Ruby 1.8 - Bug #6438

Ruby Queue in thread before fork causes segfault on GC

05/16/2012 05:36 AM - slyphon (Jonathan Simms)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	Ruby 1.8.7
ruby -v:	ruby 1.8.7 (2012-02-08 patchlevel 358) [i686-darwin11.3.0]

Description

After many hours of debugging (with immeasurable help from Eric Lindvall), I've come across a pretty nasty bug in MRI 1.8.7 that affects p249-p358 on linux and OSX.

Eric came up with this reproduction:

```
require 'thread'
50.times { Thread.new { Queue.new.pop } }
Process.waitpid fork { GC.start; puts "In child: #{$$}" }
```

produces the output:

```
/tmp/fork-crash.rb:3: [BUG] Segmentation fault
ruby 1.8.7 (2012-02-08 patchlevel 358) [i686-darwin11.3.0]
```

More specifically, this seems to be a problem with a Thread waiting on a ConditionVariable when you fork

```
require 'thread'
50.times { Thread.new { m = Mutex.new; c = ConditionVariable.new; m.synchronize { c.wait(m) } } }
Process.waitpid fork { GC.start; puts "In child: #{$$}" }
```

produces the output:

```
/tmp/mutex-crash.rb:3: [BUG] Segmentation fault
ruby 1.8.7 (2012-02-08 patchlevel 358) [i686-darwin11.3.0]
```