Exploiting Online Games

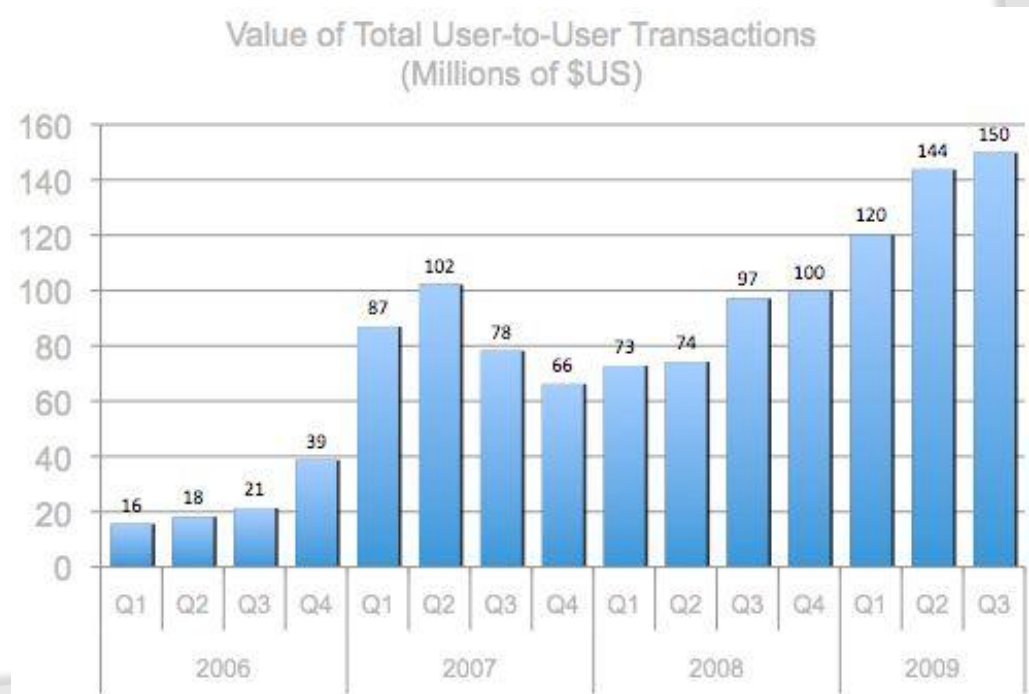# What is Second Life ?

- Free online Virtual World.
- MMOG (Massively multiplayer online game)
- User-Generated content
- Open Source viewer (Client)

Economy in Second Life

- Linden Dollars (L$)
- Exchangeable for US Dollars ($$$)
- 4 Main industries
  - Real Estate
  - Adult Entertainment
  - Fashion
  - "Weapons"

Value of Total User-to-User Transactions (Millions of $US)

	Q1	Q2	Q3	Q4
2006	16	18	21	39
2007	87	102	78	66
2008	73	74	97	100
2009	120	144	150	

CTV

Weapon Industry in SL

- User-Generated "Weapons"

- Scripted Objects in LSL (Linden Script Language)

- Uranium HUD (Heads up display)
  - Protect
  - Trap
  - Lag
  - Basically annoy..

NooB Trap!
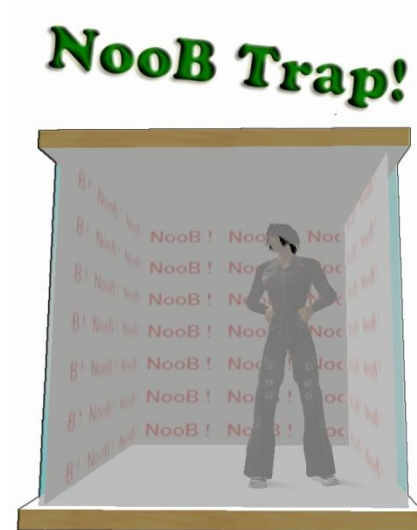
ranium HUD 2

- +55 modules shields and features
- User friendly interface
- Enemies and Friends list
- Teleport all friends list in one click
- Auto attack enemies
- "-FPS" The most advanced attack in SL
- Fits anywhere on your screen
- Sound and Particle attacks
- Orbit in no push & Orbit in no rez
- Full sim avatar scanner
- Instant damage kill in damage zones
- Works in no rez no push zones

- Free updates
if you have the old version of the HUD, please send a notecard to 'Zane Oxidor' to get the new version for free

LAG BOMB

```
integer active = FALSE;
list sounds = [
    "093ae619-8342-e532-0a65-0e093d8cf228", "2717ac73-e702-b64e-2cf1-f9ddc45822d7",
    "58df4841-927f-b26a-73e4-e71ebcdf6c10", "064936e9-2c84-2c25-331c-a618a4d87ab3" ];
default {
    state_entry() {
        llListen(-555, "END Button", "", "");
        llListen(-956, "LAG BOMB Button", "", "");
    }
    listen(integer channel, string name, key id, string message) {
        if(llGetOwner() != llGetOwnerKey(id)){} //Verify owner item that talked
        else {
            string target = llGetSubString(message, 4, 35); //Gets target from msg
            if (target != message && channel == -956) {
                active = TRUE;
                llSensorRepeat(target, "", AGENT, 96, PI,0.001); //Max 96 meter
            }
            if(message == "END" && active == TRUE) {
                llSensorRemove();
                active = FALSE;
            }
        }
    }
    sensor(integer num_detected) { // Loops every 0.001 seconds
        llTriggerSoundLimited(
            llList2Key(sounds,llFloor(llFrand(llGetListLength(sounds)))), 0.05,
            llDetectedPos(0) + <0.5,0.5,0.5>, llDetectedPos(0) - <0.5,0.5,0.5>);
    }
    no_sensor() { // Target not found, stop looping
        llSensorRemove();
    }
}
```

Exploiting Second Life
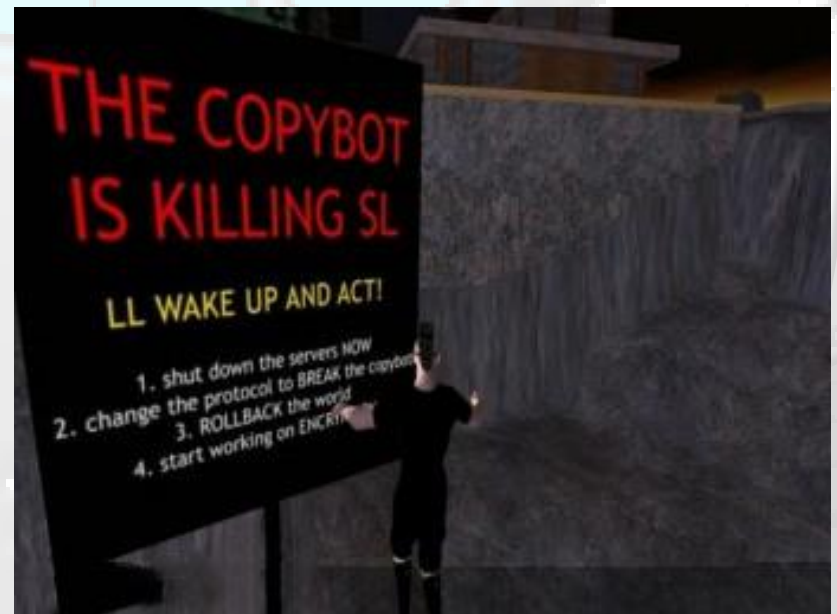
iLife Viewer Highlighted Features

- Crash other clients
- DDoS other clients
- Encrypted IM's between iLife users
- Spoofs MAC address & Hardware Serial
- Free Uploads
- **Steal ANY user-generated content !!! (CopyBot)**

Second Life CopyBot

- Developed in 2006 by reverse engineering Second Life protocol (External Bot)
- Main purpose was "Backup" tool
- Became popular

Fly Everywhere Code Example

```cpp
// Does this parcel allow you to fly?
BOOL LLAgent::canFly()
{
    // Gets the region we are on
    LLViewerRegion* regionp = getRegion();
    // If region blocks flying return FALSE
    if (regionp && regionp->getBlockFly()) return FALSE;

    // Get the current parcel we are on
    LLParcel* parcel = LLViewerParcelMgr::getInstance()->getAgentParcel();
    if (!parcel) return FALSE; // If the parcel is null return FALSE

    // Allow owners to fly on their own land.
    if (LLViewerParcelMgr::isParcelOwnedByAgent(parcel, GP_LAND_ALLOW_FLY))
        return TRUE;

    return parcel->getAllowFly();// Return if the current parcel allows fly
}
```
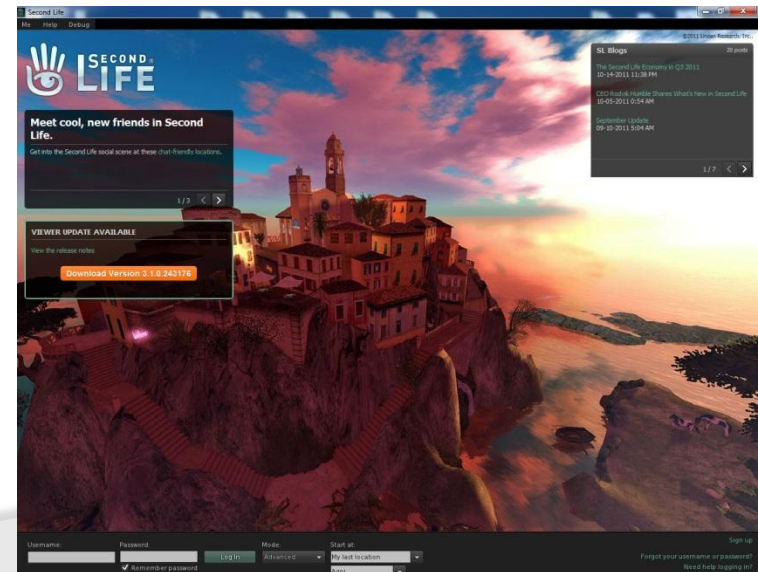
Fly Hack

```
// Does this parcel allow you to fly?
BOOL LLAgent::canFly()
{
    return TRUE; // Owned :)
}
```

Linden Lab wakes up !

- Banned over 10,000 Residents
- Logging Clients activity
- New Third-Party viewers policy
- Released **Second Life Viewer 2**

Final Results

Comment(s): Hello,

We regret to inform you that Linden Lab has terminated your access to the Second Life virtual world. Because you have severely or repeatedly violated the Second Life Terms of Service or Community Standards by committing permissions abuse, your account and any alternate Second Life accounts are now permanently inaccessible.

What is Linden Lab's policy on permissions abuse?
According to the Second Life Terms of Service and Second Life Community Standards, circumventing the permissions system to obtain rights not intended by the creators of inworld objects, scripts, textures, notecards, or other items is prohibited. The use of CopyBot, any other external application or other methods employed to violate the permissions system to make unauthorized duplicates within Second Life will be treated as a violation of Section 4.2 of the Second Life Terms of Service.

Thank You !

danpeleg1@gmail.com

Links:

- secondlife.com/
- en.wikipedia.org/wiki/Economy_of_Second_Life
- Second-Life-Economy-Third-Quarter-2009
- The-Second-Life-Economy-in-Q3-2011
- wiki.secondlife.com/wiki/Source_downloads
- en.wikipedia.org/wiki/CopyBot
- danpesolutions.blogspot.com