Analysis

Since we were given a VMware Virtual machine consisting of vmdk (hard drive) and vmem (memory) files, I pretended like during my investigation of the suspected server I was able to perform a dump of physical memory and hard drive contents. With these files I can perform offline forensics. Which I think would be the right approach when you can’t trust the integrity of the OS you are examining.

I started my investigation by looking at the .vmem file using Volatility.

First looking at a process list. Processes that I marked in red, are immediately suspicious to me as I’m not familiar with the names.

Fast

```
No.  PID    Time created             Time exited              Offset     PDB        Remarks
---- ------ ------------------------ ------------------------ ---------- ---------- ----------------

   1      0                                                   0x00552a20 0x0073a000 Idle
   2    672 Mon Mar 14 01:27:58 2011 Mon Mar 14 01:30:44 2011 0x01a54868 0x067002a0 ForceField.exe
   3   2392 Mon Mar 14 01:32:04 2011                          0x01a9e020 0x06700320 wscntfy.exe
   4   2804 Mon Mar 14 01:32:12 2011                          0x01aa2da0 0x067002a0 RapportService.
   5   1832 Mon Mar 14 03:04:44 2011 Mon Mar 14 03:04:44 2011 0x01ae5020 0x06700500 mrublaster.exe
   6   2724 Mon Mar 14 03:03:44 2011 Mon Mar 14 03:03:44 2011 0x01b6b020 0x06700440 mrublaster.exe
   7   2680 Mon Mar 14 03:02:44 2011 Mon Mar 14 03:02:44 2011 0x01c5f5c0 0x067004a0 mrublaster.exe
   8   2812 Mon Mar 14 01:32:13 2011                          0x01c784e0 0x067004c0 alg.exe
   9    404 Mon Mar 14 01:31:45 2011                          0x01ca02c8 0x06700400 DTLite.exe
  10    448 Mon Mar 14 01:31:46 2011                          0x01ca0da0 0x06700420 scheduler.exe
  11    396 Mon Mar 14 01:31:45 2011                          0x01ca7a20 0x067003e0 ctfmon.exe
  12   3048 Mon Mar 14 01:32:48 2011 Mon Mar 14 01:32:52 2011 0x01cb3330 0x067003c0 mrublaster.exe
  13   1784 Mon Mar 14 01:31:38 2011                          0x01cb4be0 0x06700140 VMwareTray.exe
  14   3368 Mon Mar 14 03:06:17 2011                          0x01cb55a8 0x067002c0 Dbgview.exe
  15    216 Mon Mar 14 01:31:43 2011                          0x01cb9be0 0x067003a0 zlclient.exe
  16   1812 Mon Mar 14 01:31:39 2011                          0x01cbbda0 0x06700380 VMwareUser.exe
  17   1744 Mon Mar 14 01:31:38 2011                          0x01cde5b8 0x06700360 VMUpgradeHelper
  18   3492 Mon Mar 14 03:06:44 2011 Mon Mar 14 03:06:44 2011 0x01cf35d8 0x06700540 mrublaster.exe
  19   2456 Mon Mar 14 03:01:44 2011 Mon Mar 14 03:01:45 2011 0x01d0f998 0x067004e0 mrublaster.exe
  20   1256 Mon Mar 14 01:31:34 2011                          0x01d43980 0x06700340 vmtoolsd.exe
  21    680 Mon Mar 14 01:31:32 2011                          0x01d4b5c8 0x06700300 explorer.exe
  22   2620 Mon Mar 14 01:32:27 2011                          0x01d6bbf8 0x067002e0 ForceField.exe
  23    336 Mon Mar 14 01:31:30 2011                          0x01d795b0 0x06700240 hxdef100.exe
  24    412 Mon Mar 14 01:31:30 2011                          0x01d846a0 0x06700280 taskmgr.exe
  25    372 Mon Mar 14 01:31:30 2011                          0x01d87240 0x06700260 mysqld.exe
  26   2032 Mon Mar 14 01:31:27 2011                          0x01dd9020 0x06700220 svchost.exe
  27   1944 Mon Mar 14 01:31:27 2011                          0x01deeda0 0x06700200 spoolsv.exe
  28   1484 Mon Mar 14 01:31:16 2011                          0x01e3dc00 0x067001c0 vsmon.exe
  29   1356 Mon Mar 14 01:31:14 2011                          0x01e53268 0x067001a0 svchost.exe
  30   1260 Mon Mar 14 01:31:13 2011                          0x01e55da0 0x06700180 svchost.exe
  31   1200 Mon Mar 14 01:31:12 2011                          0x01e6f860 0x06700160 svchost.exe
  32   1036 Mon Mar 14 01:31:09 2011                          0x01e80be0 0x06700100 svchost.exe
  33   1132 Mon Mar 14 01:31:09 2011                          0x01ecb340 0x06700120 RapportMgmtServ
  34    948 Mon Mar 14 01:31:09 2011                          0x01ed26a0 0x067000e0 svchost.exe
  35   3476 Mon Mar 14 03:06:42 2011                          0x01ee4020 0x06700520 notepad.exe
  36    932 Mon Mar 14 01:31:09 2011                          0x01f025c8 0x067000c0 vmacthlp.exe
  37    764 Mon Mar 14 01:31:08 2011                          0x01f1bda0 0x06700080 services.exe
  38    776 Mon Mar 14 01:31:08 2011                          0x01f1c6f0 0x067000a0 lsass.exe
  39   3240 Mon Mar 14 03:05:44 2011 Mon Mar 14 03:05:44 2011 0x01f1d6b0 0x06700480 mrublaster.exe
  40    720 Mon Mar 14 01:31:08 2011                          0x01f2fbe0 0x06700060 winlogon.exe
  41    612 Mon Mar 14 01:31:07 2011                          0x01f7d320 0x06700020 smss.exe
  42   1884 Mon Mar 14 01:31:27 2011                          0x01feca20 0x067001e0 ISWSVC.exe
  43    696 Mon Mar 14 01:31:07 2011                          0x0218f4a8 0x06700040 csrss.exe
  44    660 Mon Mar 14 03:00:44 2011 Mon Mar 14 03:00:47 2011 0x024afda0 0x06700460 mrublaster.exe
  45      0                                                   0x025c8830 0x0073a000 System
```

Time for google ☺

ForceField.exe, and ISWSVC.exe seem to be a part of a ZoneAlarm ForceShield

RapportServer.exe and RapportMgmtService.exe – Rapport is a lightweight security software solution that protects web communication between enterprises, such as banks, and their customers and employees. Not sure why this is running maybe part of a MITRE Pilot?

Zlclient.exe – Zone alarm

Mrublaster.exe – for protecting most recently used privacy? Maybe xeno and corey used to help get rid of hints?

Vmacthlp.exe – Vmware Process, safe

Hxdef100.exe – Hacker Defender Rootkit ☺

DTLite.exe – Daemon Tools, seems safe

Next I Had Volatility dump the modules. Which show all of the drivers loaded in the Operating System. Due to the large amount of modules, I only highlight a few in red that stood out.

```
Name                                               Base
\WINDOWS\system32\ntkrnlpa.exe                      0x804d7000
\WINDOWS\system32\hal.dll                           0x806d0000
\WINDOWS\system32\KDCOM.DLL                         0xf8b9a000
\WINDOWS\system32\BOOTVID.dll                       0xf8aaa000
sptd.sys                                            0xf8489000
\WINDOWS\System32\Drivers\WMILIB.SYS                0xf8b9c000
\WINDOWS\System32\Drivers\SCSIPORT.SYS              0xf8471000
ACPI.sys                                            0xf8443000
pci.sys                                             0xf8432000
isapnp.sys                                          0xf869a000
compbatt.sys                                        0xf8aae000
\WINDOWS\system32\DRIVERS\BATTC.SYS                 0xf8ab2000
intelide.sys                                        0xf8b9e000
\WINDOWS\system32\drivers\PCIIDEX.SYS               0xf891a000
MountMgr.sys                                        0xf86aa000
ftdisk.sys                                          0xf8413000
dmload.sys                                          0xf8ba0000
dmio.sys                                            0xf83ed000
PartMgr.sys                                         0xf8922000
VolSnap.sys                                         0xf86ba000
atapi.sys                                           0xf83d5000
vmscsi.sys                                          0xf8ab6000
disk.sys                                            0xf86ca000
\WINDOWS\system32\DRIVERS\CLASSPNP.SYS              0xf86da000
fltMgr.sys                                          0xf83b5000
sr.sys                                              0xf83a3000
KSecDD.sys                                          0xf838c000
Ntfs.sys                                            0xf82ff000
NDIS.sys                                            0xf82d2000
RapportKELL.sys                                     0xf86ea000
Mup.sys                                             0xf82b8000
agp440.sys                                          0xf86fa000
\SystemRoot\system32\DRIVERS\intelppm.sys           0xf872a000
```

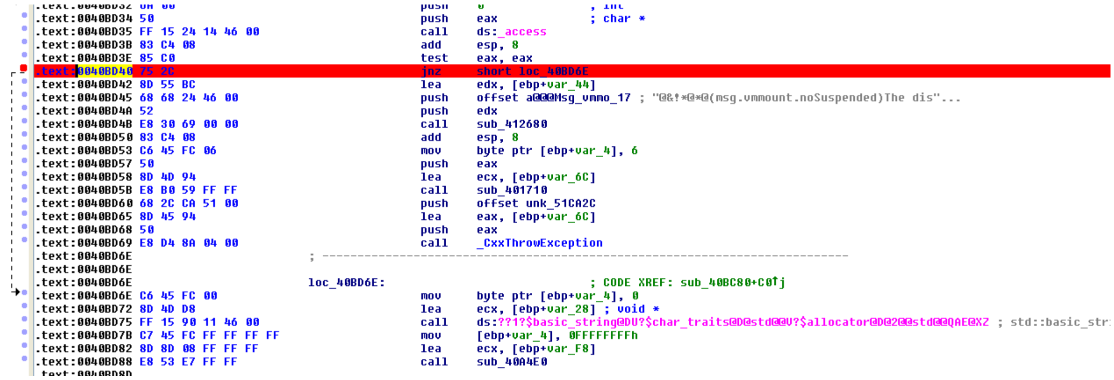
```
\SystemRoot\System32\DRIVERS\i8042prt.sys           0xf873a000
\SystemRoot\system32\DRIVERS\kbdclass.sys           0xf8952000
\SystemRoot\System32\Drivers\Ctrl2cap.SYS           0xf8d18000
\SystemRoot\system32\DRIVERS\mouclass.sys           0xf895a000
\SystemRoot\system32\DRIVERS\parport.sys            0xf824b000
\SystemRoot\system32\DRIVERS\serial.sys             0xf874a000
\SystemRoot\system32\DRIVERS\serenum.sys            0xf8b46000
\SystemRoot\system32\DRIVERS\fdc.sys                0xf896a000
\SystemRoot\system32\DRIVERS\imapi.sys              0xf875a000
\SystemRoot\system32\DRIVERS\cdrom.sys              0xf876a000
\SystemRoot\system32\DRIVERS\redbook.sys            0xf877a000
\SystemRoot\system32\DRIVERS\ks.sys                 0xf8228000
\SystemRoot\system32\DRIVERS\vmx_svga.sys           0xf8982000
\SystemRoot\system32\DRIVERS\VIDEOPRT.SYS           0xf8214000
\SystemRoot\system32\DRIVERS\vmxnet.sys             0xf898a000
\SystemRoot\System32\Drivers\azdow88m.SYS           0xf81d7000
\SystemRoot\system32\DRIVERS\CmBatt.sys             0xf8b66000
\SystemRoot\system32\DRIVERS\audstub.sys            0xf8d36000
\SystemRoot\system32\DRIVERS\rasl2tp.sys            0xf878a000
\SystemRoot\system32\DRIVERS\ndistapi.sys           0xf8b6e000
\SystemRoot\system32\DRIVERS\ndiswan.sys            0xf81c0000
\SystemRoot\system32\DRIVERS\raspppoe.sys           0xf879a000
\SystemRoot\system32\DRIVERS\raspptp.sys            0xf87aa000
\SystemRoot\system32\DRIVERS\TDI.SYS                0xf8a12000
\SystemRoot\system32\DRIVERS\psched.sys             0xf8187000
\SystemRoot\system32\DRIVERS\msgpc.sys              0xf87ba000
\SystemRoot\system32\DRIVERS\ptilink.sys            0xf8a22000
\SystemRoot\system32\DRIVERS\raspti.sys             0xf8a32000
\SystemRoot\system32\DRIVERS\rdpdr.sys              0xf8157000
\SystemRoot\system32\DRIVERS\termdd.sys             0xf87ca000
\SystemRoot\system32\DRIVERS\swenum.sys             0xf8bac000
\SystemRoot\system32\DRIVERS\update.sys             0xf80f9000
\SystemRoot\system32\DRIVERS\mssmbios.sys           0xf8b92000
\SystemRoot\system32\DRIVERS\dtsoftbus01.sys        0xf80be000
\SystemRoot\System32\Drivers\NDProxy.SYS            0xf87da000
\SystemRoot\system32\DRIVERS\flpydisk.sys           0xf8a5a000
\SystemRoot\System32\Drivers\Fs_Rec.SYS             0xf8bb0000
\SystemRoot\System32\Drivers\Null.SYS               0xf8d7a000
\SystemRoot\System32\Drivers\Beep.SYS               0xf8bb4000
\SystemRoot\System32\drivers\vga.sys                0xf8a72000
\SystemRoot\System32\Drivers\mnmdd.SYS              0xf8bb8000
\SystemRoot\System32\DRIVERS\RDPCDD.sys             0xf8bbc000
\SystemRoot\System32\Drivers\Msfs.SYS               0xf8a82000
\SystemRoot\System32\Drivers\Npfs.SYS               0xf8a92000
\SystemRoot\system32\DRIVERS\rasacd.sys             0xf8b4e000
\SystemRoot\system32\DRIVERS\ipsec.sys              0xf4c86000
\SystemRoot\system32\DRIVERS\tcpip.sys              0xf4c2d000
\SystemRoot\system32\DRIVERS\netbt.sys              0xf4c05000
\SystemRoot\system32\DRIVERS\ipnat.sys              0xf4bdf000
\SystemRoot\System32\vsdatant.sys                   0xf4b5e000
\SystemRoot\System32\drivers\ws2ifsl.sys            0xf81bc000
\SystemRoot\System32\drivers\afd.sys                0xf4b14000
\SystemRoot\system32\DRIVERS\netbios.sys            0xf87fa000
\SystemRoot\System32\DRIVERS\vmhgfs.sys             0xf4af6000
\??\C:\WINDOWS\system32\drivers\sysenter.sys        0xf8db7000
\SystemRoot\system32\DRIVERS\rdbss.sys              0xf4acb000
\??\C:\Program Files\Trusteer\Rapport\bin\RapportPG.sys  0xf4aa6000
\SystemRoot\system32\DRIVERS\wanarp.sys             0xf881a000
\??\C:\Program Files\Trusteer\Rapport\bin\RapportEI.sys  0xf882a000
\??\C:\Documents and Settings\All Users.WINDOWS\Application
Data\Trusteer\Rapport\store\exts\RapportCerberus\baseline\RapportCerberus_23645.sys
0xf883a000
\SystemRoot\system32\DRIVERS\mrxsmb.sys             0xf4a36000
\SystemRoot\System32\Drivers\Fips.SYS               0xf884a000
\??\C:\WINDOWS\system32\drivers\Ctr12Cap.sys        0xf8dd6000
\??\C:\WINDOWS\system32\drivers\BASIC.sys           0xf8dd8000
\SystemRoot\System32\Drivers\Cdfs.SYS               0xf886a000
\SystemRoot\System32\Drivers\dump_atapi.sys         0xf49f6000
\SystemRoot\System32\Drivers\dump_WMILIB.SYS        0xf8bc8000
\SystemRoot\System32\win32k.sys                     0xbf800000
\SystemRoot\System32\drivers\Dxapi.sys              0xf5f69000
```

```
\SystemRoot\System32\watchdog.sys                    0xf89b2000
\SystemRoot\System32\drivers\dxg.sys                 0xbf000000
\SystemRoot\System32\drivers\dxgthk.sys              0xf8cfe000
\SystemRoot\System32\vmx_fb.dll                      0xbf012000
\SystemRoot\System32\ATMFD.DLL                       0xbffa0000
\SystemRoot\system32\DRIVERS\ndisuio.sys             0xf48de000
\??\C:\Program Files\CheckPoint\ZAForceField\ISWKL.sys  0xf8a8a000
\SystemRoot\system32\DRIVERS\mrxdav.sys              0xf44a1000
\SystemRoot\System32\Drivers\ParVdm.SYS              0xf8c50000
\??\C:\Program Files\VMware\VMware Tools\Drivers\memctl\vmmemctl.sys  0xf8c52000
\??\C:\hxdef100r\hxdefdrv.sys                        0xf8ce5000
\SystemRoot\system32\DRIVERS\srv.sys                 0xf4331000
\SystemRoot\System32\Drivers\HTTP.sys                0xf3cd8000
\??\C:\WINDOWS\system32\Drivers\Dbgv.sys             0xf3b1f000
```

Now that I have some hints, I want to examine the contents of the hard drive to look at these .sys file in more detail. I searched the Internet to find that vmware has a tool available for download called vmware-mount.exe. It allows you to mount a vmdk file as a drive letter on your computer. When initially trying to run the tool as documented, it would not work because it stated that the hard drive is from a suspended virtual machine.

http://www.petri.co.il/virtual_mount_vmware_virtual_disk_without_vmware.htm

I decided to take a look in IDA to find where that check was being made.



```
.text:0040BD34 50                                push    eax             ; char *
.text:0040BD35 FF 15 24 14 46 00                 call    ds:_access
.text:0040BD3B 83 C4 08                          add     esp, 8
.text:0040BD3E 85 C0                             test    eax, eax
.text:0040BD40 75 2C                             jnz     short loc_40BD6E
.text:0040BD42 8D 55 BC                          lea     edx, [ebp+var_44]
.text:0040BD45 68 68 24 46 00                    push    offset a@@@Msg_vmmo_17 ; "@&!*@*@(msg.vmmount.noSuspended)The dis"...
.text:0040BD4A 52                                push    edx
.text:0040BD4B E8 30 69 00 00                    call    sub_412680
.text:0040BD50 83 C4 08                          add     esp, 8
.text:0040BD53 C6 45 FC 06                       mov     byte ptr [ebp+var_4], 6
.text:0040BD57 50                                push    eax
.text:0040BD58 8D 4D 94                          lea     ecx, [ebp+var_6C]
.text:0040BD5B E8 B0 59 FF FF                    call    sub_401710
.text:0040BD60 68 2C CA 51 00                    push    offset unk_51CA2C
.text:0040BD65 8D 45 94                          lea     eax, [ebp+var_6C]
.text:0040BD68 50                                push    eax
.text:0040BD69 E8 D4 8A 04 00                    call    _CxxThrowException
.text:0040BD6E                    ; ---------------------------------------------------------------------------
.text:0040BD6E
.text:0040BD6E                    loc_40BD6E:                            ; CODE XREF: sub_40BC80+C0↑j
.text:0040BD6E C6 45 FC 00                       mov     byte ptr [ebp+var_4], 0
.text:0040BD72 8D 4D D8                          lea     ecx, [ebp+var_28] ; void *
.text:0040BD75 FF 15 90 11 46 00                 call    ds:??1?$basic_string@DU?$char_traits@D@std@@V?$allocator@D@2@@std@@QAE@XZ ; std::basic_str
.text:0040BD7B C7 45 FC FF FF FF FF              mov     [ebp+var_4], 0FFFFFFFFh
.text:0040BD82 8D 8D 08 FF FF FF                 lea     ecx, [ebp+var_F8]
.text:0040BD88 E8 53 E7 FF FF                    call    sub_40A4E0
```

Above is a screen shot of the where the test and jump are located (0x0040BD40). If you set a breakpoint at that location, and when the breakpoint hits modify the EIP register value to 0x0040BD6E, then continue. The process will exit normally and your drive letter will be mapped.

NOTE: In the debugger menu under process options, the parameters textbox should have the following contents.

```
j: "c:\rootvm\RootkitClassVM_v1.1\RootkitClassVM.vmdk"
```

Just make sure the path in the above text points to your vmdk file. I do not guaranty this method to always work.

MAKE SURE YOU DO THIS ON A COPY OF THE VMDK FILE. This volume will be mounted as read write, so be careful.

Once the drive has been mounted, I can navigate the file system.

```
J:\>dir
 Volume in drive J has no label.
 Volume Serial Number is B48F-163D

 Directory of J:\

11/17/2008  12:02 AM                 0 AUTOEXEC.BAT
11/17/2008  12:02 AM                 0 CONFIG.SYS
11/17/2008  12:08 AM    <DIR>          Documents and Settings
03/13/2011  08:38 PM    <DIR>          hxdef100r
03/06/2011  10:02 PM               244 INSTALL.LOG
03/13/2011  05:23 PM    <DIR>          Program Files
03/06/2011  10:08 PM    <DIR>          vanquish-0.2.1
03/13/2011  08:16 PM               486 vanquish.log
03/11/2011  05:01 PM    <DIR>          WinDDK
03/13/2011  09:24 PM    <DIR>          WINDOWS
               4 File(s)            730 bytes
               6 Dir(s)   3,030,482,944 bytes free
```

Three things pop out right away when viewing the directory listing. The directory for hacker defender rootkit and a program called vanquish which is a user space rootkit.

At this point I decided to examine the registry to see what services are installed, and what programs are set to startup on reboot. I used the following link for how to use regedit to view registry files from another computer. I found that this caused some changes to be made in the vmdk file that can corrupt the image. Please make sure you do this while using a backup copy.

http://4sysops.com/archives/regedit-as-offline-registry-editor/

Once I'm able to view the registry using regedit I used the following link to figure out where services are located.

http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.dc36556_1500/html/histserv/X37757.htm

I went through all of the services listed and the ones that stand out are:

- BASIC.sys – Set as device driver, running strings shows reference to rootkit.
- BreakOnThruToTheOtherSide.sys – Manual Startup, from intermediate x86.
- Ctr12Cap.sys – Set as device driver, seems very strange? 1 (one) instead of L, set as device driver. Strings shows api for KeServiceDescriptorTable, which it probably hooks.
- Gmer.sys – Looks like this is installed to help us find rootkits.
- C:\hxdef100r\hxdef100.exe – Set to start up.

- hxdefdrv.sys – Set to manual, but it was listed in the modules list so we know that it was started manually.
- sysenter.sys – nothing found on google. But running strings on the .sys file, you see the term rootkit. Set to start as a driver.
- "C:\WINDOWS\vanquish.exe" – Set to automatically start.

Next I went through all of the other registry locations listed in the following link to look for more programs that can startup on reboot.

http://www.bleepingcomputer.com/tutorials/tutorial44.html

- HKLM\Microsoft\Windows\CurrentVersion\Run
    - wscript.exe "C:\WINDOWS\fat.vbs" "C:\WINDOWS\fat.bat"

```
$ cat 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
```

Above is the only entry I found that looked out of the norm.

This using the FU rootkit to install and hide a driver called mmpc. Running strings on mmpc.sys shows references to shadow walker/ corey directory. Definitely a rootkit. ☺

mmpc.sys and msdirectx.sys are rootkit related.

Removal

I thought that the removal would be an easy process but I ran into a snag.

First I booted up the VM, and restarted it to go into safe mode.

Once in safe mode, I went through all off the registry locations and set all the drivers listed above to be manual by setting the startup entry to the value 3. I also removed the entry to fat.bat from running. One thing I noticed while I was in the registry was no reference to the HackerDefender rootkit. I thought this was really strange. I found a really good pdf on HackerDefender. The paper only described the way to remove the rootkit was to remove all the files associated, however no files were visible because the rootkit was running.

So, I shutdown the VM. I remounted the vmdk file using the same trick described above, but this time using the real vmdk not a backup copy. Once I had the volume mounted I tried to make a copy.

```
J:\hxdef100r>copy hxdef100.exe ..
Access is denied.
        0 file(s) copied.
```

After trying to copy I did a directory listing and found that the file was missing. My local virus software had quarantined the file. At first I thought that the vmdk file would become corrupted because of this. I unmounted the volume and restarted the VM. I was happy to see that HackerDefender was no longer running. ☺

The HackerDefender directory is now visible in my VM.

References:

http://www.bleepingcomputer.com/startups/RapportMgmtService.exe-26152.html
http://infocenter.sybase.com/help/index.jsp?topic=/com.sybase.dc36556_1500/html/histserv/X37757.htm
http://www.bleepingcomputer.com/tutorials/tutorial44.html
http://www.softpedia.com/get/System/System-Miscellaneous/Ctrl2cap.shtml
http://www.fbmsoftware.com/spyware-net/process/mrublaster_exe/3191/
http://4sysops.com/archives/regedit-as-offline-registry-editor/
http://www.f-secure.com/v-descs/fu.shtml
http://www.techbytes.ca/techbyte74.html
www.carnal0wnage.com/papers/rootkit_for_the_masses.pdf