ISSN: 2675-1828

ARTIGO

Software anti-cheat: Uma maneira de prevenir trapaças em jogos multiplayer

Anti-cheat software: A way to prevent cheating in multiplayer games

Augusto Luciano Vicentine [1]
Gabriela Cristina Mendes da Silva [2]
João Pedro Domingues Guedes do Nascimento [3]
João Emmanuel D Alkmin Neves [4]

Resumo: *O presente artigo é uma revisão bibliográfica, que tem como intuito informar sobre segurança em jogos multiplayer, relatando sobre cheats e softwares de trapaças que concedem vantagens aos adversários, uns dos maiores problemas que os usuários de jogos online enfrentam, e os softwares anti-cheats que tem como finalidade detectar trapaças em jogos online com múltiplos jogadores. Nesse contexto, o artigo explora as vantagens e desvantagens causadas por esses softwares e o estudo acerca de um anti-cheat criado para um jogo online que que vem provocando danos a alguns de seus usuários.*

Palavras-Chave: *anti-cheat; cheat; segurança.*

Abstract. *This article is a bibliographic review, which aims to inform about security in multiplayer games, reporting on cheats and cheating software that provide advantages to opponents, one of the biggest problems that users of online games face, and anti-cheat software, which aims to detect cheats in multiplayer online games. In this context, the article explores the advantages and disadvantages caused by these software and the study about an anti-cheat created for an online game that has been causing damage to some of its users.*

Keywords: *anti-cheat; cheat; security.*

1. Introdução

O mundo dos jogos *multiplayer* é famoso por suas competições online, porém dentro desses jogos existem os temidos *cheats*. Através deles é possível obter vantagens contra os seus adversários. Nem sempre os *cheats* são utilizados de formas ilegais, quando disponibilizados pelos seus fabricantes, eles podem ser favoráveis ao usuário.

[1] Faculdade de Tecnologia de Araraquara. E-mail: augusto.vicentine@fatec.sp.gov.br
[2] Faculdade de Tecnologia de Araraquara. E-mail: gabriela.silva122@fatec.sp.gov.br
[3] Faculdade de Tecnologia de Araraquara. E-mail: joao.nascimento19@fatec.sp.gov.br
[4] Faculdade de Tecnologia de Araraquara. E-mail: joao.neves@fatec.sp.gov.br

Entretanto, quando usados de forma ilegal, tirando proveito de uma falha do sistema ou erro de *software*, ele pode causar até a expulsão permanente do jogador - esses casos são mais comuns em jogos *multiplayer e-sports*. Em 2019 o um projeto enviado ao senado tinha como proposta:

> "Esse projeto de lei visa tornar o ambiente de lazer virtual mais seguro, de modo a proteger todos que usufruam dos jogos online. Criminosos utilizam "*cheats*" e "*hacks*" para levar vantagem em jogos competitivos e assim ganhar de forma ilegal, seja uma partida ou um campeonato que valha dinheiro." (COELHO,2019).

Apesar de não ter recebido a quantidade necessária de votos, o projeto visava a proteção e a integridade dos usuários de jogos *online*, tornado ilegal prática e o uso de *cheat*, mediante a lei, e não somente dentro das plataformas de jogos, que é o que acontece hoje por meio da punição ao trapaceiro.

Este artigo parte da justificativa que uma das maiores preocupações entre os usuários de jogos *multiplayer* são os chamados *cheats*. Segundo Kasperky (2020):

> "Aqueles que violam as regras têm potencial para impedir que jogadores honestos ou profissionais participem de competições, afetando os relacionamentos na comunidade dos jogos. Além disso, essas violações podem ter impacto sobre a popularidade e a reputação de um torneio e, eventualmente, reduzir a receita ou o número de possíveis parcerias para os organizadores."

São diversas as formas de ataque que um *cheater* pode utilizar para tirar proveito dos seus adversários e chegar de forma ilegal ao topo do *ranking*. Os mais comuns são os *aimbot* e *wallhack.*

O objetivo desse artigo é esclarecer a importância dos *softwares anti-cheats* dentro dos jogos. De acordo com Favorito (2014) "Com a evolução e difusão dos jogos *online* e para celulares, cresce também a preocupação a segurança com os dados dos jogadores.".

Os *cheats* são frequentes dentro dos jogos *online* de competições, eles são os responsáveis por fazer o adversário tirar vantagem de forma ilegal sobre o seu oponente, principalmente dos jogadores mais novos e menos informados. "*Cheaters*: Os velhos trapaceiros, que usam clientes adulterados e *bots* para obter vantagens irregulares dentro dos jogos. Também há aqueles que tentam se aproveitar da falta de experiência dos novatos para trapaças." (FAVORITO, 2014).

Uma maneira de tentar prevenir essas trapaças é por meio de *software anti-cheats*, que tem como objetivo identificar mudanças no padrão no sistema operacional, erro de memória e *hardware*.

No mercado existem vários *softwares* anti-trapaças, desenvolvidos por empresas de segurança, com intuito de proteger o jogo *online* e os jogadores. Suas vantagens são diversas, entre elas tornar as competições mais justas, detectando fraudes. Porém, também possuem algumas desvantagens, tais como: podem ser invasivos, tendo a acesso a dados dos usuários no computador.

O *software anti-cheat* da *Riot Games*, o *Vanguard*, atualmente tem causado controvérsias entre os seus usuários. Apesar de ser um *software* que promete identificar trapaças indetectáveis por outros *anti-cheats*, vem prejudicando o desempenho e causando danos nos computadores de alguns jogadores. Contudo, mesmo contendo algumas falhas e apesar da evolução dos *cheats*, os *softwares anti-cheats* têm grande importância dentro do cenário dos jogos *online*, por isso a importância de se investir em segurança e em atualizações dos *softwares* para proteger seus usuários e garantir a integridade.

2. O que são *cheats*?

Cheat é uma linguagem própria utilizada por usuários de jogos para denominar trapaças, códigos e truques usados para alterar o grau de dificuldade de um jogo, deixando-o mais fácil ou mais difícil. Também é conhecido como batota, que significa fraude em jogo ou forma de trapaça.

Os *cheats* não são novidades em jogo de *videogames*, já que alguns são criados pelos próprios fabricantes dos jogos, sendo ativados por meio de códigos ou sequência de botões. Nem sempre são considerados trapaças, às vezes são utilizados para exibir o segredo de um jogo e oferecer ao jogador caminhos mais rápidos, recursos infinitos, avanço de fase ou estágio, entre outras facilidades.

Segundo um canal do *YouTube*, um *cheat* foi descoberto no título *God of War*, lançado em 22 de março de 2005 com exclusividade para o *PlayStation 2*, no qual ao executar uma sequência de comandos em seu menu inicial, o jogador já tinha acesso a literalmente tudo do jogo, sem precisar terminar ele diversas vezes. E esse *cheat* se manteve na continuação do jogo de nome *God of War 2*, lançado em 7 de março de 2007, também exclusivo do *PlayStation 2* na época (FERREIRA, 2020).

De acordo com Sora (2020) muitos jogos, principalmente os mais antigos, são conhecidos pelos seus desafios e, para ajudar os usuários, os desenvolvedores criaram alguns *cheats*, que acabaram ficando marcados na história – podemos citar o *Rosebud*, do jogo *The Sims*, que permitia ao jogador ganhar a moeda virtual imediatamente e sem limite de vezes para realizar o código; o *DK Mode*, do *GoldenEye 007*, que fazia com que os personagens tivessem o tamanho de sua cabeça e de seus braços aumentados; o código para habilitar o sangue na versão de *Mega Drive* do primeiro *Mortal Kombat*; os diversos códigos da franquia *Grand Theft Auto* (popularmente chamada pela sigla *GTA*) em geral, mas principalmente os do jogo *GTA San Andreas*; e *Konami Code*, visto pela primeira vez no *game* de naves desenvolvido pela *Konami* em 1986, com o nome de *Radius*, no qual ao realizar a famosa sequência de botões cima, cima, baixo, baixo, esquerda, direita, esquerda, direita, botão B e botão A, eram ativados todos os upgrades da nave. Esse código foi visto em mais vários jogos feitos pela *Konami* durante a época do *Super Nintendo* e até hoje existem referências a ele, inclusive na animação da *Disney* de nome Detona Ralph lançada no dia 4 de janeiro de 2013.

Mas em alguns casos os *cheats*, principalmente em jogos *online*, acabam beneficiando e dando vantagens a alguns jogadores, nesse caso se tornando trapaças, como é a tradução da palavra *cheats* para a língua portuguesa.

Em jogos *multiplayer*, que são jogos geralmente *online* que permitem que vários usuários joguem de modo simultâneo a mesma partida, utiliza-se o chamado *exploit:* "geralmente é uma sequência de comandos, dados ou uma parte de um *software* elaborados por *hackers* que conseguem tirar proveito de um defeito ou vulnerabilidade." (Canal Tech, 2017). Isso permite criar um *cheat* e ter acesso ao jogo de maneira ilegal, pois oferece vantagens para o jogador que não foram colocadas pelo fabricante, dando privilégios indevidos contra o seu adversário.

De acordo com Thiago Maia, diretor geral do Flamengo *e-Sports*, tudo o que um player faz dentro do jogo é dividido em três etapas, sendo a primeira delas o conhecimento sobre o jogo, do que pode ou não ser feito e situações que já foram vistas pelo jogador dentro das partidas; a de decisão, que consiste em pensar na jogada e a terceira etapa sendo a execução, que é de fato realizar o movimento. Porém, dentro dessa execução existe um limite do aceitável, que é aquilo que pode ou não ser realizado dentro da limitação humana. Os *cheats* que alguns jogadores utilizam fazem com que eles tenham vantagem tanto na execução, sendo possível fazer coisas sobre-humanas, quanto na decisão a ser tomada, já que o jogador terá informações privilegiadas às quais ele não deveria ter acesso (MAIA, 2020).

As trapaças em jogos *online* podem ser realizadas por meio de editores de memória, que alteram as informações dos jogos, podendo ser executadas de diferentes formas. Entre as mais comuns estão o *AimBot* e o *WallHack* (LIMA, 2018). O chamado *AimBot* trata-se de um *bot* que auxilia a mira do jogador, colocando a mira geralmente na cabeça dos adversários de uma maneira precisa, assim facilitando com que o jogador acerte o tiro na cabeça e elimine seu oponente mais rápido. O *AimBot* auxilia tanto na etapa de execução como na de decisão, já que ele ignora paredes impostas pelo mapa e coloca a mira precisamente onde quer que o oponente esteja, permitindo ao jogador saber onde seu oponente está, mesmo sem vê-lo.

Outro *cheat* bem comum segundo Madruga (2017) é o chamado *WallHack*, que mostra a posição dos oponentes através das paredes e objetos opacos, dando informação privilegiada para que o jogador possa tomar suas decisões e fazer suas jogadas. Diferente do *AimBot*, o *WallHack* não mira automaticamente para o oponente, ele apenas mostra a posição dele através das paredes, além de outras informações, como arma que o oponente está utilizando e a quantidade de vida do personagem.

Segundo Lima (2018), geralmente jogadores que são pegos utilizando *cheats* são banidos dos jogos, e isso não acontece apenas casualmente. Já ocorreram casos de jogadores serem banidos durante torneios profissionais, seja sendo pegos por algum *anti-cheat* ou alguém da organização que tenha visto o jogador utilizando a ferramenta, ou até mesmo por decisão da organização do torneio após rever replays das partidas e chegar a um veredicto.

A questão tem sido pautada por Abreu (2018), que cita o exemplo do jogador Nikhil Kumawat, ex-jogador do time *Optic India*, que foi banido após ser flagrado trapaceando durante um jogo presencial pelo campeonato *Zowie eXSTREMELAND Asia*. Isso aconteceu após a organização *ESL India* verificar os arquivos do jogador durante o campeonato e confirmar a utilização de *cheats*. Além desse, também existe o caso de Joel Mako, que durante a *FragByte Masters III*, atuando pelo time *Team Property*, foi

desconectado da partida por ser pego pelo *anti-cheat* e sendo então banido. Um dos casos mais famosos de utilização de *cheats* é o do brasileiro Pedro Leone, durante o qualificatório brasileiro para a *World Cyber Games* em 2009, cujas jogadas e atos suspeitos do jogador fizeram os oponentes desconfiarem do mesmo, principalmente pelo fato do jogador tentar esconder o seu monitor e se mostrar muito nervoso durante as partidas. Após o torneio, ele foi banido após ter sido constatado que em sua tela havia um ponto branco que podia ser ativado e desativado e que seguia os inimigos mostrando suas posições para o jogador.

3. O que são *anti-cheats*?

Dentro dos jogos *online* existem muitas formas de trapaças, entretanto desenvolvedores de jogos e *softwares* criaram uma tecnologia que tenta evitar essas fraudes, os chamados *anti-cheats*. Eles atuam de forma a detectar trapaças em jogos. Os *softwares anti-cheats* são desenvolvidos por algumas empresas de segurança, entre eles o *NProtect GameGuard*, desenvolvido pela *INCA*, o *Battleye* desenvolvido pela *Battleye*, o *VAC* desenvolvido pela *Valve Corporation*, o *Easy* desenvolvido pela *Kamu*, o *Xingcode3* desenvolvido pela *Wellbia*, entre outros. Os *softwares* anti-trapaças detectam a fraude no sistema operacional do jogador, e esse jogador fica sujeito a ser banido. Também detectam erros na memória ou no *hardware* do jogador e isso também pode causar a sua expulsão da plataforma.

Ultimamente estão aumentando as punições aos jogadores que utilizam de formas ilegais e de trapaças para conseguir vantagens em jogos. Normalmente quando se percebe as trapaças as punições podem variar desde bloqueios temporários até suspensão da conta.

4. Vantagens e desvantagens dos *anti-cheats*.

Como tudo no meio tecnológico, os *anti-cheats* também possuem suas vantagens e desvantagens.

De forma geral, as vantagens são: a busca por tornar os jogos e as competições de *e-Sports* mais justas; a existência de boas opções gratuitas, com foco em partidas e jogadores casuais; os *anti-cheats* mais intrusivos detectam e agem contra *cheats* mais complexos e de difícil detecção, como os que atuam no *kernel* (núcleo do sistema operacional); o banimento, temporário ou permanente, dos jogadores pegos utilizando trapaças.

Em contrapartida, suas desvantagens incluem: o alto custo de bons programas (aqueles com foco em partidas competitivas e de *e-Sports*); o fato de que serão, em algum momento, ignorados e ultrapassados por *cheats* mais bem elaborados; os *anti-cheats* mais intrusivos terão acesso a grandes quantidades de dados no computador do cliente, além de poder danificar a máquina; podem atrapalhar as *system calls*.

Existem vários programas que buscam combater as trapaças em jogos *online*, sendo uns mais famosos e/ou polêmicos que outros. Como exemplo podemos citar o *VAC*, da *Valve Corporation*, também conhecida como *Valve Software*, que possui como vantagens o fato de ser gratuito, não precisar ser instalado manualmente, banir os

trapaceadores e exibir em seu perfil *Steam* (*software* mais famoso da empresa, usado para a compra de jogos de computador, principalmente) um indicador da quantidade e da data do(s) banimento(s), além de possuir uma grande capacidade de monitoramento das atividades dos usuários. As desvantagens mais conhecidas são o fato de ser lento e fácil de ser contornado. Apesar de tentativas da empresa para uma melhoria do mesmo, tornando-o mais intrusivo, a comunidade não recebeu de forma positiva e tornou-se contra tais alterações, difamando o *VAC*.

5. Estudo de caso

Atualmente, um *anti-cheat* muito falado pelos jogadores e pela mídia dos *e-Sports* é o *Vanguard*, da *Riot Games*. Recentemente a *Riot Games*, preocupada com a integridade dos jogadores no seu novo jogo chamado VALORANT, lançou junto do jogo um novo *anti-cheat* no mercado chamado *Riot Vanguard*. Ele consiste em um cliente que roda durante a execução do jogo e conta também com um *driver* contra *cheats* no modo *kernel* da máquina.

Isso não é uma novidade já que outros *anti-cheats* como *Battleye*, *Xingcode3* e *EasyAntiCheat* já utilizam *drivers* em modo *kernel* para a segurança de jogos Triplo-A, que são jogos com grandes orçamentos e são esperados que sejam de altíssima qualidade. Mas o que a *Riot Games* espera é trazer um nível de segurança elevado para seu jogo e garantir uma melhor experiência competitiva para os jogadores, pois eles acreditam que a ferramenta contra *cheats* é uma das mais importantes dentro de um jogo e, com o *Riot Vanguard*, esperam tornar a vida dos trapaceiros mais difícil.

De acordo com o líder de sistemas *anti-cheat*, Chamberlain (2020), a estratégia que querem utilizar para proteger os jogadores de *cheaters* é a de aplicar uma abordagem de defesa aprofundada. Ou seja, primeiramente, eles criam um jogo resistente a *cheats*, após isso dificultam a criação de novos *cheats* utilizando o *Riot Vanguard* e outros métodos de antiviolação e, por último, banem e removem os *cheaters* do jogo do jeito mais eficiente possível com a detecção de *cheats* do *Vanguard*, além de denúncias feitas pelos próprios jogadores. Mas claro que dentro da segurança da informação não existe nenhum método totalmente confiável e efetivo para acabar com os trapaceiros dos jogos, sendo isso uma guerra eterna entre os desenvolvedores. Durante o tempo de Beta do VALORANT já foram criadas trapaças para o jogo como era previsto, mas com essa estratégia eles esperam que seja dificultada a criação desses *cheats*, além de sua manutenção, fazendo com que esse desenvolvimento tenha um custo muito elevado e consequentemente aumentando o preço desses recursos para os usuários, assim desencorajando os mesmos a utilizarem essas ferramentas para obter vantagens no jogo. Portanto, diminuindo o tamanho da comunidade que desenvolve esses *cheats*, a *Riot Games* terá mais facilidade em rastrear as trapaças e tomar providências para mantê-las longe de seus jogos.

O *Riot Vanguard* já se mostrou efetivo também durante as partidas de VALORANT, interrompendo-as e exibindo uma mensagem dizendo que um *cheater* foi detectado e banido dessa partida e do jogo. Essa mensagem também informa que nenhuma vitória ou derrota será creditada aos jogadores. Após essa mensagem, os

jogadores são direcionados de volta ao menu principal do jogo de onde podem tranquilamente procurar outra partida e jogar normalmente.

Mas com todo esse *hype* em cima do VALORANT, muitos usuários de todas as regiões vêm fazendo reclamações sobre o *Riot Vanguard* ter causado problemas em suas máquinas, que variam de bloquear programas importantes até problemas que levam à tela azul da morte (erro grave no sistema), superaquecer as peças do *hardware*, seja desligando *softwares* de resfriamento ou o *cooler*, desconectar dispositivos I/O como o teclado e o *mouse*, desligar o computador, além de afetar seu desempenho de outras maneiras e, além desses problemas, o bloqueio de *drivers* pode impactar negativamente no funcionamento de aplicativos.

Um dos usuários reportou que o *Vanguard* bloqueou um programa chamado *MSI Afterburner*, que é utilizado para checagem de temperatura do *hardware* e outra pessoa disse que o *anti-cheat* bloqueou o controle do seu *mouse* e teclado e apenas conseguiu reativar esse controle após reiniciar o computador no modo de segurança. Já problemas que geram a famigerada tela azul da morte acontecem pois o *Vanguard* inicia ao mesmo tempo em que o computador está iniciando, e o *anti-cheat* entra em conflito com alguns programas, mas não consegue discernir os programas importantes dos não essenciais. Pelo suporte da própria *Riot Games* responderam que o *Vanguard* não causa interferência em nenhum *driver* ou *hardware* do computador e que, caso esteja ocorrendo qualquer anormalidade, sugerem que verifiquem se todos os *drivers* estão atualizados corretamente.

Enquanto para alguns o *Vanguard* vem trazendo problemas, para outros o *anti-cheat* tem funcionado normalmente e garantido a segurança e integridade das partidas. Com certeza receberá mais atualizações para resolver esses possíveis problemas, mas no geral o *Riot Vanguard* tem se mostrado um ótimo *anti-cheat* e realmente faz o que deve ser feito para proteger o cenário casual e o competitivo, que tende a ser bem grande no futuro. Com isso, muitos poderão tentar utilizar de programas ilegais para chegar ao topo do *ranking*, mas felizmente teremos o Vanguard para parar os trapaceiros e termos um cenário saudável para todos os tipos de jogadores.

6. Discussões

Esta investigação de caráter qualitativo foi realizada através de pesquisa bibliográfica, relatos de fóruns e de empresas de segurança e desenvolvedoras de *softwares*. A Tabela 1 contém comparativos entre o *Anti-Cheat Riot Vanguard* e o *anti-cheats* de outras empresas.

Considerando o contexto de jogos *online* no qual a diversidade de *hacks* é uma das maiores preocupações dos usuários de jogos de *multiplayer*, os *anti-cheats* sem dúvida são de grande valia, além de serem uma das ferramentas de segurança mais indicadas para essa finalidade. Apesar de algumas desvantagens como o preço de bons *softwares* e o fato de que em algum momento serão ignorados e ultrapassados pelos *cheats*/*hacks*, ainda são a melhor solução no mercado para combater essas trapaças, já que banem os jogadores que utilizam de meios não convencionais para obterem vantagens e costumam receber grande investimento para tornar os jogos e competições mais justos.

Tabela 1 - *Anti-cheats*: vantagens e desvantagens

	Vantagens	Desvantagens
VAC	Gratuito	Lento
	Não precisa ser instalado manualmente	Fácil de contornar
	Bane trapaceadores e indica no perfil público dos mesmos	Não é mais intrusivo porque a própria comunidade é contra; *fake news* difamaram esse *anti-cheat*
	Possui grande capacidade de monitoramento	
VANGUARD	Gratuito	Pode prejudicar o desempenho do jogo
	Atua no *kernel*, cobrindo uma maior área contra *cheats* (muitos atuam no kernel)	Pode ocasionar tela azul
	Detecta muitos *cheats* tidos como indetectáveis por *anti-cheats* tradicionais	Superaquece as peças do hardware (desliga *softwares* de resfriamento, desliga o *cooler*)
	Busca garantir o cumprimento das leis regionais de privacidade de dados	Pode ocasionar a desconexão de dispositivos I/O
		Desliga o computador, afeta de outras maneiras o desempenho
	Bloqueia *drivers* vulneráveis	Bloqueia *drivers*
GERAL	Buscam tornar os jogos e competições mais justas	Bons *anti-cheats* costumam ser pagos
	Existem opções gratuitas e de boa qualidade	Eventualmente serão ignorados por *cheats* mais bem elaborados
	Os mais intrusivos detectam e agem contra *cheats* mais complexos, como os que atuam no *kernel*	Os mais intrusivos terão acesso a grande quantidade de dados no computador do cliente; podem danificar a máquina
	Banem os jogadores pegos utilizando trapaças	Podem atrapalhar as *system calls*

7. Considerações finais

De acordo com nossa pesquisa, os *anti-cheats* vêm melhorando cada vez mais em sua busca de barrar os trapaceiros nos jogos de nível casual, amador e competitivo, e essa melhora exemplifica bem a eterna batalha entre aqueles que tentam burlar um sistema contra aqueles que tentam defendê-lo.

Mesmo que o tempo passe, sempre haverá desenvolvedores de *cheats* criando métodos para burlar a segurança dos *anti-cheats*, pois não existe nenhum método infalível de segurança. Contudo, esse trabalho será cada vez mais complicado, principalmente por causa das tecnologias que vêm sendo utilizadas nos *softwares* anti-trapaças, fazendo com que nesse desenvolvimento seja necessária a utilização de ferramentas caras e que consumem muito tempo do desenvolvedor, fazendo com que no final de todo esse processo tenha sido criado um produto com o preço de mercado muito elevado, o que irá desencorajar o uso dos *cheats*.

Mesmo que alguns *anti-cheats* rodem no modo *kernel*, como por exemplo o *Riot Vanguard*, desde que respeitem as leis de proteção de dados e sejam otimizados para não causar problemas com outros processos, não serão considerados intrusivos, já que buscam apenas trazer uma proteção para os jogos. Como alguns *cheats* são criados também em modo *kernel*, o único jeito de serem pegos é trazendo uma ferramenta de segurança que atue no mesmo nível de sistema que a trapaça, para que seja possível barrar sua utilização e banir os trapaceiros.

Referências Bibliográficas

ABREU, Victor. CS:GO: **ESL confirma que forsaken, da OpTic India, usou cheat**. Disponível em:<https://www.techtudo.com.br/noticias/2018/10/csgo-esl-confirma-que-forsaken-da-optic-india-usou-cheat-esports.ghtml. Acesso em: 02/07/2020.

CANAL TECH. **O que é exploit?** Disponível em: https://canaltech.com.br/produtos/O-que-e-exploit/#:~:text=Um%20exploit%20geralmente%20%C3%A9%20uma,de%20um%20defeito%20ou%20vulnerabilidade. Acesso em: 01/07/2020

CHAMBERLAIN, Paul. **Estratégias contra cheats em Valorant**. Disponível em:<https://playvalorant.com/pt-br/news/dev/estrategia-contra-cheats-em-valorant-o-que-por-que-como/>.Acesso em: 23/06/2020.

COELHO, David. **Tonar crime o uso de "hacks" e "cheats" em jogos online.** Disponível em:<https://www12.senado.leg.br/ecidadania/visualizacaoideia?id=119094. Acesso em: 02/07/2020.

FAVORITO, Fernanda. **Conheça as 5 principais ameaças aos usuários de jogos online**. Disponível em:<https://fernandafav.jusbrasil.com.br/noticias/119755778/conheca-as-5-principais-ameacas-aos-usuarios-de-jogos-online?ref=feed. Acesso em: 02/07/2020.

FERREIRA, ReviewdeGames. **SEGREDO DESCOBERTO 15 ANOS DEPOIS - God 1 e God 2.** YouTube, 10/06/2020. Disponível em:< https://www.youtube.com/watch?v=r_jFloKr_Qo>. Acesso em 23/06/2020.

KASPERSKY**. Apresenta solução para identificar trapaças em e-sports.** Disponível em:<https://tiinside.com.br/24/09/2019/kaspersky-apresenta-solucao-para-identificar-trapacas-em-esports/. Acesso em: 02/07/2020

LIMA, Luiz Felipe. **Hacks e cheats no CS:GO: 5 jogadores que foram banidos do jogo.** Disponível em:<https://www.techtudo.com.br/listas/2018/07/hacks-e-cheats-no-csgo-5-jogadores-que-foram-banidos-do-jogo-esports.ghtml. Acesso em: 02/07/2020.

MADRUGA, Cleiton. **Wallhack: entenda hack proibido no CS:GO, Free Fire e jogos de tiro.** Disponível em:<https://www.techtudo.com.br/noticias/2019/12/wallhack-entenda-hack-proibido-no-csgo-free-fire-e-jogos-de-tiro-esports.ghtml. Acesso em: 02/07/2020.

MAIA, Flow Podcast. **DJOKO - Flow Podcast #146**. YouTube, 26/06/2020. Disponível em:<https://www.youtube.com/watch?v=A9S81hn4jpo&feature=youtu.be&t=4913>. Acesso em: 30/06/2020.

SORA. **Os Cheat Codes mais famosos dos games**. 2020. Clube do Vídeo Game. Disponível em: https://clubedovideogame.com.br/cheat-codes-mais-famosos-games/. Acesso em: 23/06/2020.