
# Once a Cheater Always a Cheater

*Gotta Catch `em All*

Eugen Harton
DayZ
@eugenharton

# Who am I and how to contact me

- Working on DayZ in Production
- Worked on mobile games before
- Started in Enterprise (Operations)
- Focusing on game security for last two years.

- Twitter/Email @eugenharton

# Business of Cheating

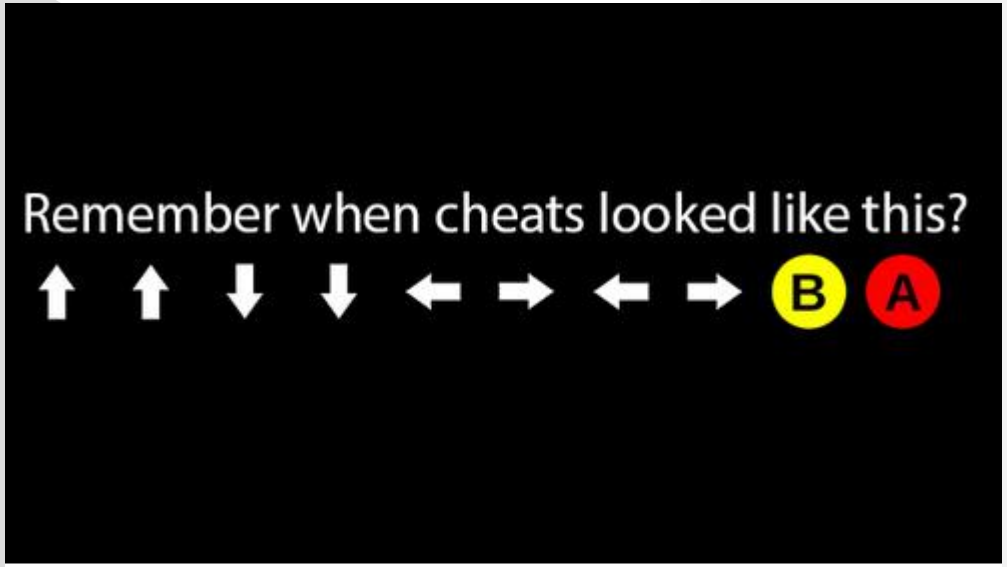
Bohemia Interactive

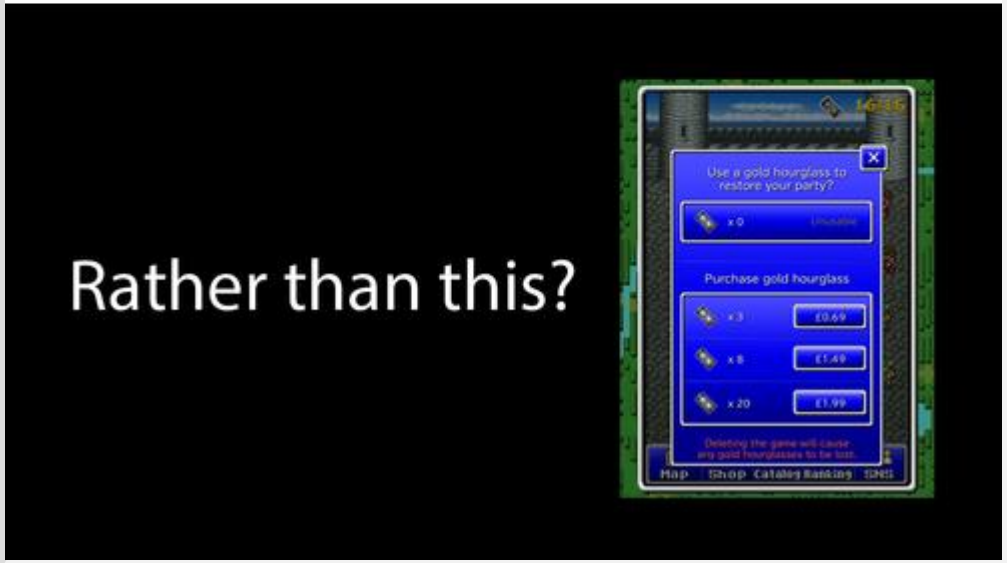
# Disclaimers!

- This talk applies to always online multiplayer games
- Based on my experience on DayZ and discussions with people in the field.

# What it is?

- Gaining an unfair advantage
- Breakdown :
  - Exploiting
  - Game state manipulation
  - Services
  - Automation




# History!

- Debug tools
- Easter eggs
- Alternate modes
- Secret Content

# Gotta Catch`em all !

- Unhackable game is a myth
- Cheats have evolved
- Dedicated business

# Let`s ask the audience

- Have you used any cheats in the past?
- Have you cheated in a multiplayer game?

# Who they are?

- Creators (Hackers, Scripters)
  - Programmers
- Customers (Cheaters)
  - Users
  - griefers (Vandals)
  - Resellers (Copycats)

# How do they sell?

- Dedicated web sites
  - Artificial Aiming
  - Perfect Aim
- Advertising on forums and social media
  - Unknown Cheaters
  - Hacker Forums
  - Closed communities

# Legitimate Business?

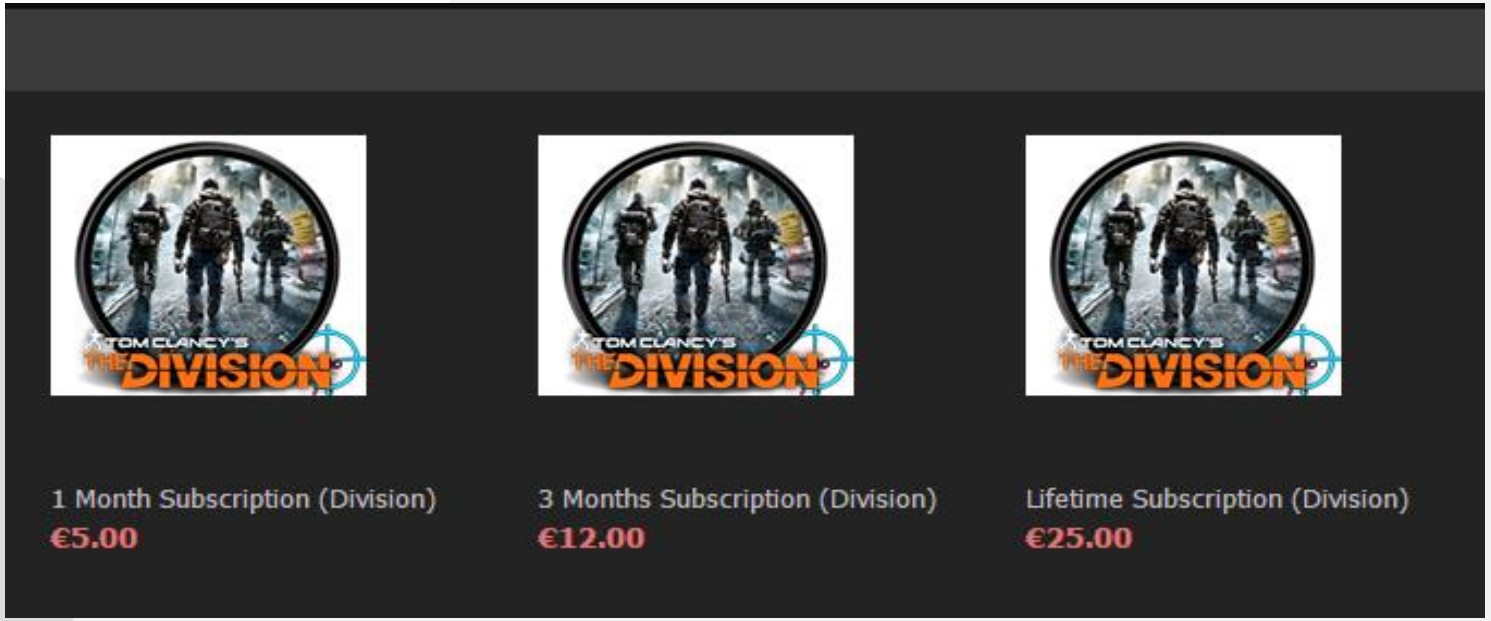
- Advertising
  - Youtube, Twitch, Twitter, Facebook
- Companies created
- Web presence
- Business model

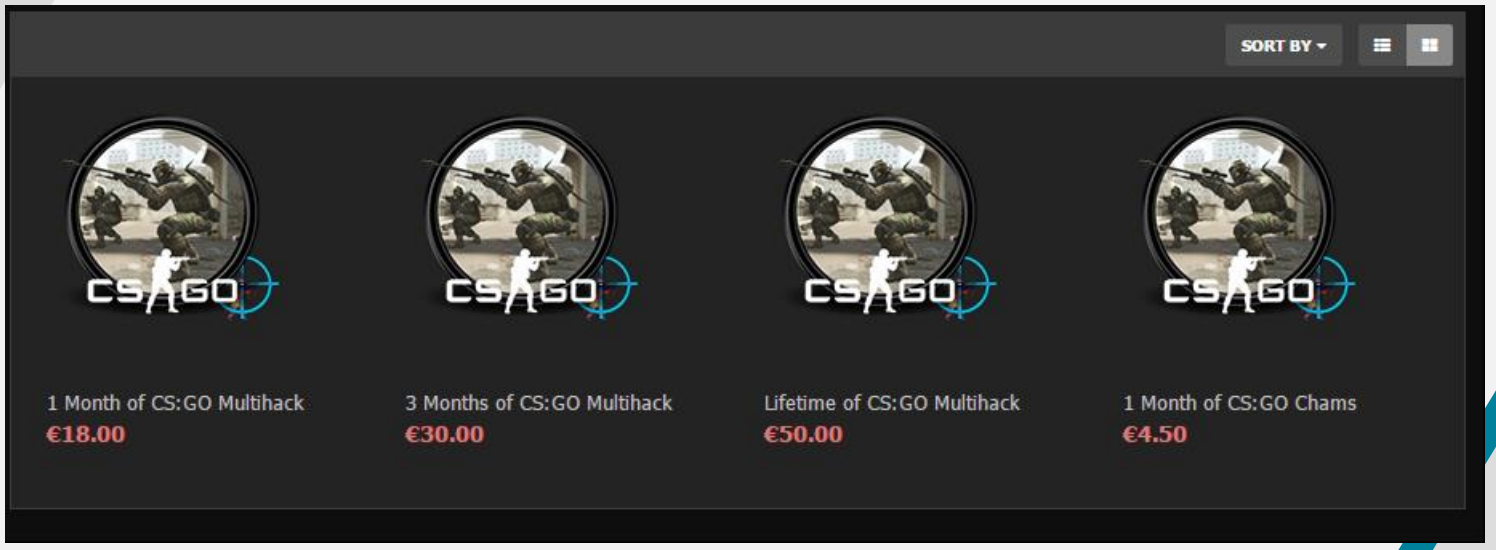
# Business Model

- Subscription model
  - Website
- Standalone purchase
  - IM (Skype, ICQ, IRC, VK, FB)
  - Forums (Private/Public)
  - Dedicated website

# What does it cost?

- Standalone purchase :
  - 1-500$
- Subscription model :
  - 1-25$ a month


1 Month Subscription (Division)
€5.00
3 Months Subscription (Division)
€12.00
Lifetime Subscription (Division)
€25.00


SORT BY
1 Month of CS:GO Multihack
€18.00
3 Months of CS:GO Multihack
€30.00
Lifetime of CS:GO Multihack
€50.00
1 Month of CS:GO Chams
€4.50

# Competition!

- What makes the difference
  - Features
  - Service
  - Reliability
  - Communication


Early Access Alpha
Version: 0.48.124737
Radar
Kamyshovo
Elektrozavodsk
Unconnected
Solnichniy
Zelenogorsk
Aimbot
Active
Humanize
Bones
Binds
Active
NoSway
Perfect
Priority
Field of View
ESP
Player
Loot
Animal
Radar
Active
Zombies
Names
Weapon
Distance
Skeleton
Box
Misc
Active
Fast Travel
Loot
Always Daylight
No Fall Damage
Display Server Name
DAYZ
Play
Character
Change server
Configure
Exit
Chods cheats
Unconnected
M4A1
3.9m
Copyright © 2013 Bohemia Interactive. Created by Dean Hall. All Rights Reserved.
23:12pm
Aimbot
ESP
Misc
Radar
Console

## FEATURES

### AIMBOT

- Autoshoot
- Deduct Recoil
- Aim Through Smoke
- Aim at Time
- Predict Lag
- Randomize Aim Spot
- Hitbox, Bone and Vector Positions
- FOV 0-180
- Smart FOV
- Keybind

### TRIGGERBOT

- Custom Timings per Weapon Group
- Keybind
- Delay (ms)
- Time to Attack (ms)
- Ground Stability (Running Speed m/s)
- Head Only

### ESP

- ESP active on sound
- Health
- Armor
- Skeleton
- Distance
- Name
- Show Team
- Spotted on Radar
- Weapon
- Weapon Clip
- Box
- Only Draw Visible
- Aim Spot
- Engine Glow
- Custom Glow Intensity
- Barrel Line
- Trails
- Helmet

## FEATURES

### CHEAT

- Friendly ESP (friendly NPC, animals, civilians)
- Enemy ESP (aggressive NPC, other players)
- Teleport to safezone
- Teleport to darkzone
- Teleport to custom location (COMING SOON)
- Anti-Fall
- Speedhack with customizable speed
- Noclip (You can speedhack through walls and go inside buildings)
- Flyhack
- Unlimited ammo
- External crosshair

### SECURITY

- Improved Security by PerfectSecurity™

## FEATURES

### ESP

- Enemy ESP
- Team ESP
- Draw Only Visible/Invisible or both
- Name
- Distance
- Skeleton
- 2D Box
- Snapline
- Engine Chams
- Custom RGB Colour Control

### MISC

- No Overheat
- No Recoil
- Instant (One hit) Kill

### OTHERS

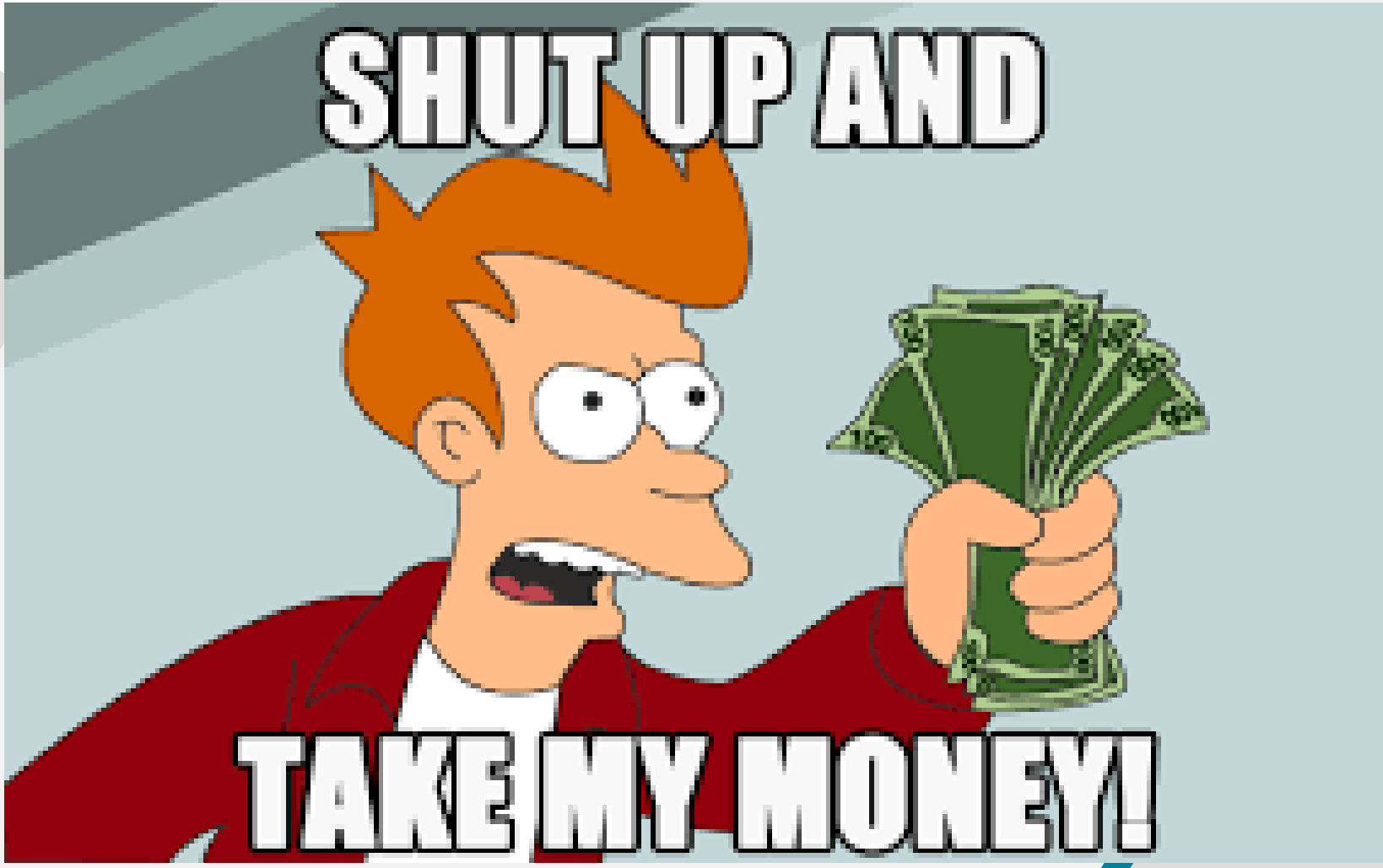
- Responsive and toggleable mouse GUI
- Supports borderless mode

# And a lot more!

Bohemia Interactive

# Buying Cheats is not so easy

- Public services vs Private services
- Precautions to limit leaks (Copycats or developers)
  - HWID lock (always online cheats)
  - Citizen ID
  - Skype Interview
  - Facebook/VK account check


SHUT UP AND
TAKE MY MONEY!

# Cheats in DayZ

- ESP (Showing or highlighting objects of importance in game)
- Item/player magnets (Remote execution of actions)
- Remote Damage
- Aimbots
- Speedhacks
- Server Crashes

# How Cheats Work

Bohemia Interactive

# How do they do it?

- Finding vulnerability vectors within the system
- Use of reverse engineering tools (IDA, Ollydbg, Wireshark)
- Building libraries or dedicated drivers and applications

# Where is it done

- PC
- Consoles
- Mobile
- So basically everywhere

# Breakdown

- Client-side local manipulation
- Server-side active attacks
- Attacks on other players in p2p systems
- Hardware and/or software hacks
- Botting/Automation
- Exploiting

# Client-side local manipulation

- Common base
- Internal/External hacks
- Most start with github projects
  - Xenos
  - Cheatengine

# Server-side active attacks

- Manipulation of transmitted data
- Way to go around server side checks
- Can be used outside of the client PC

# Why it works

- Bugs and/or exploits
- Lack of encryption
- Lack of server-side authentication
- Use of client-side authentication
- We still are in a world where we cannot run everything server side
  - Genre specific/design specific

# Protecting Your Game

Bohemia Interactive

# Approach

- Standalone application protecting the game process
- Proper architecture (server-client)
- Network encryption
- Stats based checks
- TOS ! (Banning licenses)
- Probably all of it together!

# RULES !

- Anything on the client can be and will be hacked
- Server side code is only as secure as the server

# Where we are at with DayZ

- Battleye – Standalone application
- Proper architecture (server-client) (WIP)
- Network encryption (WIP)
- Stats based checks (Not yet started)
- Probably all of it together!

# Where to start?

- Start buying cheats yourselves
- Reverse engineer them!
- Be proactive, use the same tools they do
- Start building a solid base
- Consider the features of cheats which harm your userbase the most

# Layered protection

- Prevention
- Detection
- Obfuscation
- Banning strategy
- Legal

# Prevention

- Standalone kernel driver (Battleye)
  - Kernel API (similar to antiviruses)
  - Hiding the process
- Proper architecture
- Legal
  - Scare tactics
  - Site takedown
  - Tax reports

# Detection

- Standalone kernel driver (Battleye)
  - Strings, Certificates, Patterns, Vector abuse, processes, Memory
- Stat based data and analysis
- Logging (Keep the history!)
- Sanity Checks

# Obfuscation

- Change code often (Client, Kernel driver)
- Use of binary/string obfuscation
- Use of VMs
- Ban waves
- Random ban times
- Waste their time <3

# Banning strategy

- Consider time based bans (options for rehabilitation)
- Consider Permanent bans
- Consider use of HWID bans (griefers)
- Ban waves
- Be mindful of false positives

# Some interesting numbers

- The number of bans usually floats around 1–2% of sold licenses (1.41% now for us)
- Look at your repeated offense rate if possible (72.09% now for us)
- VAC bans float around 1.5 %

# Banning, Legal and Community

Bohemia Interactive

# Who needs to get involved

- Legal
- Production
- Dedicated staff
- Programmers
- Build engineers
- Design
- Cheaters

# Roles – Legal

- Tax fraud reporting
- Protection of people involved
- Take down of sites
  - Legal notice
  - Contact the hosting service

# Roles – Production

- Keep your priorities straight
- Be mindful of what is hurting your userbase
- Be transparent
- Work with everybody involved

# Roles – Dedicated staff

- Start buying cheats
- Start being part of the cheating world
- Create fake identities
  - Use VPNs, Hosted servers
  - Physically separate network
  - Start building reputation

# Roles – Programmers

- Look at the architecture and changes needed
- Prioritize , there is a lot to do.
  - Server-side validation
  - Network Encryption
  - Client-Server Architecture

# Roles – Build Engineers

- Encrypt your data
- Obfuscate where you can
- Remove debug functions
- Don’t loose your source ;)

# Roles – Design

- Think about why people cheat
- How to change the systems design to close these holes
- Look at the data and think about how to rehabilitate.

# What else?

- Create feedback loop for people to report
- Create a competition for people willing to share security flaws
- Don`t taunt
- Don`t retaliate
- Try not to make it personal

# Q&A + please rate my presentation!

# Feedback is important.

Bohemia Interactive