Hacking MMORPGs for Fun and Mostly Profit

Josh Phillips
Mike Donnelly

About Us

Josh

Real Life

- Kaspersky Lab Sr Researcher
- Virus Analyst at MSFT
- Named/Responded to Conficker

Underground

- Gold farmer
- Bot writer

About us

Mike

Real life

- Sold most commercially successful bot. Ever!
- Also got sued. Badly.

Underground

- What underground?
- Public record.

Goals

To suck or not to suck

- Briefly explain the history of game hacking and Real Money Trade
- Explain why we hack
- Provide a good overview of game hacking
- Provide a good overview of bot writing

“ **He who knows when he can fight and when he cannot will be victorious”**

Sun Tzu

Brief Legal Blurb

We are not lawyers but...

- Everything you know doesn't matter.
- Your clever legal ideas don't matter. Even if right.
- If you get sued, *you are fucked*.
- Avoid getting sued: run away, give up, offshore, offplanet, etc.
- Blizzard *will* show up on your door.

Disclaimer

We’re weasels

- Don’t try this at home, kids
- What you are about to see is true. The names and places have been changed to protect the innocent. (Us).

Why we hack

For the lulz

Money

- RMT
- Bot sales

Fame

- Street cred
- Wimmenz

Why we hack

For the lulz

Revenge

Cheating

Game Hacking 101

Yeah, I want to go to *that* school

Game Hacking 101

Tools of the Trade

- IDA
- Ollydbg
- Your favorite memory editor/searcher
- 010 Editor
- Wireshark
- Custom tools – you make them. Very key.

Game Hacking 101

Classification

Cheats

- Godmode
- Dupes
- Speed hack
- Extra powers
- etc

Bots

- PVP
- PVE
- Auction house
- Crafting
- Buffing

Game Hacking 101

Classification

Custom Client/Server

- RunUO
- Iris
- Mangos

Exploits

- Dupes
- Theft
- DoS

Game Hacking 101

Classification

Asset Hacks

- Map hacking
- Pathfinding

Game Hacking 201

Weeding the noobs

Game Hacking 201

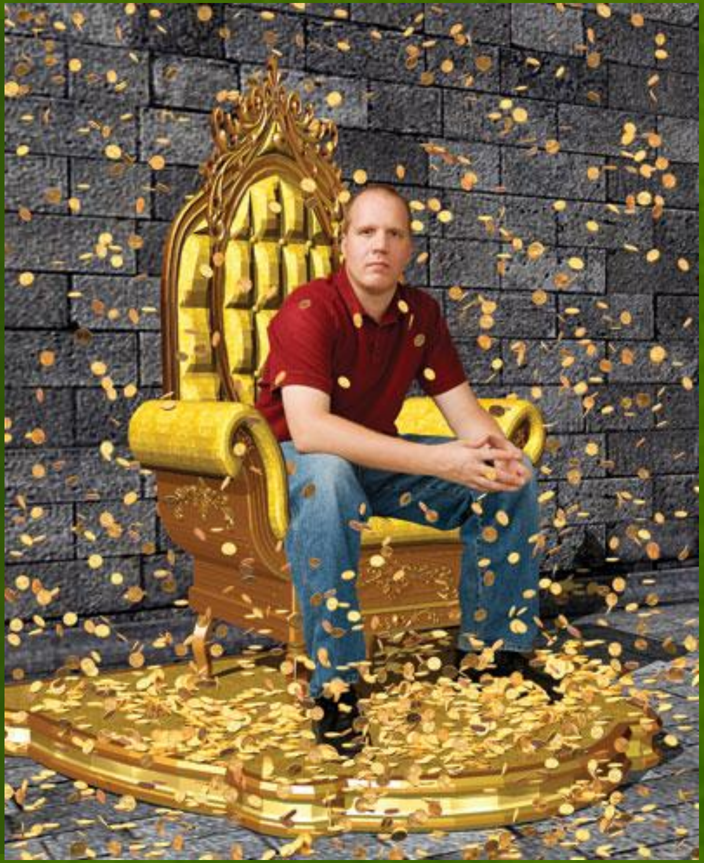
Required Skillset

- Learn C/C++
- Learn Intel assembly language
- Learn Win32 API
- Learn how to write drivers (Maybe)
- Noobs need not apply

Game Hacking 201

A craftsman and his tools

- Play with memory editing
- Locate key data structures
- Profit



Game Hacking 201

I put on my robe and wizard’s hat

- Memory searching is an arcane art
- Script engines are your friend (WoW/LUA, Eve/Python, Java/Darkfall).

Game Hacking 242

A history of ‘sploitin

Game Hacking 242

All your bits were belong to us

Ultima Online

- First major MMO
- Game hackers wettest dream
- Loads of open source servers
- Open source game client
- UOExtreme

WoW

- MMO for the masses
- Open source servers
- Legal action
- Ez-mode reversing due to LUA
- Huge number of players = big sales

Game Hacking 242

All your bits were belong to us

Eve Online	Darkfall
• Python	• 500k lines of Java

Game Hacking 242

All your bits were belong to us

Age of Conan

- Detailed debug strings

Aion

- Packed with Themida
- GameGuard

Game Hacking 242

All your bits were belong to us

Super powers

- Age of Conan
- WoW
- UO
- EQ
- Vanguard

Speedhacks

- Every game imaginable

Game Hacking 242

All your bits were belong to us

Dupes

- Age of Conan
- WoW
- UO
- EQ
- Vanguard
- Others

Teleports

- Every game imaginable

Game Hacking 303

Anatomy of a hack

Game Hacking 303

Poof

- Logic attacks
- Input validation attacks
- Integer over/underflows

Game Hacking 303

Poof

Teleport

- Overwrite players position
- Modify movement packets
- Ghost mode
- Client side hack, server side effects

Speedhack

- Modify CPU clock speed
- Modify players “run” speed
- Squeeze network to skip server code

Game Hacking 303

Poof

Dupes

- Server save logic attacks
- Vendor logic attacks
- Integer over/under flow conditions

Super powers

- Integer over/underflows
- Fall damage
- GM mode
- Stealing from NPCs

Game Hacking 303

Poof

UI hacks

- Camera Zoom
- Distance checks
- Language translation

Game Hacking 360

I’m in your base killing your mans

Game Hacking 360

Writing a Teleport hack

Easy ways

- WPM current player location
- Call game function responsible for repositioning player
- Is there a teleport spell? Use its code

Hard ways

- Forge movement packets

Game Hacking 360

Logic Attacks

- Substitute <unique id> in a packet for desired id.
  - Player trading attacks
  - Fall damage
  - NPC vendor attacks

Game Hacking 360

Item dupes

- Exploit the way world saves work
- Server line issues
- Repetition attacks

Game Hacking 360

Asset hacking

- Reversing file formats
- Really complex
- E.g. map modifications

Game Hacking 420

Icwutudidthar hur hur

“ Never was anything great achieved without danger.”

Niccolo Machiavelli

Game Hacking 420

Bots

Pixel reading

- Simple
- No RE required
- Super limited scope

Memory reading

- Simple
- Some RE required
- Limited scope (scope = attack surface!)

Game Hacking 420

Bots

Code injection

- More complicated
- RE required
- Increased detection surface

Dll Injection

- Detailed RE means more powerful code
- You are the game
- Easy to detect you
- Hooking

Game Hacking 420

Bots

Network/Packet	Custom Client
• Detailed RE required • Hard to detect depending on implementation	• Intense RE required • Full network protocol reversing • Skilled coding • Ultra profit

Game Hacking 515

Anti-anti cheat

“ Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness.”

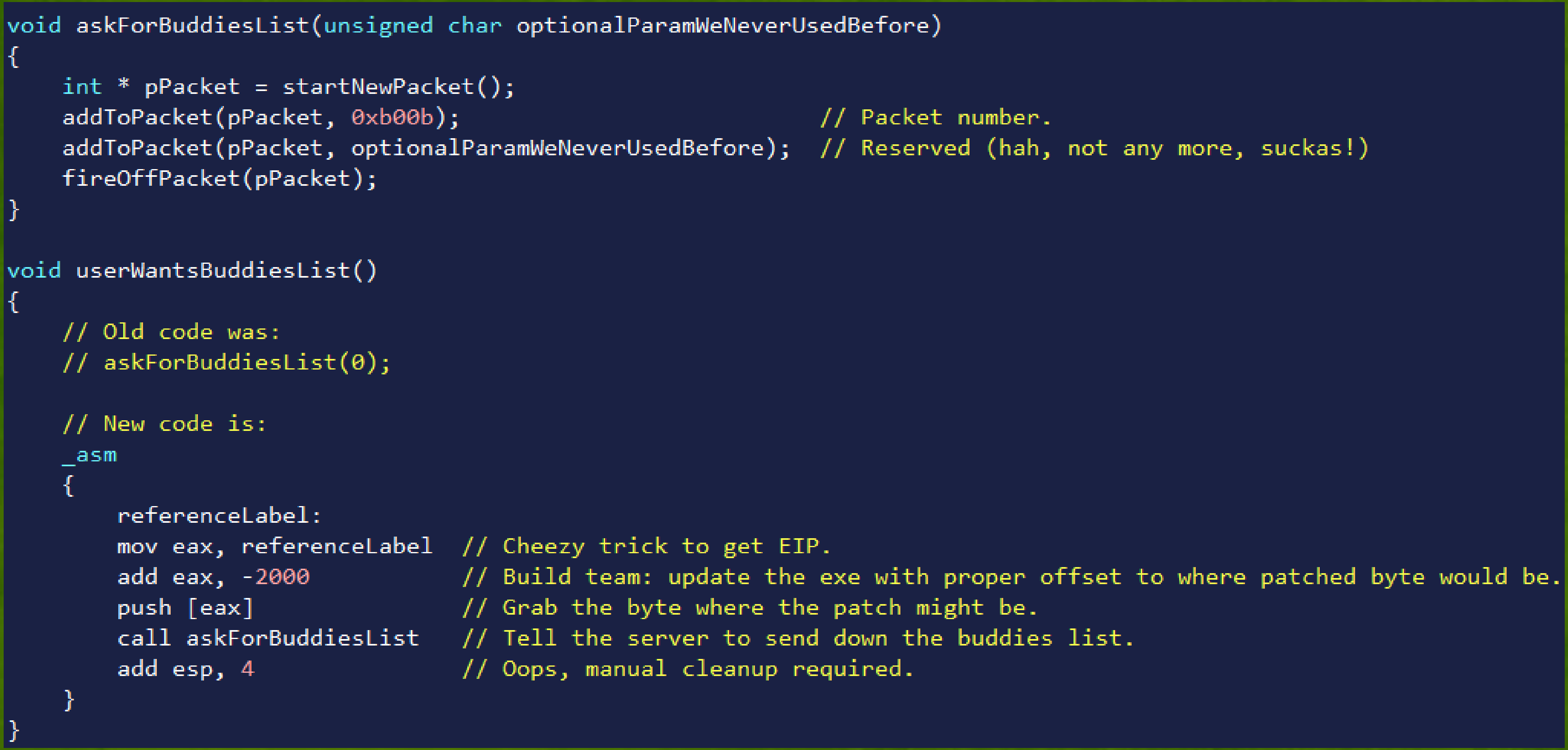
Sun Tzu

Game Hacking 515

Jedi mind tricks

- Tenet #1 of detection: attack surface
- Tenet #2 of detection: intelligence
- Attack surface affects intelligence!
- Attack surface is affected by features!

Client side attack surface



```
void askForBuddiesList(unsigned char optionalParamWeNeverUsedBefore)
{
    int * pPacket = startNewPacket();
    addToPacket(pPacket, 0xb00b);                             // Packet number.
    addToPacket(pPacket, optionalParamWeNeverUsedBefore);   // Reserved (hah, not any more, suckas!)
    fireOffPacket(pPacket);
}

void userWantsBuddiesList()
{
    // Old code was:
    // askForBuddiesList(0);

    // New code is:
    _asm
    {
        referenceLabel:
        mov eax, referenceLabel  // Cheezy trick to get EIP.
        add eax, -2000           // Build team: update the exe with proper offset to where patched byte would be.
        push [eax]               // Grab the byte where the patch might be.
        call askForBuddiesList   // Tell the server to send down the buddies list.
        add esp, 4               // Oops, manual cleanup required.
    }
}
```

Game Hacking 515

Client side intelligence gathering

- Detection code all in one spot? Easy.
- Detection code sneaky in client? Not so easy.
- Knowing what is going on is *very* difficult.
- Knowing what is going on is *very* valuable.
- More attack surface makes this job harder.
- Intelligence gathering in your product will be tricked.
- Don't be lazy.

Game Hacking 515

Overcoming anti-cheats

Client side

- Obfuscation
- Memory Validation
- Debugger detection
- Injected Dll detection
- Unpacking

Server side

- Data mining
- Validation of packets

Game Hacking 515

Overcoming anti-cheats

Client/Server side

- Warden
- Punkbuster
- Like a C&C

Game Hacking

Post doctoral research

Advanced Game Hacking

Post doctoral Reseach

Automation

- Dealing with game updates
- Fully automated game play
- Automated delivery systems

RE Knowledge

- Full structure recovery
- Vtable recovery
- Plugin API
- Seamless integration

Advanced Game Hacking

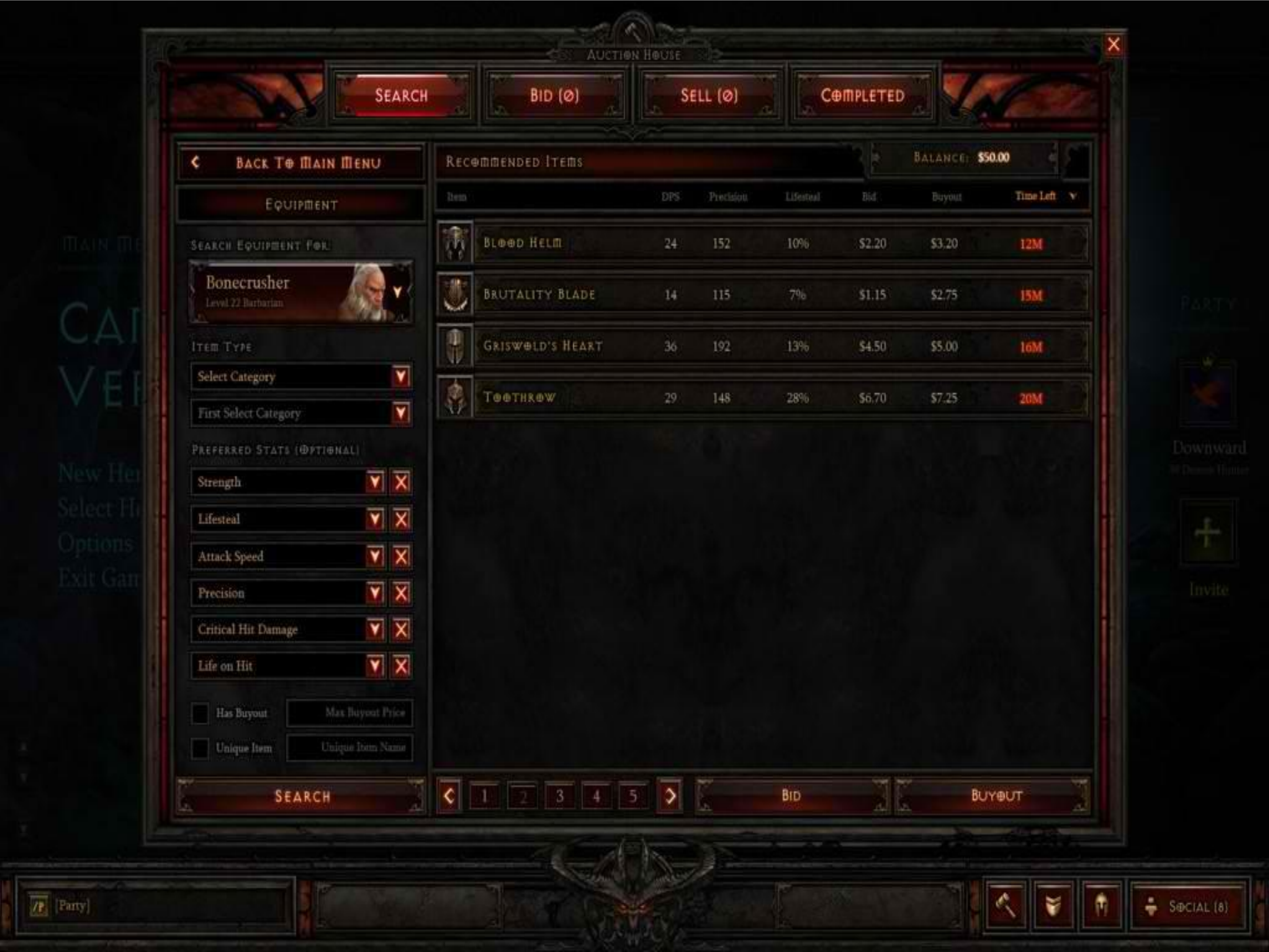
Post Doctoral Research

Frameworks

- RE libraries
- Bot skeletons
- etc

Profit

- RMT
- Bot sales
  - Private
  - Public



Search Equipment For:

Bonecrusher
Level 22 Barbarian

Item Type

Select Category

First Select Category

Preferred Stats (Optional)

Strength

Lifesteal

Attack Speed

Precision

Critical Hit Damage

Life on Hit

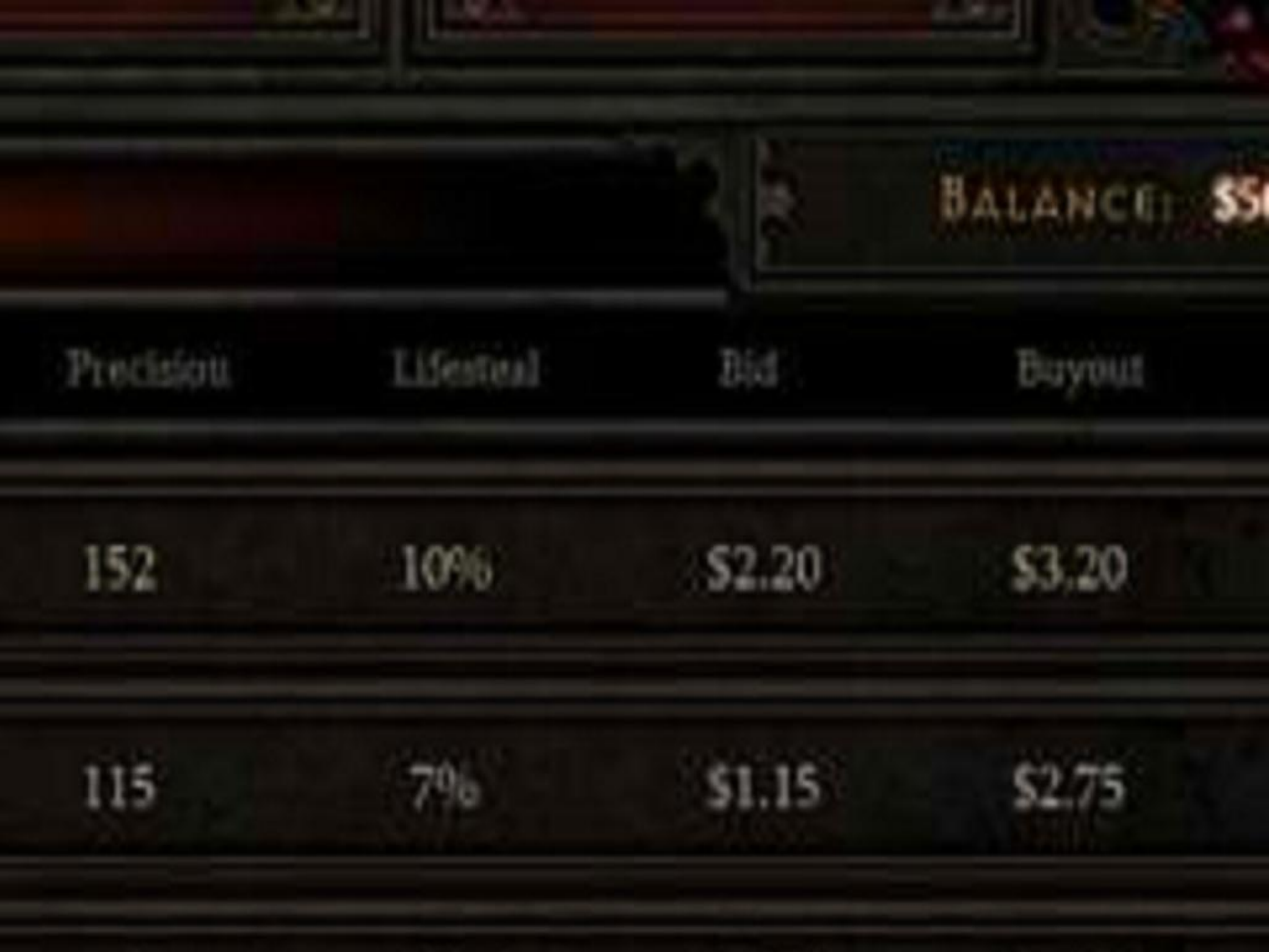
□ Has Buyout — Max Buyout Price

□ Unique Item — Unique Item Name

Recommended Items

Balance: $50.00

Item	DPS	Precision	Lifesteal	Bid	Buyout	Time Left ▼
Blood Helm	24	152	10%	$2.20	$3.20	12M
Brutality Blade	14	115	7%	$1.15	$2.75	15M
Griswold's Heart	36	192	13%	$4.50	$5.00	16M
Toothrow	29	148	28%	$6.70	$7.25	20M



BALANCE: $5

Precision	Lifesteal	Bid	Buyout
152	10%	$2.20	$3.20
115	7%	$1.15	$2.75

Buyout

$3.20

Greetz to all our friends in PL, DE, NZ and OZ

Thanks

raindog@macrohmasheen.com
miked@mdyindustries.com