Once a Cheater
always a Cheater,
Gotta catch `em All

Eugen Harton
Associate Producer & Bohemia Interactive

GDC 'Eu

GAME DEVELOPERS CONFERENCE™ EUROPE
CONGRESS-CENTRUM OST KOELNMESSE · COLOGNE, GERMANY
AUGUST 3-4, 2015

Cheating Bussiness (Analysis)

- What it is?
- Types of cheating
  - Exploiting
  - Cheating
  - Gear / Items
  - Services

Gotta Catch`em all ;)

- Unhackable game is a myth
- Question : Who out of all of you cheated?
    - Did you buy dedicated software?
    - Was it a multiplayer game?

Cheating Bussiness (Motivation)

- Who they are?
  - Creators (Hackers, Scripters)
  - Buyers (Cheaters)
  - Wannabes (Cheaters)
  - Griefers (Vandals)

Cheating Bussiness (Marketing)

- Peer Promotion (reputation building)
- Advertising (Youtube, Twitch, Twitter etc.)
- Social Engineering
  - Creating an enemy
  - Reputation
  - Features

Cheating Bussiness (Sellers)

- Who sells cheats?
- Subscription model / single buy
- Where do they get sold?
  - IM (Skype, ICQ, IRC etc.)
  - Forums (Private / Public)
  - Web portals

Cheating Bussiness (Revenue)

- How much does it cost?
  - 1-500 $ per cheat
- What makes the difference?
  - Features
  - Service
  - Reliability
  - Communication

Cheating Bussiness (Revenue)

- It is a full-time source of income
- Public services vs Private services
- Precautions to limit leaks
  - HWID lock (Online status required)
  - Citizen ID
  - Skype Call
  - Facebook/VK account check

Cheating Bussiness (Numbers)

- 1.39% of sold licenses are banned
- Cheaters rather stop playing than stop cheating (76.11% repeated offense rate)
- Total of 44 007 banned Accounts
- Public sector / Private sector

Cheating Bussiness (Numbers)

- VAC bans : 1.42% of total accounts
- Revenue for some of the public sites goes up to 1.25million $ a year.
- Public sellers in DayZ can go up to 40k $ a month
- Private sellers in DayZ can go up to 5k $ a month.

Cheating Bussiness (DayZ)

- Gear Selling
- ESP (player/item)
- Item/player magnets
- Remote damage
- Aimbots
- Speedhacks
- Server crashes

How they cheat (analysis)

- Differences in external / internal hacks
- Attack vectors within
  - Windows
  - Engine (client)
    - Script
    - Data
  - Anti-cheat

How they cheat (analysis)

- Memory manipulation and Library injection
- Common base (github)
  - Xenos (https://github.com/DarthTon/Xenos)
  - Cheatengine (https://github.com/cheat-engine/cheat-engine/
  - And More (reclass, MemorySharp, dllinjector...)

How they cheat (analysis)

- Dedicated application / driver
    - Direct memory manipulation
    - Abusing gameplay script
    - Patching the data and executable
    - Gameplay exploits

How they cheat (Analysis)

- Bypassing the protection
- Finding the right offsets
- Finding execution methods for gameplay script
- Combination with exploits and gameplay logic

How they cheat (analysis)

- What is the future?
- Drivers in VMs, possible use of bytecode.
- Controller hacks with direct access to memory (custom firmware)
- Dedicated hacking HW

How do we protect the game!

- Consider damage done to user experience
- EULA/ TOS
- Fair use
- Identify the core gameplay

How do we protect the game!

- Layered protection
  - Prevention
  - Detection
  - Obfuscation
  - Banning strategy
  - Legal

How do we protect the game!

- Prevention how?
  - Ring0 kernel agent
    - OB_callback routines
    - Dll Whitelist
    - Protecting the processes from hooks
    - Disable running of the game in Windows test mode
    - Etc.

How do we protect the game!

- Detection how?
  - Pattern detection
    - Strings (names, scripts etc.)
    - Certificates
    - Driver memory patterns
    - Bypass vectors (registry entries, unsp journal)
    - Process/Memory scanning
    - File Scanning

How do we protect the game!

- Protect the ring0 agent
  - From reverse engineering (VMProtect)
  - Remove parts of code, reintroduce them later
  - Live update
  - Use authoritative master server for detection and processing
  - Encryption
  - Byte code?

How do we protect the game!

- Client – Server Architecture
  - Extensive sanity checks
    - Consider performance and impact
  - Extensive logging
    - Keep history!
  - Don`t trust the client! Authoritative servers

How do we protect the game!

- Protect the data / executable
  - Make it harder to unpack
  - Make it harder to extract offsets (obfuscation)
  - Make it harder to identify functionality
  - Find the balance between performance/protection

How do we protect the game!

- Obfuscation!
  - Use client side checks as fake
  - Leave bypasses open to gather bans
  - Fake the detections when needed
  - Use ban waves
  - Use delayed bans
  - Waste time for the creator of the cheat

How do we protect the game!

- False positives
    - They do happen
    - Customer support
    - Be mindful
    - Better be safe than sorry

How do we protect the game!

- Banning (how & why)
  - Time based bans / Permanent bans
  - License based bans / game content bans
  - HWID / License / IP bans
    - Griefers and repeated offenders

Who needs to get involved?

- Legal
- Production
- Dedicated staff
- Cheaters

Who needs to get involved!

- Legal
  - Taking down the sites offering the cheats
  - Tax Fraud
  - Personal Harrasment
  - DDOS attacks
  - Make focusing on your game inconvenient for creators and let them move on.

Who needs to get involved!

- Production
  - Hire dedicated staff
  - Programmers, Community managers and cheaters
  - Involve the community through reporting

Who needs to get involved!

- Dedicated staff
  - Programmers
    - Focus on network/controller , authoritative client<server architecture
  - Community managers
    - Inflitrate the hack provider sites
    - Infiltrate hacking forums
    - Inflitrate private communites

Who needs to get involved!

- Community
  - Make friends!
  - Public reward systems
    - Focus on the creative cheaters
    - Get them payed for find the exploits
  - Public report systems
    - Reporting exploits/cheats/cheaters

Lessons to be learned

- Try not to make it personal
- Don’t retaliate
- Don’t taunt
- Be aware of the reprecussions

Open Questions!

- Ask away!
- Hopefuly I`ll be able to answer them! :