RESPONSE TO SPECIFIC QUESTIONS POSED BY THE DFRWS 2005 MEMORY CHALLENGE

by RossettoeCioccolato <rossettoecioccolato@yahoo.com>
and Robert-Jan Mora <rob@mora.demon.nl>

August 6, 2005.

1. What hidden processes were running on the system, and how were they hidden?

Computer users and information specialists use a variety of tools to locate resources on Microsoft Windows™ systems, including running processes. These tools have varying levels of sophistication and may have both user and kernel mode components. At the most basic level is user mode tools such as the *Windows Task Manager* which is part of the Windows shell and command line tools such as *pslist* (http://www.sysinternals.com/Utilities/PsList.html) and *tlist* (http://www.microsoft.com/ddk/debugging/). More recently, sophisticated tools which incorporate both user and kernel mode components (e.g. http://www.sysinternals.com/utilities/rootkitrevealer.html) have been introduced to obtain an accurate enumeration of running processes on a Microsoft Windows™ system. A process is said to be "hidden" if it is invisible with respect to a particular tool or class of tools designed to accurately detect running processes on a system.

A. Hacker Defender.

A variety of techniques have been introduced to "hide" running processes from common means of detection. These techniques have varying levels of sophistication just as the tools which they are designed to defeat. The simplest technique is to directly attack the tool and prevent it from running. This actually may have occurred in this case according to Daniels' report. With respect to *pslist* and *fport* all of the processes (both legitimate and malicious) were hidden.

However, this method is bound to arouse suspicion and is therefore ultimately self-defeating. A slightly more subtle approach is to modify user mode processes in such a manner as to divert (i.e. "hook") the execution path of process threads when they attempt to discover the existence of "hidden" resources. *Hacker Defender* is an example of a rootkit that installs a large number of user mode "hooks" to hide files, processes, network ports and other resources. http://www.megasecurity.org/trojans/h/hackerdefender/Hackerdefender1.00.html. *Clamscan* (http://www.clamav.net/) was run on evidence file *dfrws2005-physical-memory1.dmp* and identified the file as containing Trojan.HacDef.073.B. In addition, *dfrwsdrv.sys* was extracted from the memory “image” using *dd* and

the loaded system module list from *kntlist*. *Kaspersky* antivirus identified the file as containing Backdoor.Win32.HacDef.073.b.

Other indications of the presence of *Hacker Defender* were found among the strings extracted from *dfrws2005-physical-memory1.dmp*. The memory page beginning at offset 0x5549000 contains apparent configuration-file contents for *Hacker Defender*. The configuration information contains a section entitled "[H<<<idden T>>a/"ble]" which proceeds as follows:

```
>d"frws"*
r|c<md\.ex<e::
e<og|han
um\gr|32.e<xe
```

According to the documentation for *Hacker Defender*, "Extra characters |, <, >, :, \, / and " are ignored on all lines except [Startup Run], [Free Space] and [Hidden Ports] items and values in [Settings] after first = character." A trailing '*' character is used to indicate a wildcard similar to the Microsoft Windows "dir" command. Assuming that the version of *Hacker Defender* on this computer followed the default behavior, any file, directory or process starting with the characters "dfrws" and any file, directory or process named “rcmd.exe,” “eoghan” or “umgr32.exe” would be hidden from user mode processes.

An attempt was made to locate the owner of the memory page described above by cross-referencing the physical address to the physical addresses identified by *kntlist*. However, this attempt was unsuccessful. Analysis of the VAD descriptors for each process might shed some light on this matter. Currently this analysis must be done by hand. The presence of allocation pool tags (e.g. 'MmSt') elsewhere in this memory page identifies the page as being a part (or at least formerly a part) of the kernel address space. See the documentation for *ExAllocatePoolWithTag* for more information on allocation pool tags. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/kmarch/hh/kmarch/k102_13ab2d7e-dd96-4474-bf27-59ee9b7d84d6.xml.asp. The configuration file would likely have been read on system startup. Since memory pages are not zeroed until they are reallocated, it is entirely possible that this page has been discarded but its contents remain in memory.

The apparent configuration file contents also include the name of the section object that *Hacker Defender* is using as a means of inter-process communication between kernel and user mode components of the rootkit:

```
FiI:eMappin\gN/ame=_.-=[DFRWS2005]=-._
```

Using the output from *kntlist*, a section object by this name was located in one of the handle tables at virtual address 0xFF15E168 belonging to process 0xFF191640:

```
OBJECT: 0xE1E22A80(54d3a80) Type: 17 Section
Object Header: 0xE1E22A68
GrantedAccess: f0007 PointerCount: 2 HandleCount: 1
Directory: 0xFCC68730 Name: _.-=[DFRWS2005]=-._
```

The active process list revealed that this process is named *dfrws2005.exe*.

```
+ 250  dfrws2005.exe
       Source: from_active_process_list
       Eprocess Block: 0xFF191640 (0x2138624)
       CreateTime: 0x1c5696a6185ff0 2005-06-05 01:00:53Z
```

Based on these observations we may conclude that components of a rootkit exhibiting the characteristics of the *Hacker Defender* rootkit were loaded into memory and actively running at the time that the first memory "image" was taken. Any process named "rcmd.exe," "eoghan" or "umgr32.exe" or which name began with "dfrws" would have been hidden to user mode processes at the time that the first memory “image” was taken.

Artifacts relating to *Hacker Defender* also were found in the second memory “image.”

The approach taken by *Hacker Defender* is cumbersome in that every running process (with a few exceptions) must be modified for it to work. To avoid this complication techniques have been developed to “hook” system services at the kernel level. With kernel mode hooks only a single process (i.e. the kernel) needs to be modified to affect all processes.

B. Kernel mode hooks.

Kernel hooks may be applied at a broad variety of locations. The GDT and IDT base addresses, as well as IDTR, GDTR and LDTR registers in the processor control block were examined based on *kntlist* output and were found to be unremarkable. Selector/offset pairs in the IDT and GDT tables also were examined and found to be unremarkable. Function pointers in the system and shadow system service tables were found to point to values within *ntoskrnl* or *win32k.sys*. There are nevertheless many other locations where kernel services may be “hooked” and this cannot be ruled out entirely. For more information on hooking system services and ways to detect it, see James Butler, "*VICE - Catch the hookers!*" Black Hat, Las Vegas, July, 2004. http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf.

C. Direct kernel object manipulation (*DKOM*).

Most kernel and user mode hooks are readily detected by modern rootkit detection tools. For this reason, the more sophisticated rootkits are gravitating towards a new technique invented by fuzenop (a.k.a. Jamie Butler). Direct kernel object manipulation subverts system services by modifying the kernel structures on which they depend. There are many kernel structures which may be modified to hide processes. The Windows kernel creates a list of processes at a user's request by walking a doubly linked list. The FU rootkit attempts to achieve invisibility by un-linking the "hidden" process from this list.

DKOM based rootkits are difficult to detect using current detection methods but there have been some examples of success. Kernel objects, including processes, are woven together by an intricate web of undocumented structures. The handle table list is one such structure. Every process has a handle table and every table refers back to the process that created it. *Blacklight* from FSecure attempts to discover hidden processes by walking this table and correlating the table to processes in the active process list. If a handle table points to a process that is not in the active process list, the process is marked as hidden. *F-Secure BlackLight* (Helsinki, Finland: F-Secure Corporation, 2005): http://www.fsecure.com/blacklight/.

Kntlist walks the handle table list as well as every object in every handle table and every object in the object directory looking for references to processes. Three cloaked processes were identified using this method, two instances of "metasploit.exe" and one instance of "dfrws2005.exe." Each of these processes appears to have terminated.

Twenty one (21) orphaned threads also were found in the handle tables or the object directory that were not found in the thread list of any known process. All of these threads appear also to have terminated. This large amount of kernel object detritus is difficult to explain without some reference to kernel object modification. Kernel objects are tracked very closely by the kernel to prevent memory leaks. A very small memory leak can, over time, bring a system down particularly where, as here, the leak is in the non-paged pool. A process that terminates abnormally may remain for some time in the active process list before the process and its resources are torn down. This hypothesis does not explain the presence of a process outside of the active process list, however.

Ironically, the primary effect of *DKOM* in this case (if that is what it was), has been to preserve evidence which might otherwise have disappeared by the time Daniels arrived on the scene.

Finally, mention should be made of the orphaned handle table at 0xFCE25668:

2. TABLE: 0xFCE25668(1442668):
    Table: 0xE1003000
    QuotaProcess:
    ProcessId: 0
    HandleCount: 62
    CapturedHandleCount: 62
    TableLevel: 2
    StrictFIFO: No

This handle table is suspicious both because it lacks a reference to the quota process (usually the originating process) and because its order in the list indicates that a process ran immediately after *ntoskrnl* and before *smss.exe*. The FU rootkit recently has been modified to remove references in the handle table list and object directory to the hidden process. http://www.phrack.org/show.php?p=63&a=8. This handle table might be an artifact of the modified FU rootkit. Additionally, recursion was detected in the object directory at entry 0xE1E25128 which might indicate that an object, probably a driver, was removed from the directory.

Perhaps this is all a peculiarity of this particular version of Windows. However, at this point additional cloaked processes cannot be ruled out.

Also to be noted is that the Hidden section of the Hacker Defender rootkit configuration information mentions a file, directory or process named "eoghan" and no such file, directory or process by this name has been found. Perhaps the attacker was testing the rootkit on his own system and left the name in as an oversight. However, this remains an inconsistency that needs to be resolved.

The command prompt started by *nc.exe* cannot be found in the active process list and has not otherwise been located.

In addition, the origin of the command prompt (cmd.exe) at 0xFF191C40 with a create time of 2005-06-05 00:35:18Z has not been explained.

2. What other evidence of the intrusion can be extracted from the memory dumps?

A. B02K trojan.

Multiple memory pages were found in both memory dumps that contain strings characteristic of the B02K trojan.

For example in the first memory dump:

```
03DE6C60   8E 00 00 00 00 53 54 43  50 49 4F 00 4E 55 4C 4C   Ž....STCPIO.NULL
03DE6C70   00 4E 55 4C 4C 41 55 54  48 00 63 3A 5C 44 6F 63   .NULLAUTH.c:\Doc
[...]
0004D590   00 00 29 00 00 00 00 00  00 00 28 30 29 20 53 54   ..).......(0) ST
0004D5A0   43 50 49 4F 3A 20 42 4F  32 4B 20 53 74 65 61 6C   CPIO: BO2K Steal
0004D5B0   74 68 79 20 54 43 50 20  49 4F 20 4D 6F 64 75 6C   thy TCP IO Modul
0004D5C0   65 0A 00 00 00 00 00 7C  0A 00 00 00 00 00 00 00   e......|........
[...]
0004D980   00 00 02 00 00 00 FF FF  FF FF 8F B7 1A 00 01 00   ......ÿÿÿÿ• ·....
0004D990   00 00 23 00 00 00 00 00  00 00 28 30 29 20 4E 55   ..#.......(0) NU
0004D9A0   4C 4C 45 4E 43 3A 20 42  4F 32 4B 20 4E 55 4C 4C   LLENC: BO2K NULL
0004D9B0   20 45 6E 63 72 79 70 74  69 6F 6E 0A 00 00 00 00    Encryption.....
```

And from the second memory dump:

```
003B35A0   42 4F 32 4B 20 4C 65 67  61 63 79 20 42 75 74 74   BO2K Legacy Butt
003B35B0   70 6C 75 67 20 53 75 70  70 6F 72 74 00 00 00 00   plug Support....
003B35C0   73 72 76 5F 6C 65 67 61  63 79 2E 64 6C 6C 00 00   srv_legacy.dll..
003B35D0   F0                                                 ð
[...]
003B35A0   42 4F 32 4B 20 4C 65 67  61 63 79 20 42 75 74 74   BO2K Legacy Butt
003B35B0   70 6C 75 67 20 53 75 70  70 6F 72 74 00 00 00 00   plug Support....
003B35C0   73 72 76 5F 6C 65 67 61  63 79 2E 64 6C 6C 00 00   srv_legacy.dll..
003B35D0   F0                                                 ð
[...]
003B35A0   42 4F 32 4B 20 4C 65 67  61 63 79 20 42 75 74 74   BO2K Legacy Butt
003B35B0   70 6C 75 67 20 53 75 70  70 6F 72 74 00 00 00 00   plug Support....
003B35C0   73 72 76 5F 6C 65 67 61  63 79 2E 64 6C 6C 00 00   srv_legacy.dll..
003B35D0   F0                                                 ð
```

The active process list of both memory dumps contains a process named *UMGR32.EXE* (for each memory dump in order):

+ 29c UMGR32.EXE
  Source: from_active_process_list
  Eprocess Block: 0xFF15B020 (0x95f004)
  CreateTime: 0x1c56969385796d0 2005-06-05 00:55:08Z

+ 224 UMGR32.EXE
  Source: from_active_process_list
  Eprocess Block: 0xFF2461E0 (0x4be51e0)
  CreateTime: 0x1c569df9628aa90 2005-06-05 15:02:26Z

In both cases the section file name is \WINNT\System32\UMGR32.EXE. This is consistent with the default behavior for BO2K which may copy itself to %systemroot%\System32\UMGR32.EXE; then the initial copy exits leaving the clone to run. BO2K also can copy itself into a remote thread in an existing process and so it is possible that this trojan is running in other processes on the system. http://vil.nai.com/vil/content/Print10229.htm

B. Metasploit.exe.

Two "cloaked" processes were found that were referenced by kernel objects but not included in the *eprocess* list.

```
+ 314   metasploit.exe
        Source: from_kernel_object
        Cloaked: Yes
        Eprocess Block: 0xFF1B5CC0 (0x2686ca4)
        CreateTime: 0x1c56966e9b473b0 2005-06-05 00:38:37Z

+ 258   metasploit.exe
        Source: from_kernel_object
        Cloaked: Yes
        Eprocess Block: 0xFF129460 (0x6601444)
        CreateTime: 0x1c5696938454090 2005-06-05 00:55:08Z
```

Metasploit.exe is the name of a popular egg-dropper package. http://metasploit.com/shellcode.html. One of the components in this package downloads an executable to a hidden file in the root directory named *metasploit.exe* and then executes that program. http://seclists.org/lists/vuln-dev/2004/Apr/0011.html.

The *Sleuthkit* timeline contains three references to metasploit.exe, two in close proximity to references to *UMGR32.EXE*:

```
Sat Jun 04 2005 01:00:00    35600 .a. -/-rwxrwxrwx 0       0       9195131  /WINNT/system32/ipconfig.exe
[…]
Sat Jun 04 2005 01:00:00
                    155648 .a. -/-r-xr-xr-x 0       0       35      /metasploit.exe (METASP~1.EXE)
[…]
Sat Jun 04 2005 19:50:18   155648 ..c -/-r-xr-xr-x 0       0       35      /metasploit.exe (METASP~1.EXE)
                    155648 ..c -/-r-xr-xr-x 0       0       16698193 /WINNT/system32/UMGR32.EXE
[…]

Sat Jun 04 2005 21:22:04      854 ..c -/-rwxrwxrwx 0       0       16698216 /WINNT/system32/dfrws2005.ini

(DFRWS2~1.INI)
[…]
Sat Jun 04 2005 21:55:10   155648 m.. -/-r-xr-xr-x 0       0       35      /metasploit.exe (METASP~1.EXE)
                    155648 m.. -/-r-xr-xr-x 0       0       16698193 /WINNT/system32/UMGR32.EXE
Sat Jun 04 2005 21:59:10     3342 ..c -/--wx-wx-wx 0       0       16698237 /WINNT/system32/dfrwsdrv.sys
                     3342 ..c -/-rwxrwxrwx 0       0       16698229 /WINNT/system32/_frwsdrv.sys

(deleted)
                     3342 ..c -/-rwxrwxrwx 0       0       16698236 /WINNT/system32/_frwsdrv.sys

(deleted)
                      854 m.. -/-rwxrwxrwx 0       0       16698216 /WINNT/system32/dfrws2005.ini
```

The timeline suggests that multiple drops occurred. In each case the dropped files were 155648 bytes in size. However files of identical size and name need not be identical files. Curiously, the timeline contains a file access entry for *metasploit.exe* that is prior to the file creation record for this file. At a minimum this suggests that one or more intruders have been active on this system for some time. It is also possible that the timeline has been manipulated. As has

been previously noted, there are possible signs of more sophisticated intrusion techniques and so we need to be careful taking things at face value.

Reference also was found to *metasploit.exe* on the kernel mode stack of two threads in the system. The first is a thread belonging to the system process, whose start address lies within a kernel mode driver, *UdfReadr.SYS*:

```
028902F0   04 00 02 00 00 01 0E 00  43 3A 5C 6D 65 74 61 73   ........C:\metas
02890300   70 6C 6F 69 74 2E 65 78  65 00 00 00 00 00 00 00   ploit.exe.......

        THREAD: 0xFCD619E0 (0x137e9e0)   Cid: 8.64
        CreateTime: 0x1c5696613e4c370 2005-06-05 00:32:39Z

        [...]
        Start Address: 0xF8389CCC  \SystemRoot\System32\Drivers\UdfReadr.SYS
        [...]

        Kernel Stack: 0xF08C3CF8(2871000 ***2890000*** 286f000 ) Resident: 1
```

The second reference occurs within a thread belonging to the process *tgcmd.exe*.

```
052E6580   00 AA 1D FF 6D 00 65 00  74 00 61 00 73 00 70 00   .ª.ÿm.e.t.a.s.p.
052E6590   6C 00 6F 00 69 00 74 00  2E 00 65 00 78 00 65 00   l.o.i.t...e.x.e.

       THREAD: 0xFF170020 (0x611e020)   Cid: 3f4.410 tgcmd.exe
       CreateTime: 0x1c5696645df5860 2005-06-05 00:34:02Z
       [...]
       Start Address: 0x77E83775  C:\WINNT\system32\KERNEL32.DLL
       Win32 Start Address: 0x778321FE  C:\WINNT\System32\RTUTILS.DLL
       Service Descriptor Table: 0x8046B840 KeServiceDescriptorTable
       Initial stack: 0xF7AD7000 Stack Limit: 0xF7AD4000
       Kernel Stack: 0xF7AD6930(***52e6000*** NA NA ) Resident: 0
```

C. TGCmd.exe

One of the memory pages referenced above in connection with *UMGR32.EXE* (a.k.a B02K) contains a reference to *tgcmd*:

```
03DE6EB0   24 00 64 02 00 01 0C 00  F4 03 00 00 88 10 16 00   $.d.....ô...ˆ...
03DE6EC0   74 67 63 6D 64 00 00 00  00 00 00 00 00 00 00 00   tgcmd...........
```

This program is listening over all interfaces on tcp ports 641 an 653, as was noted in our initial response to the challenge. While some may consider it legitimate software, *tgcmd* is essentially a backdoor that is installed by certain vendors as a means of providing support to their customers. The vendor's intention doubtless is to provide support with the owner's permission. However when a listening server is placed on a poorly secured computer it is always possible that someone may offer the user more support than he or she desires. Typically this server listens over TCP port 641. The additional presence of TCP port 653 is unusual for this server.

D. Possible RDO exploit.

One of the memory pages that contains strings characteristic of the B02K trojan also contains what appears to be a file listing. Many of these files, MSRDO20.DLL in particular, are mentioned in relation to a possible remote data object (RDO) exploit. http://www.google.com/search?hl=en&lr=&q=MSRDO20.DLL+EXPLOIT.

```
03DE60B0   00 00 00 00 00 00 4D 00  53 00 52 00 44 00 4F 00   ......M.S.R.D.O.
03DE60C0   32 00 30 00 2E 00 44 00  4C 00 4C 00 BA 9B C0 01   2.0...D.L.L.º›À.
03DE60D0   78 00 00 00 20 E5 00 00  00 17 B9 1E 75 21 BF 01   x... å....¹.u!¿.
03DE60E0   00 20 F8 70 BA 90 C0 01  00 17 B9 1E 75 21 BF 01   . øpº• À...¹.u!¿.
03DE60F0   00 00 00 00 00 00 00 00  10 67 00 00 00 00 00 00   .........g......
03DE6100   00 70 00 00 00 00 00 00  20 00 00 00 16 00 00 00   .p...... .......
03DE6110   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

E. Elevated security context.

UMGR32.EXE, *dfrws2005.exe* (*pid* 0x250) and *nc.exe*, as well as the two "cloaked" copies of *metasploit.exe* and the cloaked copy of *dfrws200.exe* are all running in the system security context:

UserSid: S-1-5-18

The combination of listening network connections and elevated security privileges is especially dangerous.

F. Netstat output.

Probable *netstat* output was located at page 0x1cba000 in the first memory "image" which is quoted in abbreviated form below.

```
01CBA000   37 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00   7. . . . . . .
01CBA010   20 00 20 00 20 00 20 00  30 00 2E 00 30 00 2E 00    . . . .0...0...
01CBA020   30 00 2E 00 30 00 3A 00  30 00 20 00 20 00 20 00   0...0.:.0. . . .
01CBA030   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
01CBA040   20 00 20 00 20 00 4C 00  49 00 53 00 54 00 45 00    . . .L.I.S.T.E.
01CBA050   4E 00 49 00 4E 00 47 00  20 00 20 00 20 00 20 00   N.I.N.G. . . . .
01CBA060   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
01CBA070   20 00 20 00 20 00 20 00  20 00 20 00 54 00 43 00    . . . . . .T.C.
01CBA080   50 00 20 00 20 00 20 00  20 00 30 00 2E 00 30 00   P. . . . .0...0.
01CBA090   2E 00 30 00 2E 00 30 00  3A 00 31 00 30 00 33 00   ..0...0.:.1.0.3.
01CBA0A0   33 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00   3. . . . . . . .
01CBA0B0   20 00 20 00 20 00 20 00  30 00 2E 00 30 00 2E 00    . . . .0...0...
01CBA0C0   30 00 2E 00 30 00 3A 00  30 00 20 00 20 00 20 00   0...0.:.0. . . .
01CBA0D0   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
01CBA0E0   20 00 20 00 20 00 4C 00  49 00 53 00 54 00 45 00    . . .L.I.S.T.E.
01CBA0F0   4E 00 49 00 4E 00 47 00  20 00 20 00 20 00 20 00   N.I.N.G. . . . .
01CBA100   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .

[...]

01CBA250   20 00 20 00 20 00 20 00  20 00 20 00 54 00 43 00    . . . . . .T.C.
01CBA260   50 00 20 00 20 00 20 00  20 00 31 00 39 00 32 00   P. . . . .1.9.2.
01CBA270   2E 00 31 00 36 00 38 00  2E 00 30 00 2E 00 32 00   ..1.6.8...0...2.
01CBA280   3A 00 31 00 30 00 33 00  33 00 20 00 20 00 20 00   :.1.0.3.3. . . .
01CBA290   20 00 20 00 20 00 20 00  31 00 39 00 32 00 2E 00    . . . .1.9.2...
01CBA2A0   31 00 36 00 38 00 2E 00  30 00 2E 00 35 00 3A 00   1.6.8...0...5.:.
01CBA2B0   34 00 33 00 32 00 31 00  20 00 20 00 20 00 20 00   4.3.2.1. . . . .
```

```
01CBA2C0   20 00 20 00 20 00 45 00  53 00 54 00 41 00 42 00    . . .E.S.T.A.B.
01CBA2D0   4C 00 49 00 53 00 48 00  45 00 44 00 20 00 20 00   L.I.S.H.E.D. . .
01CBA2E0   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
01CBA2F0   20 00 20 00 20 00 20 00  20 00 20 00 54 00 43 00    . . . . .T.C.
01CBA300   50 00 20 00 20 00 20 00  20 00 31 00 39 00 32 00   P. . . . .1.9.2.
01CBA310   2E 00 31 00 36 00 38 00  2E 00 30 00 2E 00 32 00   ..1.6.8...0...2.
01CBA320   3A 00 31 00 30 00 34 00  35 00 20 00 20 00 20 00   :.1.0.4.5. . . .
01CBA330   20 00 20 00 20 00 20 00  31 00 39 00 32 00 2E 00    . . . .1.9.2...
01CBA340   31 00 36 00 38 00 2E 00  30 00 2E 00 32 00 3A 00   1.6.8...0...2.:.
01CBA350   34 00 35 00 36 00 37 00  38 00 20 00 20 00 20 00   4.5.6.7.8. . . .
01CBA360   20 00 20 00 20 00 54 00  49 00 4D 00 45 00 5F 00    . . .T.I.M.E._.
01CBA370   57 00 41 00 49 00 54 00  20 00 20 00 20 00 20 00   W.A.I.T. . . . .
01CBA380   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
01CBA390   20 00 20 00 20 00 20 00  20 00 20 00 54 00 43 00    . . . . .T.C.
01CBA3A0   50 00 20 00 20 00 20 00  20 00 31 00 39 00 32 00   P. . . . .1.9.2.
01CBA3B0   2E 00 31 00 36 00 38 00  2E 00 30 00 2E 00 32 00   ..1.6.8...0...2.
01CBA3C0   3A 00 34 00 34 00 34 00  34 00 34 00 20 00 20 00   :.4.4.4.4.4. . .
01CBA3D0   20 00 20 00 20 00 20 00  31 00 39 00 32 00 2E 00    . . . .1.9.2...
01CBA3E0   31 00 36 00 38 00 2E 00  30 00 2E 00 35 00 3A 00   1.6.8...0...5.:.
01CBA3F0   31 00 31 00 30 00 35 00  20 00 20 00 20 00 20 00   1.1.0.5. . . . .
01CBA400   20 00 20 00 20 00 45 00  53 00 54 00 41 00 42 00    . . .E.S.T.A.B.
01CBA410   4C 00 49 00 53 00 48 00  45 00 44 00 20 00 20 00   L.I.S.H.E.D. . .
01CBA420   20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00    . . . . . . . .
```

Significantly, the output indicates two established connections and one connection in the time wait state. All of the connections are between local interface 192.168.0.2 and the remote host 192.168.0.5. The local ports are TCP 1033, 1045 and 44444. These ports are not among the "hidden" ports in the previously mentioned *Hacker Defender* configuration information in the first memory "image:"

```
05549D70   63 65 5D 0D 0A 0D 0A 22  5B 3E 48 3C 69 3E 64 22   ce]...."[>H<i>d"
05549D80   64 3A 65 6E 3C 3E 5C 20  50 2F 3A 6F 72 3A 74 3C   d:en<>\ P/:or:t<
05549D90   73 22 5D 5C 3A 0D 0A 54  43 50 3A 31 33 31 33 2C   s"]\:..TCP:1313,
05549DA0   33 30 30 30 0D 0A 0D 0A  5B 53 65 74 2F 74 69 6E   3000....[Set/tin
```

Curiously, the attacker does not bother to hide TCP port 44444 (*UMGR32.exe*, a.k.a. B02K). This is an artifact either of the attacker testing his rootkit or of Daniels incident response script. However, Daniels had difficulty running some of his tools and host 192.168.0.5 does not appear in Goatboy's arp cache. The first hypothesis seems the more probable, therefore.

G. Anomalies with executable sections.

Finally, it should be noted that there are a large number of processes whose base addresses could not be translated into physical addresses. The page directory for several of these processes was checked manually and the corresponding page directory entry (PDE) was found to be blank. This is odd. Typically a PDE is initialized from the process's virtual address descriptors (VAD) the first time that the corresponding virtual address is referenced. Since a process's base address must be referenced when the process is loaded, the PDE for the process base address is usually valid. The segment *based address* also was checked in the corresponding section object for several processes and was

found to be relocated from the section *base address* in the process's *eprocess* block. Typically these are the same.

One possible explanation is that this is an artifact of the process section being modified as part of the infection process. Process sections are copy-on-write. When someone writes to a page that is part of a process section the modified page is copied to a new location that is backed by the page file, not the executable file on disk. Perhaps the PDE entries are invalidated as part of this copy-on-write process. On the other hand, in examining a Windows 2000 system available to us, several processes (by a certain anti-virus vendor) were found that exhibited similar features. Further study is required before any conclusions may be drawn from this phenomenon. Unfortunately, the relevant page file was overwritten when Daniels allowed Goatboy's laptop to reboot so we may not be able to answer the question in this case.

A logical next step would be to extract modules related to the rootkit for further study. Unfortunately, the process section anomalies make this difficult to do directly. The source code is available for both *Hacker Defender* and B02K. With time a reference copy of the rootkit could be compiled and the modules located using a page by page comparison of the reference copy with the contents of the two memory "images." The same may be done with rootkit files remaining on the hard drive of Goatboy's computer. However, this is beyond the scope of the present report.

3. Why did "plist.exe" and "fport.exe" not work on the compromised system?

We were not able determine the answer to this question. Logically it would not be due to the normal operation of the rootkit. The purpose of a rootkit is to hide, in part by modifying the output of tools such as *pslist* and *fport*. Not allowing these tools to run is bound to attract suspicion and is therefore counter productive.

It should be noted that *Helix* is using a relative path to load at least some of its tools:

```
      Command Line: ..\Acquisition\FAU\dd.exe if=\\.\PhysicalMemory
of=F:\intrusion2005\physicalmemory.dd conv=noerror --md5sum --verifymd5
--md5out=F:\intrusion2005\physicalmemory.dd.md5                    --
log=F:\intrusion2005\audit.log
```

The subject computer contains files named *fport.exe* and *pslist.exe* in its system32 directory. The system32 directory does not contain any file by the name of *dd.exe*. Perhaps Daniels accidentally loaded the *pslist* and *fport* from the rootkit rather than from his tools.

4. Was the intruder specifically seeking Professor Goatboy's research materials?

The challenge description does not specifically identify Professor Goatboy's research; however, presumably the question relates to certain *pdf* documents that are contained in a directory conveniently labeled "New Research - Private." Memory pages from the first memory dump apparently relating to B02K reference Professor Goatboy's research. In fact, taken as a whole, the attacker who used B02K appears to have been interested in little else.

```
03DE6C50   42 00 00 00 7D C1 1B 00  00 00 00 00 16 00 00 00   B...}Á.........
03DE6C60   8E 00 00 00 00 53 54 43  50 49 4F 00 4E 55 4C 4C   Ž....STCPIO.NULL
03DE6C70   00 4E 55 4C 4C 41 55 54  48 00 63 3A 5C 44 6F 63   .NULLAUTH.c:\Doc
03DE6C80   75 6D 65 6E 74 73 20 61  6E 64 20 53 65 74 74 69   uments and Setti
03DE6C90   6E 67 73 5C 41 64 6D 69  6E 69 73 74 72 61 74 6F   ngs\Administrato
03DE6CA0   72 5C 4D 79 20 44 6F 63  75 6D 65 6E 74 73 5C 4E   r\My Documents\N
03DE6CB0   65 77 20 52 65 73 65 61  72 63 68 20 2D 20 50 72   ew Research - Pr
03DE6CC0   69 76 61 74 65 21 5C 44  6F 20 6E 6F 74 20 64 69   ivate!\Do not di
03DE6CD0   73 74 72 69 62 75 74 65  5C 53 65 6D 61 70 68 6F   stribute\Semapho
03DE6CE0   72 65 73 20 55 73 69 6E  67 20 53 74 6F 63 68 61   res Using Stocha
03DE6CF0   73 74 69 63 20 43 6F 6E  66 69 67 75 72 61 74 69   stic Configurati
03DE6D00   6F 6E 73 2E 70 64 66 00  00 00 00 00 00 00 00 00   ons.pdf.........
03DE6D10   1B 00 1A 00 00 01 0C 00  00 00 00 00 00 1A B7 93   ..............·“
03DE6D20   C4 00 00 00 01 00 00 00  42 00 00 00 7D C1 1B 00   Ä.......B...}Á..
03DE6D30   00 00 00 00 16 00 00 00  8E 00 00 00 2C 53 54 43   ........Ž...,STC
03DE6D40   50 49 4F 2C 4E 55 4C 4C  2C 4E 55 4C 4C 41 55 54   PIO,NULL,NULLAUT
03DE6D50   48 00 63 3A 5C 44 6F 63  75 6D 65 6E 74 73 20 61   H.c:\Documents a
03DE6D60   6E 64 20 53 65 74 74 69  6E 67 73 5C 41 64 6D 69   nd Settings\Admi
03DE6D70   6E 69 73 74 72 61 74 6F  72 5C 4D 79 20 44 6F 63   nistrator\My Doc
03DE6D80   75 6D 65 6E 74 73 5C 4E  65 77 20 52 65 73 65 61   uments\New Resea
03DE6D90   72 63 68 20 2D 20 50 72  69 76 61 74 65 21 5C 44   rch - Private!\D
03DE6DA0   6F 20 6E 6F 74 20 64 69  73 74 72 69 62 75 74 65   o not distribute
03DE6DB0   5C 53 65 6D 61 70 68 6F  72 65 73 20 55 73 69 6E   \Semaphores Usin
03DE6DC0   67 20 53 74 6F 63 68 61  73 74 69 63 20 43 6F 6E   g Stochastic Con
03DE6DD0   66 69 67 75 72 61 74 69  6F 6E 73 2E 70 64 66 00   figurations.pdf.
03DE6DE0   00 00 00 00 00 00 00 00  29 00 1B 00 00 01 0C 00   ........).......
```

and

```
0004E190   00 00 3F 00 00 00 00 00  00 00 46 69 6C 65 20 65   ..?.......File e
0004E1A0   6D 69 74 20 73 74 61 72  74 65 64 20 66 72 6F 6D   mit started from
0004E1B0   3A 20 31 39 32 2E 31 36  38 2E 30 2E 32 3A 31 30   : 192.168.0.2:10
0004E1C0   36 39 2C 53 54 43 50 49  4F 2C 4E 55 4C 4C 2C 4E   69,STCPIO,NULL,N
0004E1D0   55 4C 4C 41 55 54 48 0A  00 00 00 00 00 00 00 00   ULLAUTH.........
0004E1E0   74 73 7C 0A 00 00 00 00  00 00 00 00 00 00 00 00   ts|.............
0004E1F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
0004E200   00 00 0C 00 00 E3 04 00  00 03 05 00 00 00 0C 02   .....ã..........
0004E210   1A 70 2D 01 36 00 00 00  54 E1 A9 07 B4 85 00 00   .p-.6...Tá©.´….. 
0004E220   00 00 E2 8A C4 6B 08 00  46 18 65 AD 08 00 45 00   ..âŠÄk..F.e-..E.
0004E230   00 34 12 1B 40 00 80 06  67 51 C0 A8 00 02 C0 A8   .4..@.€.gQÀ¨..À¨
0004E240   00 05 04 2D 04 D7 C7 63  80 AA 7E BF B0 2A 80 12   ...-.×Çc€ª~¿°*€.
0004E250   44 70 29 44 00 00 02 04  05 B4 01 03 03 00 01 01   Dp)D.....´......
0004E260   04 02 1F 22 00 00 5A BF  73 2B 8A D8 67 0B 46 FF   ..."..Z¿s+ŠØg.Fÿ
0004E270   34 4E 8A 0D 08 E2 CD C3  13 37 00 15 C2 89 7E 00   4NŠ..âÍÃ.7..Â‰~.
0004E280   00 00 02 00 00 00 FF FF  FF FF 1A 0A 1B 00 01 00   ......ÿÿÿÿ......
0004E290   00 00 5E 00 00 00 00 00  00 00 53 45 4D 41 50 48   ..^.......SEMAPH
0004E2A0   7E 31 2E 50 44 46 20 20  20 20 20 39 38 36 32 39   ~1.PDF     98629
0004E2B0   20 2D 41 2D 2D 2D 2D 2D  20 30 35 2D 33 30 2D 30    -A----- 05-30-0
0004E2C0   35 20 31 32 3A 34 37 20  53 65 6D 61 70 68 6F 72   5 12:47 Semaphor
0004E2D0   65 73 20 55 73 69 6E 67  20 53 74 6F 63 68 61 73   es Using Stochas
0004E2E0   74 69 63 20 43 6F 6E 66  69 67 75 72 61 74 69 6F   tic Configuratio
0004E2F0   6E 73 2E 70 64 66 0A 00  00 00 00 00 00 00 00 00   ns.pdf.........
```

```
[...]

0004E290   00 00 5E 00 00 00 00 00  00 00 53 45 4D 41 50 48   ..^.......SEMAPH
0004E2A0   7E 31 2E 50 44 46 20 20  20 20 20 39 38 36 32 39   ~1.PDF     98629
0004E2B0   20 2D 41 2D 2D 2D 2D 2D  20 30 35 2D 33 30 2D 30    -A----- 05-30-0
0004E2C0   35 20 31 32 3A 34 37 20  53 65 6D 61 70 68 6F 72   5 12:47 Semaphor
0004E2D0   65 73 20 55 73 69 6E 67  20 53 74 6F 63 68 61 73   es Using Stochas
0004E2E0   74 69 63 20 43 6F 6E 66  69 67 75 72 61 74 69 6F   tic Configuratio
0004E2F0   6E 73 2E 70 64 66 0A 00  00 00 00 00 00 00 00 00   ns.pdf.........

[...]

0004E480   01 00 02 00 00 00 FF FF  FF FF 1A 0A 1B 00 01 00   ......ÿÿÿÿ......
0004E490   00 00 46 00 00 00 00 00  00 00 50 32 50 4D 4F 44   ..F.......P2PMOD
0004E4A0   7E 31 2E 50 44 46 20 20  20 20 20 35 38 33 37 34   ~1.PDF     58374
0004E4B0   20 2D 41 2D 2D 2D 2D 2D  20 30 35 2D 33 30 2D 30    -A----- 05-30-0
0004E4C0   35 20 31 32 3A 34 39 20  50 32 50 20 4D 6F 64 65   5 12:49 P2P Mode
0004E4D0   6C 20 43 68 65 63 6B 69  6E 67 2E 70 64 66 0A 00   l Checking.pdf..

and

00E53190   00 00 3F 00 00 00 00 00  00 00 46 69 6C 65 20 65   ..?.......File e
00E531A0   6D 69 74 20 73 74 61 72  74 65 64 20 66 72 6F 6D   mit started from
00E531B0   3A 20 31 39 32 2E 31 36  38 2E 30 2E 32 3A 31 30   : 192.168.0.2:10
00E531C0   36 39 2C 53 54 43 50 49  4F 2C 4E 55 4C 4C 2C 4E   69,STCPIO,NULL,N
00E531D0   55 4C 4C 41 55 54 48 0A  00 00 00 00 00 00 00 00   ULLAUTH.........
00E531E0   74 73 7C 0A 00 00 00 00  00 00 00 00 00 00 00 00   ts|.............
00E531F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00E53200   00 00 0C 00 00 E3 04 00  00 03 05 00 00 00 0C 02   .....ã..........
00E53210   1A 70 2D 01 36 00 00 00  54 E1 A9 07 B4 85 00 00   .p-.6...Tá©.´….. 
00E53220   00 00 E2 8A C4 6B 08 00  46 18 65 AD 08 00 45 00   ..âŠÄk..F.e-..E.
00E53230   00 34 12 1B 40 00 80 06  67 51 C0 A8 00 02 C0 A8   .4..@.€.gQÀ¨..À¨
00E53240   00 05 04 2D 04 D7 C7 63  80 AA 7E BF B0 2A 80 12   ...-.×Çc€ª~¿°*€.
00E53250   44 70 29 44 00 00 02 04  05 B4 01 03 03 00 01 01   Dp)D.....´......
00E53260   04 02 1F 22 00 00 5A BF  73 2B 8A D8 67 0B 46 FF   ..."..Z¿s+ŠØg.Fÿ
00E53270   34 4E 8A 0D 08 E2 CD C3  13 37 00 15 C2 89 7E 00   4NŠ..âÍÃ.7..Â‰~.
00E53280   00 00 02 00 00 00 FF FF  FF FF 1A 0A 1B 00 01 00   ......ÿÿÿÿ......
00E53290   00 00 5E 00 00 00 00 00  00 00 53 45 4D 41 50 48   ..^.......SEMAPH
00E532A0   7E 31 2E 50 44 46 20 20  20 20 20 39 38 36 32 39   ~1.PDF     98629
00E532B0   20 2D 41 2D 2D 2D 2D 2D  20 30 35 2D 33 30 2D 30    -A----- 05-30-0
00E532C0   35 20 31 32 3A 34 37 20  53 65 6D 61 70 68 6F 72   5 12:47 Semaphor
00E532D0   65 73 20 55 73 69 6E 67  20 53 74 6F 63 68 61 73   es Using Stochas
00E532E0   74 69 63 20 43 6F 6E 66  69 67 75 72 61 74 69 6F   tic Configuratio
00E532F0   6E 73 2E 70 64 66 0A 00  00 00 00 00 00 00 00 00   ns.pdf.........
[...]
00E53590   00 00 12 00 00 00 00 00  00 00 33 20 6D 61 74 63   ..........3 matc
00E535A0   68 65 73 20 66 6F 75 6E  64 2E 0A 00 00 00 00 00   hes found.......
[...]
00E53B80   00 00 02 00 00 00 FF FF  FF FF 00 00 00 00 01 00   ......ÿÿÿÿ......
00E53B90   00 00 48 00 00 00 00 00  00 00 50 32 50 4D 4F 44   ..H.......P2PMOD
00E53BA0   7E 31 2E 50 44 46 20 20  20 20 20 35 38 33 37 34   ~1.PDF     58374
00E53BB0   20 2D 41 2D 2D 2D 2D 2D  20 30 35 2D 33 30 2D 32    -A----- 05-30-2
00E53BC0   30 30 35 20 31 32 3A 34  39 20 50 32 50 20 4D 6F   005 12:49 P2P Mo
00E53BD0   64 65 6C 20 43 68 65 63  6B 69 6E 67 2E 70 64 66   del Checking.pdf

and also,

07548010   76 00 00 00 2C 53 54 43  50 49 4F 2C 4E 55 4C 4C   v...,STCPIO,NULL
07548020   2C 4E 55 4C 4C 41 55 54  48 00 63 3A 5C 44 6F 63   ,NULLAUTH.c:\Doc
07548030   75 6D 65 6E 74 73 20 61  6E 64 20 53 65 74 74 69   uments and Setti
07548040   6E 67 73 5C 41 64 6D 69  6E 69 73 74 72 61 74 6F   ngs\Administrato
07548050   72 5C 4D 79 20 44 6F 63  75 6D 65 6E 74 73 5C 4E   r\My Documents\N
07548060   65 77 20 52 65 73 65 61  72 63 68 20 2D 20 50 72   ew Research - Pr
07548070   69 76 61 74 65 21 5C 44  6F 20 6E 6F 74 20 64 69   ivate!\Do not di
07548080   73 74 72 69 62 75 74 65  5C 50 32 50 20 4D 6F 64   stribute\P2P Mod
07548090   65 6C 20 43 68 65 63 6B  69 6E 67 2E 70 64 66 00   el Checking.pdf.
075480A0   00 00 00 00 00 00 00 00  06 00 18 00 00 01 0C 00   ................
[...]
07548280   00 00 00 00 3F 00 00 00  00 00 00 00 00 46 69 6C   ....?.......File
07548290   20 65 6D 69 74 20 73 74  61 72 74 65 64 20 66 72    emit started fr
075482A0   6F 6D 3A 20 31 39 32 2E  31 36 38 2E 30 2E 32 3A   om: 192.168.0.2:
```

```
075482B0   31 30 36 39 2C 53 54 43  50 49 4F 2C 4E 55 4C 4C   1069,STCPIO,NULL
075482C0   2C 4E 55 4C 4C 41 55 54  48 0A 00 00 00 00 00 00   ,NULLAUTH.......
075482D0   10 00 0D 00 00 01 0D 00  00 00 00 00 00 1B 05 56   ...............V
075482E0   6B 00 00 00 02 00 00 00  FF FF FF FF 8F B7 1A 00   k.......ÿÿÿÿ• ·..
075482F0   01 00 00 00 4B 00 00 00  00 00 00 00 28 37 31 29   ....K.......(71)
07548300   20 50 72 6F 63 65 73 73  20 43 6F 6E 74 72 6F 6C    Process Control
07548310   5C 53 74 61 72 74 20 50  72 6F 63 65 73 73 7C 30   \Start Process|0
07548320   3D 53 68 6F 77 2C 20 31  3D 48 69 64 65 7C 50 61   =Show, 1=Hide|Pa
07548330   74 68 6E 61 6D 65 20 61  6E 64 20 61 72 67 75 6D   thname and argum
07548340   65 6E 74 73 7C 0A 00 00  00 00 00 00 00 00 00 00   ents|...........
07548350   0D 00 10 00 00 01 0C 00  00 00 00 00 00 1B 05 6A   ...............j
07548360   54 00 00 00 02 00 00 00  FF FF FF FF 00 00 00 00   T.......ÿÿÿÿ....
07548370   01 00 00 00 34 00 00 00  00 00 00 00 20 20 20 20   ....4.......
07548380   20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
07548390   20 30 20 44 2D 2D 2D 2D  2D 2D 20 30 35 2D 33 30    0 D------ 05-30
075483A0   2D 32 30 30 35 20 31 32  3A 34 37 20 2E 2E 0A 00   -2005 12:47 ....
075483B0   00 00 00 00 00 00 00 00  11 00 0D 00 00 01 08 00   ................
075483C0   1F 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
075483D0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
075483E0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
075483F0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
07548400   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
07548410   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
07548420   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
07548430   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
07548440   12 00 11 00 00 01 08 00  00 00 00 00 00 1B 05 6B   ...............k
07548450   80 00 00 00 02 00 00 00  FF FF FF FF 00 00 00 00   €.......ÿÿÿÿ....
07548460   01 00 00 00 60 00 00 00  00 00 00 00 53 45 4D 41   ....`.......SEMA
07548470   50 48 7E 31 2E 50 44 46  20 20 20 20 20 39 38 36   PH~1.PDF     986
07548480   32 39 20 2D 41 2D 2D 2D  2D 2D 20 30 35 2D 33 30   29 -A----- 05-30
07548490   2D 32 30 30 35 20 31 32  3A 34 37 20 53 65 6D 61   -2005 12:47 Sema
075484A0   70 68 6F 72 65 73 20 55  73 69 6E 67 20 53 74 6F   phores Using Sto
075484B0   63 68 61 73 74 69 63 20  43 6F 6E 66 69 67 75 72   chastic Configur
075484C0   61 74 69 6F 6E 73 2E 70  64 66 0A 00 00 00 00 00   ations.pdf......
[...]
07548C30   81 00 00 00 02 00 00 00  FF FF FF FF 00 00 00 00   • .......ÿÿÿÿ....
07548C40   01 00 00 00 61 00 00 00  00 00 00 00 49 4E 54 55   ....a.......INTU
07548C50   49 54 7E 31 2E 50 44 46  20 20 20 20 20 38 37 39   IT~1.PDF     879
07548C60   38 34 20 2D 41 2D 2D 2D  2D 2D 20 30 35 2D 33 30   84 -A----- 05-30
07548C70   2D 32 30 30 35 20 31 32  3A 34 39 20 49 6E 74 75   -2005 12:49 Intu
07548C80   69 74 69 76 65 20 55 6E  69 66 69 63 61 74 69 6F   itive Unificatio
07548C90   6E 20 6F 66 20 46 69 62  65 72 2D 4F 70 74 69 63   n of Fiber-Optic
07548CA0   20 43 61 62 6C 65 73 2E  70 64 66 0A 00 00 00 00    Cables.pdf.....
```

The second memory dump contained similar references.

5. Did the intruder obtain the Professor's research?

A search of the handle tables and object directory in the first and second memory "images" did not reveal any open file handles containing *.pdf* extensions or the terms "stochastic," "New Research," "semaphore," "P2P," or "intuitive." This should come as no surprise. An open file handle would not need to be kept open once the intruder loaded its file contents into memory. It is also possible for a kernel mode driver to obtain access to the file by means of a pointer rather than by handle. In additional the intruder might simply bypass the files system altogether and read file contents directly from the volume or drive.

The next logical step would be to take Goatboy's research and compare the file contents with the contents of each physical page. If all or part of one of Goatboy's files was loaded into memory it might be reasonable to infer that the

intruder was successful in his attempt. But we do not have access to Goatboy's research files.

As a poor substitute we searched for the term "goatboy" under the assumption that any self-respecting professor would put his own name in his research (lest someone else stumble on the research and think that it was his own). In retrospect this was probably a foolish assumption since *pdf* files usually have high levels of entropy and are encrypted. However the search led to a startling discovery. There are a number of memory pages which contain the term "Goatboy" within the context of "Ghostscript 7.07," "dvips" and "latex." One of these pages is reproduced in relevant part below:

```
00AAA280   37 0A 35 38 37 5D 0A 3E  3E 0A 65 6E 64 6F 62 6A   7.587].>>.endobj
00AAA290   0A 32 20 30 20 6F 62 6A  0A 3C 3C 2F 50 72 6F 64   .2 0 obj.<</Prod
00AAA2A0   75 63 65 72 28 47 4E 55  20 47 68 6F 73 74 73 63   ucer(GNU Ghostsc
00AAA2B0   72 69 70 74 20 37 2E 30  37 29 0A 2F 43 72 65 61   ript 7.07)./Crea
00AAA2C0   74 6F 72 28 64 76 69 70  73 5C 28 6B 5C 29 20 35   tor(dvips\(k\) 5
00AAA2D0   2E 39 32 62 20 43 6F 70  79 72 69 67 68 74 20 32   .92b Copyright 2
00AAA2E0   30 30 32 20 52 61 64 69  63 61 6C 20 45 79 65 20   002 Radical Eye
00AAA2F0   53 6F 66 74 77 61 72 65  29 0A 2F 54 69 74 6C 65   Software)./Title
00AAA300   28 73 63 69 6D 61 6B 65  6C 61 74 65 78 2E 38 35   (scimakelatex.85
00AAA310   32 34 36 2E 47 6F 61 74  62 6F 79 2E 64 76 69 29   246.Goatboy.dvi)
00AAA320   3E 3E 65 6E 64 6F 62 6A  0A 78 72 65 66 0A 30 20   >>endobj.xref.0
00AAA330   37 34 0A 30 30 30 30 30  30 30 30 30 30 20 36 35   74.0000000000 65
00AAA340   35 33 35 20 66 20 0A 30  30 30 30 30 33 34 36 33   535 f .000003463
00AAA350   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
00AAA360   38 36 32 37 33 20 30 30  30 30 30 20 6E 20 0A 30   86273 00000 n .0
00AAA370   30 30 30 30 33 34 35 35  31 20 30 30 30 30 30 20   000034551 00000
00AAA380   6E 20 0A 30 30 30 30 30  33 34 36 38 36 20 30 30   n .0000034686 00
00AAA390   30 30 30 20 6E 20 0A 30  30 30 30 30 33 33 38 31   000 n .000003381
00AAA3A0   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
00AAA3B0   30 30 30 31 35 20 30 30  30 30 30 20 6E 20 0A 30   00015 00000 n .0
00AAA3C0   30 30 30 30 30 35 31 30  35 20 30 30 30 30 30 20   000005105 00000
00AAA3D0   6E 20 0A 30 30 30 30 30  34 30 30 35 31 20 30 30   n .0000040051 00
00AAA3E0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 39 37 37   000 n .000003977
00AAA3F0   37 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   7 00000 n .00000
00AAA400   38 33 34 34 36 20 30 30  30 30 30 20 6E 20 0A 30   83446 00000 n .0
00AAA410   30 30 30 30 33 38 37 32  35 20 30 30 30 30 30 20   000038725 00000
00AAA420   6E 20 0A 30 30 30 30 30  33 38 35 30 32 20 30 30   n .0000038502 00
00AAA430   30 30 30 20 6E 20 0A 30  30 30 30 30 38 33 31 30   000 n .000008310
00AAA440   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
00AAA450   33 35 34 34 39 20 30 30  30 30 30 20 6E 20 0A 30   35449 00000 n .0
00AAA460   30 30 30 30 33 35 31 36  32 20 30 30 30 30 30 20   000035162 00000
00AAA470   6E 20 0A 30 30 30 30 30  38 32 31 37 39 20 30 30   n .0000082179 00
00AAA480   30 30 30 20 6E 20 0A 30  30 30 30 30 34 38 37 34   000 n .000004874
00AAA490   30 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   0 00000 n .00000
00AAA4A0   34 38 32 33 33 20 30 30  30 30 30 20 6E 20 0A 30   48233 00000 n .0
00AAA4B0   30 30 30 30 38 31 33 37  36 20 30 30 30 30 30 20   000081376 00000
00AAA4C0   6E 20 0A 30 30 30 30 30  33 34 37 34 31 20 30 30   n .0000034741 00
00AAA4D0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 37 37   000 n .000003477
00AAA4E0   31 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   1 00000 n .00000
00AAA4F0   33 33 39 37 35 20 30 30  30 30 30 20 6E 20 0A 30   33975 00000 n .0
00AAA500   30 30 30 30 30 35 31 32  35 20 30 30 30 30 30 20   000005125 00000
00AAA510   6E 20 0A 30 30 30 30 30  31 30 36 30 38 20 30 30   n .0000010608 00
00AAA520   30 30 30 20 6E 20 0A 30  30 30 30 30 38 33 30 34   000 n .000008304
00AAA530   36 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   6 00000 n .00000
00AAA540   38 32 39 37 31 20 30 30  30 30 30 20 6E 20 0A 30   82971 00000 n .0
00AAA550   30 30 30 30 34 34 32 38  34 20 30 30 30 30 30 20   000044284 00000
00AAA560   6E 20 0A 30 30 30 30 30  34 33 39 34 33 20 30 30   n .0000043943 00
00AAA570   30 30 30 20 6E 20 0A 30  30 30 30 30 38 30 35 37   000 n .000008057
00AAA580   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
00AAA590   34 33 34 33 34 20 30 30  30 30 30 20 6E 20 0A 30   43434 00000 n .0
00AAA5A0   30 30 30 30 34 33 32 32  33 20 30 30 30 30 30 20   000043223 00000
00AAA5B0   6E 20 0A 30 30 30 30 30  38 30 34 33 39 20 30 30   n .0000080439 00
```

```
00AAA5C0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 38 33   000 n .000003483
00AAA5D0   36 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   6 00000 n .00000
00AAA5E0   33 34 31 31 39 20 30 30  30 30 30 20 6E 20 0A 30   34119 00000 n .0
00AAA5F0   30 30 30 30 31 30 36 32  39 20 30 30 30 30 30 20   000010629 00000
00AAA600   6E 20 0A 30 30 30 30 30  32 32 30 37 39 20 30 30   n .0000022079 00
00AAA610   30 30 30 20 6E 20 0A 30  30 30 30 30 38 30 33 37   000 n .000008037
00AAA620   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
00AAA630   37 39 35 31 31 20 30 30  30 30 30 20 6E 20 0A 30   79511 00000 n .0
00AAA640   30 30 30 30 36 34 38 31  30 20 30 30 30 30 30 20   000064810 00000
00AAA650   6E 20 0A 30 30 30 30 30  36 34 35 32 30 20 30 30   n .0000064520 00
00AAA660   30 30 30 20 6E 20 0A 30  30 30 30 30 37 39 35 38   000 n .000007958
00AAA670   34 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   4 00000 n .00000
00AAA680   36 32 39 34 39 20 30 30  30 30 30 20 6E 20 0A 30   62949 00000 n .0
00AAA690   30 30 30 30 36 32 37 31  38 20 30 30 30 30 30 20   000062718 00000
00AAA6A0   6E 20 0A 30 30 30 30 30  37 39 32 38 30 20 30 30   n .0000079280 00
00AAA6B0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 39 31   000 n .000003491
00AAA6C0   32 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   2 00000 n .00000
00AAA6D0   33 34 32 36 33 20 30 30  30 30 30 20 6E 20 0A 30   34263 00000 n .0
00AAA6E0   30 30 30 30 32 32 31 30  31 20 30 30 30 30 30 20   000022101 00000
00AAA6F0   6E 20 0A 30 30 30 30 30  33 32 38 37 38 20 30 30   n .0000032878 00
00AAA700   30 30 30 20 6E 20 0A 30  30 30 30 30 35 36 38 31   000 n .000005681
00AAA710   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
00AAA720   35 36 34 30 30 20 30 30  30 30 30 20 6E 20 0A 30   56400 00000 n .0
00AAA730   30 30 30 30 38 35 34 37  35 20 30 30 30 30 30 20   000085475 00000
00AAA740   6E 20 0A 30 30 30 30 30  37 34 33 36 32 20 30 30   n .0000074362 00
00AAA750   30 30 30 20 6E 20 0A 30  30 30 30 30 37 34 30 34   000 n .000007404
00AAA760   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
00AAA770   38 35 30 32 36 20 30 30  30 30 30 20 6E 20 0A 30   85026 00000 n .0
00AAA780   30 30 30 30 36 38 31 36  37 20 30 30 30 30 30 20   000068167 00000
00AAA790   6E 20 0A 30 30 30 30 30  36 37 38 32 37 20 30 30   n .0000067827 00
00AAA7A0   30 30 30 20 6E 20 0A 30  30 30 30 30 38 34 32 33   000 n .000008423
00AAA7B0   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
00AAA7C0   33 34 39 38 38 20 30 30  30 30 30 20 6E 20 0A 30   34988 00000 n .0
00AAA7D0   30 30 30 30 33 34 34 30  37 20 30 30 30 30 30 20   000034407 00000
00AAA7E0   6E 20 0A 30 30 30 30 30  33 32 39 30 30 20 30 30   n .0000032900 00
00AAA7F0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 33 37 39   000 n .000003379
00AAA800   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
00AAA810   33 35 30 39 37 20 30 30  30 30 30 20 6E 20 0A 30   35097 00000 n .0
00AAA820   30 30 30 30 33 38 34 38  31 20 30 30 30 30 30 20   000038481 00000
00AAA830   6E 20 0A 30 30 30 30 30  33 39 37 35 37 20 30 30   n .0000039757 00
00AAA840   30 30 30 20 6E 20 0A 30  30 30 30 30 34 33 32 30   000 n .000004320
00AAA850   32 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   2 00000 n .00000
00AAA860   34 33 39 32 33 20 30 30  30 30 30 20 6E 20 0A 30   43923 00000 n .0
00AAA870   30 30 30 30 34 38 32 31  32 20 30 30 30 30 30 20   000048212 00000
00AAA880   6E 20 0A 30 30 30 30 30  35 36 33 37 39 20 30 30   n .0000056379 00
00AAA890   30 30 30 20 6E 20 0A 30  30 30 30 30 36 32 36 39   000 n .000006269
00AAA8A0   37 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   7 00000 n .00000
00AAA8B0   36 34 34 39 39 20 30 30  30 30 30 20 6E 20 0A 30   64499 00000 n .0
00AAA8C0   30 30 30 30 36 37 38 30  36 20 30 30 30 30 30 20   000067806 00000
00AAA8D0   6E 20 0A 30 30 30 30 30  37 34 30 32 38 20 30 30   n .0000074028 00
00AAA8E0   30 30 30 20 6E 20 0A 30  30 30 30 30 37 39 32 35   000 n .000007925
00AAA8F0   39 20 30 30 30 30 30 20  6E 20 0A 74 72 61 69 6C   9 00000 n .trail
00AAA900   65 72 0A 3C 3C 20 2F 53  69 7A 65 20 37 34 20 2F   er.<< /Size 74 /
00AAA910   52 6F 6F 74 20 31 20 30  20 52 20 2F 49 6E 66 6F   Root 1 0 R /Info
00AAA920   20 32 20 30 20 52 0A 3E  3E 0A 73 74 61 72 74 78    2 0 R.>>.startx
00AAA930   72 65 66 0A 38 36 34 32  35 0A 25 25 45 4F 46 0A   ref.86425.%%EOF.
00AAA940   2B C1 74 11 89 1E 89 4F  1C C7 45 F4 10 00 00 C0   +Át.‰.‰O.ÇEô...À
00AAA950   E9 DC 01 00 00 8B 06 8B  56 04 89 1E 89 45 E8 8D   éÜ...‹.‹V.‰.‰Eè•
00AAA960   45 E8 89 55 FC 50 8D 45  B8 50 8D 45 DC 68 FF 0F   Eè‰UüP• E¸P• EÜhÿ.
00AAA970   1F 00 50 89 4F 1C C7 45  B8 18 00 00 00 89 5D BC   ..P‰O.ÇE¸....‰]¼
00AAA980   89 5D C0 89 5D C4 89 5D  C8 89 5D CC 89 5D EC FF   ‰]À‰]Ä‰]È‰]Ì‰]ìÿ
00AAA990   15 F8 07 01 00 85 C0 0F  8C 94 01 00 00 8B 45 FC   .ø...…À.Œ”...‹Eü
00AAA9A0   89 5D EC 89 45 E8 8D 45  E8 50 8D 45 B8 50 8D 45   ‰]ì‰Eè• EèP• E¸P• E
00AAA9B0   F0 68 FF 0F 1F 00 50 FF  15 F8 07 01 00 85 C0 7C   ðhÿ...Pÿ.ø...…À|
00AAA9C0   6C 8D 45 0C 50 68 FF 00  0F 00 FF 75 F0 FF 15 F4   l• E.Phÿ...ÿuðÿ.ô
00AAA9D0   07 01 00 85 C0 7C 4D 8D  45 D0 50 6A 01 8D 45 B8   ...…À|M• EÐPj.• E¸
00AAA9E0   53 50 68 FF 00 0F 00 FF  75 0C FF 15 F0 07 01 00   SPhÿ...ÿu.ÿ.ð...
00AAA9F0   85 C0 7C 27 8D 45 D0 6A  08 50 6A 09 FF 75 DC 89   …À|'• EÐj.Pj.ÿuÜ‰
00AAAA00   5D D4 FF 15 EC 07 01 00  85 C0 7C 06 C7 06 01 00   ]Ôÿ.ì...…À|.Ç...
00AAAA10   00 00 FF 75 D0 FF 15 C0  07 01 00 FF 75 0C FF 15   ..ÿuÐÿ.À...ÿu.ÿ.
```

```
00AAAA20   C0 07 01 00 FF 75 F0 FF  15 C0 07 01 00 FF 75 DC   À...ÿuðÿ.À...ÿuÜ
00AAAA30   FF 15 C0 07 01 00 E9 F6  00 00 00 8B 0E 8D 46 04   ÿ.À...éö...‹.• F.
00AAAA40   89 45 FC 89 1E 8B 00 C7  47 1C 04 00 00 00 89 45   ‰Eü‰.‹.ÇG.....‰E
00AAAA50   D8 8D 45 F8 50 51 FF 15  E4 07 01 00 85 C0 0F 8C   Ø• EøPQÿ.ä....…À.Œ
00AAAA60   CD 00 00 00 FF 75 F8 FF  15 E0 07 01 00 8D 45 E0   Í...ÿuøÿ.à...• Eà
00AAAA70   53 50 53 53 68 00 00 00  80 FF 75 D8 FF 15 DC 07   SPSSh...€ÿuØÿ.Ü.
00AAAA80   01 00 85 C0 0F 8C 98 00  00 00 8B 45 E0 66 83 38   ..…À.Œ˜...‹Eàfƒ8
00AAAA90   05 75 2C 66 83 78 02 70  75 25 56 50 E8 E7 FC FF   .u,fƒx.pu%VPèçüÿ
00AAAAA0   FF 3B C3 89 45 E4 74 7A  8B 4D FC C7 06 01 00 00   ÿ;Ã‰Eätz‹MüÇ....
00AAAAB0   00 8B 45 E4 01 47 1C 83  C0 F4 66 89 01 EB 63 8D   .‹Eä.G.ƒÀôf‰.ëc•
00AAAAC0   4D E4 51 8D 8D B8 FB FF  FF 68 00 04 00 00 51 50   MäQ•• ¸ûÿÿh....QP
00AAAAD0   FF 15 CC 07 01 00 85 C0  7C 3F 39 9D BC FB FF FF   ÿ.Ì...…À|?9• ¼ûÿÿ
00AAAAE0   74 37 A1 84 08 01 00 53  8B 5D FC 83 C0 EC 66 89   t7¡„...S‹]üƒÀìf‰
00AAAAF0   46 06 8D 46 0C 89 46 08  8D 85 B8 FB FF FF 50 53   F.• F.‰F.• …¸ûÿÿPS
00AAAB00   FF 15 C8 07 01 00 85 C0  7C 0F 0F B7 03 83 C0 08   ÿ.È...…À|..·.ƒÀ.
00AAAB10   C7 06 01 00 00 00 01 47  1C 8B 4D E0 FF 15 D8 07   Ç......G.‹Màÿ.Ø.
00AAAB20   01 00 FF 15 D4 07 01 00  8B 4D F8 FF 15 D8 07 01   ..ÿ.Ô...‹Møÿ.Ø..
00AAAB30   00 8B 75 F4 32 D2 8B CF  89 77 18 FF 15 D0 07 01   .‹uô2Ò‹Ï‰w.ÿ.Ð..
00AAAB40   00 8B C6 5F 5E 5B C9 C2  08 00 5C 00 44 00 6F 00   .‹Æ_^[ÉÂ..\.D.o.
00AAAB50   73 00 44 00 65 00 76 00  69 00 63 00 65 00 73 00   s.D.e.v.i.c.e.s.
00AAAB60   5C 00 48 00 78 00 44 00  65 00 66 00 44 00 72 00   \.H.x.D.e.f.D.r.
00AAAB70   69 00 76 00 65 00 72 00  00 00 55 8B EC 51 51 8D   i.v.e.r...U‹ìQQ•
00AAAB80   45 F8 68 62 06 01 00 50  FF 15 04 08 01 00 8D 45   Eøhb...Pÿ.....• E
00AAAB90   F8 50 FF 15 00 08 01 00  FF 35 80 08 01 00 FF 15   øPÿ.....ÿ5€...ÿ.
00AAABA0   FC 07 01 00 C9 C2 04 00  5C 00 44 00 65 00 76 00   ü...ÉÂ..\.D.e.v.
00AAABB0   69 00 63 00 65 00 5C 00  48 00 78 00 44 00 65 00   i.c.e.\.H.x.D.e.
00AAABC0   66 00 44 00 72 00 69 00  76 00 65 00 72 00 00 00   f.D.r.i.v.e.r...
00AAABD0   5C 00 44 00 6F 00 73 00  44 00 65 00 76 00 69 00   \.D.o.s.D.e.v.i.
00AAABE0   63 00 65 00 73 00 5C 00  48 00 78 00 44 00 65 00   c.e.s.\.H.x.D.e.
00AAABF0   66 00 44 00 72 00 69 00  76 00 65 00 72 00 00 00   f.D.r.i.v.e.r...
00AAAC00   55 8B EC 83 EC 10 56 57  8B 3D 04 08 01 00 8D 45   U‹ìƒì.VW‹=....• E
```

The pages appear to be related to printing divps and ghostscript printing. The divps homepage may be found at http://www.radicaleye.com/dvips.html. The Ghostscript homepage may be found at http://www.ghostscript.com/. LaTex is a typesetting package that is popular in many academic computing environments. http://www.latex-project.org/. These pages are likely to be an artifact of Ghostscript/dvips/LaTex printing.

The timeline includes a number of entries with *.pdf* extensions that appear to relate to Goatboy's research:

Mon May 30 2005 13:47:42 98629 ..c -/-rwxrwxrwx 0 0 92646153

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Semaphores Using Stochastic Configurations.pdf (_EMAPH~1.PDF)

(deleted)
Mon May 30 2005 13:47:56 98629 m.. -/-rwxrwxrwx 0 0 92646153

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Semaphores Using Stochastic Configurations.pdf (_EMAPH~1.PDF)

(deleted)
Mon May 30 2005 13:48:50 87984 ..c -/-rwxrwxrwx 0 0 92646158

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Intuitive Unification of Fiber-Optic Cables.pdf (_NTUIT~1.PDF)

(deleted)
Mon May 30 2005 13:49:04 87984 m.. -/-rwxrwxrwx 0 0 92646158

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Intuitive Unification of Fiber-Optic Cables.pdf (_NTUIT~1.PDF)

(deleted)
Mon May 30 2005 13:49:38 58374 ..c -/-rwxrwxrwx 0 0 92646161

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/P2P Model Checking.pdf (_2PMOD~1.PDF) (deleted)
Mon May 30 2005 13:49:50 58374 m.. -/-rwxrwxrwx 0 0 92646161

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/P2P Model Checking.pdf (_2PMOD~1.PDF) (deleted)

[...]

Sun Jun 05 2005 01:00:00
58374 .a. -/-rwxrwxrwx 0 0 92646161

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/P2P Model Checking.pdf (_2PMOD~1.PDF) (deleted)
58374 .a. -/-rwxrwxrwx 0 0 92646161

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/P2P Model Checking.pdf (_2PMOD~1.PDF) (deleted)
58374 .a. -/-rwxrwxrwx 0 0 92646161

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/P2P Model Checking.pdf (_2PMOD~1.PDF) (deleted)
98629 .a. -/-rwxrwxrwx 0 0 92646153

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Semaphores Using Stochastic Configurations.pdf (_EMAPH~1.PDF)

(deleted)
87984 .a. -/-rwxrwxrwx 0 0 92646158

/DOCUME~1/ADMINI~1/MYDOCU~1/NEWRES~1/DONOTD~1/Intuitive Unification of Fiber-Optic Cables.pdf (_NTUIT~1.PDF)

(deleted)

All of the entries are marked "(deleted)" in the timeline. These timeline entries might be an artifact of printing Goatboy's documents. To prove or disprove this hypothesis we would need to set up a test environment with Ghostscript/dvips/LaTex print software installed. But this cannot be accomplished within the timeframe of this challenge.

Assuming that Goatboy's documents were printed, the next question is by whom? Some of the timeline entries dated back to May 30, 2005, apparently before the present intrusion. The second memory "image" also contains pages that are similar to the excerpt from page 0x00AAA000 quoted above:

```
02A28190   31 20 34 30 36 20 35 38  37 20 35 35 37 20 37 36   1 406 587 557 76
02A281A0   37 20 33 35 34 20 35 35  37 20 34 36 36 20 35 32   7 354 557 466 52
02A281B0   36 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   6 354 354 354 35
02A281C0   34 0A 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4.354 354 354 35
02A281D0   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A281E0   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A281F0   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28200   34 0A 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4.354 354 354 35
02A28210   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28220   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28230   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28240   34 0A 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4.354 354 354 35
02A28250   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28260   34 20 33 35 34 20 33 35  34 20 33 35 34 20 33 35   4 354 354 354 35
02A28270   34 20 33 35 34 20 33 35  34 20 36 31 37 20 35 38   4 354 354 617 58
```

```
02A28280   37 0A 35 38 37 5D 0A 3E  3E 0A 65 6E 64 6F 62 6A   7.587].>>.endobj
02A28290   0A 32 20 30 20 6F 62 6A  0A 3C 3C 2F 50 72 6F 64   .2 0 obj.<</Prod
02A282A0   75 63 65 72 28 47 4E 55  20 47 68 6F 73 74 73 63   ucer(GNU Ghostsc
02A282B0   72 69 70 74 20 37 2E 30  37 29 0A 2F 43 72 65 61   ript 7.07)./Crea
02A282C0   74 6F 72 28 64 76 69 70  73 5C 28 6B 5C 29 20 35   tor(dvips\(k\) 5
02A282D0   2E 39 32 62 20 43 6F 70  79 72 69 67 68 74 20 32   .92b Copyright 2
02A282E0   30 30 32 20 52 61 64 69  63 61 6C 20 45 79 65 20   002 Radical Eye
02A282F0   53 6F 66 74 77 61 72 65  29 0A 2F 54 69 74 6C 65   Software)./Title
02A28300   28 73 63 69 6D 61 6B 65  6C 61 74 65 78 2E 38 35   (scimakelatex.85
02A28310   32 34 36 2E 47 6F 61 74  62 6F 79 2E 64 76 69 29   246.Goatboy.dvi)
02A28320   3E 3E 65 6E 64 6F 62 6A  0A 78 72 65 66 0A 30 20   >>endobj.xref.0
02A28330   37 34 0A 30 30 30 30 30  30 30 30 30 30 20 36 35   74.0000000000 65
02A28340   35 33 35 20 66 20 0A 30  30 30 30 30 33 34 36 33   535 f .000003463
02A28350   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
02A28360   38 36 32 37 33 20 30 30  30 30 30 20 6E 20 0A 30   86273 00000 n .0
02A28370   30 30 30 30 33 34 35 35  31 20 30 30 30 30 30 20   000034551 00000
02A28380   6E 20 0A 30 30 30 30 30  33 34 36 38 36 20 30 30   n .0000034686 00
02A28390   30 30 30 20 6E 20 0A 30  30 30 30 30 33 33 38 31   000 n .000003381
02A283A0   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
02A283B0   30 30 30 31 35 20 30 30  30 30 30 20 6E 20 0A 30   00015 00000 n .0
02A283C0   30 30 30 30 30 35 31 30  35 20 30 30 30 30 30 20   000005105 00000
02A283D0   6E 20 0A 30 30 30 30 30  34 30 30 35 31 20 30 30   n .0000040051 00
02A283E0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 39 37 37   000 n .000003977
02A283F0   37 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   7 00000 n .00000
02A28400   38 33 34 34 36 20 30 30  30 30 30 20 6E 20 0A 30   83446 00000 n .0
02A28410   30 30 30 30 33 38 37 32  35 20 30 30 30 30 30 20   000038725 00000
02A28420   6E 20 0A 30 30 30 30 30  33 38 35 30 32 20 30 30   n .0000038502 00
02A28430   30 30 30 20 6E 20 0A 30  30 30 30 30 38 33 31 30   000 n .000008310
02A28440   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
02A28450   33 35 34 34 39 20 30 30  30 30 30 20 6E 20 0A 30   35449 00000 n .0
02A28460   30 30 30 30 33 35 31 36  32 20 30 30 30 30 30 20   000035162 00000
02A28470   6E 20 0A 30 30 30 30 30  38 32 31 37 39 20 30 30   n .0000082179 00
02A28480   30 30 30 20 6E 20 0A 30  30 30 30 30 34 38 37 34   000 n .000004874
02A28490   30 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   0 00000 n .00000
02A284A0   34 38 32 33 33 20 30 30  30 30 30 20 6E 20 0A 30   48233 00000 n .0
02A284B0   30 30 30 30 38 31 33 37  36 20 30 30 30 30 30 20   000081376 00000
02A284C0   6E 20 0A 30 30 30 30 30  33 34 37 34 31 20 30 30   n .0000034741 00
02A284D0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 37 37   000 n .000003477
02A284E0   31 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   1 00000 n .00000
02A284F0   33 33 39 37 35 20 30 30  30 30 30 20 6E 20 0A 30   33975 00000 n .0
02A28500   30 30 30 30 30 35 31 32  35 20 30 30 30 30 30 20   000005125 00000
02A28510   6E 20 0A 30 30 30 30 30  31 30 36 30 38 20 30 30   n .0000010608 00
02A28520   30 30 30 20 6E 20 0A 30  30 30 30 30 38 33 30 34   000 n .000008304
02A28530   36 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   6 00000 n .00000
02A28540   38 32 39 37 31 20 30 30  30 30 30 20 6E 20 0A 30   82971 00000 n .0
02A28550   30 30 30 30 34 34 32 38  34 20 30 30 30 30 30 20   000044284 00000
02A28560   6E 20 0A 30 30 30 30 30  34 33 39 34 33 20 30 30   n .0000043943 00
02A28570   30 30 30 20 6E 20 0A 30  30 30 30 30 38 30 35 37   000 n .000008057
02A28580   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
02A28590   34 33 34 33 34 20 30 30  30 30 30 20 6E 20 0A 30   43434 00000 n .0
02A285A0   30 30 30 30 34 33 32 32  33 20 30 30 30 30 30 20   000043223 00000
02A285B0   6E 20 0A 30 30 30 30 30  38 30 34 33 39 20 30 30   n .0000080439 00
02A285C0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 38 33   000 n .000003483
02A285D0   36 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   6 00000 n .00000
02A285E0   33 34 31 31 39 20 30 30  30 30 30 20 6E 20 0A 30   34119 00000 n .0
02A285F0   30 30 30 30 31 30 36 32  39 20 30 30 30 30 30 20   000010629 00000
02A28600   6E 20 0A 30 30 30 30 30  32 32 30 37 39 20 30 30   n .0000022079 00
02A28610   30 30 30 20 6E 20 0A 30  30 30 30 30 38 30 33 37   000 n .000008037
02A28620   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
02A28630   37 39 35 31 31 20 30 30  30 30 30 20 6E 20 0A 30   79511 00000 n .0
02A28640   30 30 30 30 36 34 38 31  30 20 30 30 30 30 30 20   000064810 00000
02A28650   6E 20 0A 30 30 30 30 30  36 34 35 32 30 20 30 30   n .0000064520 00
02A28660   30 30 30 20 6E 20 0A 30  30 30 30 30 37 39 35 38   000 n .000007958
02A28670   34 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   4 00000 n .00000
02A28680   36 32 39 34 39 20 30 30  30 30 30 20 6E 20 0A 30   62949 00000 n .0
02A28690   30 30 30 30 36 32 37 31  38 20 30 30 30 30 30 20   000062718 00000
02A286A0   6E 20 0A 30 30 30 30 30  37 39 32 38 30 20 30 30   n .0000079280 00
02A286B0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 34 39 31   000 n .000003491
02A286C0   32 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   2 00000 n .00000
02A286D0   33 34 32 36 33 20 30 30  30 30 30 20 6E 20 0A 30   34263 00000 n .0
02A286E0   30 30 30 30 32 32 31 30  31 20 30 30 30 30 30 20   000022101 00000
```

```
02A286F0   6E 20 0A 30 30 30 30 30  33 32 38 37 38 20 30 30   n .0000032878 00
02A28700   30 30 30 20 6E 20 0A 30  30 30 30 30 35 36 38 31   000 n .000005681
02A28710   38 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   8 00000 n .00000
02A28720   35 36 34 30 30 20 30 30  30 30 30 20 6E 20 0A 30   56400 00000 n .0
02A28730   30 30 30 30 38 35 34 37  35 20 30 30 30 30 30 20   000085475 00000
02A28740   6E 20 0A 30 30 30 30 30  37 34 33 36 32 20 30 30   n .0000074362 00
02A28750   30 30 30 20 6E 20 0A 30  30 30 30 30 37 34 30 34   000 n .000007404
02A28760   39 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   9 00000 n .00000
02A28770   38 35 30 32 36 20 30 30  30 30 30 20 6E 20 0A 30   85026 00000 n .0
02A28780   30 30 30 30 36 38 31 36  37 20 30 30 30 30 30 20   000068167 00000
02A28790   6E 20 0A 30 30 30 30 30  36 37 38 32 37 20 30 30   n .0000067827 00
02A287A0   30 30 30 20 6E 20 0A 30  30 30 30 30 38 34 32 33   000 n .000008423
02A287B0   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
02A287C0   33 34 39 38 38 20 30 30  30 30 30 20 6E 20 0A 30   34988 00000 n .0
02A287D0   30 30 30 30 33 34 34 30  37 20 30 30 30 30 30 20   000034407 00000
02A287E0   6E 20 0A 30 30 30 30 30  33 32 39 30 30 20 30 30   n .0000032900 00
02A287F0   30 30 30 20 6E 20 0A 30  30 30 30 30 33 33 37 39   000 n .000003379
02A28800   35 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   5 00000 n .00000
02A28810   33 35 30 39 37 20 30 30  30 30 30 20 6E 20 0A 30   35097 00000 n .0
02A28820   30 30 30 30 33 38 34 38  31 20 30 30 30 30 30 20   000038481 00000
02A28830   6E 20 0A 30 30 30 30 30  33 39 37 35 37 20 30 30   n .0000039757 00
02A28840   30 30 30 20 6E 20 0A 30  30 30 30 30 34 33 32 30   000 n .000004320
02A28850   32 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   2 00000 n .00000
02A28860   34 33 39 32 33 20 30 30  30 30 30 20 6E 20 0A 30   43923 00000 n .0
02A28870   30 30 30 30 34 38 32 31  32 20 30 30 30 30 30 20   000048212 00000
02A28880   6E 20 0A 30 30 30 30 30  35 36 33 37 39 20 30 30   n .0000056379 00
02A28890   30 30 30 20 6E 20 0A 30  30 30 30 30 36 32 36 39   000 n .000006269
02A288A0   37 20 30 30 30 30 30 20  6E 20 0A 30 30 30 30 30   7 00000 n .00000
02A288B0   36 34 34 39 39 20 30 30  30 30 30 20 6E 20 0A 30   64499 00000 n .0
02A288C0   30 30 30 30 36 37 38 30  36 20 30 30 30 30 30 20   000067806 00000
02A288D0   6E 20 0A 30 30 30 30 30  37 34 30 32 38 20 30 30   n .0000074028 00
02A288E0   30 30 30 20 6E 20 0A 30  30 30 30 30 37 39 32 35   000 n .000007925
02A288F0   39 20 30 30 30 30 30 20  6E 20 0A 74 72 61 69 6C   9 00000 n .trail
02A28900   65 72 0A 3C 3C 20 2F 53  69 7A 65 20 37 34 20 2F   er.<< /Size 74 /
02A28910   52 6F 6F 74 20 31 20 30  20 52 20 2F 49 6E 66 6F   Root 1 0 R /Info
02A28920   20 32 20 30 20 52 0A 3E  3E 0A 73 74 61 72 74 78    2 0 R.>>.startx
02A28930   72 65 66 0A 38 36 34 32  35 0A 25 25 45 4F 46 0A   ref.86425.%%EOF.
```

So perhaps there are print spool documents lying around on Goatboy's hard drive that were read into memory. An amazing amount of information is read into memory by anti-virus, defragmentation and other software. Or perhaps the portion quoted above from the second memory dump is a header that is contained within some executable code to which the actual document or other information will be appended.

The relevant pages in the second memory dump do not contain any reference *\DosDevices\HxDefDriver* or *\Device\HxDefDriver*. These device names are most probably the destination of the document. Presumably Professor Goatboy would not knowingly print his research to the attacker's rootkit; though he might unwittingly do so if there is a trojaned print driver on his computer.

An entry for "\Device\HxDefDriver" may be found in the object directory of both memory "images:"

```
\Device\HxDefDriver
OBJECT: 0xFF1FC810(d0b810)  Type: 23 Device
SecurityDescriptor: (null)

Driver: 0xFF25D890
```

SecurityDescriptor: 0xE12AAC98(18cbc98)
Revision: 1
Sbz1: 0
Control: DaclPresent SelfRelative
O: S-1-5-32-544
G: S-1-5-18
D:(A;;FA;;;SY)(A;;0x1200a9;;;BA)
Section: 0xFF178B08 \??\c:\winnt\system32\dfrwsdrv.sys

(First memory dump.)

\Device\HxDefDriver
OBJECT: 0xFF25C330(1982330) Type: 23 Device
SecurityDescriptor: (null)

Driver: 0xFF25C490
SecurityDescriptor: 0xE12AEC98(18cfc98)
Revision: 1
Sbz1: 0
Control: DaclPresent SelfRelative
O: S-1-5-32-544
G: S-1-5-18
D:(A;;FA;;;SY)(A;;0x1200a9;;;BA)
Section: 0xFF25C7E8 \??\c:\winnt\system32\dfrwsdrv.sys

(Second memory dump.)

The attacker (or Goatboy unwittingly) apparently printed or faxed something from Goatboy's computer. Since the attacker was looking for Goatboy's research it is reasonable to infer that he got it.

6. What computer was the intrusion launched from?

A number of memory pages in both images reference a TCPIP host with an IP address of 92.168.000.005. The following pages in particular references this host in connection with a file emit statement.

```
065070B0   00 00 00 00 46 69 6C 65  20 65 6D 69 74 20 73 74   ....File emit st
065070C0   61 72 74 65 64 20 66 72  6F 6D 3A 20 31 39 32 2E   arted from: 192.
065070D0   31 36 38 2E 30 2E 32 3A  31 30 36 39 2C 53 54 43   168.0.2:1069,STC
065070E0   50 49 4F 2C 4E 55 4C 4C  2C 4E 55 4C 4C 41 55 54   PIO,NULL,NULLAUT
065070F0   48 0A 00 00 00 00 00 00  13 00 12 00 00 01 0E 00   H...............
06507100   28 CC 14 00 65 00 67 00  69 00 73 00 74 00 72 00   (Ì..e.g.i.s.t.r.
06507110   79 00 5C 00 4D 00 61 00  63 00 68 00 69 00 6E 00   y.\.M.a.c.h.i.n.
06507120   65 00 5C 00 53 00 79 00  73 00 74 00 65 00 6D 00   e.\.S.y.s.t.e.m.
06507130   5C 00 43 00 75 00 72 00  72 00 65 00 6E 00 74 00   \.C.u.r.r.e.n.t.
06507140   43 00 6F 00 6E 00 74 00  72 00 6F 00 6C 00 53 00   C.o.n.t.r.o.l.S.
06507150   65 00 74 00 5C 00 53 00  65 00 72 00 76 00 69 00   e.t.\.S.e.r.v.i.
06507160   63 00 65 00 73 00 5C 00  54 00 63 00 70 00 69 00   c.e.s.\.T.c.p.i.
06507170   70 00 5C 00 50 00 61 00  72 00 61 00 6D 00 65 00   p.\.P.a.r.a.m.e.
06507180   74 00 65 00 72 00 73 00  00 00 0A 00 00 00 00 00   t.e.r.s.........
06507190   23 00 13 00 00 00 0C 00  90 02 13 00 90 02 13 00   #.......• ...• ...
065071A0   00 00 00 00 00 39 32 2E  31 36 38 2E 30 30 30 2E   .....92.168.000.
065071B0   30 30 35 00 00 00 00 00  00 00 00 00 00 00 00 00   005.............
```

The TWTCB table in the second "image" contained 4 entries all to the network interface with IP address 192.168.0.5:

TWTCB: 0xFF1A2CC8 (364ecc8)
Connection: 0x200a8c0:604-->0x500a8c0:8504 192.168.0.2:1030-->192.168.0.5:1157
SomeSequenceNumber1: 0x718b796b
SomeSequenceNumber2: 0x718b796b

TWTCB: 0xFF192B28 (3992b28)
Connection: 0x200a8c0:9cad-->0x500a8c0:8104 192.168.0.2:44444-->192.168.0.5:1153
SomeSequenceNumber1: 0x70b75eaf
SomeSequenceNumber2: 0x70b75eaf

TWTCB: 0xFF1A36E8 (362e6e8)
Connection: 0x200a8c0:404-->0x500a8c0:8304 192.168.0.2:1028-->192.168.0.5:1155
SomeSequenceNumber1: 0x71756a79
SomeSequenceNumber2: 0x71756a79

TWTCB: 0xFF2007E8 (4dd87e8)
Connection: 0x200a8c0:504-->0x500a8c0:8404 192.168.0.2:1029-->192.168.0.5:1156
SomeSequenceNumber1: 0x71814e57
SomeSequenceNumber2: 0x71814e57

The connections are to a host with an IP address of 192.168.0.5, not 92.168.0.5. Nevertheless, the quoted passage above from the first memory dump contains another string (to a registry key) where the first character obviously is missing. An attacker clearly was communicating with 192.168.0.5 both before and after the computer rebooted. See, 2(F), above. Perhaps this represents a bug in this particular release of B02K.

On the other hand, this interpretation does not explain the entries in the arp cache of the first memory dump.

The laptop has two network interfaces, one of which is probably a Conexant modem (from first memory dump):

```
00A14E50   00 43 6F 6E 65 78 61 6E  74 2D 41 6D 62 69 74 20   .Conexant-Ambit
00A14E60   53 6F 66 74 4B 35 36 20  44 61 74 61 2C 46 61 78   SoftK56 Data,Fax
00A14E70   20 49 43 48 20 4D 6F 64  65 6D 00 00 00 00 00 00    ICH Modem......
```

The arp cache similarly has two dynamic entries, one for each interface:

The first is bound to local interface 08-00-46-02-22-f0 and the following remote interface:

ArpCacheEntry: 0xFCCA5828 (12c2828)
CreateTime: 0x4
InetAddress: 92.0.94.0

PhysicalAddress: 00-00-00-00-00-00
CacheLife: 0x201800e
Type: dynamic

The second arp cache entry is bound to local interface 08-00-46-18-65-ad and the following remote interface:

ArpCacheEntry: 0xFCCA62D0 (12c32d0)
CreateTime: 0xfcc9ae30
InetAddress: 18.0.0.0
PhysicalAddress: 20-6e-58-f0-00-00
CacheLife: 0xfcca6378
Type: dynamic

The IP addresses are odd in that they are network rather than host addresses and the MAC-address in the first entry is empty. Our first inclination would be to consider this a bug in *kntlist*. However, the arp cache entry from the second memory dump is consistent with our expectations.

ArpCacheEntry: 0xFCA37968 (1054968)
CreateTime: 0xcc0cf
InetAddress: 192.168.0.5
PhysicalAddress: 00-00-e2-8a-c4-6b
CacheLife: 0x34
Type: dynamic

The fact that the same IP addresses were found in both memory "images" does not prove that the referenced hosts were the same. The same IP address may be mapped successively to two different computers by flushing the arp cache. This in fact would have occurred when Goatboy's computer was allowed to reboot.

The fact that Goatboy's arp cache in the first memory "image" does not reference a host with an IP address of 192.168.0.5 may be explained by the fact that suspicious network logs reference traffic that occurred the night before. Dynamic arp entries are labile.

The fact that Goatboy's TCB table was empty in both memory dumps does not mean that the attacker was not actively communicating with the victim computer while Daniels was on the scene. Transmission control blocks are set up and torn down very quickly. Absence of active TCB's in the first memory dump does suggest that the attacker was not engaging in an extended network conversation, such as a file transfer, during the first memory "image's" acquisition.

This version of Microsoft Windows does not use a TCB pool to recycle TCB blocks after they are no longer in use.

The competing hypotheses are not mutually exclusive. It is entirely possible, indeed probable, that a single attacker would communicate with a victim computer via multiple intermediate hosts. It is also possible for multiple intruders to attack the same host, particularly where the host is as vulnerable as a default Windows 2000 installation. There are possible signs of a more sophisticated attacker operating on this computer, as has previously been noted. It is impossible to resolve these competing hypotheses without examining the computers referenced by the arp caches and IP addresses.

7. Is there any indication of who the intruder might be?

The *Hacker Defender* configuration information mentioned under 1., above, includes reference to a hidden file, directory or process named "eoghan:"

```
05549B90   F8 DE 14 00 00 18 25 D2  5B 48 3C 3C 3C 69 64 64   øÞ....%Ò[H<<<idd
05549BA0   65 6E 20 54 3E 3E 61 2F  22 62 6C 65 5D 0D 0A 3E   en T>>a/"ble]..>
05549BB0   64 22 66 72 77 73 22 2A  0D 0A 72 7C 63 3C 6D 64   d"frws"*..r|c<md
05549BC0   5C 2E 65 78 3C 65 3A 3A  0D 0A 65 3C 6F 67 7C 68   \.ex<e::..e<og|h
05549BD0   61 6E 0D 0A 75 6D 5C 67  72 7C 33 32 2E 65 3C 78   an..um\gr|32.e<x
```

It is tempting to blame the intrusion on someone named “Eoghan.” Perhaps the attacker was testing the rootkit on his own system and simply forgot to remove the name before deploying it to Goatboy's computer. One interpretation might be that someone wants us to think that it is “Eoghan.” However, the second memory "image" also contains what appears to be *Hacker Defender* configuration information in the page that begins at offset 0x2d9000. Reference to "eoghan" is omitted from this second version of the configuration information. If the attacker wanted us to suspect “Eoghan” why did he delete reference to “eoghan” by the time the second memory "image" was taken?

Pages in the second memory "image" relating to B02K contain several "delete" statements suggesting that an attacker was busy destroying evidence of the intrusion while Daniels was collecting the second memory "image:"

```
0004E790   00 00 3F 00 00 00 00 00  00 00 46 69 6C 65 20 65   ..?.......File e
0004E7A0   6D 69 74 20 73 74 61 72  74 65 64 20 66 72 6F 6D   mit started from
0004E7B0   3A 20 31 39 32 2E 31 36  38 2E 30 2E 32 3A 31 30   : 192.168.0.2:10
0004E7C0   32 38 2C 53 54 43 50 49  4F 2C 4E 55 4C 4C 2C 4E   28,STCPIO,NULL,N
0004E7D0   55 4C 4C 41 55 54 48 0A  00 00 00 00 00 20 6F 72   ULLAUTH...... or
0004E7E0   20 6E 6F 29 0A 00 00 00  00 00 5C 42 52 4F 57 53    no)......\BROWS
0004E7F0   45 00 02 00 56 41 49 4F  00 00 00 00 00 00 00 00   E...VAIO........
0004E800   00 00 04 00 00 E9 04 00  FF FF FF FF 8D 00 0C 00   .....é..ÿÿÿÿ• ...
0004E810   2A 9E 39 01 36 00 00 00  54 71 A9 02 B4 85 00 00   *ž9.6...Tq©.´….. 
0004E820   00 00 E2 8A C4 6B 08 00  46 18 65 AD 08 00 45 00   ..âŠÄk..F.e-..E.
0004E830   00 7F 01 DF 40 00 80 06  77 42 C0 A8 00 02 C0 A8   .•.ß@.€.wBÀ¨..À¨
0004E840   00 05 AD 9C 04 82 70 EA  66 88 82 36 17 B5 50 18   ..-œ.,pêfˆ,6.µP.
0004E850   43 99 4B BD 00 00 63 36  00 00 41 0D 00 00 02 71   C™K½..c6..A....q
0004E860   00 00 E3 4A 00 00 2C 44  7C 50 22 57 57 5F 7A 1C   ..ãJ..,D|P"WW_z.
0004E870   D1 35 BC 5F 0E 6C CD C3  13 37 00 0E 30 3E 2F 00   Ñ5¼_.lÍÃ.7..0>/.
0004E880   00 00 02 00 00 00 FF FF  FF FF F4 17 42 00 00 00   ......ÿÿÿÿô.B...
```

```
0004E890   00 00 0F 00 00 00 00 00  00 00 46 69 6C 65 20 64   ..........File d
0004E8A0   65 6C 65 74 65 64 2E 0A  00 00 00 00 00 20 20 30   eleted.......  0
0004E8B0   20 44 2D 48 2D 52 2D 2D  20 30 32 2D 32 30 2D 32    D-H-R-- 02-20-2
0004E8C0   30 30 31 20 31 38 3A 32  33 20 52 65 63 65 6E 74   001 18:23 Recent
0004E8D0   0A 00 00 00 00 00 6E 64  20 61 72 67 75 6D 65 6E   ......nd argumen
0004E8E0   74 73 7C 0A 00 00 00 00  00 54 5C 42 52 4F 57 53   ts|......T\BROWS
0004E8F0   45 00 02 00 56 41 49 4F  00 00 00 00 00 00 00 00   E...VAIO........
0004E900   00 00 04 00 00 EA 04 00  FF FF FF FF 8D 00 0C 00   .....ê..ÿÿÿÿ• ...
0004E910   1A 90 39 01 36 00 00 00  08 77 A9 02 B4 85 00 00   .• 9.6....w©.´….. 
0004E920   00 00 E2 8A C4 6B 08 00  46 18 65 AD 08 00 45 00   ..âŠÄk..F.e-..E.
0004E930   00 7F 01 E0 40 00 80 06  77 41 C0 A8 00 02 C0 A8   .•.à@.€.wAÀ¨..À¨
0004E940   00 05 AD 9C 04 82 70 EA  66 DF 82 36 18 73 50 18   ..-œ.,pêfß‚6.sP.
0004E950   42 DB 9F EF 00 00 EB 37  00 00 92 3B 00 00 D6 26   BÛŸï..ë7..’;..Ö&
0004E960   00 00 91 5A 00 00 6B 9A  65 91 39 B5 71 08 BE D4   ..‘Z..kše‘9µq.¾Ô
0004E970   00 7B FF 4E 7C 60 CD C3  13 37 00 0E 30 3F 2F 00   .{ÿN|`ÍÃ.7..0?/.
0004E980   00 00 02 00 00 00 FF FF  FF FF C6 18 42 00 00 00   ......ÿÿÿÿÆ.B...
0004E990   00 00 0F 00 00 00 00 00  00 00 46 69 6C 65 20 64   ..........File d
0004E9A0   65 6C 65 74 65 64 2E 0A  00 00 00 00 00 00 00 00   eleted..........
0004E9B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
```

If you are an elite hacker with the perfect "invisible" rootkit, why do you need to delete anything?

Certainly “Eoghan” must be considered a "person of interest." However it is too early to consider him a suspect, at least not until we have examined the other computers reference by the IP addresses and arp cache entries mention above. At some point we may want to seek “Eoghan's” ISP records. However, that is for another day.

Network logs may be very helpful in this case. In reviewing the logs we will want to look very carefully at whoever connected to the two ports that were hidden by the Hacker Defender rootkit (TCP 1313 and 3000), since that is likely to be our culprit.

References

Burdach, Mariusz. *An Introduction to Windows Memory Forensics.* Available from http://forensic.seccure.net/pdf/introduction_to_windows_memory_forensic.pdf.

Butler, James. "*VICE - Catch the hookers!*" Black Hat, Las Vegas, July, 2004. Available from http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-butler/bh-us-04-butler.pdf.

Butler, Jamie and Sparks, Sherrie. “*Shadow Walker*.” Phrack. Volume 0x0b, Issue 0x3d, Phile #0x08 of 0x14. Available from http://www.phrack.org/show.php?p=63&a=8.

Russinovich, Mark E. and Solomon, David A. *Microsoft Windows Internals*. 4th edition. Redmond: Microsoft Press, 2005.

Rutkowska, Joanna. *Rootkits Detection on Windows Systems*. Available from http://invisiblethings.org/papers/ITUnderground2004_Win_rtks_detection.ppt.