JAN 31, 2019 - 3 MINUTE READ - COMMENTS - GAME HACKING SOAPBOX

Cheating at Moonlighter - Part 4 - Defense

I am going to talk about defense. This is a mainly non-technical post. It's a bit different from other posts on this topic and in general. With the existence of a trainer and the debug HUD, I decided to can the idea of using Cheat Engine on Moonlighter.

Other parts:

- Cheating at Moonlighter - Part 1 - Save File
- Cheating at Moonlighter - Part 2 - Changing Game Logic with dnSpy
- Cheating at Moonlighter - Part 3 - Enabling Debug HUD

Who am I?

I am Parsia, a security engineer at Electronic Arts.

I write about application security, reverse engineering, Go, cryptography, and (obviously) videogames.

Click on About Me! to know more.

Collections

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Defending Against Save Game Edits

I was recently asked

> *Assume we have a single player game that uploads the save game to the cloud every hour. How can we detect these edits?*

It's not really possible. Anything you can collect from the machine can be tampered with. Unlike a multiplayer game where the server has access to raw data. You can't trust anything collected from the client.

- Let's say we collect a log of events happened in the game and then upload it with the save game to detect discrepancies.
  - The player can edit the events.
  - The player can cut the internet connection to disrupt the sync. You cannot really make people have to be online all the time to play a singleplayer game.

I see the same thing at work. Client-side encryptions and controls can be defeated.

What can we do?

We can detect some anomalies. Things like level and grind gates are very common in RPG games and can be used in our favor.

- If the player has an item that drops in level 4 of the dungeon but the game progress only marks the 1st level boss kill, then this is an anomaly.
  - The player can modify the save game/events to indicate that progress.
- If the player has suddenly gained 10 million gold (see our initial gold edit) between syncs, then it's probably a cheat.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

    - The player can modify the save game before the sync to show a small number.

We can run anti-cheat measures

- This can only slow down attackers. It can and will be defeated.
- Again there's no way to report cheating if there's no internet connection. When dealing with Moonlighter, I used a Virtual Machine with no internet access and Steam offline mode.

Defending Against Game Logic Manipulation

In the case of Moonlighter or other Unity Games, it's easy. Unity DLLs can be decompiled from CIL and modified. It's a problem managed code (and Java bytecode) have.

- We could use obfuscators, anti-debuggers, etc.
    - These just slow down the process.
- We could check the integrity of game files through hashes and signing.
    - It's a client-side control that can be defeated.
- We could use native code.
    - Modification will be harder but still possible.

What's the Point?

You could argue that a singleplayer game is not worth it. Who cares if players cheat at Moonlighter? Why should we even care? We don't.

Posted by Parsia • Jan 31, 2019 • Tags: Moonlighter

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD

Cheating at Moonlighter - Part 3 - Enabling Debug HUD

path.Join Considered Harmful

0 Comments Parsiya

1 Login

♡ Recommend Tweet Share

Sort by Best

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

Subscribe Add Disqus to your site Disqus' Privacy Policy DISQUS

Copyright © 2019 Parsia - License - Powered by Hugo and Hugo-Octopress theme.

Create PDF in your applications with the Pdfcrowd HTML to PDF API PDFCROWD