RootKit VM Analysis for TSV 426

Tools Used:
Manual spelunking
Rootkit Revealer
Sophos Anti-Rootkit
F-Secure Blacklight
GMER
Root Repeal
Microsoft Malicious Software Removal Tool
McAfee Stinger
MalwareBytes Anti-Malware

Malware Found:
Hacker Defender
Vanquish
Possible other unnamed malware (see *discussion*)

Technique/Discussion

Manual
Wonder why debugger DebugView (SysInternals) is running
    Further research determines that debuggers are an excellent (if manual) way to detect rootkits: see `http://www.reconstructer.org/papers/Hunting rootkits with Windbg.pdf`
Found hack-bin.0.4.exe in Firefox downloads: Hacker Defender rootkit – apparently a user download it
Found Vanquish on C:\, suspected possible hacker tool for hiding files/processes: Google confirms rootkit

Winddk - Windows driver kit, possible hacking tool
Conduit - Create toolbar, possible hacking tool

Tools
Rootkit Revealer found
Hacker Defender [C:\HxDef100r, hidden]
_Cool_Beans & **FU.exe** in c:\windows\systems32\drivers\

Noticed Daemon Tools Lite running (System Tray)
Noticed MRU Blaster running (System Tray)

Sophos Anti-Rootkit found c:\windows\system\drivers\sptd.sys, possible hacker tool, total 45 items
    Could not remove much/anything

F-Secure Blacklight found 27 objects, Could not remove much/anything
zlclient.exe
hxdef100.exe
mysqld.exe (pos. legit install)
lsw service ... ?
ForceField.exe ...?
RapportService.exe ...?

GMER found numerous objects related to Hacker Defender
Trusteer Rapport now suspicious - Google search suggests it provides lightweight online security
MRU Blaster now suspicious - quick Google search suggests benign

GMER found hidden processes
    taskmgr.exe
    winlogin.exe
    svchost.exe
    procid 0 (unnamed)

GMER found ...\drivers\msdirectx.sys & mmpc.sys ... Cool_Beans & FU?

RootRepeal results similar to GMER, could not remove

Found manual removal instructions via Google:
hxdef100.ini contains password `hxdef-rulez`, admin tool can be downloaded & used to remove HxDef

Microsoft Malicious Software Removal Tool found win32\hackdef.BJ & hacty.Gen!A
    killed some processes & files, requires reboot (did not)

    GMER confirmed not all processes removed, specifically msdirectx.sys & mmpc.sys still found

Rootkit Buster seemed to install, but complained that tmcomm service was not running - could not find

McAfee Stinger found
c:\windows\system32\InstDriver.exe - Artemis!546FBC978DB6 trojan & deleted
Google search: one page said, “If you are using McAfee, Artemis is not a Trojan. It is McAfee's technology. http://www.mcafee.com/us/enterprise/products/artemis_technology/index.html” ... However, this machine doesn’t appear to be running McAfee other than Stinger

MalwareBytes Anti-Malware Quick Scan found
Vanquish & related registry key
fake system service msdirectx
PUM.Hijack.StartMenu Start_ShowHelp registry key

MalwareBytes indicates all 4 objects removed, wants restart (did not) - next scan showed Vanquish still there

VIPRE Rescue Scanner indicated it was starting a deep scan, but showed no CPU usage - assumed hung