Rootkit Class Report

I examined C:\Windows\System32 and found some files that were very out of place. The following files were suspect because their modify date was way to early:

- He4HookInv.sys – 11/8/2002
- Ctl.exe – 11/10/2002
- Instdriver.exe – 02/12/2003

I then used mdd.exe to take a memory dump. After that I started playing around with Volatility 1.3 to examine the memory dump. I did a pslist and found some processes that were out of place. From there, I explored the capability of Volatility to dump portions of ram and ran strings on those portions of RAM. I then ran SysInternals Autorun on the running system to look for entries that were out of place. SysInternals Process Explorer did not show anything out of the ordinary.

He4Hook

He4HookInv.sys is a sign of the He4Hook tool that allows files to be hidden. This is good to know in an investigation. The live file system cannot be trusted. I think He4Hook might be started by services.exe. I used volatility to dump the memory for services.exe (PID 764) I found the following:

```
00220d0: 4800 6500 3400 4800 6f00 6f00 6b00 4900  H.e.4.H.o.o.k.I.
00220e0: 6e00 7600 2e00 7300 7900 7300 0000 3000  n.v...s.y.s...0.
```

Vanquish

C:\vanquish-0.2.1\ directory was found on the computer. I have not yet verified that it is running. The log file in C:\vanquish.txt has 2 failed attempts to inject svchost.exe and one, that looks successful, by the log, for winlogon.exe. Although, when examining with Volatility I see no traces of vanquish.dll in winlogon. I did find a reference to vanquish.exe when reviewing strings of the memory dump for services.exe:

```
***Application: C:\WINDOWS\vanquish.exe
```

I looked at the system with Autoruns, the SysInternals tool. In there, I found an entry for C:\windows\vanquish.exe under HKLM\System\CurrentControlSet\Services\. The start type of vanquish.exe is 2, so it starts automatically.

HackerDefender

Hxdef100.exe was running on the system, as evidenced by it showing up in the Volatility pslist. This piece of malware is running on the computer. The service was running from the executable: C:\hxdef100r\hxdef100.exe. This directory was hidden to the system. I could not see it in Windows Explorer. The service was

loaded on March 14 at 01:31AM. The PID is 336 and the PPID is 764. PID 764 is services.exe. Services.exe has a PPID of 720. PID 720 is winlogon.exe. Services.exe being launched by winlogon.exe was consistent with a known good system. However, PID 336 is the PPID for taskmgr.exe. This info was found with volatility using the psscan option.
PID 336 is accessing the following files:

- `File \WINDOWS\system32`
- `File \net\NtControlPipe13`
- `File \hxdef-rk100s6825727F`
- `File \hxdef-rk100s6825727F`
- `File \WINDOWS\WinSxS\x86_Microsoft.VC80.CRT_1fc8b3b9a1e18e3b_8.0.50727.3053_x-ww_b80fa8ca`

I did a process memory dump on PID 336. Hxdefdrv.sys is the driver for Hacker Defender as evidenced by:

```
0002cf0: 822d 4000 1b44 7269 7665 7246 696c 654e  .-@..DriverFileN
0002d00: 616d 653d 6878 6465 6664 7276 2e73 7973  ame=hxdefdrv.sys
```

The registry key HKLM\System\CurrentControlSet\Services\Hackerdefender100 was created on 03/07/11. It also has a service type of 2, which means it starts automatically. It points to C:\hxdef100r\hxdef100.exe.

FU.exe

Upon offline examination of the file system and prefetch files, the following files appeared on the system on 03/07/11 at 02:07 UTC:

- system32\drivers\fu.exe
- system32\drivers\msdirectx.sys
- system32\drivers\mmpc.sys
- system32\InstDriver.exe

I took all these files and put them in a WinXP VM. I used RegShot to take a before image of the system. I ran fu.exe from the command line with –ph and the PID of services.exe:

- `Fu.exe –ph 676`

Upon running Regshot for a second time, I saw that a new service, msdirectx.exe was created. It had a start type 3. Start type 3 is manual start type. So, this service was not started automatically on boot. RegShot did not find any new directories created on the machine. I looked at the registry keys associated with fu.exe on the original rootkit VM and they were created on 03/13/11.
I ran fu.exe a few more times after reverting my test VM. This time I monitored with SysInternals tools like Process Explorer and Process Monitor. When I run the same command with fu.exe, services.exe cannot be seen in Process Explorer. The Parent PID for svchost.exe still shows services.exe (PID 676) when double clicking on svchost.exe. However, in Process Monitor, the child processes for services.exe are sort of orphaned.

The registry key for msdirectx service on the exploited machine had a start type of 4, which means disabled. This differs from the start type of 3 that I saw when executing on my clean system.

MRU-Blaster

MRU-Blaster was running on the system. There were many process entries in the pslist output for mrublaster.exe. MRU-Blaster removes the most recently used files and programs. All instances of mrublaster.exe have a PPID of 448, which is scheduler.exe. MRU-Blaster entries are in the startup folder. I don't think it is a rootkit but it certainly is cleaning up tracks for something. MRU-Blaster has a scheduled job and it is running constantly. It gets in the way of my monitoring with Process Monitor.

Trusteer Rapport

RapportMgmtServ.exe and RapportService.exe were running on the system. Trusteer Rapport appears to be a legitimate piece of software installed on the machine on 03/07/11, based on dates files were written to the file system. Trusteer Rapport is a piece of security software that uses rootkit techniques to "protect online banking." However, the services are viewable in task manager on the live running machine. I did find the following string in the RAM dump of services.exe:

- `//updates.trusteer.com/rapport/update?o=ebay&r=34598&c=3.5.1007.36-standard-release&d=2&m=FF75D1D00A0CEA5F4F1E71507D5F390D&t=2f7b7bdd&ms=00000000&a=4CDCDE98ACC5AEEEE62A8618DCD5C53FFF75D1D00A0CEA5F4F1E71507D5F390D&as=00000000&cu=1&ext_RapportCerberus=23645&dext_RapportCerberus=23645`

This is probably the URL for updating the rules.
When looking at SysInternals Autorun, I see this service is set to start in HKLM\System\CurrentControlSet\Services\.

Hacktool.Rootkit

When examining Autoruns, I found an entry pointing to an entry in HKLM\System\CurrentControlSet\Services\ referencing C:\Windows\System32\drivers\passthru.sys. This was an indication of the Hacktool.Rootkit, as named by Symantec. Autoruns says the file does not exist. Upon live examination of the file system, I could not see passthru.sys and offline examination of the file system did not show the file as in that path either. Also, ThreatExpert says a service with the following name should be running: ipsechlp.exe. That service name does not show up on a pslist of the running memory dump.

Misc

I found a bunch of lines like the following when reviewing strings of services.exe
`%s [%x.%x] ERROR IS_HOOKED(hRestoreKey) == FALSE, returning STATUS_ACCESS_DENIED`
The lines differed in the function within the parenthesis. I am not sure if these are malicious but they appear out of place.
I found the following suspicious references when looking through strings in the memory space for services.exe:

- `C:\Documents and Settings\user\Desktop\20t0r147.exe`
- `C:\Documents and Settings\user\Desktop\WpdPack_4_0_2.zip`
- `C:\Documents and Settings\user\Desktop\mrublastersetup.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\030611210235\RDBValidate.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\030611210235\cpes_clean.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\030611210235\z4barSpInstall.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\GLB3C.tmp`
- `C:\Documents and Settings\user\Local Settings\Temp\GLF3B.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\SIT24336.tmp\setup.exe`
- `C:\Documents and Settings\user\Local Settings\Temp\is-UIDHH.tmp\is-P329Q.tmp`
- `C:\Documents and Settings\user\My Documents\rk\Aphex_RootKit.htm`

Suspicious entries from SysInternals Autorun tool

There were several suspect entries in HKLM\System\CurrentControlSet\Services\:

- Azdow88m – Pointing to an entry in System32\Drivers
- BreakOnThruToTheOtherSide - Pointing to an entry in System32\Drivers. The sys file does exist and is visible on the file system, or the file was deleted.
- SelfCheck – Pointing to C:\mordor\branches\POCAP\i386\stop. The file does not exist on the file system. The directory was not visible upon an offline examination of the file system. When running strings on the RAM dump, I do see evidence of the directory C:\mordor. The directory was probably deleted.