

DEFEATING ANTI-CHEAT WITH HARDWARE

Trapaceando em jogos sem ser (facilmente) detectado

Ricardo Gomes da Silva

TDC Innovation 2021

\$ whoami



rgsilva.com



Disclaimer

As opiniões são minhas, sem relação com o meu empregador.
Não apoio uso de cheating :)



Anti-cheating

- » Software pra evitar.. bem, trapacear! :)
- » Via implementações específicas
 - » Validação server-side
 - » Ofuscação de memória
 - » Supervisão do jogador
 - » ... e outras técnicas variadas

Anti-cheating

» Via ferramentas de terceiros

» PunkBuster

» Valve Anti-Cheat (VAC)

» EasyAntiCheat 

» Software e mais software...

Muitos anos atrás...



Ragnarök Online



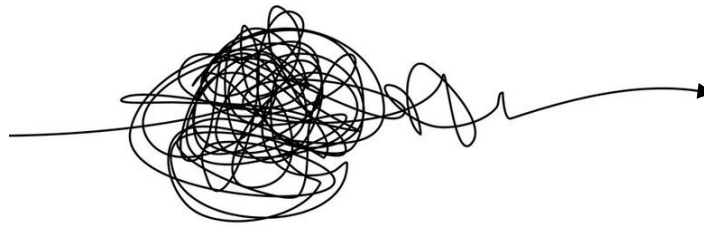
» MMORPG coreano

» Lançado em 2002 🇰🇷

» Chegou aqui em 2004 🇧🇷

» 2011 tinha ~25 milhões de assinantes 🌍

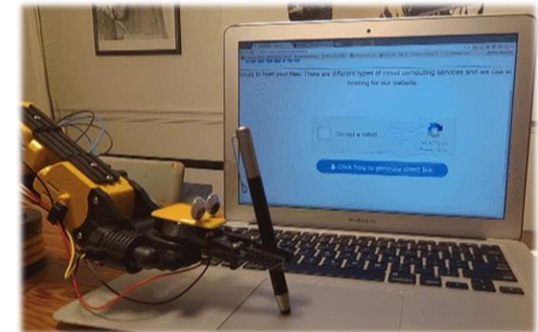
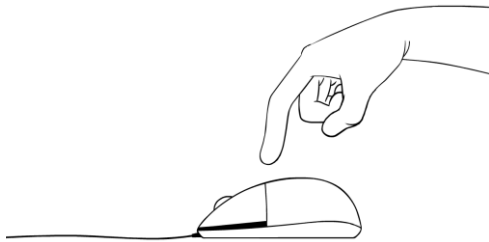
Ragnarök Online



* possivelmente contra os termos de uso

Ragnarök Online

» Como todo bom irmão dev: “dá pra automatizar isso não?”



Ragnarök Online

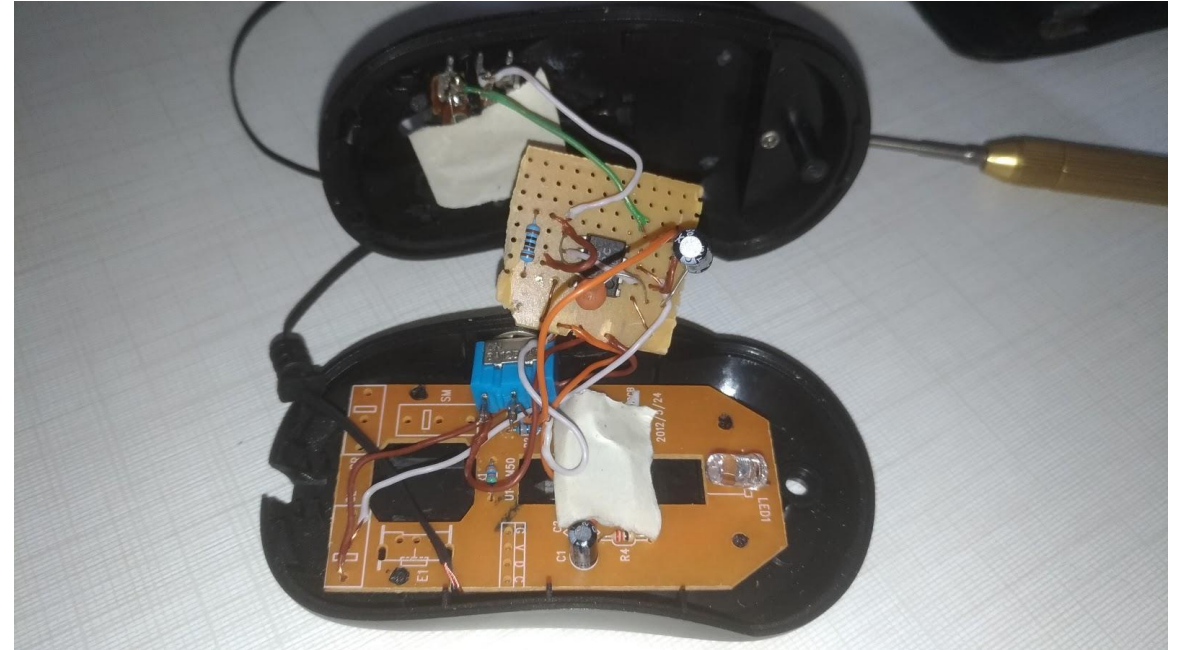


- » Anti-cheat via nProtect GameGuard
 - » Migrou para o EasyAntiCheat em 2019-06-18 (RIP VMs)
 - » Bloqueia macros de teclado e mouse por software
 - » Bloqueia ferramentas de automação (eg. AutoHotkey)
- » E como fica o hardware?

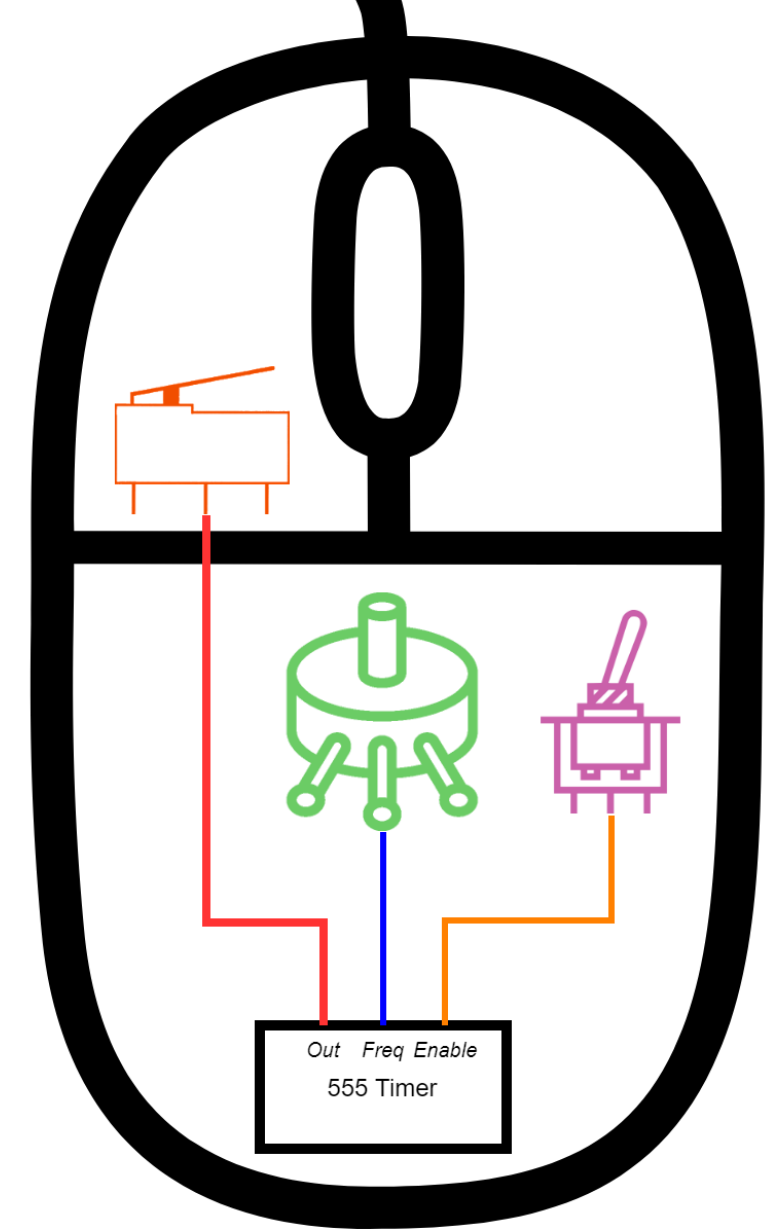
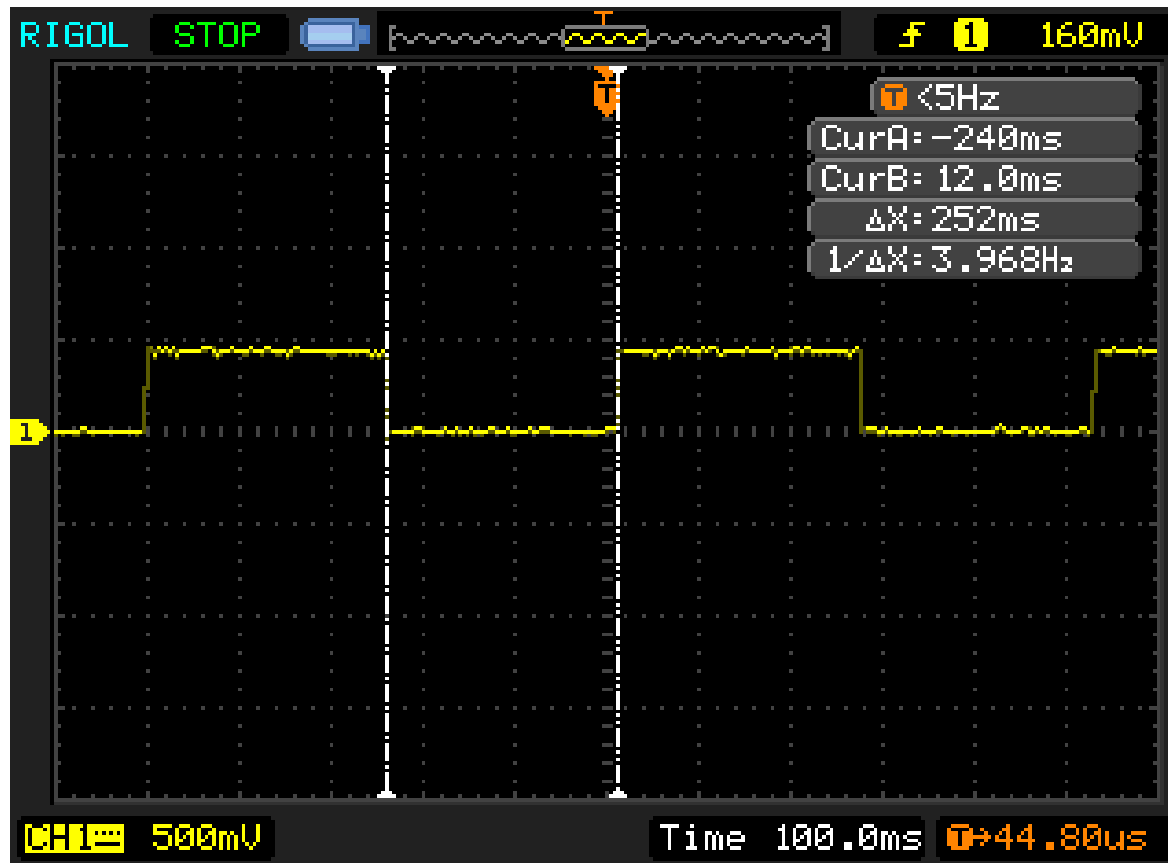
The Auto-Clicker ©

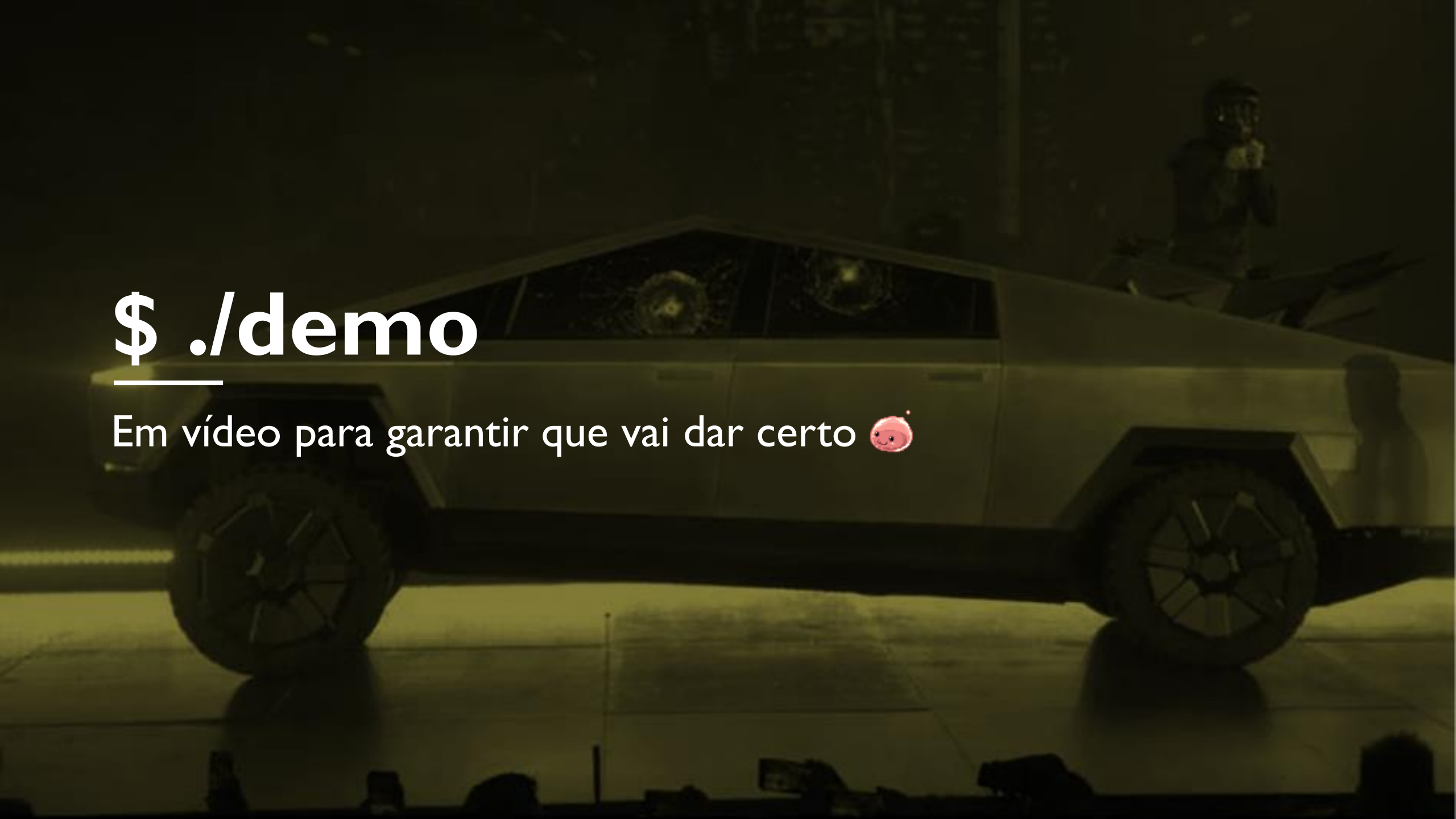
- » Botões são apenas (micro)switches!
- » Utiliza um 555 (timer) para fechar o circuito do botão
- » Frequência pode ser ajustada por um potenciômetro
- » Switch para ligar/desligar
- » RIP mouse

The Auto-Clicker ©



The Auto-Clicker ©





\$./demo

Em vídeo para garantir que vai dar certo 🍀

But why?

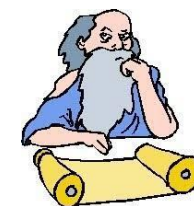


» Vantagens no jogo

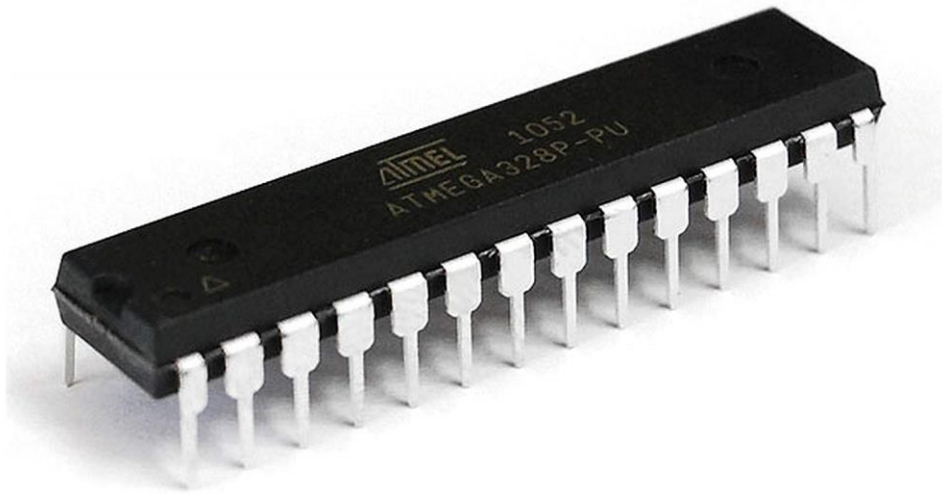
- » Clicar automaticamente em NPCs por (muitas) horas dava dinheiro 💰
- » Ferramenta anti-cheat não tinha (e ainda não tem) como detectar
 - » Foco é unicamente em hacks de software e não em nível de hardware

Até onde o ~~jogo~~ sistema operacional sabe, é apenas um mouse!

Mas o que é um mouse?

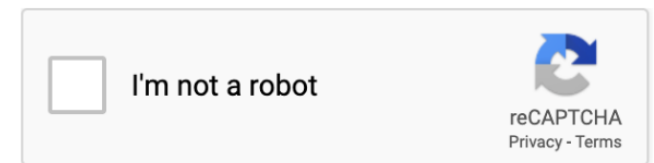


Isto é um mouse?



Bug's Fake Mouse ©

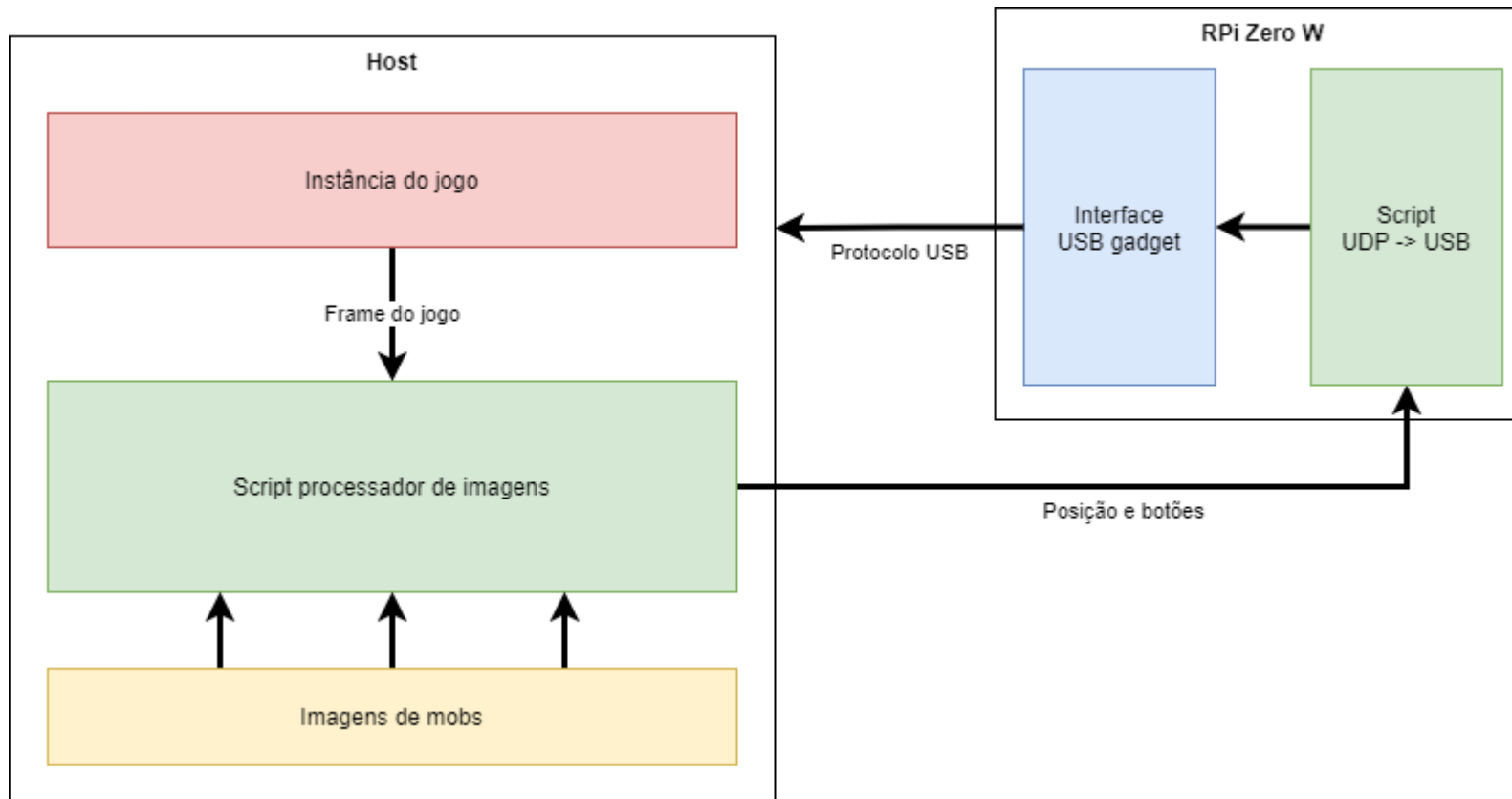
- » Baseado em uma Raspberry Pi Zero W
- » Modo USB gadget
 - » Permite tornar a RPi um dispositivo USB qualquer
 - » Script recebe dados pela rede e envia para a USB
- » Para o host é tudo apenas um mouse USB que se move *bem* rápido



Bug's Fake Mouse ©



Bug's Fake Mouse ©



Bug's Fake Mouse ©

- » Processador de imagens (~~aka script do bot~~)
 - » Encontra o mob, move o cursor e clica
 - » Em teoria dá pra fazer qualquer coisa com isso
- » Jogo permanece intacto
 - » Apenas captura de tela, o que é aceitável para stream
 - » Sem alteração de memória, sem análise de rede, sem injeção de DLL, nada
 - » Exceto um script Python, é claro :)



\$./demo

Acharam que não ia ter demo, né?



Como se proteger?

(se você for o dev, claro)

Detecções nível I

» Análise simples das entradas do jogo

- » Cliques com frequência ou duração constante
- » Teclados e mouses com entradas excessivamente rápidos

» Soluções triviais:

- » Introdução de fator aleatório nas entradas
- » Controlar o *timing* das entradas baseado em comportamento real

Detecções nível II

- » Dinâmica de digitação (*keystroke dynamics*)
 - » Biometria baseada em “como” digitamos
 - » Identificaria jogador a níveis individuais
- » Uso improvável ainda
 - » Biometria oscila muito durante o dia, além de fatores externos
 - » Complexidade alta para implementação em um simples jogo

Detecções nível III

- » Comportamento anômalo do jogador
 - » Alterações nas horas e duração das partidas
 - » Anomalia de progresso (*level* alto)
- » Relativamente trivial de burlar
 - » Requer modelagem do comportamento real como base da automação

Detecções nível IV

- » Controles dedicados (a la *consoles*)
 - » Uso de técnicas anti-tampering para (tentar) impedir modificações
 - » Uso de comunicação criptografada/autenticada para (tentar) impedir MITM
- » A não ser que teu jogo seja *muito* legal, eu não jogaria :)
 - » Custo do hardware se tornaria alto
 - » Base de jogadores ficaria limitada a quem pode comprar o hardware

Detecções nível...V?

» Combinação de técnicas

- » Técnicas tradicionais de detecção
- » Técnicas para detectar “anomalias” em hardware
- » Supervisão de jogo em caso de alta chance de trapaça

A stylized, dark green game controller is the central focus, surrounded by a glowing yellow aura and numerous floating yellow cubes of various sizes. The controller features a directional pad on the left, two analog sticks on the right, and several buttons. The background is dark with a pattern of yellow cubes.

Tá, e agora?

Mouse evolui para.... Mousemon!

Partiu hardware?



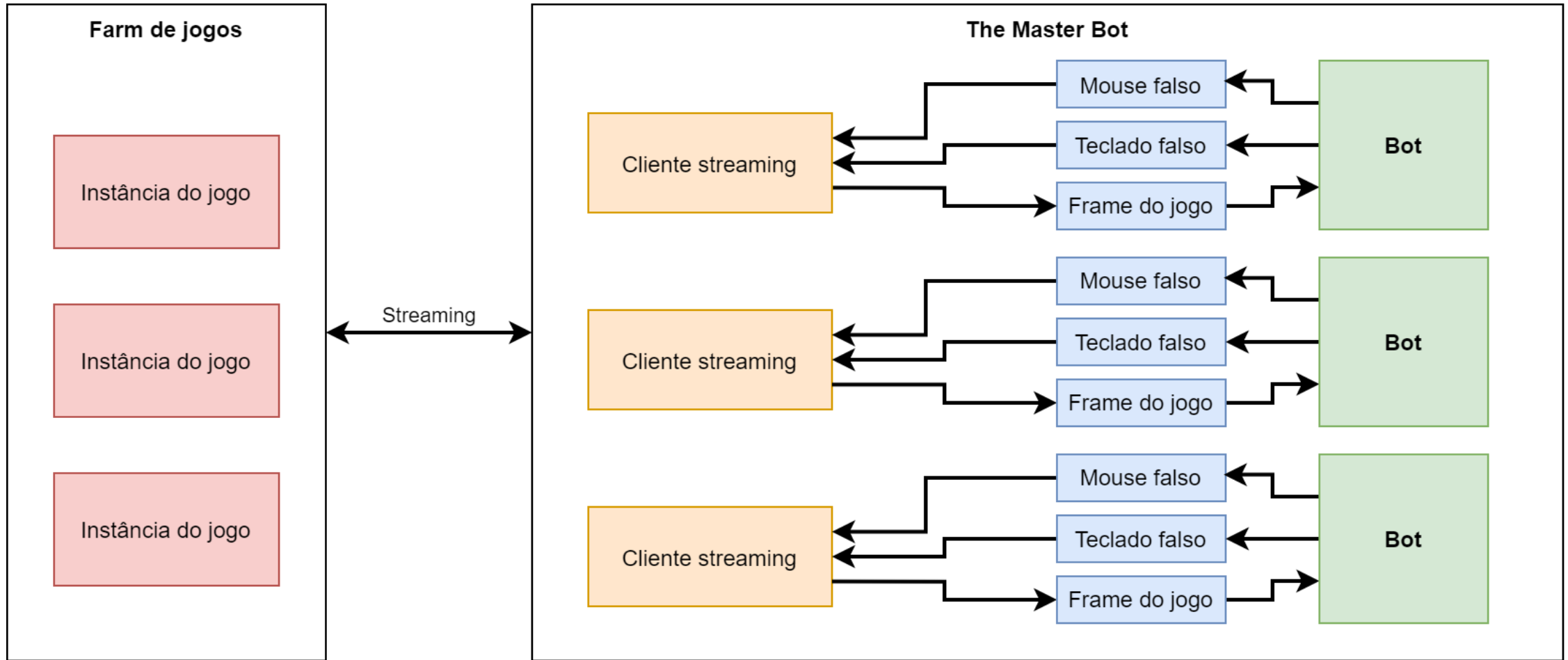
- » Captura de vídeo via HDMI
- » Processamento de imagens em hardware
- » Mouse via protocolo USB
- » Complexo e caro, mas não impossível



Ou partiu software?

- » Dispositivos virtuais (... *cof cof* webcams)
- » Ferramentas de streaming
 - » NVIDIA Shield
 - » Steam In-Home Streaming
- » Máquinas virtuais com o jogo
- » Tantas coisas tornando o ataque ainda mais imperceptível... :)

Fazendinha Feliz



E qual a moral disso tudo?

(fora que dá pra trapacear no Ragnarök)

Moral da história?



- » Moral da história não – lições!
- » Não confiar no hardware é não confiar no software
- » Uma proteção complexa nem sempre quer dizer que é boa
- » Nem tudo é perfeito: sempre vai ter um furo!

“Eu nunca”



- » “Ninguém nunca vai mudar esse campo na API”
- » “Ninguém nunca vai digitar um nome com aspas”
- » “Ninguém nunca vai trocar o ID na URL”
- » “Ninguém nunca vai usar essa senha da config de exemplo”
- » “Ninguém nunca vai hackear um mouse”

Trust issues!



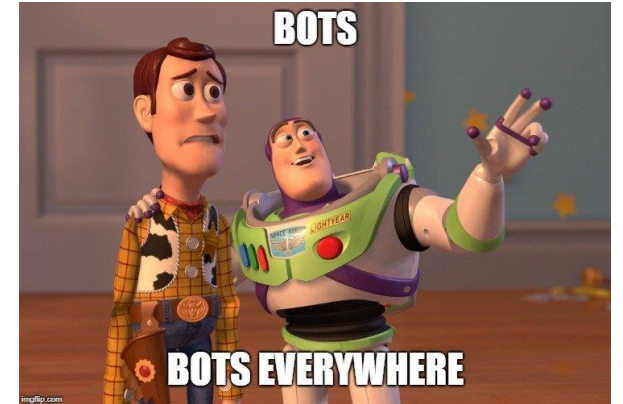
Vamos perder quanto se alguém atacar isto?

vs.

Vamos gastar quanto nos protegendo contra isto?

Concluindo

- » Ataque não muito trivial de se proteger
 - » Sempre confiamos que nosso hardware nunca nos trairá
- » Necessário definir até *onde* queremos nos proteger
 - » Introdução de custos e complexidades adicionais
 - » Não dá pra se proteger 100% :)
- » Automação em geral
 - » Nada impede isto de ser expandido para um Selenium versão hardcore



Pera, mas o quão eficiente é isso tudo?

- » Poucos meses de pesquisa e sabe o EasyAntiCheat que falei antes?
 - » Total de 440 138 jogos “protegidos” (incluindo Fortnite e Apex)
 - » Não detectou nenhum dos mouses até agora





DEFEATING ANTI-CHEAT WITH HARDWARE

Trapaceando em jogos sem ser (facilmente) detectado

Ricardo Gomes da Silva

TDC Innovation 2021

