

Malwarebytes Anti-Malware - provedeno čištění

5.5.2013 9:43:05

mbam-log-2013-05-05 (09-43-05).txt

Typ: Rychlá kontrola

Nastavení kontroly povoleno: Paměť | Po spuštění | Registr | Systémové soubory | Heuristická analýza Extra |
Heuristická analýza Shuriken | PUP | PUM

Nastavení kontroly zakázáno: P2P

Kontrolované objekty: 245275

Uplynulý čas: 7 minut, 26 sekund

Nalezené procesy v paměti: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené moduly v paměti: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené klíče v registru: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené hodnoty v registru: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené datové položky v registru: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené složky: 0

(Žádné škodlivé položky nebyly zjištěny)

Nalezené soubory: 0

(Žádné škodlivé položky nebyly zjištěny)

TDSS rootkit removing tool - log1

09:41:42.0564 0324 TDSS rootkit removing tool 2.8.16.0 Feb 11 2013 18:50:42

09:41:43.0280 0324 =====

09:41:43.0280 0324 Current date / time: 2013/05/05 09:41:43.0280

09:41:43.0280 0324 SystemInfo:

09:41:43.0280 0324

09:41:43.0280 0324 OS Version: 6.1.7600 ServicePack: 0.0

09:41:43.0280 0324 Product type: Workstation

09:41:43.0280 0324 ComputerName: USER-LAPTOP

09:41:43.0281 0324 UserName: User

09:41:43.0281 0324 Windows directory: C:\Windows

09:41:43.0281 0324 System windows directory: C:\Windows

09:41:43.0281 0324 Processor architecture: Intel x86

09:41:43.0281 0324 Number of processors: 2

09:41:43.0281 0324 Page size: 0x1000

09:41:43.0281 0324 Boot type: Normal boot

09:41:43.0281 0324 =====

09:41:45.0630 0324 Drive \Device\Harddisk0\DR0 - Size: 0x3A38B2E000 (232.89 Gb), SectorSize: 0x200, Cylinders: 0x76C1, SectorsPerTrack: 0x3F, TracksPerCylinder: 0xFF, Type 'K0', Flags 0x00000050

09:41:45.0661 0324 =====

09:41:45.0661 0324 \Device\Harddisk0\DR0:

09:41:45.0682 0324 MBR partitions:

09:41:45.0682 0324 \Device\Harddisk0\DR0\Partition1: MBR, Type 0x7, StartLBA 0x800, BlocksNum 0x32000

09:41:45.0682 0324 \Device\Harddisk0\DR0\Partition2: MBR, Type 0x7, StartLBA 0x32800, BlocksNum 0x5014000

09:41:45.0682 0324 \Device\Harddisk0\DR0\Partition3: MBR, Type 0x7, StartLBA 0x5046800, BlocksNum 0x16C10000

09:41:45.0713 0324 =====

09:41:45.0803 0324 C: <-> \Device\Harddisk0\DR0\Partition2

09:41:45.0863 0324 D: <-> \Device\Harddisk0\DR0\Partition3

09:41:45.0863 0324 =====

09:41:45.0863 0324 Initialize success

09:41:45.0863 0324 =====

09:41:49.0070 1060 Deinitialize success

TDSS rootkit removing tool - log2

09:57:57.0580 6108 TDSS rootkit removing tool 2.8.16.0 Feb 11 2013 18:50:42

09:57:57.0866 6108 =====

09:57:57.0866 6108 Current date / time: 2013/05/05 09:57:57.0866

09:57:57.0866 6108 SystemInfo:

09:57:57.0866 6108

09:57:57.0866 6108 OS Version: 6.1.7600 ServicePack: 0.0

09:57:57.0866 6108 Product type: Workstation

09:57:57.0867 6108 ComputerName: USER-LAPTOP

09:57:57.0867 6108 UserName: User

09:57:57.0867 6108 Windows directory: C:\Windows

09:57:57.0867 6108 System windows directory: C:\Windows

09:57:57.0867 6108 Processor architecture: Intel x86

09:57:57.0867 6108 Number of processors: 2

09:57:57.0867 6108 Page size: 0x1000

09:57:57.0867 6108 Boot type: Normal boot

09:57:57.0867 6108 =====

09:57:58.0860 6108 Drive \Device\Harddisk0\DR0 - Size: 0x3A38B2E000 (232.89 Gb), SectorSize: 0x200, Cylinders: 0x76C1, SectorsPerTrack: 0x3F, TracksPerCylinder: 0xFF, Type 'K0', Flags 0x00000050

09:57:58.0871 6108 =====

09:57:58.0872 6108 \Device\Harddisk0\DR0:

09:57:58.0882 6108 MBR partitions:

09:57:58.0883 6108 \Device\Harddisk0\DR0\Partition1: MBR, Type 0x7, StartLBA 0x800, BlocksNum 0x32000

09:57:58.0883 6108 \Device\Harddisk0\DR0\Partition2: MBR, Type 0x7, StartLBA 0x32800, BlocksNum 0x5014000

09:57:58.0883 6108 \Device\Harddisk0\DR0\Partition3: MBR, Type 0x7, StartLBA 0x5046800, BlocksNum 0x16C10000

09:57:58.0913 6108 =====

09:57:58.0970 6108 C: <-> \Device\Harddisk0\DR0\Partition2

09:57:58.0997 6108 D: <-> \Device\Harddisk0\DR0\Partition3

09:57:58.0998 6108 =====

09:57:58.0998 6108 Initialize success

09:57:58.0998 6108 =====

09:58:00.0432 5540 =====

09:58:00.0432 5540 Scan started

09:58:00.0433 5540 Mode: Manual;

09:58:00.0433 5540 =====

09:58:01.0533 5540 ===== Scan system memory =====

09:58:01.0534 5540 System memory - ok

09:58:01.0534 5540 ===== Scan services =====

09:58:01.0698 5540 [6D2ACA41739BFE8CB86EE8E85F29697D] 1394ohci
C:\Windows\system32\DRIVERS\1394ohci.sys

09:58:01.0700 5540 1394ohci - ok

09:58:01.0727 5540 [F0E07D144C8685B8774BC32FC8DA4DF0] ACPI
C:\Windows\system32\DRIVERS\ACPI.sys

09:58:01.0730 5540 ACPI - ok

09:58:01.0754 5540 [98D81CA942D19F7D9153B095162AC013] AcpiPmi
C:\Windows\system32\DRIVERS\acpipmi.sys

09:58:01.0755 5540 AcpiPmi - ok

09:58:01.0835 5540 [3927397AC60D943DAF8808AFFED582B7] AdobeARMservice C:\Program Files\Common
Files\Adobe\ARM\1.0\armsvc.exe

09:58:01.0837 5540 AdobeARMservice - ok

09:58:01.0910 5540 [479901C99FA62D1C3261B7ACB1228DAD] AdobeFlashPlayerUpdateSvc
C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe

09:58:01.0916 5540 AdobeFlashPlayerUpdateSvc - ok

09:58:01.0963 5540 [21E785EBD7DC90A06391141AAC7892FB] adp94xx
C:\Windows\system32\DRIVERS\adp94xx.sys

09:58:01.0967 5540 adp94xx - ok

09:58:02.0014 5540 [0C676BC278D5B59FF5ABD57BBE9123F2] adpahci
C:\Windows\system32\DRIVERS\adpahci.sys

09:58:02.0017 5540 adpahci - ok

09:58:02.0044 5540 [7C7B5EE4B7B822EC85321FE23A27DB33] adpu320
C:\Windows\system32\DRIVERS\adpu320.sys

09:58:02.0047 5540 adpu320 - ok

09:58:02.0083 5540 [8B5EEFEEC1E6D1A72A06C526628AD161] AeLookupSvc C:\Windows\System32\aelupsvc.dll

09:58:02.0084 5540 AeLookupSvc - ok

09:58:02.0122 5540 [DDC040FDB01EF1712A6B13E52AFB104C] AFD C:\Windows\system32\drivers\afd.sys

09:58:02.0128 5540 AFD - ok

09:58:02.0193 5540 [7E10E3BB9B258AD8A9300F91214D67B9] AgereSoftModem
C:\Windows\system32\DRIVERS\AGRSM.sys

09:58:02.0201 5540 AgereSoftModem - ok

09:58:02.0236 5540 [507812C3054C21CEF746B6EE3D04DD6E] agp440
C:\Windows\system32\DRIVERS\agp440.sys

09:58:02.0238 5540 agp440 - ok

09:58:02.0264 5540 [8B30250D573A8F6B4BD23195160D8707] aic78xx
C:\Windows\system32\DRIVERS\djsvs.sys

09:58:02.0265 5540 aic78xx - ok

09:58:02.0328 5540 [18A54E132947CD98FEA9ACCC57F98F13] ALG C:\Windows\System32\alg.exe

09:58:02.0331 5540 ALG - ok

09:58:02.0351 5540 [0D40BCF52EA90FC7DF2AEAB6503DEA44] aliide
C:\Windows\system32\DRIVERS\aliide.sys

09:58:02.0352 5540 aliide - ok

09:58:02.0367 5540 [3C6600A0696E90A463771C7422E23AB5] amdagp
C:\Windows\system32\DRIVERS\amdagp.sys

09:58:02.0369 5540 amdagp - ok

09:58:02.0388 5540 [CD5914170297126B6266860198D1D4F0] amdide
C:\Windows\system32\DRIVERS\amdide.sys

09:58:02.0389 5540 amdide - ok

09:58:02.0414 5540 [00DDA200D71BAC534BF56A9DB5DFD666] AmdK8
C:\Windows\system32\DRIVERS\amdK8.sys

09:58:02.0415 5540 AmdK8 - ok

09:58:02.0423 5540 [3CBF30F5370FDA40DD3E87DF38EA53B6] AmdPPM
C:\Windows\system32\DRIVERS\amdppm.sys

09:58:02.0425 5540 AmdPPM - ok

09:58:02.0444 5540 [2101A86C25C154F8314B24EF49D7FBC2] amdsgata
C:\Windows\system32\DRIVERS\amdsgata.sys

09:58:02.0445 5540 amdsgata - ok

09:58:02.0459 5540 [EA43AF0C423FF267355F74E7A53BDABA] amdsgbs
C:\Windows\system32\DRIVERS\amdsgbs.sys

09:58:02.0462 5540 amdsgbs - ok

09:58:02.0481 5540 [B81C2B5616F6420A9941EA093A92B150] amdsgata
C:\Windows\system32\DRIVERS\amdsgata.sys

09:58:02.0482 5540 amdsgata - ok

09:58:02.0504 5540 [FEB834C02CE1E84B6A38F953CA067706] AppID
C:\Windows\system32\drivers\appid.sys

09:58:02.0505 5540 AppID - ok

09:58:02.0541 5540 [62A9C86CB6085E20DB4823E4E97826F5] AppIDSvc C:\Windows\System32\appidsgvc.dll

09:58:02.0543 5540 AppIDSvc - ok

09:58:02.0558 5540 [7DEAD9E3F65DCB2794F2711003BBF650] Appinfo C:\Windows\System32\appinfo.dll

09:58:02.0560 5540 Appinfo - ok

09:58:02.0622 5540 [4FE5C6D40664AE07BE5105874357D2ED] Apple Mobile Device C:\Program Files\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe

09:58:02.0625 5540 Apple Mobile Device - ok

09:58:02.0652 5540 [A45D184DF6A8803DA13A0B329517A64A] AppMgmt
C:\Windows\System32\appmgmts.dll

09:58:02.0654 5540 AppMgmt - ok

09:58:02.0695 5540 [2932004F49677BD84DBC72EDB754FFB3] arc C:\Windows\system32\DRIVERS\arc.sys

09:58:02.0696 5540 arc - ok

09:58:02.0705 5540 [5D6F36C46FD283AE1B57BD2E9FEB0BC7] arcsas
C:\Windows\system32\DRIVERS\arcsas.sys

09:58:02.0707 5540 arcsas - ok

09:58:02.0745 5540 [CCDA8D84FD02AEC52E62F296433AE9DC] aswFsBlk
C:\Windows\system32\drivers\aswFsBlk.sys

09:58:02.0746 5540 aswFsBlk - ok

09:58:02.0773 5540 [A6E20E62871A28A0F1C05B1681848FA7] aswMonFlt
C:\Windows\system32\drivers\aswMonFlt.sys

09:58:02.0774 5540 aswMonFlt - ok

09:58:02.0788 5540 [6844738D52970A0F482768EEA941C78E] aswRdr
C:\Windows\System32\Drivers\aswRdr.sys

09:58:02.0789 5540 aswRdr - ok

09:58:02.0813 5540 [657A61979F40D67CA29716149766FFA7] aswRvrt
C:\Windows\system32\drivers\aswRvrt.sys

09:58:02.0814 5540 aswRvrt - ok

09:58:02.0852 5540 [0E604867FC28F00D91CB0B00D2EC830D] aswSnx
C:\Windows\system32\drivers\aswSnx.sys

09:58:02.0858 5540 aswSnx - ok

09:58:02.0897 5540 [6FC4AA106AA505394C908D37CCCB9148] aswSP
C:\Windows\system32\drivers\aswSP.sys

09:58:02.0900 5540 aswSP - ok

09:58:02.0920 5540 [33E21FFB063CA6C7E00D568467DC72E4] aswTdi
C:\Windows\system32\drivers\aswTdi.sys

09:58:02.0922 5540 aswTdi - ok

09:58:02.0954 5540 [EDB0C9BA44B748E420CCA989FD8B826E] aswVmm
C:\Windows\system32\drivers\aswVmm.sys

09:58:02.0956 5540 aswVmm - ok

09:58:02.0978 5540 [ADD2ADE1C2B285AB8378D2DAAF991481] AsyncMac
C:\Windows\system32\DRIVERS\asyncmac.sys

09:58:02.0979 5540 AsyncMac - ok

09:58:03.0004 5540 [338C86357871C167A96AB976519BF59E] atapi
C:\Windows\system32\DRIVERS\atapi.sys

09:58:03.0005 5540 atapi - ok

09:58:03.0080 5540 [10A82E63B50672987B6B09B215213CC4] athr C:\Windows\system32\DRIVERS\athr.sys

09:58:03.0099 5540 athr - ok

09:58:03.0149 5540 [510C873BFA135AA829F4180352772734] AudioEndpointBuilder
C:\Windows\System32\Audiosrv.dll

09:58:03.0153 5540 AudioEndpointBuilder - ok

09:58:03.0167 5540 [510C873BFA135AA829F4180352772734] Audiosrv C:\Windows\System32\Audiosrv.dll

09:58:03.0172 5540 Audiosrv - ok

09:58:03.0233 5540 [41735B82DB57E4EBE9504EC400FD120E] avast! Antivirus C:\Program Files\AVAST
Software\Avast\AvastSvc.exe

09:58:03.0235 5540 avast! Antivirus - ok

09:58:03.0273 5540 [DD6A431B43E34B91A767D1CE33728175] AxInstSV C:\Windows\System32\AxInstSV.dll

09:58:03.0276 5540 AxInstSV - ok

09:58:03.0323 5540 [1A231ABEC60FD316EC54C66715543CEC] b06bdrv
C:\Windows\system32\DRIVERS\b06bdx.sys

09:58:03.0328 5540 b06bdrv - ok

09:58:03.0373 5540 [744663C3183CE5A11308F20C7B90C63E] b57nd60x
C:\Windows\system32\DRIVERS\b57nd60x.sys

09:58:03.0377 5540 b57nd60x - ok

09:58:03.0427 5540 [EE1E9C3BB8228AE423DD38DB69128E71] BDESVC C:\Windows\System32\bdesvc.dll

09:58:03.0430 5540 BDESVC - ok

09:58:03.0460 5540 [505506526A9D467307B3C393DEDAF858] Beep
C:\Windows\system32\drivers\Beep.sys

09:58:03.0461 5540 Beep - ok

09:58:03.0495 5540 [85AC71C045CEB054ED48A7841AAE0C11] BFE C:\Windows\System32\bfe.dll

09:58:03.0500 5540 BFE - ok

09:58:03.0540 5540 [53F476476F55A27F580661BDE09C4EC4] BITS C:\Windows\System32\qmgr.dll

09:58:03.0550 5540 BITS - ok

09:58:03.0572 5540 [2287078ED48FCFC477B05B20CF38F36F] blbdrive
C:\Windows\system32\DRIVERS\blbdrive.sys

09:58:03.0573 5540 blbdrive - ok

09:58:03.0630 5540 [DB5BEA73EDAF19AC68B2C0FAD0F92B1A] Bonjour Service C:\Program
Files\Bonjour\mDNSResponder.exe

09:58:03.0637 5540 Bonjour Service - ok

09:58:03.0679 5540 [FCAFAEF6798D7B51FF029F99A9898961] bowser
C:\Windows\system32\DRIVERS\bowser.sys

09:58:03.0680 5540 bowser - ok

09:58:03.0695 5540 [9F9ACC7F7CCDE8A15C282D3F88B43309] BrFiltLo
C:\Windows\system32\DRIVERS\BrFiltLo.sys

09:58:03.0696 5540 BrFiltLo - ok

09:58:03.0705 5540 [56801AD62213A41F6497F96DEE83755A] BrFiltUp
C:\Windows\system32\DRIVERS\BrFiltUp.sys

09:58:03.0707 5540 BrFiltUp - ok

09:58:03.0734 5540 [598E1280E7FF3744F4B8329366CC5635] Browser C:\Windows\System32\browser.dll

09:58:03.0737 5540 Browser - ok

09:58:03.0760 5540 [845B8CE732E67F3B4133164868C666EA] Brserid
C:\Windows\System32\Drivers\Brserid.sys

09:58:03.0763 5540 Brserid - ok

09:58:03.0782 5540 [203F0B1E73ADADBBB7B7B1FABD901F6B] BrSerWdm
C:\Windows\System32\Drivers\BrSerWdm.sys

09:58:03.0784 5540 BrSerWdm - ok

09:58:03.0792 5540 [BD456606156BA17E60A04E18016AE54B] BrUsbMdm
C:\Windows\System32\Drivers\BrUsbMdm.sys

09:58:03.0794 5540 BrUsbMdm - ok

09:58:03.0803 5540 [AF72ED54503F717A43268B3CC5FAEC2E] BrUsbSer
C:\Windows\System32\Drivers\BrUsbSer.sys

09:58:03.0804 5540 BrUsbSer - ok

09:58:03.0814 5540 [ED3DF7C56CE0084EB2034432FC56565A] BTHMODEM
C:\Windows\system32\DRIVERS\bthmodem.sys

09:58:03.0816 5540 BTHMODEM - ok

09:58:03.0861 5540 [1DF19C96EEF6C29D1C3E1A8678E07190] bthserv C:\Windows\system32\bthserv.dll

09:58:03.0864 5540 bthserv - ok

09:58:03.0892 5540 [77EA11B065E0A8AB902D78145CA51E10] cdfs C:\Windows\system32\DRIVERS\cdfs.sys

09:58:03.0894 5540 cdfs - ok

09:58:03.0938 5540 [BA6E70AA0E6091BC39DE29477D866A77] cdrom
C:\Windows\system32\DRIVERS\cdrom.sys

09:58:03.0940 5540 cdrom - ok

09:58:03.0986 5540 [628A9E30EC5E18DD5DE6BE4DBDC12198] CertPropSvc C:\Windows\System32\certprop.dll

09:58:03.0989 5540 CertPropSvc - ok

09:58:04.0019 5540 [3FE3FE94A34DF6FB06E6418D0F6A0060] circlass
C:\Windows\system32\DRIVERS\circlass.sys

09:58:04.0020 5540 circlass - ok

09:58:04.0048 5540 [635181E0E9BBF16871BF5380D71DB02D] CLFS C:\Windows\system32\CLFS.sys

09:58:04.0053 5540 CLFS - ok

09:58:04.0141 5540 [D88040F816FDA31C3B466F0FA0918F29] clr_optimization_v2.0.50727_32
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe

09:58:04.0144 5540 clr_optimization_v2.0.50727_32 - ok

09:58:04.0169 5540 [DEA805815E587DAD1DD2C502220B5616] CmBatt
C:\Windows\system32\DRIVERS\CmBatt.sys

09:58:04.0170 5540 CmBatt - ok

09:58:04.0199 5540 [C537B1DB64D495B9B4717B4D6D9EDBF2] cmdide
C:\Windows\system32\DRIVERS\cmdide.sys

09:58:04.0201 5540 cmdide - ok

09:58:04.0228 5540 [1B675691ED940766149C93E8F4488D68] CNG C:\Windows\system32\Drivers\cng.sys

09:58:04.0232 5540 CNG - ok

09:58:04.0269 5540 [A6023D3823C37043986713F118A89BEE] Compbatt
C:\Windows\system32\DRIVERS\compbatt.sys

09:58:04.0270 5540 Compbatt - ok

09:58:04.0309 5540 [F1724BA27E97D627F808FB0BA77A28A6] CompositeBus
C:\Windows\system32\DRIVERS\CompositeBus.sys

09:58:04.0310 5540 CompositeBus - ok

09:58:04.0330 5540 COMSysApp - ok

09:58:04.0361 5540 [2C4EBCFC84A9B44F209DFF6C6E6C61D1] crcdisk
C:\Windows\system32\DRIVERS\crcdisk.sys

09:58:04.0363 5540 crcdisk - ok

09:58:04.0401 5540 [9C231178CE4FB385F4B54B0A9080B8A4] CryptSvc C:\Windows\system32\cryptsvc.dll

09:58:04.0405 5540 CryptSvc - ok

09:58:04.0432 5540 [27C9490BDD0AE48911AB8CF1932591ED] CSC C:\Windows\system32\drivers\csc.sys

09:58:04.0436 5540 CSC - ok

09:58:04.0467 5540 [56FB5F222EA30D3D3FC459879772CB73] CscService C:\Windows\System32\cscsvc.dll

09:58:04.0475 5540 CscService - ok

09:58:04.0514 5540 [B82CD39E336973359D7C9BF911E8E84F] DcomLaunch C:\Windows\system32\rpcss.dll

09:58:04.0523 5540 DcomLaunch - ok

09:58:04.0567 5540 [8D6E10A2D9A5EED59562D9B82CF804E1] defragsvc C:\Windows\System32\defragsvc.dll

09:58:04.0573 5540 defragsvc - ok

09:58:04.0614 5540 [8E09E52EE2E3CEB199EF3DD99CF9E3FB] DfsC C:\Windows\system32\Drivers\dfsc.sys

09:58:04.0615 5540 DfsC - ok

09:58:04.0651 5540 [7BEF2E2159EDB03105BC7A8BABE04726] dg_ssudbus
C:\Windows\system32\DRIVERS\ssudbus.sys

09:58:04.0653 5540 dg_ssudbus - ok

09:58:04.0699 5540 [C56495FBD770712367CAD35E5DE72DA6] Dhcp C:\Windows\system32\dhcpcore.dll

09:58:04.0704 5540 Dhcp - ok

09:58:04.0718 5540 [1A050B0274BFB3890703D490F330C0DA] discache
C:\Windows\system32\drivers\discache.sys

09:58:04.0720 5540 discache - ok

09:58:04.0757 5540 [565003F326F99802E68CA78F2A68E9FF] Disk C:\Windows\system32\DRIVERS\disk.sys

09:58:04.0758 5540 Disk - ok

09:58:04.0779 5540 [D0722E963D3C6145446874241401B209] Dnscache C:\Windows\System32\dnsrslvr.dll

09:58:04.0782 5540 Dnscache - ok

09:58:04.0843 5540 [4408C85C21EEA48EB0CE486BAEEF0502] dot3svc C:\Windows\System32\dot3svc.dll

09:58:04.0849 5540 dot3svc - ok

09:58:04.0955 5540 [B5E479EB83707DD698F66953E922042C] Dot4
C:\Windows\system32\DRIVERS\Dot4.sys

09:58:04.0957 5540 Dot4 - ok

09:58:05.0054 5540 [C25FEA07A8E7767E8B89AB96A3B96519] Dot4Print
C:\Windows\system32\DRIVERS\Dot4Prt.sys

09:58:05.0055 5540 Dot4Print - ok

09:58:05.0077 5540 [CF491FF38D62143203C065260567E2F7] dot4usb
C:\Windows\system32\DRIVERS\dot4usb.sys

09:58:05.0078 5540 dot4usb - ok

09:58:05.0103 5540 [7FA81C6E11CAA594ADB52084DA73A1E5] DPS C:\Windows\system32\dps.dll

09:58:05.0108 5540 DPS - ok

09:58:05.0175 5540 [B918E7C5F9BF77202F89E1A9539F2EB4] drmkaud
C:\Windows\system32\drivers\drmkaud.sys

09:58:05.0176 5540 drmkaud - ok

09:58:05.0275 5540 [687AF6BB383885FF6A64071B189A7F3E] dtsoftbus01
C:\Windows\system32\DRIVERS\dtsoftbus01.sys

09:58:05.0278 5540 dtsoftbus01 - ok

09:58:05.0400 5540 [39806CFEDDCC55E686A49BCCD2972F23] DXGKrnl
C:\Windows\System32\drivers\dxgkrnl.sys

09:58:05.0406 5540 DXGKrnl - ok

09:58:05.0445 5540 [8600142FA91C1B96367D3300AD0F3F3A] EapHost C:\Windows\System32\eapsvc.dll

09:58:05.0449 5540 EapHost - ok

09:58:05.0556 5540 [024E1B5CAC09731E4D868E64DBFB4AB0] ebdrv
C:\Windows\system32\DRIVERS\evbdx.sys

09:58:05.0580 5540 ebdrv - ok

09:58:05.0611 5540 [F42309C4191C506B71DB5D1126D26318] EFS C:\Windows\System32\lsass.exe

09:58:05.0616 5540 EFS - ok

09:58:05.0686 5540 [3A74A6E33685662B125A3269B1F2114F] ehRecvr C:\Windows\ehome\ehRecvr.exe

09:58:05.0697 5540 ehRecvr - ok

09:58:05.0709 5540 [D389BFF34F80CAEDE417BF9D1507996A] ehSched C:\Windows\ehome\ehsched.exe

09:58:05.0712 5540 ehSched - ok

09:58:05.0764 5540 [0ED67910C8C326796FAA00B2BF6D9D3C] elxstor
C:\Windows\system32\DRIVERS\elxstor.sys

09:58:05.0768 5540 elxstor - ok

09:58:05.0789 5540 [8FC3208352DD3912C94367A206AB3F11] ErrDev
C:\Windows\system32\DRIVERS\errdev.sys

09:58:05.0791 5540 ErrDev - ok

09:58:05.0837 5540 [F6916EFC29D9953D5D0DF06882AE8E16] EventSystem C:\Windows\system32\es.dll

09:58:05.0845 5540 EventSystem - ok

09:58:05.0880 5540 [2DC9108D74081149CC8B651D3A26207F] exfat C:\Windows\system32\drivers\exfat.sys

09:58:05.0882 5540 exfat - ok

09:58:05.0925 5540 [7E0AB74553476622FB6AE36F73D97D35] fastfat
C:\Windows\system32\drivers\fastfat.sys

09:58:05.0927 5540 fastfat - ok

09:58:05.0999 5540 [F7EA23CC5E6BF2181F3F399D54F6EFC1] Fax C:\Windows\system32\fxssvc.exe

09:58:06.0010 5540 Fax - ok

09:58:06.0033 5540 [E817A017F82DF2A1F8CFDBDA29388B29] fdc C:\Windows\system32\DRIVERS\fdc.sys

09:58:06.0035 5540 fdc - ok

09:58:06.0062 5540 [F3222C893BD2F5821A0179E5C71E88FB] fdPHost C:\Windows\system32\fdPHost.dll

09:58:06.0065 5540 fdPHost - ok

09:58:06.0116 5540 [7DBE8CBFE79EFBDEB98C9FB08D3A9A5B] FDResPub C:\Windows\system32\fdrespub.dll

09:58:06.0120 5540 FDResPub - ok

09:58:06.0189 5540 [6CF00369C97F3CF563BE99BE983D13D8] FileInfo
C:\Windows\system32\drivers\fileinfo.sys

09:58:06.0191 5540 FileInfo - ok

09:58:06.0212 5540 [42C51DC94C91DA21CB9196EB64C45DB9] Filetrace
C:\Windows\system32\drivers\filetrace.sys

09:58:06.0213 5540 Filetrace - ok

09:58:06.0221 5540 [87907AA70CB3C56600F1C2FB8841579B] flpydisk
C:\Windows\system32\DRIVERS\flpydisk.sys

09:58:06.0223 5540 flpydisk - ok

09:58:06.0272 5540 [7520EC808E0C35E0EE6F841294316653] FltMgr
C:\Windows\system32\drivers\fltMgr.sys

09:58:06.0275 5540 FltMgr - ok

09:58:06.0310 5540 [B6512A85815FDC3D560C3705F5BDB93D] FontCache C:\Windows\system32\FntCache.dll

09:58:06.0318 5540 FontCache - ok

09:58:06.0354 5540 [E56F39F6B7FDA0AC77A79B0FD3DE1A2F] FontCache3.0.0.0
C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe

09:58:06.0357 5540 FontCache3.0.0.0 - ok

09:58:06.0394 5540 [1A16B57943853E598CFF37FE2B8CBF1D] FsDepends
C:\Windows\system32\drivers\FsDepends.sys

09:58:06.0395 5540 FsDepends - ok

09:58:06.0416 5540 [A574B4360E438977038AAE4BF60D79A2] Fs_Rec
C:\Windows\system32\drivers\Fs_Rec.sys

09:58:06.0417 5540 Fs_Rec - ok

09:58:06.0451 5540 [5592F5DBA26282D24D2B080EB438A4D7] fvevol
C:\Windows\system32\DRIVERS\fvevol.sys

09:58:06.0453 5540 fvevol - ok

09:58:06.0480 5540 [65EE0C7A58B65E74AE05637418153938] gagp30kx
C:\Windows\system32\DRIVERS\gagp30kx.sys

09:58:06.0482 5540 gagp30kx - ok

09:58:06.0506 5540 [185ADA973B5020655CEE342059A86CBB] GEARAspiWDM
C:\Windows\system32\DRIVERS\GEARAspiWDM.sys

09:58:06.0507 5540 GEARAspiWDM - ok

09:58:06.0551 5540 [8BA3C04702BF8F927AB36AE8313CA4EE] gpsvc C:\Windows\System32\gpsvc.dll

09:58:06.0558 5540 gpsvc - ok

09:58:06.0607 5540 [506708142BC63DABA64F2D3AD1DCD5BF] gupdate C:\Program
Files\Google\Update\GoogleUpdate.exe

09:58:06.0609 5540 gupdate - ok

09:58:06.0615 5540 [506708142BC63DABA64F2D3AD1DCD5BF] gupdatem C:\Program
Files\Google\Update\GoogleUpdate.exe

09:58:06.0618 5540 gupdatem - ok

09:58:06.0659 5540 [833051C6C6C42117191935F734CFBD97] hamachi
C:\Windows\system32\DRIVERS\hamachi.sys

09:58:06.0661 5540 hamachi - ok

09:58:06.0758 5540 [6D12BDA1715C38BE1746B195B1E4337E] Hamachi2Svc C:\Program Files\LogMeIn
Hamachi\hamachi-2.exe

09:58:06.0781 5540 Hamachi2Svc - ok

09:58:06.0817 5540 [C44E3C2BAB6837DB337DDEE7544736DB] hcw85cir
C:\Windows\system32\drivers\hcw85cir.sys

09:58:06.0818 5540 hcw85cir - ok

09:58:06.0846 5540 [3530CAD25DEBA7DC7DE8BB51632CBC5F] HdAudAddService
C:\Windows\system32\drivers\HdAudio.sys

09:58:06.0850 5540 HdAudAddService - ok

09:58:06.0875 5540 [717A2207FD6F13AD3E664C7D5A43C7BF] HDAudBus
C:\Windows\system32\DRIVERS\HDAudBus.sys

09:58:06.0877 5540 HDAudBus - ok

09:58:06.0899 5540 [1D58A7F3E11A9731D0EAAAA8405ACC36] HidBatt
C:\Windows\system32\DRIVERS\HidBatt.sys

09:58:06.0900 5540 HidBatt - ok

09:58:06.0909 5540 [89448F40E6DF260C206A193A4683BA78] HidBth
C:\Windows\system32\DRIVERS\hidbth.sys

09:58:06.0911 5540 HidBth - ok

09:58:06.0923 5540 [CF50B4CF4A4F229B9F3C08351F99CA5E] HidIr C:\Windows\system32\DRIVERS\hidir.sys

09:58:06.0926 5540 HidIr - ok

09:58:06.0955 5540 [2BC6F6A1992B3A77F5F41432CA6B3B6B] hidserv C:\Windows\system32\hidserv.dll

09:58:06.0958 5540 hidserv - ok

09:58:06.0990 5540 [25072FB35AC90B25F9E4E3BACF774102] HidUsb
C:\Windows\system32\DRIVERS\hidusb.sys

09:58:06.0991 5540 HidUsb - ok

09:58:07.0023 5540 [741C2A45CA8407E374AABA3E330B7872] hkmsvc C:\Windows\system32\kmsvc.dll

09:58:07.0029 5540 hkmsvc - ok

09:58:07.0052 5540 [A768CA158BB06782A2835B907F4873C3] HomeGroupListener
C:\Windows\system32\ListSvc.dll

09:58:07.0059 5540 HomeGroupListener - ok

09:58:07.0079 5540 [FB08DEC5EF43D0C66D83B8E9694E7549] HomeGroupProvider
C:\Windows\system32\provsvc.dll

09:58:07.0087 5540 HomeGroupProvider - ok

09:58:07.0174 5540 [5DA42D24712E00728CEA2342A65009B2] hpqcxs08 C:\Program Files\HP\Digital
Imaging\bin\hpqcxs08.dll

09:58:07.0179 5540 hpqcxs08 - ok

09:58:07.0201 5540 [D86A39BF100069444D026D22D9A6E555] hpqddsvc C:\Program Files\HP\Digital
Imaging\bin\hpqddsvc.dll

09:58:07.0205 5540 hpqddsvc - ok

09:58:07.0229 5540 [295FDC419039090EB8B49FFDBB374549] HpSAMD
C:\Windows\system32\DRIVERS\HpSAMD.sys

09:58:07.0231 5540 HpSAMD - ok

09:58:07.0261 5540 [950CC1E6AE3A6CD23E0945CDE089B02C] HTCAND32
C:\Windows\system32\Drivers\ANDROIDUSB.sys

09:58:07.0262 5540 HTCAND32 - ok

09:58:07.0308 5540 [5C8BC8A28798FD010E7ABC4E0D588CAA] HTCMonitorService C:\Program Files\HTC Sync
Manager\HSMServiceEntry.exe

09:58:07.0310 5540 HTCMonitorService - ok

09:58:07.0331 5540 [339ADEFAD60353F960E3CA67CE468C24] htcnprot
C:\Windows\system32\DRIVERS\htcnprot.sys

09:58:07.0332 5540 htcnprot - ok

09:58:07.0370 5540 [C531C7FD9E8B62021112787C4E2C5A5A] HTTP
C:\Windows\system32\drivers\HTTP.sys

09:58:07.0375 5540 HTTP - ok

09:58:07.0402 5540 [8305F33CDE89AD6C7A0763ED0B5A8D42] hwpolicy
C:\Windows\system32\drivers\hwpolicy.sys

09:58:07.0403 5540 hwpolicy - ok

09:58:07.0423 5540 [F151F0BDC47F4A28B1B20A0818EA36D6] i8042prt
C:\Windows\system32\DRIVERS\i8042prt.sys

09:58:07.0425 5540 i8042prt - ok

09:58:07.0463 5540 [934AF4D7C5F457B9F0743F4299B77B67] iaStorV
C:\Windows\system32\DRIVERS\iaStorV.sys

09:58:07.0467 5540 iaStorV - ok

09:58:07.0530 5540 [5AF815EB5BC9802E5A064E2BA62BFC0C] idsvc
C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe

09:58:07.0556 5540 idsvc - ok

09:58:07.0739 5540 [9467514EA189475A6E7FDC5D7BDE9D3F] igfx
C:\Windows\system32\DRIVERS\igdkmd32.sys

09:58:07.0775 5540 igfx - ok

09:58:07.0810 5540 [4173FF5708F3236CF25195FEC742915] iirsp C:\Windows\system32\DRIVERS\iirsp.sys

09:58:07.0812 5540 iirsp - ok

09:58:07.0869 5540 [FAC0EE6562B121B1399D6E855583F7A5] IKEEXT C:\Windows\System32\ikeext.dll

09:58:07.0877 5540 IKEEXT - ok

09:58:07.0921 5540 InCDFs - ok

09:58:07.0930 5540 InCDPass - ok

09:58:07.0941 5540 InCDRm - ok

09:58:08.0037 5540 [DCE087456521FA31EEA20223A1937E42] IntcAzAudAddService
C:\Windows\system32\drivers\RTKVHDA.sys

09:58:08.0058 5540 IntcAzAudAddService - ok

09:58:08.0093 5540 [A0F12F2C9BA6C72F3987CE780E77C130] intelide
C:\Windows\system32\DRIVERS\intelide.sys

09:58:08.0095 5540 intelide - ok

09:58:08.0128 5540 [3B514D27BFC4ACCB4037BC6685F766E0] intelppm
C:\Windows\system32\DRIVERS\intelppm.sys

09:58:08.0130 5540 intelppm - ok

09:58:08.0165 5540 [ACB364B9075A45C0736E5C47BE5CAE19] IPBusEnum
C:\Windows\system32\ipbusenum.dll

09:58:08.0170 5540 IPBusEnum - ok

09:58:08.0182 5540 [709D1761D3B19A932FF0238EA6D50200] IpFilterDriver
C:\Windows\system32\DRIVERS\ipfltdrv.sys

09:58:08.0184 5540 IpFilterDriver - ok

09:58:08.0221 5540 [477397B432A256A50EE7E4339EB9EA14] iphlpsvc C:\Windows\System32\iphlpvc.dll

09:58:08.0228 5540 iphlpsvc - ok

09:58:08.0236 5540 [E4454B6C37D7FFD5649611F6496308A7] IPMIDRV
C:\Windows\system32\DRIVERS\IPMIDrv.sys

09:58:08.0238 5540 IPMIDRV - ok

09:58:08.0248 5540 [A5FA468D67ABCDAA36264E463A7BB0CD] IPNAT
C:\Windows\system32\drivers\ipnat.sys

09:58:08.0250 5540 IPNAT - ok

09:58:08.0310 5540 [E46B17060D3962A384AE484094614788] iPod Service C:\Program
Files\iPod\bin\iPodService.exe

09:58:08.0320 5540 iPod Service - ok

09:58:08.0354 5540 [42996CFF20A3084A56017B7902307E9F] IRENUM
C:\Windows\system32\drivers\irenum.sys

09:58:08.0355 5540 IRENUM - ok

09:58:08.0374 5540 [1F32BB6B38F62F7DF1A7AB7292638A35] isapnp
C:\Windows\system32\DRIVERS\isapnp.sys

09:58:08.0376 5540 isapnp - ok

09:58:08.0403 5540 [ED46C223AE46C6866AB77CDC41C404B7] iScsiPrt
C:\Windows\system32\DRIVERS\msiscsi.sys

09:58:08.0406 5540 iScsiPrt - ok

09:58:08.0434 5540 [ADEF52CA1AEAE82B50DF86B56413107E] kbdclass
C:\Windows\system32\DRIVERS\kbdclass.sys

09:58:08.0435 5540 kbdclass - ok

09:58:08.0460 5540 [3D9F0EBF350EDCFD6498057301455964] kbdhid
C:\Windows\system32\DRIVERS\kbdhid.sys

09:58:08.0461 5540 kbdhid - ok

09:58:08.0478 5540 [F42309C4191C506B71DB5D1126D26318] KeyIso C:\Windows\system32\lsass.exe

09:58:08.0482 5540 KeyIso - ok

09:58:08.0503 5540 [E36A061EC11B373826905B21BE10948F] KSecDD
C:\Windows\system32\Drivers\ksecdd.sys

09:58:08.0505 5540 KSecDD - ok

09:58:08.0535 5540 [26C046977E85B95036453D7B88BA1820] KSecPkg
C:\Windows\system32\Drivers\ksecpkg.sys

09:58:08.0537 5540 KSecPkg - ok

09:58:08.0568 5540 [89A7B9CC98D0D80C6F31B91C0A310FCD] KtmRm C:\Windows\system32\msdtckrm.dll

09:58:08.0578 5540 KtmRm - ok

09:58:08.0609 5540 [BCA92CB047A4326925ECEF759DBAA233] LanmanServer C:\Windows\system32\svrsvc.dll

09:58:08.0616 5540 LanmanServer - ok

09:58:08.0657 5540 [B9891F885DCF1F0513A51CB58493CB1F] LanmanWorkstation
C:\Windows\System32\wkssvc.dll

09:58:08.0664 5540 LanmanWorkstation - ok

09:58:08.0702 5540 [5001C2B3557B53DED02ABED3BCC6FD2D] LHidFilt
C:\Windows\system32\DRIVERS\LHidFilt.Sys

09:58:08.0704 5540 LHidFilt - ok

09:58:08.0739 5540 [F7611EC07349979DA9B0AE1F18CCC7A6] lltidio
C:\Windows\system32\DRIVERS\lltdio.sys

09:58:08.0740 5540 lltidio - ok

09:58:08.0774 5540 [5700673E13A2117FA3B9020C852C01E2] lltdsvc C:\Windows\System32\lltdsvc.dll

09:58:08.0781 5540 lltdsvc - ok

09:58:08.0801 5540 [55CA01BA19D0006C8F2639B6C045E08B] lmhosts C:\Windows\System32\lmhsvc.dll

09:58:08.0805 5540 lmhosts - ok

09:58:08.0839 5540 [3AD9369E5D17014971A11728F198994C] LMouFilt
C:\Windows\system32\DRIVERS\LMouFilt.Sys

09:58:08.0841 5540 LMouFilt - ok

09:58:08.0885 5540 [EB119A53CCF2ACC000AC71B065B78FEF] LSI_FC
C:\Windows\system32\DRIVERS\lsi_fc.sys

09:58:08.0887 5540 LSI_FC - ok

09:58:08.0895 5540 [8ADE1C877256A22E49B75D1CC9161F9C] LSI_SAS
C:\Windows\system32\DRIVERS\lsi_sas.sys

09:58:08.0899 5540 LSI_SAS - ok

09:58:08.0908 5540 [DC9DC3D3DAA0E276FD2EC262E38B11E9] LSI_SAS2
C:\Windows\system32\DRIVERS\lsi_sas2.sys

09:58:08.0910 5540 LSI_SAS2 - ok

09:58:08.0921 5540 [0A036C7D7CAB643A7F07135AC47E0524] LSI_SCSI
C:\Windows\system32\DRIVERS\lsi_scsi.sys

09:58:08.0923 5540 LSI_SCSI - ok

09:58:08.0938 5540 [6703E366CC18D3B6E534F5CF7DF39CEE] luafv C:\Windows\system32\drivers\luafv.sys

09:58:08.0940 5540 luafv - ok

09:58:08.0994 5540 [4470E3C1E0C3378E4CAB137893C12C3A] MBAMProtector
C:\Windows\system32\drivers\mbam.sys

09:58:08.0996 5540 MBAMProtector - ok

09:58:09.0032 5540 [65085456FD9A74D7F1A999520C299ECB] MBAMScheduler C:\Program Files\Malwarebytes' Anti-Malware\mbamscheduler.exe

09:58:09.0039 5540 MBAMScheduler - ok

09:58:09.0089 5540 [E0D7732F2D2E24B2DB3F67B6750295B8] MBAMService C:\Program Files\Malwarebytes' Anti-Malware\mbamservice.exe

09:58:09.0102 5540 MBAMService - ok

09:58:09.0134 5540 [E2B0887816ED336685954E3D8FDAA51D] Mcx2Svc C:\Windows\system32\Mcx2Svc.dll

09:58:09.0140 5540 Mcx2Svc - ok

09:58:09.0177 5540 [0FFF5B045293002AB38EB1FD1FC2FB74] megasas C:\Windows\system32\DRIVERS\megasas.sys

09:58:09.0179 5540 megasas - ok

09:58:09.0228 5540 [DCBAB2920C75F390CAF1D29F675D03D6] MegaSR C:\Windows\system32\DRIVERS\MegaSR.sys

09:58:09.0231 5540 MegaSR - ok

09:58:09.0303 5540 [FAFE367D032ED82E9332B4C741A20216] Microsoft Office Groove Audit Service C:\Program Files\Microsoft Office\Office12\GrooveAuditService.exe

09:58:09.0306 5540 Microsoft Office Groove Audit Service - ok

09:58:09.0335 5540 [146B6F43A673379A3C670E86D89BE5EA] MMCSS C:\Windows\system32\mmcsc.dll

09:58:09.0340 5540 MMCSS - ok

09:58:09.0352 5540 [F001861E5700EE84E2D4E52C712F4964] Modem C:\Windows\system32\drivers\modem.sys

09:58:09.0353 5540 Modem - ok

09:58:09.0397 5540 [79D10964DE86B292320E9DFE02282A23] monitor C:\Windows\system32\DRIVERS\monitor.sys

09:58:09.0399 5540 monitor - ok

09:58:09.0418 5540 [FB18CC1D4C2E716B6B903B0AC0CC0609] mouclass C:\Windows\system32\DRIVERS\mouclass.sys

09:58:09.0419 5540 mouclass - ok

09:58:09.0433 5540 [2C388D2CD01C9042596CF3C8F3C7B24D] mouhid C:\Windows\system32\DRIVERS\mouhid.sys

09:58:09.0435 5540 mouhid - ok

09:58:09.0454 5540 [921C18727C5920D6C0300736646931C2] mountmgr C:\Windows\system32\drivers\mountmgr.sys

09:58:09.0456 5540 mountmgr - ok

09:58:09.0501 5540 [9C3758018DED02F4AE53CCA1C5F084A2] MozillaMaintenance C:\Program Files\Mozilla Maintenance Service\maintenanceservice.exe

09:58:09.0504 5540 MozillaMaintenance - ok

09:58:09.0529 5540 [2AF5997438C55FB79D33D015C30E1974] mpio
C:\Windows\system32\DRIVERS\mpio.sys

09:58:09.0531 5540 mpio - ok

09:58:09.0564 5540 [AD2723A7B53DD1AACAE6AD8C0BFBF4D0] mpsdrv
C:\Windows\system32\drivers\mpsdrv.sys

09:58:09.0565 5540 mpsdrv - ok

09:58:09.0606 5540 [5CD996CECF45CBC3E8D109C86B82D69E] MpsSvc C:\Windows\system32\mpssvc.dll

09:58:09.0614 5540 MpsSvc - ok

09:58:09.0637 5540 [B1BE47008D20E43DA3ADC37C24CDB89D] MRxDAV
C:\Windows\system32\drivers\mrxdav.sys

09:58:09.0639 5540 MRxDAV - ok

09:58:09.0654 5540 [F4A054BE78AF7F410129C4B64B07DC9B] mrxsm
C:\Windows\system32\DRIVERS\mrxsm.sys

09:58:09.0656 5540 mrxsm - ok

09:58:09.0680 5540 [DEFFA295BD1895C6ED8E3078412AC60B] mrxsm10
C:\Windows\system32\DRIVERS\mrxsm10.sys

09:58:09.0683 5540 mrxsm10 - ok

09:58:09.0699 5540 [24D76ABE5DCAD22F19D105F76FDF0CE1] mrxsm20
C:\Windows\system32\DRIVERS\mrxsm20.sys

09:58:09.0701 5540 mrxsm20 - ok

09:58:09.0722 5540 [4326D168944123F38DD3B2D9C37A0B12] msahci
C:\Windows\system32\DRIVERS\msahci.sys

09:58:09.0723 5540 msahci - ok

09:58:09.0742 5540 [455029C7174A2DBB03DBA8A0D8BDDD9A] msdsm
C:\Windows\system32\DRIVERS\msdsm.sys

09:58:09.0744 5540 msdsm - ok

09:58:09.0773 5540 [E1BCE74A3BD9902B72599C0192A07E27] MSDTC C:\Windows\System32\msdtc.exe

09:58:09.0781 5540 MSDTC - ok

09:58:09.0803 5540 [DAEFB28E3AF5A76ABCC2C3078C07327F] Msfs C:\Windows\system32\drivers\Msfs.sys

09:58:09.0805 5540 Msfs - ok

09:58:09.0834 5540 [3E1E5767043C5AF9367F0056295E9F84] mshidkmdf
C:\Windows\System32\drivers\mshidkmdf.sys

09:58:09.0835 5540 mshidkmdf - ok

09:58:09.0854 5540 [0A4E5757AE09FA9622E3158CC1AEF114] msisadrv
C:\Windows\system32\DRIVERS\msisadrv.sys

09:58:09.0855 5540 msisadrv - ok

09:58:09.0901 5540 [90F7D9E6B6F27E1A707D4A297F077828] MSiSCSI C:\Windows\system32\iscsiexe.dll

09:58:09.0906 5540 MSiSCSI - ok

09:58:09.0918 5540 msiserver - ok

09:58:09.0954 5540 [8C0860D6366AAFFB6C5BB9DF9448E631] MSKSSRV
C:\Windows\system32\drivers\MSKSSRV.sys

09:58:09.0955 5540 MSKSSRV - ok

09:58:09.0968 5540 [3EA8B949F963562CEDBB549EAC0C11CE] MSPCLOCK
C:\Windows\system32\drivers\MSPCLOCK.sys

09:58:09.0969 5540 MSPCLOCK - ok

09:58:09.0999 5540 [F456E973590D663B1073E9C463B40932] MSPQM
C:\Windows\system32\drivers\MSPQM.sys

09:58:10.0001 5540 MSPQM - ok

09:58:10.0037 5540 [0E008FC4819D238C51D7C93E7B41E560] MsRPC
C:\Windows\system32\drivers\MsRPC.sys

09:58:10.0040 5540 MsRPC - ok

09:58:10.0147 5540 [FC6B9FF600CC585EA38B12589BD4E246] mssmbios
C:\Windows\system32\DRIVERS\mssmbios.sys

09:58:10.0149 5540 mssmbios - ok

09:58:10.0190 5540 [B42C6B921F61A6E55159B8BE6CD54A36] MSTEE
C:\Windows\system32\drivers\MSTEE.sys

09:58:10.0191 5540 MSTEE - ok

09:58:10.0222 5540 [33599130F44E1F34631CEA241DE8AC84] MTConfig
C:\Windows\system32\DRIVERS\MTConfig.sys

09:58:10.0224 5540 MTConfig - ok

09:58:10.0301 5540 [159FAD02F64E6381758C990F753BCC80] Mup C:\Windows\system32\Drivers\mup.sys

09:58:10.0303 5540 Mup - ok

09:58:10.0381 5540 [80284F1985C70C86F0B5F86DA2DFE1DF] napagent C:\Windows\system32\qagentRT.dll

09:58:10.0389 5540 napagent - ok

09:58:10.0429 5540 [26384429FCD85D83746F63E798AB1480] NativeWifiP
C:\Windows\system32\DRIVERS\nwifi.sys

09:58:10.0433 5540 NativeWifiP - ok

09:58:10.0482 5540 [23759D175A0A9BAAF04D05047BC135A8] NDIS C:\Windows\system32\drivers\ndis.sys

09:58:10.0489 5540 NDIS - ok

09:58:10.0526 5540 [0E1787AA6C9191D3D319E8BAFE86F80C] NdisCap
C:\Windows\system32\DRIVERS\ndiscap.sys

09:58:10.0528 5540 NdisCap - ok

09:58:10.0550 5540 [E4A8AEC125A2E43A9E32AFEEA7C9C888] NdisTapi
C:\Windows\system32\DRIVERS\ndistapi.sys

09:58:10.0551 5540 NdisTapi - ok

09:58:10.0565 5540 [B30AE7F2B6D7E343B0DF32E6C08FCE75] Ndisuio
C:\Windows\system32\DRIVERS\ndisuio.sys

09:58:10.0566 5540 Ndisuio - ok

09:58:10.0584 5540 [267C415EADCBE53C9CA873DEE39CF3A4] NdisWan
C:\Windows\system32\DRIVERS\ndiswan.sys

09:58:10.0586 5540 NdisWan - ok

09:58:10.0599 5540 [AF7E7C63DCEF3F8772726F86039D6EB4] NDPProxy
C:\Windows\system32\drivers\NDProxy.sys

09:58:10.0600 5540 NDPProxy - ok

09:58:10.0643 5540 [A081CB6FB9A12668F233EB5414BE3A0E] Net Driver HPZ12
C:\Windows\system32\HPZinw12.dll

09:58:10.0647 5540 Net Driver HPZ12 - ok

09:58:10.0687 5540 [80B275B1CE3B0E79909DB7B39AF74D51] NetBIOS
C:\Windows\system32\DRIVERS\netbios.sys

09:58:10.0688 5540 NetBIOS - ok

09:58:10.0709 5540 [DD52A733BF4CA5AF84562A5E2F963B91] NetBT
C:\Windows\system32\DRIVERS\netbt.sys

09:58:10.0711 5540 NetBT - ok

09:58:10.0745 5540 [F42309C4191C506B71DB5D1126D26318] Netlogon C:\Windows\system32\lsass.exe

09:58:10.0749 5540 Netlogon - ok

09:58:10.0804 5540 [7CCCFCA7510684768DA22092D1FA4DB2] Netman C:\Windows\System32\netman.dll

09:58:10.0813 5540 Netman - ok

09:58:10.0849 5540 [8C338238C16777A802D6A9211EB2BA50] netprofm C:\Windows\System32\netprofm.dll

09:58:10.0860 5540 netprofm - ok

09:58:10.0903 5540 [76B1157EF850830C5ECE61D3E591CA8B] netr73
C:\Windows\system32\DRIVERS\netr73.sys

09:58:10.0909 5540 netr73 - ok

09:58:10.0949 5540 [FE2AA5A684B0DD9B1FAE57B7817C198B] NetTcpPortSharing
C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\SMHost.exe

09:58:10.0953 5540 NetTcpPortSharing - ok

09:58:11.0000 5540 [1D85C4B390B0EE09C7A46B91EFB2C097] nfrd960
C:\Windows\system32\DRIVERS\nfrd960.sys

09:58:11.0002 5540 nfrd960 - ok

09:58:11.0029 5540 [2226496E34BD40734946A054B1CD657F] NlaSvc C:\Windows\System32\ntlasvc.dll

09:58:11.0037 5540 NlaSvc - ok

09:58:11.0054 5540 [1DB262A9F8C087E8153D89BEF3D2235F] Npfs C:\Windows\system32\drivers\Npfs.sys

09:58:11.0055 5540 Npfs - ok

09:58:11.0084 5540 [BA387E955E890C8A88306D9B8D06BF17] nsi C:\Windows\system32\ntsisvc.dll

09:58:11.0089 5540 nsi - ok

09:58:11.0106 5540 [E9A0A4D07E53D8FEA2BB8387A3293C58] nsiproxy
C:\Windows\system32\drivers\ntsiprxy.sys

09:58:11.0108 5540 nsiproxy - ok

09:58:11.0163 5540 [3795DCD21F740EE799FB7223234215AF] Ntfs C:\Windows\system32\drivers\Ntfs.sys

09:58:11.0173 5540 Ntfs - ok

09:58:11.0188 5540 [F9756A98D69098DCA8945D62858A812C] Null C:\Windows\system32\drivers\Null.sys

09:58:11.0189 5540 Null - ok

09:58:11.0224 5540 [3F3D04B1D08D43C16EA7963954EC768D] nvraid
C:\Windows\system32\DRIVERS\nvraid.sys

09:58:11.0226 5540 nvraid - ok

09:58:11.0236 5540 [C99F251A5DE63C6F129CF71933ACED0F] nvstor
C:\Windows\system32\DRIVERS\nvstor.sys

09:58:11.0238 5540 nvstor - ok

09:58:11.0261 5540 [5A0983915F02BAE73267CC2A041F717D] nv_agp
C:\Windows\system32\DRIVERS\nv_agp.sys

09:58:11.0263 5540 nv_agp - ok

09:58:11.0332 5540 [84DE1DD996B48B05ACE31AD015FA108A] odserv C:\Program Files\Common Files\Microsoft Shared\OFFICE12\ODSERV.EXE

09:58:11.0342 5540 odserv - ok

09:58:11.0373 5540 [08A70A1F2CDDE9BB49B885CB817A66EB] ohci1394 C:\Windows\system32\DRIVERS\ohci1394.sys

09:58:11.0375 5540 ohci1394 - ok

09:58:11.0411 5540 [5A432A042DAE460ABE7199B758E8606C] ose C:\Program Files\Common Files\Microsoft Shared\Source Engine\OSE.EXE

09:58:11.0415 5540 ose - ok

09:58:11.0450 5540 [82A8521DDC60710C3D3D3E7325209BEC] p2pimsvc C:\Windows\system32\pnrpsvc.dll

09:58:11.0458 5540 p2pimsvc - ok

09:58:11.0476 5540 [59C3DDD501E39E006DAC31BF55150D91] p2psvc C:\Windows\system32\p2psvc.dll

09:58:11.0483 5540 p2psvc - ok

09:58:11.0540 5540 [1011C779C9FCD01AFA96490C86A50421] PanService C:\Program Files\PANDORA.TV\PanService\PandoraService.exe

09:58:11.0545 5540 PanService - ok

09:58:11.0575 5540 [2EA877ED5DD9713C5AC74E8EA7348D14] Parport C:\Windows\system32\DRIVERS\parport.sys

09:58:11.0576 5540 Parport - ok

09:58:11.0596 5540 [FF4218952B51DE44FE910953A3E686B9] partmgr C:\Windows\system32\drivers\partmgr.sys

09:58:11.0598 5540 partmgr - ok

09:58:11.0611 5540 [EB0A59F29C19B86479D36B35983DAADC] Parvdm C:\Windows\system32\DRIVERS\parvdm.sys

09:58:11.0612 5540 Parvdm - ok

09:58:11.0654 5540 [3CAE2BBC86FCF7F94C9696994AF30386] PassThru Service C:\Program Files\HTC\Internet Pass-Through\PassThruSvr.exe

09:58:11.0658 5540 PassThru Service - ok

09:58:11.0694 5540 [358AB7956D3160000726574083DFC8A6] PcaSvc C:\Windows\System32\pcasvc.dll

09:58:11.0700 5540 PcaSvc - ok

09:58:11.0724 5540 [C858CB77C577780ECC456A892E7E7D0F] pci C:\Windows\system32\DRIVERS\pci.sys

09:58:11.0726 5540 pci - ok

09:58:11.0747 5540 [AFE86F419014DB4E5593F69FFE26CE0A] pciide C:\Windows\system32\DRIVERS\pciide.sys

09:58:11.0749 5540 pciide - ok

09:58:11.0770 5540 [F396431B31693E71E8A80687EF523506] pcmcia
C:\Windows\system32\DRIVERS\pcmcia.sys

09:58:11.0772 5540 pcmcia - ok

09:58:11.0792 5540 [250F6B43D2B613172035C6747AEFB19F] pcw C:\Windows\system32\drivers\pcw.sys

09:58:11.0794 5540 pcw - ok

09:58:11.0832 5540 [9E0104BA49F4E6973749A02BF41344ED] PEAUTH
C:\Windows\system32\drivers\peauth.sys

09:58:11.0838 5540 PEAUTH - ok

09:58:11.0898 5540 [AF4D64D2A57B9772CF3801950B8058A6] PeerDistSvc
C:\Windows\system32\peerdistsvc.dll

09:58:11.0911 5540 PeerDistSvc - ok

09:58:11.0992 5540 [9C1BFF7910C89A1D12E57343475840CB] pla C:\Windows\system32\pla.dll

09:58:12.0008 5540 pla - ok

09:58:12.0038 5540 [2CC2008F1296968FBA162ED9F9AFE328] PlugPlay C:\Windows\system32\umprnmgr.dll

09:58:12.0047 5540 PlugPlay - ok

09:58:12.0140 5540 [65BC271F337637731D3C71455AE1F476] Pml Driver HPZ12
C:\Windows\system32\HPZipm12.dll

09:58:12.0143 5540 Pml Driver HPZ12 - ok

09:58:12.0169 5540 [63FF8572611249931EB16BB8EED6AFC8] PNRPAutoReg
C:\Windows\system32\pnrpauto.dll

09:58:12.0175 5540 PNRPAutoReg - ok

09:58:12.0206 5540 [82A8521DDC60710C3D3D3E7325209BEC] PNRPsvc C:\Windows\system32\pnrpsvc.dll

09:58:12.0213 5540 PNRPsvc - ok

09:58:12.0250 5540 [48E1B75C6DC0232FD92BAAE4BD344721] PolicyAgent C:\Windows\System32\ipsecsvc.dll

09:58:12.0260 5540 PolicyAgent - ok

09:58:12.0285 5540 [DBFF83F709A91049621C1D35DD45C92C] Power C:\Windows\system32\umpo.dll

09:58:12.0293 5540 Power - ok

09:58:12.0328 5540 [631E3E205AD6D86F2AED6A4A8E69F2DB] PptpMiniport
C:\Windows\system32\DRIVERS\raspptp.sys

09:58:12.0330 5540 PptpMiniport - ok

09:58:12.0360 5540 [85B1E3A0C7585BC4AAE6899EC6FCF011] Processor
C:\Windows\system32\DRIVERS\processr.sys

09:58:12.0362 5540 Processor - ok

09:58:12.0395 5540 [630CF26F0227498B7D5A92B12548960F] ProfSvc C:\Windows\system32\profsvc.dll

09:58:12.0403 5540 ProfSvc - ok

09:58:12.0422 5540 [F42309C4191C506B71DB5D1126D26318] ProtectedStorage C:\Windows\system32\lsass.exe

09:58:12.0427 5540 ProtectedStorage - ok

09:58:12.0457 5540 [6270CCAE2A86DE6D146529FE55B3246A] Psched
C:\Windows\system32\DRIVERS\pacer.sys

09:58:12.0460 5540 Psched - ok

09:58:12.0492 5540 [0B6DEA0A1662CAB8F2BF339DC0752EF4] PSI_SVC_2 c:\Program Files\Common
Files\Protexis\License Service\PsiService_2.exe

09:58:12.0497 5540 PSI_SVC_2 - ok

09:58:12.0550 5540 [AB95ECF1F6659A60DDC166D8315B0751] ql2300
C:\Windows\system32\DRIVERS\ql2300.sys

09:58:12.0562 5540 ql2300 - ok

09:58:12.0596 5540 [B4DD51DD25182244B86737DC51AF2270] ql40xx
C:\Windows\system32\DRIVERS\ql40xx.sys

09:58:12.0598 5540 ql40xx - ok

09:58:12.0629 5540 [31AC809E7707EB580B2BDB760390765A] QWAVE C:\Windows\system32\qwwave.dll

09:58:12.0636 5540 QWAVE - ok

09:58:12.0653 5540 [584078CA1B95CA72DF2A27C336F9719D] QWAVEdrv
C:\Windows\system32\drivers\qwavedrv.sys

09:58:12.0655 5540 QWAVEdrv - ok

09:58:12.0666 5540 [30A81B53C766D0133BB86D234E5556AB] RasAcid
C:\Windows\system32\DRIVERS\rasacd.sys

09:58:12.0668 5540 RasAcid - ok

09:58:12.0709 5540 [57EC4AEF73660166074D8F7F31C0D4FD] RasAgileVpn
C:\Windows\system32\DRIVERS\AgileVpn.sys

09:58:12.0711 5540 RasAgileVpn - ok

09:58:12.0734 5540 [A60F1839849C0C00739787FD5EC03F13] RasAuto C:\Windows\System32\rasauto.dll

09:58:12.0740 5540 RasAuto - ok

09:58:12.0780 5540 [D9F91EAFEC2815365CBE6D167E4E332A] Rasl2tp
C:\Windows\system32\DRIVERS\rasl2tp.sys

09:58:12.0782 5540 Rasl2tp - ok

09:58:12.0816 5540 [0CE66EC736B7FC526D78F7624C7D2A94] RasMan C:\Windows\System32\rasmans.dll

09:58:12.0824 5540 RasMan - ok

09:58:12.0843 5540 [0FE8B15916307A6AC12BFB6A63E45507] RasPppoe
C:\Windows\system32\DRIVERS\rasppoe.sys

09:58:12.0844 5540 RasPppoe - ok

09:58:12.0866 5540 [44101F495A83EA6401D886E7FD70096B] RasSstp
C:\Windows\system32\DRIVERS\rassstp.sys

09:58:12.0868 5540 RasSstp - ok

09:58:12.0893 5540 [835D7E81BF517A3B72384BDCC85E1CE6] rdbss
C:\Windows\system32\DRIVERS\rdbss.sys

09:58:12.0896 5540 rdbss - ok

09:58:12.0913 5540 [0D8F05481CB76E70E1DA06EE9F0DA9DF] rdpbus
C:\Windows\system32\DRIVERS\rdpbus.sys

09:58:12.0915 5540 rdpbus - ok

09:58:12.0935 5540 [1E016846895B15A99F9A176A05029075] RDPCDD
C:\Windows\system32\DRIVERS\RDPCDD.sys

09:58:12.0936 5540 RDPCDD - ok

09:58:12.0965 5540 [C5FF95883FFEF704D50C40D21CFB3AB5] RDPDR
C:\Windows\system32\drivers\rdpdr.sys

09:58:12.0967 5540 RDPDR - ok

09:58:12.0997 5540 [5A53CA1598DD4156D44196D200C94B8A] RDPENCDD
C:\Windows\system32\drivers\rdpencdd.sys

09:58:12.0999 5540 RDPENCDD - ok

09:58:13.0010 5540 [44B0A53CD4F27D50ED461DAE0C0B4E1F] RDPREFMP
C:\Windows\system32\drivers\rdprefmp.sys

09:58:13.0012 5540 RDPREFMP - ok

09:58:13.0030 5540 [801371BA9782282892D00AADB08EE367] RDPWD
C:\Windows\system32\drivers\RDPWD.sys

09:58:13.0032 5540 RDPWD - ok

09:58:13.0058 5540 [4EA225BF1CF05E158853F30A99CA29A7] rdyboost
C:\Windows\system32\drivers\rdyboost.sys

09:58:13.0061 5540 rdyboost - ok

09:58:13.0098 5540 [7B5E1419717FAC363A31CC302895217A] RemoteAccess C:\Windows\System32\mprdim.dll

09:58:13.0104 5540 RemoteAccess - ok

09:58:13.0133 5540 [CB9A8683F4EF2BF99E123D79950D7935] RemoteRegistry C:\Windows\system32\regsvc.dll

09:58:13.0139 5540 RemoteRegistry - ok

09:58:13.0169 5540 [3015A847EBA796EAC070F3F70079E15A] rp24msdrv
C:\Windows\system32\drivers\rp24msdrv.sys

09:58:13.0170 5540 rp24msdrv - ok

09:58:13.0201 5540 [78D072F35BC45D9E4E1B61895C152234] RpcEptMapper
C:\Windows\System32\RpcEpMap.dll

09:58:13.0207 5540 RpcEptMapper - ok

09:58:13.0224 5540 [94D36C0E44677DD26981D2BFEEF2A29D] RpcLocator C:\Windows\system32\locator.exe

09:58:13.0229 5540 RpcLocator - ok

09:58:13.0259 5540 [B82CD39E336973359D7C9BF911E8E84F] RpcSs C:\Windows\system32\rpcss.dll

09:58:13.0267 5540 RpcSs - ok

09:58:13.0314 5540 [032B0D36AD92B582D869879F5AF5B928] rspndr
C:\Windows\system32\DRIVERS\rspndr.sys

09:58:13.0316 5540 rspndr - ok

09:58:13.0330 5540 [5423D8437051E89DD34749F242C98648] s3cap
C:\Windows\system32\DRIVERS\vms3cap.sys

09:58:13.0332 5540 s3cap - ok

09:58:13.0345 5540 [F42309C4191C506B71DB5D1126D26318] SamSs C:\Windows\system32\lsass.exe

09:58:13.0349 5540 SamSs - ok

09:58:13.0374 5540 [34EE0C44B724E3E4CE2EFF29126DE5B5] sbp2port
C:\Windows\system32\DRIVERS\sbp2port.sys

09:58:13.0376 5540 sbp2port - ok

09:58:13.0411 5540 [8FC518FFE9519C2631D37515A68009C4] SCardSvr C:\Windows\System32\SCardSvr.dll

09:58:13.0418 5540 SCardSvr - ok

09:58:13.0434 5540 [A95C54B2AC3CC9C73FCDF9E51A1D6B51] scfilter
C:\Windows\system32\DRIVERS\scfilter.sys

09:58:13.0436 5540 scfilter - ok

09:58:13.0467 5540 [3E8B0C453E25613A1F59762A5C42AA75] Schedule C:\Windows\system32\schedsvc.dll

09:58:13.0478 5540 Schedule - ok

09:58:13.0497 5540 [628A9E30EC5E18DD5DE6BE4DBDC12198] SCPolicySvc C:\Windows\System32\certprop.dll

09:58:13.0499 5540 SCPolicySvc - ok

09:58:13.0531 5540 [5FD90ABDBFAEE85986802622CBB03446] SDRSVC C:\Windows\System32\SDRSVC.dll

09:58:13.0538 5540 SDRSVC - ok

09:58:13.0571 5540 [90A3935D05B494A5A39D37E71F09A677] secdrv
C:\Windows\system32\drivers\secdrv.sys

09:58:13.0573 5540 secdrv - ok

09:58:13.0598 5540 [A59B3A4442C52060CC7A85293AA3546F] seclogon C:\Windows\system32\seclogon.dll

09:58:13.0605 5540 seclogon - ok

09:58:13.0637 5540 [DCB7FCDCC97F87360F75D77425B81737] SENS C:\Windows\System32\sens.dll

09:58:13.0644 5540 SENS - ok

09:58:13.0674 5540 [50087FE1EE447009C9CC2997B90DE53F] SensrSvc C:\Windows\system32\sensrsvc.dll

09:58:13.0681 5540 SensrSvc - ok

09:58:13.0709 5540 [9AD8B8B515E3DF6ACD4212EF465DE2D1] Serenum
C:\Windows\system32\DRIVERS\serenum.sys

09:58:13.0711 5540 Serenum - ok

09:58:13.0719 5540 [5FB7FCEA0490D821F26F39CC5EA3D1E2] Serial
C:\Windows\system32\DRIVERS\serial.sys

09:58:13.0722 5540 Serial - ok

09:58:13.0729 5540 [79BFFB520327FF916A582DFEA17AA813] sermouse
C:\Windows\system32\DRIVERS\sermouse.sys

09:58:13.0731 5540 sermouse - ok

09:58:13.0775 5540 [8F55CE568C543D5ADF45C409D16718FC] SessionEnv C:\Windows\system32\sessenv.dll

09:58:13.0782 5540 SessionEnv - ok

09:58:13.0790 5540 [9F976E1EB233DF46FCE808D9DEA3EB9C] sffdisk
C:\Windows\system32\DRIVERS\sffdisk.sys

09:58:13.0792 5540 sffdisk - ok

09:58:13.0800 5540 [932A68EE27833CFD57C1639D375F2731] sffp_mmc
C:\Windows\system32\DRIVERS\sffp_mmc.sys

09:58:13.0802 5540 sffp_mmc - ok

09:58:13.0810 5540 [4F1E5B0FE7C8050668DBFADE8999AEFB] sffp_sd
C:\Windows\system32\DRIVERS\sffp_sd.sys

09:58:13.0812 5540 sffp_sd - ok

09:58:13.0820 5540 [DB96666CC8312EBC45032F30B007A547] sfloppy
C:\Windows\system32\DRIVERS\sfloppy.sys

09:58:13.0822 5540 sfloppy - ok

09:58:13.0860 5540 [D1A079A0DE2EA524513B6930C24527A2] SharedAccess C:\Windows\System32\ipnathlp.dll

09:58:13.0869 5540 SharedAccess - ok

09:58:13.0903 5540 [CD2E48FA5B29EE2B3B5858056D246EF2] ShellHWDetection C:\Windows\System32\shsvcs.dll

09:58:13.0912 5540 ShellHWDetection - ok

09:58:13.0925 5540 [2565CAC0DC9FE0371BDCE60832582B2E] sisagp
C:\Windows\system32\DRIVERS\sisagp.sys

09:58:13.0927 5540 sisagp - ok

09:58:13.0988 5540 [A9F0486851BECB6DDA1D89D381E71055] SiSRaid2
C:\Windows\system32\DRIVERS\SiSRaid2.sys

09:58:13.0990 5540 SiSRaid2 - ok

09:58:13.0999 5540 [3727097B55738E2F554972C3BE5BC1AA] SiSRaid4
C:\Windows\system32\DRIVERS\sisraid4.sys

09:58:14.0001 5540 SiSRaid4 - ok

09:58:14.0071 5540 [2F5AF9D91D51E832773D4A9EAF65CB33] SkypeUpdate C:\Program
Files\Skype\Updater\Updater.exe

09:58:14.0074 5540 SkypeUpdate - ok

09:58:14.0100 5540 [3E21C083B8A01CB70BA1F09303010FCE] Smb
C:\Windows\system32\DRIVERS\smb.sys

09:58:14.0102 5540 Smb - ok

09:58:14.0140 5540 [6A984831644ECA1A33FFEAE4126F4F37] SNMPTRAP
C:\Windows\System32\snmptrap.exe

09:58:14.0147 5540 SNMPTRAP - ok

09:58:14.0163 5540 [95CF1AE7527FB70F7816563CBC09D942] spldr C:\Windows\system32\drivers\spldr.sys

09:58:14.0165 5540 spldr - ok

09:58:14.0195 5540 [49B6DD6AB3715B7A67965F17194E98A9] Spooler C:\Windows\System32\spoolsv.exe

09:58:14.0205 5540 Spooler - ok

09:58:14.0299 5540 [4C287F9069FEDBD791178876EE9DE536] sppsvc C:\Windows\system32\sppsvc.exe

09:58:14.0331 5540 sppsvc - ok

09:58:14.0371 5540 [D8E3E19EEBDAB49DD4A8D3062EAD4EC7] sppuinotify
C:\Windows\system32\sppuinotify.dll

09:58:14.0377 5540 sppuinotify - ok

09:58:14.0433 5540 [CDDDEC541BC3C96F91ECB48759673505] sptd C:\Windows\system32\Drivers\sptd.sys

09:58:14.0433 5540 Suspicious file (NoAccess): C:\Windows\system32\Drivers\sptd.sys. md5:
CDDDEC541BC3C96F91ECB48759673505

09:58:14.0445 5540 sptd (LockedFile.Multi.Generic) - warning

09:58:14.0446 5540 sptd - detected LockedFile.Multi.Generic (1)

09:58:14.0497 5540 [2BA4EBC7DFBA845A1EDBE1F75913BE33] srv C:\Windows\system32\DRIVERS\srv.sys

09:58:14.0501 5540 srv - ok

09:58:14.0532 5540 [DCE7E10FEAABD4CAE95948B3DE5340BB] srv2
C:\Windows\system32\DRIVERS\srv2.sys

09:58:14.0535 5540 srv2 - ok

09:58:14.0552 5540 [B5665BAA2120B8A54E22E9CD07C05106] srvnet
C:\Windows\system32\DRIVERS\srvnet.sys

09:58:14.0554 5540 srvnet - ok

09:58:14.0591 5540 [D887C9FD02AC9FA880F6E5027A43E118] SSDPSRV C:\Windows\System32\ssdpsrv.dll

09:58:14.0599 5540 SSDPSRV - ok

09:58:14.0620 5540 [D318F23BE45D5E3A107469EB64815B50] SstpSvc C:\Windows\system32\sstpsvc.dll

09:58:14.0628 5540 SstpSvc - ok

09:58:14.0685 5540 [BCB4E273147AFCAFD0DA59AF9E6E25] ssudmdm
C:\Windows\system32\DRIVERS\ssudmdm.sys

09:58:14.0687 5540 ssudmdm - ok

09:58:14.0726 5540 [A651B8D404FB1C0DA03FDC6549E35750] ssudserd
C:\Windows\system32\DRIVERS\ssudserd.sys

09:58:14.0729 5540 ssudserd - ok

09:58:14.0759 5540 [DB32D325C192B801DF274BFD12A7E72B] stexstor
C:\Windows\system32\DRIVERS\stexstor.sys

09:58:14.0760 5540 stexstor - ok

09:58:14.0803 5540 [A22825E7BB7018E8AF3E229A5AF17221] StiSvc C:\Windows\System32\wiaservc.dll

09:58:14.0814 5540 StiSvc - ok

09:58:14.0847 5540 [957E346CA948668F2496A6CCF6FF82CC] storflt
C:\Windows\system32\DRIVERS\vmstorfl.sys

09:58:14.0849 5540 storflt - ok

09:58:14.0877 5540 [D5751969DC3E4B88BF482AC8EC9FE019] storvsc
C:\Windows\system32\DRIVERS\storvsc.sys

09:58:14.0879 5540 storvsc - ok

09:58:14.0901 5540 [E58C78A848ADD9610A4DB6D214AF5224] swenum
C:\Windows\system32\DRIVERS\swenum.sys

09:58:14.0903 5540 swenum - ok

09:58:15.0004 5540 [F577910A133A592234EBAAD3F3AFA258] SwitchBoard C:\Program Files\Common
Files\Adobe\SwitchBoard\SwitchBoard.exe

09:58:15.0013 5540 SwitchBoard - ok

09:58:15.0057 5540 [A28BD92DF340E57B024BA433165D34D7] swprv C:\Windows\System32\swprv.dll

09:58:15.0066 5540 swprv - ok

09:58:15.0113 5540 [04105C8DA62353589C29BDAEB8D88BD8] SysMain C:\Windows\system32\sysmain.dll

09:58:15.0128 5540 SysMain - ok

09:58:15.0157 5540 [FCFB6C552FBC0DA299799CBD50AD9FD4] TabletInputService
C:\Windows\System32\TabSvc.dll

09:58:15.0163 5540 TabletInputService - ok

09:58:15.0183 5540 [2F46B0C70A4ADC8C90CF825DA3B4FEAF] TapiSrv C:\Windows\System32\tapisrv.dll

09:58:15.0191 5540 TapiSrv - ok

09:58:15.0216 5540 [B799D9FDB26111737F58288D8DC172D9] TBS C:\Windows\System32\tbssvc.dll

09:58:15.0223 5540 TBS - ok

09:58:15.0285 5540 [2CC3D75488ABD3EC628BBB9A4FC84EFC] Tcpip
C:\Windows\system32\drivers\tcpip.sys

09:58:15.0296 5540 Tcpip - ok

09:58:15.0327 5540 [2CC3D75488ABD3EC628BBB9A4FC84EFC] TCPIP6
C:\Windows\system32\DRIVERS\tcpip.sys

09:58:15.0337 5540 TCPIP6 - ok

09:58:15.0358 5540 [E64444523ADD154F86567C469BC0B17F] tcpipreg
C:\Windows\system32\drivers\tcpipreg.sys

09:58:15.0360 5540 tcpipreg - ok

09:58:15.0391 5540 [1875C1490D99E70E449E3AFAE9FCBADF] TDPIPE
C:\Windows\system32\drivers\tdpipe.sys

09:58:15.0392 5540 TDPIPE - ok

09:58:15.0400 5540 [7551E91EA999EE9A8E9C331D5A9C31F3] TDTCP
C:\Windows\system32\drivers\tdtcp.sys

09:58:15.0402 5540 TDTCP - ok

09:58:15.0421 5540 [CB39E896A2A83702D1737BFD402B3542] tdx C:\Windows\system32\DRIVERS\tdx.sys

09:58:15.0423 5540 tdx - ok

09:58:15.0610 5540 [7C8DD5576695B3362202EF09B20C425E] TeamViewer8 C:\Program
Files\TeamViewer\Version8\TeamViewer_Service.exe

09:58:15.0777 5540 TeamViewer8 - ok

09:58:15.0818 5540 [C36F41EE20E6999DBF4B0425963268A5] TermDD
C:\Windows\system32\DRIVERS\termdd.sys

09:58:15.0820 5540 TermDD - ok

09:58:15.0857 5540 [A01E50A04D7B1960B33E92B9080E6A94] TermService C:\Windows\System32\termsrv.dll

09:58:15.0867 5540 TermService - ok

09:58:15.0886 5540 [42FB6AFD6B79D9FE07381609172E7CA4] Themes
C:\Windows\system32\themeservice.dll

09:58:15.0893 5540 Themes - ok

09:58:15.0913 5540 [146B6F43A673379A3C670E86D89BE5EA] THREADORDER C:\Windows\system32\mmcscs.dll

09:58:15.0918 5540 THREADORDER - ok

09:58:15.0944 5540 [4792C0378DB99A9BC2AE2DE6CFFF0C3A] TrkWks C:\Windows\System32\trkwks.dll

09:58:15.0950 5540 TrkWks - ok

09:58:15.0998 5540 [ED5E4CE36C54F55E7698642E94D32EC7] truecrypt
C:\Windows\system32\drivers>truecrypt.sys

09:58:16.0001 5540 truecrypt - ok

09:58:16.0049 5540 [41A4C781D2286208D397D72099304133] TrustedInstaller
C:\Windows\servicing\TrustedInstaller.exe

09:58:16.0054 5540 TrustedInstaller - ok

09:58:16.0112 5540 [98AE6FA07D12CB4EC5CF4A9BFA5F4242] tssecsrv
C:\Windows\system32\DRIVERS\tssecsrv.sys

09:58:16.0114 5540 tssecsrv - ok

09:58:16.0142 5540 [3E461D890A97F9D4C168F5FDA36E1D00] tunnel
C:\Windows\system32\DRIVERS\tunnel.sys

09:58:16.0144 5540 tunnel - ok

09:58:16.0180 5540 [750FBCB269F4D7DD2E420C56B795DB6D] uagp35
C:\Windows\system32\DRIVERS\uagp35.sys

09:58:16.0182 5540 uagp35 - ok

09:58:16.0220 5540 [09CC3E16F8E5EE7168E01CF8FCBE061A] udfs C:\Windows\system32\DRIVERS\udfs.sys

09:58:16.0223 5540 udfs - ok

09:58:16.0255 5540 [8344FD4FCE927880AA1AA7681D4927E5] UI0Detect
C:\Windows\system32\UI0Detect.exe

09:58:16.0262 5540 UI0Detect - ok

09:58:16.0313 5540 [44E8048ACE47BEFBDC2E9BE4CBC8880] uliagpkx
C:\Windows\system32\DRIVERS\uliagpkx.sys

09:58:16.0315 5540 uliagpkx - ok

09:58:16.0335 5540 [049B3A50B3D646BAEEEE9EEC9B0668DC] umbus
C:\Windows\system32\DRIVERS\umbus.sys

09:58:16.0337 5540 umbus - ok

09:58:16.0356 5540 [7550AD0C6998BA1CB4843E920EE0FEAC] UmPass
C:\Windows\system32\DRIVERS\umpass.sys

09:58:16.0358 5540 UmPass - ok

09:58:16.0385 5540 [8ECACA5454844F66386F7BE4AE0D7CD1] UmRdpService C:\Windows\System32\umrdp.dll

09:58:16.0393 5540 UmRdpService - ok

09:58:16.0435 5540 [833FBB672460EFCE8011D262175FAD33] upnphost C:\Windows\System32\upnphost.dll

09:58:16.0443 5540 upnphost - ok

09:58:16.0496 5540 [6E421CCC57059B0186C6259CA3B6DFC9] USBAAPL
C:\Windows\system32\Drivers\usbaapl.sys

09:58:16.0497 5540 USBAAPL - ok

09:58:16.0535 5540 [8455C4ED038EFD09E99327F9D2D48FFA] usbccgp
C:\Windows\system32\DRIVERS\usbccgp.sys

09:58:16.0537 5540 usbccgp - ok

09:58:16.0567 5540 [04EC7CEC62EC3B6D9354EEE93327FC82] usbcir
C:\Windows\system32\DRIVERS\usbcir.sys

09:58:16.0568 5540 usbcir - ok

09:58:16.0584 5540 [1C333BFD60F2FED2C7AD5DAF533CB742] usbehci
C:\Windows\system32\DRIVERS\usbehci.sys

09:58:16.0586 5540 usbehci - ok

09:58:16.0622 5540 [EE6EF93CCFA94FAE8C6AB298273D8AE2] usbhub
C:\Windows\system32\DRIVERS\usbhub.sys

09:58:16.0625 5540 usbhub - ok

09:58:16.0644 5540 [A6FB7957EA7AFB1165991E54CE934B74] usbohci
C:\Windows\system32\DRIVERS\usbohci.sys

09:58:16.0646 5540 usbohci - ok

09:58:16.0684 5540 [797D862FE0875E75C7CC4C1AD7B30252] usbprint
C:\Windows\system32\DRIVERS\usbprint.sys

09:58:16.0685 5540 usbprint - ok

09:58:16.0713 5540 [576096CCBC07E7C4EA4F5E6686D6888F] usbscan
C:\Windows\system32\DRIVERS\usbscan.sys

09:58:16.0715 5540 usbscan - ok

09:58:16.0731 5540 [D8889D56E0D27E57ED4591837FE71D27] USBSTOR
C:\Windows\system32\DRIVERS\USBSTOR.SYS

09:58:16.0733 5540 USBSTOR - ok

09:58:16.0749 5540 [78780C3EBCE17405B1CCD07A3A8A7D72] usbhci
C:\Windows\system32\DRIVERS\usbuhci.sys

09:58:16.0750 5540 usbhci - ok

09:58:16.0794 5540 [F642A7E4BF78CFA359CCA0A3557C28D7] usbvideo
C:\Windows\system32\Drivers\usbvideo.sys

09:58:16.0796 5540 usbvideo - ok

09:58:16.0821 5540 [081E6E1C91AEC36758902A9F727CD23C] UxSms C:\Windows\System32\uxsms.dll

09:58:16.0828 5540 UxSms - ok

09:58:16.0845 5540 [F42309C4191C506B71DB5D1126D26318] VaultSvc C:\Windows\system32\lsass.exe

09:58:16.0849 5540 VaultSvc - ok

09:58:16.0871 5540 [A059C4C3EDB09E07D21A8E5C0AABD3CB] vdrvroot
C:\Windows\system32\DRIVERS\vdrvroot.sys

09:58:16.0873 5540 vdrvroot - ok

09:58:16.0909 5540 [8C4E7C49D3641BC9E299E466A7F8867D] vds C:\Windows\System32\vds.exe

09:58:16.0919 5540 vds - ok

09:58:16.0950 5540 [17C408214EA61696CEC9C66E388B14F3] vga
C:\Windows\system32\DRIVERS\vgapnp.sys

09:58:16.0952 5540 vga - ok

09:58:16.0968 5540 [8E38096AD5C8570A6F1570A61E251561] VgaSave C:\Windows\System32\drivers\vga.sys

09:58:16.0969 5540 VgaSave - ok

09:58:16.0979 5540 [3BE6E1F3A4F1AFEC8CEE0D7883F93583] vhdmp
C:\Windows\system32\DRIVERS\vhdmp.sys

09:58:16.0982 5540 vhdmp - ok

09:58:16.0997 5540 [C829317A37B4BEA8F39735D4B076E923] viaagp
C:\Windows\system32\DRIVERS\viaagp.sys

09:58:16.0999 5540 viaagp - ok

09:58:17.0011 5540 [E02F079A6AA107F06B16549C6E5C7B74] ViaC7
C:\Windows\system32\DRIVERS\viac7.sys

09:58:17.0013 5540 ViaC7 - ok

09:58:17.0031 5540 [E43574F6A56A0EE11809B48C09E4FD3C] viaide
C:\Windows\system32\DRIVERS\viaide.sys

09:58:17.0032 5540 viaide - ok

09:58:17.0052 5540 [379B349F65F453D2A6E75EA6B7448E49] vmbus
C:\Windows\system32\DRIVERS\vmbus.sys

09:58:17.0056 5540 vmbus - ok

09:58:17.0066 5540 [EC2BBAB4B84D0738C6C83D2234DC36FE] VMBusHID
C:\Windows\system32\DRIVERS\VMBusHID.sys

09:58:17.0068 5540 VMBusHID - ok

09:58:17.0092 5540 [384E5A2AA49934295171E499F86BA6F3] volmgr
C:\Windows\system32\DRIVERS\volmgr.sys

09:58:17.0094 5540 volmgr - ok

09:58:17.0118 5540 [B5BB72067DDDBBFB04B2F89FF8C3C87] volmgrx
C:\Windows\system32\drivers\volmgrx.sys

09:58:17.0123 5540 volmgrx - ok

09:58:17.0162 5540 [58DF9D2481A56EDDE167E51B334D44FD] volsnap
C:\Windows\system32\DRIVERS\volsnap.sys

09:58:17.0166 5540 volsnap - ok

09:58:17.0199 5540 [9DFA0CC2F8855A04816729651175B631] vsmraid
C:\Windows\system32\DRIVERS\vsmraid.sys

09:58:17.0202 5540 vsmraid - ok

09:58:17.0249 5540 [7EA2BCD94D9CFAF4C556F5CC94532A6C] VSS C:\Windows\system32\vssvc.exe

09:58:17.0263 5540 VSS - ok

09:58:17.0281 5540 [90567B1E658001E79D7C8BBD3DDE5AA6] vwifibus
C:\Windows\system32\DRIVERS\vwifibus.sys

09:58:17.0283 5540 vwifibus - ok

09:58:17.0311 5540 [7090D3436EEB4E7DA3373090A23448F7] vwififlt
C:\Windows\system32\DRIVERS\vwififlt.sys

09:58:17.0313 5540 vwififlt - ok

09:58:17.0342 5540 [55187FD710E27D5095D10A472C8BAF1C] W32Time C:\Windows\system32\w32time.dll

09:58:17.0352 5540 W32Time - ok

09:58:17.0381 5540 [DE3721E89C653AA281428C8A69745D90] WacomPen
C:\Windows\system32\DRIVERS\wacompen.sys

09:58:17.0383 5540 WacomPen - ok

09:58:17.0407 5540 [692A712062146E96D28BA0B7D75DE31B] WANARP
C:\Windows\system32\DRIVERS\wanarp.sys

09:58:17.0409 5540 WANARP - ok

09:58:17.0417 5540 [692A712062146E96D28BA0B7D75DE31B] Wanarpv6
C:\Windows\system32\DRIVERS\wanarp.sys

09:58:17.0419 5540 Wanarpv6 - ok

09:58:17.0477 5540 [7790B77FE1E5EE47DCC66247095BB4C9] wbengine C:\Windows\system32\wbengine.exe

09:58:17.0493 5540 wbengine - ok

09:58:17.0513 5540 [9614B5D29DC76AC3C29F6D2D3AA70E67] WbioSrv C:\Windows\System32\wbiosrv.dll

09:58:17.0523 5540 WbioSrv - ok

09:58:17.0553 5540 [D0F88AA11EE1A62BCC6D6A8A7783CA11] wcnscvc C:\Windows\System32\wcnscvc.dll

09:58:17.0562 5540 wcnscvc - ok

09:58:17.0604 5540 [5D930B6357A6D2AF4D7653BDABBF352F] WcsPlugInService
C:\Windows\System32\WcsPlugInService.dll

09:58:17.0612 5540 WcsPlugInService - ok

09:58:17.0642 5540 [1112A9BADACB47B7C0BB0392E3158DFF] Wd C:\Windows\system32\DRIVERS\wd.sys

09:58:17.0644 5540 Wd - ok

09:58:17.0674 5540 [9950E3D0F08141C7E89E64456AE7DC73] Wdf01000
C:\Windows\system32\drivers\Wdf01000.sys

09:58:17.0679 5540 Wdf01000 - ok

09:58:17.0699 5540 [46EF9DC96265FD0B423DB72E7C38C2A5] WdiServiceHost C:\Windows\system32\wdi.dll

09:58:17.0706 5540 WdiServiceHost - ok

09:58:17.0719 5540 [46EF9DC96265FD0B423DB72E7C38C2A5] WdiSystemHost C:\Windows\system32\wdi.dll

09:58:17.0728 5540 WdiSystemHost - ok

09:58:17.0764 5540 [D87C7D2C517F82A5AB7A73E203063D9E] WebClient C:\Windows\System32\webclnt.dll

09:58:17.0773 5540 WebClient - ok

09:58:17.0809 5540 [760F0AFE937A77CFF27153206534F275] Wecsvc C:\Windows\system32\wecsvc.dll

09:58:17.0818 5540 Wecsvc - ok

09:58:17.0849 5540 [AC804569BB2364FB6017370258A4091B] wercplsupport
C:\Windows\System32\wercplsupport.dll

09:58:17.0856 5540 wercplsupport - ok

09:58:17.0890 5540 [08E420D873E4FD85241EE2421B02C4A4] WerSvc C:\Windows\System32\WerSvc.dll

09:58:17.0901 5540 WerSvc - ok

09:58:17.0915 5540 [8B9A943F3B53861F2BFAF6C186168F79] WfpLwf
C:\Windows\system32\DRIVERS\wfplwf.sys

09:58:17.0917 5540 WfpLwf - ok

09:58:17.0950 5540 [5CF95B35E59E2A38023836FFF31BE64C] WIMMount
C:\Windows\system32\drivers\wimmount.sys

09:58:17.0952 5540 WIMMount - ok

09:58:18.0018 5540 [3FAE8F94296001C32EAB62CD7D82E0FD] WinDefend C:\Program Files\Windows
Defender\mpsvc.dll

09:58:18.0030 5540 WinDefend - ok

09:58:18.0040 5540 WinHttpAutoProxySvc - ok

09:58:18.0095 5540 [F62E510B6AD4C21EB9FE8668ED251826] Winmgmt
C:\Windows\system32\wbem\WMIsvc.dll

09:58:18.0099 5540 Winmgmt - ok

09:58:18.0164 5540 [C4F5D3901D1B41D602DDC196E0B95B51] WinRM C:\Windows\system32\WsmSvc.dll

09:58:18.0180 5540 WinRM - ok

09:58:18.0228 5540 [30FC6E5448D0CBAAA95280EEEF7FEDAE] WinUsb
C:\Windows\system32\DRIVERS\WinUsb.sys

09:58:18.0229 5540 WinUsb - ok

09:58:18.0285 5540 [16935C98FF639D185086A3529B1F2067] Wlansvc C:\Windows\System32\wlansvc.dll

09:58:18.0298 5540 Wlansvc - ok

09:58:18.0324 5540 [0217679B8FCA58714C3BF2726D2CA84E] WmiAcpi
C:\Windows\system32\DRIVERS\wmiaapi.sys

09:58:18.0326 5540 WmiAcpi - ok

09:58:18.0359 5540 [6EB6B66517B048D87DC1856DDF1F4C3F] wmiApSrv
C:\Windows\system32\wbem\WmiApSrv.exe

09:58:18.0361 5540 wmiApSrv - ok

09:58:18.0450 5540 [77FBD400984CF72BA0FC4B3489D65F74] WMPNetworkSvc C:\Program Files\Windows
Media Player\wmpnetwk.exe

09:58:18.0467 5540 WMPNetworkSvc - ok

09:58:18.0498 5540 [A2F0EC770A92F2B3F9DE6D518E11409C] WPCSvc C:\Windows\System32\wpcsvc.dll

09:58:18.0506 5540 WPCSvc - ok

09:58:18.0522 5540 [B7F658A2EBC07129538AD9AB35212637] WPDBusEnum
C:\Windows\system32\wpdbusenum.dll

09:58:18.0531 5540 WPDBusEnum - ok

09:58:18.0551 5540 [6DB3276587B853BF886B69528FDB048C] ws2ifsl
C:\Windows\system32\drivers\ws2ifsl.sys

09:58:18.0552 5540 ws2ifsl - ok

09:58:18.0573 5540 [6F5D49EFE0E7164E03AE773A3FE25340] wscsvc C:\Windows\System32\wscsvc.dll

09:58:18.0580 5540 wscsvc - ok

09:58:18.0588 5540 WSearch - ok

09:58:18.0661 5540 [A33408CC036F9C08142B11BE5E93F0A1] wuauserv C:\Windows\system32\wuaueng.dll

09:58:18.0682 5540 wuauserv - ok

09:58:18.0712 5540 [6F9B6C0C93232CFF47D0F72D6DB1D21E] WudfPf
C:\Windows\system32\drivers\WudfPf.sys

09:58:18.0715 5540 WudfPf - ok

09:58:18.0757 5540 [F91FF1E51FCA30B3C3981DB7D5924252] WUDFRd
C:\Windows\system32\DRIVERS\WUDFRd.sys

09:58:18.0759 5540 WUDFRd - ok

09:58:18.0794 5540 [DDEE3682FE97037C45F4D7AB467CB8B6] wudfsvc C:\Windows\System32\WUDFSvc.dll

09:58:18.0802 5540 wudfsvc - ok

09:58:18.0822 5540 [FF2D745B560F7C71B31F30F4D49F73D2] WwanSvc C:\Windows\System32\wwansvc.dll

09:58:18.0831 5540 WwanSvc - ok

09:58:18.0872 5540 ===== Scan global =====

09:58:18.0912 5540 [9A595DF601070DA78C40481120DD2C06] C:\Windows\system32\basesrv.dll

09:58:18.0941 5540 [827E4F75901CA3F990B1487D3301841E] C:\Windows\system32\winsrv.dll

09:58:18.0957 5540 [827E4F75901CA3F990B1487D3301841E] C:\Windows\system32\winsrv.dll

09:58:18.0986 5540 [364455805E64882844EE9ACB72522830] C:\Windows\system32\sxssrv.dll

09:58:19.0006 5540 [5F1B6A9C35D3D5CA72D6D6FDEF9747D6] C:\Windows\system32\services.exe

09:58:19.0014 5540 [Global] - ok

09:58:19.0015 5540 ===== Scan MBR =====

09:58:19.0025 5540 [A3095E5B8060D0D6B97E87EC1BB50C3C] \Device\Harddisk0\DR0

09:58:19.0115 5540 \Device\Harddisk0\DR0 - ok

09:58:19.0120 5540 ===== Scan VBR =====

09:58:19.0125 5540 [B9EB424879F862772B4E9EC1E35E02A4] \Device\Harddisk0\DR0\Partition1

09:58:19.0127 5540 \Device\Harddisk0\DR0\Partition1 - ok

09:58:19.0141 5540 [446378B598BE7135D4F0424B2087C738] \Device\Harddisk0\DR0\Partition2

09:58:19.0143 5540 \Device\Harddisk0\DR0\Partition2 - ok

09:58:19.0168 5540 [CE36AE7FA02C7A5BBE6124818331320B] \Device\Harddisk0\DR0\Partition3

09:58:19.0170 5540 \Device\Harddisk0\DR0\Partition3 - ok

09:58:19.0170 5540 =====

09:58:19.0170 5540 Scan finished

09:58:19.0170 5540 =====

09:58:19.0190 1916 Detected object count: 1

09:58:19.0190 1916 Actual detected object count: 1

09:58:31.0750 1916 sptd (LockedFile.Multi.Generic) - skipped by user

09:58:31.0750 1916 sptd (LockedFile.Multi.Generic) - User select action: Skip

09:58:36.0410 4508 =====

09:58:36.0410 4508 Scan started

09:58:36.0410 4508 Mode: Manual;

09:58:36.0410 4508 =====

09:58:36.0787 4508 ===== Scan system memory =====

09:58:36.0787 4508 System memory - ok

09:58:36.0788 4508 ===== Scan services =====

09:58:36.0947 4508 [6D2ACA41739BFE8CB86EE8E85F29697D] 1394ohci
C:\Windows\system32\DRIVERS\1394ohci.sys

09:58:36.0949 4508 1394ohci - ok

09:58:36.0976 4508 [F0E07D144C8685B8774BC32FC8DA4DF0] ACPI
C:\Windows\system32\DRIVERS\ACPI.sys

09:58:36.0978 4508 ACPI - ok

09:58:36.0992 4508 [98D81CA942D19F7D9153B095162AC013] AcpiPmi
C:\Windows\system32\DRIVERS\acpipmi.sys

09:58:36.0993 4508 AcpiPmi - ok

09:58:37.0072 4508 [3927397AC60D943DAF8808AFFED582B7] AdobeARMservice C:\Program Files\Common Files\Adobe\ARM\1.0\armsvc.exe

09:58:37.0073 4508 AdobeARMservice - ok

09:58:37.0142 4508 [479901C99FA62D1C3261B7ACB1228DAD] AdobeFlashPlayerUpdateSvc
C:\Windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe

09:58:37.0145 4508 AdobeFlashPlayerUpdateSvc - ok

09:58:37.0178 4508 [21E785EBD7DC90A06391141AAC7892FB] adp94xx
C:\Windows\system32\DRIVERS\adp94xx.sys

09:58:37.0181 4508 adp94xx - ok

09:58:37.0226 4508 [0C676BC278D5B59FF5ABD57BBE9123F2] adpahci
C:\Windows\system32\DRIVERS\adpahci.sys

09:58:37.0229 4508 adpahci - ok

09:58:37.0249 4508 [7C7B5EE4B7B822EC85321FE23A27DB33] adpu320
C:\Windows\system32\DRIVERS\adpu320.sys

09:58:37.0251 4508 adpu320 - ok

09:58:37.0287 4508 [8B5EEFEEC1E6D1A72A06C526628AD161] AeLookupSvc C:\Windows\System32\aelupsvc.dll

09:58:37.0289 4508 AeLookupSvc - ok

09:58:37.0315 4508 [DDC040FDB01EF1712A6B13E52AFB104C] AFD C:\Windows\system32\drivers\afd.sys

09:58:37.0318 4508 AFD - ok

09:58:37.0376 4508 [7E10E3BB9B258AD8A9300F91214D67B9] AgereSoftModem
C:\Windows\system32\DRIVERS\AGRSM.sys

09:58:37.0384 4508 AgereSoftModem - ok

09:58:37.0418 4508 [507812C3054C21CEF746B6EE3D04DD6E] agp440
C:\Windows\system32\DRIVERS\agp440.sys

09:58:37.0420 4508 agp440 - ok

09:58:37.0446 4508 [8B30250D573A8F6B4BD23195160D8707] aic78xx
C:\Windows\system32\DRIVERS\djsvs.sys

09:58:37.0447 4508 aic78xx - ok

09:58:37.0488 4508 [18A54E132947CD98FEA9ACCC57F98F13] ALG C:\Windows\System32\alg.exe

09:58:37.0489 4508 ALG - ok

09:58:37.0511 4508 [0D40BCF52EA90FC7DF2AEAB6503DEA44] aliide
C:\Windows\system32\DRIVERS\aliide.sys

09:58:37.0512 4508 aliide - ok

09:58:37.0527 4508 [3C6600A0696E90A463771C7422E23AB5] amdagp
C:\Windows\system32\DRIVERS\amdagp.sys

09:58:37.0528 4508 amdagp - ok

09:58:37.0548 4508 [CD5914170297126B6266860198D1D4F0] amdide
C:\Windows\system32\DRIVERS\amdide.sys

09:58:37.0549 4508 amdide - ok

09:58:37.0557 4508 [00DDA200D71BAC534BF56A9DB5DFD666] AmdK8
C:\Windows\system32\DRIVERS\amd8k.sys

09:58:37.0559 4508 AmdK8 - ok

09:58:37.0567 4508 [3CBF30F5370FDA40DD3E87DF38EA53B6] AmdPPM
C:\Windows\system32\DRIVERS\amdppm.sys

09:58:37.0569 4508 AmdPPM - ok

09:58:37.0593 4508 [2101A86C25C154F8314B24EF49D7FBC2] amdsata
C:\Windows\system32\DRIVERS\amdsata.sys

09:58:37.0594 4508 amdsata - ok

09:58:37.0608 4508 [EA43AF0C423FF267355F74E7A53BDABA] amdsbs
C:\Windows\system32\DRIVERS\amdsbs.sys

09:58:37.0610 4508 amdsbs - ok

09:58:37.0641 4508 [B81C2B5616F6420A9941EA093A92B150] amdxxata
C:\Windows\system32\DRIVERS\amdxxata.sys

09:58:37.0642 4508 amdxxata - ok

09:58:37.0664 4508 [FEB834C02CE1E84B6A38F953CA067706] AppID
C:\Windows\system32\drivers\appid.sys

09:58:37.0665 4508 AppID - ok

09:58:37.0690 4508 [62A9C86CB6085E20DB4823E4E97826F5] AppIDSvc C:\Windows\System32\appidsvc.dll

09:58:37.0691 4508 AppIDSvc - ok

09:58:37.0707 4508 [7DEAD9E3F65DCB2794F2711003BBF650] Appinfo C:\Windows\System32\appinfo.dll

09:58:37.0708 4508 Appinfo - ok

09:58:37.0749 4508 [4FE5C6D40664AE07BE5105874357D2ED] Apple Mobile Device C:\Program Files\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe

09:58:37.0751 4508 Apple Mobile Device - ok

09:58:37.0767 4508 [A45D184DF6A8803DA13A0B329517A64A] AppMgmt
C:\Windows\System32\appmgmts.dll

09:58:37.0769 4508 AppMgmt - ok

09:58:37.0799 4508 [2932004F49677BD84DBC72EDB754FFB3] arc C:\Windows\system32\DRIVERS\arc.sys

09:58:37.0800 4508 arc - ok

09:58:37.0809 4508 [5D6F36C46FD283AE1B57BD2E9FEB0BC7] arcsas
C:\Windows\system32\DRIVERS\arcsas.sys

09:58:37.0811 4508 arcsas - ok

09:58:37.0838 4508 [CCDA8D84FD02AEC52E62F296433AE9DC] aswFsBlk
C:\Windows\system32\drivers\aswFsBlk.sys

09:58:37.0839 4508 aswFsBlk - ok

09:58:37.0847 4508 [A6E20E62871A28A0F1C05B1681848FA7] aswMonFlt
C:\Windows\system32\drivers\aswMonFlt.sys

09:58:37.0849 4508 aswMonFlt - ok

09:58:37.0870 4508 [6844738D52970A0F482768EEA941C78E] aswRdr
C:\Windows\System32\Drivers\aswrdr2.sys

09:58:37.0872 4508 aswRdr - ok

09:58:37.0895 4508 [657A61979F40D67CA29716149766FFA7] aswRvrt
C:\Windows\system32\drivers\aswRvrt.sys

09:58:37.0896 4508 aswRvrt - ok

09:58:37.0934 4508 [0E604867FC28F00D91CB0B00D2EC830D] aswSnx
C:\Windows\system32\drivers\aswSnx.sys

09:58:37.0940 4508 aswSnx - ok

09:58:37.0979 4508 [6FC4AA106AA505394C908D37CCCB9148] aswSP
C:\Windows\system32\drivers\aswSP.sys

09:58:37.0983 4508 aswSP - ok

09:58:38.0024 4508 [33E21FFB063CA6C7E00D568467DC72E4] aswTdi
C:\Windows\system32\drivers\aswTdi.sys

09:58:38.0026 4508 aswTdi - ok

09:58:38.0047 4508 [EDB0C9BA44B748E420CCA989FD8B826E] aswVmm
C:\Windows\system32\drivers\aswVmm.sys

09:58:38.0049 4508 aswVmm - ok

09:58:38.0071 4508 [ADD2ADE1C2B285AB8378D2DAAF991481] AsyncMac
C:\Windows\system32\DRIVERS\asyncmac.sys

09:58:38.0072 4508 AsyncMac - ok

09:58:38.0097 4508 [338C86357871C167A96AB976519BF59E] atapi
C:\Windows\system32\DRIVERS\atapi.sys

09:58:38.0098 4508 atapi - ok

09:58:38.0175 4508 [10A82E63B50672987B6B09B215213CC4] athr C:\Windows\system32\DRIVERS\athr.sys
09:58:38.0193 4508 athr - ok
09:58:38.0242 4508 [510C873BFA135AA829F4180352772734] AudioEndpointBuilder
C:\Windows\System32\Audiosrv.dll
09:58:38.0246 4508 AudioEndpointBuilder - ok
09:58:38.0260 4508 [510C873BFA135AA829F4180352772734] Audiosrv C:\Windows\System32\Audiosrv.dll
09:58:38.0265 4508 Audiosrv - ok
09:58:38.0326 4508 [41735B82DB57E4EBE9504EC400FD120E] avast! Antivirus C:\Program Files\AVAST
Software\Avast\AvastSvc.exe
09:58:38.0328 4508 avast! Antivirus - ok
09:58:38.0355 4508 [DD6A431B43E34B91A767D1CE33728175] AxInstSV C:\Windows\System32\AxInstSV.dll
09:58:38.0357 4508 AxInstSV - ok
09:58:38.0394 4508 [1A231ABEC60FD316EC54C66715543CEC] b06bdrv
C:\Windows\system32\DRIVERS\bxbvdx.sys
09:58:38.0398 4508 b06bdrv - ok
09:58:38.0433 4508 [744663C3183CE5A11308F20C7B90C63E] b57nd60x
C:\Windows\system32\DRIVERS\b57nd60x.sys
09:58:38.0437 4508 b57nd60x - ok
09:58:38.0465 4508 [EE1E9C3BB8228AE423DD38DB69128E71] BDESVC C:\Windows\System32\bdesvc.dll
09:58:38.0467 4508 BDESVC - ok
09:58:38.0486 4508 [505506526A9D467307B3C393DEDAF858] Beep
C:\Windows\system32\drivers\Beep.sys
09:58:38.0488 4508 Beep - ok
09:58:38.0588 4508 [85AC71C045CEB054ED48A7841AAE0C11] BFE C:\Windows\System32\bfe.dll
09:58:38.0593 4508 BFE - ok
09:58:38.0678 4508 [53F476476F55A27F580661BDE09C4EC4] BITS C:\Windows\System32\qmgr.dll
09:58:38.0689 4508 BITS - ok
09:58:38.0709 4508 [2287078ED48FCFC477B05B20CF38F36F] blbdrive
C:\Windows\system32\DRIVERS\blbdrive.sys
09:58:38.0710 4508 blbdrive - ok
09:58:38.0746 4508 [DB5BEA73EDAF19AC68B2C0FAD0F92B1A] Bonjour Service C:\Program
Files\Bonjour\mDNSResponder.exe
09:58:38.0749 4508 Bonjour Service - ok

09:58:38.0772 4508 [FCAFAEF6798D7B51FF029F99A9898961] browser
C:\Windows\system32\DRIVERS\browser.sys

09:58:38.0773 4508 browser - ok

09:58:38.0789 4508 [9F9ACC7F7CCDE8A15C282D3F88B43309] BrFiltLo
C:\Windows\system32\DRIVERS\BrFiltLo.sys

09:58:38.0790 4508 BrFiltLo - ok

09:58:38.0797 4508 [56801AD62213A41F6497F96DEE83755A] BrFiltUp
C:\Windows\system32\DRIVERS\BrFiltUp.sys

09:58:38.0798 4508 BrFiltUp - ok

09:58:38.0827 4508 [598E1280E7FF3744F4B8329366CC5635] Browser C:\Windows\System32\browser.dll

09:58:38.0829 4508 Browser - ok

09:58:38.0853 4508 [845B8CE732E67F3B4133164868C666EA] Brserid
C:\Windows\System32\Drivers\Brserid.sys

09:58:38.0856 4508 Brserid - ok

09:58:38.0876 4508 [203F0B1E73ADADBBB7B7B1FABD901F6B] BrSerWdm
C:\Windows\System32\Drivers\BrSerWdm.sys

09:58:38.0877 4508 BrSerWdm - ok

09:58:38.0885 4508 [BD456606156BA17E60A04E18016AE54B] BrUsbMdm
C:\Windows\System32\Drivers\BrUsbMdm.sys

09:58:38.0886 4508 BrUsbMdm - ok

09:58:38.0895 4508 [AF72ED54503F717A43268B3CC5FAEC2E] BrUsbSer
C:\Windows\System32\Drivers\BrUsbSer.sys

09:58:38.0897 4508 BrUsbSer - ok

09:58:38.0905 4508 [ED3DF7C56CE0084EB2034432FC56565A] BTHMODEM
C:\Windows\system32\DRIVERS\bthmodem.sys

09:58:38.0907 4508 BTHMODEM - ok

09:58:38.0932 4508 [1DF19C96EEF6C29D1C3E1A8678E07190] bthserv C:\Windows\system32\bthserv.dll

09:58:38.0934 4508 bthserv - ok

09:58:38.0952 4508 [77EA11B065E0A8AB902D78145CA51E10] cdfs C:\Windows\system32\DRIVERS\cdfs.sys

09:58:38.0954 4508 cdfs - ok

09:58:38.0987 4508 [BA6E70AA0E6091BC39DE29477D866A77] cdrom
C:\Windows\system32\DRIVERS\cdrom.sys

09:58:38.0988 4508 cdrom - ok

09:58:39.0024 4508 [628A9E30EC5E18DD5DE6BE4DBDC12198] CertPropSvc C:\Windows\System32\certprop.dll

09:58:39.0026 4508 CertPropSvc - ok

09:58:39.0045 4508 [3FE3FE94A34DF6FB06E6418D0F6A0060] circlass
C:\Windows\system32\DRIVERS\circlass.sys

09:58:39.0046 4508 circlass - ok

09:58:39.0074 4508 [635181E0E9BBF16871BF5380D71DB02D] CLFS C:\Windows\system32\CLFS.sys

09:58:39.0077 4508 CLFS - ok

09:58:39.0134 4508 [D88040F816FDA31C3B466F0FA0918F29] clr_optimization_v2.0.50727_32
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe

09:58:39.0136 4508 clr_optimization_v2.0.50727_32 - ok

09:58:39.0151 4508 [DEA805815E587DAD1DD2C502220B5616] CmBatt
C:\Windows\system32\DRIVERS\CmBatt.sys

09:58:39.0152 4508 CmBatt - ok

09:58:39.0182 4508 [C537B1DB64D495B9B4717B4D6D9EDBF2] cmdide
C:\Windows\system32\DRIVERS\cmdide.sys

09:58:39.0183 4508 cmdide - ok

09:58:39.0210 4508 [1B675691ED940766149C93E8F4488D68] CNG C:\Windows\system32\Drivers\cng.sys

09:58:39.0214 4508 CNG - ok

09:58:39.0229 4508 [A6023D3823C37043986713F118A89BEE] Compbatt
C:\Windows\system32\DRIVERS\compbatt.sys

09:58:39.0230 4508 Compbatt - ok

09:58:39.0247 4508 [F1724BA27E97D627F808FB0BA77A28A6] CompositeBus
C:\Windows\system32\DRIVERS\CompositeBus.sys

09:58:39.0248 4508 CompositeBus - ok

09:58:39.0255 4508 COMSysApp - ok

09:58:39.0277 4508 [2C4EBCFC84A9B44F209DFF6C6E6C61D1] crcdisk
C:\Windows\system32\DRIVERS\crcdisk.sys

09:58:39.0278 4508 crcdisk - ok

09:58:39.0317 4508 [9C231178CE4FB385F4B54B0A9080B8A4] CryptSvc C:\Windows\system32\cryptsvc.dll

09:58:39.0319 4508 CryptSvc - ok

09:58:39.0348 4508 [27C9490BDD0AE48911AB8CF1932591ED] CSC C:\Windows\system32\drivers\csc.sys

09:58:39.0352 4508 CSC - ok

09:58:39.0382 4508 [56FB5F222EA30D3D3FC459879772CB73] CscService C:\Windows\System32\cscsvc.dll

09:58:39.0388 4508 CscService - ok

09:58:39.0430 4508 [B82CD39E336973359D7C9BF911E8E84F] DcomLaunch C:\Windows\system32\rpcss.dll

09:58:39.0438 4508 DcomLaunch - ok

09:58:39.0483 4508 [8D6E10A2D9A5EED59562D9B82CF804E1] defragsvc C:\Windows\System32\defragsvc.dll

09:58:39.0486 4508 defragsvc - ok

09:58:39.0518 4508 [8E09E52EE2E3CEB199EF3DD99CF9E3FB] DfsC C:\Windows\system32\Drivers\dfsc.sys

09:58:39.0519 4508 DfsC - ok

09:58:39.0555 4508 [7BEF2E2159EDB03105BC7A8BABE04726] dg_ssudbus
C:\Windows\system32\DRIVERS\ssudbus.sys

09:58:39.0557 4508 dg_ssudbus - ok

09:58:39.0581 4508 [C56495FBD770712367CAD35E5DE72DA6] Dhcp C:\Windows\system32\dhcpcore.dll

09:58:39.0585 4508 Dhcp - ok

09:58:39.0600 4508 [1A050B0274BFB3890703D490F330C0DA] discache
C:\Windows\system32\drivers\discache.sys

09:58:39.0602 4508 discache - ok

09:58:39.0617 4508 [565003F326F99802E68CA78F2A68E9FF] Disk C:\Windows\system32\DRIVERS\disk.sys

09:58:39.0618 4508 Disk - ok

09:58:39.0650 4508 [D0722E963D3C6145446874241401B209] Dnscache C:\Windows\System32\dnsrslvr.dll

09:58:39.0653 4508 Dnscache - ok

09:58:39.0680 4508 [4408C85C21EEA48EB0CE486BAEEF0502] dot3svc C:\Windows\System32\dot3svc.dll

09:58:39.0685 4508 dot3svc - ok

09:58:39.0717 4508 [B5E479EB83707DD698F66953E922042C] Dot4
C:\Windows\system32\DRIVERS\Dot4.sys

09:58:39.0719 4508 Dot4 - ok

09:58:39.0747 4508 [C25FEA07A8E7767E8B89AB96A3B96519] Dot4Print
C:\Windows\system32\DRIVERS\Dot4Prt.sys

09:58:39.0748 4508 Dot4Print - ok

09:58:39.0770 4508 [CF491FF38D62143203C065260567E2F7] dot4usb
C:\Windows\system32\DRIVERS\dot4usb.sys

09:58:39.0772 4508 dot4usb - ok

09:58:39.0796 4508 [7FA81C6E11CAA594ADB52084DA73A1E5] DPS C:\Windows\system32\dps.dll

09:58:39.0800 4508 DPS - ok

09:58:39.0829 4508 [B918E7C5F9BF77202F89E1A9539F2EB4] drmkaud
C:\Windows\system32\drivers\drmkaud.sys

09:58:39.0830 4508 drmkau - ok

09:58:39.0858 4508 [687AF6BB383885FF6A64071B189A7F3E] dtsoftbus01
C:\Windows\system32\DRIVERS\dtsoftbus01.sys

09:58:39.0860 4508 dtsoftbus01 - ok

09:58:39.0905 4508 [39806CFEDDCC55E686A49BCCD2972F23] DXGKrn
C:\Windows\System32\drivers\dxgkrnl.sys

09:58:39.0911 4508 DXGKrn - ok

09:58:39.0938 4508 [8600142FA91C1B96367D3300AD0F3F3A] EapHost C:\Windows\System32\eapsvc.dll

09:58:39.0941 4508 EapHost - ok

09:58:40.0197 4508 [024E1B5CAC09731E4D868E64DBFB4AB0] ebdrv
C:\Windows\system32\DRIVERS\evbdx.sys

09:58:40.0221 4508 ebdrv - ok

09:58:40.0249 4508 [F42309C4191C506B71DB5D1126D26318] EFS C:\Windows\System32\lsass.exe

09:58:40.0253 4508 EFS - ok

09:58:40.0313 4508 [3A74A6E33685662B125A3269B1F2114F] ehRecvr C:\Windows\ehome\ehRecvr.exe

09:58:40.0318 4508 ehRecvr - ok

09:58:40.0336 4508 [D389BFF34F80CAEDE417BF9D1507996A] ehSched C:\Windows\ehome\ehsched.exe

09:58:40.0337 4508 ehSched - ok

09:58:40.0379 4508 [0ED67910C8C326796FAA00B2BF6D9D3C] elxstor
C:\Windows\system32\DRIVERS\elxstor.sys

09:58:40.0384 4508 elxstor - ok

09:58:40.0406 4508 [8FC3208352DD3912C94367A206AB3F11] ErrDev
C:\Windows\system32\DRIVERS\errdev.sys

09:58:40.0407 4508 ErrDev - ok

09:58:40.0443 4508 [F6916EFC29D9953D5D0DF06882AE8E16] EventSystem C:\Windows\system32\es.dll

09:58:40.0448 4508 EventSystem - ok

09:58:40.0473 4508 [2DC9108D74081149CC8B651D3A26207F] exfat C:\Windows\system32\drivers\exfat.sys

09:58:40.0475 4508 exfat - ok

09:58:40.0496 4508 [7E0AB74553476622FB6AE36F73D97D35] fastfat
C:\Windows\system32\drivers\fastfat.sys

09:58:40.0498 4508 fastfat - ok

09:58:40.0526 4508 [F7EA23CC5E6BF2181F3F399D54F6EFC1] Fax C:\Windows\system32\fxssvc.exe

09:58:40.0532 4508 Fax - ok

09:58:40.0560 4508 [E817A017F82DF2A1F8CFDBDA29388B29] fdc C:\Windows\system32\DRIVERS\fdc.sys
09:58:40.0561 4508 fdc - ok

09:58:40.0589 4508 [F3222C893BD2F5821A0179E5C71E88FB] fdPHost C:\Windows\system32\fdPHost.dll
09:58:40.0591 4508 fdPHost - ok

09:58:40.0610 4508 [7DBE8CBFE79EFBDEB98C9FB08D3A9A5B] FDResPub C:\Windows\system32\fdrespub.dll
09:58:40.0612 4508 FDResPub - ok

09:58:40.0627 4508 [6CF00369C97F3CF563BE99BE983D13D8] FileInfo
C:\Windows\system32\drivers\fileinfo.sys
09:58:40.0628 4508 FileInfo - ok

09:58:40.0650 4508 [42C51DC94C91DA21CB9196EB64C45DB9] Filetrace
C:\Windows\system32\drivers\filetrace.sys
09:58:40.0651 4508 Filetrace - ok

09:58:40.0660 4508 [87907AA70CB3C56600F1C2FB8841579B] flpydisk
C:\Windows\system32\DRIVERS\flpydisk.sys
09:58:40.0661 4508 flpydisk - ok

09:58:40.0688 4508 [7520EC808E0C35E0EE6F841294316653] FltMgr
C:\Windows\system32\drivers\fltmgr.sys
09:58:40.0691 4508 FltMgr - ok

09:58:40.0726 4508 [B6512A85815FDC3D560C3705F5BDB93D] FontCache C:\Windows\system32\FntCache.dll
09:58:40.0735 4508 FontCache - ok

09:58:40.0781 4508 [E56F39F6B7FDA0AC77A79B0FD3DE1A2F] FontCache3.0.0.0
C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe
09:58:40.0782 4508 FontCache3.0.0.0 - ok

09:58:40.0810 4508 [1A16B57943853E598CFF37FE2B8CBF1D] FsDepends
C:\Windows\system32\drivers\FsDepends.sys
09:58:40.0811 4508 FsDepends - ok

09:58:40.0831 4508 [A574B4360E438977038AAE4BF60D79A2] Fs_Rec
C:\Windows\system32\drivers\Fs_Rec.sys
09:58:40.0832 4508 Fs_Rec - ok

09:58:40.0855 4508 [5592F5DBA26282D24D2B080EB438A4D7] fvevol
C:\Windows\system32\DRIVERS\fvevol.sys
09:58:40.0858 4508 fvevol - ok

09:58:40.0873 4508 [65EE0C7A58B65E74AE05637418153938] gagp30kx
C:\Windows\system32\DRIVERS\gagp30kx.sys

09:58:40.0874 4508 gagp30kx - ok

09:58:40.0899 4508 [185ADA973B5020655CEE342059A86CBB] GEARAspiWDM
C:\Windows\system32\DRIVERS\GEARAspiWDM.sys

09:58:40.0900 4508 GEARAspiWDM - ok

09:58:40.0944 4508 [8BA3C04702BF8F927AB36AE8313CA4EE] gpsvc C:\Windows\System32\gpsvc.dll

09:58:40.0952 4508 gpsvc - ok

09:58:40.0989 4508 [506708142BC63DABA64F2D3AD1DCD5BF] gupdate C:\Program
Files\Google\Update\GoogleUpdate.exe

09:58:40.0990 4508 gupdate - ok

09:58:40.0997 4508 [506708142BC63DABA64F2D3AD1DCD5BF] gupdatem C:\Program
Files\Google\Update\GoogleUpdate.exe

09:58:40.0999 4508 gupdatem - ok

09:58:41.0030 4508 [833051C6C6C42117191935F734CFBD97] hamachi
C:\Windows\system32\DRIVERS\hamachi.sys

09:58:41.0031 4508 hamachi - ok

09:58:41.0096 4508 [6D12BDA1715C38BE1746B195B1E4337E] Hamachi2Svc C:\Program Files\LogMeIn
Hamachi\hamachi-2.exe

09:58:41.0108 4508 Hamachi2Svc - ok

09:58:41.0144 4508 [C44E3C2BAB6837DB337DDEE7544736DB] hcw85cir
C:\Windows\system32\drivers\hcw85cir.sys

09:58:41.0145 4508 hcw85cir - ok

09:58:41.0184 4508 [3530CAD25DEBA7DC7DE8BB51632CBC5F] HdAudAddService
C:\Windows\system32\drivers\HdAudio.sys

09:58:41.0188 4508 HdAudAddService - ok

09:58:41.0213 4508 [717A2207FD6F13AD3E664C7D5A43C7BF] HDAudBus
C:\Windows\system32\DRIVERS\HDAudBus.sys

09:58:41.0216 4508 HDAudBus - ok

09:58:41.0225 4508 [1D58A7F3E11A9731D0EAAAA8405ACC36] HidBatt
C:\Windows\system32\DRIVERS\HidBatt.sys

09:58:41.0227 4508 HidBatt - ok

09:58:41.0237 4508 [89448F40E6DF260C206A193A4683BA78] HidBth
C:\Windows\system32\DRIVERS\hidbth.sys

09:58:41.0239 4508 HidBth - ok

09:58:41.0255 4508 [CF50B4CF4A4F229B9F3C08351F99CA5E] HidIr C:\Windows\system32\DRIVERS\hidir.sys

09:58:41.0256 4508 Hidlr - ok

09:58:41.0292 4508 [2BC6F6A1992B3A77F5F41432CA6B3B6B] hidserv C:\Windows\system32\hidserv.dll

09:58:41.0296 4508 hidserv - ok

09:58:41.0317 4508 [25072FB35AC90B25F9E4E3BACF774102] HidUsb
C:\Windows\system32\DRIVERS\hidusb.sys

09:58:41.0318 4508 HidUsb - ok

09:58:41.0350 4508 [741C2A45CA8407E374AABA3E330B7872] hkmsvc C:\Windows\system32\kmsvc.dll

09:58:41.0354 4508 hkmsvc - ok

09:58:41.0378 4508 [A768CA158BB06782A2835B907F4873C3] HomeGroupListener
C:\Windows\system32>ListSvc.dll

09:58:41.0383 4508 HomeGroupListener - ok

09:58:41.0405 4508 [FB08DEC5EF43D0C66D83B8E9694E7549] HomeGroupProvider
C:\Windows\system32\provsvc.dll

09:58:41.0412 4508 HomeGroupProvider - ok

09:58:41.0500 4508 [5DA42D24712E00728CEA2342A65009B2] hpqcx08 C:\Program Files\HP\Digital
Imaging\bin\hpqcx08.dll

09:58:41.0503 4508 hpqcx08 - ok

09:58:41.0528 4508 [D86A39BF100069444D026D22D9A6E555] hpqddsvc C:\Program Files\HP\Digital
Imaging\bin\hpqddsvc.dll

09:58:41.0529 4508 hpqddsvc - ok

09:58:41.0567 4508 [295FDC419039090EB8B49FFDBB374549] HpSAMD
C:\Windows\system32\DRIVERS\HpSAMD.sys

09:58:41.0568 4508 HpSAMD - ok

09:58:41.0588 4508 [950CC1E6AE3A6CD23E0945CDE089B02C] HTCAND32
C:\Windows\system32\Drivers\ANDROIDUSB.sys

09:58:41.0589 4508 HTCAND32 - ok

09:58:41.0623 4508 [5C8BC8A28798FD010E7ABC4E0D588CAA] HTCMonitorService C:\Program Files\HTC Sync
Manager\HSMServiceEntry.exe

09:58:41.0625 4508 HTCMonitorService - ok

09:58:41.0646 4508 [339ADEFAD60353F960E3CA67CE468C24] htcnprot
C:\Windows\system32\DRIVERS\htcnprot.sys

09:58:41.0647 4508 htcnprot - ok

09:58:41.0697 4508 [C531C7FD9E8B62021112787C4E2C5A5A] HTTP
C:\Windows\system32\drivers\HTTP.sys

09:58:41.0702 4508 HTTP - ok

09:58:41.0728 4508 [8305F33CDE89AD6C7A0763ED0B5A8D42] hwpolicy
C:\Windows\system32\drivers\hwpolicy.sys

09:58:41.0730 4508 hwpolicy - ok

09:58:41.0750 4508 [F151F0BDC47F4A28B1B20A0818EA36D6] i8042prt
C:\Windows\system32\DRIVERS\i8042prt.sys

09:58:41.0752 4508 i8042prt - ok

09:58:41.0800 4508 [934AF4D7C5F457B9F0743F4299B77B67] iaStorV
C:\Windows\system32\DRIVERS\iaStorV.sys

09:58:41.0804 4508 iaStorV - ok

09:58:41.0890 4508 [5AF815EB5BC9802E5A064E2BA62BFC0C] idsvc
C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\infocard.exe

09:58:41.0898 4508 idsvc - ok

09:58:42.0121 4508 [9467514EA189475A6E7FDC5D7BDE9D3F] igfx
C:\Windows\system32\DRIVERS\igdkmd32.sys

09:58:42.0157 4508 igfx - ok

09:58:42.0182 4508 [4173FF5708F3236CF25195FECD742915] iirsp C:\Windows\system32\DRIVERS\iirsp.sys

09:58:42.0183 4508 iirsp - ok

09:58:42.0229 4508 [FAC0EE6562B121B1399D6E855583F7A5] IKEEXT C:\Windows\System32\ikeext.dll

09:58:42.0237 4508 IKEEXT - ok

09:58:42.0245 4508 InCDFs - ok

09:58:42.0254 4508 InCDPass - ok

09:58:42.0264 4508 InCDRm - ok

09:58:42.0365 4508 [DCE087456521FA31EEA20223A1937E42] IntcAzAudAddService
C:\Windows\system32\drivers\RTKVHDA.sys

09:58:42.0385 4508 IntcAzAudAddService - ok

09:58:42.0420 4508 [A0F12F2C9BA6C72F3987CE780E77C130] intelide
C:\Windows\system32\DRIVERS\intelide.sys

09:58:42.0421 4508 intelide - ok

09:58:42.0433 4508 [3B514D27BFC4ACCB4037BC6685F766E0] intelppm
C:\Windows\system32\DRIVERS\intelppm.sys

09:58:42.0434 4508 intelppm - ok

09:58:42.0470 4508 [ACB364B9075A45C0736E5C47BE5CAE19] IPBusEnum
C:\Windows\system32\ipbusenum.dll

09:58:42.0473 4508 IPBusEnum - ok

09:58:42.0487 4508 [709D1761D3B19A932FF0238EA6D50200] IpFilterDriver
C:\Windows\system32\DRIVERS\ipfltdrv.sys

09:58:42.0488 4508 IpFilterDriver - ok

09:58:42.0514 4508 [477397B432A256A50EE7E4339EB9EA14] iphlpsvc C:\Windows\System32\iphlpvc.dll

09:58:42.0521 4508 iphlpsvc - ok

09:58:42.0530 4508 [E4454B6C37D7FFD5649611F6496308A7] IPMIDRV
C:\Windows\system32\DRIVERS\IPMIDrv.sys

09:58:42.0532 4508 IPMIDRV - ok

09:58:42.0541 4508 [A5FA468D67ABCDAA36264E463A7BB0CD] IPNAT
C:\Windows\system32\drivers\ipnat.sys

09:58:42.0543 4508 IPNAT - ok

09:58:42.0581 4508 [E46B17060D3962A384AE484094614788] iPod Service C:\Program
Files\iPod\bin\iPodService.exe

09:58:42.0586 4508 iPod Service - ok

09:58:42.0614 4508 [42996CFF20A3084A56017B7902307E9F] IRENUM
C:\Windows\system32\drivers\irenum.sys

09:58:42.0615 4508 IRENUM - ok

09:58:42.0634 4508 [1F32BB6B38F62F7DF1A7AB7292638A35] isapnp
C:\Windows\system32\DRIVERS\isapnp.sys

09:58:42.0635 4508 isapnp - ok

09:58:42.0663 4508 [ED46C223AE46C6866AB77CDC41C404B7] iScsiPrt
C:\Windows\system32\DRIVERS\msiscsi.sys

09:58:42.0666 4508 iScsiPrt - ok

09:58:42.0683 4508 [ADEF52CA1AEAE82B50DF86B56413107E] kbdclass
C:\Windows\system32\DRIVERS\kbdclass.sys

09:58:42.0684 4508 kbdclass - ok

09:58:42.0697 4508 [3D9F0EBF350EDCFD6498057301455964] kbdhid
C:\Windows\system32\DRIVERS\kbdhid.sys

09:58:42.0698 4508 kbdhid - ok

09:58:42.0716 4508 [F42309C4191C506B71DB5D1126D26318] KeyIso C:\Windows\system32\lsass.exe

09:58:42.0720 4508 KeyIso - ok

09:58:42.0741 4508 [E36A061EC11B373826905B21BE10948F] KSecDD
C:\Windows\system32\Drivers\ksecdd.sys

09:58:42.0742 4508 KSecDD - ok

09:58:42.0762 4508 [26C046977E85B95036453D7B88BA1820] KSecPkg
C:\Windows\system32\Drivers\ksecpkg.sys

09:58:42.0764 4508 KSecPkg - ok

09:58:42.0806 4508 [89A7B9CC98D0D80C6F31B91C0A310FCD] KtmRm C:\Windows\system32\msdtckrm.dll

09:58:42.0813 4508 KtmRm - ok

09:58:42.0847 4508 [BCA92CB047A4326925ECEF759DBAA233] LanmanServer C:\Windows\system32\srsvcs.dll

09:58:42.0854 4508 LanmanServer - ok

09:58:42.0883 4508 [B9891F885DCF1F0513A51CB58493CB1F] LanmanWorkstation
C:\Windows\System32\wkssvc.dll

09:58:42.0891 4508 LanmanWorkstation - ok

09:58:42.0918 4508 [5001C2B3557B53DED02ABED3BCC6FD2D] LHidFilt
C:\Windows\system32\DRIVERS\LHidFilt.Sys

09:58:42.0919 4508 LHidFilt - ok

09:58:42.0943 4508 [F7611EC07349979DA9B0AE1F18CCC7A6] lltadio
C:\Windows\system32\DRIVERS\lltdio.sys

09:58:42.0945 4508 lltadio - ok

09:58:42.0978 4508 [5700673E13A2117FA3B9020C852C01E2] lltdsvc C:\Windows\System32\lltdsvc.dll

09:58:42.0983 4508 lltdsvc - ok

09:58:43.0005 4508 [55CA01BA19D0006C8F2639B6C045E08B] lmhosts C:\Windows\System32\lmhsvc.dll

09:58:43.0010 4508 lmhosts - ok

09:58:43.0033 4508 [3AD9369E5D17014971A11728F198994C] LMouFilt
C:\Windows\system32\DRIVERS\LMouFilt.Sys

09:58:43.0034 4508 LMouFilt - ok

09:58:43.0067 4508 [EB119A53CCF2ACC000AC71B065B78FEF] LSI_FC
C:\Windows\system32\DRIVERS\lsi_fc.sys

09:58:43.0069 4508 LSI_FC - ok

09:58:43.0077 4508 [8ADE1C877256A22E49B75D1CC9161F9C] LSI_SAS
C:\Windows\system32\DRIVERS\lsi_sas.sys

09:58:43.0080 4508 LSI_SAS - ok

09:58:43.0089 4508 [DC9DC3D3DAA0E276FD2EC262E38B11E9] LSI_SAS2
C:\Windows\system32\DRIVERS\lsi_sas2.sys

09:58:43.0090 4508 LSI_SAS2 - ok

09:58:43.0099 4508 [0A036C7D7CAB643A7F07135AC47E0524] LSI_SCSI
C:\Windows\system32\DRIVERS\lsi_scsi.sys

09:58:43.0101 4508 LSI_SCSI - ok

09:58:43.0120 4508 [6703E366CC18D3B6E534F5CF7DF39CEE] luafv C:\Windows\system32\drivers\luafv.sys

09:58:43.0122 4508 luafv - ok

09:58:43.0154 4508 [4470E3C1E0C3378E4CAB137893C12C3A] MBAMProtector
C:\Windows\system32\drivers\mbam.sys

09:58:43.0155 4508 MBAMProtector - ok

09:58:43.0192 4508 [65085456FD9A74D7F1A999520C299ECB] MBAMSchedul C:\Program Files\Malwarebytes'
Anti-Malware\mbamscheduler.exe

09:58:43.0195 4508 MBAMSchedul - ok

09:58:43.0227 4508 [E0D7732F2D2E24B2DB3F67B6750295B8] MBAMService C:\Program Files\Malwarebytes'
Anti-Malware\mbamservice.exe

09:58:43.0233 4508 MBAMService - ok

09:58:43.0261 4508 [E2B0887816ED336685954E3D8FDAA51D] Mcx2Svc C:\Windows\system32\Mcx2Svc.dll

09:58:43.0266 4508 Mcx2Svc - ok

09:58:43.0304 4508 [0FFF5B045293002AB38EB1FD1FC2FB74] megasas
C:\Windows\system32\DRIVERS\megasas.sys

09:58:43.0305 4508 megasas - ok

09:58:43.0332 4508 [DCBAB2920C75F390CAF1D29F675D03D6] MegaSR
C:\Windows\system32\DRIVERS\MegaSR.sys

09:58:43.0335 4508 MegaSR - ok

09:58:43.0397 4508 [FAFE367D032ED82E9332B4C741A20216] Microsoft Office Groove Audit Service C:\Program
Files\Microsoft Office\Office12\GrooveAuditService.exe

09:58:43.0398 4508 Microsoft Office Groove Audit Service - ok

09:58:43.0418 4508 [146B6F43A673379A3C670E86D89BE5EA] MMCSS C:\Windows\system32\mmcscs.dll

09:58:43.0422 4508 MMCSS - ok

09:58:43.0434 4508 [F001861E5700EE84E2D4E52C712F4964] Modem
C:\Windows\system32\drivers\modem.sys

09:58:43.0435 4508 Modem - ok

09:58:43.0446 4508 [79D10964DE86B292320E9DFE02282A23] monitor
C:\Windows\system32\DRIVERS\monitor.sys

09:58:43.0448 4508 monitor - ok

09:58:43.0478 4508 [FB18CC1D4C2E716B6B903B0AC0CC0609] mouclass
C:\Windows\system32\DRIVERS\mouclass.sys

09:58:43.0479 4508 mouclass - ok

09:58:43.0493 4508 [2C388D2CD01C9042596CF3C8F3C7B24D] mouhid
C:\Windows\system32\DRIVERS\mouhid.sys

09:58:43.0495 4508 mouhid - ok

09:58:43.0514 4508 [921C18727C5920D6C0300736646931C2] mountmgr
C:\Windows\system32\drivers\mountmgr.sys

09:58:43.0516 4508 mountmgr - ok

09:58:43.0572 4508 [9C3758018DED02F4AE53CCA1C5F084A2] MozillaMaintenance C:\Program Files\Mozilla
Maintenance Service\maintenanceservice.exe

09:58:43.0573 4508 MozillaMaintenance - ok

09:58:43.0589 4508 [2AF5997438C55FB79D33D015C30E1974] mpio
C:\Windows\system32\DRIVERS\mpio.sys

09:58:43.0591 4508 mpio - ok

09:58:43.0613 4508 [AD2723A7B53DD1AACAE6AD8C0BFBF4D0] mpsdrv
C:\Windows\system32\drivers\mpsdrv.sys

09:58:43.0614 4508 mpsdrv - ok

09:58:43.0655 4508 [5CD996CECF45CBC3E8D109C86B82D69E] MpsSvc C:\Windows\system32\mpssvc.dll

09:58:43.0664 4508 MpsSvc - ok

09:58:43.0686 4508 [B1BE47008D20E43DA3ADC37C24CDB89D] MRxDAV
C:\Windows\system32\drivers\mrxdav.sys

09:58:43.0688 4508 MRxDAV - ok

09:58:43.0703 4508 [F4A054BE78AF7F410129C4B64B07DC9B] mrxsmmb
C:\Windows\system32\DRIVERS\mrxsmmb.sys

09:58:43.0706 4508 mrxsmmb - ok

09:58:43.0729 4508 [DEFFA295BD1895C6ED8E3078412AC60B] mrxsmmb10
C:\Windows\system32\DRIVERS\mrxsmmb10.sys

09:58:43.0731 4508 mrxsmmb10 - ok

09:58:43.0748 4508 [24D76ABE5DCAD22F19D105F76FDF0CE1] mrxsmmb20
C:\Windows\system32\DRIVERS\mrxsmmb20.sys

09:58:43.0750 4508 mrxsmmb20 - ok

09:58:43.0771 4508 [4326D168944123F38DD3B2D9C37A0B12] msahci
C:\Windows\system32\DRIVERS\msahci.sys

09:58:43.0772 4508 msahci - ok

09:58:43.0791 4508 [455029C7174A2DBB03DBA8A0D8BDDD9A] msdsm
C:\Windows\system32\DRIVERS\msdsm.sys

09:58:43.0793 4508 msdsm - ok

09:58:43.0811 4508 [E1BCE74A3BD9902B72599C0192A07E27] MSDTC C:\Windows\System32\msdtc.exe

09:58:43.0817 4508 MSDTC - ok

09:58:43.0841 4508 [DAEFB28E3AF5A76ABCC2C3078C07327F] Msfs C:\Windows\system32\drivers\Msfs.sys

09:58:43.0843 4508 Msfs - ok

09:58:43.0872 4508 [3E1E5767043C5AF9367F0056295E9F84] mshidkmdf
C:\Windows\System32\drivers\mshidkmdf.sys

09:58:43.0873 4508 mshidkmdf - ok

09:58:43.0891 4508 [0A4E5757AE09FA9622E3158CC1AEF114] msisadv
C:\Windows\system32\DRIVERS\msisadv.sys

09:58:43.0893 4508 msisadv - ok

09:58:43.0930 4508 [90F7D9E6B6F27E1A707D4A297F077828] MSiSCSI C:\Windows\system32\iscsiexe.dll

09:58:43.0935 4508 MSiSCSI - ok

09:58:43.0942 4508 msiserver - ok

09:58:43.0969 4508 [8C0860D6366AAFFB6C5BB9DF9448E631] MSKSSRV
C:\Windows\system32\drivers\MSKSSRV.sys

09:58:43.0971 4508 MSKSSRV - ok

09:58:43.0983 4508 [3EA8B949F963562CEDBB549EAC0C11CE] MSPCLOCK
C:\Windows\system32\drivers\MSPCLOCK.sys

09:58:43.0984 4508 MSPCLOCK - ok

09:58:44.0015 4508 [F456E973590D663B1073E9C463B40932] MSPQM
C:\Windows\system32\drivers\MSPQM.sys

09:58:44.0016 4508 MSPQM - ok

09:58:44.0041 4508 [0E008FC4819D238C51D7C93E7B41E560] MsRPC
C:\Windows\system32\drivers\MsRPC.sys

09:58:44.0044 4508 MsRPC - ok

09:58:44.0077 4508 [FC6B9FF600CC585EA38B12589BD4E246] mssmbios
C:\Windows\system32\DRIVERS\mssmbios.sys

09:58:44.0078 4508 mssmbios - ok

09:58:44.0110 4508 [B42C6B921F61A6E55159B8BE6CD54A36] MSTEE
C:\Windows\system32\drivers\MSTEE.sys

09:58:44.0111 4508 MSTEE - ok

09:58:44.0127 4508 [33599130F44E1F34631CEA241DE8AC84] MTConfig
C:\Windows\system32\DRIVERS\MTConfig.sys

09:58:44.0128 4508 MTConfig - ok

09:58:44.0161 4508 [159FAD02F64E6381758C990F753BCC80] Mup C:\Windows\system32\Drivers\mup.sys

09:58:44.0163 4508 Mup - ok

09:58:44.0196 4508 [80284F1985C70C86F0B5F86DA2DFE1DF] napagent C:\Windows\system32\qagentRT.dll

09:58:44.0204 4508 napagent - ok

09:58:44.0223 4508 [26384429FCD85D83746F63E798AB1480] NativeWifiP
C:\Windows\system32\DRIVERS\nwifi.sys

09:58:44.0229 4508 NativeWifiP - ok

09:58:44.0266 4508 [23759D175A0A9BAAF04D05047BC135A8] NDIS C:\Windows\system32\drivers\ndis.sys

09:58:44.0272 4508 NDIS - ok

09:58:44.0297 4508 [0E1787AA6C9191D3D319E8BAFE86F80C] NdisCap
C:\Windows\system32\DRIVERS\ndiscap.sys

09:58:44.0299 4508 NdisCap - ok

09:58:44.0321 4508 [E4A8AEC125A2E43A9E32AFEEA7C9C888] NdisTapi
C:\Windows\system32\DRIVERS\ndistapi.sys

09:58:44.0322 4508 NdisTapi - ok

09:58:44.0336 4508 [B30AE7F2B6D7E343B0DF32E6C08FCE75] Ndisuio
C:\Windows\system32\DRIVERS\ndisuio.sys

09:58:44.0337 4508 Ndisuio - ok

09:58:44.0355 4508 [267C415EADCBCE53C9CA873DEE39CF3A4] NdisWan
C:\Windows\system32\DRIVERS\ndiswan.sys

09:58:44.0357 4508 NdisWan - ok

09:58:44.0370 4508 [AF7E7C63DCEF3F8772726F86039D6EB4] NDPProxy
C:\Windows\system32\drivers\NDProxy.sys

09:58:44.0371 4508 NDPProxy - ok

09:58:44.0392 4508 [A081CB6FB9A12668F233EB5414BE3A0E] Net Driver HPZ12
C:\Windows\system32\HPZinw12.dll

09:58:44.0395 4508 Net Driver HPZ12 - ok

09:58:44.0414 4508 [80B275B1CE3B0E79909DB7B39AF74D51] NetBIOS
C:\Windows\system32\DRIVERS\netbios.sys

09:58:44.0415 4508 NetBIOS - ok

09:58:44.0435 4508 [DD52A733BF4CA5AF84562A5E2F963B91] NetBT
C:\Windows\system32\DRIVERS\netbt.sys

09:58:44.0438 4508 NetBT - ok

09:58:44.0460 4508 [F42309C4191C506B71DB5D1126D26318] Netlogon C:\Windows\system32\lsass.exe

09:58:44.0465 4508 Netlogon - ok

09:58:44.0508 4508 [7CCCFCA7510684768DA22092D1FA4DB2] Netman C:\Windows\System32\netman.dll

09:58:44.0516 4508 Netman - ok

09:58:44.0543 4508 [8C338238C16777A802D6A9211EB2BA50] netprofm C:\Windows\System32\netprofm.dll

09:58:44.0550 4508 netprofm - ok

09:58:44.0597 4508 [76B1157EF850830C5ECE61D3E591CA8B] netr73
C:\Windows\system32\DRIVERS\netr73.sys

09:58:44.0602 4508 netr73 - ok

09:58:44.0642 4508 [FE2AA5A684B0DD9B1FAE57B7817C198B] NetTcpPortSharing
C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation\SMSSvcHost.exe

09:58:44.0644 4508 NetTcpPortSharing - ok

09:58:44.0682 4508 [1D85C4B390B0EE09C7A46B91EFB2C097] nfrd960
C:\Windows\system32\DRIVERS\nfrd960.sys

09:58:44.0683 4508 nfrd960 - ok

09:58:44.0712 4508 [2226496E34BD40734946A054B1CD657F] NlaSvc C:\Windows\System32\ntlasvc.dll

09:58:44.0718 4508 NlaSvc - ok

09:58:44.0736 4508 [1DB262A9F8C087E8153D89BEF3D2235F] Npfs C:\Windows\system32\drivers\Npfs.sys

09:58:44.0738 4508 Npfs - ok

09:58:44.0767 4508 [BA387E955E890C8A88306D9B8D06BF17] nsi C:\Windows\system32\nsisvc.dll

09:58:44.0772 4508 nsi - ok

09:58:44.0789 4508 [E9A0A4D07E53D8FEA2BB8387A3293C58] nsiproxy
C:\Windows\system32\drivers\nsiproxy.sys

09:58:44.0791 4508 nsiproxy - ok

09:58:44.0845 4508 [3795DCD21F740EE799FB7223234215AF] Ntfs C:\Windows\system32\drivers\Ntfs.sys

09:58:44.0855 4508 Ntfs - ok

09:58:44.0870 4508 [F9756A98D69098DCA8945D62858A812C] Null C:\Windows\system32\drivers\Null.sys

09:58:44.0872 4508 Null - ok

09:58:44.0906 4508 [3F3D04B1D08D43C16EA7963954EC768D] nvraid
C:\Windows\system32\DRIVERS\nvraid.sys

09:58:44.0908 4508 nvraid - ok

09:58:44.0918 4508 [C99F251A5DE63C6F129CF71933ACED0F] nvstor
C:\Windows\system32\DRIVERS\nvstor.sys

09:58:44.0920 4508 nvstor - ok

09:58:44.0944 4508 [5A0983915F02BAE73267CC2A041F717D] nv_agp
C:\Windows\system32\DRIVERS\nv_agp.sys

09:58:44.0946 4508 nv_agp - ok

09:58:45.0015 4508 [84DE1DD996B48B05ACE31AD015FA108A] odserv C:\Program Files\Common
Files\Microsoft Shared\OFFICE12\ODSERV.EXE

09:58:45.0019 4508 odserv - ok

09:58:45.0044 4508 [08A70A1F2CDDE9BB49B885CB817A66EB] ohci1394
C:\Windows\system32\DRIVERS\ohci1394.sys

09:58:45.0046 4508 ohci1394 - ok

09:58:45.0071 4508 [5A432A042DAE460ABE7199B758E8606C] ose C:\Program Files\Common
Files\Microsoft Shared\Source Engine\OSE.EXE

09:58:45.0073 4508 ose - ok

09:58:45.0110 4508 [82A8521DDC60710C3D3D3E7325209BEC] p2pimsvc C:\Windows\system32\pnrpsvc.dll

09:58:45.0117 4508 p2pimsvc - ok

09:58:45.0136 4508 [59C3DDD501E39E006DAC31BF55150D91] p2psvc C:\Windows\system32\p2psvc.dll

09:58:45.0143 4508 p2psvc - ok

09:58:45.0200 4508 [1011C779C9FCD01AFA96490C86A50421] PanService C:\Program
Files\PANDORA.TV\PanService\PandoraService.exe

09:58:45.0205 4508 PanService - ok

09:58:45.0235 4508 [2EA877ED5DD9713C5AC74E8EA7348D14] Parport
C:\Windows\system32\DRIVERS\parport.sys

09:58:45.0237 4508 Parport - ok

09:58:45.0256 4508 [FF4218952B51DE44FE910953A3E686B9] partmgr
C:\Windows\system32\drivers\partmgr.sys

09:58:45.0258 4508 partmgr - ok

09:58:45.0271 4508 [EB0A59F29C19B86479D36B35983DAADC] Parvdm
C:\Windows\system32\DRIVERS\parvdm.sys

09:58:45.0272 4508 Parvdm - ok

09:58:45.0303 4508 [3CAE2BBC86FCF7F94C9696994AF30386] PassThru Service C:\Program Files\HTC\Internet
Pass-Through\PassThruSvr.exe

09:58:45.0305 4508 PassThru Service - ok

09:58:45.0332 4508 [358AB7956D3160000726574083DFC8A6] PcaSvc C:\Windows\System32\pcasvc.dll

09:58:45.0338 4508 PcaSvc - ok

09:58:45.0362 4508 [C858CB77C577780ECC456A892E7E7D0F] pci C:\Windows\system32\DRIVERS\pci.sys

09:58:45.0364 4508 pci - ok

09:58:45.0385 4508 [AFE86F419014DB4E5593F69FFE26CE0A] pciide
C:\Windows\system32\DRIVERS\pciide.sys

09:58:45.0386 4508 pciide - ok

09:58:45.0408 4508 [F396431B31693E71E8A80687EF523506] pcmcia
C:\Windows\system32\DRIVERS\pcmcia.sys

09:58:45.0410 4508 pcmcia - ok

09:58:45.0430 4508 [250F6B43D2B613172035C6747AEEB19F] pcw C:\Windows\system32\drivers\pcw.sys

09:58:45.0432 4508 pcw - ok

09:58:45.0459 4508 [9E0104BA49F4E6973749A02BF41344ED] PEAUTH
C:\Windows\system32\drivers\peauth.sys

09:58:45.0464 4508 PEAUTH - ok

09:58:45.0514 4508 [AF4D64D2A57B9772CF3801950B8058A6] PeerDistSvc
C:\Windows\system32\peerdistsvc.dll

09:58:45.0527 4508 PeerDistSvc - ok

09:58:45.0607 4508 [9C1BFF7910C89A1D12E57343475840CB] pla C:\Windows\system32\pla.dll

09:58:45.0623 4508 pla - ok

09:58:45.0654 4508 [2CC2008F1296968FBA162ED9F9AFE328] PlugPlay C:\Windows\system32\umpnpgm.dll

09:58:45.0662 4508 PlugPlay - ok

09:58:45.0678 4508 [65BC271F337637731D3C71455AE1F476] Pml Driver HPZ12
C:\Windows\system32\HPZipm12.dll

09:58:45.0681 4508 Pml Driver HPZ12 - ok

09:58:45.0707 4508 [63FF8572611249931EB16BB8EED6AFC8] PNRPAutoReg
C:\Windows\system32\pnrpauto.dll

09:58:45.0713 4508 PNRPAutoReg - ok

09:58:45.0744 4508 [82A8521DDC60710C3D3D3E7325209BEC] PNRPsvc C:\Windows\system32\pnrpsvc.dll

09:58:45.0751 4508 PNRPsvc - ok

09:58:45.0788 4508 [48E1B75C6DC0232FD92BAAE4BD344721] PolicyAgent C:\Windows\System32\ipsecsvc.dll

09:58:45.0793 4508 PolicyAgent - ok

09:58:45.0823 4508 [DBFF83F709A91049621C1D35DD45C92C] Power C:\Windows\system32\umpo.dll

09:58:45.0831 4508 Power - ok

09:58:45.0855 4508 [631E3E205AD6D86F2AED6A4A8E69F2DB] PptpMiniport
C:\Windows\system32\DRIVERS\raspppt.sys

09:58:45.0857 4508 PptpMiniport - ok

09:58:45.0887 4508 [85B1E3A0C7585BC4AAE6899EC6FCF011] Processor
C:\Windows\system32\DRIVERS\processr.sys

09:58:45.0888 4508 Processor - ok

09:58:45.0914 4508 [630CF26F0227498B7D5A92B12548960F] ProfSvc C:\Windows\system32\profsvc.dll

09:58:45.0920 4508 ProfSvc - ok

09:58:45.0938 4508 [F42309C4191C506B71DB5D1126D26318] ProtectedStorage C:\Windows\system32\lsass.exe

09:58:45.0942 4508 ProtectedStorage - ok

09:58:45.0973 4508 [6270CCAE2A86DE6D146529FE55B3246A] Psched
C:\Windows\system32\DRIVERS\pacer.sys

09:58:45.0975 4508 Psched - ok

09:58:45.0996 4508 [0B6DEA0A1662CAB8F2BF339DC0752EF4] PSI_SVC_2 c:\Program Files\Common
Files\Protexis\License Service\PsiService_2.exe

09:58:45.0999 4508 PSI_SVC_2 - ok

09:58:46.0055 4508 [AB95ECF1F6659A60DDC166D8315B0751] ql2300
C:\Windows\system32\DRIVERS\ql2300.sys

09:58:46.0067 4508 ql2300 - ok

09:58:46.0100 4508 [B4DD51DD25182244B86737DC51AF2270] ql40xx
C:\Windows\system32\DRIVERS\ql40xx.sys

09:58:46.0102 4508 ql40xx - ok

09:58:46.0134 4508 [31AC809E7707EB580B2BDB760390765A] QWAVE C:\Windows\system32\qwave.dll

09:58:46.0141 4508 QWAVE - ok

09:58:46.0168 4508 [584078CA1B95CA72DF2A27C336F9719D] QWAVEdrv
C:\Windows\system32\drivers\qwavedrv.sys

09:58:46.0171 4508 QWAVEdrv - ok

09:58:46.0193 4508 [30A81B53C766D0133BB86D234E5556AB] RasAcid
C:\Windows\system32\DRIVERS\rasacd.sys

09:58:46.0194 4508 RasAcid - ok

09:58:46.0214 4508 [57EC4AEF73660166074D8F7F31C0D4FD] RasAgileVpn
C:\Windows\system32\DRIVERS\AgileVpn.sys

09:58:46.0215 4508 RasAgileVpn - ok

09:58:46.0239 4508 [A60F1839849C0C00739787FD5EC03F13] RasAuto C:\Windows\System32\rasauto.dll

09:58:46.0246 4508 RasAuto - ok

09:58:46.0285 4508 [D9F91EAFEC2815365CBE6D167E4E332A] Rasl2tp
C:\Windows\system32\DRIVERS\rasl2tp.sys

09:58:46.0287 4508 Rasl2tp - ok

09:58:46.0332 4508 [0CE66EC736B7FC526D78F7624C7D2A94] RasMan C:\Windows\System32\rasmans.dll

09:58:46.0340 4508 RasMan - ok

09:58:46.0358 4508 [0FE8B15916307A6AC12BFB6A63E45507] RasPppoe
C:\Windows\system32\DRIVERS\rasppoe.sys

09:58:46.0360 4508 RasPppoe - ok

09:58:46.0383 4508 [44101F495A83EA6401D886E7FD70096B] RasSstp
C:\Windows\system32\DRIVERS\rassstp.sys

09:58:46.0385 4508 RasSstp - ok

09:58:46.0409 4508 [835D7E81BF517A3B72384BDCC85E1CE6] rdbss
C:\Windows\system32\DRIVERS\rdbss.sys

09:58:46.0412 4508 rdbss - ok

09:58:46.0429 4508 [0D8F05481CB76E70E1DA06EE9F0DA9DF] rdpbus
C:\Windows\system32\DRIVERS\rdpbus.sys

09:58:46.0430 4508 rdpbus - ok

09:58:46.0450 4508 [1E016846895B15A99F9A176A05029075] RDPCDD
C:\Windows\system32\DRIVERS\RDPCDD.sys

09:58:46.0452 4508 RDPCDD - ok

09:58:46.0480 4508 [C5FF95883FFEF704D50C40D21CFB3AB5] RDPDR
C:\Windows\system32\drivers\rdpdr.sys

09:58:46.0483 4508 RDPDR - ok

09:58:46.0502 4508 [5A53CA1598DD4156D44196D200C94B8A] RDPENCDD
C:\Windows\system32\drivers\rdpencdd.sys

09:58:46.0503 4508 RDPENCDD - ok

09:58:46.0517 4508 [44B0A53CD4F27D50ED461DAE0C0B4E1F] RDPREFMP
C:\Windows\system32\drivers\rdprefmp.sys

09:58:46.0520 4508 RDPREFMP - ok

09:58:46.0557 4508 [801371BA9782282892D00AADB08EE367] RDPWD
C:\Windows\system32\drivers\RDPWD.sys

09:58:46.0559 4508 RDPWD - ok

09:58:46.0596 4508 [4EA225BF1CF05E158853F30A99CA29A7] rdyboost
C:\Windows\system32\drivers\rdyboost.sys

09:58:46.0599 4508 rdyboost - ok

09:58:46.0636 4508 [7B5E1419717FAC363A31CC302895217A] RemoteAccess C:\Windows\System32\mprdim.dll

09:58:46.0641 4508 RemoteAccess - ok

09:58:46.0670 4508 [CB9A8683F4EF2BF99E123D79950D7935] RemoteRegistry C:\Windows\system32\regsvc.dll

09:58:46.0677 4508 RemoteRegistry - ok

09:58:46.0707 4508 [3015A847EBA796EAC070F3F70079E15A] rp24msdrv
C:\Windows\system32\drivers\rp24msdrv.sys

09:58:46.0709 4508 rp24msdrv - ok

09:58:46.0728 4508 [78D072F35BC45D9E4E1B61895C152234] RpcEptMapper
C:\Windows\System32\RpcEpMap.dll

09:58:46.0734 4508 RpcEptMapper - ok

09:58:46.0751 4508 [94D36C0E44677DD26981D2BFEEF2A29D] RpcLocator C:\Windows\system32\locator.exe

09:58:46.0755 4508 RpcLocator - ok

09:58:46.0785 4508 [B82CD39E336973359D7C9BF911E8E84F] RpcSs C:\Windows\system32\rpcss.dll

09:58:46.0795 4508 RpcSs - ok

09:58:46.0830 4508 [032B0D36AD92B582D869879F5AF5B928] rspndr
C:\Windows\system32\DRIVERS\rspndr.sys

09:58:46.0832 4508 rspndr - ok

09:58:46.0857 4508 [5423D8437051E89DD34749F242C98648] s3cap
C:\Windows\system32\DRIVERS\vms3cap.sys

09:58:46.0859 4508 s3cap - ok

09:58:46.0882 4508 [F42309C4191C506B71DB5D1126D26318] SamSs C:\Windows\system32\lsass.exe

09:58:46.0886 4508 SamSs - ok

09:58:46.0946 4508 [34EE0C44B724E3E4CE2EFF29126DE5B5] sbp2port
C:\Windows\system32\DRIVERS\sbp2port.sys

09:58:46.0948 4508 sbp2port - ok

09:58:47.0005 4508 [8FC518FFE9519C2631D37515A68009C4] SCardSvr C:\Windows\System32\SCardSvr.dll

09:58:47.0015 4508 SCardSvr - ok

09:58:47.0094 4508 [A95C54B2AC3CC9C73FCDF9E51A1D6B51] scfilter
C:\Windows\system32\DRIVERS\scfilter.sys

09:58:47.0096 4508 scfilter - ok

09:58:47.0160 4508 [3E8B0C453E25613A1F59762A5C42AA75] Schedule C:\Windows\system32\schedsvc.dll

09:58:47.0173 4508 Schedule - ok

09:58:47.0190 4508 [628A9E30EC5E18DD5DE6BE4DBDC12198] SCPolicySvc C:\Windows\System32\certprop.dll

09:58:47.0192 4508 SCPolicySvc - ok

09:58:47.0224 4508 [5FD90ABDBFAEE85986802622CBB03446] SDRSVC C:\Windows\System32\SDRSVC.dll

09:58:47.0232 4508 SDRSVC - ok

09:58:47.0253 4508 [90A3935D05B494A5A39D37E71F09A677] secdrv
C:\Windows\system32\drivers\secdrv.sys

09:58:47.0255 4508 secdrv - ok

09:58:47.0280 4508 [A59B3A4442C52060CC7A85293AA3546F] seclogon C:\Windows\system32\seclogon.dll

09:58:47.0286 4508 seclogon - ok

09:58:47.0308 4508 [DCB7FCDCC97F87360F75D77425B81737] SENS C:\Windows\System32\sens.dll

09:58:47.0316 4508 SENS - ok

09:58:47.0334 4508 [50087FE1EE447009C9CC2997B90DE53F] SensrSvc C:\Windows\system32\sensrsvc.dll

09:58:47.0340 4508 SensrSvc - ok

09:58:47.0358 4508 [9AD8B8B515E3DF6ACD4212EF465DE2D1] Serenum
C:\Windows\system32\DRIVERS\serenum.sys

09:58:47.0359 4508 Serenum - ok

09:58:47.0372 4508 [5FB7FCEA0490D821F26F39CC5EA3D1E2] Serial
C:\Windows\system32\DRIVERS\serial.sys

09:58:47.0374 4508 Serial - ok

09:58:47.0382 4508 [79BFFB520327FF916A582DFEA17AA813] sermouse
C:\Windows\system32\DRIVERS\sermouse.sys

09:58:47.0384 4508 sermouse - ok

09:58:47.0424 4508 [8F55CE568C543D5ADF45C409D16718FC] SessionEnv C:\Windows\system32\sessenv.dll

09:58:47.0431 4508 SessionEnv - ok

09:58:47.0438 4508 [9F976E1EB233DF46FCE808D9DEA3EB9C] sffdisk
C:\Windows\system32\DRIVERS\sffdisk.sys

09:58:47.0440 4508 sffdisk - ok

09:58:47.0449 4508 [932A68EE27833CFD57C1639D375F2731] sffp_mmc
C:\Windows\system32\DRIVERS\sffp_mmc.sys

09:58:47.0451 4508 sffp_mmc - ok

09:58:47.0460 4508 [4F1E5B0FE7C8050668DBFADE8999AEFB] sffp_sd
C:\Windows\system32\DRIVERS\sffp_sd.sys

09:58:47.0462 4508 sffp_sd - ok

09:58:47.0470 4508 [DB96666CC8312EBC45032F30B007A547] sfloppy
C:\Windows\system32\DRIVERS\sfloppy.sys

09:58:47.0472 4508 sfloppy - ok

09:58:47.0509 4508 [D1A079A0DE2EA524513B6930C24527A2] SharedAccess C:\Windows\System32\ipnathlp.dll

09:58:47.0515 4508 SharedAccess - ok

09:58:47.0552 4508 [CD2E48FA5B29EE2B3B5858056D246EF2] ShellHWDetection C:\Windows\System32\shsvcs.dll

09:58:47.0561 4508 ShellHWDetection - ok

09:58:47.0569 4508 [2565CAC0DC9FE0371BDCE60832582B2E] sisagp
C:\Windows\system32\DRIVERS\sisagp.sys

09:58:47.0571 4508 sisagp - ok

09:58:47.0604 4508 [A9F0486851BECB6DDA1D89D381E71055] SiSRaid2
C:\Windows\system32\DRIVERS\SiSRaid2.sys

09:58:47.0605 4508 SiSRaid2 - ok

09:58:47.0614 4508 [3727097B55738E2F554972C3BE5BC1AA] SiSRaid4
C:\Windows\system32\DRIVERS\sisraid4.sys

09:58:47.0616 4508 SiSRaid4 - ok

09:58:47.0653 4508 [2F5AF9D91D51E832773D4A9EAF65CB33] SkypeUpdate C:\Program
Files\Skype\Updater\Updater.exe

09:58:47.0655 4508 SkypeUpdate - ok

09:58:47.0671 4508 [3E21C083B8A01CB70BA1F09303010FCE] Smb
C:\Windows\system32\DRIVERS\smb.sys

09:58:47.0673 4508 Smb - ok

09:58:47.0700 4508 [6A984831644ECA1A33FFEAE4126F4F37] SNMPTRAP
C:\Windows\System32\snmptrap.exe

09:58:47.0707 4508 SNMPTRAP - ok

09:58:47.0723 4508 [95CF1AE7527FB70F7816563CBC09D942] spldr C:\Windows\system32\drivers\spldr.sys

09:58:47.0725 4508 spldr - ok

09:58:47.0766 4508 [49B6DD6AB3715B7A67965F17194E98A9] Spooler C:\Windows\System32\spoolsv.exe

09:58:47.0775 4508 Spooler - ok

09:58:47.0887 4508 [4C287F9069FEDBD791178876EE9DE536] sppsvc C:\Windows\system32\sppsvc.exe

09:58:47.0922 4508 sppsvc - ok

09:58:47.0964 4508 [D8E3E19EEBDAB49DD4A8D3062EAD4EC7] sppuinotify
C:\Windows\system32\sppuinotify.dll

09:58:47.0971 4508 sppuinotify - ok

09:58:48.0015 4508 [CDDDEC541BC3C96F91ECB48759673505] sptd C:\Windows\system32\Drivers\sptd.sys

09:58:48.0016 4508 Suspicious file (NoAccess): C:\Windows\system32\Drivers\sptd.sys. md5:
CDDDEC541BC3C96F91ECB48759673505

09:58:48.0019 4508 sptd (LockedFile.Multi.Generic) - warning

09:58:48.0019 4508 sptd - detected LockedFile.Multi.Generic (1)

09:58:48.0057 4508 [2BA4EBC7DFBA845A1EDBE1F75913BE33] srv C:\Windows\system32\DRIVERS\srv.sys

09:58:48.0061 4508 srv - ok

09:58:48.0081 4508 [DCE7E10FEAABD4CAE95948B3DE5340BB] srv2
C:\Windows\system32\DRIVERS\srv2.sys

09:58:48.0085 4508 srv2 - ok

09:58:48.0101 4508 [B5665BAA2120B8A54E22E9CD07C05106] srvnet
C:\Windows\system32\DRIVERS\srvnet.sys

09:58:48.0104 4508 srvnet - ok

09:58:48.0189 4508 [D887C9FD02AC9FA880F6E5027A43E118] SSDPSRV C:\Windows\System32\ssdpsrv.dll

09:58:48.0197 4508 SSDPSRV - ok

09:58:48.0225 4508 [D318F23BE45D5E3A107469EB64815B50] SstpSvc C:\Windows\system32\sstpsvc.dll

09:58:48.0232 4508 SstpSvc - ok

09:58:48.0267 4508 [BCB4E273147AFCAFDFC0DA59AF9E6E25] ssudmdm
C:\Windows\system32\DRIVERS\ssudmdm.sys

09:58:48.0270 4508 ssudmdm - ok

09:58:48.0287 4508 [A651B8D404FB1C0DA03FDC6549E35750] ssudserd
C:\Windows\system32\DRIVERS\ssudserd.sys

09:58:48.0289 4508 ssudserd - ok

09:58:48.0308 4508 [DB32D325C192B801DF274BFD12A7E72B] stexstor
C:\Windows\system32\DRIVERS\stexstor.sys

09:58:48.0310 4508 stexstor - ok

09:58:48.0352 4508 [A22825E7BB7018E8AF3E229A5AF17221] StiSvc C:\Windows\System32\wiaservc.dll

09:58:48.0364 4508 StiSvc - ok

09:58:48.0396 4508 [957E346CA948668F2496A6CCF6FF82CC] storflt
C:\Windows\system32\DRIVERS\vmstorfl.sys

09:58:48.0398 4508 storflt - ok

09:58:48.0415 4508 [D5751969DC3E4B88BF482AC8EC9FE019] storvsc
C:\Windows\system32\DRIVERS\storvsc.sys

09:58:48.0417 4508 storvsc - ok

09:58:48.0439 4508 [E58C78A848ADD9610A4DB6D214AF5224] swenum
C:\Windows\system32\DRIVERS\swenum.sys

09:58:48.0441 4508 swenum - ok

09:58:48.0519 4508 [F577910A133A592234EBAAD3F3AFA258] SwitchBoard C:\Program Files\Common
Files\Adobe\SwitchBoard\SwitchBoard.exe

09:58:48.0525 4508 SwitchBoard - ok

09:58:48.0573 4508 [A28BD92DF340E57B024BA433165D34D7] swprv C:\Windows\System32\swprv.dll

09:58:48.0582 4508 swprv - ok

09:58:48.0629 4508 [04105C8DA62353589C29BDAEB8D88BD8] SysMain C:\Windows\system32\sysmain.dll

09:58:48.0645 4508 SysMain - ok

09:58:48.0683 4508 [FCFB6C552FBC0DA299799CBD50AD9FD4] TabletInputService
C:\Windows\System32\TabSvc.dll

09:58:48.0691 4508 TabletInputService - ok

09:58:48.0720 4508 [2F46B0C70A4ADC8C90CF825DA3B4FEAF] TapiSrv C:\Windows\System32\tapisrv.dll

09:58:48.0729 4508 TapiSrv - ok

09:58:48.0754 4508 [B799D9FDB26111737F58288D8DC172D9] TBS C:\Windows\System32\tbssvc.dll

09:58:48.0761 4508 TBS - ok

09:58:48.0823 4508 [2CC3D75488ABD3EC628BBB9A4FC84EFC] Tcpip
C:\Windows\system32\drivers\tcpip.sys

09:58:48.0835 4508 Tcpip - ok

09:58:48.0869 4508 [2CC3D75488ABD3EC628BBB9A4FC84EFC] TCPIP6
C:\Windows\system32\DRIVERS\tcpip.sys

09:58:48.0881 4508 TCPIP6 - ok

09:58:48.0907 4508 [E64444523ADD154F86567C469BC0B17F] tcpipreg
C:\Windows\system32\drivers\tcpipreg.sys

09:58:48.0912 4508 tcpipreg - ok

09:58:48.0940 4508 [1875C1490D99E70E449E3AFAE9FCBADF] TDPIPE
C:\Windows\system32\drivers\tdpipe.sys

09:58:48.0941 4508 TDPIPE - ok

09:58:48.0950 4508 [7551E91EA999EE9A8E9C331D5A9C31F3] TDTCP
C:\Windows\system32\drivers\tdtcp.sys

09:58:48.0952 4508 TDTCP - ok

09:58:48.0970 4508 [CB39E896A2A83702D1737BFD402B3542] tdx C:\Windows\system32\DRIVERS\tdx.sys

09:58:48.0973 4508 tdx - ok

09:58:49.0135 4508 [7C8DD5576695B3362202EF09B20C425E] TeamViewer8 C:\Program
Files\TeamViewer\Version8\TeamViewer_Service.exe

09:58:49.0167 4508 TeamViewer8 - ok

09:58:49.0189 4508 [C36F41EE20E6999DBF4B0425963268A5] TermDD
C:\Windows\system32\DRIVERS\termdd.sys

09:58:49.0191 4508 TermDD - ok

09:58:49.0227 4508 [A01E50A04D7B1960B33E92B9080E6A94] TermService C:\Windows\System32\termsrv.dll

09:58:49.0238 4508 TermService - ok

09:58:49.0257 4508 [42FB6AFD6B79D9FE07381609172E7CA4] Themes
C:\Windows\system32\themeservice.dll

09:58:49.0265 4508 Themes - ok

09:58:49.0284 4508 [146B6F43A673379A3C670E86D89BE5EA] THREADORDER C:\Windows\system32\mmcss.dll

09:58:49.0289 4508 THREADORDER - ok

09:58:49.0303 4508 [4792C0378DB99A9BC2AE2DE6CFFF0C3A] TrkWks C:\Windows\System32\trkwks.dll

09:58:49.0311 4508 TrkWks - ok

09:58:49.0336 4508 [ED5E4CE36C54F55E7698642E94D32EC7] truecrypt
C:\Windows\system32\drivers>truecrypt.sys

09:58:49.0339 4508 truecrypt - ok

09:58:49.0387 4508 [41A4C781D2286208D397D72099304133] TrustedInstaller
C:\Windows\servicing\TrustedInstaller.exe

09:58:49.0389 4508 TrustedInstaller - ok

09:58:49.0428 4508 [98AE6FA07D12CB4EC5CF4A9BFA5F4242] tssecsrv
C:\Windows\system32\DRIVERS\tssecsrv.sys

09:58:49.0429 4508 tssecsrv - ok

09:58:49.0446 4508 [3E461D890A97F9D4C168F5FDA36E1D00] tunnel
C:\Windows\system32\DRIVERS\tunnel.sys

09:58:49.0449 4508 tunnel - ok

09:58:49.0462 4508 [750FBCB269F4D7DD2E420C56B795DB6D] uagp35
C:\Windows\system32\DRIVERS\uagp35.sys

09:58:49.0464 4508 uagp35 - ok

09:58:49.0491 4508 [09CC3E16F8E5EE7168E01CF8FCBE061A] udfs C:\Windows\system32\DRIVERS\udfs.sys

09:58:49.0495 4508 udfs - ok

09:58:49.0526 4508 [8344FD4FCE927880AA1AA7681D4927E5] UI0Detect
C:\Windows\system32\UI0Detect.exe

09:58:49.0534 4508 UI0Detect - ok

09:58:49.0551 4508 [44E8048ACE47BEFBFDC2E9BE4CBC8880] uliagpkx
C:\Windows\system32\DRIVERS\uliagpkx.sys

09:58:49.0553 4508 uliagpkx - ok

09:58:49.0584 4508 [049B3A50B3D646BAEEEE9EEC9B0668DC] umbus
C:\Windows\system32\DRIVERS\umbus.sys

09:58:49.0586 4508 umbus - ok

09:58:49.0602 4508 [7550AD0C6998BA1CB4843E920EE0FEAC] UmPass
C:\Windows\system32\DRIVERS\umpass.sys

09:58:49.0604 4508 UmPass - ok

09:58:49.0623 4508 [8ECACA5454844F66386F7BE4AE0D7CD1] UmRdpService C:\Windows\System32\umrdp.dll

09:58:49.0631 4508 UmRdpService - ok

09:58:49.0662 4508 [833FBB672460EFCE8011D262175FAD33] upnphost C:\Windows\System32\upnphost.dll

09:58:49.0671 4508 upnphost - ok

09:58:49.0711 4508 [6E421CCC57059B0186C6259CA3B6DFC9] USBAAPL
C:\Windows\system32\Drivers\usbaapl.sys

09:58:49.0713 4508 USBAAPL - ok

09:58:49.0740 4508 [8455C4ED038EFD09E99327F9D2D48FFA] usbccgp
C:\Windows\system32\DRIVERS\usbccgp.sys

09:58:49.0742 4508 usbccgp - ok

09:58:49.0750 4508 [04EC7CEC62EC3B6D9354EEE93327FC82] usbcir
C:\Windows\system32\DRIVERS\usbcir.sys

09:58:49.0753 4508 usbcir - ok

09:58:49.0766 4508 [1C333BFD60F2FED2C7AD5DAF533CB742] usbehci
C:\Windows\system32\DRIVERS\usbehci.sys

09:58:49.0768 4508 usbehci - ok

09:58:49.0793 4508 [EE6EF93CCFA94FAE8C6AB298273D8AE2] usbhub
C:\Windows\system32\DRIVERS\usbhub.sys

09:58:49.0796 4508 usbhub - ok

09:58:49.0816 4508 [A6FB7957EA7AFB1165991E54CE934B74] usbohci
C:\Windows\system32\DRIVERS\usbohci.sys

09:58:49.0817 4508 usbohci - ok

09:58:49.0844 4508 [797D862FE0875E75C7CC4C1AD7B30252] usbprint
C:\Windows\system32\DRIVERS\usbprint.sys

09:58:49.0846 4508 usbprint - ok

09:58:49.0873 4508 [576096CCBC07E7C4EA4F5E6686D6888F] usbscan
C:\Windows\system32\DRIVERS\usbscan.sys

09:58:49.0875 4508 usbscan - ok

09:58:49.0891 4508 [D8889D56E0D27E57ED4591837FE71D27] USBSTOR
C:\Windows\system32\DRIVERS\USBSTOR.SYS

09:58:49.0893 4508 USBSTOR - ok

09:58:49.0913 4508 [78780C3EBCE17405B1CCD07A3A8A7D72] usbuhci
C:\Windows\system32\DRIVERS\usbuhci.sys

09:58:49.0914 4508 usbuhci - ok

09:58:49.0954 4508 [F642A7E4BF78CFA359CCA0A3557C28D7] usbvideo
C:\Windows\system32\Drivers\usbvideo.sys

09:58:49.0956 4508 usbvideo - ok

09:58:49.0981 4508 [081E6E1C91AEC36758902A9F727CD23C] UxSms C:\Windows\System32\uxsms.dll

09:58:49.0989 4508 UxSms - ok

09:58:50.0004 4508 [F42309C4191C506B71DB5D1126D26318] VaultSvc C:\Windows\system32\lsass.exe

09:58:50.0009 4508 VaultSvc - ok

09:58:50.0020 4508 [A059C4C3EDB09E07D21A8E5C0AABD3CB] vdrvroot
C:\Windows\system32\DRIVERS\vdrvroot.sys

09:58:50.0022 4508 vdrvroot - ok

09:58:50.0058 4508 [8C4E7C49D3641BC9E299E466A7F8867D] vds C:\Windows\System32\vds.exe

09:58:50.0071 4508 vds - ok

09:58:50.0099 4508 [17C408214EA61696CEC9C66E388B14F3] vga
C:\Windows\system32\DRIVERS\vgapnp.sys

09:58:50.0101 4508 vga - ok

09:58:50.0116 4508 [8E38096AD5C8570A6F1570A61E251561] VgaSave C:\Windows\System32\drivers\vga.sys

09:58:50.0118 4508 VgaSave - ok

09:58:50.0129 4508 [3BE6E1F3A4F1AFEC8CEE0D7883F93583] vhdmp
C:\Windows\system32\DRIVERS\vhdmp.sys

09:58:50.0132 4508 vhdmp - ok

09:58:50.0142 4508 [C829317A37B4BEA8F39735D4B076E923] viaagp
C:\Windows\system32\DRIVERS\viaagp.sys

09:58:50.0145 4508 viaagp - ok

09:58:50.0154 4508 [E02F079A6AA107F06B16549C6E5C7B74] ViaC7
C:\Windows\system32\DRIVERS\viac7.sys

09:58:50.0156 4508 ViaC7 - ok

09:58:50.0179 4508 [E43574F6A56A0EE11809B48C09E4FD3C] viaide
C:\Windows\system32\DRIVERS\viaide.sys

09:58:50.0182 4508 viaide - ok

09:58:50.0201 4508 [379B349F65F453D2A6E75EA6B7448E49] vmbus
C:\Windows\system32\DRIVERS\vmbus.sys

09:58:50.0204 4508 vmbus - ok

09:58:50.0211 4508 [EC2BBAB4B84D0738C6C83D2234DC36FE] VMBusHID
C:\Windows\system32\DRIVERS\VMBusHID.sys

09:58:50.0213 4508 VMBusHID - ok

09:58:50.0230 4508 [384E5A2AA49934295171E499F86BA6F3] volmgr
C:\Windows\system32\DRIVERS\volmgr.sys

09:58:50.0231 4508 volmgr - ok

09:58:50.0252 4508 [B5BB72067DDDBBFB04B2F89FF8C3C87] volmgrx
C:\Windows\system32\drivers\volmgrx.sys

09:58:50.0256 4508 volmgrx - ok

09:58:50.0278 4508 [58DF9D2481A56EDDE167E51B334D44FD] volsnap
C:\Windows\system32\DRIVERS\volsnap.sys

09:58:50.0282 4508 volsnap - ok

09:58:50.0315 4508 [9DFA0CC2F8855A04816729651175B631] vsmraid
C:\Windows\system32\DRIVERS\vsmraid.sys

09:58:50.0317 4508 vsmraid - ok

09:58:50.0365 4508 [7EA2BCD94D9CFAF4C556F5CC94532A6C] VSS C:\Windows\system32\vssvc.exe

09:58:50.0381 4508 VSS - ok

09:58:50.0399 4508 [90567B1E658001E79D7C8BBD3DDE5AA6] vwifibus
C:\Windows\system32\DRIVERS\vwifibus.sys

09:58:50.0400 4508 vwifibus - ok

09:58:50.0415 4508 [7090D3436EEB4E7DA3373090A23448F7] vwififlt
C:\Windows\system32\DRIVERS\vwififlt.sys

09:58:50.0417 4508 vwififlt - ok

09:58:50.0447 4508 [55187FD710E27D5095D10A472C8BAF1C] W32Time C:\Windows\system32\w32time.dll

09:58:50.0457 4508 W32Time - ok

09:58:50.0509 4508 [DE3721E89C653AA281428C8A69745D90] WacomPen
C:\Windows\system32\DRIVERS\wacompen.sys

09:58:50.0511 4508 WacomPen - ok

09:58:50.0533 4508 [692A712062146E96D28BA0B7D75DE31B] WANARP
C:\Windows\system32\DRIVERS\wanarp.sys

09:58:50.0535 4508 WANARP - ok

09:58:50.0543 4508 [692A712062146E96D28BA0B7D75DE31B] Wanarpv6
C:\Windows\system32\DRIVERS\wanarp.sys

09:58:50.0546 4508 Wanarpv6 - ok

09:58:50.0604 4508 [7790B77FE1E5EE47DCC66247095BB4C9] wbengine C:\Windows\system32\wbengine.exe

09:58:50.0621 4508 wbengine - ok

09:58:50.0652 4508 [9614B5D29DC76AC3C29F6D2D3AA70E67] WbioSrv C:\Windows\System32\wbiosrv.dll

09:58:50.0661 4508 WbioSrv - ok

09:58:50.0691 4508 [D0F88AA11EE1A62BCC6D6A8A7783CA11] wcnscvc C:\Windows\System32\wcnscvc.dll

09:58:50.0700 4508 wcnscvc - ok

09:58:50.0733 4508 [5D930B6357A6D2AF4D7653BDABBF352F] WcsPlugInService
C:\Windows\System32\WcsPlugInService.dll

09:58:50.0741 4508 WcsPlugInService - ok

09:58:50.0769 4508 [1112A9BADACB47B7C0BB0392E3158DFF] Wd C:\Windows\system32\DRIVERS\wd.sys

09:58:50.0771 4508 Wd - ok

09:58:50.0802 4508 [9950E3D0F08141C7E89E64456AE7DC73] Wdf01000
C:\Windows\system32\drivers\Wdf01000.sys

09:58:50.0807 4508 Wdf01000 - ok

09:58:50.0837 4508 [46EF9DC96265FD0B423DB72E7C38C2A5] WdiServiceHost C:\Windows\system32\wdi.dll

09:58:50.0845 4508 WdiServiceHost - ok

09:58:50.0858 4508 [46EF9DC96265FD0B423DB72E7C38C2A5] WdiSystemHost C:\Windows\system32\wdi.dll

09:58:50.0865 4508 WdiSystemHost - ok

09:58:50.0891 4508 [D87C7D2C517F82A5AB7A73E203063D9E] WebClient C:\Windows\System32\webclnt.dll

09:58:50.0900 4508 WebClient - ok

09:58:50.0937 4508 [760F0AFE937A77CFF27153206534F275] Wecsvc C:\Windows\system32\wecsvc.dll

09:58:50.0946 4508 Wecsvc - ok

09:58:50.0964 4508 [AC804569BB2364FB6017370258A4091B] wercplsupport
C:\Windows\System32\wercplsupport.dll

09:58:50.0972 4508 wercplsupport - ok

09:58:50.0996 4508 [08E420D873E4FD85241EE2421B02C4A4] WerSvc C:\Windows\System32\WerSvc.dll

09:58:51.0004 4508 WerSvc - ok

09:58:51.0029 4508 [8B9A943F3B53861F2BFAF6C186168F79] WfpLwf
C:\Windows\system32\DRIVERS\wfplwf.sys

09:58:51.0032 4508 WfpLwf - ok

09:58:51.0054 4508 [5CF95B35E59E2A38023836FFF31BE64C] WIMMount
C:\Windows\system32\drivers\wimmount.sys

09:58:51.0056 4508 WIMMount - ok

09:58:51.0134 4508 [3FAE8F94296001C32EAB62CD7D82E0FD] WinDefend C:\Program Files\Windows
Defender\mpsvc.dll

09:58:51.0140 4508 WinDefend - ok

09:58:51.0155 4508 WinHttpAutoProxySvc - ok

09:58:51.0211 4508 [F62E510B6AD4C21EB9FE8668ED251826] Winmgmt
C:\Windows\system32\wbem\WMIsvc.dll

09:58:51.0213 4508 Winmgmt - ok

09:58:51.0280 4508 [C4F5D3901D1B41D602DDC196E0B95B51] WinRM C:\Windows\system32\WsmSvc.dll

09:58:51.0297 4508 WinRM - ok

09:58:51.0332 4508 [30FC6E5448D0CBAAA95280EEEF7FEDAE] WinUsb
C:\Windows\system32\DRIVERS\WinUsb.sys

09:58:51.0333 4508 WinUsb - ok

09:58:51.0380 4508 [16935C98FF639D185086A3529B1F2067] Wlansvc C:\Windows\System32\wlansvc.dll

09:58:51.0394 4508 Wlansvc - ok

09:58:51.0440 4508 [0217679B8FCA58714C3BF2726D2CA84E] WmiAcpi
C:\Windows\system32\DRIVERS\wmiacpi.sys

09:58:51.0441 4508 WmiAcpi - ok

09:58:51.0474 4508 [6EB6B66517B048D87DC1856DDF1F4C3F] wmiApSrv
C:\Windows\system32\wbem\WmiApSrv.exe

09:58:51.0477 4508 wmiApSrv - ok

09:58:51.0555 4508 [77FBD400984CF72BA0FC4B3489D65F74] WMPNetworkSvc C:\Program Files\Windows
Media Player\wmpnetwk.exe

09:58:51.0564 4508 WMPNetworkSvc - ok

09:58:51.0592 4508 [A2F0EC770A92F2B3F9DE6D518E11409C] WPCSvc C:\Windows\System32\wpcsvc.dll

09:58:51.0600 4508 WPCSvc - ok

09:58:51.0627 4508 [B7F658A2EBC07129538AD9AB35212637] WPDBusEnum
C:\Windows\system32\wpdbusenum.dll

09:58:51.0635 4508 WPDBusEnum - ok

09:58:51.0655 4508 [6DB3276587B853BF886B69528FDB048C] ws2ifsl
C:\Windows\system32\drivers\ws2ifsl.sys

09:58:51.0657 4508 ws2ifsl - ok

09:58:51.0688 4508 [6F5D49EFE0E7164E03AE773A3FE25340] wscsvc C:\Windows\System32\wscsvc.dll

09:58:51.0696 4508 wscsvc - ok

09:58:51.0708 4508 WSearch - ok

09:58:51.0788 4508 [A33408CC036F9C08142B11BE5E93F0A1] wuauserv C:\Windows\system32\wuaueng.dll

09:58:51.0813 4508 wuauserv - ok

09:58:51.0850 4508 [6F9B6C0C93232CFF47D0F72D6DB1D21E] WudfPf
C:\Windows\system32\drivers\WudfPf.sys

09:58:51.0852 4508 WudfPf - ok

09:58:51.0895 4508 [F91FF1E51FCA30B3C3981DB7D5924252] WUDFRd
C:\Windows\system32\DRIVERS\WUDFRd.sys

09:58:51.0898 4508 WUDFRd - ok

09:58:51.0932 4508 [DDEE3682FE97037C45F4D7AB467CB8B6] wudfsvc C:\Windows\System32\WUDFSvc.dll

09:58:51.0940 4508 wudfsvc - ok

09:58:51.0992 4508 [FF2D745B560F7C71B31F30F4D49F73D2] WwanSvc C:\Windows\System32\wwansvc.dll

09:58:52.0002 4508 WwanSvc - ok

09:58:52.0024 4508 ===== Scan global =====

09:58:52.0059 4508 [9A595DF601070DA78C40481120DD2C06] C:\Windows\system32\basesrv.dll

09:58:52.0089 4508 [827E4F75901CA3F990B1487D3301841E] C:\Windows\system32\winsrv.dll

09:58:52.0106 4508 [827E4F75901CA3F990B1487D3301841E] C:\Windows\system32\winsrv.dll

09:58:52.0134 4508 [364455805E64882844EE9ACB72522830] C:\Windows\system32\svchost.exe

09:58:52.0176 4508 [5F1B6A9C35D3D5CA72D6D6FDEF9747D6] C:\Windows\system32\services.exe

09:58:52.0184 4508 [Global] - ok

09:58:52.0185 4508 ===== Scan MBR =====

09:58:52.0195 4508 [A3095E5B8060D0D6B97E87EC1BB50C3C] \Device\Harddisk0\DR0

09:58:52.0285 4508 \Device\Harddisk0\DR0 - ok

09:58:52.0286 4508 ===== Scan VBR =====

09:58:52.0292 4508 [B9EB424879F862772B4E9EC1E35E02A4] \Device\Harddisk0\DR0\Partition1

09:58:52.0294 4508 \Device\Harddisk0\DR0\Partition1 - ok

09:58:52.0311 4508 [446378B598BE7135D4F0424B2087C738] \Device\Harddisk0\DR0\Partition2

09:58:52.0313 4508 \Device\Harddisk0\DR0\Partition2 - ok

09:58:52.0338 4508 [CE36AE7FA02C7A5BBE6124818331320B] \Device\Harddisk0\DR0\Partition3

09:58:52.0340 4508 \Device\Harddisk0\DR0\Partition3 - ok

09:58:52.0340 4508 =====

09:58:52.0340 4508 Scan finished

09:58:52.0340 4508 =====

09:58:52.0362 1532 Detected object count: 1

09:58:52.0362 1532 Actual detected object count: 1

09:59:02.0610 1532 sptd (LockedFile.Multi.Generic) - skipped by user

09:59:02.0611 1532 sptd (LockedFile.Multi.Generic) - User select action: Skip

09:59:04.0848 6112 Deinitialize Access

ComboFix

* Vytvořen nový Bod Obnovení

.
.

((Ostatní výmazы))

.
.

c:\windows\PFRO.log

.
.

((((((((((((((((((((((((Soubory vytvořené od 2013-04-05 do 2013-05-05))

2013-05-05 08:24	. 2013-05-05 08:24	-----	d-----w-	c:\users\Free\AppData\Local\temp
2013-05-05 08:24	. 2013-05-05 08:24	-----	d-----w-	c:\users\Default\AppData\Local\temp
2013-05-03 19:53	. 2013-05-03 19:56	-----	d-----w-	c:\users\User\AppData\Roaming\TrueCrypt
2013-05-03 19:50	. 2013-05-03 19:50	-----	d-----w-	c:\programdata\StarApp
2013-05-03 19:50	. 2013-05-03 19:50	-----	d-----w-	c:\programdata\InstallMate
2013-05-03 19:34	. 2013-05-03 19:34	231760	----a-w-	c:\windows\system32\drivers\truecrypt.sys
2013-05-03 19:33	. 2013-05-03 19:34	-----	d-----w-	c:\program files\TrueCrypt
2013-05-01 13:49	. 2013-05-03 07:17	-----	d-----w-	c:\users\Free\AppData\Local\LogMeIn Hamachi
2013-05-01 10:19	. 2013-05-05 08:24	-----	d-----w-	c:\users\User\AppData\Local\LogMeIn Hamachi
2013-05-01 10:18	. 2013-05-01 10:18	-----	d-----w-	c:\program files\LogMeIn Hamachi
2013-05-01 08:44	. 2013-05-01 08:44	-----	d-----w-	c:\users\User\AppData\Roaming\Malwarebytes
2013-05-01 08:43	. 2013-05-01 08:43	-----	d-----w-	c:\programdata\Malwarebytes
2013-05-01 08:43	. 2013-05-01 08:43	-----	d-----w-	c:\program files\Malwarebytes' Anti-Malware
2013-05-01 08:43	. 2013-04-04 12:50	22856	----a-w-	c:\windows\system32\drivers\mbam.sys
2013-05-01 08:15	. 2013-05-01 08:18	-----	d-----w-	c:\program files\Common Files\Steam
2013-04-24 16:28	. 2013-04-24 16:28	-----	d-----w-	c:\users\User\AppData\Local\Xenocode
2013-04-24 16:28	. 2013-04-24 16:28	-----	d-----w-	c:\program files\Xenocode

2013-04-22 19:12 . 2013-04-22 19:12	-----	d-----w-	c:\users\Free\AppData\Roaming\HP
2013-04-22 19:07 . 2013-04-22 19:07	-----	d-----w-	c:\users\Free\AppData\Roaming\LibreOffice
2013-04-17 19:00 . 2013-04-17 19:00	-----	d-----w-	c:\program files\Common Files\Java
2013-04-17 19:00 . 2013-04-04 03:35	94112	----a-w-	c:\windows\system32\WindowsAccessBridge.dll
2013-04-15 09:24 . 2010-12-01 06:52	23296	----a-w-	c:\windows\system32\drivers\rp24msdrv.sys
2013-04-15 09:24 . 2013-04-15 09:24	-----	d-----w-	c:\program files\Rapoo
2013-04-15 09:24 . 2013-04-15 09:24	1478609	----a-w-	c:\windows\unins000.exe
2013-04-14 09:29 . 2010-03-30 23:00	169064	----a-w-	c:\windows\system32\everest_cpl.cpl
2013-04-10 14:54 . 2013-04-10 14:54	691696	----a-w-	c:\windows\system32\drivers\sptd.sys
2013-04-08 21:16 . 2013-04-08 21:16	-----	d-----w-	c:\users\User\AppData\Roaming\HPAppData
2013-04-08 11:56 . 2013-04-08 13:32	-----	d-----w-	c:\users\Free\AppData\Roaming\AIMP3
2013-04-07 10:20 . 2013-04-07 10:20	-----	d-----w-	c:\users\Free\AppData\Roaming\GHISLER
.			
.			
.			
((Find3M výpis))			
.			
2013-05-01 09:36 . 2013-01-26 08:23	71048	----a-w-	c:\windows\system32\FlashPlayerCPLApp.cpl
2013-05-01 09:36 . 2013-01-26 08:23	691592	----a-w-	c:\windows\system32\FlashPlayerApp.exe
2013-03-07 10:19 . 2013-01-26 08:14	861088	----a-w-	c:\windows\system32\npDeployJava1.dll
2013-03-07 10:19 . 2013-01-26 08:14	782240	----a-w-	c:\windows\system32\deployJava1.dll
2013-03-06 23:33 . 2013-03-25 06:59	164736	----a-w-	c:\windows\system32\drivers\aswVmm.sys
2013-03-06 23:33 . 2013-03-25 06:59	49248	----a-w-	c:\windows\system32\drivers\aswRvrt.sys
2013-03-06 23:33 . 2013-01-26 08:18	368176	----a-w-	c:\windows\system32\drivers\aswSP.sys
2013-03-06 23:33 . 2013-01-26 08:18	62376	----a-w-	c:\windows\system32\drivers\aswTdi.sys
2013-03-06 23:33 . 2013-01-26 08:18	765736	----a-w-	c:\windows\system32\drivers\aswSnx.sys
2013-03-06 23:33 . 2013-01-26 08:18	60656	----a-w-	c:\windows\system32\drivers\aswRdr2.sys
2013-03-06 23:33 . 2013-01-26 08:18	66336	----a-w-	c:\windows\system32\drivers\aswMonFlt.sys
2013-03-06 23:33 . 2013-01-26 08:18	29816	----a-w-	c:\windows\system32\drivers\aswFsBlk.sys
2013-03-06 23:32 . 2013-01-26 08:18	41664	----a-w-	c:\windows\avastSS.scr

2013-03-06 23:32 . 2013-01-26 08:18	228600	----a-w-	c:\windows\system32\aswBoot.exe
2013-02-12 12:56 . 2013-02-12 12:55	466944	-----w-	c:\windows\Setup1.exe
2013-02-12 12:56 . 2013-02-12 12:55	73216	----a-w-	c:\windows\ST6UNST.EXE
2013-02-05 16:53 . 2013-02-28 11:46	4659712	----a-w-	c:\windows\system32\Redemption.dll
2013-02-05 16:52 . 2013-02-05 16:52	90112	----a-w-	c:\windows\MAMCityDownload.ocx
2013-02-05 16:52 . 2013-02-05 16:52	330240	----a-w-	c:\windows\MASetupCaller.dll
2013-02-05 16:52 . 2013-02-05 16:52	30568	----a-w-	c:\windows\MusiccityDownload.exe
2013-02-05 16:52 . 2013-02-05 16:52	974848	----a-w-	c:\windows\system32\cis-2.4.dll
2013-02-05 16:52 . 2013-02-05 16:52	81920	----a-w-	c:\windows\system32\issacapi_bs-2.3.dll
2013-02-05 16:52 . 2013-02-05 16:52	65536	----a-w-	c:\windows\system32\issacapi_pe-2.3.dll
2013-02-05 16:52 . 2013-02-05 16:52	57344	----a-w-	c:\windows\system32\MTXSYNCICON.dll
2013-02-05 16:52 . 2013-02-05 16:52	57344	----a-w-	c:\windows\system32\MK_Lyric.dll
2013-02-05 16:52 . 2013-02-05 16:52	57344	----a-w-	c:\windows\system32\issacapi_se-2.3.dll
2013-02-05 16:52 . 2013-02-05 16:52	569344	----a-w-	c:\windows\system32\muzdecode.ax
2013-02-05 16:52 . 2013-02-05 16:52	491520	----a-w-	c:\windows\system32\muzapp.dll
2013-02-05 16:52 . 2013-02-05 16:52	49152	----a-w-	c:\windows\system32\MaJGUILib.dll
2013-02-05 16:52 . 2013-02-05 16:52	45320	----a-w-	c:\windows\system32\MAMACEExtract.dll
2013-02-05 16:52 . 2013-02-05 16:52	45056	----a-w-	c:\windows\system32\MaXMLProto.dll
2013-02-05 16:52 . 2013-02-05 16:52	45056	----a-w-	c:\windows\system32\MACXMLProto.dll
2013-02-05 16:52 . 2013-02-05 16:52	40960	----a-w-	c:\windows\system32\MTTELECHIP.dll
2013-02-05 16:52 . 2013-02-05 16:52	352256	----a-w-	c:\windows\system32\MSLUR71.dll
2013-02-05 16:52 . 2013-02-05 16:52	258048	----a-w-	c:\windows\system32\muzogdsp.ax
2013-02-05 16:52 . 2013-02-05 16:52	245760	----a-w-	c:\windows\system32\MSCLib.dll
2013-02-05 16:52 . 2013-02-05 16:52	24576	----a-w-	c:\windows\system32\MASetupCleaner.exe
2013-02-05 16:52 . 2013-02-05 16:52	200704	----a-w-	c:\windows\system32\muzwmtd.dll
2013-02-05 16:52 . 2013-02-05 16:52	172032	----a-w-	c:\windows\system32\muzapp.exe
2013-02-05 16:52 . 2013-02-05 16:52	155648	----a-w-	c:\windows\system32\MSFLib.dll
2013-02-05 16:52 . 2013-02-05 16:52	143360	----a-w-	c:\windows\system32\3DAudio.ax
2013-02-05 16:52 . 2013-02-05 16:52	135168	----a-w-	c:\windows\system32\muzaf1.dll
2013-02-05 16:52 . 2013-02-05 16:52	131072	----a-w-	c:\windows\system32\muzmpgsp.ax

2013-02-05 16:52 . 2013-02-05 16:52 122880 ----a-w- c:\windows\system32\muzeffect.ax
2013-02-05 16:52 . 2013-02-05 16:52 118784 ----a-w- c:\windows\system32\MaDRM.dll
2013-02-05 16:52 . 2013-02-05 16:52 110592 ----a-w- c:\windows\system32\muzmp4sp.ax
2013-02-05 16:52 . 2013-02-28 11:46 821824 ----a-w- c:\windows\system32\dgderapi.dll
2013-01-16 20:10 . 2013-01-26 11:59 262552 ----a-w- c:\program files\mozilla
firefox\components\browsercomps.dll

.
.

((((((((((((((((((((((((((((((((((Spouštěcí body v registru))))))))))))))))))))))))))))))))))))

.
.

Poznámka prázdné záznamy a legitimní výchozí údaje nejsou zobrazeny.

REGEDIT4

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\00avast]

@="{472083B0-C522-11CF-8763-00608CC02F24}"

[HKEY_CLASSES_ROOT\CLSID\{472083B0-C522-11CF-8763-00608CC02F24}]

2013-03-06 23:32 121968 ----a-w- c:\program files\AVAST Software\Avast\ashShell.dll

.

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

"uTorrent"="c:\program files\uTorrent\uTorrent.exe" [2013-05-01 802136]

"DAEMON Tools Lite"="c:\program files\DAEMON Tools Lite\DTLite.exe" [2012-11-06 3673728]

"BgMonitor_{79662E04-7C6C-4d9f-84C7-88D8A56B10AA}"="c:\program files\Common
Files\Ahead\Lib\NMBgMonitor.exe" [2005-09-25 94208]

"KiesPreload"="c:\program files\Samsung\Kies\Kies.exe" [2013-02-13 1509232]

"Skype"="c:\program files\Skype\Phone\Skype.exe" [2013-02-28 18643048]

.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

"IgfxTray"="c:\windows\system32\igfxtray.exe" [2009-09-23 141848]

"HotKeysCmds"="c:\windows\system32\hkcmd.exe" [2009-09-23 173592]

"Persistence"="c:\windows\system32\igfxpers.exe" [2009-09-23 150552]

"RTHDVCPL"="c:\program files\Realtek\Audio\HDA\RtHDVCpl.exe" [2012-12-13 11734240]

"avast"="c:\program files\AVAST Software\Avast\avastUI.exe" [2013-03-06 4767304]

"Adobe ARM"="c:\program files\Common Files\Adobe\ARM\1.0\AdobeARM.exe" [2012-12-03 946352]

"GrooveMonitor"="c:\program files\Microsoft Office\Office12\GrooveMonitor.exe" [2006-10-26 31016]

"AdobeAAMUpdater-1.0"="c:\program files\Common Files\Adobe\OOBE\PDApp\UWA\UpdaterStartupUtility.exe" [2012-04-04 446392]

"SwitchBoard"="c:\program files\Common Files\Adobe\SwitchBoard\SwitchBoard.exe" [2010-02-19 517096]

"AdobeCS6ServiceManager"="c:\program files\Common Files\Adobe\CS6ServiceManager\CS6ServiceManager.exe" [2012-03-09 1073312]

"NeroFilterCheck"="c:\windows\system32\NeroCheck.exe" [2005-09-25 155648]

"HP Software Update"="c:\program files\HP\HP Software Update\HPWuSchd2.exe" [2009-11-18 54576]

"APSDaemon"="c:\program files\Common Files\Apple\Apple Application Support\APSDaemon.exe" [2013-01-28 59720]

"KiesTrayAgent"="c:\program files\Samsung\Kies\KiesTrayAgent.exe" [2013-02-13 310128]

"iTunesHelper"="c:\program files\iTunes\iTunesHelper.exe" [2013-02-20 152392]

"Rapoo 9200"="c:\program files\Rapoo\9200\9200_Mouse.exe" [2010-12-29 2622464]

"SunJavaUpdateSched"="c:\program files\Common Files\Java\Java Update\jusched.exe" [2013-03-12 253816]

"LogMeIn Hamachi Ui"="c:\program files\LogMeIn Hamachi\hamachi-2-ui.exe" [2012-12-14 2255360]

.

c:\programdata\Microsoft\Windows\Start Menu\Programs\Startup\

HP Digital Imaging Monitor.lnk - c:\program files\HP\Digital Imaging\bin\hpqtra08.exe [2009-11-18 275072]

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system]

"ConsentPromptBehaviorAdmin"= 5 (0x5)

"ConsentPromptBehaviorUser"= 3 (0x3)

"EnableUIADesktopToggle"= 0 (0x0)

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\drivers32]

"aux"=wdmaud.driv

.

R2 SkypeUpdate;Skype Updater;c:\program files\Skype\Updater\Updater.exe [x]

R3 aswVmm;aswVmm; [x]

R3 dg_ssudbus;SAMSUNG Mobile USB Composite Device Driver (DEVGURU Ver.);c:\windows\system32\DRIVERS\ssudbus.sys [x]

R3 HTCAND32;HTC Device Driver;c:\windows\system32\Drivers\ANDROIDUSB.sys [x]

R3 htcnprot;HTC NDIS Protocol Driver;c:\windows\system32\DRIVERS\htcnprot.sys [x]

R3 netr73;RT73 USB - ovladač karty pro bezdrátovou síť LAN pro systém Windows Vista;c:\windows\system32\DRIVERS\netr73.sys [x]

R3 rp24msdrv;2.4g Device;c:\windows\system32\drivers\rp24msdrv.sys [x]

R3 ssudmdm;SAMSUNG Mobile USB Modem Drivers (DEVGURU Ver.);c:\windows\system32\DRIVERS\ssudmdm.sys [x]

R3 ssudserd;SAMSUNG Mobile USB Diagnostic Serial Port(DEVGURU Ver.);c:\windows\system32\DRIVERS\ssudserd.sys [x]

R3 SwitchBoard;SwitchBoard;c:\program files\Common Files\Adobe\SwitchBoard\SwitchBoard.exe [x]

S0 aswRvrt;aswRvrt; [x]

S0 sptd;sptd;c:\windows\System32\Drivers\sptd.sys [x]

S1 aswSnx;aswSnx; [x]

S1 aswSP;aswSP; [x]

S1 dtsoftbus01;DAEMON Tools Virtual Bus Driver;c:\windows\system32\DRIVERS\dtsoftbus01.sys [x]

S2 aswFsBlk;aswFsBlk; [x]

S2 aswMonFlt;aswMonFlt;c:\windows\system32\drivers\aswMonFlt.sys [x]

S2 Hamachi2Svc;LogMeIn Hamachi Tunneling Engine;c:\program files\LogMeIn Hamachi\hamachi-2.exe [x]

S2 HTCMonitorService;HTCMonitorService;c:\program files\HTC Sync Manager\HSMServiceEntry.exe [x]

S2 MBAMService;MBAMService;c:\program files\Malwarebytes' Anti-Malware\mbamservice.exe [x]

S2 PanService;PandoraService;c:\program files\PANDORA.TV\PanService\PandoraService.exe [x]

S2 PassThru Service;Internet Pass-Through Service;c:\program files\HTC\Internet Pass-Through\PassThruSvr.exe [x]

S2 TeamViewer8;TeamViewer 8;c:\program files\TeamViewer\Version8\TeamViewer_Service.exe [x]

S3 MBAMProtector;MBAMProtector;c:\windows\system32\drivers\mbam.sys [x]

.

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\svchost]

HPZ12 REG_MULTI_SZ Pml Driver HPZ12 Net Driver HPZ12

hpdevmgmt REG_MULTI_SZ hpqcxs08 hpqddsvc

.
[HKEY_LOCAL_MACHINE\software\microsoft\active setup\installed components\{8A69D345-D564-463c-AFF1-A69D9E530F96}]

2013-04-11 15:05 1642448 ----a-w- c:\program
files\Google\Chrome\Application\26.0.1410.64\Installer\chromstp.exe

.
Obsah adresáře 'Naplánované úlohy'

.
2013-05-05 c:\windows\Tasks\Adobe Flash Player Updater.job

- c:\windows\system32\Macromed\Flash\FlashPlayerUpdateService.exe [2013-01-26 09:36]

.
2013-05-05 c:\windows\Tasks\GoogleUpdateTaskMachineCore.job

- c:\program files\Google\Update\GoogleUpdate.exe [2013-01-26 07:55]

.
2013-05-05 c:\windows\Tasks\GoogleUpdateTaskMachineUA.job

- c:\program files\Google\Update\GoogleUpdate.exe [2013-01-26 07:55]

.
----- Doplnkový sken -----

.
uStart Page = hxxp://websearch.greatresults.info/

mStart Page = hxxp://websearch.greatresults.info/

IE: E&xportovat do aplikace Microsoft Excel - c:\progra~1\MICROS~2\Office12\EXCEL.EXE/3000

FF - ProfilePath - c:\users\User\AppData\Roaming\Mozilla\Firefox\Profiles\tb8hazwi.default\

FF - prefs.js: browser.search.defaulturl - hxxp://websearch.greatresults.info/?l=1&q=

FF - prefs.js: browser.search.selectedEngine - WebSearch

FF - prefs.js: browser.startup.homepage - hxxp://websearch.greatresults.info/

FF - prefs.js: keyword.URL - hxxp://websearch.greatresults.info/?l=1&q=

FF - ExtSQL: !HIDDEN! 2013-01-26 12:51; smartwebprinting@hp.com; c:\program files\HP\Digital Imaging\Smart
Web Printing\MozillaAddOn3

--- NEPLATNÉ POLOŽKY ODSTRANĚNÉ Z REGISTRU ---

.

HKCU-Run-AdobeBridge - (no file)

AddRemove-{27BECDBE-DF20-1E3B-8AF3-80DA182A8578} - c:\progra~2\INSTAL~1\FCE41~1\Setup.exe

AddRemove-{48DF88CA-A835-6228-A3EE-A083ACAE011B} - c:\progra~2\INSTAL~1\{1303C~1\Setup.exe

AddRemove-{9BBF1BB1-94DC-FF68-9670-9FB060B80C1A} - c:\progra~2\INSTAL~1\F8984~1\Setup.exe

AddRemove-01_Simmental - c:\program files\SAMSUNG\USB Drivers\01_Simmental\Uninstall.exe

AddRemove-02_Siberian - c:\program files\SAMSUNG\USB Drivers\02_Siberian\Uninstall.exe

AddRemove-03_Swallowtail - c:\program files\SAMSUNG\USB Drivers\03_Swallowtail\Uninstall.exe

AddRemove-04_semseyite - c:\program files\SAMSUNG\USB Drivers\04_semseyite\Uninstall.exe

AddRemove-05_Sloan - c:\program files\SAMSUNG\USB Drivers\05_Sloan\Uninstall.exe

AddRemove-06_Spencer - c:\program files\SAMSUNG\USB Drivers\06_Spencer\Uninstall.exe

AddRemove-07_Schorl - c:\program files\SAMSUNG\USB Drivers\07_Schorl\Uninstall.exe

AddRemove-08_EMPChipset - c:\program files\SAMSUNG\USB Drivers\08_EMPChipset\Uninstall.exe

AddRemove-09_Hsp - c:\program files\SAMSUNG\USB Drivers\09_Hsp\Uninstall.exe

AddRemove-11_HSP_Plus_Default - c:\program files\SAMSUNG\USB Drivers\11_HSP_Plus_Default\Uninstall.exe

AddRemove-16_Shrewsbury - c:\program files\SAMSUNG\USB Drivers\16_Shrewsbury\Uninstall.exe

AddRemove-17_EMP_Chipset2 - c:\program files\SAMSUNG\USB Drivers\17_EMP_Chipset2\Uninstall.exe

AddRemove-18_Zinia_Serial_Driver - c:\program files\SAMSUNG\USB Drivers\18_Zinia_Serial_Driver\Uninstall.exe

AddRemove-19_VIA_driver - c:\program files\SAMSUNG\USB Drivers\19_VIA_driver\Uninstall.exe

AddRemove-20_NXP_Driver - c:\program files\SAMSUNG\USB Drivers\20_NXP_Driver\Uninstall.exe

AddRemove-21_Searsburg - c:\program files\SAMSUNG\USB Drivers\21_Searsburg\Uninstall.exe

AddRemove-22_WiBro_WiMAX - c:\program files\SAMSUNG\USB Drivers\22_WiBro_WiMAX\Uninstall.exe

AddRemove-24_flashusbdriver - c:\program files\SAMSUNG\USB Drivers\24_flashusbdriver\Uninstall.exe

AddRemove-25_escape - c:\program files\SAMSUNG\USB Drivers\25_escape\Uninstall.exe

.

.

.

----- ZAMKNUTÉ KLÍČE V REGISTRU -----

.

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}\0000\AllUserSettings]

@Denied: (A) (Users)

@Denied: (A) (Everyone)

@Allowed: (B 1 2 3 4 5) (S-1-5-20)

"BlindDial"=dword:00000000

"MSCurrentCountry"=dword:000000b5

.

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E96D-E325-11CE-BFC1-08002BE10318}\0001\AllUserSettings]

@Denied: (A) (Users)

@Denied: (A) (Everyone)

@Allowed: (B 1 2 3 4 5) (S-1-5-20)

"BlindDial"=dword:00000000

.

[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\PCW\Security]

@Denied: (Full) (Everyone)

.

Celkový čas: 2013-05-05 10:27:17

ComboFix-quarantined-files.txt 2013-05-05 08:27

.

Před spuštěním: Volných bajtů: 15 137 054 720

Po spuštění: Volných bajtů: 14 947 270 656

.

-- End Of File -- 9BB605141F490101C1B50CCCCF22BE8D1