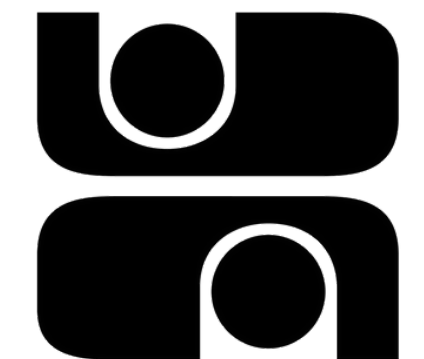




SBSEG'24

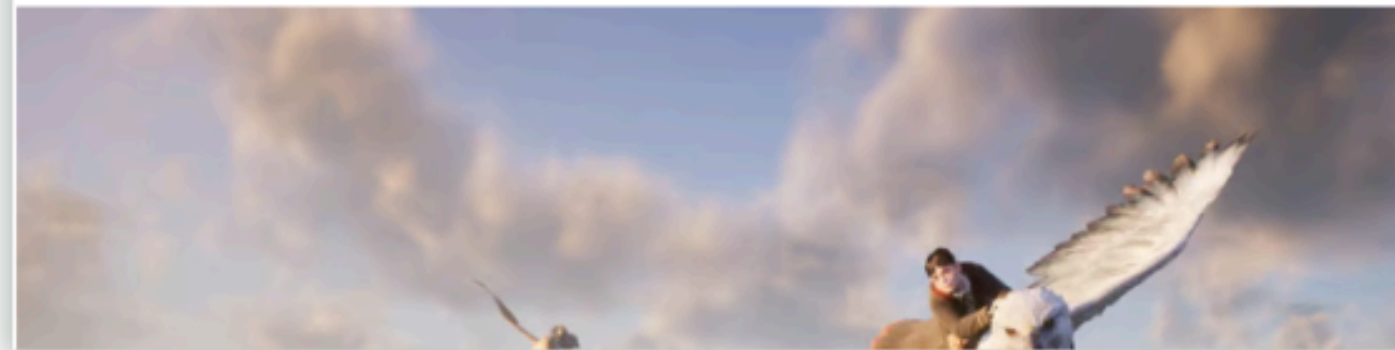
# O IMPACTO DE SOFTWARE ANTI-CHEAT NA PRIVACIDADE DO USUÁRIO

Vinicius Matheus, Tiago Heinrich, Vinicius Fulber-Garcia,  
Newton C. Will, Rafael R. Obelheiro, Carlos A. Maziero



As video games grow, they are eating the media

The games business has lessons for other industries and for governments



**SUCESSO** no Brasil  
e no mundo!

# MERCADO DE VIDEOGAMES

Mercado de games: tendências e oportunidades

Uma indústria que não para de crescer e apresenta bom potencial para empreendedores.

4 min de leitura • Atualizado em 11/06/2023



Duplicação de itens

Wallhack

Editores de  
personagem

Supressão de  
gravidade

Disparo  
assistido

Bots

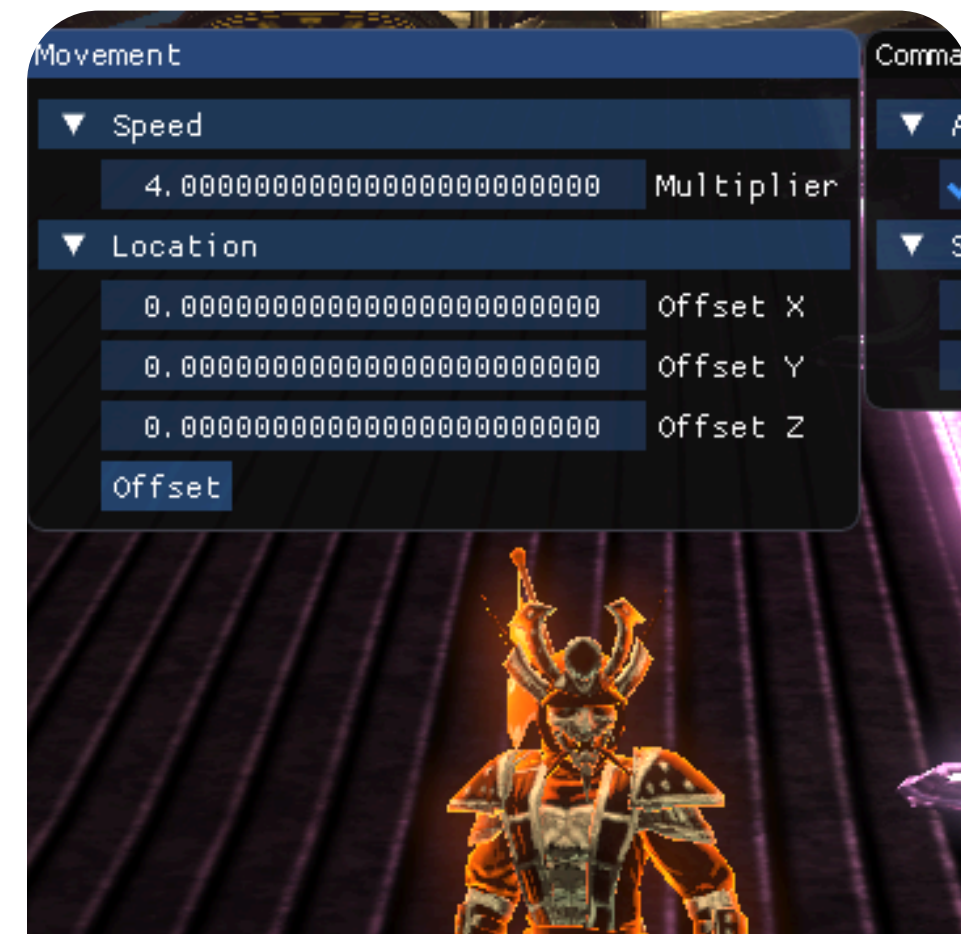
# O PROBLEMA DOS CHEATS

Invencibilidade

Acesso a  
regiões ilegais

Mira assistida

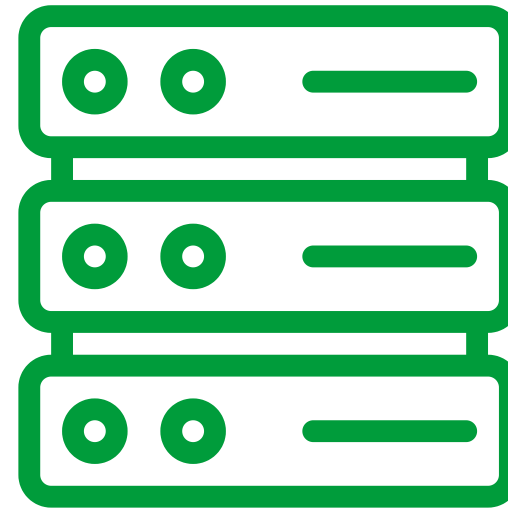
Aumento de  
velocidade



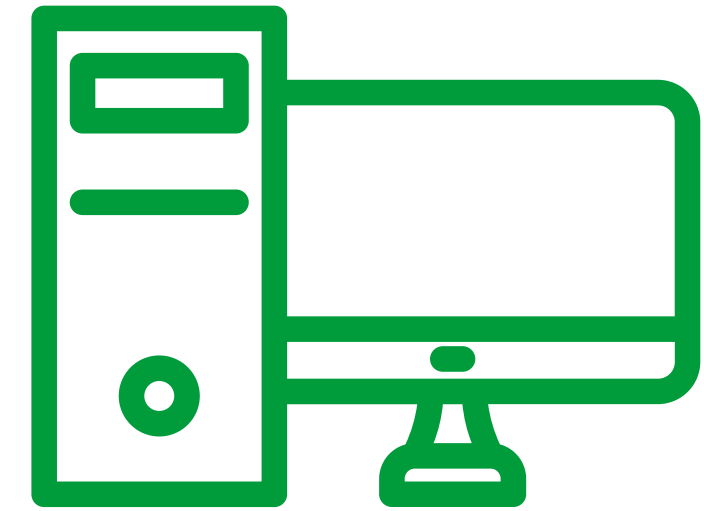
# CONTRAMEDIDAS



**COLETA E ANÁLISE  
DE DENÚNCIAS**



**USO DE SOFTWARE  
ESPECIALIZADO  
NO SERVIDOR**



**USO DE SOFTWARE  
ESPECIALIZADO  
NO CLIENTE**

**SOFTWARE ANTI-CHEAT**



# E OS SOFTWARE **ANTI-CHEAT?**

**ACESSO PRIVILEGIADO** À REDE

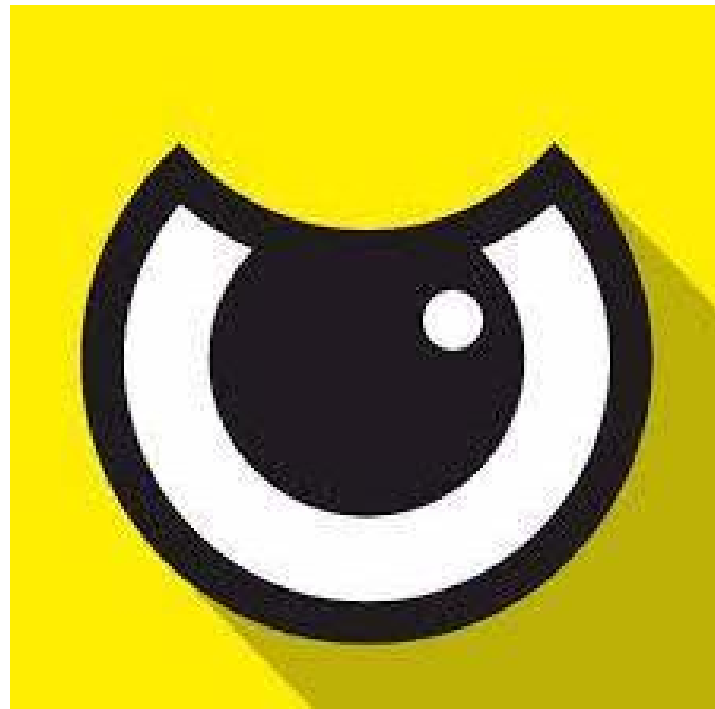
**ACESSO PRIVILEGIADO** AO SISTEMA DE ARQUIVOS

**ACESSO PRIVILEGIADO** ÀS OPERAÇÕES DO SISTEMA

**EXECUÇÃO COMPULSÓRIA** E CONTÍNUA

**A EXECUÇÃO DE SOFTWARES ANTI-CHEAT NA MÁQUINA DO USUÁRIO PODE REPRESENTAR UMA **INVASÃO DE PRIVACIDADE?****

# SOFTWARES ANTI-CHEAT **SÃO UM MUNDO...**



O que analisam?

O que executam?

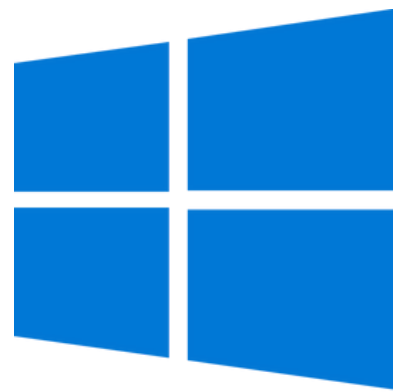
O que enviam?

O que "prometem"?

... QUE PRECISAMOS  
**EXPLORAR!**

# CENÁRIO DE TESTES

## Sistema Operacional



Windows 10

Windows 10 Pro  
Versão 22H2  
Build 19045.4046

## Análise



PE 17.08 e PM 3.96



Wireshark 4.2.3-0

## Meio



Tibia 13.34



Valorant 8.02

## Anti-cheat



BattlEye



Vanguard



# UMA ANÁLISE OPERACIONAL



## BattlEye

1. Carregamento de DLLs do sistema;
2. Leitura do *Safer* e *CodeIdentifiers*;
3. Verificação de integridade de DLLs;
4. Verificação de integridade do AC;
5. Ciclo de operação principal.
  - a. Abertura de DLL ou driver;
  - b. Verificação de integridade;
  - c. Acesso a certificados;
  - d. Envio de pacote UDP;
  - e. Escrita de *logs*.

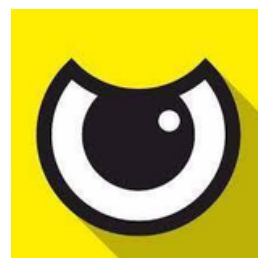


## Vanguard

1. Carregamento de DLLs do sistema;
2. Leitura do *Safer* e *CodeIdentifiers*;
3. Verificação de integridade do AC;
4. Consulta a registros do sistema;
5. Ciclo de operação principal.
  - a. Abertura de diretórios, arquivos e DLLs;
  - b. Verificação de conteúdo e integridade;
  - c. Envio de pacotes TCP;
  - d. Escrita de *logs*.

# UMA ANÁLISE OPERACIONAL EM DETALHES

BattlEye



Vanguard

## DLLs

63

42%

50

17,0 MB

## Tráfego 2m

16,2 MB

CDN Battleye

## Destino Comunicação

CDN Cloudfare

cfgmgr32

## Atenção

SHCore

shell32

shlwapi



FWPUCLNT

wtsapi32

# E DO PONTO DE **VISTA LEGAL?** POLÍTICA DE PRIVACIDADE E EULA

Declaração de acesso e processamento de dados pessoais  

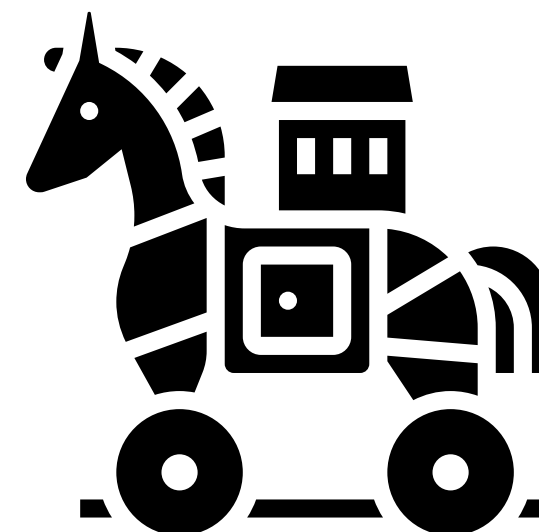
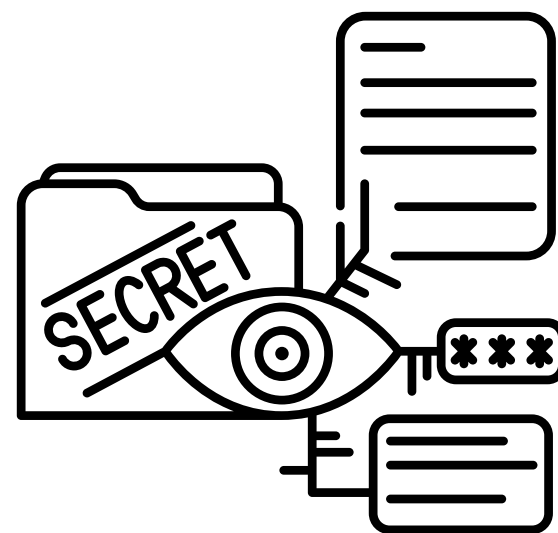
Declaração de compartilhamento de dados com terceiros 

Declaração de envio de resultados de análises  

Declaração de envio de arquivos suspeitos  

A PRIVACIDADE É GARANTIDA NA AUSÊNCIA DE COMPORTAMENTOS SUSPEITOS!

MAS, **O QUE É SUSPEITO???**

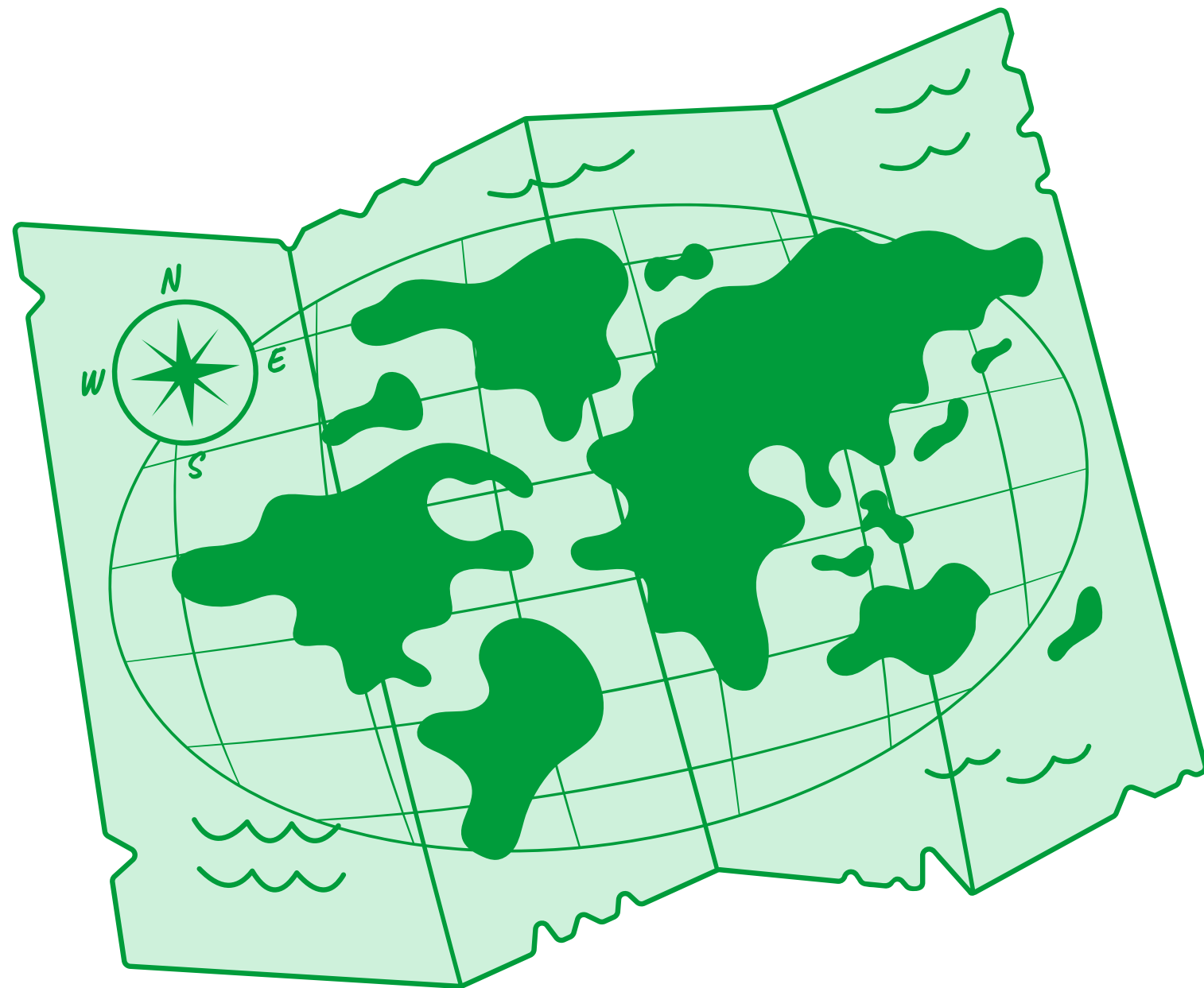


**UM ANTI-CHEAT? ...**

**UM SPYWARE? ...**

**UM TROJAN? ...**

**DO PONTO DE VISTA DO USUÁRIO  
COMUM E BENIGNO: DIFÍCIL DIZER!**



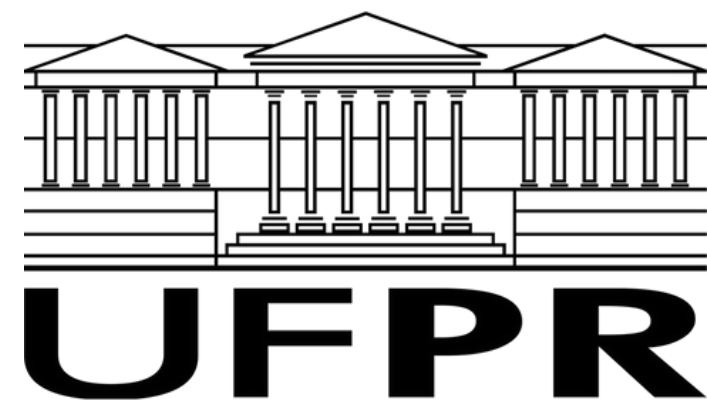
## MAPA PARA O **FUTURO**

- Aumentar o número de anti-cheats analisados;
- Fazer uma análise técnica-operacional entre anti-cheats e spywares;
- Fazer uma autointerceptação de comunicação para verificar os dados trocados entre cliente e servidor de anti-cheat;
- Desenvolver mecanismos e políticas menos intrusivas para a detecção de cheats.

# MUITO OBRIGADO!

---

Vinicius Fulber-Garcia



**SECRET**



[www.inf.ufpr.br/vinicius](http://www.inf.ufpr.br/vinicius)



[vinicius@inf.ufpr.br](mailto:vinicius@inf.ufpr.br)