

# Cheating: The Malware for Video Games

**Tamás Boczán**  
Threat Researcher

**SOPHOS**

# Motivation

- Seen a lot of malware, started digging into cheats
- Cheat: Software for changing an **online**, competitive game real-time

# Motivation

- Seen a lot of malware, started digging into cheats
- Cheat: Software for changing an **online**, competitive game real-time



# Motivation

- Seen a lot of malware, started digging into cheats
- Cheat: Software for changing an **online**, competitive game real-time



# Motivation

- Seen a lot of malware, started digging into cheats
- Cheat: Software for changing an **online**, competitive game real-time
- Pretty similar to malware
  - Methods
  - Economy: cheat groups and anti-cheat companies - an arms race for 15 years
- Sophisticated solutions:
  - behind security industry, but comparable
- Topics
  - Why cheat?
  - How do cheats work?
  - How do anti-cheats work?

# Cheat Basics

- Online game:
  - Many players connected by a server
  - Mutual game state computed
- Cheater (attacker) is one of the players
- Goal: **unfair** advantage

# Anti-Cheat Basics

- ~10 anti-cheat solutions, by different companies
- Two components: on **server** and **client**
- Client component is compiled together with the game
- Inherent weakness: attacker has control over the client
- Heavy obfuscation: code and memory content
- Most of the cheat is for bypassing, small portion is the payload

# Why Cheat?

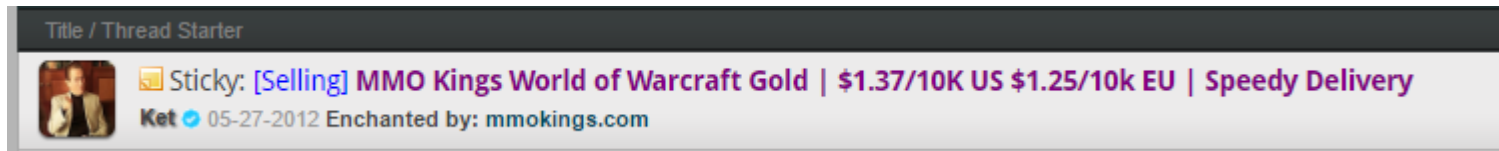


# Evolution of Attackers

- First for fun
- Industry grows
- Games go online
- Cheat for profit
- Anti-Cheat development

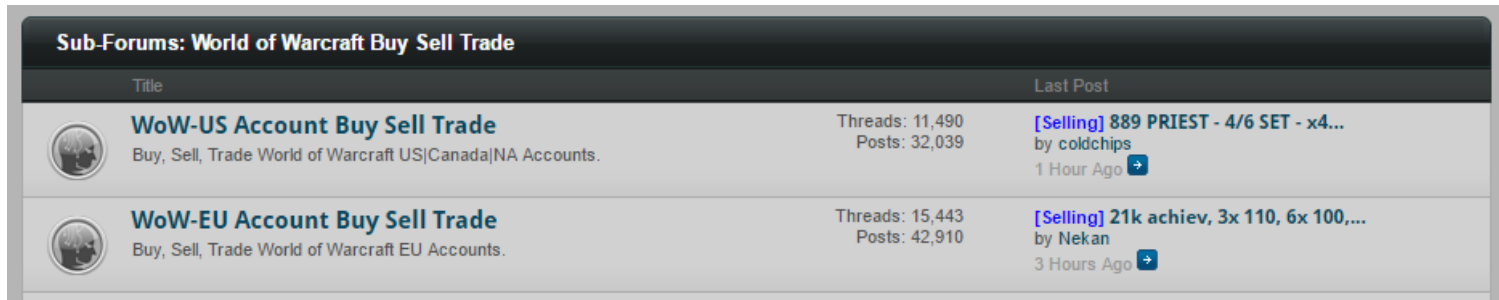
# An Ideal Platform



- Profitable
  - In-game money = Real money



A screenshot of a forum thread starter. The header reads "Title / Thread Starter". Below it, there is a user profile picture of a woman, a yellow sticky icon, and the text: "Sticky: [Selling] MMO Kings World of Warcraft Gold | \$1.37/10K US \$1.25/10k EU | Speedy Delivery". Below that, it says "Ket" with a verified badge, "05-27-2012", and "Enchanted by: mmokings.com".

- Accounts can be sold for up to \$5000



Sub-Forums: World of Warcraft Buy Sell Trade		
Title		Last Post
 <b>WoW-US Account Buy Sell Trade</b> Buy, Sell, Trade World of Warcraft US Canada NA Accounts.	Threads: 11,490 Posts: 32,039	[Selling] 889 PRIEST - 4/6 SET - x4... by coldchips 1 Hour Ago →
 <b>WoW-EU Account Buy Sell Trade</b> Buy, Sell, Trade World of Warcraft EU Accounts.	Threads: 15,443 Posts: 42,910	[Selling] 21k achiev, 3x 110, 6x 100,... by Nekan 3 Hours Ago →

- Options:
  - Win valuable things in-game
  - Steal accounts
  - Cheat as a Service

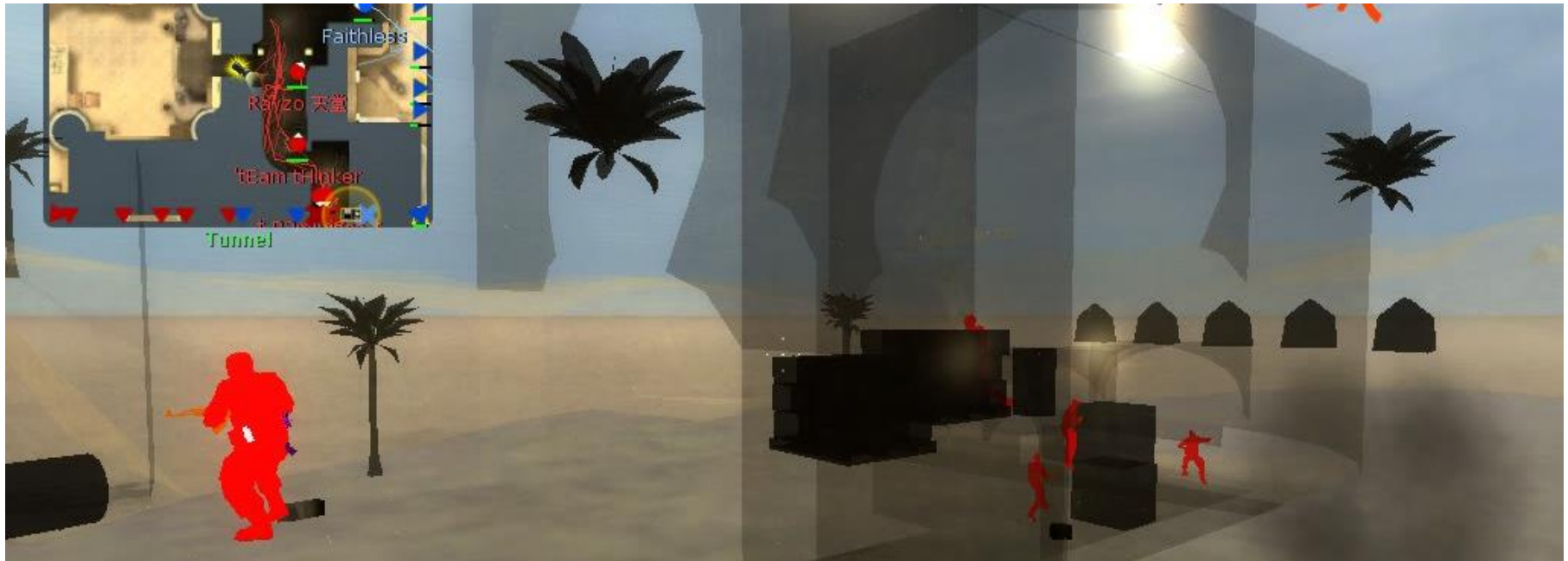
# An Ideal Platform

- Performance-sensitive environment
  - Players expect realistic look, instant reaction
  - Avoid network latencies: distributed computation, data from untrusted clients
- Legal grey zone

# Attacks

# Old Method: File Injectors

- **Change code on disk**
- E.g. make textures transparent to see through walls
- Not flexible, updates break it, easy to detect



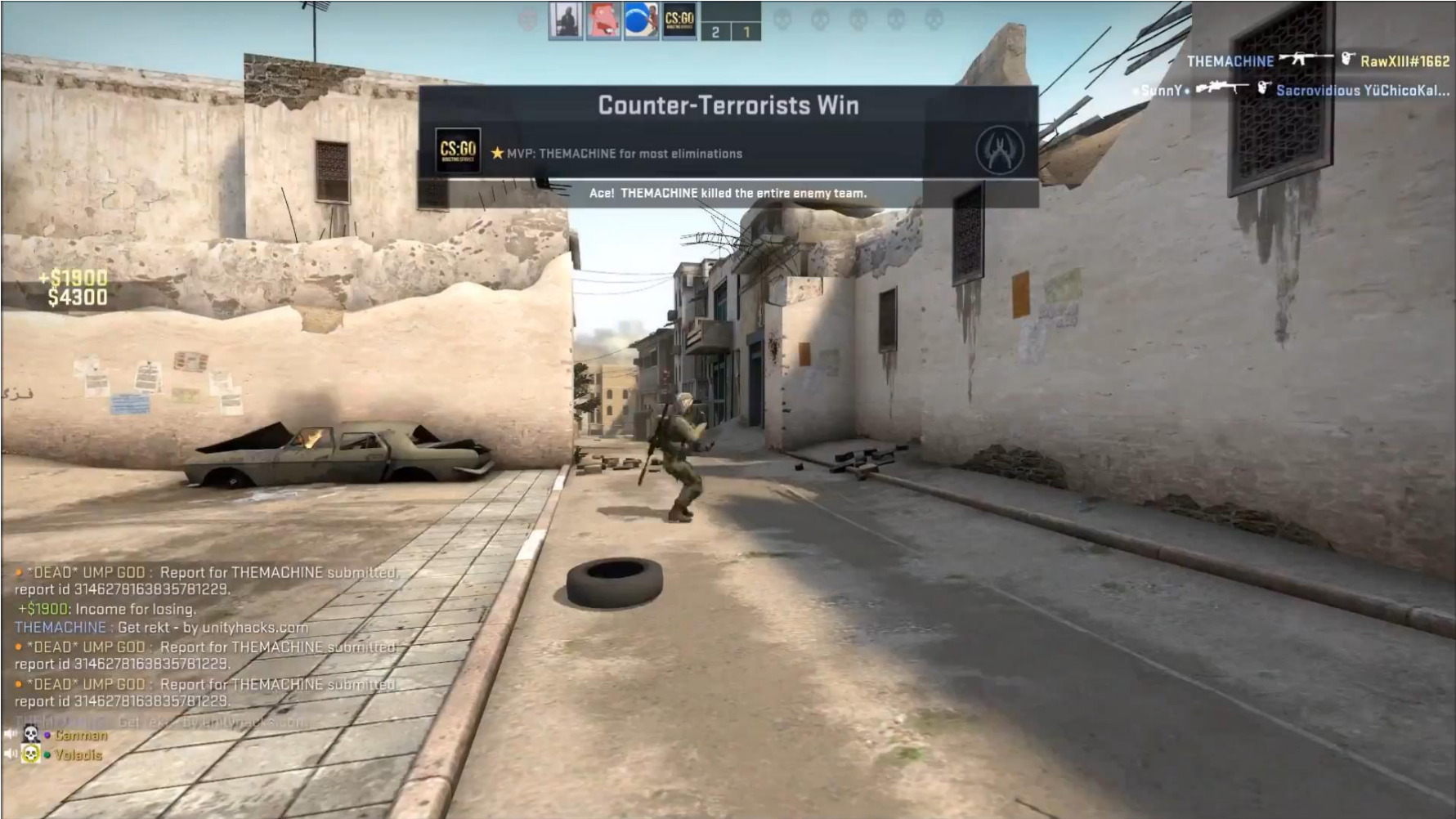
# Uncommon Method: MitM Attack

- Sniffs and modifies data **in transit**
- Often unencrypted, or key is easily accessible, unsigned packages
- Allows more advanced methods, like timestamp forgery
  - React before the event
- Need to implement large part of the game logic, not practical anymore

# Common Method 1: Injection

- Modifies game data or code in memory
- Easy and powerful after deobfuscation
  1. Access memory: DLL injection, or patching known loaded DLLs
  2. Find relevant structure
- Anti-cheat developers are focused on this

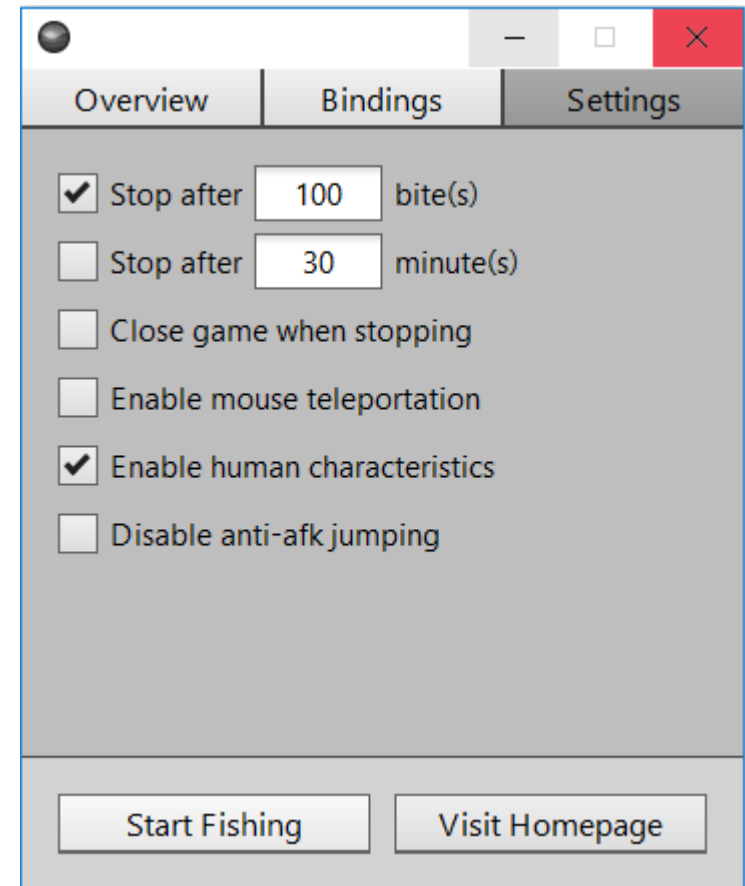
# Injection Example





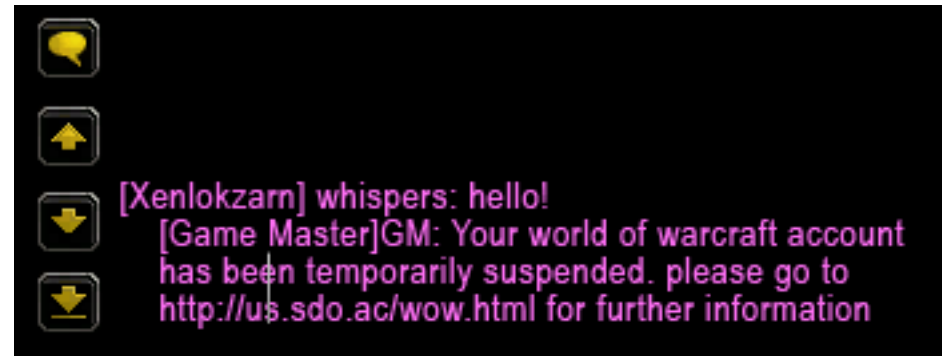
## Common Method 2: Bots

- In games where mechanical tasks are rewarded
- Goal: Online 24/7
- Sold as a service or used for Botnets
- Big difference in features
  - from fishing to complex quests
- Mitigated by behavior analysis



# Different Methods: Spam, Phishing

- Not cheat, but related
  - For advertisement or stealing accounts
- Communicate on in-game chat
  - No anti-spam solutions
  - Usually not mitigated at all



# Mitigations

# Client-side Component

- Responsibility: Supply useful data to the server
- Invasive approaches, spying
- Checks: periodical, on request by server, or on events
- Methods:
  - Dump all DLLs loaded in-game
  - Screenshot
  - Full memory scan
  - Title of all active windows
  - All running process names
  - Start of code section of all running processes
- Approach is mostly signature-based
- Heuristic detection for new cheats

# Server-side Component

- Responsible for convictions
- Flag accounts, bans them in waves
- Based on:
  - Data from the client
  - Player behavior
- Behavior-based detection in infancy
  - Distinguish cheaters from very skilled players

# Future of Anti-Cheat

- Role of behavioral analysis increasing
- Machine learning

# SOPHOS

Security made simple.