For TSV436 –

What about the system was maliciously changed?
Looks like a number of changes

- hxdef rootkit (including source/installer in hidden hxdef100r)
- Vanquish rootkit (and NOT hidden installer)
- FU Rootkit
- Zonealarm modified
- taskmanager, winlogin, svchost modified
- hidden running process 0
- restorepoint could be a malware repository

How was the change caused?
The changes were made deliberately. Not sure of all the details, though. Hope to get to this from the clases.
Would be best to know the point of entry into the system, order of changes, potential scope.

How can you remove the changes?

- stop corrupt services
- disable/remove known corrupt executables – replace with clean ones
- use tools in iterative process to clean
- Safest bet is to make an image for analysis and then wipe the system

What tools and techniques were used to garner these conclusions?
See log below. Basically, visual inspection, RootkitRevealer, gmer, Rootkit Hook Analyzer, Accessenum, RootRepeal, regedit, dbgview, SAR

Investigation Log 4/3/2011

Get VM running, turn off networking

First Look –

XP 2002 SP3, registered to ‘yo mama’, name tehroot
system restore is off

First look initially suspect items –

- Zone Alarm – would typically need to subvert, probably is
- DAEMON Tools lite – virtual device library; could hold
- Vanquish.log in c:\ – why still here? decoy?
- **vanquish rootkit** install directory
- MRU blaster in system tray – cleaning tracks?
- screen not clearing talkbar popups - display i/f could be compromised; screen/key logger?

RootkitRevealer (from CD) found –

- security policy files with embedded nulls
- secondary control set
- vanquish -0.2.1
- Hackerdefender100 (keys)
- hidden directory c:\hxdef100r\* - **hxdef** rootkit
- corruption in restore point (or a big data store)
- c:\windows\system32\drivers_cool_beans
- c:\windows\system32\drivers_fu.exe – FU rootkit can hide processes, elevate process privileges, fake out the Windows Event Viewer so that forensics is impossible, and even hide device drivers (NEW!). (Look, Mom, no hands!) It does all this by Direct Kernel Object Manipulation (TM); no hooking! This project has been evolving other time.

gmer (from CD) found rootkit activity in –

- msdirectx.sys (hidden) @F3C73000 86016B
- mmpc.sys (hidden) @F8BF2000 8192B – not a known system file (and probably not from microsoft malware protection center)
- hxdef100.exe and library (hidden)
- taskmgr.exe
- winlogon.exe
- svchost.exe
- [hidden process]
- service HackerDevender100 (hidden) – part of hxdef
- service hxdefdrv (hidden) – part of hxdef
- file hxdef100.exe 70656 bytes, .sys 3342 bytes *executable*

gmer (from CD) found services –
service HackerDefender autostart with interesting text ‘powerful NT rootkit’ – part of hxdef

gmer (from CD) found processes –

- blank process with pid 0 [825C8830]
- taskmgr.exe hacked to hide something
    - 3 hidden DLLs loaded (at 0x01AE0000, 710000 and 740000, each C000 in size)
- winlogon.exe also
    - 3 hidden DLLs loaded (at 0x01480000, 14F0000 and 1520000, each C000 in size)
- svchost also (loaded 4 times)

Rootkit Hook Analyzer found hooks in Services for 33 system calls:

- Module RapportCerberus_23645.sys - NtCreateThread, SetValueKey, DeleteFile, SetInformationFile
- RapportPG.sys – NtRenameKey, ReplaceKey, SetContextThread, QueryValueKey, RestoreKey…
- Module sptd.sys – NtQueryKey, NtOpenKey
- Module vsdatant.sys – corrupt ZoneAlarm

Accessenum found –

- Odd deny guests setting on c:\windows\system32\Macromed\flash\flash6.ocx
- Windows\WinSxS (side-by-side assemblies) – multiple DLL versions could be exploited
- c:\Windows\system32\config\systemprofile\LocalSettings\Temp\Microsoft.Net Framework 2.0-KB….. has odd Deny Guests setting

RootRepeal –

- Hidden Handle in crss.exe, services.exe, scheduler.exe
- Hidden Code in Ntfs, Mup, Ptilink, Cdrom, rdpdr, ParVdm, NetBT, azdow88mS.., WS2IFSL, Serial, Parport, AFD, msdirectx, RAW, MRxDAV, Rdbss, vmhgfs, MRxSmb, Npfs…tCtrl2cap.SYS, Msfs….., Fs_Rec, sys – – IRP_MJ_<system call>
- Trusteer\Rapport\bin\RapportPG.sys – hooked (this is a lockdown technology)

Regedit – poked around a bit

- looked at control sets (because of ControlSet002 hidden hxdef keys)

Sophos Anti-Rootkit – tried it out

- hxdef_private_version[1].png