Dompnier Silvio
Vitry Benjamin

Rapport Info 001 : Cryptographie

La triche et les anti triche dans les jeux vidéos

Sommaire

Préface

Nous le savons tous, aujourd'hui le monde du jeu vidéo prend de plus en plus de place dans notre monde et pas seulement au niveau "loisir", mais dans bien d'autres domaines. Plusieurs milliers de jeux sortent par an, sur différentes plateformes (console, mobile, PC, ...) et tous avec des thématiques et des mécaniques différentes. Certains racontent une histoire, d'autres permettent de créer notre propre histoire, tout seul ou avec nos amis et enfin d'autres permettent de jouer contre des joueurs du monde entier.

Ces derniers se font appeler "des jeux compétitifs". Ils ont pour but de mettre à niveau nos réflexes, nos connaissances du jeu et de ses mécaniques, notre esprit d'équipe et aussi notre mental. Ces jeux compétitifs sont devenus le principal marché du monde du jeu vidéo, que ce soit en termes de quantité ou de budget. Ce sont eux qui font rester le plus longtemps les joueurs, car ils permettent de jouer avec nos amis ou avec des inconnus si l'envie nous prend, mais aussi de se mesurer à eux. Comme dans tous les sports, la compétition nous retient et pousse à continuer pour devenir de plus en plus forts.

Mais aujourd'hui, le monde du jeu vidéo ne s'arrête pas à acheter le jeu et à y jouer seul ou en groupe. Ce monde s'est développé dans de nombreux domaines, comme la vidéo, où les joueurs enregistrent leurs parties pour les mettre en ligne, telles quelles ou montées pour ne montrer que les meilleurs moments, sur des plateformes de partage comme YouTube, pour que d'autres puissent les regarder, en parler et faire connaître l'auteur. Mais aussi en se filmant en direct, comme sur la plateforme Twitch, pour être regardé comme une émission de télé. Et enfin, dans le domaine de la compétition. Appelé l'ESport, les meilleurs joueurs des plus grands jeux s'affrontent et se mesurent pour savoir quel joueur ou quelle équipe est la meilleure de sa saison. Et cela, à la manière du sport d'aujourd'hui, dans des stades devant des milliers de personnes et retranscrit aussi en direct à la télé ou sur internet.

Et bien sûr, tous ces domaines rapportent beaucoup d'argent, non seulement aux développeurs et éditeurs des jeux, mais aussi à toutes les plateformes qui hébergent le contenu (Youtube, Twitch, ...), aux joueurs professionnels qui remportent des tournois, et enfin au simple joueur dans sa chambre qui joue avec ses amis et qui décide de montrer son niveau aux autres joueurs en se filmant.

Sauf que, comme dans tous les domaines de la compétition, il y a des joueurs plus forts que d'autres et certains n'arrivent jamais à monter bien haut même avec beaucoup de temps de jeu. Du coup, certains joueurs vont tricher pour grimper plus facilement et le monde du jeu vidéo n’y a pas échappé mais ces méthodes sont bien différentes.

Le jeux vidéo et la triche

Pourquoi tricher

En raison du développement rapide des jeux vidéo et de leur démocratisation, la triche est devenue un problème majeur qui nécessite des ressources considérables pour garantir un espace de jeu équitable, amusant et engageant pour tous. En effet, l'expansion rapide du domaine a d'un côté permis sa démocratisation, augmentant grandement le nombre de tricheurs potentiels, mais aussi sa professionnalisation, ajoutant un intérêt financier important à la triche.

Les différents acteurs impliqués dans la triche sont pour la plupart des joueurs lambda désireux d'obtenir des avantages. Cependant, certains jouissent d'une notoriété plus importante et utilisent tous les moyens possibles pour conserver cette notoriété ou pour se faire un nom plus rapidement. D'autres, moins scrupuleux, trichent lors de compétitions pour gagner des prix, de la gloire et des récompenses sous le feu des projecteurs.

Les tricheurs sont nombreux et prêts à payer le prix fort pour leurs avantages. Par exemple, on estime que plus de 40% des joueurs de jeux de tir sont prêts à tricher. En extrapolant cette statistique au jeu "Call of Duty: Warzone", qui compte plus de 100 millions de joueurs, on obtient un nombre important de 40 millions de tricheurs potentiels. Si un développeur facture ses services à 10€ par tricheur, cela représente la somme de 400 millions d'euros pour le marché d'un seul jeu à succès.

“Si tricher est plus difficile que jouer, alors les gens ne trichent pas”, mais les développeurs ont beaucoup moins de ressources, notamment financières, pour rendre la triche difficile. En effet, les jeux ont tendance à avoir des budgets ne dépassant pas les 100 millions de dollars, sauf exceptions très rares, pour l’exemple de "Call of Duty: Warzone" cela donnerait un facteur 4 entre le budget total de développement, qui n’est alloué qu’en faible partie à la lutte contre la triche, et le potentiel marché de la triche pour le jeu.

Comment trichent-ils ?

On peut classer les triches en trois catégories en fonction de la propriété du jeu qu'elles attaquent : la confidentialité, l'intégrité et l'accessibilité. Ces propriétés peuvent être définies comme suit :

1. Confidentialité : les tricheurs potentiels ne doivent avoir accès qu'aux informations qui leur sont destinées, afin qu'ils ne soient pas avantagés en prenant en compte ces informations pour prendre des décisions.
2. Intégrité : les tricheurs potentiels ne doivent pas être en mesure de modifier l'état du jeu d'une manière qui leur donnerait un avantage.
3. Accessibilité : les tricheurs potentiels ne doivent pas empêcher d'autres joueurs d'accéder à tout ou partie du jeu.

Cette classification a l’avantage d’être simple, mais ne permet pas d'aller grandement en détail.

En se penchant plutôt sur le niveau où arrive la triche que sur la cible de la triche, cela nous permet d'établir une classification plus technique des triches que l'on peut rencontrer. On identifie quatre niveaux :

1. niveau du jeu : ce type de triche ne requiert aucun outil ou logiciel extérieur, et se déroule intégralement au sein du jeu.
2. niveau application : ce type de triche se passe au niveau logiciel. Il consiste à modifier les exécutables ou données du jeu ou a utilisé un logiciel tierce pour lire et/ou écrire dans la mémoire utilisée par le jeu au cours de l'utilisation.
3. niveau protocole : ce type de triche consiste à interférer avec les protocoles de communication du jeu. Le but est d'altérer les paquets transmis et envoyés, soit en insérant, supprimant, ou modifiant des paquets.
4. niveau infrastructure : ce type de triche requiert la modification de l'infrastructure, logicielle ou matérielle, que le jeux utilise (réseaux, drivers, etc)

Au sein de chacun de ces niveaux on discerne ensuite différents types de triche. L'avantage de cette classification est qu'elle peut être facilement étendue si de nouvelles façons de tricher apparaissent.

Triche au niveau du jeu

On discerne principalement deux types de triche au sein de cette catégorie, l'utilisation de bugs et les RMT (Real Money Transaction ou Transaction d'Argent Réel en français). On classe aussi dans cette catégorie la connivence (collusion), où des tricheurs qui ne sont pas supposés travailler ensemble allient leurs efforts.

Utilisation de bugs

Les triches utilisant des bugs exploitent les erreurs de conception ou d'implémentation pour obtenir un avantage au sein du jeu. Les bugs ne nécessitent pas une connaissance approfondie de la façon et des raisons pour lesquelles ils fonctionnent, et ne nécessitent pas l'utilisation de programmes ou de modifications supplémentaires.

Par exemple, le système de classement des joueurs dans Warcraft II contenait une erreur de conception qui a permis aux joueurs de s'organiser pour grimper dans le classement sans jouer de matchs valables. Le principe était comme suit : des joueurs qui collaborent commencent à plusieurs reprises des matchs les uns contre les autres, puis se rendent alternativement pour donner à chacun des points de victoire sans effort et monter dans le classement. Ce concept s'appelle le commerce de victoires (win trading). Dans Warcraft III, le commerce de victoires est empêché en choisissant les participants de façon aléatoire lors de la création de matchs. Cependant, cela ne fonctionne que si le groupe de joueurs est grand.

RMT

Les triches utilisant des RMT utilisent des mécaniques d'échange d'objets ou de monnaie virtuels en place au sein du jeu. Le principe est d'acheter avec de l'argent réel des services, des objets ou autres éléments du jeu à d'autres joueurs afin d'obtenir un avantage que l'on aurait pas pu obtenir autrement.

Souvent ce genre de triche est organisé par des vendeurs, comme dans le cas de World Of Warcraft, le célèbre MMORPG (Massively Multiplayer Online Role Playing Game, ou Jeu de Rôle Massivement Multijoueur en Ligne en français) de la société Blizzard entertainment, où des joueurs chinois s'organisent en groupe pour obtenir des objets rares et les vendre au prix fort à d'autres. Ce genre de transaction est souvent strictement interdite par les termes de services des jeux, notamment car il peut y avoir concurrence entre ces vendeurs, et les systèmes mis en place par les développeurs, tels que des systèmes de micro transactions ou interférer avec le système de progression normal du jeu.

Connivence
Les triches de connivence impliquent que plusieurs tricheurs travaillent ensemble pour obtenir un avantage alors qu'ils ne sont pas censés travailler ensemble. Ce type de triche implique souvent des communications supposément interdites entre les tricheurs.

On retrouve ces cas de triche régulièrement dans des jeux multi joueurs sans équipe où des joueurs vont s'allier en dépit des règles.

Triche au niveau applicatif

La triche au niveau applicatif consiste à modifier les exécutables ou les données du jeu lors de son utilisation, ou d'utiliser des programmes et outils tierces pour le faire. Ce type de triche requiert souvent des connaissances techniques importantes pour les développer, mais les utiliser est souvent trivial. La triche au niveau applicatif se sépare en trois grands types de triche. L'exposition d'information (information exposure), la génération d'entrées utilisateurs (user input generation) et l'utilisation de commandes invalides (invalid commands).

L'exposition d'informations
L'exposition d'information consiste à accéder à des informations auxquels le tricheur n'est pas supposé accéder. Ce type de triche est possible dans beaucoup de cas car les développeurs supposent souvent que le client du jeu ne révélera pas les informations qu'il n'est pas supposé révéler. Les informations sont acquises en modifiant le client, ou en exécutant un autre programme qui les extrait de la mémoire. L'exposition d'information peut aussi arriver au niveau infrastructure à l'aide d'autres méthodes.

Un des exemples les plus courants sont les "wallhack" (piratage de murs) au sein des jeux de tirs, où le tricheur révèle la position des autres joueurs à travers les murs.

Génération d'entrées utilisateur
La génération d'entrées utilisateur consiste à utiliser des modifications au client du jeu ou un logiciel tierce pour créer des entrées utilisateurs en lieu et place du tricheur afin de gagner un avantage. Ce type de triche se scinde globalement en deux sous catégories, les bots et les augmentateurs de réflexes (reflex enhancers).

Le but des bots est de jouer à la place du tricheur, souvent pour permettre la progression sans jouer au jeu. On peut citer par exemple la famille de bots "kkwut" sur le jeu "Yu Gi Oh! : Master Duel" de Konami, qui jouent des duels à la place des tricheurs pour progresser au sein du système de battle pass saisonnier rapidement.

Les augmentateurs de réflexes sont similaires aux bots, mais ne contrôlent qu'une partie des actions du joueur dans le but d'améliorer ses performances. Les plus courants sont sur les jeux de tir comme Halflife, où les augmentateurs de réflexes permettent de viser automatiquement les adversaires avant de tirer.

Commandes invalides
Le but de ce genre de triche est de modifier le client du jeu pour lui faire envoyer des commandes qui ne seraient pas possible avec un client non modifié. Le tricheur va ensuite utiliser ces commandes pour effectuer des actions qui ne seraient pas possibles autrement, ou modifier les caractéristiques du jeu ou des personnages à son avantage, par exemple, augmenter la vitesse de son avatar.

Triche au niveau du protocole

La triche au niveau du protocole consiste à interférer avec les paquets envoyés et reçues par les protocoles de communication du jeu. Les tricheurs vont altérer les paquets en supprimant, modifiant ou dupliquant des paquets existants, ils peuvent aussi parfois insérer de nouveaux paquets. Les triches possibles au niveau du protocole sont nombreuses, on en compte huit : suppression de mise à jour (suppressed update), introduction de délai fixe (fixed delay), introduction d'inconsistance (inconsistency), falsification d'horodatage (timestamp), usurpation d'identité (spoofing), replay (replay), aveuglement (blind opponent), annulation (undo).

Suppression de mise à jour
Ce genre de triche exploite l'implémentation de "dead reckoning", un système permettant d'anticiper le contenu d'une communication en cas de perte ou de délai dans les communications. Cette technologie est utilisée dans les jeux en ligne pour permettre des mouvements fluides pour tous les joueurs en cas de problème réseau.

Le "dead reckoning" permet d'anticiper un nombre n de paquets avant qu'un joueur soit déconnecté, mais si un tricheur venait à bloqué n-1 paquets sortant, les paquets qu'il doit envoyer pour permettre aux autres joueurs de voir ses actions par exemple, mais pas les paquets arrivant, les paquets qui lui permettent de voir les actions des autres joueurs par exemple, il pourra obtenir un avantage significatif.

Introduction de délai fixe
L'introduction de délai fixe consiste à introduire un délai de temps constant entre les paquets sortant. Cela permet à un tricheur de recevoir les mises à jour envoyées par ses adversaires rapidement, mais d'envoyer ses informations avec un délai important.

Ce type de triche est particulièrement efficace dans les jeux rapides, tels que les jeux de tir moderne, ou des jeux de sport, comme "Madden NFL Football" où ce type de triche a été découvert.

Introduction d’inconsistances
Ce type de triche consiste à envoyer des informations erronées aux autres joueurs, l’objectif est d’introduire des inconsistances dans les jeux des autres joueurs, ce qui pourrait causer leur partie de se retrouver dans un état corrompu et ainsi les faire quitter le jeu.

Falsification d’horodatage
La falsification d’horodatage consiste à envoyer des paquets dont l’horodatage a été mis dans le passé, avant les horodatages des autres joueurs. Cela permet au tricheur d’effectuer des actions avant les autres joueurs, en sachant ce qu’ils ont fait.

Usurpation d’identité
L’usurpation d’identité est réminiscente des problèmes de sécurité plus classique où un attaquant va tenter de se faire passer pour sa cible. Ici, un tricheur peut tenter de se faire passer pour un joueur autre, et envoyer des commandes en son nom.

Il pourrait par exemple lui faire lâcher ses objets afin de le désavantager.

Replay
Le but du replay est de faire refaire un adversaire des actions qu’il a déjà commis. Pour se faire, le tricheur va renvoyer des paquets qu’il a reçu d’autres joueurs en leur nom.

Aveuglement
L’aveuglement consiste pour le tricheur à abandonner les mises à jour de ses adversaires, tout en continuant d'accepter les leurs. Cela n’est possible que si le tricheur est l'hôte de la partie. Cette manipulation permet au tricheur de voir ce que font les adversaires, sans que eux ne peuvent voir ce que font les autres.

Annulation
De nombreux jeux ont mis en place des systèmes “commit/reveal” pour empêcher nombre de ces triches impliquant les protocoles de communication. Cependant, si l’étape de révélation n’est pas forcée, un tricheur peut décider d’attendre que les communications de ses adversaires, puis décider ou non de révéler ses actions. S'il ne révèle pas ses actions, il les annule.

Triche au niveau de l’infrastructure

La triche au niveau infrastructure implique de modifier ou d’interférer avec l'infrastructure, logicielle ou matérielle, que le jeu utilise. Cela peut être des drivers ou du matériel par exemple. On dénombre deux types de triche sur infrastructure principaux : l’exposition d’information, et l'augmentateur de réflexe par proxy.

Exposition d’information
Il est possible d’observer l’infrastructure utilisée par le jeu pour obtenir des informations supplémentaires. Une façon classique de le faire est d’utiliser un hôte différent qui va observer le trafic dirigé vers celui du jeu pour en extraire ensuite les informations voulues. Un cas de ce genre de triche est le logiciel ShowEq qui permet d’écouter, identifier et analyser les paquets qui passent par la carte réseau pour le jeu Everquest.

Une autre façon d’exposé de l’information à travers la couche infrastructure est de modifier les drivers d’affichage pour que le monde de jeu soit dessiné de façon avantageuse, par exemple en rendant les murs invisibles.

Augmentateur de réflexes par proxy
Les augmentateurs de réflexes fonctionnent au niveau infrastructure en installant un proxy entre le client et le serveur pour modifier les paquets du client. Lorsque les paquets passent dans le proxy, il va analyser et améliorer les commandes envoyées par le client pour avantager le tricheur.

Le jeu Quake est un des premiers à avoir souffert de ce genre de pratique, des proxy améliorant la visée des tricheurs en insérant des commandes correctives de visée avant chaque commande de tir.

Les problèmes engendrés

Au premier abord, on pourrait penser que les éditeurs de jeux vidéo n'ont aucun intérêt à réagir face aux problèmes de triche, puisque les joueurs eux-mêmes sont les seuls à en souffrir. Cependant, la triche pose plusieurs problèmes pour les éditeurs et développeurs de jeux. En effet, un grand nombre de tricheurs peut ternir l'image du jeu, de la marque et des entreprises impliquées (éditeurs, studios de développement, etc.), et ainsi nuire à de futurs investissements ou projets.

De plus, si les joueurs ne peuvent pas profiter du jeu, ils seront moins enclins à rester, comme cela a été le cas pour le jeu "Destiny 2" qui a perdu plus de 50% de ses joueurs après une vague de triche massive soudaine. Cette perte de joueurs est particulièrement problématique aujourd'hui, avec l'avènement de l'ère du "jeu en tant que service", qui nécessite de retenir un grand nombre de joueurs afin qu'ils dépensent graduellement leur argent dans le jeu, notamment par le biais de microtransactions.

Ces deux facteurs combinés peuvent entraîner une importante perte d'attrait pour le jeu auprès de sponsors ou de partenaires potentiels, ainsi qu'un manque à gagner important pour l'éditeur et développeur du jeu.

La réponse des industriels

Suite au développement rapide de la triche et du nombre de tricheurs sur leurs jeux vidéo, de nombreux joueurs ont commencé à se plaindre car leur expérience de jeu devenait de plus en plus difficile. Perdre contre un bon joueur peut nous pousser à devenir plus forts pour espérer être à son niveau et pourquoi pas le battre la prochaine fois qu'on jouera contre lui, mais perdre contre un tricheur, sans avoir la moindre chance de rivaliser avec lui pendant les parties, dégoûte forcément les joueurs qui ne trichent pas, même s'ils ne jouent pas dans des parties spéciales pour la compétition.

Pour un joueur normal, il ne reste que deux solutions face à l'augmentation des tricheurs sur les jeux. Soit investir dans un logiciel de triche pour être au même niveau que ses adversaires les plus fréquents et recommencer à gagner des parties, même si cela se fait de façon différente. Soit quitter le jeu pour aller voir la concurrence ou découvrir de nouveaux types de jeu qui n'ont pas encore ce problème.

Heureusement, la plupart des joueurs choisissent la deuxième option. De ce fait, les développeurs de jeux vidéo ont commencé à voir leur nombre de joueurs actifs par jour diminuer de plus en plus, même après l'ajout de nouveau contenu. C'est ce qui est arrivé au mode multijoueur du jeu Destiny 2, qui, au bout de deux semaines à peine après sa sortie, a vu une vague colossale de tricheurs, et le reste des joueurs n'est pas resté plus longtemps.

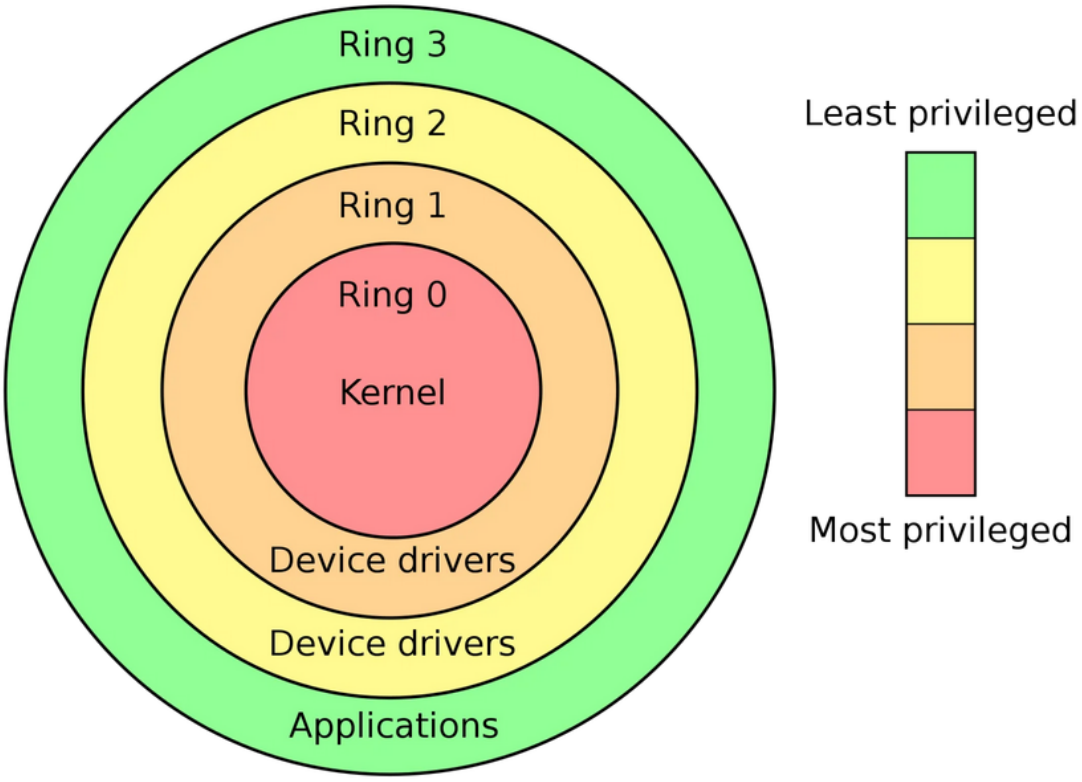
Pour régler ce problème, les développeurs ont dû commencer à apprendre et à comprendre comment les joueurs modifiaient le jeu ou développaient des logiciels de triche, mais surtout, ils ont dû déployer eux-mêmes des logiciels pour contrer les tricheurs.

Anti-cheat

Les anti-cheats sont des programmes informatiques conçus pour détecter et empêcher les joueurs de tricher dans les jeux vidéo en ligne. Leur fonctionnement peut varier en fonction du jeu et de l'anti-cheat utilisé, mais généralement, ils fonctionnent de la manière suivante :

1. Détection des tricheurs : Les anti-cheats surveillent en permanence le jeu pour détecter tout comportement suspect qui pourrait indiquer qu'un joueur triche. Cela peut inclure la détection de logiciels tiers qui altèrent le gameplay, les mouvements du joueur ou les résultats des actions dans le jeu.
2. Analyse des données du jeu : Les anti-cheats analysent les données du jeu en temps réel pour détecter les modèles de comportement inhabituels, tels que des taux de réussite anormaux ou des mouvements qui ne sont pas possibles sans tricher.
3. Rapport des violations : Si un joueur est détecté en train de tricher, l'anti-cheat peut enregistrer des informations sur le joueur et le signaler aux développeurs du jeu ou aux administrateurs de serveur pour prendre des mesures.

Pour aller un peu plus dans les détailles, il faut voir les niveau de privilège des logiciel sur un ordinateur, comme illustré ci-dessous:



Le ring 3 est le plus petit niveau de privilège. C'est ce à quoi les applications ont accès comme les fichiers, documents, … C'est aussi ce qu'un utilisateur lambda à accès.

Le ring 0 est le plus haut niveau de privilège. Ils ont accès à tout ce que peut voir le ring 3 mais aussi, la carte graphique, la mémoire, les périphériques, qui sont accessibles depuis le ring 1 et 2. Et de plus, il à accès au noyau du système lui-même.

Ce niveau de privilège est très important, car un logiciel en ring 3 n'a pas accès à ce qui se passe en ring 0 normalement. Ce qui veut dire qu'un anti-cheat en ring 3 ne pourra pas détecter un cheat qui se situe en ring 0. Et c'est là qu'arrive toute les subtilités de ce monde et cette guerre entre les cheat et les anti-cheat avec les joueurs et leur ordinateur au milieu.

Au commencement des anti-cheat (et encore aujourd'hui pour certain), ils étaient au niveau 3, pour analyser les fichiers client du joueur, l'utilisation de quelques logiciels et d'autres problèmes. Comme exemple de jeu qui à fait beaucoup parler de lui pour son nombre remarquable de tricheur, c'est Call of Duty et principalement son mode Warzone. Il y a encore aujourd'hui beaucoup trop de tricheurs et c'est pourquoi la communauté se demande s' il y a vraiment un anti-cheat. Mais le problème c'est qu'il y en a bien un mais qu'il est encore en ring 3.

Un moyen simple de le contourner, c'est de lancer le jeu sur votre compte principal de l'ordinateur et ensuite, de lancer le logiciel de triche sur un autre compte de l'ordinateur. L'anti-cheat n'ayant accès qu'aux données de l'utilisateur qui la lancé, donc l'utilisateur qui à lancé le jeu, il ne peut pas vérifier les logiciels lancés et les fichiers d'un autre utilisateur, même si c'est le même ordinateur.

En fin de compte, tous les anti-cheat développé pour du ring 3 sont presque inutile, même si ils sont très intelligent, certain font des analyses de mouvement des personnages ou utilise des “sommes de contrôle” pour vérifier en permanence les données utilisé, mais là encore, ce sont des contrôles beaucoup trop simple à contourner.

Le pire exemple d’anti-cheat sur les jeux vidéo reste encore celui de Battlefield et de CS-GO, car leur but était de faire de l’analyse heuristique en machine learning pour analyser le gameplay des joueurs. Cela à engendrer des problèmes de faux-positif, car si un joueur était juste très bon au jeu, il pouvait avoir des sanctions et ça ne bloquait absolument pas l’utilisation de logiciel tiers.
Par contre, il a beau être critiqué comme “pire anti-cheat”, ça reste le seul qui pouvait contrer l’utilisation de “macro”. C’est un système qui permet de prédéfinir l’utilisation de plusieurs touches à la suite ou les mouvements de la souris, tout ça condensé en une seule touche. Cela permet notamment de réduire le recul d’une arme sur les jeux de tir, ou d’avoir les mouvements parfaits qui sont censés être très durs à réaliser.

Pour la suite, nous n’allons pas parler des ring 1 et 2 car ils sont très rarement utilisés pour des systèmes de triche et encore moins pour les anti-cheat.

Par contre, pour le niveau ring 0, c’est là que nous allons trouver les meilleurs anti-cheat. Nous pouvons citer “Vanguard”, celui du jeu Valorant, ou encore Batteye et Easy anti-cheat, des anti cheat développés et commercialisés pour les développeurs qui n’ont pas les moyens technique de mettre en place leur propre anti-cheat. Ils ont tous la particularité d’être au niveau ring 0, ce qui veut dire qu'ils ont accès à tous les fichiers de l’ordinateur et tous les logiciels qui se lancent (ou presque). Certains, comme Vanguard, tournent en permanence sur l’ordinateur, que leur jeu soit lancé ou non, et dès le lancement du système. L’une des failles qu’il peut y avoir, ce serait de lancer le logiciel de triche avant l'anti cheat, pour qu’il ne soit pas détecté. Et c’est pour cela, que Vanguard ne permet de lancer son jeu que sur des ordinateurs “de confiance”, ça veut dire qu’il demande à être le premier logiciel à être lancé au démarrage.

Aujourd’hui, cela reste la meilleure solution pour contrer la multitude de triche sur les jeux vidéo. Cela ne veut pas dire que les anticheat au niveau ring 0 sont parfaits. Il existe encore des tricheurs sur ces jeux vidéo et des communautés de hackers pour développer de nouveaux logiciels pour contourner ces barrières, mais de moins en moins quand même. L’utilisation d’anti-cheat du niveau ring 0 reste quand même beaucoup plus efficace et ralenti le développement de nouveaux cheats.

Inconvénient du ring 0

Comme mentionné précédemment, les anti-cheats de ring 0 sont devenus beaucoup plus efficaces que les générations précédentes. Cependant, pour atteindre un tel niveau de sécurité, ces anti-cheats ne sont pas tout blancs et ont causé quelques problèmes et désaccords sur la toile après leur sortie.

Tout d'abord, un programme qui se lance en premier sur un ordinateur, et qui en plus scanne tous les fichiers et autres logiciels de l’ordinateur, suscite des préoccupations en matière de

confidentialité. Les joueurs de Valorant ont rapidement compris que ce nouvel anti-cheat avait accès à leur machine, même sans jouer. Bien que les joueurs qui ne s'intéressent pas à ce sujet et qui ne comprennent pas comment fonctionne cet anti-cheat puissent penser que le logiciel en profite pour faire autre chose, même ceux qui comprennent son utilité et sa nécessité de se lancer en permanence et tôt au démarrage d'un ordinateur ne peuvent pas mettre de côté le fait qu'il a accès à encore plus de choses que l'utilisateur lui-même. Bien que Riot Games, l'éditeur de Valorant et de son anti-cheat, ait répondu sur des forums que son anti-cheat ne volait pas de données et qu'il ne servait qu'à la vérification et au scan, ils ne peuvent pas nous donner son code, et nous sommes donc obligés de les croire sans plus d'explications.

Deuxièmement, les anti-cheats peuvent avoir un impact sur les performances du jeu. Étant donné que ces anti-cheats sont au cœur du système et tournent en permanence, certains joueurs se sont demandé s'il n'y avait pas d'impact sur les performances du jeu ou même de l'ordinateur. L'exemple le plus connu est celui du jeu Doom Eternal, qui en 2017 a sorti un tout nouveau anti-cheat en ring 0. Et dès ce moment, les joueurs ont constaté une forte baisse de FPS pendant leurs parties. Il n'a pas fallu beaucoup de temps pour faire le lien entre ce tout nouveau problème et la sortie du nouvel anti-cheat. Bien que les développeurs aient contesté le fait que l'anti-cheat soit lié à cette baisse de performance, nous pouvons quand même nous poser la question de l'impact de ces anti-cheats sur nos machines.

D’autres méthodes connues

Les développeurs ont bien compris l'importance des anti-cheat dans les jeux vidéo compétitifs s'ils veulent garder leur communauté et leur nombre de joueurs. Ainsi, nous nous retrouvons dans une guerre du plus malin ou du plus rapide. Aujourd'hui, les développeurs consacrent beaucoup de temps et d'argent à la lutte contre les cheaters et les hackers qui développent ces logiciels de cheat. Mais faire des logiciels d'anti-cheat n’est pas leur seule arme dans cette guerre.

La plupart implémentent des systèmes de pénalités. En effet, trouver un tricheur dans son jeu est une chose, mais l'empêcher de revenir ou de diffuser son cheat est différent et nécessaire. La plupart des jeux vidéo ont la même approche pour punir les tricheurs sur leur jeu, c’est-à-dire de bannir leur compte et de le supprimer pour qu'ils ne puissent plus jouer. C'est le même comportement que pour punir les joueurs qui ont un comportement inadapté dans leur jeu (chat abusif, anti-jeu, etc.). Cependant, cette méthode n'est plus efficace et en fait davantage peur au tricheur. Surtout pour les jeux free-to-play, où il suffit de créer un compte pour jouer au jeu (pas besoin de l’acheter). Même sur les jeux payants, ce système n'a jamais été concluant, car si les tricheurs payent environ 50 euros par semaine pour leur cheat, ils n'hésiteront pas à racheter le jeu pour continuer.

Cependant, certains éditeurs ont été plus imaginatifs dans leur pénalité, comme le ban IP, où non seulement le compte du joueur est interdit de jouer, mais aussi son ordinateur et sa connexion. Pour les serveurs coréens du jeu League of Legends de Riot Games, un numéro de sécurité sociale est requis pour créer un compte, ce qui signifie que si un utilisateur se fait bannir, il ne pourra pas créer un second compte, même avec une autre adresse mail.

Enfin, la sortie du célèbre jeu Fortnite en 2017 a beaucoup fait parler de lui sur l'aspect des pénalités en cas de triche. Le jeu a annoncé qu'il irait jusqu'aux procès s'il trouvait les coordonnées des tricheurs sur leur jeu. Et cela n'a pas manqué, quelques mois après sa sortie, ils ont lancé une série de procédures pénales contre certains tricheurs de manière très médiatisée pour convaincre leurs joueurs de ne pas utiliser de cheat sur leur jeu.

Il est parfois aussi utile de rendre l’accès au code plus difficile. En plus de développer des logiciels anti-cheat, certains éditeurs utilisent une méthode de hash pour rendre leur code sécurisé et illisible. Cela permet de ralentir les hackers dans leur compréhension du code. Ils peuvent également rajouter des lignes inutiles pour le rendre encore plus illisible et incompréhensible. Tout cela combiné avec des moyens de chiffrement des communications client-client ou client-serveur permet de lutter encore un peu plus contre les hackers, mais cela ne rend pas les anti-cheat parfaits. Cependant, ces moyens ont pour but de ralentir les hackers.

Malgré ces mesures, la principale source du problème reste les hackers, qui développent les cheats et les revendent sur les marchés aux joueurs. Les développeurs de jeux vidéo savent qu'ils sont nombreux, compétents et font preuve de beaucoup d'imagination pour contourner les systèmes. L'idée est venue de Valorant, à sa sortie, où ils ont proposé aux hackers un serveur spécial pour eux, où ils pourront s'amuser à trouver des failles dans leur système et pour chaque problème trouvé, ils recevaient une récompense. De ce fait, les développeurs

d'anti-cheat peuvent savoir plus précisément comment les cheats sont faits et quelles failles ils exploitent.

Certains développeurs ont aussi des idées plus originales. Nous ne pouvions pas oublier de citer la meilleure idée du jeu CS:GO. Pour rappel, CS:GO est un jeu de tir multijoueur qui utilise un anti-cheat de ring 3 (donc très inefficace de nos jours). Après une très grosse vague de tricheurs qui est apparue sur leur jeu et qui a fait fuir une grosse partie de leur communauté, les développeurs ont mis en place un système pour lutter contre les tricheurs. Ce système est un menu dans le jeu, accessible uniquement par les joueurs qui ont plus de 20 heures de jeu environ, et qui permet de regarder le point de vue d'un autre joueur qui a été signalé, pour juger par nous-mêmes si cet utilisateur est un tricheur ou non. Ce qui veut dire que ce sont les joueurs qui jugent et pénalisent les autres joueurs...

Sources

https://www.showeq.net/forums/forum.php

https://www.youtube.com/watch?v=_8Kx9S0Optw

https://espace.curtin.edu.au/bitstream/handle/20.500.11937/10134/20769_downloaded_stream_225.pdf?sequence=2&isAllowed=y

https://www.jeuxvideo.com/news/1234686/denuvo-l-anti-piratage-et-anti-cheat-incompris-decryptage-des-polemiques.htm

https://en.wikipedia.org/wiki/Cheating_in_online_games

https://www.reddit.com/r/GlobalOffensive/comments/47dv61/insights_from_an_ex_anticheat_developer_on_the/

https://www.gamesindustry.biz/the-art-of-fair-play-developing-the-best-systems-to-deal-with-players-who-cheat

https://www.engadget.com/valorant-vanguard-riot-games-security-interview-video-170025435.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFgOsh8GETuBh9jD_MUqg-j2zQDr98xj8Hx_KsDyFXkzlFeEZnQSocUaFVG_WbYtiEmzGPIAWM1x38j8n7N2ijbsOx_KAQqr1ZDTEIX0B0sDogTV5o0GfQe9VoVfVPpyx3kv1biWfIABCxREcQHH8Nt-o5Z71fo7lh9umdlUDUgq