Rootkit Investigation Summary
Date Submitted; April 3rd 2011

**Brief Summary:**

The following rootkits were detected:

1. Vanquish
2. FU
3. HackerDefender
4. Ctl.exe
5. Fat.bat, (and related files)
6. Sysenter.sys
7. Ctr12Cap.sys
8. Basic.sys
9. He4HookInv.sys

**Files Removed:**

*The following files were in c:\Windows\system32\drivers

1. Sysenter.sys
2. Ctr12Cap.sys
3. Basic.sys
4. The _cool_beans directory was hidden, but there was nothing in it which was weird. It's not malicious as far as I can tell, but it was being hidden by malicious programs so I deleted it to be on the safe side.
5. Fu.exe

*The following files were in C:\Windows\

1. fat.bat
2. fat.vbs
3. fat_init.bat
4. vanquish.exe
5. vanquish.dll

*The following files were in C:\Windows\system32\

1. He4HookInv.sys – Got lucky and saw this one when eyeballing the dir results. Noticed it's install date was 6:35 PM 11/02/2002
2. Ctl.exe

*The following files were in C:\

1. Deleted the entire vanquish d-0.2.1 directory along with vanquish.log
2. Deleted the entire hxdef100r directory

*The following files were in C:\Windows\tasks\

1. Ctl1.job
2. Ctl2.job
3. Ctl3.job

**Cleanup on the running system:**

1. Used Windows autoruns to stop Windows from attempting to load the deleted drivers and scripts
2. Checked the browser extensions for IE. I disabled the following services:

a. {C95FE080-8F5d……}
b. I also disabled Diagnose Connection Problems, and Windows Messenger since they did not have a publisher associated with them, and I doubt that they would be missed by a user if they are legitimate

**Cleanup left to do:**

There are a lot of registry entries for the various programs that I haven't bothered to delete yet. They may cause a problem with antivirus signatures in the future, but for this class I didn't feel the need to go through all of the hassle of cleaning up the registry. For example: www.exterminate-it.com/malpedia/remove-vanquish

**How the malicious files were started:**

1. There were three Windows tasks, (run when the user logged on) that invoked ctl.exe. At least one of them looks like it starts FU.
2. Fat.bat was initiated by fat_init which was called by fat.vbs which was started by placing it in the Windows\currentversion\run\ system registry.
3. Several of them, such as Vanquish, Ctr12cap, basic and sysenter, were started as system services.
4. I needed better notes, since I don't recall how he4hookinv or HackerDefender were started. Reading up on he4hook, it looks like it does some fairly sophisticated techniques to load itself as a driver using a custom InstallDriver() function.

**Suspicious files that were not removed but would merit more investigation:**

1. Sptd.sys: It probably is a legitimate driver used by VMWare, but the signature was not parsed correctly by Windows Autoruns. Suggested way to verify it would be to compare it's hash against a known good version
2. BreackOnThroughToTheOtherSide.sys: Looks like the file used in the IntermediateX86 class which was not malicious. Once again a quick hash check should be able to verify it.
3. MRU-Blaster: It deletes the most recently used files on the computer. This might be used by an attacker, (or an authorized user who was up to no good), to delete evidence of them viewing files. Of course, there are many legitimate privacy/security uses for this as well. Suggested solution, check the corporate policy to see if the program is allowed, and check the hash of the program to make sure it hasn't been modified, (since it is not digitally signed).
4. The gmer anti-rootkit tool does not have a valid signature. Recommend checking the hash of this as well.
5. Ctrl2cap (the sysinternals one, not the known rootkit one with a 'one' instead of a 'l' does not have a valid signature. Recommend checking this with a known good hash.

**Checking for User-Mode rootkits:**

I did not run an anti-virus program on this windows image, (I didn't want to bother downloading a free antivirus program, and I'm sure the MITRE security people would love it if I put Symantec on it and had it alert to them…), but it's important to keep in mind that user-mode programs may be infected as well. Basically I'm saying this to cover my rear, without having to do any actual work to look for them…