Malwarebytes' Anti-Malware 1.36
Database version: 2056
Windows 5.1.2600 Service Pack 2

4/28/2009 4:08:56 PM
mbam-log-2009-04-28 (16-08-56).txt

Scan type: Quick Scan
Objects scanned: 111134
Time elapsed: 8 minute(s), 48 second(s)

Memory Processes Infected: 0
Memory Modules Infected: 0
Registry Keys Infected: 3
Registry Values Infected: 4
Registry Data Items Infected: 2
Folders Infected: 1
Files Infected: 4

Memory Processes Infected:
(No malicious items detected)

Memory Modules Infected:
(No malicious items detected)

Registry Keys Infected:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{1d4db7d2-6ec9-47a3-bd87-1e41684e07bb} (Adware.MyWebSearch) -> Quarantined and deleted successfully.
HKEY_CURRENT_USER\SOFTWARE\AvScan (Malware.Trace) -> Quarantined and deleted successfully.
HKEY_LOCAL_MACHINE\SOFTWARE\AGprotect (Malware.Trace) -> Quarantined and deleted successfully.

Registry Values Infected:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\lmotav (Trojan.Agent) -> Delete on reboot.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\UID (Malware.Trace) -> Quarantined and deleted successfully.
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\system tool (Trojan.FakeAlert) -> Quarantined and deleted successfully.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\reader_s (Malware.Trace) -> Quarantined and deleted successfully.

Registry Data Items Infected:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit (Trojan.FakeAlert) -> Data: c:\windows\system32\sdra64.exe -> Delete on reboot.
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit (Hijack.UserInit) -> Bad:
(C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,) Good:
(userinit.exe) -> Quarantined and deleted successfully.

Folders Infected:
C:\WINDOWS\system32\lowsec (Stolen.Data) -> Delete on reboot.

Files Infected:
C:\WINDOWS\system32\lowsec\local.ds (Stolen.Data) -> Delete on reboot.
C:\WINDOWS\system32\lowsec\user.ds (Stolen.Data) -> Delete on reboot.
C:\WINDOWS\owonowet.dll (Trojan.Agent) -> Delete on reboot.
C:\WINDOWS\system32\sdra64.exe (Trojan.FakeAlert) -> Delete on reboot.

trojan.win32.cd