auszuführen (Telefone, Konsolen). Aber sie werden den Markt auf dem PC wahrscheinlich nicht dominieren, bis die Leistung dieser Technik mit traditionellen Techniken gleichgezogen hat.«

Cheat-Entwickler Niedrigfrittiert sieht wirklich sinnvolle Anwendungsbereiche von Machine Learning, abseits des mit Userviz vorgestellten Aim- und Triggerbots, eigentlich nur in zwei Bereichen:

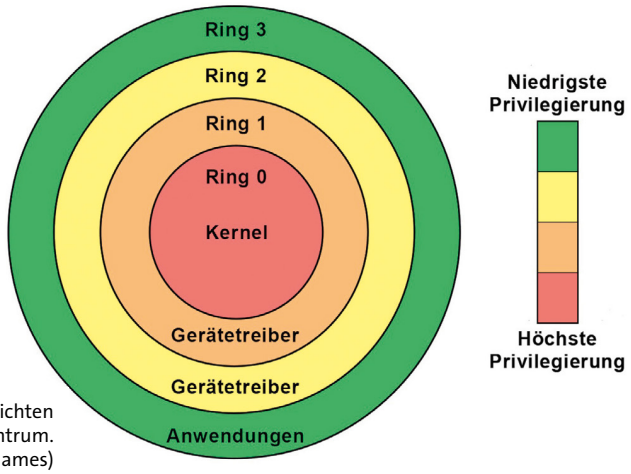
1. Sound parsing: Wenn man komplett extern bleiben möchte (keine Software auf dem Gerät ausführen, wo das Spiel läuft), um die ungefähre Position eines Gegners beispielsweise hinter einer Wand auf Basis von Sounds zu bestimmen (Schritte/Schüsse/Munitionieren emittieren alle einen Sound) – quasi cheaten per Ohr.

2. Heatmap-Analyse aus Sicht von Trainern in E-Sport-Shootern (etwa CS:GO): Ein Gegner wird auf A gespottet, bleibt für 20 Sekunden verschwunden und emittiert keine Informationen über seine Position. Zu welcher Position hat er sich in diesen 20 Sekunden womöglich bewegt, wenn

Cheats sind so alt wie das Hobby Computerspiele selbst, schon für The Last Ninja 2 auf dem C64 gab es jede Menge Tricks.

WAS IST DER KERNEL?

Ein Kernel, oder auch Kern, ist der zentrale Bestandteil eines jeden Betriebssystems. Er bildet die unterste Schicht von Windows, MacOS und Co. und hat somit direkten Zugriff auf die Hardware. In der Hierarchie eines Systems folgen auf den Kernel zunächst die wichtigsten Gerätetreiber, ehe Software und damit auch Spiele zum Zuge kommen. Letztere sind mit den geringsten Zugriffsprivilegien ausgestattet, wie die Grafik noch einmal verdeutlicht. Hat eine Cheat-Software Zugriff auf den Systemkern, kann sie meist ohne große Hindernisse Daten aus dem Speicher via DMA (Direct Memory Access, Speicherdirektzugriff) auslesen und sogar verändern. Der Clou dabei: Spiele und deren Schutzvorkehrungen haben diese Möglichkeit in der Regel nicht und sind dadurch im Nachteil.



Ein Betriebssystem ist in mehreren Zugriffsschichten aufgebaut – der Kernel steht dabei im Zentrum. (Bild: Riot Games)

man die anderen Parameter wie Money Management, Waffe, Anzahl der Spieler, Bias des einzelnen Spielers kennt?

Allerdings erklärt der Cheat-Entwickler, selbst in absehbarer Zukunft keine Cheats mit Machine Learning entwickeln zu wollen: »Es ist keine ›Silberkugel‹ für all unsere Probleme und hat ganz klare Limitierungen (Latenz, Ungenauigkeit) und Nachteile (sieht nur das, was der Mensch sieht).«

Auch Crotle, einen Entwickler bei einem großen, international tätigen Cheat-Anbieter, fragten wir, ob Machine Learning für sein Unternehmen eine Rolle spielt. Obgleich der Anbieter während der Corona-Pandemie stark gewachsen sei, denke man derzeit nicht viel über KI-Cheats nach, hieß es. Zumindest hält sich der Entwickler die Option für die Zukunft offen: »Auf ganz lange Sicht vielleicht, zur jetzigen Zeit ergibt es aber noch keinen Sinn. Unsere aktuellen Tools sind funktional vielseitig genug.«

KI-Cheats vs. Kernel-Anti-Cheat

Indes bleiben künftig wohl die Anti-Cheat-Entwickler nicht bei traditionellen Methoden, um Betrüger in Online-Spielen zu überführen. Ein Patent von Microsoft zeigte bereits 2018, dass Machine Learning in Anti-Cheat-Software eine Rolle spielen kann.

Ein Thema, das konventionelle Anti-Cheat-Methoden bei Spielern häufig in ein schlechtes Licht rückt, sind Programme, die auf Kernel-Ebene operieren – also ganz tief im Betriebssystem des PCs. Schließlich lässt sich kein Nutzer gern von irgendeinem Programm so einfach im Betriebssystem herumpfuschen. Experten sind allerdings der Meinung, dass nichts so effektiv gegen Cheater wirke wie ein Kernel-Anti-Cheat. Laut Paul Chamberlain kann diese Herangehensweise auch helfen, mögliche KI-Cheats zu erkennen: »Kernel-Anti-Cheat-Systeme sind ein wichtiges Instrument zur Überprüfung der Integrität der Umgebung, in der das Spiel läuft. Sie können Anti-Cheat-Teams zusätzliche Optionen zur Verhinderung und Erkennung von Cheats bieten. Für die Erkennung von Betrügereien im Stil der maschinellen Bildverarbeitung/Eingabe-Injektion sind sie hilfreich, aber nur ein Teil des Puzzles. Eine Vielzahl anderer Techniken wird wahrscheinlich in Verbindung mit Kernel-Komponenten eingesetzt werden.«

Bereits bei traditionellen Cheats erweist sich Kernel-Technik aktuell als stärkste Waffe der Anti-Cheat-Entwickler. Durch den Zutritt zur Kernel-Ebene des Betriebssystems begeben sich diese Programme praktisch auf Augenhöhe mit den Cheats, die häufig ebenfalls dort operieren.

Des Cheaters Kernel

Neben dem kontrovers diskutierten Vanguard-System von Valorant setzen auch die

Obwohl Starcraft 2 eindeutig auf Mehrspielerpartien ausgelegt ist, gibt es für den Solomodus Cheats von Blizzard.

So sieht es in CS:GO aus, wenn sich ein Spieler per Wallhack Vorteile verschafft, Valve schwingt regelmäßig den Bannhammer.

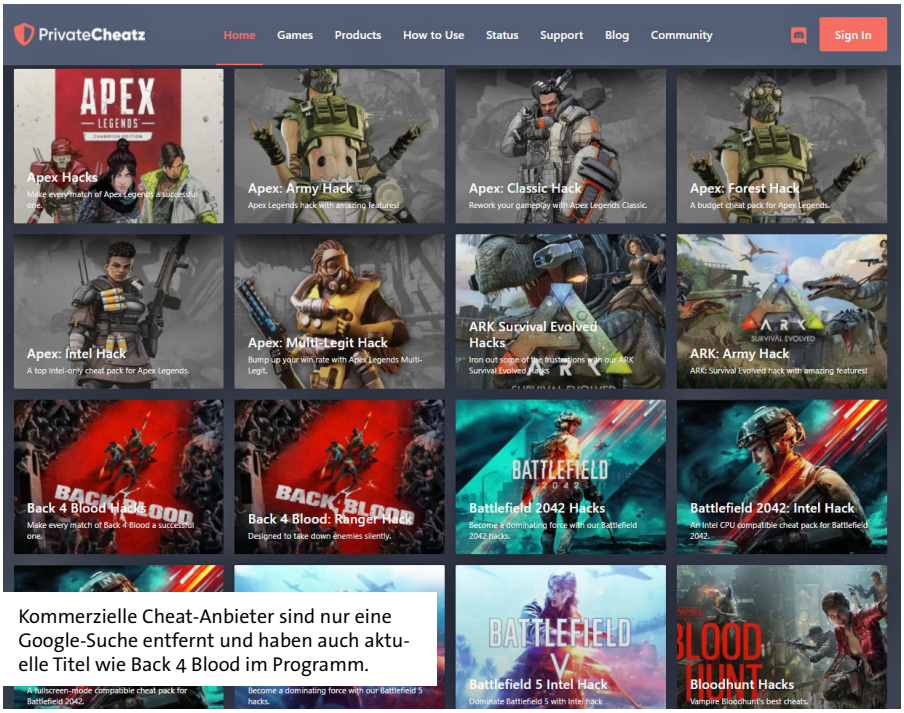
bekannten Tools Easy Anti-Cheat und BattlEye auf Kernel-Zugriff. Dennoch kann die Leistung ein und desselben Programms von Spiel zu Spiel stark variieren, was laut Cheat-Forummoderatorin Toothless nicht mit der Potenz des Programms, sondern mit den Entwicklern des jeweiligen Spiels zusammenhängt: »Viele Spiele haben zwar ›fancy‹ Kernel-Anti-Cheats, aber sie nutzen die Möglichkeiten nicht aus. Beispielsweise hat Apex Legends zwar Easy Anti-Cheat, jedoch ist es hier sehr lasch konfiguriert, und Cheater haben es leicht. Rust benutzt ebenfalls EAC, jedoch um einiges aggressiver konfiguriert und besser integriert. Hier ist es deutlich schwieriger, langfristig unerkannt zu bleiben. Solange es einfach bleibt, die Anti-Cheats zu umgehen, besteht einfach kein großer Bedarf für Machine Learning Cheats (zumindest auf dem PC).«

Der Knackpunkt besteht laut einem Brancheninsider, der anonym bleiben möchte, weniger darin, welche Anti-Cheat-Technik zum Einsatz kommt, sondern vielmehr darin, wie spezialisiert und motiviert die Teams bei den Spieleentwicklern sind, langfristig mit den Cheat-Entwicklern Schritt zu halten. Denn der Kampf gegen Cheater endet nicht mit der Integration eines Anti-Cheat-Programms, sondern fängt da erst an. Cheat-Entwickler Crotle ergänzt: »Es kommt wirklich darauf an, wie viel Mühe sich die Spieleentwickler geben, welche Engine oder welches Anti-Cheat-Tool benutzt wird. Usermode-Anti-Cheats wie von Call of Duty oder Battlefield sind mit Kernel-Mode-Cheats relativ gut zu kontern. Außerdem spielt es eine Rolle, ob man als Cheat-Provider im Fadenkreuz steht oder ›unter dem Radar‹ fliegt. Das liegt prinzipiell erstmal an der Größe des Providers oder wie extrovertiert er auf Social Media aktiv ist.«

Was Cheater denken

Was halten eigentlich Cheat-Nutzer von KI-Cheats? Wir haben mit mehreren früheren Cheatern gesprochen, um ein Stimmungsbild zu zeichnen. Unsere Interviewpartner zeigen sich durchaus interessiert an Machine Learning, es gibt aber auch kritische Kommentare. Der ehemalige Cheat-Nutzer »Marcel« etwa meint: »Ich finde das Thema KI-Cheats sehr interessant und verfolge dies auch (obwohl ich selbst nicht mehr cheate). Ich bin der Meinung, dass über die Zeit immer mehr Projekte, die das Thema ›Machine Learning‹ behandeln, aufkommen werden. Jedoch denke ich, dass KI-Cheats die ›klassischen‹ Cheats nicht ablösen werden. Im Endeffekt sind auch KI-Cheats erkennbar. [...] Es wird immer ein Katz-und-Maus-Spiel zwischen Cheat-Entwickler und Spieleentwickler bleiben. Es werden immer wieder neue Lücken entstehen und ausgenutzt werden, welche es dann zu schließen gilt.«

Auch »V-Ice« hat dem Cheating inzwischen abgeschworen, beobachtet die Entwicklungen zu Cheats und Machine Learning heute allerdings mit Sorge: »Ich war wirklich



Kommerzielle Cheat-Anbieter sind nur eine Google-Suche entfernt und haben auch aktuelle Titel wie Back 4 Blood im Programm.

fasziniert von dieser Technologie und wie daraus Userviz entstand. Ich sehe es aber auch als Gefahr, da dies eine neue Generation an Hacks hervorbringen könnte, die Entwickler noch mehr unter Druck setzt. Der Kampf gegen Hacker ist jetzt schon hart, und ich denke, sowas könnte noch eine riesige Herausforderung werden. Wenn solche KI-Cheats erst ausgereift sind, werden sie vermutlich die erste Wahl sein.«

Keine schwarzweiße Zukunft

Wo heutzutage der Begriff KI fällt, schwingt immer ein Bild des Terminators und von Skynet mit, das Überlegenheit, Unbesiegbarkeit und potenzielle Gefahr suggeriert. Kein Wunder, dass ehrliche Spieler mit Sorgen in Richtung KI-Cheats wie User Vision Pro blicken. Glaubt man aber den Profis, wird Machine Learning auf dem PC in Zukunft keine dominierende Rolle einnehmen, sondern sich eher in die bereits bestehenden Cheat-Systeme einreihen. Vielleicht entsteht aber ein Markt auf Konsolen oder Smartphones, die von Haus aus besser vor konventionellen Cheats geschützt sind. Oder aber Machine Learning vervollständigt und verbessert lediglich eine klassische Cheat-Technik, wie es bereits jetzt gelegentlich vorkommt. Von einer virtuellen Dystopie, in der die Cheater gewonnen haben und die Anti-Cheat-Entwickler weinend in der Ecke sitzen, sind wir aber vermutlich noch weit entfernt.

Dennoch bleibt eine Schlussfolgerung, die viele beunruhigen dürfte: Experten sehen Anti-Cheat-Technik auf dem Kernel-Level als wirksamste Maßnahme zur Erkennung und Bekämpfung von Schummel-Software. Je versierter die Cheats – auch dank KI – in Zukunft werden, desto schwerere Geschütze müssen Anti-Cheat-Entwickler auffahren, um Schritt zu halten. Das Wettrüsten wird wohl nie enden, was angesichts der brisanten Implikationen schon fast wie eine gute Nachricht klingt. Alle Personen, die wir hierzu befragt haben, sind sich einig, dass Machine Learning nur ein weiteres Stück im Cheat-Gesamtbild darstelle, das die Technik zwar verbessern, aber nicht revolutionieren werde. Hoffen wir, dass sie Recht behalten. ★

Wer in GTA 3 gern schlechtes Wetter hat, gibt den Rockstar-Cheat »ILOVESCOTLAND« ein.