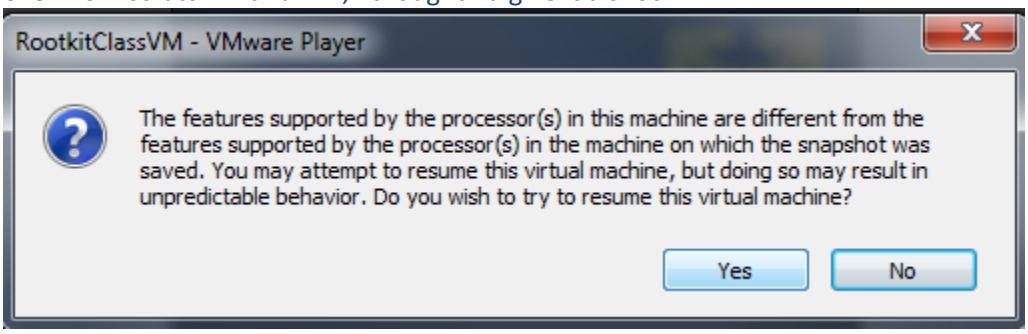
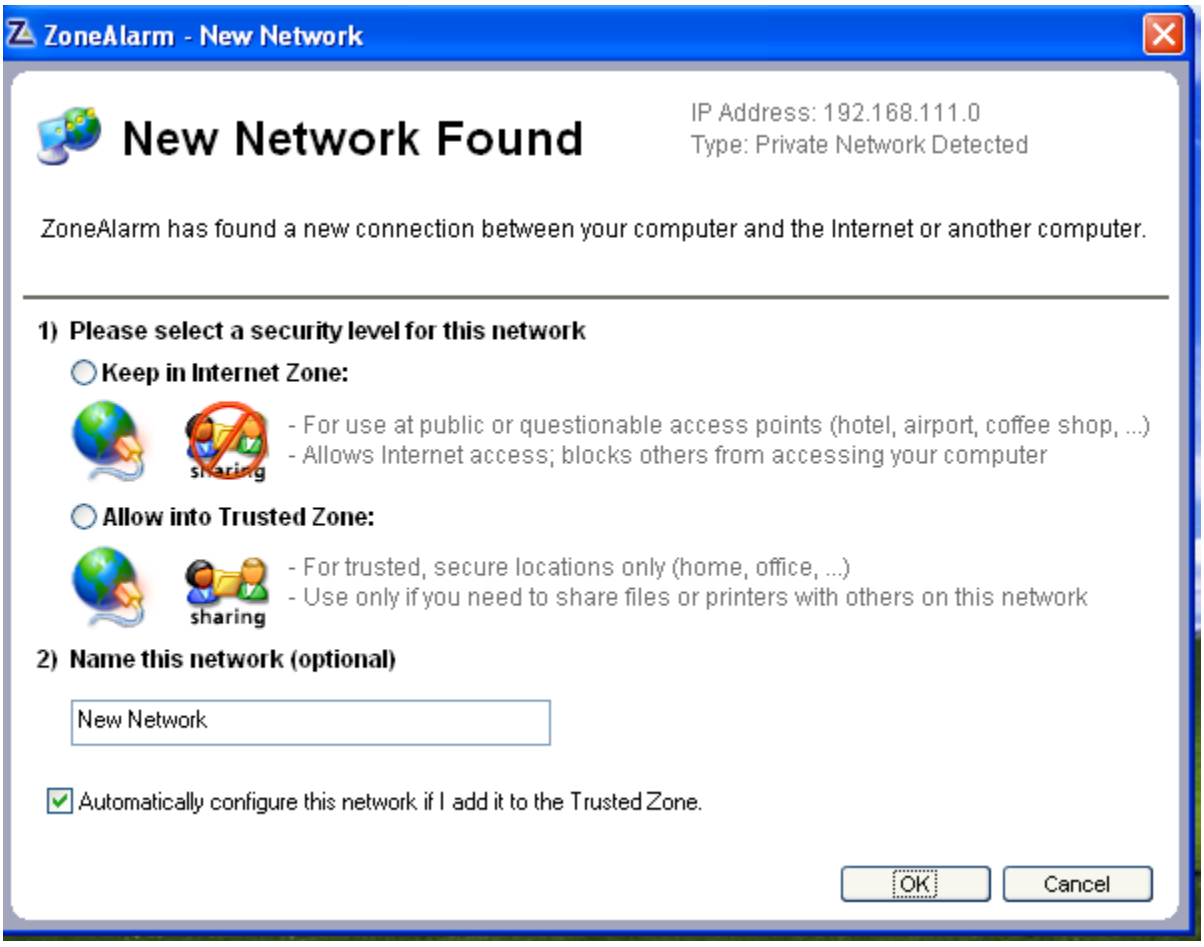
First attempted booting it up using VMware Player 3.1.4 build 385536, since I already had it available on my machine. It complained that the processor features didn't match, but since it's easy enough to start over from scratch with a VM, I thought I'd give it a shot.

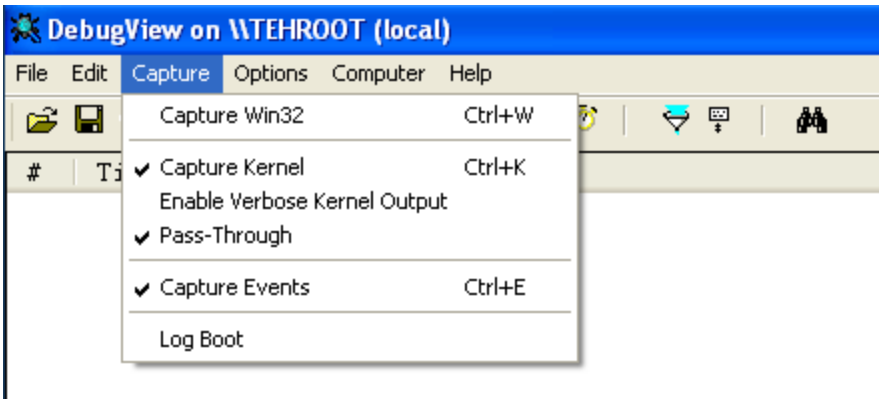



Zone Alarm found a new network:



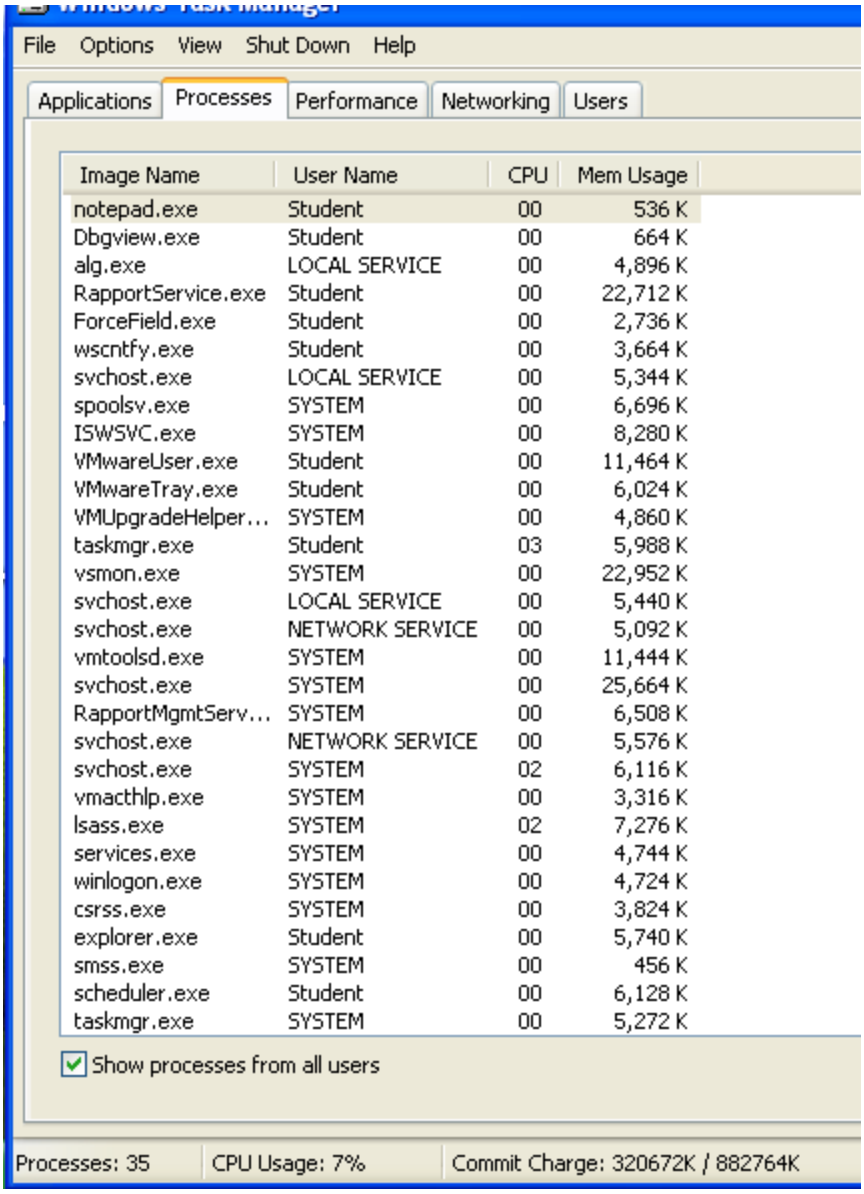

Left it in Internet Zone for now.

Also running was the following. It looks to be capturing the kernel and Events, but not Win32.



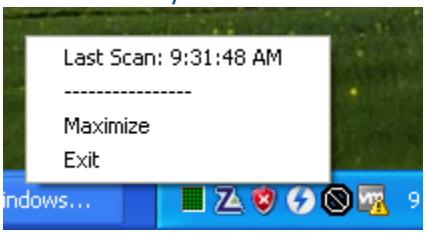

The HD and CD lights are both going off with some regularity. Also the mouse seems a little jumpy. May not be related. (Update: Mouse probably related to outdated VMware Tools. When the mouse jumps, the VM loses focus.

The C:\temp folder was moved into the recycle bin. It looks like it contains one executable claiming to be an IE8 patch. It has KB982381 in the file name, which does match an IE patch from MS.

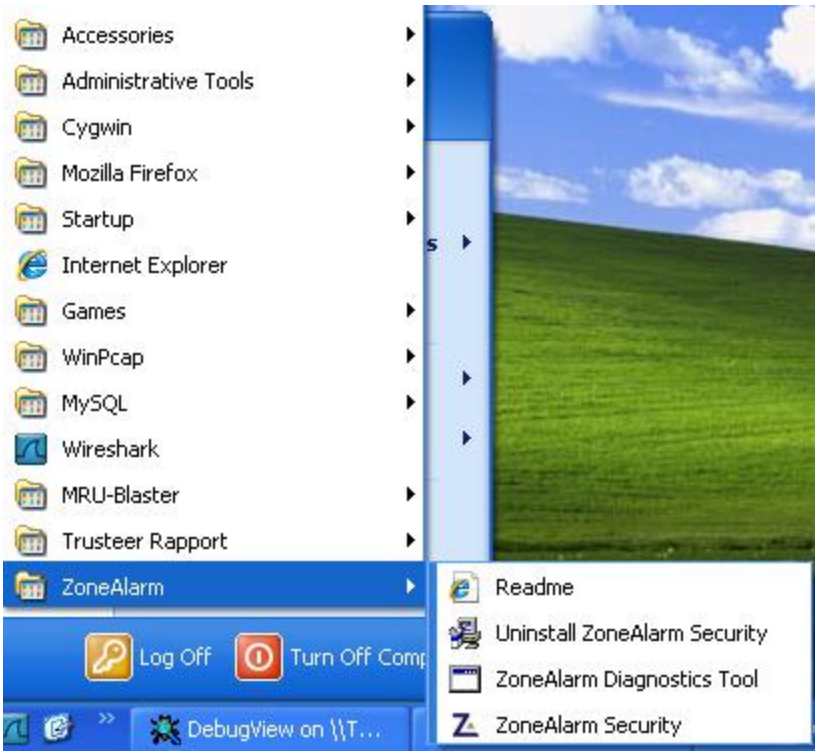



Only 35 processes listed.
ForceField looks suspicious. (Update: Part of ZoneAlarm)

In the task tray we have MRU-Blaster




Since it cleans out the most recently used list, that will limit our ability to see recent activity.




The Vanquish rootkit has an installer on there:

C:\vanquish-0.2.1

File Edit View Favorites Tools Help

ReadMe.txt - Notepad

File Edit Format View Help

```
************************************************************************************
*                                                                                  *
*                                 Vanquish v0.2.1                                  *
*                                                                                  *
************************************************************************************
            *                                                                *
            *  Copyright (c)2003-2005 XShadow. All rights reserved.          *
            *                                                                *
            ******************************************************************

                              *** USE AT OWN RISK ***


What's new
====================
     WARNING THIS IS NOT AN OFFICIAL VERSION. THIS IS AN INTERMEDIATE
VERSION THAT FIXES THE WIN2K REGISTRY PROBLEMS.

Installation/Removal
====================
Simple: copy the files to a folder on your HD and then
        double-click setup.cmd and follow the instructions from there.

Please note that setup.cmd is a wrapper to installer.cmd that allows it to
detect vanquish even if it is installed. So no other commands are needed
before issuing a setup command.
Also, take great care for path entries. On my system, typing 'setup' in a
command prompt -- besides the folder with vanquish -- runs setup.exe from
c:\windows\system32 because it is in the current path.

As a side note, vanquish was designed to run with **Adminstrator** privilege.
Please, before mailing that vanquish doesn't work check that you have this
privilege, and that you installed vanquish as Administrator.
Also, vanquish cannot run concurrently with other API rewriting apps(rootkits).
```

Following the instructions listed in the Readme, I was able to verify that Vanquish is installed:

C:\WINDOWS\system32\cmd.exe

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\user>cd C:\vanquish-0.2.1

C:\vanquish-0.2.1>setup.cmd do install
************************************************************************************
*                                                                                  *
*                                 Install Vanquish                                 *
*                                                                                  *
************************************************************************************

Checking for previous version...
Vanquish is already installed. Please remove first.
Press any key to continue.

C:\vanquish-0.2.1>exit

C:\vanquish-0.2.1>
```

At this point, I would recommend decommissioning the system and starting with a fresh image. Hopefully this course will provide additional tools for mitigating compromised systems.

Other Candidates:
Shadow Walker (hides itself from being read in memory)
There are almost certainly other nasties hiding like this, but I'm not sure how to find them.

Checked for AppInit_DLLs injection