```
15:27:23.0752 2124     TDSS rootkit removing tool 2.7.45.0 Jul  9 2012
12:46:35
15:27:24.0172 2124
      ============================================================
15:27:24.0172 2124     Current date / time: 2012/07/09 15:27:24.0172
15:27:24.0172 2124     SystemInfo:
15:27:24.0172 2124
15:27:24.0172 2124     OS Version: 6.1.7601 ServicePack: 1.0
15:27:24.0172 2124     Product type: Workstation
15:27:24.0172 2124     ComputerName: ONDRAPC
15:27:24.0172 2124     UserName: Ondra
15:27:24.0172 2124     Windows directory: C:\Windows
15:27:24.0172 2124     System windows directory: C:\Windows
15:27:24.0172 2124     Running under WOW64
15:27:24.0172 2124     Processor architecture: Intel x64
15:27:24.0172 2124     Number of processors: 2
15:27:24.0172 2124     Page size: 0x1000
15:27:24.0172 2124     Boot type: Normal boot
15:27:24.0172 2124
      ============================================================
15:27:25.0137 2124     Drive \Device\Harddisk0\DR0 - Size: 0x7470AFDE00
(465.76 Gb), SectorSize: 0x200, Cylinders: 0xED81, SectorsPerTrack: 0x3F,
TracksPerCylinder: 0xFF, Type 'K0', Flags 0x00000040
15:27:25.0143 2124
      ============================================================
15:27:25.0143 2124     \Device\Harddisk0\DR0:
15:27:25.0143 2124     MBR partitions:
15:27:25.0143 2124     \Device\Harddisk0\DR0\Partition0: MBR, Type 0x7,
StartLBA 0x3F, BlocksNum 0x6403941
15:27:25.0143 2124     \Device\Harddisk0\DR0\Partition1: MBR, Type 0x7,
StartLBA 0x6403980, BlocksNum 0x33F812C1
15:27:25.0143 2124
      ============================================================
15:27:25.0163 2124     C: <-> \Device\Harddisk0\DR0\Partition0
15:27:25.0188 2124     D: <-> \Device\Harddisk0\DR0\Partition1
15:27:25.0188 2124
      ============================================================
15:27:25.0188 2124     Initialize success
15:27:25.0188 2124
      ============================================================
15:33:34.0703 4080
      ============================================================
15:33:34.0703 4080     Scan started
15:33:34.0703 4080     Mode: Manual;
15:33:34.0703 4080
      ============================================================
15:33:35.0617 4080     1394ohci        (a87d604aea360176311474c87a63bb88)
C:\Windows\system32\drivers\1394ohci.sys
15:33:35.0621 4080     1394ohci - ok
15:33:35.0666 4080     ACPI            (d81d9e70b8a6dd14d42d7b4efa65d5f2)
C:\Windows\system32\drivers\ACPI.sys
15:33:35.0667 4080     ACPI - ok
15:33:35.0683 4080     AcpiPmi         (99f8e788246d495ce3794d7e7821d2ca)
C:\Windows\system32\drivers\acpipmi.sys
15:33:35.0685 4080     AcpiPmi - ok
15:33:35.0748 4080     AdobeARMservice (11a52cf7b265631deeb24c6149309eff)
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
15:33:35.0748 4080     AdobeARMservice - ok
```

```
15:33:35.0892 4080     AdobeFlashPlayerUpdateSvc
(76d5a3d2a50402a0b9b6ed13c4371e79)
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
15:33:35.0894 4080     AdobeFlashPlayerUpdateSvc - ok
15:33:35.0955 4080     adp94xx          (2f6b34b83843f0c5118b63ac634f5bf4)
C:\Windows\system32\DRIVERS\adp94xx.sys
15:33:35.0996 4080     adp94xx - ok
15:33:36.0023 4080     adpahci          (597f78224ee9224ea1a13d6350ced962)
C:\Windows\system32\DRIVERS\adpahci.sys
15:33:36.0027 4080     adpahci - ok
15:33:36.0050 4080     adpu320          (e109549c90f62fb570b9540c4b148e54)
C:\Windows\system32\DRIVERS\adpu320.sys
15:33:36.0050 4080     adpu320 - ok
15:33:36.0080 4080     AeLookupSvc      (4b78b431f225fd8624c5655cb1de7b61)
C:\Windows\System32\aelupsvc.dll
15:33:36.0080 4080     AeLookupSvc - ok
15:33:36.0144 4080     AFD              (1c7857b62de5994a75b054a9fd4c3825)
C:\Windows\system32\drivers\afd.sys
15:33:36.0148 4080     AFD - ok
15:33:36.0171 4080     agp440           (608c14dba7299d8cb6ed035a68a15799)
C:\Windows\system32\drivers\agp440.sys
15:33:36.0171 4080     agp440 - ok
15:33:36.0187 4080     ALG              (3290d6946b5e30e70414990574883ddb)
C:\Windows\System32\alg.exe
15:33:36.0187 4080     ALG - ok
15:33:36.0197 4080     aliide           (5812713a477a3ad7363c7438ca2ee038)
C:\Windows\system32\drivers\aliide.sys
15:33:36.0197 4080     aliide - ok
15:33:36.0205 4080     amdide           (1ff8b4431c353ce385c875f194924c0c)
C:\Windows\system32\drivers\amdide.sys
15:33:36.0205 4080     amdide - ok
15:33:36.0226 4080     AmdK8            (7024f087cff1833a806193ef9d22cda9)
C:\Windows\system32\DRIVERS\amdk8.sys
15:33:36.0226 4080     AmdK8 - ok
15:33:36.0244 4080     AmdPPM           (1e56388b3fe0d031c44144eb8c4d6217)
C:\Windows\system32\DRIVERS\amdppm.sys
15:33:36.0246 4080     AmdPPM - ok
15:33:36.0267 4080     amdsata          (d4121ae6d0c0e7e13aa221aa57ef2d49)
C:\Windows\system32\drivers\amdsata.sys
15:33:36.0269 4080     amdsata - ok
15:33:36.0289 4080     amdsbs           (f67f933e79241ed32ff46a4f29b5120b)
C:\Windows\system32\DRIVERS\amdsbs.sys
15:33:36.0291 4080     amdsbs - ok
15:33:36.0306 4080     amdxata          (540daf1cea6094886d72126fd7c33048)
C:\Windows\system32\drivers\amdxata.sys
15:33:36.0306 4080     amdxata - ok
15:33:36.0335 4080     AppID            (89a69c3f2f319b43379399547526d952)
C:\Windows\system32\drivers\appid.sys
15:33:36.0337 4080     AppID - ok
15:33:36.0353 4080     AppIDSvc         (0bc381a15355a3982216f7172f545de1)
C:\Windows\System32\appidsvc.dll
15:33:36.0353 4080     AppIDSvc - ok
15:33:36.0382 4080     Appinfo          (3977d4a871ca0d4f2ed1e7db46829731)
C:\Windows\System32\appinfo.dll
15:33:36.0384 4080     Appinfo - ok
15:33:36.0412 4080     AppMgmt          (4aba3e75a76195a3e38ed2766c962899)
C:\Windows\System32\appmgmts.dll
15:33:36.0414 4080     AppMgmt - ok
```

```
15:33:36.0431 4080     arc             (c484f8ceb1717c540242531db7845c4e)
C:\Windows\system32\DRIVERS\arc.sys
15:33:36.0431 4080     arc - ok
15:33:36.0439 4080     arcsas          (019af6924aefe7839f61c830227fe79c)
C:\Windows\system32\DRIVERS\arcsas.sys
15:33:36.0441 4080     arcsas - ok
15:33:36.0468 4080     AsyncMac        (769765ce2cc62867468cea93969b2242)
C:\Windows\system32\DRIVERS\asyncmac.sys
15:33:36.0468 4080     AsyncMac - ok
15:33:36.0503 4080     atapi           (02062c0b390b7729edc9e69c680a6f3c)
C:\Windows\system32\drivers\atapi.sys
15:33:36.0505 4080     atapi - ok
15:33:36.0576 4080     AudioEndpointBuilder
(f23fef6d569fce88671949894a8becf1) C:\Windows\System32\Audiosrv.dll
15:33:36.0587 4080     AudioEndpointBuilder - ok
15:33:36.0607 4080     AudioSrv        (f23fef6d569fce88671949894a8becf1)
C:\Windows\System32\Audiosrv.dll
15:33:36.0617 4080     AudioSrv - ok
15:33:36.0644 4080     AxInstSV        (a6bf31a71b409dfa8cac83159e1e2aff)
C:\Windows\System32\AxInstSV.dll
15:33:36.0646 4080     AxInstSV - ok
15:33:36.0671 4080     Axtmvflt        (344b907477ff1bc01bd315ab93df9764)
C:\Windows\system32\DRIVERS\Axtmvflt.sys
15:33:36.0671 4080     Axtmvflt - ok
15:33:36.0685 4080     Axtmvmdm        (4f8d9a8c04c33496403cc4dde3e9d6ce)
C:\Windows\system32\DRIVERS\Axtmvmdm.sys
15:33:36.0687 4080     Axtmvmdm - ok
15:33:36.0699 4080     Axtmvprt        (c24f39e3cc13fa14477ebe12461739ff)
C:\Windows\system32\Drivers\Axtmvprt.sys
15:33:36.0699 4080     Axtmvprt - ok
15:33:36.0740 4080     b06bdrv         (3e5b191307609f7514148c6832bb0842)
C:\Windows\system32\DRIVERS\bxvbda.sys
15:33:36.0744 4080     b06bdrv - ok
15:33:36.0771 4080     b57nd60a        (b5ace6968304a3900eeb1ebfd9622df2)
C:\Windows\system32\DRIVERS\b57nd60a.sys
15:33:36.0789 4080     b57nd60a - ok
15:33:36.0816 4080     BDESVC          (fde360167101b4e45a96f939f388aeb0)
C:\Windows\System32\bdesvc.dll
15:33:36.0816 4080     BDESVC - ok
15:33:36.0853 4080     Beep            (16a47ce2decc9b099349a5f840654746)
C:\Windows\system32\drivers\Beep.sys
15:33:36.0853 4080     Beep - ok
15:33:36.0906 4080     BFE             (82974d6a2fd19445cc5171fc378668a4)
C:\Windows\System32\bfe.dll
15:33:36.0912 4080     BFE - ok
15:33:36.0966 4080     BITS            (1ea7969e3271cbc59e1730697dc74682)
C:\Windows\System32\qmgr.dll
15:33:36.0974 4080     BITS - ok
15:33:37.0041 4080     blbdrive        (61583ee3c3a17003c4acd0475646b4d3)
C:\Windows\system32\DRIVERS\blbdrive.sys
15:33:37.0041 4080     blbdrive - ok
15:33:37.0072 4080     bowser          (6c02a83164f5cc0a262f4199f0871cf5)
C:\Windows\system32\DRIVERS\bowser.sys
15:33:37.0074 4080     bowser - ok
15:33:37.0085 4080     BrFiltLo        (f09eee9edc320b5e1501f749fde686c8)
C:\Windows\system32\DRIVERS\BrFiltLo.sys
15:33:37.0087 4080     BrFiltLo - ok
```

```
15:33:37.0101 4080     BrFiltUp         (b114d3098e9bdb8bea8b053685831be6)
C:\Windows\system32\DRIVERS\BrFiltUp.sys
15:33:37.0103 4080     BrFiltUp - ok
15:33:37.0156 4080     Browser          (8ef0d5c41ec907751b8429162b1239ed)
C:\Windows\System32\browser.dll
15:33:37.0158 4080     Browser - ok
15:33:37.0181 4080     Brserid          (43bea8d483bf1870f018e2d02e06a5bd)
C:\Windows\System32\Drivers\Brserid.sys
15:33:37.0183 4080     Brserid - ok
15:33:37.0193 4080     BrSerWdm         (a6eca2151b08a09caceca35c07f05b42)
C:\Windows\System32\Drivers\BrSerWdm.sys
15:33:37.0210 4080     BrSerWdm - ok
15:33:37.0226 4080     BrUsbMdm         (b79968002c277e869cf38bd22cd61524)
C:\Windows\System32\Drivers\BrUsbMdm.sys
15:33:37.0226 4080     BrUsbMdm - ok
15:33:37.0244 4080     BrUsbSer         (a87528880231c54e75ea7a44943b38bf)
C:\Windows\System32\Drivers\BrUsbSer.sys
15:33:37.0244 4080     BrUsbSer - ok
15:33:37.0291 4080     BthEnum          (cf98190a94f62e405c8cb255018b2315)
C:\Windows\system32\drivers\BthEnum.sys
15:33:37.0292 4080     BthEnum - ok
15:33:37.0316 4080     BTHMODEM         (9da669f11d1f894ab4eb69bf546a42e8)
C:\Windows\system32\DRIVERS\bthmodem.sys
15:33:37.0318 4080     BTHMODEM - ok
15:33:37.0353 4080     BthPan           (02dd601b708dd0667e1331fa8518e9ff)
C:\Windows\system32\DRIVERS\bthpan.sys
15:33:37.0355 4080     BthPan - ok
15:33:37.0414 4080     BTHPORT          (64c198198501f7560ee41d8d1efa7952)
C:\Windows\System32\Drivers\BTHport.sys
15:33:37.0419 4080     BTHPORT - ok
15:33:37.0460 4080     bthserv          (95f9c2976059462cbbf227f7aab10de9)
C:\Windows\system32\bthserv.dll
15:33:37.0460 4080     bthserv - ok
15:33:37.0496 4080     BTHUSB           (f188b7394d81010767b6df3178519a37)
C:\Windows\System32\Drivers\BTHUSB.sys
15:33:37.0498 4080     BTHUSB - ok
15:33:37.0527 4080     cdfs             (b8bd2bb284668c84865658c77574381a)
C:\Windows\system32\DRIVERS\cdfs.sys
15:33:37.0529 4080     cdfs - ok
15:33:37.0578 4080     cdrom            (f036ce71586e93d94dab220d7bdf4416)
C:\Windows\system32\DRIVERS\cdrom.sys
15:33:37.0580 4080     cdrom - ok
15:33:37.0609 4080     CertPropSvc      (f17d1d393bbc69c5322fbfafaca28c7f)
C:\Windows\System32\certprop.dll
15:33:37.0609 4080     CertPropSvc - ok
15:33:37.0625 4080     circlass         (d7cd5c4e1b71fa62050515314cfb52cf)
C:\Windows\system32\DRIVERS\circlass.sys
15:33:37.0625 4080     circlass - ok
15:33:37.0664 4080     CLFS             (fe1ec06f2253f691fe36217c592a0206)
C:\Windows\system32\CLFS.sys
15:33:37.0705 4080     CLFS - ok
15:33:37.0775 4080     clr_optimization_v2.0.50727_32
(d88040f816fda31c3b466f0fa0918f29)
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
15:33:37.0777 4080     clr_optimization_v2.0.50727_32 - ok
15:33:37.0830 4080     clr_optimization_v2.0.50727_64
(d1ceea2b47cb998321c579651ce3e4f8)
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
```

```
15:33:37.0830 4080     clr_optimization_v2.0.50727_64 - ok
15:33:37.0892 4080     clr_optimization_v4.0.30319_32
(c5a75eb48e2344abdc162bda79e16841)
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
15:33:37.0896 4080     clr_optimization_v4.0.30319_32 - ok
15:33:37.0917 4080     clr_optimization_v4.0.30319_64
(c6f9af94dcd58122a4d7e89db6bed29d)
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
15:33:37.0919 4080     clr_optimization_v4.0.30319_64 - ok
15:33:37.0943 4080     CmBatt          (0840155d0bddf1190f84a663c284bd33)
C:\Windows\system32\DRIVERS\CmBatt.sys
15:33:37.0943 4080     CmBatt - ok
15:33:37.0970 4080     cmdide          (e19d3f095812725d88f9001985b94edd)
C:\Windows\system32\drivers\cmdide.sys
15:33:37.0972 4080     cmdide - ok
15:33:38.0013 4080     CNG             (c4943b6c962e4b82197542447ad599f4)
C:\Windows\system32\Drivers\cng.sys
15:33:38.0017 4080     CNG - ok
15:33:38.0027 4080     Compbatt        (102de219c3f61415f964c88e9085ad14)
C:\Windows\system32\DRIVERS\compbatt.sys
15:33:38.0029 4080     Compbatt - ok
15:33:38.0066 4080     CompositeBus    (03edb043586cceba243d689bdda370a8)
C:\Windows\system32\drivers\CompositeBus.sys
15:33:38.0068 4080     CompositeBus - ok
15:33:38.0076 4080     COMSysApp - ok
15:33:38.0099 4080     crcdisk         (1c827878a998c18847245fe1f34ee597)
C:\Windows\system32\DRIVERS\crcdisk.sys
15:33:38.0101 4080     crcdisk - ok
15:33:38.0142 4080     CryptSvc        (4f5414602e2544a4554d95517948b705)
C:\Windows\system32\cryptsvc.dll
15:33:38.0148 4080     CryptSvc - ok
15:33:38.0207 4080     CSC             (54da3dfd29ed9f1619b6f53f3ce55e49)
C:\Windows\system32\drivers\csc.sys
15:33:38.0210 4080     CSC - ok
15:33:38.0253 4080     CscService      (3ab183ab4d2c79dcf459cd2c1266b043)
C:\Windows\System32\cscsvc.dll
15:33:38.0259 4080     CscService - ok
15:33:38.0298 4080     DcomLaunch      (5c627d1b1138676c0a7ab2c2c190d123)
C:\Windows\system32\rpcss.dll
15:33:38.0304 4080     DcomLaunch - ok
15:33:38.0333 4080     defragsvc       (3cec7631a84943677aa8fa8ee5b6b43d)
C:\Windows\System32\defragsvc.dll
15:33:38.0337 4080     defragsvc - ok
15:33:38.0402 4080     DfsC            (9bb2ef44eaa163b29c4a4587887a0fe4)
C:\Windows\system32\Drivers\dfsc.sys
15:33:38.0402 4080     DfsC - ok
15:33:38.0425 4080     Dhcp            (43d808f5d9e1a18e5eeb5ebc83969e4e)
C:\Windows\system32\dhcpcore.dll
15:33:38.0429 4080     Dhcp - ok
15:33:38.0462 4080     discache        (13096b05847ec78f0977f2c0f79e9ab3)
C:\Windows\system32\drivers\discache.sys
15:33:38.0494 4080     discache - ok
15:33:38.0511 4080     Disk            (9819eee8b5ea3784ec4af3b137a5244c)
C:\Windows\system32\DRIVERS\disk.sys
15:33:38.0511 4080     Disk - ok
15:33:38.0542 4080     Dnscache        (16835866aaa693c7d7fceba8fff706e4)
C:\Windows\System32\dnsrslvr.dll
15:33:38.0546 4080     Dnscache - ok
```

```
15:33:38.0582 4080     dot3svc         (b1fb3ddca0fdf408750d5843591afbc6)
C:\Windows\System32\dot3svc.dll
15:33:38.0583 4080     dot3svc - ok
15:33:38.0615 4080     DPS             (b26f4f737e8f9df4f31af6cf31d05820)
C:\Windows\system32\dps.dll
15:33:38.0617 4080     DPS - ok
15:33:38.0640 4080     drmkaud         (9b19f34400d24df84c858a421c205754)
C:\Windows\system32\drivers\drmkaud.sys
15:33:38.0642 4080     drmkaud - ok
15:33:38.0734 4080     DXGKrnl         (f5bee30450e18e6b83a5012c100616fd)
C:\Windows\System32\drivers\dxgkrnl.sys
15:33:38.0751 4080     DXGKrnl - ok
15:33:38.0767 4080     EagleX64 - ok
15:33:38.0802 4080     eamonm          (398fdc5694f2ba9e51e321ca40d1706e)
C:\Windows\system32\DRIVERS\eamonm.sys
15:33:38.0804 4080     eamonm - ok
15:33:38.0830 4080     EapHost         (e2dda8726da9cb5b2c4000c9018a9633)
C:\Windows\System32\eapsvc.dll
15:33:38.0832 4080     EapHost - ok
15:33:38.0996 4080     ebdrv           (dc5d737f51be844d8c82c695eb17372f)
C:\Windows\system32\DRIVERS\evbda.sys
15:33:39.0021 4080     ebdrv - ok
15:33:39.0113 4080     EFS             (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\System32\lsass.exe
15:33:39.0115 4080     EFS - ok
15:33:39.0148 4080     ehdrv           (e99457900012b53b2226f146ecaf9136)
C:\Windows\system32\DRIVERS\ehdrv.sys
15:33:39.0150 4080     ehdrv - ok
15:33:39.0218 4080     ehRecvr         (c4002b6b41975f057d98c439030cea07)
C:\Windows\ehome\ehRecvr.exe
15:33:39.0224 4080     ehRecvr - ok
15:33:39.0263 4080     ehSched         (4705e8ef9934482c5bb488ce28afc681)
C:\Windows\ehome\ehsched.exe
15:33:39.0265 4080     ehSched - ok
15:33:39.0330 4080     EhttpSrv        (11c3ad68dcf80201c9f74edee6da3804)
C:\Program Files\ESET\ESET NOD32 Antivirus\EHttpSrv.exe
15:33:39.0330 4080     EhttpSrv - ok
15:33:39.0414 4080     ekrn            (efa198f8983d064a81052851f7bb80c2)
C:\Program Files\ESET\ESET NOD32 Antivirus\x86\ekrn.exe
15:33:39.0425 4080     ekrn - ok
15:33:39.0550 4080     elxstor         (0e5da5369a0fcaea12456dd852545184)
C:\Windows\system32\DRIVERS\elxstor.sys
15:33:39.0554 4080     elxstor - ok
15:33:39.0576 4080     epfwwfpr        (a2af094dcbe8bff7e898d327750506a0)
C:\Windows\system32\DRIVERS\epfwwfpr.sys
15:33:39.0578 4080     epfwwfpr - ok
15:33:39.0603 4080     ErrDev          (34a3c54752046e79a126e15c51db409b)
C:\Windows\system32\drivers\errdev.sys
15:33:39.0605 4080     ErrDev - ok
15:33:39.0648 4080     EventSystem     (4166f82be4d24938977dd1746be9b8a0)
C:\Windows\system32\es.dll
15:33:39.0652 4080     EventSystem - ok
15:33:39.0671 4080     exfat           (a510c654ec00c1e9bdd91eeb3a59823b)
C:\Windows\system32\drivers\exfat.sys
15:33:39.0705 4080     exfat - ok
15:33:39.0734 4080     fastfat         (0adc83218b66a6db380c330836f3e36d)
C:\Windows\system32\drivers\fastfat.sys
15:33:39.0736 4080     fastfat - ok
```

```
15:33:39.0785 4080     Fax             (dbefd454f8318a0ef691fdd2eaab44eb)
C:\Windows\system32\fxssvc.exe
15:33:39.0791 4080     Fax - ok
15:33:39.0798 4080     fdc             (d765d19cd8ef61f650c384f62fac00ab)
C:\Windows\system32\DRIVERS\fdc.sys
15:33:39.0800 4080     fdc - ok
15:33:39.0808 4080     fdPHost         (0438cab2e03f4fb61455a7956026fe86)
C:\Windows\system32\fdPHost.dll
15:33:39.0810 4080     fdPHost - ok
15:33:39.0820 4080     FDResPub        (802496cb59a30349f9a6dd22d6947644)
C:\Windows\system32\fdrespub.dll
15:33:39.0822 4080     FDResPub - ok
15:33:39.0855 4080     FileInfo        (655661be46b5f5f3fd454e2c3095b930)
C:\Windows\system32\drivers\fileinfo.sys
15:33:39.0855 4080     FileInfo - ok
15:33:39.0869 4080     Filetrace       (5f671ab5bc87eea04ec38a6cd5962a47)
C:\Windows\system32\drivers\filetrace.sys
15:33:39.0869 4080     Filetrace - ok
15:33:39.0886 4080     flpydisk        (c172a0f53008eaeb8ea33fe10e177af5)
C:\Windows\system32\DRIVERS\flpydisk.sys
15:33:39.0886 4080     flpydisk - ok
15:33:39.0916 4080     FltMgr          (da6b67270fd9db3697b20fce94950741)
C:\Windows\system32\drivers\fltmgr.sys
15:33:39.0919 4080     FltMgr - ok
15:33:39.0998 4080     FontCache       (5c4cb4086fb83115b153e47add961a0c)
C:\Windows\system32\FntCache.dll
15:33:40.0007 4080     FontCache - ok
15:33:40.0078 4080     FontCache3.0.0.0
(a8b7f3818ab65695e3a0bb3279f6dce6)
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
15:33:40.0080 4080     FontCache3.0.0.0 - ok
15:33:40.0115 4080     FsDepends       (d4370349614997189070 3b4b1b723eac)
C:\Windows\system32\drivers\FsDepends.sys
15:33:40.0115 4080     FsDepends - ok
15:33:40.0142 4080     Fs_Rec          (6bd9295cc032dd3077c671fccf579a7b)
C:\Windows\system32\drivers\Fs_Rec.sys
15:33:40.0144 4080     Fs_Rec - ok
15:33:40.0187 4080     fvevol          (1f7b25b858fa27015169fe95e54108ed)
C:\Windows\system32\DRIVERS\fvevol.sys
15:33:40.0189 4080     fvevol - ok
15:33:40.0207 4080     gagp30kx        (8c778d335c9d272cfd3298ab02abe3b6)
C:\Windows\system32\DRIVERS\gagp30kx.sys
15:33:40.0208 4080     gagp30kx - ok
15:33:40.0255 4080     gpsvc           (277bbc7e1aa1ee957f573a10eca7ef3a)
C:\Windows\System32\gpsvc.dll
15:33:40.0261 4080     gpsvc - ok
15:33:40.0271 4080     hcw85cir        (f2523ef6460fc42405b12248338ab2f0)
C:\Windows\system32\drivers\hcw85cir.sys
15:33:40.0271 4080     hcw85cir - ok
15:33:40.0306 4080     HdAudAddService (975761c778e33cd22498059b91e7373a)
C:\Windows\system32\drivers\HdAudio.sys
15:33:40.0310 4080     HdAudAddService - ok
15:33:40.0355 4080     HDAudBus        (97bfed39b6b79eb12cddbfeed51f56bb)
C:\Windows\system32\drivers\HDAudBus.sys
15:33:40.0361 4080     HDAudBus - ok
15:33:40.0378 4080     HidBatt         (78e86380454a7b10a5eb255dc44a355f)
C:\Windows\system32\DRIVERS\HidBatt.sys
15:33:40.0380 4080     HidBatt - ok
```

```
15:33:40.0408 4080     HidBth          (7fd2a313f7afe5c4dab14798c48dd104)
C:\Windows\system32\DRIVERS\hidbth.sys
15:33:40.0410 4080     HidBth - ok
15:33:40.0439 4080     HidIr           (0a77d29f311b88cfae3b13f9c1a73825)
C:\Windows\system32\DRIVERS\hidir.sys
15:33:40.0441 4080     HidIr - ok
15:33:40.0455 4080     hidserv         (bd9eb3958f213f96b97b1d897dee006d)
C:\Windows\system32\hidserv.dll
15:33:40.0457 4080     hidserv - ok
15:33:40.0478 4080     HidUsb          (9592090a7e2b61cd582b612b6df70536)
C:\Windows\system32\DRIVERS\hidusb.sys
15:33:40.0480 4080     HidUsb - ok
15:33:40.0505 4080     hkmsvc          (387e72e739e15e3d37907a86d9ff98e2)
C:\Windows\system32\kmsvc.dll
15:33:40.0509 4080     hkmsvc - ok
15:33:40.0533 4080     HomeGroupListener
(efdfb3dd38a4376f93e7985173813abd) C:\Windows\system32\ListSvc.dll
15:33:40.0537 4080     HomeGroupListener - ok
15:33:40.0572 4080     HomeGroupProvider
(908acb1f594274965a53926b10c81e89) C:\Windows\system32\provsvc.dll
15:33:40.0574 4080     HomeGroupProvider - ok
15:33:40.0601 4080     HpSAMD          (39d2abcd392f3d8a6dce7b60ae7b8efc)
C:\Windows\system32\drivers\HpSAMD.sys
15:33:40.0605 4080     HpSAMD - ok
15:33:40.0658 4080     HTTP            (0ea7de1acb728dd5a369fd742d6eee28)
C:\Windows\system32\drivers\HTTP.sys
15:33:40.0664 4080     HTTP - ok
15:33:40.0703 4080     hwpolicy        (a5462bd6884960c9dc85ed49d34ff392)
C:\Windows\system32\drivers\hwpolicy.sys
15:33:40.0720 4080     hwpolicy - ok
15:33:40.0746 4080     i8042prt        (fa55c73d4affa7ee23ac4be53b4592d3)
C:\Windows\system32\drivers\i8042prt.sys
15:33:40.0748 4080     i8042prt - ok
15:33:40.0800 4080     iaStorV         (aaaf44db3bd0b9d1fb6969b23ecc8366)
C:\Windows\system32\drivers\iaStorV.sys
15:33:40.0804 4080     iaStorV - ok
15:33:40.0900 4080     idsvc           (5988fc40f8db5b0739cd1e3a5d0d78bd)
C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\infocard.exe
15:33:40.0906 4080     idsvc - ok
15:33:40.0931 4080     iirsp           (5c18831c61933628f5bb0ea2675b9d21)
C:\Windows\system32\DRIVERS\iirsp.sys
15:33:40.0933 4080     iirsp - ok
15:33:40.0984 4080     IKEEXT          (fcd84c381e0140af901e58d48882d26b)
C:\Windows\System32\ikeext.dll
15:33:40.0990 4080     IKEEXT - ok
15:33:41.0115 4080     IntcAzAudAddService
(e8017f1662d9142f45ceab694d013c00)
C:\Windows\system32\drivers\RTKVHD64.sys
15:33:41.0132 4080     IntcAzAudAddService - ok
15:33:41.0251 4080     intelide        (f00f20e70c6ec3aa366910083a0518aa)
C:\Windows\system32\drivers\intelide.sys
15:33:41.0251 4080     intelide - ok
15:33:41.0279 4080     intelppm        (ada036632c664caa754079041cf1f8c1)
C:\Windows\system32\DRIVERS\intelppm.sys
15:33:41.0281 4080     intelppm - ok
15:33:41.0312 4080     IPBusEnum       (098a91c54546a3b878dad6a7e90a455b)
C:\Windows\system32\ipbusenum.dll
```

```
15:33:41.0316 4080     IPBusEnum - ok
15:33:41.0355 4080     IpFilterDriver  (c9f0e1bd74365a8771590e9008d22ab6)
C:\Windows\system32\DRIVERS\ipfltdrv.sys
15:33:41.0357 4080     IpFilterDriver - ok
15:33:41.0388 4080     iphlpsvc        (a34a587fffd45fa649fba6d03784d257)
C:\Windows\System32\iphlpsvc.dll
15:33:41.0394 4080     iphlpsvc - ok
15:33:41.0427 4080     IPMIDRV         (0fc1aea580957aa8817b8f305d18ca3a)
C:\Windows\system32\drivers\IPMIDrv.sys
15:33:41.0431 4080     IPMIDRV - ok
15:33:41.0445 4080     IPNAT           (af9b39a7e7b6caa203b3862582e9f2d0)
C:\Windows\system32\drivers\ipnat.sys
15:33:41.0468 4080     IPNAT - ok
15:33:41.0478 4080     IRENUM          (3abf5e7213eb28966d55d58b515d5ce9)
C:\Windows\system32\drivers\irenum.sys
15:33:41.0478 4080     IRENUM - ok
15:33:41.0501 4080     isapnp          (2f7b28dc3e1183e5eb418df55c204f38)
C:\Windows\system32\drivers\isapnp.sys
15:33:41.0503 4080     isapnp - ok
15:33:41.0533 4080     iScsiPrt        (d931d7309deb2317035b07c9f9e6b0bd)
C:\Windows\system32\drivers\msiscsi.sys
15:33:41.0535 4080     iScsiPrt - ok
15:33:41.0562 4080     kbdclass        (bc02336f1cba7dcc7d1213bb588a68a5)
C:\Windows\system32\DRIVERS\kbdclass.sys
15:33:41.0564 4080     kbdclass - ok
15:33:41.0621 4080     kbdhid          (0705eff5b42a9db58548eec3b26bb484)
C:\Windows\system32\DRIVERS\kbdhid.sys
15:33:41.0621 4080     kbdhid - ok
15:33:41.0646 4080     KeyIso          (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:33:41.0648 4080     KeyIso - ok
15:33:41.0658 4080     KSecDD          (da1e991a61cfdd755a589e206b97644b)
C:\Windows\system32\Drivers\ksecdd.sys
15:33:41.0660 4080     KSecDD - ok
15:33:41.0683 4080     KSecPkg         (7e33198d956943a4f11a5474c1e9106f)
C:\Windows\system32\Drivers\ksecpkg.sys
15:33:41.0683 4080     KSecPkg - ok
15:33:41.0695 4080     ksthunk         (6869281e78cb31a43e969f06b57347c4)
C:\Windows\system32\drivers\ksthunk.sys
15:33:41.0695 4080     ksthunk - ok
15:33:41.0728 4080     KtmRm           (6ab66e16aa859232f64deb66887a8c9c)
C:\Windows\system32\msdtckrm.dll
15:33:41.0732 4080     KtmRm - ok
15:33:41.0775 4080     LanmanServer    (d9f42719019740baa6d1c6d536cbdaa6)
C:\Windows\system32\srvsvc.dll
15:33:41.0779 4080     LanmanServer - ok
15:33:41.0806 4080     LanmanWorkstation
(851a1382eed3e3a7476db004f4ee3e1a) C:\Windows\System32\wkssvc.dll
15:33:41.0810 4080     LanmanWorkstation - ok
15:33:41.0826 4080     lltdio          (1538831cf8ad2979a04c423779465827)
C:\Windows\system32\DRIVERS\lltdio.sys
15:33:41.0826 4080     lltdio - ok
15:33:41.0857 4080     lltdsvc         (c1185803384ab3feed115f79f109427f)
C:\Windows\System32\lltdsvc.dll
15:33:41.0859 4080     lltdsvc - ok
15:33:41.0875 4080     lmhosts         (f993a32249b66c9d622ea5592a8b76b8)
C:\Windows\System32\lmhsvc.dll
15:33:41.0876 4080     lmhosts - ok
```

```
15:33:41.0902 4080     LSI_FC          (1a93e54eb0ece102495a51266dcdb6a6)
C:\Windows\system32\DRIVERS\lsi_fc.sys
15:33:41.0902 4080     LSI_FC - ok
15:33:41.0923 4080     LSI_SAS         (1047184a9fdc8bdbff857175875ee810)
C:\Windows\system32\DRIVERS\lsi_sas.sys
15:33:41.0939 4080     LSI_SAS - ok
15:33:41.0951 4080     LSI_SAS2        (30f5c0de1ee8b5bc9306c1f0e4a75f93)
C:\Windows\system32\DRIVERS\lsi_sas2.sys
15:33:41.0951 4080     LSI_SAS2 - ok
15:33:41.0966 4080     LSI_SCSI        (0504eacaff0d3c8aed161c4b0d369d4a)
C:\Windows\system32\DRIVERS\lsi_scsi.sys
15:33:41.0968 4080     LSI_SCSI - ok
15:33:41.0988 4080     luafv           (43d0f98e1d56ccddb0d5254cff7b356e)
C:\Windows\system32\drivers\luafv.sys
15:33:41.0992 4080     luafv - ok
15:33:42.0025 4080     MBAMProtector   (dbc08862a71459e74f7538b432c114cc)
C:\Windows\system32\drivers\mbam.sys
15:33:42.0025 4080     MBAMProtector - ok
15:33:42.0099 4080     MBAMService     (ba400ed640bca1eae5c727ae17c10207)
C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamservice.exe
15:33:42.0109 4080     MBAMService - ok
15:33:42.0138 4080     Mcx2Svc         (0be09cd858abf9df6ed259d57a1a1663)
C:\Windows\system32\Mcx2Svc.dll
15:33:42.0142 4080     Mcx2Svc - ok
15:33:42.0166 4080     megasas         (a55805f747c6edb6a9080d7c633bd0f4)
C:\Windows\system32\DRIVERS\megasas.sys
15:33:42.0205 4080     megasas - ok
15:33:42.0271 4080     MegaSR          (baf74ce0072480c3b6b7c13b2a94d6b3)
C:\Windows\system32\DRIVERS\MegaSR.sys
15:33:42.0273 4080     MegaSR - ok
15:33:42.0308 4080     Microsoft SharePoint Workspace Audit Service - ok
15:33:42.0328 4080     MMCSS           (e40e80d0304a73e8d269f7141d77250b)
C:\Windows\system32\mmcss.dll
15:33:42.0332 4080     MMCSS - ok
15:33:42.0341 4080     Modem           (800ba92f7010378b09f9ed9270f07137)
C:\Windows\system32\drivers\modem.sys
15:33:42.0343 4080     Modem - ok
15:33:42.0382 4080     monitor         (b03d591dc7da45ece20b3b467e6aadaa)
C:\Windows\system32\DRIVERS\monitor.sys
15:33:42.0384 4080     monitor - ok
15:33:42.0425 4080     mouclass        (7d27ea49f3c1f687d357e77a470aea99)
C:\Windows\system32\DRIVERS\mouclass.sys
15:33:42.0427 4080     mouclass - ok
15:33:42.0451 4080     mouhid          (d3bf052c40b0c4166d9fd86a4288c1e6)
C:\Windows\system32\DRIVERS\mouhid.sys
15:33:42.0453 4080     mouhid - ok
15:33:42.0474 4080     mountmgr        (32e7a3d591d671a6df2db515a5cbe0fa)
C:\Windows\system32\drivers\mountmgr.sys
15:33:42.0496 4080     mountmgr - ok
15:33:42.0535 4080     MozillaMaintenance
(15d5398eed42c2504bb3d4fc875c15d1) C:\Program Files (x86)\Mozilla
Maintenance Service\maintenanceservice.exe
15:33:42.0537 4080     MozillaMaintenance - ok
15:33:42.0566 4080     mpio            (a44b420d30bd56e145d6a2bc8768ec58)
C:\Windows\system32\drivers\mpio.sys
15:33:42.0566 4080     mpio - ok
15:33:42.0582 4080     mpsdrv          (6c38c9e45ae0ea2fa5e551f2ed5e978f)
C:\Windows\system32\drivers\mpsdrv.sys
```

```
15:33:42.0599 4080     mpsdrv - ok
15:33:42.0652 4080     MpsSvc          (54ffc9c8898113ace189d4aa7199d2c1)
C:\Windows\system32\mpssvc.dll
15:33:42.0660 4080     MpsSvc - ok
15:33:42.0695 4080     MRxDAV          (dc722758b8261e1abafd31a3c0a66380)
C:\Windows\system32\drivers\mrxdav.sys
15:33:42.0697 4080     MRxDAV - ok
15:33:42.0720 4080     mrxsmb          (a5d9106a73dc88564c825d317cac68ac)
C:\Windows\system32\DRIVERS\mrxsmb.sys
15:33:42.0724 4080     mrxsmb - ok
15:33:42.0761 4080     mrxsmb10        (d711b3c1d5f42c0c2415687be09fc163)
C:\Windows\system32\DRIVERS\mrxsmb10.sys
15:33:42.0763 4080     mrxsmb10 - ok
15:33:42.0787 4080     mrxsmb20        (9423e9d355c8d303e76b8cfbd8a5c30c)
C:\Windows\system32\DRIVERS\mrxsmb20.sys
15:33:42.0787 4080     mrxsmb20 - ok
15:33:42.0806 4080     msahci          (c25f0bafa182cbca2dd3c851c2e75796)
C:\Windows\system32\drivers\msahci.sys
15:33:42.0808 4080     msahci - ok
15:33:42.0832 4080     msdsm           (db801a638d011b9633829eb6f663c900)
C:\Windows\system32\drivers\msdsm.sys
15:33:42.0849 4080     msdsm - ok
15:33:42.0878 4080     MSDTC           (de0ece52236cfa3ed2dbfc03f28253a8)
C:\Windows\System32\msdtc.exe
15:33:42.0880 4080     MSDTC - ok
15:33:42.0923 4080     Msfs            (aa3fb40e17ce1388fa1bedab50ea8f96)
C:\Windows\system32\drivers\Msfs.sys
15:33:42.0925 4080     Msfs - ok
15:33:42.0933 4080     mshidkmdf       (f9d215a46a8b9753f61767fa72a20326)
C:\Windows\System32\drivers\mshidkmdf.sys
15:33:42.0935 4080     mshidkmdf - ok
15:33:42.0955 4080     msisadrv        (d916874bbd4f8b07bfb7fa9b3ccae29d)
C:\Windows\system32\drivers\msisadrv.sys
15:33:42.0955 4080     msisadrv - ok
15:33:42.0980 4080     MSiSCSI         (808e98ff49b155c522e6400953177b08)
C:\Windows\system32\iscsiexe.dll
15:33:42.0982 4080     MSiSCSI - ok
15:33:42.0986 4080     msiserver - ok
15:33:43.0000 4080     MSKSSRV         (49ccf2c4fea34ffad8b1b59d49439366)
C:\Windows\system32\drivers\MSKSSRV.sys
15:33:43.0001 4080     MSKSSRV - ok
15:33:43.0015 4080     MSPCLOCK        (bdd71ace35a232104ddd349ee70e1ab3)
C:\Windows\system32\drivers\MSPCLOCK.sys
15:33:43.0015 4080     MSPCLOCK - ok
15:33:43.0019 4080     MSPQM           (4ed981241db27c3383d72092b618a1d0)
C:\Windows\system32\drivers\MSPQM.sys
15:33:43.0039 4080     MSPQM - ok
15:33:43.0074 4080     MsRPC           (759a9eeb0fa9ed79da1fb7d4ef78866d)
C:\Windows\system32\drivers\MsRPC.sys
15:33:43.0078 4080     MsRPC - ok
15:33:43.0099 4080     mssmbios        (0eed230e37515a0eaee3c2e1bc97b288)
C:\Windows\system32\drivers\mssmbios.sys
15:33:43.0099 4080     mssmbios - ok
15:33:43.0109 4080     MSTEE           (2e66f9ecb30b4221a318c92ac2250779)
C:\Windows\system32\drivers\MSTEE.sys
15:33:43.0109 4080     MSTEE - ok
15:33:43.0125 4080     MTConfig        (7ea404308934e675bffde8edf0757bcd)
C:\Windows\system32\DRIVERS\MTConfig.sys
```

```
15:33:43.0126 4080     MTConfig - ok
15:33:43.0144 4080     Mup             (f9a18612fd3526fe473c1bda678d61c8)
C:\Windows\system32\Drivers\mup.sys
15:33:43.0144 4080     Mup - ok
15:33:43.0173 4080     napagent        (582ac6d9873e31dfa28a4547270862dd)
C:\Windows\system32\qagentRT.dll
15:33:43.0179 4080     napagent - ok
15:33:43.0205 4080     NativeWifiP     (1ea3749c4114db3e3161156ffffa6b33)
C:\Windows\system32\DRIVERS\nwifi.sys
15:33:43.0208 4080     NativeWifiP - ok
15:33:43.0261 4080     NDIS            (79b47fd40d9a817e932f9d26fac0a81c)
C:\Windows\system32\drivers\ndis.sys
15:33:43.0269 4080     NDIS - ok
15:33:43.0283 4080     NdisCap         (9f9a1f53aad7da4d6fef5bb73ab811ac)
C:\Windows\system32\DRIVERS\ndiscap.sys
15:33:43.0283 4080     NdisCap - ok
15:33:43.0292 4080     NdisTapi        (30639c932d9fef22b31268fe25a1b6e5)
C:\Windows\system32\DRIVERS\ndistapi.sys
15:33:43.0292 4080     NdisTapi - ok
15:33:43.0316 4080     Ndisuio         (136185f9fb2cc61e573e676aa5402356)
C:\Windows\system32\DRIVERS\ndisuio.sys
15:33:43.0318 4080     Ndisuio - ok
15:33:43.0345 4080     NdisWan         (53f7305169863f0a2bddc49e116c2e11)
C:\Windows\system32\DRIVERS\ndiswan.sys
15:33:43.0345 4080     NdisWan - ok
15:33:43.0357 4080     NDProxy         (015c0d8e0e0421b4cfd48cffe2825879)
C:\Windows\system32\drivers\NDProxy.sys
15:33:43.0357 4080     NDProxy - ok
15:33:43.0369 4080     NetBIOS         (86743d9f5d2b1048062b14b1d84501c4)
C:\Windows\system32\DRIVERS\netbios.sys
15:33:43.0384 4080     NetBIOS - ok
15:33:43.0435 4080     NetBT           (09594d1089c523423b32a4229263f068)
C:\Windows\system32\DRIVERS\netbt.sys
15:33:43.0476 4080     NetBT - ok
15:33:43.0480 4080     Scan interrupted by user!
15:33:43.0480 4080     Scan interrupted by user!
15:33:43.0480 4080     Scan interrupted by user!
15:33:43.0480 4080
      ============================================================
15:33:43.0480 4080     Scan finished
15:33:43.0480 4080
      ============================================================
15:33:43.0509 0324     Detected object count: 0
15:33:43.0511 0324     Actual detected object count: 0
15:33:45.0611 3616
      ============================================================
15:33:45.0611 3616     Scan started
15:33:45.0611 3616     Mode: Manual;
15:33:45.0611 3616
      ============================================================
15:33:45.0945 3616     1394ohci        (a87d604aea360176311474c87a63bb88)
C:\Windows\system32\drivers\1394ohci.sys
15:33:45.0947 3616     1394ohci - ok
15:33:45.0980 3616     ACPI            (d81d9e70b8a6dd14d42d7b4efa65d5f2)
C:\Windows\system32\drivers\ACPI.sys
15:33:45.0982 3616     ACPI - ok
15:33:46.0000 3616     AcpiPmi         (99f8e788246d495ce3794d7e7821d2ca)
C:\Windows\system32\drivers\acpipmi.sys
```

```
15:33:46.0000 3616     AcpiPmi - ok
15:33:46.0054 3616     AdobeARMservice (11a52cf7b265631deeb24c6149309eff)
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
15:33:46.0056 3616     AdobeARMservice - ok
15:33:46.0125 3616     AdobeFlashPlayerUpdateSvc
(76d5a3d2a50402a0b9b6ed13c4371e79)
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
15:33:46.0126 3616     AdobeFlashPlayerUpdateSvc - ok
15:33:46.0169 3616     adp94xx         (2f6b34b83843f0c5118b63ac634f5bf4)
C:\Windows\system32\DRIVERS\adp94xx.sys
15:33:46.0173 3616     adp94xx - ok
15:33:46.0207 3616     adpahci         (597f78224ee9224ea1a13d6350ced962)
C:\Windows\system32\DRIVERS\adpahci.sys
15:33:46.0208 3616     adpahci - ok
15:33:46.0240 3616     adpu320         (e109549c90f62fb570b9540c4b148e54)
C:\Windows\system32\DRIVERS\adpu320.sys
15:33:46.0240 3616     adpu320 - ok
15:33:46.0261 3616     AeLookupSvc     (4b78b431f225fd8624c5655cb1de7b61)
C:\Windows\System32\aelupsvc.dll
15:33:46.0261 3616     AeLookupSvc - ok
15:33:46.0302 3616     AFD             (1c7857b62de5994a75b054a9fd4c3825)
C:\Windows\system32\drivers\afd.sys
15:33:46.0306 3616     AFD - ok
15:33:46.0328 3616     agp440          (608c14dba7299d8cb6ed035a68a15799)
C:\Windows\system32\drivers\agp440.sys
15:33:46.0330 3616     agp440 - ok
15:33:46.0343 3616     ALG             (3290d6946b5e30e70414990574883ddb)
C:\Windows\System32\alg.exe
15:33:46.0345 3616     ALG - ok
15:33:46.0355 3616     aliide          (5812713a477a3ad7363c7438ca2ee038)
C:\Windows\system32\drivers\aliide.sys
15:33:46.0355 3616     aliide - ok
15:33:46.0361 3616     amdide          (1ff8b4431c353ce385c875f194924c0c)
C:\Windows\system32\drivers\amdide.sys
15:33:46.0363 3616     amdide - ok
15:33:46.0375 3616     AmdK8           (7024f087cff1833a806193ef9d22cda9)
C:\Windows\system32\DRIVERS\amdk8.sys
15:33:46.0375 3616     AmdK8 - ok
15:33:46.0382 3616     AmdPPM          (1e56388b3fe0d031c44144eb8c4d6217)
C:\Windows\system32\DRIVERS\amdppm.sys
15:33:46.0384 3616     AmdPPM - ok
15:33:46.0410 3616     amdsata         (d4121ae6d0c0e7e13aa221aa57ef2d49)
C:\Windows\system32\drivers\amdsata.sys
15:33:46.0410 3616     amdsata - ok
15:33:46.0429 3616     amdsbs          (f67f933e79241ed32ff46a4f29b5120b)
C:\Windows\system32\DRIVERS\amdsbs.sys
15:33:46.0431 3616     amdsbs - ok
15:33:46.0447 3616     amdxata         (540daf1cea6094886d72126fd7c33048)
C:\Windows\system32\drivers\amdxata.sys
15:33:46.0449 3616     amdxata - ok
15:33:46.0468 3616     AppID           (89a69c3f2f319b43379399547526d952)
C:\Windows\system32\drivers\appid.sys
15:33:46.0470 3616     AppID - ok
15:33:46.0494 3616     AppIDSvc        (0bc381a15355a3982216f7172f545de1)
C:\Windows\System32\appidsvc.dll
15:33:46.0496 3616     AppIDSvc - ok
15:33:46.0515 3616     Appinfo         (3977d4a871ca0d4f2ed1e7db46829731)
C:\Windows\System32\appinfo.dll
```

```
15:33:46.0517 3616     Appinfo - ok
15:33:46.0544 3616     AppMgmt         (4aba3e75a76195a3e38ed2766c962899)
C:\Windows\System32\appmgmts.dll
15:33:46.0546 3616     AppMgmt - ok
15:33:46.0580 3616     arc             (c484f8ceb1717c540242531db7845c4e)
C:\Windows\system32\DRIVERS\arc.sys
15:33:46.0582 3616     arc - ok
15:33:46.0589 3616     arcsas          (019af6924aefe7839f61c830227fe79c)
C:\Windows\system32\DRIVERS\arcsas.sys
15:33:46.0589 3616     arcsas - ok
15:33:46.0617 3616     AsyncMac        (769765ce2cc62867468cea93969b2242)
C:\Windows\system32\DRIVERS\asyncmac.sys
15:33:46.0617 3616     AsyncMac - ok
15:33:46.0644 3616     atapi           (02062c0b390b7729edc9e69c680a6f3c)
C:\Windows\system32\drivers\atapi.sys
15:33:46.0646 3616     atapi - ok
15:33:46.0697 3616     AudioEndpointBuilder
(f23fef6d569fce88671949894a8becf1) C:\Windows\System32\Audiosrv.dll
15:33:46.0701 3616     AudioEndpointBuilder - ok
15:33:46.0710 3616     AudioSrv        (f23fef6d569fce88671949894a8becf1)
C:\Windows\System32\Audiosrv.dll
15:33:46.0714 3616     AudioSrv - ok
15:33:46.0736 3616     AxInstSV        (a6bf31a71b409dfa8cac83159e1e2aff)
C:\Windows\System32\AxInstSV.dll
15:33:46.0736 3616     AxInstSV - ok
15:33:46.0753 3616     Axtmvflt        (344b907477ff1bc01bd315ab93df9764)
C:\Windows\system32\DRIVERS\Axtmvflt.sys
15:33:46.0755 3616     Axtmvflt - ok
15:33:46.0769 3616     Axtmvmdm        (4f8d9a8c04c33496403cc4dde3e9d6ce)
C:\Windows\system32\DRIVERS\Axtmvmdm.sys
15:33:46.0769 3616     Axtmvmdm - ok
15:33:46.0781 3616     Axtmvprt        (c24f39e3cc13fa14477ebe12461739ff)
C:\Windows\system32\Drivers\Axtmvprt.sys
15:33:46.0783 3616     Axtmvprt - ok
15:33:46.0816 3616     b06bdrv         (3e5b191307609f7514148c6832bb0842)
C:\Windows\system32\DRIVERS\bxvbda.sys
15:33:46.0818 3616     b06bdrv - ok
15:33:46.0845 3616     b57nd60a        (b5ace6968304a3900eeb1ebfd9622df2)
C:\Windows\system32\DRIVERS\b57nd60a.sys
15:33:46.0863 3616     b57nd60a - ok
15:33:46.0890 3616     BDESVC          (fde360167101b4e45a96f939f388aeb0)
C:\Windows\System32\bdesvc.dll
15:33:46.0890 3616     BDESVC - ok
15:33:46.0902 3616     Beep            (16a47ce2decc9b099349a5f840654746)
C:\Windows\system32\drivers\Beep.sys
15:33:46.0902 3616     Beep - ok
15:33:46.0955 3616     BFE             (82974d6a2fd19445cc5171fc378668a4)
C:\Windows\System32\bfe.dll
15:33:46.0960 3616     BFE - ok
15:33:47.0007 3616     BITS            (1ea7969e3271cbc59e1730697dc74682)
C:\Windows\System32\qmgr.dll
15:33:47.0015 3616     BITS - ok
15:33:47.0039 3616     blbdrive        (61583ee3c3a17003c4acd0475646b4d3)
C:\Windows\system32\DRIVERS\blbdrive.sys
15:33:47.0041 3616     blbdrive - ok
15:33:47.0064 3616     bowser          (6c02a83164f5cc0a262f4199f0871cf5)
C:\Windows\system32\DRIVERS\bowser.sys
15:33:47.0064 3616     bowser - ok
```

```
15:33:47.0078 3616     BrFiltLo        (f09eee9edc320b5e1501f749fde686c8)
C:\Windows\system32\DRIVERS\BrFiltLo.sys
15:33:47.0078 3616     BrFiltLo - ok
15:33:47.0093 3616     BrFiltUp        (b114d3098e9bdb8bea8b053685831be6)
C:\Windows\system32\DRIVERS\BrFiltUp.sys
15:33:47.0093 3616     BrFiltUp - ok
15:33:47.0123 3616     Browser         (8ef0d5c41ec907751b8429162b1239ed)
C:\Windows\System32\browser.dll
15:33:47.0123 3616     Browser - ok
15:33:47.0148 3616     Brserid         (43bea8d483bf1870f018e2d02e06a5bd)
C:\Windows\System32\Drivers\Brserid.sys
15:33:47.0150 3616     Brserid - ok
15:33:47.0160 3616     BrSerWdm        (a6eca2151b08a09caceca35c07f05b42)
C:\Windows\System32\Drivers\BrSerWdm.sys
15:33:47.0162 3616     BrSerWdm - ok
15:33:47.0175 3616     BrUsbMdm        (b79968002c277e869cf38bd22cd61524)
C:\Windows\System32\Drivers\BrUsbMdm.sys
15:33:47.0175 3616     BrUsbMdm - ok
15:33:47.0193 3616     BrUsbSer        (a87528880231c54e75ea7a44943b38bf)
C:\Windows\System32\Drivers\BrUsbSer.sys
15:33:47.0193 3616     BrUsbSer - ok
15:33:47.0216 3616     BthEnum         (cf98190a94f62e405c8cb255018b2315)
C:\Windows\system32\drivers\BthEnum.sys
15:33:47.0216 3616     BthEnum - ok
15:33:47.0230 3616     BTHMODEM        (9da669f11d1f894ab4eb69bf546a42e8)
C:\Windows\system32\DRIVERS\bthmodem.sys
15:33:47.0232 3616     BTHMODEM - ok
15:33:47.0283 3616     BthPan          (02dd601b708dd0667e1331fa8518e9ff)
C:\Windows\system32\DRIVERS\bthpan.sys
15:33:47.0287 3616     BthPan - ok
15:33:47.0341 3616     BTHPORT         (64c198198501f7560ee41d8d1efa7952)
C:\Windows\System32\Drivers\BTHport.sys
15:33:47.0351 3616     BTHPORT - ok
15:33:47.0384 3616     bthserv         (95f9c2976059462cbbf227f7aab10de9)
C:\Windows\system32\bthserv.dll
15:33:47.0386 3616     bthserv - ok
15:33:47.0404 3616     BTHUSB          (f188b7394d81010767b6df3178519a37)
C:\Windows\System32\Drivers\BTHUSB.sys
15:33:47.0406 3616     BTHUSB - ok
15:33:47.0419 3616     cdfs            (b8bd2bb284668c84865658c77574381a)
C:\Windows\system32\DRIVERS\cdfs.sys
15:33:47.0419 3616     cdfs - ok
15:33:47.0453 3616     cdrom           (f036ce71586e93d94dab220d7bdf4416)
C:\Windows\system32\DRIVERS\cdrom.sys
15:33:47.0455 3616     cdrom - ok
15:33:47.0482 3616     CertPropSvc     (f17d1d393bbc69c5322fbfafaca28c7f)
C:\Windows\System32\certprop.dll
15:33:47.0484 3616     CertPropSvc - ok
15:33:47.0498 3616     circlass        (d7cd5c4e1b71fa62050515314cfb52cf)
C:\Windows\system32\DRIVERS\circlass.sys
15:33:47.0500 3616     circlass - ok
15:33:47.0529 3616     CLFS            (fe1ec06f2253f691fe36217c592a0206)
C:\Windows\system32\CLFS.sys
15:33:47.0533 3616     CLFS - ok
15:33:47.0609 3616     clr_optimization_v2.0.50727_32
(d88040f816fda31c3b466f0fa0918f29)
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
15:33:47.0609 3616     clr_optimization_v2.0.50727_32 - ok
```

```
15:33:47.0654 3616     clr_optimization_v2.0.50727_64
(d1ceea2b47cb998321c579651ce3e4f8)
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
15:33:47.0656 3616     clr_optimization_v2.0.50727_64 - ok
15:33:47.0701 3616     clr_optimization_v4.0.30319_32
(c5a75eb48e2344abdc162bda79e16841)
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
15:33:47.0703 3616     clr_optimization_v4.0.30319_32 - ok
15:33:47.0726 3616     clr_optimization_v4.0.30319_64
(c6f9af94dcd58122a4d7e89db6bed29d)
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
15:33:47.0728 3616     clr_optimization_v4.0.30319_64 - ok
15:33:47.0750 3616     CmBatt          (0840155d0bddf1190f84a663c284bd33)
C:\Windows\system32\DRIVERS\CmBatt.sys
15:33:47.0751 3616     CmBatt - ok
15:33:47.0771 3616     cmdide          (e19d3f095812725d88f9001985b94edd)
C:\Windows\system32\drivers\cmdide.sys
15:33:47.0771 3616     cmdide - ok
15:33:47.0812 3616     CNG             (c4943b6c962e4b82197542447ad599f4)
C:\Windows\system32\Drivers\cng.sys
15:33:47.0816 3616     CNG - ok
15:33:47.0828 3616     Compbatt        (102de219c3f61415f964c88e9085ad14)
C:\Windows\system32\DRIVERS\compbatt.sys
15:33:47.0828 3616     Compbatt - ok
15:33:47.0857 3616     CompositeBus    (03edb043586cceba243d689bdda370a8)
C:\Windows\system32\drivers\CompositeBus.sys
15:33:47.0859 3616     CompositeBus - ok
15:33:47.0861 3616     COMSysApp - ok
15:33:47.0875 3616     crcdisk         (1c827878a998c18847245fe1f34ee597)
C:\Windows\system32\DRIVERS\crcdisk.sys
15:33:47.0875 3616     crcdisk - ok
15:33:47.0906 3616     CryptSvc        (4f5414602e2544a4554d95517948b705)
C:\Windows\system32\cryptsvc.dll
15:33:47.0908 3616     CryptSvc - ok
15:33:47.0955 3616     CSC             (54da3dfd29ed9f1619b6f53f3ce55e49)
C:\Windows\system32\drivers\csc.sys
15:33:47.0958 3616     CSC - ok
15:33:48.0009 3616     CscService      (3ab183ab4d2c79dcf459cd2c1266b043)
C:\Windows\System32\cscsvc.dll
15:33:48.0015 3616     CscService - ok
15:33:48.0056 3616     DcomLaunch      (5c627d1b1138676c0a7ab2c2c190d123)
C:\Windows\system32\rpcss.dll
15:33:48.0062 3616     DcomLaunch - ok
15:33:48.0091 3616     defragsvc       (3cec7631a84943677aa8fa8ee5b6b43d)
C:\Windows\System32\defragsvc.dll
15:33:48.0093 3616     defragsvc - ok
15:33:48.0144 3616     DfsC            (9bb2ef44eaa163b29c4a4587887a0fe4)
C:\Windows\system32\Drivers\dfsc.sys
15:33:48.0146 3616     DfsC - ok
15:33:48.0177 3616     Dhcp            (43d808f5d9e1a18e5eeb5ebc83969e4e)
C:\Windows\system32\dhcpcore.dll
15:33:48.0185 3616     Dhcp - ok
15:33:48.0214 3616     discache        (13096b05847ec78f0977f2c0f79e9ab3)
C:\Windows\system32\drivers\discache.sys
15:33:48.0255 3616     discache - ok
15:33:48.0269 3616     Disk            (9819eee8b5ea3784ec4af3b137a5244c)
C:\Windows\system32\DRIVERS\disk.sys
15:33:48.0269 3616     Disk - ok
```

```
15:33:48.0310 3616     Dnscache        (16835866aaa693c7d7fceba8fff706e4)
C:\Windows\System32\dnsrslvr.dll
15:33:48.0312 3616     Dnscache - ok
15:33:48.0347 3616     dot3svc         (b1fb3ddca0fdf408750d5843591afbc6)
C:\Windows\System32\dot3svc.dll
15:33:48.0349 3616     dot3svc - ok
15:33:48.0382 3616     DPS             (b26f4f737e8f9df4f31af6cf31d05820)
C:\Windows\system32\dps.dll
15:33:48.0382 3616     DPS - ok
15:33:48.0398 3616     drmkaud         (9b19f34400d24df84c858a421c205754)
C:\Windows\system32\drivers\drmkaud.sys
15:33:48.0400 3616     drmkaud - ok
15:33:48.0458 3616     DXGKrnl         (f5bee30450e18e6b83a5012c100616fd)
C:\Windows\System32\drivers\dxgkrnl.sys
15:33:48.0464 3616     DXGKrnl - ok
15:33:48.0470 3616     EagleX64 - ok
15:33:48.0500 3616     eamonm          (398fdc5694f2ba9e51e321ca40d1706e)
C:\Windows\system32\DRIVERS\eamonm.sys
15:33:48.0501 3616     eamonm - ok
15:33:48.0529 3616     EapHost         (e2dda8726da9cb5b2c4000c9018a9633)
C:\Windows\System32\eapsvc.dll
15:33:48.0531 3616     EapHost - ok
15:33:48.0667 3616     ebdrv           (dc5d737f51be844d8c82c695eb17372f)
C:\Windows\system32\DRIVERS\evbda.sys
15:33:48.0689 3616     ebdrv - ok
15:33:48.0773 3616     EFS             (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\System32\lsass.exe
15:33:48.0775 3616     EFS - ok
15:33:48.0808 3616     ehdrv           (e99457900012b53b2226f146ecaf9136)
C:\Windows\system32\DRIVERS\ehdrv.sys
15:33:48.0812 3616     ehdrv - ok
15:33:48.0888 3616     ehRecvr         (c4002b6b41975f057d98c439030cea07)
C:\Windows\ehome\ehRecvr.exe
15:33:48.0898 3616     ehRecvr - ok
15:33:48.0929 3616     ehSched         (4705e8ef9934482c5bb488ce28afc681)
C:\Windows\ehome\ehsched.exe
15:33:48.0931 3616     ehSched - ok
15:33:48.0978 3616     EhttpSrv        (11c3ad68dcf80201c9f74edee6da3804)
C:\Program Files\ESET\ESET NOD32 Antivirus\EHttpSrv.exe
15:33:48.0980 3616     EhttpSrv - ok
15:33:49.0054 3616     ekrn            (efa198f8983d064a81052851f7bb80c2)
C:\Program Files\ESET\ESET NOD32 Antivirus\x86\ekrn.exe
15:33:49.0062 3616     ekrn - ok
15:33:49.0158 3616     elxstor         (0e5da5369a0fcaea12456dd852545184)
C:\Windows\system32\DRIVERS\elxstor.sys
15:33:49.0162 3616     elxstor - ok
15:33:49.0183 3616     epfwwfpr        (a2af094dcbe8bff7e898d327750506a0)
C:\Windows\system32\DRIVERS\epfwwfpr.sys
15:33:49.0185 3616     epfwwfpr - ok
15:33:49.0203 3616     ErrDev          (34a3c54752046e79a126e15c51db409b)
C:\Windows\system32\drivers\errdev.sys
15:33:49.0205 3616     ErrDev - ok
15:33:49.0248 3616     EventSystem     (4166f82be4d24938977dd1746be9b8a0)
C:\Windows\system32\es.dll
15:33:49.0251 3616     EventSystem - ok
15:33:49.0273 3616     exfat           (a510c654ec00c1e9bdd91eeb3a59823b)
C:\Windows\system32\drivers\exfat.sys
15:33:49.0275 3616     exfat - ok
```

```
15:33:49.0292 3616     fastfat         (0adc83218b66a6db380c330836f3e36d)
C:\Windows\system32\drivers\fastfat.sys
15:33:49.0294 3616     fastfat - ok
15:33:49.0343 3616     Fax             (dbefd454f8318a0ef691fdd2eaab44eb)
C:\Windows\system32\fxssvc.exe
15:33:49.0349 3616     Fax - ok
15:33:49.0365 3616     fdc             (d765d19cd8ef61f650c384f62fac00ab)
C:\Windows\system32\DRIVERS\fdc.sys
15:33:49.0367 3616     fdc - ok
15:33:49.0375 3616     fdPHost         (0438cab2e03f4fb61455a7956026fe86)
C:\Windows\system32\fdPHost.dll
15:33:49.0376 3616     fdPHost - ok
15:33:49.0384 3616     FDResPub        (802496cb59a30349f9a6dd22d6947644)
C:\Windows\system32\fdrespub.dll
15:33:49.0386 3616     FDResPub - ok
15:33:49.0404 3616     FileInfo        (655661be46b5f5f3fd454e2c3095b930)
C:\Windows\system32\drivers\fileinfo.sys
15:33:49.0406 3616     FileInfo - ok
15:33:49.0417 3616     Filetrace       (5f671ab5bc87eea04ec38a6cd5962a47)
C:\Windows\system32\drivers\filetrace.sys
15:33:49.0417 3616     Filetrace - ok
15:33:49.0435 3616     flpydisk        (c172a0f53008eaeb8ea33fe10e177af5)
C:\Windows\system32\DRIVERS\flpydisk.sys
15:33:49.0437 3616     flpydisk - ok
15:33:49.0457 3616     FltMgr          (da6b67270fd9db3697b20fce94950741)
C:\Windows\system32\drivers\fltmgr.sys
15:33:49.0460 3616     FltMgr - ok
15:33:49.0539 3616     FontCache       (5c4cb4086fb83115b153e47add961a0c)
C:\Windows\system32\FntCache.dll
15:33:49.0546 3616     FontCache - ok
15:33:49.0603 3616     FontCache3.0.0.0
(a8b7f3818ab65695e3a0bb3279f6dce6)
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
15:33:49.0605 3616     FontCache3.0.0.0 - ok
15:33:49.0640 3616     FsDepends       (d43703496149971890703b4b1b723eac)
C:\Windows\system32\drivers\FsDepends.sys
15:33:49.0642 3616     FsDepends - ok
15:33:49.0660 3616     Fs_Rec          (6bd9295cc032dd3077c671fccf579a7b)
C:\Windows\system32\drivers\Fs_Rec.sys
15:33:49.0662 3616     Fs_Rec - ok
15:33:49.0687 3616     fvevol          (1f7b25b858fa27015169fe95e54108ed)
C:\Windows\system32\DRIVERS\fvevol.sys
15:33:49.0689 3616     fvevol - ok
15:33:49.0707 3616     gagp30kx        (8c778d335c9d272cfd3298ab02abe3b6)
C:\Windows\system32\DRIVERS\gagp30kx.sys
15:33:49.0707 3616     gagp30kx - ok
15:33:49.0755 3616     gpsvc           (277bbc7e1aa1ee957f573a10eca7ef3a)
C:\Windows\System32\gpsvc.dll
15:33:49.0761 3616     gpsvc - ok
15:33:49.0769 3616     hcw85cir        (f2523ef6460fc42405b12248338ab2f0)
C:\Windows\system32\drivers\hcw85cir.sys
15:33:49.0771 3616     hcw85cir - ok
15:33:49.0806 3616     HdAudAddService (975761c778e33cd22498059b91e7373a)
C:\Windows\system32\drivers\HdAudio.sys
15:33:49.0808 3616     HdAudAddService - ok
15:33:49.0835 3616     HDAudBus        (97bfed39b6b79eb12cddbfeed51f56bb)
C:\Windows\system32\drivers\HDAudBus.sys
15:33:49.0839 3616     HDAudBus - ok
```

```
15:33:49.0853 3616     HidBatt         (78e86380454a7b10a5eb255dc44a355f)
C:\Windows\system32\DRIVERS\HidBatt.sys
15:33:49.0855 3616     HidBatt - ok
15:33:49.0869 3616     HidBth          (7fd2a313f7afe5c4dab14798c48dd104)
C:\Windows\system32\DRIVERS\hidbth.sys
15:33:49.0871 3616     HidBth - ok
15:33:49.0880 3616     HidIr           (0a77d29f311b88cfae3b13f9c1a73825)
C:\Windows\system32\DRIVERS\hidir.sys
15:33:49.0880 3616     HidIr - ok
15:33:49.0906 3616     hidserv         (bd9eb3958f213f96b97b1d897dee006d)
C:\Windows\system32\hidserv.dll
15:33:49.0906 3616     hidserv - ok
15:33:49.0919 3616     HidUsb          (9592090a7e2b61cd582b612b6df70536)
C:\Windows\system32\DRIVERS\hidusb.sys
15:33:49.0921 3616     HidUsb - ok
15:33:49.0947 3616     hkmsvc          (387e72e739e15e3d37907a86d9ff98e2)
C:\Windows\system32\kmsvc.dll
15:33:49.0949 3616     hkmsvc - ok
15:33:49.0974 3616     HomeGroupListener
(efdfb3dd38a4376f93e7985173813abd) C:\Windows\system32\ListSvc.dll
15:33:49.0978 3616     HomeGroupListener - ok
15:33:50.0003 3616     HomeGroupProvider
(908acb1f594274965a53926b10c81e89) C:\Windows\system32\provsvc.dll
15:33:50.0005 3616     HomeGroupProvider - ok
15:33:50.0035 3616     HpSAMD          (39d2abcd392f3d8a6dce7b60ae7b8efc)
C:\Windows\system32\drivers\HpSAMD.sys
15:33:50.0037 3616     HpSAMD - ok
15:33:50.0089 3616     HTTP            (0ea7de1acb728dd5a369fd742d6eee28)
C:\Windows\system32\drivers\HTTP.sys
15:33:50.0093 3616     HTTP - ok
15:33:50.0101 3616     hwpolicy        (a5462bd6884960c9dc85ed49d34ff392)
C:\Windows\system32\drivers\hwpolicy.sys
15:33:50.0103 3616     hwpolicy - ok
15:33:50.0128 3616     i8042prt        (fa55c73d4affa7ee23ac4be53b4592d3)
C:\Windows\system32\drivers\i8042prt.sys
15:33:50.0130 3616     i8042prt - ok
15:33:50.0173 3616     iaStorV         (aaaf44db3bd0b9d1fb6969b23ecc8366)
C:\Windows\system32\drivers\iaStorV.sys
15:33:50.0177 3616     iaStorV - ok
15:33:50.0281 3616     idsvc           (5988fc40f8db5b0739cd1e3a5d0d78bd)
C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\infocard.exe
15:33:50.0294 3616     idsvc - ok
15:33:50.0314 3616     iirsp           (5c18831c61933628f5bb0ea2675b9d21)
C:\Windows\system32\DRIVERS\iirsp.sys
15:33:50.0316 3616     iirsp - ok
15:33:50.0367 3616     IKEEXT          (fcd84c381e0140af901e58d48882d26b)
C:\Windows\System32\ikeext.dll
15:33:50.0373 3616     IKEEXT - ok
15:33:50.0492 3616     IntcAzAudAddService
(e8017f1662d9142f45ceab694d013c00)
C:\Windows\system32\drivers\RTKVHD64.sys
15:33:50.0507 3616     IntcAzAudAddService - ok
15:33:50.0599 3616     intelide        (f00f20e70c6ec3aa366910083a0518aa)
C:\Windows\system32\drivers\intelide.sys
15:33:50.0601 3616     intelide - ok
15:33:50.0628 3616     intelppm        (ada036632c664caa754079041cf1f8c1)
C:\Windows\system32\DRIVERS\intelppm.sys
```

```
15:33:50.0630 3616     intelppm - ok
15:33:50.0652 3616     IPBusEnum       (098a91c54546a3b878dad6a7e90a455b)
C:\Windows\system32\ipbusenum.dll
15:33:50.0658 3616     IPBusEnum - ok
15:33:50.0697 3616     IpFilterDriver  (c9f0e1bd74365a8771590e9008d22ab6)
C:\Windows\system32\DRIVERS\ipfltdrv.sys
15:33:50.0701 3616     IpFilterDriver - ok
15:33:50.0755 3616     iphlpsvc        (a34a587fffd45fa649fba6d03784d257)
C:\Windows\System32\iphlpsvc.dll
15:33:50.0761 3616     iphlpsvc - ok
15:33:50.0810 3616     IPMIDRV         (0fc1aea580957aa8817b8f305d18ca3a)
C:\Windows\system32\drivers\IPMIDrv.sys
15:33:50.0814 3616     IPMIDRV - ok
15:33:50.0828 3616     IPNAT           (af9b39a7e7b6caa203b3862582e9f2d0)
C:\Windows\system32\drivers\ipnat.sys
15:33:50.0830 3616     IPNAT - ok
15:33:50.0843 3616     IRENUM          (3abf5e7213eb28966d55d58b515d5ce9)
C:\Windows\system32\drivers\irenum.sys
15:33:50.0845 3616     IRENUM - ok
15:33:50.0869 3616     isapnp          (2f7b28dc3e1183e5eb418df55c204f38)
C:\Windows\system32\drivers\isapnp.sys
15:33:50.0869 3616     isapnp - ok
15:33:50.0898 3616     iScsiPrt        (d931d7309deb2317035b07c9f9e6b0bd)
C:\Windows\system32\drivers\msiscsi.sys
15:33:50.0900 3616     iScsiPrt - ok
15:33:50.0919 3616     kbdclass        (bc02336f1cba7dcc7d1213bb588a68a5)
C:\Windows\system32\DRIVERS\kbdclass.sys
15:33:50.0921 3616     kbdclass - ok
15:33:50.0945 3616     kbdhid          (0705eff5b42a9db58548eec3b26bb484)
C:\Windows\system32\DRIVERS\kbdhid.sys
15:33:50.0945 3616     kbdhid - ok
15:33:50.0962 3616     KeyIso          (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:33:50.0964 3616     KeyIso - ok
15:33:50.0974 3616     KSecDD          (da1e991a61cfdd755a589e206b97644b)
C:\Windows\system32\Drivers\ksecdd.sys
15:33:50.0974 3616     KSecDD - ok
15:33:50.0990 3616     KSecPkg         (7e33198d956943a4f11a5474c1e9106f)
C:\Windows\system32\Drivers\ksecpkg.sys
15:33:50.0992 3616     KSecPkg - ok
15:33:50.0996 3616     ksthunk         (6869281e78cb31a43e969f06b57347c4)
C:\Windows\system32\drivers\ksthunk.sys
15:33:50.0998 3616     ksthunk - ok
15:33:51.0035 3616     KtmRm           (6ab66e16aa859232f64deb66887a8c9c)
C:\Windows\system32\msdtckrm.dll
15:33:51.0041 3616     KtmRm - ok
15:33:51.0083 3616     LanmanServer    (d9f42719019740baa6d1c6d536cbdaa6)
C:\Windows\system32\srvsvc.dll
15:33:51.0085 3616     LanmanServer - ok
15:33:51.0115 3616     LanmanWorkstation
(851a1382eed3e3a7476db004f4ee3e1a) C:\Windows\System32\wkssvc.dll
15:33:51.0117 3616     LanmanWorkstation - ok
15:33:51.0134 3616     lltdio          (1538831cf8ad2979a04c423779465827)
C:\Windows\system32\DRIVERS\lltdio.sys
15:33:51.0134 3616     lltdio - ok
15:33:51.0164 3616     lltdsvc         (c1185803384ab3feed115f79f109427f)
C:\Windows\System32\lltdsvc.dll
15:33:51.0167 3616     lltdsvc - ok
```

```
15:33:51.0183 3616     lmhosts         (f993a32249b66c9d622ea5592a8b76b8)
C:\Windows\System32\lmhsvc.dll
15:33:51.0185 3616     lmhosts - ok
15:33:51.0208 3616     LSI_FC          (1a93e54eb0ece102495a51266dcdb6a6)
C:\Windows\system32\DRIVERS\lsi_fc.sys
15:33:51.0210 3616     LSI_FC - ok
15:33:51.0230 3616     LSI_SAS         (1047184a9fdc8bdbff857175875ee810)
C:\Windows\system32\DRIVERS\lsi_sas.sys
15:33:51.0232 3616     LSI_SAS - ok
15:33:51.0242 3616     LSI_SAS2        (30f5c0de1ee8b5bc9306c1f0e4a75f93)
C:\Windows\system32\DRIVERS\lsi_sas2.sys
15:33:51.0244 3616     LSI_SAS2 - ok
15:33:51.0257 3616     LSI_SCSI        (0504eacaff0d3c8aed161c4b0d369d4a)
C:\Windows\system32\DRIVERS\lsi_scsi.sys
15:33:51.0259 3616     LSI_SCSI - ok
15:33:51.0279 3616     luafv           (43d0f98e1d56ccddb0d5254cff7b356e)
C:\Windows\system32\drivers\luafv.sys
15:33:51.0281 3616     luafv - ok
15:33:51.0298 3616     MBAMProtector   (dbc08862a71459e74f7538b432c114cc)
C:\Windows\system32\drivers\mbam.sys
15:33:51.0300 3616     MBAMProtector - ok
15:33:51.0363 3616     MBAMService     (ba400ed640bca1eae5c727ae17c10207)
C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamservice.exe
15:33:51.0367 3616     MBAMService - ok
15:33:51.0394 3616     Mcx2Svc         (0be09cd858abf9df6ed259d57a1a1663)
C:\Windows\system32\Mcx2Svc.dll
15:33:51.0396 3616     Mcx2Svc - ok
15:33:51.0414 3616     megasas         (a55805f747c6edb6a9080d7c633bd0f4)
C:\Windows\system32\DRIVERS\megasas.sys
15:33:51.0414 3616     megasas - ok
15:33:51.0435 3616     MegaSR          (baf74ce0072480c3b6b7c13b2a94d6b3)
C:\Windows\system32\DRIVERS\MegaSR.sys
15:33:51.0437 3616     MegaSR - ok
15:33:51.0490 3616     Microsoft SharePoint Workspace Audit Service - ok
15:33:51.0519 3616     MMCSS           (e40e80d0304a73e8d269f7141d77250b)
C:\Windows\system32\mmcss.dll
15:33:51.0525 3616     MMCSS - ok
15:33:51.0542 3616     Modem           (800ba92f7010378b09f9ed9270f07137)
C:\Windows\system32\drivers\modem.sys
15:33:51.0544 3616     Modem - ok
15:33:51.0566 3616     monitor         (b03d591dc7da45ece20b3b467e6aadaa)
C:\Windows\system32\DRIVERS\monitor.sys
15:33:51.0566 3616     monitor - ok
15:33:51.0591 3616     mouclass        (7d27ea49f3c1f687d357e77a470aea99)
C:\Windows\system32\DRIVERS\mouclass.sys
15:33:51.0591 3616     mouclass - ok
15:33:51.0599 3616     mouhid          (d3bf052c40b0c4166d9fd86a4288c1e6)
C:\Windows\system32\DRIVERS\mouhid.sys
15:33:51.0601 3616     mouhid - ok
15:33:51.0623 3616     mountmgr        (32e7a3d591d671a6df2db515a5cbe0fa)
C:\Windows\system32\drivers\mountmgr.sys
15:33:51.0625 3616     mountmgr - ok
15:33:51.0660 3616     MozillaMaintenance
(15d5398eed42c2504bb3d4fc875c15d1) C:\Program Files (x86)\Mozilla
Maintenance Service\maintenanceservice.exe
15:33:51.0662 3616     MozillaMaintenance - ok
15:33:51.0689 3616     mpio            (a44b420d30bd56e145d6a2bc8768ec58)
C:\Windows\system32\drivers\mpio.sys
```

```
15:33:51.0691 3616     mpio - ok
15:33:51.0707 3616     mpsdrv          (6c38c9e45ae0ea2fa5e551f2ed5e978f)
C:\Windows\system32\drivers\mpsdrv.sys
15:33:51.0726 3616     mpsdrv - ok
15:33:51.0785 3616     MpsSvc          (54ffc9c8898113ace189d4aa7199d2c1)
C:\Windows\system32\mpssvc.dll
15:33:51.0791 3616     MpsSvc - ok
15:33:51.0818 3616     MRxDAV          (dc722758b8261e1abafd31a3c0a66380)
C:\Windows\system32\drivers\mrxdav.sys
15:33:51.0820 3616     MRxDAV - ok
15:33:51.0845 3616     mrxsmb          (a5d9106a73dc88564c825d317cac68ac)
C:\Windows\system32\DRIVERS\mrxsmb.sys
15:33:51.0847 3616     mrxsmb - ok
15:33:51.0914 3616     mrxsmb10        (d711b3c1d5f42c0c2415687be09fc163)
C:\Windows\system32\DRIVERS\mrxsmb10.sys
15:33:51.0916 3616     mrxsmb10 - ok
15:33:51.0935 3616     mrxsmb20        (9423e9d355c8d303e76b8cfbd8a5c30c)
C:\Windows\system32\DRIVERS\mrxsmb20.sys
15:33:51.0937 3616     mrxsmb20 - ok
15:33:51.0957 3616     msahci          (c25f0bafa182cbca2dd3c851c2e75796)
C:\Windows\system32\drivers\msahci.sys
15:33:51.0957 3616     msahci - ok
15:33:51.0982 3616     msdsm           (db801a638d011b9633829eb6f663c900)
C:\Windows\system32\drivers\msdsm.sys
15:33:51.0984 3616     msdsm - ok
15:33:52.0011 3616     MSDTC           (de0ece52236cfa3ed2dbfc03f28253a8)
C:\Windows\System32\msdtc.exe
15:33:52.0013 3616     MSDTC - ok
15:33:52.0048 3616     Msfs            (aa3fb40e17ce1388fa1bedab50ea8f96)
C:\Windows\system32\drivers\Msfs.sys
15:33:52.0048 3616     Msfs - ok
15:33:52.0058 3616     mshidkmdf       (f9d215a46a8b9753f61767fa72a20326)
C:\Windows\System32\drivers\mshidkmdf.sys
15:33:52.0058 3616     mshidkmdf - ok
15:33:52.0080 3616     msisadrv        (d916874bbd4f8b07bfb7fa9b3ccae29d)
C:\Windows\system32\drivers\msisadrv.sys
15:33:52.0080 3616     msisadrv - ok
15:33:52.0105 3616     MSiSCSI         (808e98ff49b155c522e6400953177b08)
C:\Windows\system32\iscsiexe.dll
15:33:52.0107 3616     MSiSCSI - ok
15:33:52.0113 3616     msiserver - ok
15:33:52.0125 3616     MSKSSRV         (49ccf2c4fea34ffad8b1b59d49439366)
C:\Windows\system32\drivers\MSKSSRV.sys
15:33:52.0125 3616     MSKSSRV - ok
15:33:52.0138 3616     MSPCLOCK        (bdd71ace35a232104ddd349ee70e1ab3)
C:\Windows\system32\drivers\MSPCLOCK.sys
15:33:52.0140 3616     MSPCLOCK - ok
15:33:52.0144 3616     MSPQM           (4ed981241db27c3383d72092b618a1d0)
C:\Windows\system32\drivers\MSPQM.sys
15:33:52.0144 3616     MSPQM - ok
15:33:52.0181 3616     MsRPC           (759a9eeb0fa9ed79da1fb7d4ef78866d)
C:\Windows\system32\drivers\MsRPC.sys
15:33:52.0185 3616     MsRPC - ok
15:33:52.0199 3616     mssmbios        (0eed230e37515a0eaee3c2e1bc97b288)
C:\Windows\system32\drivers\mssmbios.sys
15:33:52.0199 3616     mssmbios - ok
15:33:52.0208 3616     MSTEE           (2e66f9ecb30b4221a318c92ac2250779)
C:\Windows\system32\drivers\MSTEE.sys
```

```
15:33:52.0208 3616     MSTEE - ok
15:33:52.0224 3616     MTConfig        (7ea404308934e675bffde8edf0757bcd)
C:\Windows\system32\DRIVERS\MTConfig.sys
15:33:52.0224 3616     MTConfig - ok
15:33:52.0244 3616     Mup             (f9a18612fd3526fe473c1bda678d61c8)
C:\Windows\system32\Drivers\mup.sys
15:33:52.0244 3616     Mup - ok
15:33:52.0273 3616     napagent        (582ac6d9873e31dfa28a4547270862dd)
C:\Windows\system32\qagentRT.dll
15:33:52.0279 3616     napagent - ok
15:33:52.0304 3616     NativeWifiP     (1ea3749c4114db3e3161156ffffa6b33)
C:\Windows\system32\DRIVERS\nwifi.sys
15:33:52.0306 3616     NativeWifiP - ok
15:33:52.0361 3616     NDIS            (79b47fd40d9a817e932f9d26fac0a81c)
C:\Windows\system32\drivers\ndis.sys
15:33:52.0367 3616     NDIS - ok
15:33:52.0382 3616     NdisCap         (9f9a1f53aad7da4d6fef5bb73ab811ac)
C:\Windows\system32\DRIVERS\ndiscap.sys
15:33:52.0382 3616     NdisCap - ok
15:33:52.0392 3616     NdisTapi        (30639c932d9fef22b31268fe25a1b6e5)
C:\Windows\system32\DRIVERS\ndistapi.sys
15:33:52.0392 3616     NdisTapi - ok
15:33:52.0416 3616     Ndisuio         (136185f9fb2cc61e573e676aa5402356)
C:\Windows\system32\DRIVERS\ndisuio.sys
15:33:52.0417 3616     Ndisuio - ok
15:33:52.0445 3616     NdisWan         (53f7305169863f0a2bddc49e116c2e11)
C:\Windows\system32\DRIVERS\ndiswan.sys
15:33:52.0445 3616     NdisWan - ok
15:33:52.0457 3616     NDProxy         (015c0d8e0e0421b4cfd48cffe2825879)
C:\Windows\system32\drivers\NDProxy.sys
15:33:52.0457 3616     NDProxy - ok
15:33:52.0468 3616     NetBIOS         (86743d9f5d2b1048062b14b1d84501c4)
C:\Windows\system32\DRIVERS\netbios.sys
15:33:52.0468 3616     NetBIOS - ok
15:33:52.0490 3616     NetBT           (09594d1089c523423b32a4229263f068)
C:\Windows\system32\DRIVERS\netbt.sys
15:33:52.0494 3616     NetBT - ok
15:33:52.0529 3616     Netlogon        (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:33:52.0531 3616     Netlogon - ok
15:33:52.0566 3616     Netman          (847d3ae376c0817161a14a82c8922a9e)
C:\Windows\System32\netman.dll
15:33:52.0570 3616     Netman - ok
15:33:52.0599 3616     netprofm        (5f28111c648f1e24f7dbc87cdeb091b8)
C:\Windows\System32\netprofm.dll
15:33:52.0603 3616     netprofm - ok
15:33:52.0673 3616     NetTcpPortSharing
(3e5a36127e201ddf663176b66828fafe)
C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\SMSvcHost.exe
15:33:52.0679 3616     NetTcpPortSharing - ok
15:33:52.0703 3616     nfrd960         (77889813be4d166cdab78ddba990da92)
C:\Windows\system32\DRIVERS\nfrd960.sys
15:33:52.0755 3616     nfrd960 - ok
15:33:52.0796 3616     NlaSvc          (1ee99a89cc788ada662441d1e9830529)
C:\Windows\System32\nlasvc.dll
15:33:52.0800 3616     NlaSvc - ok
```

```
15:33:52.0824 3616     Npfs            (1e4c4ab5c9b8dd13179bbdc75a2a01f7)
C:\Windows\system32\drivers\Npfs.sys
15:33:52.0824 3616     Npfs - ok
15:33:52.0830 3616     nsi             (d54bfdf3e0c953f823b3d0bfe4732528)
C:\Windows\system32\nsisvc.dll
15:33:52.0833 3616     nsi - ok
15:33:52.0849 3616     nsiproxy        (e7f5ae18af4168178a642a9247c63001)
C:\Windows\system32\drivers\nsiproxy.sys
15:33:52.0849 3616     nsiproxy - ok
15:33:52.0941 3616     Ntfs            (a2f74975097f52a00745f9637451fdd8)
C:\Windows\system32\drivers\Ntfs.sys
15:33:52.0953 3616     Ntfs - ok
15:33:53.0050 3616     Null            (9899284589f75fa8724ff3d16aed75c1)
C:\Windows\system32\drivers\Null.sys
15:33:53.0050 3616     Null - ok
15:33:53.0085 3616     NVENETFD        (a85b4f2ef3a7304a5399ef0526423040)
C:\Windows\system32\DRIVERS\nvm62x64.sys
15:33:53.0089 3616     NVENETFD - ok
15:33:53.0626 3616     nvlddmkm        (e55cab397f77d5208db18a78b1b7c0d5)
C:\Windows\system32\DRIVERS\nvlddmkm.sys
15:33:53.0712 3616     nvlddmkm - ok
15:33:53.0775 3616     nvraid          (0a92cb65770442ed0dc44834632f66ad)
C:\Windows\system32\drivers\nvraid.sys
15:33:53.0777 3616     nvraid - ok
15:33:53.0800 3616     nvstor          (dab0e87525c10052bf65f06152f37e4a)
C:\Windows\system32\drivers\nvstor.sys
15:33:53.0802 3616     nvstor - ok
15:33:53.0826 3616     nvsvc           (43bc8151893ae6afe42e149d663c2221)
C:\Windows\system32\nvvsvc.exe
15:33:53.0830 3616     nvsvc - ok
15:33:53.0851 3616     nv_agp          (270d7cd42d6e3979f6dd0146650f0e05)
C:\Windows\system32\drivers\nv_agp.sys
15:33:53.0853 3616     nv_agp - ok
15:33:53.0880 3616     ohci1394        (3589478e4b22ce21b41fa1bfc0b8b8a0)
C:\Windows\system32\drivers\ohci1394.sys
15:33:53.0898 3616     ohci1394 - ok
15:33:53.0939 3616     ose             (9d10f99a6712e28f8acd5641e3a7ea6b)
C:\Program Files (x86)\Common Files\Microsoft Shared\Source
Engine\OSE.EXE
15:33:53.0941 3616     ose - ok
15:33:54.0140 3616     osppsvc         (61bffb5f57ad12f83ab64b7181829b34)
C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
15:33:54.0173 3616     osppsvc - ok
15:33:54.0250 3616     p2pimsvc        (3eac4455472cc2c97107b5291e0dcafe)
C:\Windows\system32\pnrpsvc.dll
15:33:54.0253 3616     p2pimsvc - ok
15:33:54.0283 3616     p2psvc          (927463ecb02179f88e4b9a17568c63c3)
C:\Windows\system32\p2psvc.dll
15:33:54.0289 3616     p2psvc - ok
15:33:54.0335 3616     Parport         (0086431c29c35be1dbc43f52cc273887)
C:\Windows\system32\DRIVERS\parport.sys
15:33:54.0351 3616     Parport - ok
15:33:54.0378 3616     partmgr         (e9766131eeade40a27dc27d2d68fba9c)
C:\Windows\system32\drivers\partmgr.sys
15:33:54.0380 3616     partmgr - ok
15:33:54.0402 3616     PcaSvc          (3aeaa8b561e63452c655dc0584922257)
C:\Windows\System32\pcasvc.dll
```

```
15:33:54.0406 3616     PcaSvc - ok
15:33:54.0453 3616     pci             (94575c0571d1462a0f70bde6bd6ee6b3)
C:\Windows\system32\drivers\pci.sys
15:33:54.0457 3616     pci - ok
15:33:54.0470 3616     pciide          (b5b8b5ef2e5cb34df8dcf8831e3534fa)
C:\Windows\system32\drivers\pciide.sys
15:33:54.0472 3616     pciide - ok
15:33:54.0500 3616     pcmcia          (b2e81d4e87ce48589f98cb8c05b01f2f)
C:\Windows\system32\DRIVERS\pcmcia.sys
15:33:54.0535 3616     pcmcia - ok
15:33:54.0552 3616     pcw             (d6b9c2e1a11a3a4b26a182ffef18f603)
C:\Windows\system32\drivers\pcw.sys
15:33:54.0552 3616     pcw - ok
15:33:54.0587 3616     PEAUTH          (68769c3356b3be5d1c732c97b9a80d6e)
C:\Windows\system32\drivers\peauth.sys
15:33:54.0611 3616     PEAUTH - ok
15:33:54.0685 3616     PeerDistSvc     (b9b0a4299dd2d76a4243f75fd54dc680)
C:\Windows\system32\peerdistsvc.dll
15:33:54.0695 3616     PeerDistSvc - ok
15:33:54.0755 3616     PerfHost        (e495e408c93141e8fc72dc0c6046ddfa)
C:\Windows\SysWow64\perfhost.exe
15:33:54.0759 3616     PerfHost - ok
15:33:54.0888 3616     pla             (c7cf6a6e137463219e1259e3f0f0dd6c)
C:\Windows\system32\pla.dll
15:33:54.0898 3616     pla - ok
15:33:54.0941 3616     PlugPlay        (25fbdef06c4d92815b353f6e792c8129)
C:\Windows\system32\umpnpmgr.dll
15:33:54.0945 3616     PlugPlay - ok
15:33:54.0964 3616     PnkBstrA - ok
15:33:54.0976 3616     PnkBstrB - ok
15:33:54.0994 3616     PNRPAutoReg     (7195581cec9bb7d12abe54036acc2e38)
C:\Windows\system32\pnrpauto.dll
15:33:54.0996 3616     PNRPAutoReg - ok
15:33:55.0025 3616     PNRPsvc         (3eac4455472cc2c97107b5291e0dcafe)
C:\Windows\system32\pnrpsvc.dll
15:33:55.0029 3616     PNRPsvc - ok
15:33:55.0058 3616     PolicyAgent     (4f15d75adf6156bf56eced6d4a55c389)
C:\Windows\System32\ipsecsvc.dll
15:33:55.0062 3616     PolicyAgent - ok
15:33:55.0105 3616     Power           (6ba9d927dded70bd1a9caded45f8b184)
C:\Windows\system32\umpo.dll
15:33:55.0113 3616     Power - ok
15:33:55.0158 3616     PptpMiniport    (f92a2c41117a11a00be01ca01a7fcde9)
C:\Windows\system32\DRIVERS\raspptp.sys
15:33:55.0160 3616     PptpMiniport - ok
15:33:55.0187 3616     Processor       (0d922e23c041efb1c3fac2a6f943c9bf)
C:\Windows\system32\DRIVERS\processr.sys
15:33:55.0189 3616     Processor - ok
15:33:55.0224 3616     ProfSvc         (53e83f1f6cf9d62f32801cf66d8352a8)
C:\Windows\system32\profsvc.dll
15:33:55.0228 3616     ProfSvc - ok
15:33:55.0246 3616     ProtectedStorage
(c118a82cd78818c29ab228366ebf81c3) C:\Windows\system32\lsass.exe
15:33:55.0248 3616     ProtectedStorage - ok
15:33:55.0291 3616     Psched          (0557cf5a2556bd58e26384169d72438d)
C:\Windows\system32\DRIVERS\pacer.sys
15:33:55.0291 3616     Psched - ok
```

```
15:33:55.0375 3616     ql2300          (a53a15a11ebfd21077463ee2c7afeef0)
C:\Windows\system32\DRIVERS\ql2300.sys
15:33:55.0390 3616     ql2300 - ok
15:33:55.0474 3616     ql40xx          (4f6d12b51de1aaeff7dc58c4d75423c8)
C:\Windows\system32\DRIVERS\ql40xx.sys
15:33:55.0476 3616     ql40xx - ok
15:33:55.0509 3616     QWAVE           (906191634e99aea92c4816150bda3732)
C:\Windows\system32\qwave.dll
15:33:55.0513 3616     QWAVE - ok
15:33:55.0550 3616     QWAVEdrv        (76707bb36430888d9ce9d705398adb6c)
C:\Windows\system32\drivers\qwavedrv.sys
15:33:55.0568 3616     QWAVEdrv - ok
15:33:55.0582 3616     RasAcd          (5a0da8ad5762fa2d91678a8a01311704)
C:\Windows\system32\DRIVERS\rasacd.sys
15:33:55.0597 3616     RasAcd - ok
15:33:55.0623 3616     RasAgileVpn     (7ecff9b22276b73f43a99a15a6094e90)
C:\Windows\system32\DRIVERS\AgileVpn.sys
15:33:55.0623 3616     RasAgileVpn - ok
15:33:55.0638 3616     RasAuto         (8f26510c5383b8dbe976de1cd00fc8c7)
C:\Windows\System32\rasauto.dll
15:33:55.0640 3616     RasAuto - ok
15:33:55.0683 3616     Rasl2tp         (471815800ae33e6f1c32fb1b97c490ca)
C:\Windows\system32\DRIVERS\rasl2tp.sys
15:33:55.0716 3616     Rasl2tp - ok
15:33:55.0750 3616     RasMan          (ee867a0870fc9e4972ba9eaad35651e2)
C:\Windows\System32\rasmans.dll
15:33:55.0753 3616     RasMan - ok
15:33:55.0765 3616     RasPppoe        (855c9b1cd4756c5e9a2aa58a15f58c25)
C:\Windows\system32\DRIVERS\raspppoe.sys
15:33:55.0767 3616     RasPppoe - ok
15:33:55.0785 3616     RasSstp         (e8b1e447b008d07ff47d016c2b0eeecb)
C:\Windows\system32\DRIVERS\rassstp.sys
15:33:55.0785 3616     RasSstp - ok
15:33:55.0830 3616     rdbss           (77f665941019a1594d887a74f301fa2f)
C:\Windows\system32\DRIVERS\rdbss.sys
15:33:55.0832 3616     rdbss - ok
15:33:55.0841 3616     rdpbus          (302da2a0539f2cf54d7c6cc30c1f2d8d)
C:\Windows\system32\DRIVERS\rdpbus.sys
15:33:55.0873 3616     rdpbus - ok
15:33:55.0890 3616     RDPCDD          (cea6cc257fc9b7715f1c2b4849286d24)
C:\Windows\system32\DRIVERS\RDPCDD.sys
15:33:55.0892 3616     RDPCDD - ok
15:33:55.0925 3616     RDPDR           (1b6163c503398b23ff8b939c67747683)
C:\Windows\system32\drivers\rdpdr.sys
15:33:55.0957 3616     RDPDR - ok
15:33:55.0972 3616     RDPENCDD        (bb5971a4f00659529a5c44831af22365)
C:\Windows\system32\drivers\rdpencdd.sys
15:33:55.0974 3616     RDPENCDD - ok
15:33:55.0982 3616     RDPREFMP        (216f3fa57533d98e1f74ded70113177a)
C:\Windows\system32\drivers\rdprefmp.sys
15:33:55.0982 3616     RDPREFMP - ok
15:33:56.0033 3616     RdpVideoMiniport
(70cba1a0c98600a2aa1863479b35cb90)
C:\Windows\system32\drivers\rdpvideominiport.sys
15:33:56.0035 3616     RdpVideoMiniport - ok
15:33:56.0068 3616     RDPWD           (e61608aa35e98999af9aaeeea6114b0a)
C:\Windows\system32\drivers\RDPWD.sys
15:33:56.0070 3616     RDPWD - ok
```

```
15:33:56.0101 3616     rdyboost        (34ed295fa0121c241bfef24764fc4520)
C:\Windows\system32\drivers\rdyboost.sys
15:33:56.0103 3616     rdyboost - ok
15:33:56.0128 3616     RemoteAccess    (254fb7a22d74e5511c73a3f6d802f192)
C:\Windows\System32\mprdim.dll
15:33:56.0130 3616     RemoteAccess - ok
15:33:56.0158 3616     RemoteRegistry  (e4d94f24081440b5fc5aa556c7c62702)
C:\Windows\system32\regsvc.dll
15:33:56.0162 3616     RemoteRegistry - ok
15:33:56.0185 3616     RFCOMM          (3dd798846e2c28102b922c56e71b7932)
C:\Windows\system32\DRIVERS\rfcomm.sys
15:33:56.0187 3616     RFCOMM - ok
15:33:56.0203 3616     RpcEptMapper    (e4dc58cf7b3ea515ae917ff0d402a7bb)
C:\Windows\System32\RpcEpMap.dll
15:33:56.0207 3616     RpcEptMapper - ok
15:33:56.0222 3616     RpcLocator      (d5ba242d4cf8e384db90e6a8ed850b8c)
C:\Windows\system32\locator.exe
15:33:56.0224 3616     RpcLocator - ok
15:33:56.0263 3616     RpcSs           (5c627d1b1138676c0a7ab2c2c190d123)
C:\Windows\system32\rpcss.dll
15:33:56.0269 3616     RpcSs - ok
15:33:56.0300 3616     rspndr          (ddc86e4f8e7456261e637e3552e804ff)
C:\Windows\system32\DRIVERS\rspndr.sys
15:33:56.0316 3616     rspndr - ok
15:33:56.0341 3616     s3cap           (e60c0a09f997826c7627b244195ab581)
C:\Windows\system32\drivers\vms3cap.sys
15:33:56.0343 3616     s3cap - ok
15:33:56.0363 3616     SamSs           (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:33:56.0365 3616     SamSs - ok
15:33:56.0384 3616     sbp2port        (ac03af3329579fffb455aa2daabbe22b)
C:\Windows\system32\drivers\sbp2port.sys
15:33:56.0386 3616     sbp2port - ok
15:33:56.0435 3616     SCardSvr        (9b7395789e3791a3b6d000fe6f8b131e)
C:\Windows\System32\SCardSvr.dll
15:33:56.0443 3616     SCardSvr - ok
15:33:56.0478 3616     scfilter        (253f38d0d7074c02ff8deb9836c97d2b)
C:\Windows\system32\DRIVERS\scfilter.sys
15:33:56.0480 3616     scfilter - ok
15:33:56.0572 3616     Schedule        (262f6592c3299c005fd6bec90fc4463a)
C:\Windows\system32\schedsvc.dll
15:33:56.0591 3616     Schedule - ok
15:33:56.0625 3616     SCPolicySvc     (f17d1d393bbc69c5322fbfafaca28c7f)
C:\Windows\System32\certprop.dll
15:33:56.0625 3616     SCPolicySvc - ok
15:33:56.0648 3616     SDRSVC          (6ea4234dc55346e0709560fe7c2c1972)
C:\Windows\System32\SDRSVC.dll
15:33:56.0652 3616     SDRSVC - ok
15:33:56.0707 3616     secdrv          (3ea8a16169c26afbeb544e0e48421186)
C:\Windows\system32\drivers\secdrv.sys
15:33:56.0708 3616     secdrv - ok
15:33:56.0736 3616     seclogon        (bc617a4e1b4fa8df523a061739a0bd87)
C:\Windows\system32\seclogon.dll
15:33:56.0740 3616     seclogon - ok
15:33:56.0755 3616     SENS            (c32ab8fa018ef34c0f113bd501436d21)
C:\Windows\System32\sens.dll
15:33:56.0759 3616     SENS - ok
```

```
15:33:56.0771 3616     SensrSvc        (0336cffafaab87a11541f1cf1594b2b2)
C:\Windows\system32\sensrsvc.dll
15:33:56.0773 3616     SensrSvc - ok
15:33:56.0792 3616     Serenum         (cb624c0035412af0debec78c41f5ca1b)
C:\Windows\system32\DRIVERS\serenum.sys
15:33:56.0794 3616     Serenum - ok
15:33:56.0808 3616     Serial          (c1d8e28b2c2adfaec4ba89e9fda69bd6)
C:\Windows\system32\DRIVERS\serial.sys
15:33:56.0810 3616     Serial - ok
15:33:56.0828 3616     sermouse        (1c545a7d0691cc4a027396535691c3e3)
C:\Windows\system32\DRIVERS\sermouse.sys
15:33:56.0828 3616     sermouse - ok
15:33:56.0867 3616     SessionEnv      (0b6231bf38174a1628c4ac812cc75804)
C:\Windows\system32\sessenv.dll
15:33:56.0871 3616     SessionEnv - ok
15:33:56.0900 3616     sffdisk         (a554811bcd09279536440c964ae35bbf)
C:\Windows\system32\drivers\sffdisk.sys
15:33:56.0917 3616     sffdisk - ok
15:33:56.0925 3616     sffp_mmc        (ff414f0baefeba59bc6c04b3db0b87bf)
C:\Windows\system32\drivers\sffp_mmc.sys
15:33:56.0927 3616     sffp_mmc - ok
15:33:56.0937 3616     sffp_sd         (dd85b78243a19b59f0637dcf284da63c)
C:\Windows\system32\drivers\sffp_sd.sys
15:33:56.0937 3616     sffp_sd - ok
15:33:56.0953 3616     sfloppy         (a9d601643a1647211a1ee2ec4e433ff4)
C:\Windows\system32\DRIVERS\sfloppy.sys
15:33:56.0955 3616     sfloppy - ok
15:33:57.0001 3616     SharedAccess    (b95f6501a2f8b2e78c697fec401970ce)
C:\Windows\System32\ipnathlp.dll
15:33:57.0005 3616     SharedAccess - ok
15:33:57.0044 3616     ShellHWDetection
(aaf932b4011d14052955d4b212a4da8d) C:\Windows\System32\shsvcs.dll
15:33:57.0050 3616     ShellHWDetection - ok
15:33:57.0068 3616     SiSRaid2        (843caf1e5fde1ffd5ff768f23a51e2e1)
C:\Windows\system32\DRIVERS\SiSRaid2.sys
15:33:57.0068 3616     SiSRaid2 - ok
15:33:57.0083 3616     SiSRaid4        (6a6c106d42e9ffff8b9fcb4f754f6da4)
C:\Windows\system32\DRIVERS\sisraid4.sys
15:33:57.0101 3616     SiSRaid4 - ok
15:33:57.0117 3616     Smb             (548260a7b8654e024dc30bf8a7c5baa4)
C:\Windows\system32\DRIVERS\smb.sys
15:33:57.0121 3616     Smb - ok
15:33:57.0136 3616     SNMPTRAP        (6313f223e817cc09aa41811daa7f541d)
C:\Windows\System32\snmptrap.exe
15:33:57.0138 3616     SNMPTRAP - ok
15:33:57.0527 3616     SNPSTD3         (b8b6b14ee7b2e9806e4373a7dc61b592)
C:\Windows\system32\DRIVERS\snpstd3.sys
15:33:57.0593 3616     SNPSTD3 - ok
15:33:57.0705 3616     spldr           (b9e31e5cacdfe584f34f730a677803f9)
C:\Windows\system32\drivers\spldr.sys
15:33:57.0707 3616     spldr - ok
15:33:57.0763 3616     Spooler         (b96c17b5dc1424d56eea3a99e97428cd)
C:\Windows\System32\spoolsv.exe
15:33:57.0769 3616     Spooler - ok
15:33:57.0931 3616     sppsvc          (e17e0188bb90fae42d83e98707efa59c)
C:\Windows\system32\sppsvc.exe
15:33:57.0958 3616     sppsvc - ok
```

```
15:33:58.0029 3616     sppuinotify     (93d7d61317f3d4bc4f4e9f8a96a7de45)
C:\Windows\system32\sppuinotify.dll
15:33:58.0031 3616     sppuinotify - ok
15:33:58.0091 3616     sptd            (602884696850c86434530790b110e8eb)
C:\Windows\system32\Drivers\sptd.sys
15:33:58.0091 3616     Suspicious file (NoAccess):
C:\Windows\system32\Drivers\sptd.sys. md5:
602884696850c86434530790b110e8eb
15:33:58.0093 3616     sptd ( LockedFile.Multi.Generic ) - warning
15:33:58.0093 3616     sptd - detected LockedFile.Multi.Generic (1)
15:33:58.0158 3616     srv             (441fba48bff01fdb9d5969ebc1838f0b)
C:\Windows\system32\DRIVERS\srv.sys
15:33:58.0162 3616     srv - ok
15:33:58.0210 3616     srv2            (b4adebbf5e3677cce9651e0f01f7cc28)
C:\Windows\system32\DRIVERS\srv2.sys
15:33:58.0212 3616     srv2 - ok
15:33:58.0248 3616     srvnet          (27e461f0be5bff5fc737328f749538c3)
C:\Windows\system32\DRIVERS\srvnet.sys
15:33:58.0250 3616     srvnet - ok
15:33:58.0279 3616     SSDPSRV         (51b52fbd583cde8aa9ba62b8b4298f33)
C:\Windows\System32\ssdpsrv.dll
15:33:58.0283 3616     SSDPSRV - ok
15:33:58.0294 3616     SstpSvc         (ab7aebf58dad8daab7a6c45e6a8885cb)
C:\Windows\system32\sstpsvc.dll
15:33:58.0296 3616     SstpSvc - ok
15:33:58.0382 3616     Stereo Service  (29662881a46db66730c62a4f1bfa3dc2)
C:\Program Files (x86)\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe
15:33:58.0386 3616     Stereo Service - ok
15:33:58.0431 3616     stexstor        (f3817967ed533d08327dc73bc4d5542a)
C:\Windows\system32\DRIVERS\stexstor.sys
15:33:58.0435 3616     stexstor - ok
15:33:58.0494 3616     stisvc          (8dd52e8e6128f4b2da92ce27402871c1)
C:\Windows\System32\wiaservc.dll
15:33:58.0500 3616     stisvc - ok
15:33:58.0539 3616     storflt         (7785dc213270d2fc066538daf94087e7)
C:\Windows\system32\drivers\vmstorfl.sys
15:33:58.0541 3616     storflt - ok
15:33:58.0558 3616     storvsc         (d34e4943d5ac096c8edeebfd80d76e23)
C:\Windows\system32\drivers\storvsc.sys
15:33:58.0560 3616     storvsc - ok
15:33:58.0580 3616     swenum          (d01ec09b6711a5f8e7e6564a4d0fbc90)
C:\Windows\system32\drivers\swenum.sys
15:33:58.0582 3616     swenum - ok
15:33:58.0625 3616     swprv           (e08e46fdd841b7184194011ca1955a0b)
C:\Windows\System32\swprv.dll
15:33:58.0632 3616     swprv - ok
15:33:58.0642 3616     Synth3dVsc - ok
15:33:58.0734 3616     SysMain         (bf9ccc0bf39b418c8d0ae8b05cf95b7d)
C:\Windows\system32\sysmain.dll
15:33:58.0750 3616     SysMain - ok
15:33:58.0837 3616     TabletInputService
(e3c61fd7b7c2557e1f1b0b4cec713585) C:\Windows\System32\TabSvc.dll
15:33:58.0843 3616     TabletInputService - ok
15:33:58.0878 3616     TapiSrv         (40f0849f65d13ee87b9a9ae3c1dd6823)
C:\Windows\System32\tapisrv.dll
15:33:58.0884 3616     TapiSrv - ok
15:33:58.0896 3616     TBS             (1be03ac720f4d302ea01d40f588162f6)
C:\Windows\System32\tbssvc.dll
```

```
15:33:58.0900 3616     TBS - ok
15:33:59.0017 3616     Tcpip           (acb82bda8f46c84f465c1afa517dc4b9)
C:\Windows\system32\drivers\tcpip.sys
15:33:59.0042 3616     Tcpip - ok
15:33:59.0167 3616     TCPIP6          (acb82bda8f46c84f465c1afa517dc4b9)
C:\Windows\system32\DRIVERS\tcpip.sys
15:33:59.0179 3616     TCPIP6 - ok
15:33:59.0236 3616     tcpipreg        (df687e3d8836bfb04fcc0615bf15a519)
C:\Windows\system32\drivers\tcpipreg.sys
15:33:59.0236 3616     tcpipreg - ok
15:33:59.0257 3616     TDPIPE          (3371d21011695b16333a3934340c4e7c)
C:\Windows\system32\drivers\tdpipe.sys
15:33:59.0259 3616     TDPIPE - ok
15:33:59.0287 3616     TDTCP           (51c5eceb1cdee2468a1748be550cfbc8)
C:\Windows\system32\drivers\tdtcp.sys
15:33:59.0289 3616     TDTCP - ok
15:33:59.0318 3616     tdx             (ddad5a7ab24d8b65f8d724f5c20fd806)
C:\Windows\system32\DRIVERS\tdx.sys
15:33:59.0318 3616     tdx - ok
15:33:59.0351 3616     TermDD          (561e7e1f06895d78de991e01dd0fb6e5)
C:\Windows\system32\drivers\termdd.sys
15:33:59.0351 3616     TermDD - ok
15:33:59.0396 3616     TermService     (2e648163254233755035b46dd7b89123)
C:\Windows\System32\termsrv.dll
15:33:59.0402 3616     TermService - ok
15:33:59.0425 3616     Themes          (f0344071948d1a1fa732231785a0664c)
C:\Windows\system32\themeservice.dll
15:33:59.0429 3616     Themes - ok
15:33:59.0453 3616     THREADORDER     (e40e80d0304a73e8d269f7141d77250b)
C:\Windows\system32\mmcss.dll
15:33:59.0453 3616     THREADORDER - ok
15:33:59.0468 3616     TrkWks          (7e7afd841694f6ac397e99d75cead49d)
C:\Windows\System32\trkwks.dll
15:33:59.0472 3616     TrkWks - ok
15:33:59.0525 3616     TrustedInstaller
(773212b2aaa24c1e31f10246b15b276c)
C:\Windows\servicing\TrustedInstaller.exe
15:33:59.0529 3616     TrustedInstaller - ok
15:33:59.0564 3616     tssecsrv        (ce18b2cdfc837c99e5fae9ca6cba5d30)
C:\Windows\system32\DRIVERS\tssecsrv.sys
15:33:59.0570 3616     tssecsrv - ok
15:33:59.0609 3616     TsUsbFlt        (d11c783e3ef9a3c52c0ebe83cc5000e9)
C:\Windows\system32\drivers\tsusbflt.sys
15:33:59.0669 3616     TsUsbFlt - ok
15:33:59.0687 3616     tsusbhub - ok
15:33:59.0718 3616     tunnel          (3566a8daafa27af944f5d705eaa64894)
C:\Windows\system32\DRIVERS\tunnel.sys
15:33:59.0720 3616     tunnel - ok
15:33:59.0751 3616     uagp35          (b4dd609bd7e282bfc683cec7eaaaad67)
C:\Windows\system32\DRIVERS\uagp35.sys
15:33:59.0769 3616     uagp35 - ok
15:33:59.0794 3616     udfs            (ff4232a1a64012baa1fd97c7b67df593)
C:\Windows\system32\DRIVERS\udfs.sys
15:33:59.0798 3616     udfs - ok
15:33:59.0824 3616     UI0Detect       (3cbdec8d06b9968aba702eba076364a1)
C:\Windows\system32\UI0Detect.exe
15:33:59.0826 3616     UI0Detect - ok
```

```
15:33:59.0847 3616     uliagpkx        (4bfe1bc28391222894cbf1e7d0e42320)
C:\Windows\system32\drivers\uliagpkx.sys
15:33:59.0865 3616     uliagpkx - ok
15:33:59.0892 3616     umbus           (dc54a574663a895c8763af0fa1ff7561)
C:\Windows\system32\drivers\umbus.sys
15:33:59.0892 3616     umbus - ok
15:33:59.0931 3616     UmPass          (b2e8e8cb557b156da5493bbddcc1474d)
C:\Windows\system32\DRIVERS\umpass.sys
15:33:59.0949 3616     UmPass - ok
15:33:59.0990 3616     UmRdpService    (a293dcd756d04d8492a750d03b9a297c)
C:\Windows\System32\umrdp.dll
15:33:59.0992 3616     UmRdpService - ok
15:34:00.0023 3616     upnphost        (d47ec6a8e81633dd18d2436b19baf6de)
C:\Windows\System32\upnphost.dll
15:34:00.0027 3616     upnphost - ok
15:34:00.0058 3616     usbaudio        (82e8f44688e6fac57b5b7c6fc7adbc2a)
C:\Windows\system32\drivers\usbaudio.sys
15:34:00.0060 3616     usbaudio - ok
15:34:00.0080 3616     usbccgp         (6f1a3157a1c89435352ceb543cdb359c)
C:\Windows\system32\DRIVERS\usbccgp.sys
15:34:00.0082 3616     usbccgp - ok
15:34:00.0107 3616     usbcir          (af0892a803fdda7492f595368e3b68e7)
C:\Windows\system32\drivers\usbcir.sys
15:34:00.0111 3616     usbcir - ok
15:34:00.0132 3616     usbehci         (c025055fe7b87701eb042095df1a2d7b)
C:\Windows\system32\DRIVERS\usbehci.sys
15:34:00.0132 3616     usbehci - ok
15:34:00.0160 3616     usbhub          (287c6c9410b111b68b52ca298f7b8c24)
C:\Windows\system32\DRIVERS\usbhub.sys
15:34:00.0162 3616     usbhub - ok
15:34:00.0169 3616     usbohci         (9840fc418b4cbd632d3d0a667a725c31)
C:\Windows\system32\DRIVERS\usbohci.sys
15:34:00.0171 3616     usbohci - ok
15:34:00.0203 3616     usbprint        (73188f58fb384e75c4063d29413cee3d)
C:\Windows\system32\DRIVERS\usbprint.sys
15:34:00.0203 3616     usbprint - ok
15:34:00.0218 3616     USBSTOR         (fed648b01349a3c8395a5169db5fb7d6)
C:\Windows\system32\DRIVERS\USBSTOR.SYS
15:34:00.0218 3616     USBSTOR - ok
15:34:00.0236 3616     usbuhci         (62069a34518bcf9c1fd9e74b3f6db7cd)
C:\Windows\system32\drivers\usbuhci.sys
15:34:00.0236 3616     usbuhci - ok
15:34:00.0259 3616     UxSms           (edbb23cbcf2cdf727d64ff9b51a6070e)
C:\Windows\System32\uxsms.dll
15:34:00.0261 3616     UxSms - ok
15:34:00.0279 3616     VaultSvc        (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:34:00.0281 3616     VaultSvc - ok
15:34:00.0298 3616     vdrvroot        (c5c876ccfc083ff3b128f933823e87bd)
C:\Windows\system32\drivers\vdrvroot.sys
15:34:00.0298 3616     vdrvroot - ok
15:34:00.0341 3616     vds             (8d6b481601d01a456e75c3210f1830be)
C:\Windows\System32\vds.exe
15:34:00.0347 3616     vds - ok
15:34:00.0357 3616     vga             (da4da3f5e02943c2dc8c6ed875de68dd)
C:\Windows\system32\DRIVERS\vgapnp.sys
15:34:00.0357 3616     vga - ok
```

```
15:34:00.0369 3616     VgaSave         (53e92a310193cb3c03bea963de7d9cfc)
C:\Windows\System32\drivers\vga.sys
15:34:00.0371 3616     VgaSave - ok
15:34:00.0394 3616     VGPU - ok
15:34:00.0423 3616     vhdmp           (2ce2df28c83aeaf30084e1b1eb253cbb)
C:\Windows\system32\drivers\vhdmp.sys
15:34:00.0425 3616     vhdmp - ok
15:34:00.0458 3616     viaide          (e5689d93ffe4e5d66c0178761240dd54)
C:\Windows\system32\drivers\viaide.sys
15:34:00.0458 3616     viaide - ok
15:34:00.0484 3616     vmbus           (86ea3e79ae350fea5331a1303054005f)
C:\Windows\system32\drivers\vmbus.sys
15:34:00.0539 3616     vmbus - ok
15:34:00.0562 3616     VMBusHID        (7de90b48f210d29649380545db45a187)
C:\Windows\system32\drivers\VMBusHID.sys
15:34:00.0564 3616     VMBusHID - ok
15:34:00.0585 3616     volmgr          (d2aafd421940f640b407aefaaebd91b0)
C:\Windows\system32\drivers\volmgr.sys
15:34:00.0587 3616     volmgr - ok
15:34:00.0619 3616     volmgrx         (a255814907c89be58b79ef2f189b843b)
C:\Windows\system32\drivers\volmgrx.sys
15:34:00.0623 3616     volmgrx - ok
15:34:00.0644 3616     volsnap         (0d08d2f3b3ff84e433346669b5e0f639)
C:\Windows\system32\drivers\volsnap.sys
15:34:00.0648 3616     volsnap - ok
15:34:00.0683 3616     vsmraid         (5e2016ea6ebaca03c04feac5f330d997)
C:\Windows\system32\DRIVERS\vsmraid.sys
15:34:00.0703 3616     vsmraid - ok
15:34:00.0787 3616     VSS             (b60ba0bc31b0cb414593e169f6f21cc2)
C:\Windows\system32\vssvc.exe
15:34:00.0798 3616     VSS - ok
15:34:00.0890 3616     vwifibus        (36d4720b72b5c5d9cb2b9c29e9df67a1)
C:\Windows\System32\drivers\vwifibus.sys
15:34:00.0894 3616     vwifibus - ok
15:34:00.0935 3616     W32Time         (1c9d80cc3849b3788048078c26486e1a)
C:\Windows\system32\w32time.dll
15:34:00.0941 3616     W32Time - ok
15:34:00.0957 3616     WacomPen        (4e9440f4f152a7b944cb1663d3935a3e)
C:\Windows\system32\DRIVERS\wacompen.sys
15:34:00.0958 3616     WacomPen - ok
15:34:00.0992 3616     WANARP          (356afd78a6ed4457169241ac3965230c)
C:\Windows\system32\DRIVERS\wanarp.sys
15:34:00.0994 3616     WANARP - ok
15:34:00.0998 3616     Wanarpv6        (356afd78a6ed4457169241ac3965230c)
C:\Windows\system32\DRIVERS\wanarp.sys
15:34:01.0000 3616     Wanarpv6 - ok
15:34:01.0085 3616     WatAdminSvc     (3cec96de223e49eaae3651fcf8faea6c)
C:\Windows\system32\Wat\WatAdminSvc.exe
15:34:01.0093 3616     WatAdminSvc - ok
15:34:01.0183 3616     wbengine        (78f4e7f5c56cb9716238eb57da4b6a75)
C:\Windows\system32\wbengine.exe
15:34:01.0195 3616     wbengine - ok
15:34:01.0283 3616     WbioSrvc        (3aa101e8edab2db4131333f4325c76a3)
C:\Windows\System32\wbiosrvc.dll
15:34:01.0285 3616     WbioSrvc - ok
15:34:01.0316 3616     wcncsvc         (7368a2afd46e5a4481d1de9d14848edd)
C:\Windows\System32\wcncsvc.dll
15:34:01.0322 3616     wcncsvc - ok
```

```
15:34:01.0337 3616     WcsPlugInService
(20f7441334b18cee52027661df4a6129)
C:\Windows\System32\WcsPlugInService.dll
15:34:01.0339 3616     WcsPlugInService - ok
15:34:01.0361 3616     Wd              (72889e16ff12ba0f235467d6091b17dc)
C:\Windows\system32\DRIVERS\wd.sys
15:34:01.0363 3616     Wd - ok
15:34:01.0400 3616     Wdf01000        (441bd2d7b4f98134c3a4f9fa570fd250)
C:\Windows\system32\drivers\Wdf01000.sys
15:34:01.0408 3616     Wdf01000 - ok
15:34:01.0429 3616     WdiServiceHost  (bf1fc3f79b863c914687a737c2f3d681)
C:\Windows\system32\wdi.dll
15:34:01.0431 3616     WdiServiceHost - ok
15:34:01.0435 3616     WdiSystemHost   (bf1fc3f79b863c914687a737c2f3d681)
C:\Windows\system32\wdi.dll
15:34:01.0439 3616     WdiSystemHost - ok
15:34:01.0478 3616     WebClient       (3db6d04e1c64272f8b14eb8bc4616280)
C:\Windows\System32\webclnt.dll
15:34:01.0484 3616     WebClient - ok
15:34:01.0507 3616     Wecsvc          (c749025a679c5103e575e3b48e092c43)
C:\Windows\system32\wecsvc.dll
15:34:01.0511 3616     Wecsvc - ok
15:34:01.0523 3616     wercplsupport   (7e591867422dc788b9e5bd337a669a08)
C:\Windows\System32\wercplsupport.dll
15:34:01.0525 3616     wercplsupport - ok
15:34:01.0537 3616     WerSvc          (6d137963730144698cbd10f202e9f251)
C:\Windows\System32\WerSvc.dll
15:34:01.0539 3616     WerSvc - ok
15:34:01.0597 3616     WfpLwf          (611b23304bf067451a9fdee01fbdd725)
C:\Windows\system32\DRIVERS\wfplwf.sys
15:34:01.0599 3616     WfpLwf - ok
15:34:01.0619 3616     WIMMount        (05ecaec3e4529a7153b3136ceb49f0ec)
C:\Windows\system32\drivers\wimmount.sys
15:34:01.0656 3616     WIMMount - ok
15:34:01.0671 3616     WinDefend - ok
15:34:01.0681 3616     WinHttpAutoProxySvc - ok
15:34:01.0753 3616     Winmgmt         (19b07e7e8915d701225da41cb3877306)
C:\Windows\system32\wbem\WMIsvc.dll
15:34:01.0757 3616     Winmgmt - ok
15:34:01.0869 3616     WinRM           (bcb1310604aa415c4508708975b3931e)
C:\Windows\system32\WsmSvc.dll
15:34:01.0888 3616     WinRM - ok
15:34:02.0000 3616     WinUsb          (fe88b288356e7b47b74b13372add906d)
C:\Windows\system32\DRIVERS\WinUsb.sys
15:34:02.0000 3616     WinUsb - ok
15:34:02.0064 3616     Wlansvc         (4fada86e62f18a1b2f42ba18ae24e6aa)
C:\Windows\System32\wlansvc.dll
15:34:02.0072 3616     Wlansvc - ok
15:34:02.0089 3616     WmiAcpi         (f6ff8944478594d0e414d3f048f0d778)
C:\Windows\system32\drivers\wmiacpi.sys
15:34:02.0091 3616     WmiAcpi - ok
15:34:02.0140 3616     wmiApSrv        (38b84c94c5a8af291adfea478ae54f93)
C:\Windows\system32\wbem\WmiApSrv.exe
15:34:02.0142 3616     wmiApSrv - ok
15:34:02.0169 3616     WMPNetworkSvc - ok
15:34:02.0181 3616     WPCSvc          (96c6e7100d724c69fcf9e7bf590d1dca)
C:\Windows\System32\wpcsvc.dll
15:34:02.0183 3616     WPCSvc - ok
```

```
15:34:02.0205 3616     WPDBusEnum      (93221146d4ebbf314c29b23cd6cc391d)
C:\Windows\system32\wpdbusenum.dll
15:34:02.0208 3616     WPDBusEnum - ok
15:34:02.0232 3616     ws2ifsl         (6bcc1d7d2fd2453957c5479a32364e52)
C:\Windows\system32\drivers\ws2ifsl.sys
15:34:02.0248 3616     ws2ifsl - ok
15:34:02.0265 3616     wscsvc          (e8b1fe6669397d1772d8196df0e57a9e)
C:\Windows\System32\wscsvc.dll
15:34:02.0269 3616     wscsvc - ok
15:34:02.0273 3616     WSearch - ok
15:34:02.0513 3616     wuauserv        (d9ef901dca379cfe914e9fa13b73b4c4)
C:\Windows\system32\wuaueng.dll
15:34:02.0546 3616     wuauserv - ok
15:34:02.0638 3616     WudfPf          (d3381dc54c34d79b22cee0d65ba91b7c)
C:\Windows\system32\drivers\WudfPf.sys
15:34:02.0638 3616     WudfPf - ok
15:34:02.0667 3616     WUDFRd          (cf8d590be3373029d57af80914190682)
C:\Windows\system32\DRIVERS\WUDFRd.sys
15:34:02.0669 3616     WUDFRd - ok
15:34:02.0697 3616     wudfsvc         (7a95c95b6c4cf292d689106bcae49543)
C:\Windows\System32\WUDFSvc.dll
15:34:02.0699 3616     wudfsvc - ok
15:34:02.0726 3616     WwanSvc         (9a3452b3c2a46c073166c5cf49fad1ae)
C:\Windows\System32\wwansvc.dll
15:34:02.0730 3616     WwanSvc - ok
15:34:02.0751 3616     MBR (0x1B8)     (a36c5e4f47e84449ff07ed3517b43a31)
\Device\Harddisk0\DR0
15:34:03.0269 3616     \Device\Harddisk0\DR0 - ok
15:34:03.0273 3616     Boot (0x1200)   (e69930abac2385be7360b2b1ebef4080)
\Device\Harddisk0\DR0\Partition0
15:34:03.0275 3616     \Device\Harddisk0\DR0\Partition0 - ok
15:34:03.0285 3616     Boot (0x1200)   (005874abee4a5ab8683099048e03c51c)
\Device\Harddisk0\DR0\Partition1
15:34:03.0287 3616     \Device\Harddisk0\DR0\Partition1 - ok
15:34:03.0287 3616
      ============================================================
15:34:03.0287 3616     Scan finished
15:34:03.0287 3616
      ============================================================
15:34:03.0298 2972     Detected object count: 1
15:34:03.0298 2972     Actual detected object count: 1
15:34:08.0503 2972     C:\Windows\system32\Drivers\sptd.sys - copied to
quarantine
15:34:08.0511 2972     sptd ( LockedFile.Multi.Generic ) - User select
action: Quarantine
15:34:17.0355 3944
      ============================================================
15:34:17.0355 3944     Scan started
15:34:17.0355 3944     Mode: Manual;
15:34:17.0355 3944
      ============================================================
15:34:17.0593 3944     1394ohci        (a87d604aea360176311474c87a63bb88)
C:\Windows\system32\drivers\1394ohci.sys
15:34:17.0595 3944     1394ohci - ok
15:34:17.0628 3944     ACPI            (d81d9e70b8a6dd14d42d7b4efa65d5f2)
C:\Windows\system32\drivers\ACPI.sys
15:34:17.0630 3944     ACPI - ok
```

```
15:34:17.0648 3944     AcpiPmi         (99f8e788246d495ce3794d7e7821d2ca)
C:\Windows\system32\drivers\acpipmi.sys
15:34:17.0648 3944     AcpiPmi - ok
15:34:17.0703 3944     AdobeARMservice (11a52cf7b265631deeb24c6149309eff)
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
15:34:17.0705 3944     AdobeARMservice - ok
15:34:17.0792 3944     AdobeFlashPlayerUpdateSvc
(76d5a3d2a50402a0b9b6ed13c4371e79)
C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
15:34:17.0796 3944     AdobeFlashPlayerUpdateSvc - ok
15:34:17.0851 3944     adp94xx         (2f6b34b83843f0c5118b63ac634f5bf4)
C:\Windows\system32\DRIVERS\adp94xx.sys
15:34:17.0859 3944     adp94xx - ok
15:34:17.0896 3944     adpahci         (597f78224ee9224ea1a13d6350ced962)
C:\Windows\system32\DRIVERS\adpahci.sys
15:34:17.0927 3944     adpahci - ok
15:34:17.0945 3944     adpu320         (e109549c90f62fb570b9540c4b148e54)
C:\Windows\system32\DRIVERS\adpu320.sys
15:34:17.0947 3944     adpu320 - ok
15:34:17.0968 3944     AeLookupSvc     (4b78b431f225fd8624c5655cb1de7b61)
C:\Windows\System32\aelupsvc.dll
15:34:17.0968 3944     AeLookupSvc - ok
15:34:18.0015 3944     AFD             (1c7857b62de5994a75b054a9fd4c3825)
C:\Windows\system32\drivers\afd.sys
15:34:18.0019 3944     AFD - ok
15:34:18.0044 3944     agp440          (608c14dba7299d8cb6ed035a68a15799)
C:\Windows\system32\drivers\agp440.sys
15:34:18.0044 3944     agp440 - ok
15:34:18.0060 3944     ALG             (3290d6946b5e30e70414990574883ddb)
C:\Windows\System32\alg.exe
15:34:18.0060 3944     ALG - ok
15:34:18.0070 3944     aliide          (5812713a477a3ad7363c7438ca2ee038)
C:\Windows\system32\drivers\aliide.sys
15:34:18.0070 3944     aliide - ok
15:34:18.0078 3944     amdide          (1ff8b4431c353ce385c875f194924c0c)
C:\Windows\system32\drivers\amdide.sys
15:34:18.0078 3944     amdide - ok
15:34:18.0089 3944     AmdK8           (7024f087cff1833a806193ef9d22cda9)
C:\Windows\system32\DRIVERS\amdk8.sys
15:34:18.0091 3944     AmdK8 - ok
15:34:18.0099 3944     AmdPPM          (1e56388b3fe0d031c44144eb8c4d6217)
C:\Windows\system32\DRIVERS\amdppm.sys
15:34:18.0099 3944     AmdPPM - ok
15:34:18.0125 3944     amdsata         (d4121ae6d0c0e7e13aa221aa57ef2d49)
C:\Windows\system32\drivers\amdsata.sys
15:34:18.0125 3944     amdsata - ok
15:34:18.0144 3944     amdsbs          (f67f933e79241ed32ff46a4f29b5120b)
C:\Windows\system32\DRIVERS\amdsbs.sys
15:34:18.0146 3944     amdsbs - ok
15:34:18.0162 3944     amdxata         (540daf1cea6094886d72126fd7c33048)
C:\Windows\system32\drivers\amdxata.sys
15:34:18.0164 3944     amdxata - ok
15:34:18.0183 3944     AppID           (89a69c3f2f319b43379399547526d952)
C:\Windows\system32\drivers\appid.sys
15:34:18.0185 3944     AppID - ok
15:34:18.0201 3944     AppIDSvc        (0bc381a15355a3982216f7172f545de1)
C:\Windows\System32\appidsvc.dll
15:34:18.0201 3944     AppIDSvc - ok
```

```
15:34:18.0222 3944     Appinfo         (3977d4a871ca0d4f2ed1e7db46829731)
C:\Windows\System32\appinfo.dll
15:34:18.0224 3944     Appinfo - ok
15:34:18.0251 3944     AppMgmt         (4aba3e75a76195a3e38ed2766c962899)
C:\Windows\System32\appmgmts.dll
15:34:18.0253 3944     AppMgmt - ok
15:34:18.0269 3944     arc             (c484f8ceb1717c540242531db7845c4e)
C:\Windows\system32\DRIVERS\arc.sys
15:34:18.0271 3944     arc - ok
15:34:18.0279 3944     arcsas          (019af6924aefe7839f61c830227fe79c)
C:\Windows\system32\DRIVERS\arcsas.sys
15:34:18.0281 3944     arcsas - ok
15:34:18.0298 3944     AsyncMac        (769765ce2cc62867468cea93969b2242)
C:\Windows\system32\DRIVERS\asyncmac.sys
15:34:18.0314 3944     AsyncMac - ok
15:34:18.0343 3944     atapi           (02062c0b390b7729edc9e69c680a6f3c)
C:\Windows\system32\drivers\atapi.sys
15:34:18.0343 3944     atapi - ok
15:34:18.0406 3944     AudioEndpointBuilder
(f23fef6d569fce88671949894a8becf1) C:\Windows\System32\Audiosrv.dll
15:34:18.0412 3944     AudioEndpointBuilder - ok
15:34:18.0419 3944     AudioSrv        (f23fef6d569fce88671949894a8becf1)
C:\Windows\System32\Audiosrv.dll
15:34:18.0425 3944     AudioSrv - ok
15:34:18.0451 3944     AxInstSV        (a6bf31a71b409dfa8cac83159e1e2aff)
C:\Windows\System32\AxInstSV.dll
15:34:18.0453 3944     AxInstSV - ok
15:34:18.0468 3944     Axtmvflt        (344b907477ff1bc01bd315ab93df9764)
C:\Windows\system32\DRIVERS\Axtmvflt.sys
15:34:18.0470 3944     Axtmvflt - ok
15:34:18.0484 3944     Axtmvmdm        (4f8d9a8c04c33496403cc4dde3e9d6ce)
C:\Windows\system32\DRIVERS\Axtmvmdm.sys
15:34:18.0484 3944     Axtmvmdm - ok
15:34:18.0496 3944     Axtmvprt        (c24f39e3cc13fa14477ebe12461739ff)
C:\Windows\system32\Drivers\Axtmvprt.sys
15:34:18.0498 3944     Axtmvprt - ok
15:34:18.0531 3944     b06bdrv         (3e5b191307609f7514148c6832bb0842)
C:\Windows\system32\DRIVERS\bxvbda.sys
15:34:18.0533 3944     b06bdrv - ok
15:34:18.0560 3944     b57nd60a        (b5ace6968304a3900eeb1ebfd9622df2)
C:\Windows\system32\DRIVERS\b57nd60a.sys
15:34:18.0580 3944     b57nd60a - ok
15:34:18.0605 3944     BDESVC          (fde360167101b4e45a96f939f388aeb0)
C:\Windows\System32\bdesvc.dll
15:34:18.0605 3944     BDESVC - ok
15:34:18.0617 3944     Beep            (16a47ce2decc9b099349a5f840654746)
C:\Windows\system32\drivers\Beep.sys
15:34:18.0617 3944     Beep - ok
15:34:18.0669 3944     BFE             (82974d6a2fd19445cc5171fc378668a4)
C:\Windows\System32\bfe.dll
15:34:18.0675 3944     BFE - ok
15:34:18.0722 3944     BITS            (1ea7969e3271cbc59e1730697dc74682)
C:\Windows\System32\qmgr.dll
15:34:18.0730 3944     BITS - ok
15:34:18.0763 3944     blbdrive        (61583ee3c3a17003c4acd0475646b4d3)
C:\Windows\system32\DRIVERS\blbdrive.sys
15:34:18.0763 3944     blbdrive - ok
```

```
15:34:18.0792 3944     bowser          (6c02a83164f5cc0a262f4199f0871cf5)
C:\Windows\system32\DRIVERS\bowser.sys
15:34:18.0794 3944     bowser - ok
15:34:18.0800 3944     BrFiltLo        (f09eee9edc320b5e1501f749fde686c8)
C:\Windows\system32\DRIVERS\BrFiltLo.sys
15:34:18.0800 3944     BrFiltLo - ok
15:34:18.0816 3944     BrFiltUp        (b114d3098e9bdb8bea8b053685831be6)
C:\Windows\system32\DRIVERS\BrFiltUp.sys
15:34:18.0816 3944     BrFiltUp - ok
15:34:18.0853 3944     Browser         (8ef0d5c41ec907751b8429162b1239ed)
C:\Windows\System32\browser.dll
15:34:18.0855 3944     Browser - ok
15:34:18.0878 3944     Brserid         (43bea8d483bf1870f018e2d02e06a5bd)
C:\Windows\System32\Drivers\Brserid.sys
15:34:18.0882 3944     Brserid - ok
15:34:18.0892 3944     BrSerWdm        (a6eca2151b08a09caceca35c07f05b42)
C:\Windows\System32\Drivers\BrSerWdm.sys
15:34:18.0892 3944     BrSerWdm - ok
15:34:18.0908 3944     BrUsbMdm        (b79968002c277e869cf38bd22cd61524)
C:\Windows\System32\Drivers\BrUsbMdm.sys
15:34:18.0908 3944     BrUsbMdm - ok
15:34:18.0923 3944     BrUsbSer        (a87528880231c54e75ea7a44943b38bf)
C:\Windows\System32\Drivers\BrUsbSer.sys
15:34:18.0925 3944     BrUsbSer - ok
15:34:18.0947 3944     BthEnum         (cf98190a94f62e405c8cb255018b2315)
C:\Windows\system32\drivers\BthEnum.sys
15:34:18.0947 3944     BthEnum - ok
15:34:18.0962 3944     BTHMODEM        (9da669f11d1f894ab4eb69bf546a42e8)
C:\Windows\system32\DRIVERS\bthmodem.sys
15:34:18.0964 3944     BTHMODEM - ok
15:34:18.0990 3944     BthPan          (02dd601b708dd0667e1331fa8518e9ff)
C:\Windows\system32\DRIVERS\bthpan.sys
15:34:18.0992 3944     BthPan - ok
15:34:19.0042 3944     BTHPORT         (64c198198501f7560ee41d8d1efa7952)
C:\Windows\System32\Drivers\BTHport.sys
15:34:19.0046 3944     BTHPORT - ok
15:34:19.0074 3944     bthserv         (95f9c2976059462cbbf227f7aab10de9)
C:\Windows\system32\bthserv.dll
15:34:19.0076 3944     bthserv - ok
15:34:19.0095 3944     BTHUSB          (f188b7394d81010767b6df3178519a37)
C:\Windows\System32\Drivers\BTHUSB.sys
15:34:19.0095 3944     BTHUSB - ok
15:34:19.0109 3944     cdfs            (b8bd2bb284668c84865658c77574381a)
C:\Windows\system32\DRIVERS\cdfs.sys
15:34:19.0111 3944     cdfs - ok
15:34:19.0142 3944     cdrom           (f036ce71586e93d94dab220d7bdf4416)
C:\Windows\system32\DRIVERS\cdrom.sys
15:34:19.0144 3944     cdrom - ok
15:34:19.0173 3944     CertPropSvc     (f17d1d393bbc69c5322fbfafaca28c7f)
C:\Windows\System32\certprop.dll
15:34:19.0173 3944     CertPropSvc - ok
15:34:19.0189 3944     circlass        (d7cd5c4e1b71fa62050515314cfb52cf)
C:\Windows\system32\DRIVERS\circlass.sys
15:34:19.0189 3944     circlass - ok
15:34:19.0220 3944     CLFS            (fe1ec06f2253f691fe36217c592a0206)
C:\Windows\system32\CLFS.sys
15:34:19.0253 3944     CLFS - ok
```

```
15:34:19.0318 3944     clr_optimization_v2.0.50727_32
(d88040f816fda31c3b466f0fa0918f29)
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe
15:34:19.0320 3944     clr_optimization_v2.0.50727_32 - ok
15:34:19.0371 3944     clr_optimization_v2.0.50727_64
(d1ceea2b47cb998321c579651ce3e4f8)
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorsvw.exe
15:34:19.0375 3944     clr_optimization_v2.0.50727_64 - ok
15:34:19.0425 3944     clr_optimization_v4.0.30319_32
(c5a75eb48e2344abdc162bda79e16841)
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
15:34:19.0429 3944     clr_optimization_v4.0.30319_32 - ok
15:34:19.0476 3944     clr_optimization_v4.0.30319_64
(c6f9af94dcd58122a4d7e89db6bed29d)
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
15:34:19.0482 3944     clr_optimization_v4.0.30319_64 - ok
15:34:19.0507 3944     CmBatt          (0840155d0bddf1190f84a663c284bd33)
C:\Windows\system32\DRIVERS\CmBatt.sys
15:34:19.0507 3944     CmBatt - ok
15:34:19.0527 3944     cmdide          (e19d3f095812725d88f9001985b94edd)
C:\Windows\system32\drivers\cmdide.sys
15:34:19.0529 3944     cmdide - ok
15:34:19.0570 3944     CNG             (c4943b6c962e4b82197542447ad599f4)
C:\Windows\system32\Drivers\cng.sys
15:34:19.0574 3944     CNG - ok
15:34:19.0583 3944     Compbatt        (102de219c3f61415f964c88e9085ad14)
C:\Windows\system32\DRIVERS\compbatt.sys
15:34:19.0583 3944     Compbatt - ok
15:34:19.0605 3944     CompositeBus    (03edb043586cceba243d689bdda370a8)
C:\Windows\system32\drivers\CompositeBus.sys
15:34:19.0607 3944     CompositeBus - ok
15:34:19.0611 3944     COMSysApp - ok
15:34:19.0623 3944     crcdisk         (1c827878a998c18847245fe1f34ee597)
C:\Windows\system32\DRIVERS\crcdisk.sys
15:34:19.0623 3944     crcdisk - ok
15:34:19.0654 3944     CryptSvc        (4f5414602e2544a4554d95517948b705)
C:\Windows\system32\cryptsvc.dll
15:34:19.0656 3944     CryptSvc - ok
15:34:19.0703 3944     CSC             (54da3dfd29ed9f1619b6f53f3ce55e49)
C:\Windows\system32\drivers\csc.sys
15:34:19.0708 3944     CSC - ok
15:34:19.0759 3944     CscService      (3ab183ab4d2c79dcf459cd2c1266b043)
C:\Windows\System32\cscsvc.dll
15:34:19.0763 3944     CscService - ok
15:34:19.0796 3944     DcomLaunch      (5c627d1b1138676c0a7ab2c2c190d123)
C:\Windows\system32\rpcss.dll
15:34:19.0802 3944     DcomLaunch - ok
15:34:19.0832 3944     defragsvc       (3cec7631a84943677aa8fa8ee5b6b43d)
C:\Windows\System32\defragsvc.dll
15:34:19.0835 3944     defragsvc - ok
15:34:19.0882 3944     DfsC            (9bb2ef44eaa163b29c4a4587887a0fe4)
C:\Windows\system32\Drivers\dfsc.sys
15:34:19.0884 3944     DfsC - ok
15:34:19.0908 3944     Dhcp            (43d808f5d9e1a18e5eeb5ebc83969e4e)
C:\Windows\system32\dhcpcore.dll
15:34:19.0912 3944     Dhcp - ok
15:34:19.0935 3944     discache        (13096b05847ec78f0977f2c0f79e9ab3)
C:\Windows\system32\drivers\discache.sys
```

```
15:34:19.0968 3944     discache - ok
15:34:19.0976 3944     Disk            (9819eee8b5ea3784ec4af3b137a5244c)
C:\Windows\system32\DRIVERS\disk.sys
15:34:19.0976 3944     Disk - ok
15:34:20.0017 3944     Dnscache        (16835866aaa693c7d7fceba8fff706e4)
C:\Windows\System32\dnsrslvr.dll
15:34:20.0019 3944     Dnscache - ok
15:34:20.0054 3944     dot3svc         (b1fb3ddca0fdf408750d5843591afbc6)
C:\Windows\System32\dot3svc.dll
15:34:20.0056 3944     dot3svc - ok
15:34:20.0087 3944     DPS             (b26f4f737e8f9df4f31af6cf31d05820)
C:\Windows\system32\dps.dll
15:34:20.0089 3944     DPS - ok
15:34:20.0105 3944     drmkaud         (9b19f34400d24df84c858a421c205754)
C:\Windows\system32\drivers\drmkaud.sys
15:34:20.0105 3944     drmkaud - ok
15:34:20.0166 3944     DXGKrnl         (f5bee30450e18e6b83a5012c100616fd)
C:\Windows\System32\drivers\dxgkrnl.sys
15:34:20.0171 3944     DXGKrnl - ok
15:34:20.0175 3944     EagleX64 - ok
15:34:20.0199 3944     eamonm          (398fdc5694f2ba9e51e321ca40d1706e)
C:\Windows\system32\DRIVERS\eamonm.sys
15:34:20.0201 3944     eamonm - ok
15:34:20.0228 3944     EapHost         (e2dda8726da9cb5b2c4000c9018a9633)
C:\Windows\System32\eapsvc.dll
15:34:20.0230 3944     EapHost - ok
15:34:20.0367 3944     ebdrv           (dc5d737f51be844d8c82c695eb17372f)
C:\Windows\system32\DRIVERS\evbda.sys
15:34:20.0388 3944     ebdrv - ok
15:34:20.0460 3944     EFS             (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\System32\lsass.exe
15:34:20.0462 3944     EFS - ok
15:34:20.0488 3944     ehdrv           (e99457900012b53b2226f146ecaf9136)
C:\Windows\system32\DRIVERS\ehdrv.sys
15:34:20.0488 3944     ehdrv - ok
15:34:20.0548 3944     ehRecvr         (c4002b6b41975f057d98c439030cea07)
C:\Windows\ehome\ehRecvr.exe
15:34:20.0554 3944     ehRecvr - ok
15:34:20.0585 3944     ehSched         (4705e8ef9934482c5bb488ce28afc681)
C:\Windows\ehome\ehsched.exe
15:34:20.0587 3944     ehSched - ok
15:34:20.0636 3944     EhttpSrv        (11c3ad68dcf80201c9f74edee6da3804)
C:\Program Files\ESET\ESET NOD32 Antivirus\EHttpSrv.exe
15:34:20.0636 3944     EhttpSrv - ok
15:34:20.0718 3944     ekrn            (efa198f8983d064a81052851f7bb80c2)
C:\Program Files\ESET\ESET NOD32 Antivirus\x86\ekrn.exe
15:34:20.0724 3944     ekrn - ok
15:34:20.0822 3944     elxstor         (0e5da5369a0fcaea12456dd852545184)
C:\Windows\system32\DRIVERS\elxstor.sys
15:34:20.0826 3944     elxstor - ok
15:34:20.0851 3944     epfwwfpr        (a2af094dcbe8bff7e898d327750506a0)
C:\Windows\system32\DRIVERS\epfwwfpr.sys
15:34:20.0851 3944     epfwwfpr - ok
15:34:20.0876 3944     ErrDev          (34a3c54752046e79a126e15c51db409b)
C:\Windows\system32\drivers\errdev.sys
15:34:20.0876 3944     ErrDev - ok
15:34:20.0921 3944     EventSystem     (4166f82be4d24938977dd1746be9b8a0)
C:\Windows\system32\es.dll
```

```
15:34:20.0925 3944     EventSystem - ok
15:34:20.0945 3944     exfat           (a510c654ec00c1e9bdd91eeb3a59823b)
C:\Windows\system32\drivers\exfat.sys
15:34:20.0947 3944     exfat - ok
15:34:20.0966 3944     fastfat         (0adc83218b66a6db380c330836f3e36d)
C:\Windows\system32\drivers\fastfat.sys
15:34:20.0968 3944     fastfat - ok
15:34:21.0027 3944     Fax             (dbefd454f8318a0ef691fdd2eaab44eb)
C:\Windows\system32\fxssvc.exe
15:34:21.0033 3944     Fax - ok
15:34:21.0046 3944     fdc             (d765d19cd8ef61f650c384f62fac00ab)
C:\Windows\system32\DRIVERS\fdc.sys
15:34:21.0048 3944     fdc - ok
15:34:21.0056 3944     fdPHost         (0438cab2e03f4fb61455a7956026fe86)
C:\Windows\system32\fdPHost.dll
15:34:21.0058 3944     fdPHost - ok
15:34:21.0066 3944     FDResPub        (802496cb59a30349f9a6dd22d6947644)
C:\Windows\system32\fdrespub.dll
15:34:21.0068 3944     FDResPub - ok
15:34:21.0085 3944     FileInfo        (655661be46b5f5f3fd454e2c3095b930)
C:\Windows\system32\drivers\fileinfo.sys
15:34:21.0087 3944     FileInfo - ok
15:34:21.0099 3944     Filetrace       (5f671ab5bc87eea04ec38a6cd5962a47)
C:\Windows\system32\drivers\filetrace.sys
15:34:21.0101 3944     Filetrace - ok
15:34:21.0117 3944     flpydisk        (c172a0f53008eaeb8ea33fe10e177af5)
C:\Windows\system32\DRIVERS\flpydisk.sys
15:34:21.0119 3944     flpydisk - ok
15:34:21.0138 3944     FltMgr          (da6b67270fd9db3697b20fce94950741)
C:\Windows\system32\drivers\fltmgr.sys
15:34:21.0142 3944     FltMgr - ok
15:34:21.0205 3944     FontCache       (5c4cb4086fb83115b153e47add961a0c)
C:\Windows\system32\FntCache.dll
15:34:21.0212 3944     FontCache - ok
15:34:21.0267 3944     FontCache3.0.0.0
(a8b7f3818ab65695e3a0bb3279f6dce6)
C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe
15:34:21.0267 3944     FontCache3.0.0.0 - ok
15:34:21.0294 3944     FsDepends       (d4370349614997189070 3b4b1b723eac)
C:\Windows\system32\drivers\FsDepends.sys
15:34:21.0296 3944     FsDepends - ok
15:34:21.0316 3944     Fs_Rec          (6bd9295cc032dd3077c671fccf579a7b)
C:\Windows\system32\drivers\Fs_Rec.sys
15:34:21.0316 3944     Fs_Rec - ok
15:34:21.0343 3944     fvevol          (1f7b25b858fa27015169fe95e54108ed)
C:\Windows\system32\DRIVERS\fvevol.sys
15:34:21.0345 3944     fvevol - ok
15:34:21.0363 3944     gagp30kx        (8c778d335c9d272cfd3298ab02abe3b6)
C:\Windows\system32\DRIVERS\gagp30kx.sys
15:34:21.0365 3944     gagp30kx - ok
15:34:21.0412 3944     gpsvc           (277bbc7e1aa1ee957f573a10eca7ef3a)
C:\Windows\System32\gpsvc.dll
15:34:21.0419 3944     gpsvc - ok
15:34:21.0435 3944     hcw85cir        (f2523ef6460fc42405b12248338ab2f0)
C:\Windows\system32\drivers\hcw85cir.sys
15:34:21.0435 3944     hcw85cir - ok
15:34:21.0470 3944     HdAudAddService (975761c778e33cd22498059b91e7373a)
C:\Windows\system32\drivers\HdAudio.sys
```

```
15:34:21.0474 3944     HdAudAddService - ok
15:34:21.0501 3944     HDAudBus        (97bfed39b6b79eb12cddbfeed51f56bb)
C:\Windows\system32\drivers\HDAudBus.sys
15:34:21.0503 3944     HDAudBus - ok
15:34:21.0517 3944     HidBatt         (78e86380454a7b10a5eb255dc44a355f)
C:\Windows\system32\DRIVERS\HidBatt.sys
15:34:21.0519 3944     HidBatt - ok
15:34:21.0535 3944     HidBth          (7fd2a313f7afe5c4dab14798c48dd104)
C:\Windows\system32\DRIVERS\hidbth.sys
15:34:21.0537 3944     HidBth - ok
15:34:21.0544 3944     HidIr           (0a77d29f311b88cfae3b13f9c1a73825)
C:\Windows\system32\DRIVERS\hidir.sys
15:34:21.0546 3944     HidIr - ok
15:34:21.0570 3944     hidserv         (bd9eb3958f213f96b97b1d897dee006d)
C:\Windows\system32\hidserv.dll
15:34:21.0572 3944     hidserv - ok
15:34:21.0593 3944     HidUsb          (9592090a7e2b61cd582b612b6df70536)
C:\Windows\system32\DRIVERS\hidusb.sys
15:34:21.0595 3944     HidUsb - ok
15:34:21.0621 3944     hkmsvc          (387e72e739e15e3d37907a86d9ff98e2)
C:\Windows\system32\kmsvc.dll
15:34:21.0623 3944     hkmsvc - ok
15:34:21.0648 3944     HomeGroupListener
(efdfb3dd38a4376f93e7985173813abd) C:\Windows\system32\ListSvc.dll
15:34:21.0652 3944     HomeGroupListener - ok
15:34:21.0693 3944     HomeGroupProvider
(908acb1f594274965a53926b10c81e89) C:\Windows\system32\provsvc.dll
15:34:21.0697 3944     HomeGroupProvider - ok
15:34:21.0716 3944     HpSAMD          (39d2abcd392f3d8a6dce7b60ae7b8efc)
C:\Windows\system32\drivers\HpSAMD.sys
15:34:21.0718 3944     HpSAMD - ok
15:34:21.0785 3944     HTTP            (0ea7de1acb728dd5a369fd742d6eee28)
C:\Windows\system32\drivers\HTTP.sys
15:34:21.0794 3944     HTTP - ok
15:34:21.0808 3944     hwpolicy        (a5462bd6884960c9dc85ed49d34ff392)
C:\Windows\system32\drivers\hwpolicy.sys
15:34:21.0810 3944     hwpolicy - ok
15:34:21.0845 3944     i8042prt        (fa55c73d4affa7ee23ac4be53b4592d3)
C:\Windows\system32\drivers\i8042prt.sys
15:34:21.0847 3944     i8042prt - ok
15:34:21.0898 3944     iaStorV         (aaaf44db3bd0b9d1fb6969b23ecc8366)
C:\Windows\system32\drivers\iaStorV.sys
15:34:21.0902 3944     iaStorV - ok
15:34:21.0990 3944     idsvc           (5988fc40f8db5b0739cd1e3a5d0d78bd)
C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\infocard.exe
15:34:21.0998 3944     idsvc - ok
15:34:22.0021 3944     iirsp           (5c18831c61933628f5bb0ea2675b9d21)
C:\Windows\system32\DRIVERS\iirsp.sys
15:34:22.0023 3944     iirsp - ok
15:34:22.0072 3944     IKEEXT          (fcd84c381e0140af901e58d48882d26b)
C:\Windows\System32\ikeext.dll
15:34:22.0080 3944     IKEEXT - ok
15:34:22.0216 3944     IntcAzAudAddService
(e8017f1662d9142f45ceab694d013c00)
C:\Windows\system32\drivers\RTKVHD64.sys
15:34:22.0234 3944     IntcAzAudAddService - ok
```

```
15:34:22.0314 3944     intelide        (f00f20e70c6ec3aa366910083a0518aa)
C:\Windows\system32\drivers\intelide.sys
15:34:22.0316 3944     intelide - ok
15:34:22.0343 3944     intelppm        (ada036632c664caa754079041cf1f8c1)
C:\Windows\system32\DRIVERS\intelppm.sys
15:34:22.0343 3944     intelppm - ok
15:34:22.0367 3944     IPBusEnum       (098a91c54546a3b878dad6a7e90a455b)
C:\Windows\system32\ipbusenum.dll
15:34:22.0369 3944     IPBusEnum - ok
15:34:22.0396 3944     IpFilterDriver  (c9f0e1bd74365a8771590e9008d22ab6)
C:\Windows\system32\DRIVERS\ipfltdrv.sys
15:34:22.0396 3944     IpFilterDriver - ok
15:34:22.0437 3944     iphlpsvc        (a34a587fffd45fa649fba6d03784d257)
C:\Windows\System32\iphlpsvc.dll
15:34:22.0441 3944     iphlpsvc - ok
15:34:22.0476 3944     IPMIDRV         (0fc1aea580957aa8817b8f305d18ca3a)
C:\Windows\system32\drivers\IPMIDrv.sys
15:34:22.0478 3944     IPMIDRV - ok
15:34:22.0494 3944     IPNAT           (af9b39a7e7b6caa203b3862582e9f2d0)
C:\Windows\system32\drivers\ipnat.sys
15:34:22.0494 3944     IPNAT - ok
15:34:22.0509 3944     IRENUM          (3abf5e7213eb28966d55d58b515d5ce9)
C:\Windows\system32\drivers\irenum.sys
15:34:22.0509 3944     IRENUM - ok
15:34:22.0533 3944     isapnp          (2f7b28dc3e1183e5eb418df55c204f38)
C:\Windows\system32\drivers\isapnp.sys
15:34:22.0535 3944     isapnp - ok
15:34:22.0564 3944     iScsiPrt        (d931d7309deb2317035b07c9f9e6b0bd)
C:\Windows\system32\drivers\msiscsi.sys
15:34:22.0582 3944     iScsiPrt - ok
15:34:22.0601 3944     kbdclass        (bc02336f1cba7dcc7d1213bb588a68a5)
C:\Windows\system32\DRIVERS\kbdclass.sys
15:34:22.0603 3944     kbdclass - ok
15:34:22.0626 3944     kbdhid          (0705eff5b42a9db58548eec3b26bb484)
C:\Windows\system32\DRIVERS\kbdhid.sys
15:34:22.0626 3944     kbdhid - ok
15:34:22.0644 3944     KeyIso          (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:34:22.0646 3944     KeyIso - ok
15:34:22.0656 3944     KSecDD          (da1e991a61cfdd755a589e206b97644b)
C:\Windows\system32\Drivers\ksecdd.sys
15:34:22.0656 3944     KSecDD - ok
15:34:22.0671 3944     KSecPkg         (7e33198d956943a4f11a5474c1e9106f)
C:\Windows\system32\Drivers\ksecpkg.sys
15:34:22.0673 3944     KSecPkg - ok
15:34:22.0677 3944     ksthunk         (6869281e78cb31a43e969f06b57347c4)
C:\Windows\system32\drivers\ksthunk.sys
15:34:22.0679 3944     ksthunk - ok
15:34:22.0716 3944     KtmRm           (6ab66e16aa859232f64deb66887a8c9c)
C:\Windows\system32\msdtckrm.dll
15:34:22.0722 3944     KtmRm - ok
15:34:22.0765 3944     LanmanServer    (d9f42719019740baa6d1c6d536cbdaa6)
C:\Windows\system32\srvsvc.dll
15:34:22.0767 3944     LanmanServer - ok
15:34:22.0796 3944     LanmanWorkstation
(851a1382eed3e3a7476db004f4ee3e1a) C:\Windows\System32\wkssvc.dll
15:34:22.0798 3944     LanmanWorkstation - ok
```

```
15:34:22.0816 3944     lltdio          (1538831cf8ad2979a04c423779465827)
C:\Windows\system32\DRIVERS\lltdio.sys
15:34:22.0816 3944     lltdio - ok
15:34:22.0845 3944     lltdsvc         (c1185803384ab3feed115f79f109427f)
C:\Windows\System32\lltdsvc.dll
15:34:22.0849 3944     lltdsvc - ok
15:34:22.0865 3944     lmhosts         (f993a32249b66c9d622ea5592a8b76b8)
C:\Windows\System32\lmhsvc.dll
15:34:22.0867 3944     lmhosts - ok
15:34:22.0890 3944     LSI_FC          (1a93e54eb0ece102495a51266dcdb6a6)
C:\Windows\system32\DRIVERS\lsi_fc.sys
15:34:22.0892 3944     LSI_FC - ok
15:34:22.0912 3944     LSI_SAS         (1047184a9fdc8bdbff857175875ee810)
C:\Windows\system32\DRIVERS\lsi_sas.sys
15:34:22.0929 3944     LSI_SAS - ok
15:34:22.0941 3944     LSI_SAS2        (30f5c0de1ee8b5bc9306c1f0e4a75f93)
C:\Windows\system32\DRIVERS\lsi_sas2.sys
15:34:22.0941 3944     LSI_SAS2 - ok
15:34:22.0957 3944     LSI_SCSI        (0504eacaff0d3c8aed161c4b0d369d4a)
C:\Windows\system32\DRIVERS\lsi_scsi.sys
15:34:22.0958 3944     LSI_SCSI - ok
15:34:22.0978 3944     luafv           (43d0f98e1d56ccddb0d5254cff7b356e)
C:\Windows\system32\drivers\luafv.sys
15:34:22.0978 3944     luafv - ok
15:34:22.0998 3944     MBAMProtector   (dbc08862a71459e74f7538b432c114cc)
C:\Windows\system32\drivers\mbam.sys
15:34:22.0998 3944     MBAMProtector - ok
15:34:23.0070 3944     MBAMService     (ba400ed640bca1eae5c727ae17c10207)
C:\Program Files (x86)\Malwarebytes' Anti-Malware\mbamservice.exe
15:34:23.0074 3944     MBAMService - ok
15:34:23.0103 3944     Mcx2Svc         (0be09cd858abf9df6ed259d57a1a1663)
C:\Windows\system32\Mcx2Svc.dll
15:34:23.0105 3944     Mcx2Svc - ok
15:34:23.0121 3944     megasas         (a55805f747c6edb6a9080d7c633bd0f4)
C:\Windows\system32\DRIVERS\megasas.sys
15:34:23.0121 3944     megasas - ok
15:34:23.0142 3944     MegaSR          (baf74ce0072480c3b6b7c13b2a94d6b3)
C:\Windows\system32\DRIVERS\MegaSR.sys
15:34:23.0144 3944     MegaSR - ok
15:34:23.0179 3944     Microsoft SharePoint Workspace Audit Service - ok
15:34:23.0218 3944     MMCSS           (e40e80d0304a73e8d269f7141d77250b)
C:\Windows\system32\mmcss.dll
15:34:23.0224 3944     MMCSS - ok
15:34:23.0240 3944     Modem           (800ba92f7010378b09f9ed9270f07137)
C:\Windows\system32\drivers\modem.sys
15:34:23.0242 3944     Modem - ok
15:34:23.0265 3944     monitor         (b03d591dc7da45ece20b3b467e6aadaa)
C:\Windows\system32\DRIVERS\monitor.sys
15:34:23.0267 3944     monitor - ok
15:34:23.0296 3944     mouclass        (7d27ea49f3c1f687d357e77a470aea99)
C:\Windows\system32\DRIVERS\mouclass.sys
15:34:23.0298 3944     mouclass - ok
15:34:23.0306 3944     mouhid          (d3bf052c40b0c4166d9fd86a4288c1e6)
C:\Windows\system32\DRIVERS\mouhid.sys
15:34:23.0306 3944     mouhid - ok
15:34:23.0337 3944     mountmgr        (32e7a3d591d671a6df2db515a5cbe0fa)
C:\Windows\system32\drivers\mountmgr.sys
15:34:23.0359 3944     mountmgr - ok
```

```
15:34:23.0392 3944     MozillaMaintenance
(15d5398eed42c2504bb3d4fc875c15d1) C:\Program Files (x86)\Mozilla
Maintenance Service\maintenanceservice.exe
15:34:23.0394 3944     MozillaMaintenance - ok
15:34:23.0421 3944     mpio            (a44b420d30bd56e145d6a2bc8768ec58)
C:\Windows\system32\drivers\mpio.sys
15:34:23.0423 3944     mpio - ok
15:34:23.0439 3944     mpsdrv          (6c38c9e45ae0ea2fa5e551f2ed5e978f)
C:\Windows\system32\drivers\mpsdrv.sys
15:34:23.0457 3944     mpsdrv - ok
15:34:23.0517 3944     MpsSvc          (54ffc9c8898113ace189d4aa7199d2c1)
C:\Windows\system32\mpssvc.dll
15:34:23.0525 3944     MpsSvc - ok
15:34:23.0550 3944     MRxDAV          (dc722758b8261e1abafd31a3c0a66380)
C:\Windows\system32\drivers\mrxdav.sys
15:34:23.0552 3944     MRxDAV - ok
15:34:23.0585 3944     mrxsmb          (a5d9106a73dc88564c825d317cac68ac)
C:\Windows\system32\DRIVERS\mrxsmb.sys
15:34:23.0587 3944     mrxsmb - ok
15:34:23.0617 3944     mrxsmb10        (d711b3c1d5f42c0c2415687be09fc163)
C:\Windows\system32\DRIVERS\mrxsmb10.sys
15:34:23.0621 3944     mrxsmb10 - ok
15:34:23.0642 3944     mrxsmb20        (9423e9d355c8d303e76b8cfbd8a5c30c)
C:\Windows\system32\DRIVERS\mrxsmb20.sys
15:34:23.0644 3944     mrxsmb20 - ok
15:34:23.0662 3944     msahci          (c25f0bafa182cbca2dd3c851c2e75796)
C:\Windows\system32\drivers\msahci.sys
15:34:23.0664 3944     msahci - ok
15:34:23.0689 3944     msdsm           (db801a638d011b9633829eb6f663c900)
C:\Windows\system32\drivers\msdsm.sys
15:34:23.0707 3944     msdsm - ok
15:34:23.0734 3944     MSDTC           (de0ece52236cfa3ed2dbfc03f28253a8)
C:\Windows\System32\msdtc.exe
15:34:23.0738 3944     MSDTC - ok
15:34:23.0771 3944     Msfs            (aa3fb40e17ce1388fa1bedab50ea8f96)
C:\Windows\system32\drivers\Msfs.sys
15:34:23.0773 3944     Msfs - ok
15:34:23.0781 3944     mshidkmdf       (f9d215a46a8b9753f61767fa72a20326)
C:\Windows\System32\drivers\mshidkmdf.sys
15:34:23.0783 3944     mshidkmdf - ok
15:34:23.0802 3944     msisadrv        (d916874bbd4f8b07bfb7fa9b3ccae29d)
C:\Windows\system32\drivers\msisadrv.sys
15:34:23.0804 3944     msisadrv - ok
15:34:23.0828 3944     MSiSCSI         (808e98ff49b155c522e6400953177b08)
C:\Windows\system32\iscsiexe.dll
15:34:23.0832 3944     MSiSCSI - ok
15:34:23.0833 3944     msiserver - ok
15:34:23.0847 3944     MSKSSRV         (49ccf2c4fea34ffad8b1b59d49439366)
C:\Windows\system32\drivers\MSKSSRV.sys
15:34:23.0849 3944     MSKSSRV - ok
15:34:23.0863 3944     MSPCLOCK        (bdd71ace35a232104ddd349ee70e1ab3)
C:\Windows\system32\drivers\MSPCLOCK.sys
15:34:23.0863 3944     MSPCLOCK - ok
15:34:23.0867 3944     MSPQM           (4ed981241db27c3383d72092b618a1d0)
C:\Windows\system32\drivers\MSPQM.sys
15:34:23.0867 3944     MSPQM - ok
15:34:23.0914 3944     MsRPC           (759a9eeb0fa9ed79da1fb7d4ef78866d)
C:\Windows\system32\drivers\MsRPC.sys
```

```
15:34:23.0916 3944     MsRPC - ok
15:34:23.0929 3944     mssmbios        (0eed230e37515a0eaee3c2e1bc97b288)
C:\Windows\system32\drivers\mssmbios.sys
15:34:23.0931 3944     mssmbios - ok
15:34:23.0939 3944     MSTEE           (2e66f9ecb30b4221a318c92ac2250779)
C:\Windows\system32\drivers\MSTEE.sys
15:34:23.0941 3944     MSTEE - ok
15:34:23.0955 3944     MTConfig        (7ea404308934e675bffde8edf0757bcd)
C:\Windows\system32\DRIVERS\MTConfig.sys
15:34:23.0957 3944     MTConfig - ok
15:34:23.0974 3944     Mup             (f9a18612fd3526fe473c1bda678d61c8)
C:\Windows\system32\Drivers\mup.sys
15:34:23.0976 3944     Mup - ok
15:34:24.0025 3944     napagent        (582ac6d9873e31dfa28a4547270862dd)
C:\Windows\system32\qagentRT.dll
15:34:24.0031 3944     napagent - ok
15:34:24.0062 3944     NativeWifiP     (1ea3749c4114db3e3161156ffffa6b33)
C:\Windows\system32\DRIVERS\nwifi.sys
15:34:24.0064 3944     NativeWifiP - ok
15:34:24.0117 3944     NDIS            (79b47fd40d9a817e932f9d26fac0a81c)
C:\Windows\system32\drivers\ndis.sys
15:34:24.0125 3944     NDIS - ok
15:34:24.0138 3944     NdisCap         (9f9a1f53aad7da4d6fef5bb73ab811ac)
C:\Windows\system32\DRIVERS\ndiscap.sys
15:34:24.0140 3944     NdisCap - ok
15:34:24.0156 3944     NdisTapi        (30639c932d9fef22b31268fe25a1b6e5)
C:\Windows\system32\DRIVERS\ndistapi.sys
15:34:24.0158 3944     NdisTapi - ok
15:34:24.0181 3944     Ndisuio         (136185f9fb2cc61e573e676aa5402356)
C:\Windows\system32\DRIVERS\ndisuio.sys
15:34:24.0181 3944     Ndisuio - ok
15:34:24.0208 3944     NdisWan         (53f7305169863f0a2bddc49e116c2e11)
C:\Windows\system32\DRIVERS\ndiswan.sys
15:34:24.0210 3944     NdisWan - ok
15:34:24.0220 3944     NDProxy         (015c0d8e0e0421b4cfd48cffe2825879)
C:\Windows\system32\drivers\NDProxy.sys
15:34:24.0222 3944     NDProxy - ok
15:34:24.0234 3944     NetBIOS         (86743d9f5d2b1048062b14b1d84501c4)
C:\Windows\system32\DRIVERS\netbios.sys
15:34:24.0234 3944     NetBIOS - ok
15:34:24.0255 3944     NetBT           (09594d1089c523423b32a4229263f068)
C:\Windows\system32\DRIVERS\netbt.sys
15:34:24.0275 3944     NetBT - ok
15:34:24.0302 3944     Netlogon        (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:34:24.0304 3944     Netlogon - ok
15:34:24.0347 3944     Netman          (847d3ae376c0817161a14a82c8922a9e)
C:\Windows\System32\netman.dll
15:34:24.0351 3944     Netman - ok
15:34:24.0380 3944     netprofm        (5f28111c648f1e24f7dbc87cdeb091b8)
C:\Windows\System32\netprofm.dll
15:34:24.0384 3944     netprofm - ok
15:34:24.0455 3944     NetTcpPortSharing
(3e5a36127e201ddf663176b66828fafe)
C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication
Foundation\SMSvcHost.exe
15:34:24.0457 3944     NetTcpPortSharing - ok
```

```
15:34:24.0501 3944     nfrd960         (77889813be4d166cdab78ddba990da92)
C:\Windows\system32\DRIVERS\nfrd960.sys
15:34:24.0503 3944     nfrd960 - ok
15:34:24.0546 3944     NlaSvc          (1ee99a89cc788ada662441d1e9830529)
C:\Windows\System32\nlasvc.dll
15:34:24.0550 3944     NlaSvc - ok
15:34:24.0564 3944     Npfs            (1e4c4ab5c9b8dd13179bbdc75a2a01f7)
C:\Windows\system32\drivers\Npfs.sys
15:34:24.0564 3944     Npfs - ok
15:34:24.0570 3944     nsi             (d54bfdf3e0c953f823b3d0bfe4732528)
C:\Windows\system32\nsisvc.dll
15:34:24.0574 3944     nsi - ok
15:34:24.0587 3944     nsiproxy        (e7f5ae18af4168178a642a9247c63001)
C:\Windows\system32\drivers\nsiproxy.sys
15:34:24.0587 3944     nsiproxy - ok
15:34:24.0691 3944     Ntfs            (a2f74975097f52a00745f9637451fdd8)
C:\Windows\system32\drivers\Ntfs.sys
15:34:24.0705 3944     Ntfs - ok
15:34:24.0791 3944     Null            (9899284589f75fa8724ff3d16aed75c1)
C:\Windows\system32\drivers\Null.sys
15:34:24.0791 3944     Null - ok
15:34:24.0826 3944     NVENETFD        (a85b4f2ef3a7304a5399ef0526423040)
C:\Windows\system32\DRIVERS\nvm62x64.sys
15:34:24.0830 3944     NVENETFD - ok
15:34:25.0271 3944     nvlddmkm        (e55cab397f77d5208db18a78b1b7c0d5)
C:\Windows\system32\DRIVERS\nvlddmkm.sys
15:34:25.0355 3944     nvlddmkm - ok
15:34:25.0416 3944     nvraid          (0a92cb65770442ed0dc44834632f66ad)
C:\Windows\system32\drivers\nvraid.sys
15:34:25.0416 3944     nvraid - ok
15:34:25.0441 3944     nvstor          (dab0e87525c10052bf65f06152f37e4a)
C:\Windows\system32\drivers\nvstor.sys
15:34:25.0443 3944     nvstor - ok
15:34:25.0457 3944     nvsvc           (43bc8151893ae6afe42e149d663c2221)
C:\Windows\system32\nvvsvc.exe
15:34:25.0458 3944     nvsvc - ok
15:34:25.0484 3944     nv_agp          (270d7cd42d6e3979f6dd0146650f0e05)
C:\Windows\system32\drivers\nv_agp.sys
15:34:25.0484 3944     nv_agp - ok
15:34:25.0511 3944     ohci1394        (3589478e4b22ce21b41fa1bfc0b8b8a0)
C:\Windows\system32\drivers\ohci1394.sys
15:34:25.0529 3944     ohci1394 - ok
15:34:25.0580 3944     ose             (9d10f99a6712e28f8acd5641e3a7ea6b)
C:\Program Files (x86)\Common Files\Microsoft Shared\Source
Engine\OSE.EXE
15:34:25.0580 3944     ose - ok
15:34:25.0773 3944     osppsvc         (61bffb5f57ad12f83ab64b7181829b34)
C:\Program Files\Common Files\Microsoft
Shared\OfficeSoftwareProtectionPlatform\OSPPSVC.EXE
15:34:25.0806 3944     osppsvc - ok
15:34:25.0914 3944     p2pimsvc        (3eac4455472cc2c97107b5291e0dcafe)
C:\Windows\system32\pnrpsvc.dll
15:34:25.0921 3944     p2pimsvc - ok
15:34:25.0958 3944     p2psvc          (927463ecb02179f88e4b9a17568c63c3)
C:\Windows\system32\p2psvc.dll
15:34:25.0964 3944     p2psvc - ok
15:34:26.0007 3944     Parport         (0086431c29c35be1dbc43f52cc273887)
C:\Windows\system32\DRIVERS\parport.sys
```

```
15:34:26.0009 3944     Parport - ok
15:34:26.0035 3944     partmgr          (e9766131eeade40a27dc27d2d68fba9c)
C:\Windows\system32\drivers\partmgr.sys
15:34:26.0037 3944     partmgr - ok
15:34:26.0058 3944     PcaSvc           (3aeaa8b561e63452c655dc0584922257)
C:\Windows\System32\pcasvc.dll
15:34:26.0062 3944     PcaSvc - ok
15:34:26.0089 3944     pci              (94575c0571d1462a0f70bde6bd6ee6b3)
C:\Windows\system32\drivers\pci.sys
15:34:26.0091 3944     pci - ok
15:34:26.0103 3944     pciide           (b5b8b5ef2e5cb34df8dcf8831e3534fa)
C:\Windows\system32\drivers\pciide.sys
15:34:26.0103 3944     pciide - ok
15:34:26.0128 3944     pcmcia           (b2e81d4e87ce48589f98cb8c05b01f2f)
C:\Windows\system32\DRIVERS\pcmcia.sys
15:34:26.0146 3944     pcmcia - ok
15:34:26.0158 3944     pcw              (d6b9c2e1a11a3a4b26a182ffef18f603)
C:\Windows\system32\drivers\pcw.sys
15:34:26.0160 3944     pcw - ok
15:34:26.0195 3944     PEAUTH           (68769c3356b3be5d1c732c97b9a80d6e)
C:\Windows\system32\drivers\peauth.sys
15:34:26.0216 3944     PEAUTH - ok
15:34:26.0292 3944     PeerDistSvc      (b9b0a4299dd2d76a4243f75fd54dc680)
C:\Windows\system32\peerdistsvc.dll
15:34:26.0302 3944     PeerDistSvc - ok
15:34:26.0361 3944     PerfHost         (e495e408c93141e8fc72dc0c6046ddfa)
C:\Windows\SysWow64\perfhost.exe
15:34:26.0363 3944     PerfHost - ok
15:34:26.0527 3944     pla              (c7cf6a6e137463219e1259e3f0f0dd6c)
C:\Windows\system32\pla.dll
15:34:26.0548 3944     pla - ok
15:34:26.0589 3944     PlugPlay         (25fbdef06c4d92815b353f6e792c8129)
C:\Windows\system32\umpnpmgr.dll
15:34:26.0593 3944     PlugPlay - ok
15:34:26.0599 3944     PnkBstrA - ok
15:34:26.0605 3944     PnkBstrB - ok
15:34:26.0626 3944     PNRPAutoReg      (7195581cec9bb7d12abe54036acc2e38)
C:\Windows\system32\pnrpauto.dll
15:34:26.0628 3944     PNRPAutoReg - ok
15:34:26.0658 3944     PNRPsvc          (3eac4455472cc2c97107b5291e0dcafe)
C:\Windows\system32\pnrpsvc.dll
15:34:26.0662 3944     PNRPsvc - ok
15:34:26.0707 3944     PolicyAgent      (4f15d75adf6156bf56eced6d4a55c389)
C:\Windows\System32\ipsecsvc.dll
15:34:26.0712 3944     PolicyAgent - ok
15:34:26.0744 3944     Power            (6ba9d927dded70bd1a9caded45f8b184)
C:\Windows\system32\umpo.dll
15:34:26.0748 3944     Power - ok
15:34:26.0769 3944     PptpMiniport     (f92a2c41117a11a00be01ca01a7fcde9)
C:\Windows\system32\DRIVERS\raspptp.sys
15:34:26.0771 3944     PptpMiniport - ok
15:34:26.0802 3944     Processor        (0d922e23c041efb1c3fac2a6f943c9bf)
C:\Windows\system32\DRIVERS\processr.sys
15:34:26.0802 3944     Processor - ok
15:34:26.0830 3944     ProfSvc          (53e83f1f6cf9d62f32801cf66d8352a8)
C:\Windows\system32\profsvc.dll
15:34:26.0833 3944     ProfSvc - ok
```

```
15:34:26.0853 3944     ProtectedStorage
(c118a82cd78818c29ab228366ebf81c3) C:\Windows\system32\lsass.exe
15:34:26.0855 3944     ProtectedStorage - ok
15:34:26.0880 3944     Psched          (0557cf5a2556bd58e26384169d72438d)
C:\Windows\system32\DRIVERS\pacer.sys
15:34:26.0880 3944     Psched - ok
15:34:26.0957 3944     ql2300          (a53a15a11ebfd21077463ee2c7afeef0)
C:\Windows\system32\DRIVERS\ql2300.sys
15:34:26.0966 3944     ql2300 - ok
15:34:27.0056 3944     ql40xx          (4f6d12b51de1aaeff7dc58c4d75423c8)
C:\Windows\system32\DRIVERS\ql40xx.sys
15:34:27.0058 3944     ql40xx - ok
15:34:27.0091 3944     QWAVE           (906191634e99aea92c4816150bda3732)
C:\Windows\system32\qwave.dll
15:34:27.0095 3944     QWAVE - ok
15:34:27.0107 3944     QWAVEdrv        (76707bb36430888d9ce9d705398adb6c)
C:\Windows\system32\drivers\qwavedrv.sys
15:34:27.0126 3944     QWAVEdrv - ok
15:34:27.0138 3944     RasAcd          (5a0da8ad5762fa2d91678a8a01311704)
C:\Windows\system32\DRIVERS\rasacd.sys
15:34:27.0138 3944     RasAcd - ok
15:34:27.0162 3944     RasAgileVpn     (7ecff9b22276b73f43a99a15a6094e90)
C:\Windows\system32\DRIVERS\AgileVpn.sys
15:34:27.0164 3944     RasAgileVpn - ok
15:34:27.0179 3944     RasAuto         (8f26510c5383b8dbe976de1cd00fc8c7)
C:\Windows\System32\rasauto.dll
15:34:27.0181 3944     RasAuto - ok
15:34:27.0207 3944     Rasl2tp         (471815800ae33e6f1c32fb1b97c490ca)
C:\Windows\system32\DRIVERS\rasl2tp.sys
15:34:27.0240 3944     Rasl2tp - ok
15:34:27.0273 3944     RasMan          (ee867a0870fc9e4972ba9eaad35651e2)
C:\Windows\System32\rasmans.dll
15:34:27.0277 3944     RasMan - ok
15:34:27.0289 3944     RasPppoe        (855c9b1cd4756c5e9a2aa58a15f58c25)
C:\Windows\system32\DRIVERS\raspppoe.sys
15:34:27.0289 3944     RasPppoe - ok
15:34:27.0298 3944     RasSstp         (e8b1e447b008d07ff47d016c2b0eeecb)
C:\Windows\system32\DRIVERS\rassstp.sys
15:34:27.0300 3944     RasSstp - ok
15:34:27.0328 3944     rdbss           (77f665941019a1594d887a74f301fa2f)
C:\Windows\system32\DRIVERS\rdbss.sys
15:34:27.0332 3944     rdbss - ok
15:34:27.0349 3944     rdpbus          (302da2a0539f2cf54d7c6cc30c1f2d8d)
C:\Windows\system32\DRIVERS\rdpbus.sys
15:34:27.0380 3944     rdpbus - ok
15:34:27.0390 3944     RDPCDD          (cea6cc257fc9b7715f1c2b4849286d24)
C:\Windows\system32\DRIVERS\RDPCDD.sys
15:34:27.0390 3944     RDPCDD - ok
15:34:27.0423 3944     RDPDR           (1b6163c503398b23ff8b939c67747683)
C:\Windows\system32\drivers\rdpdr.sys
15:34:27.0455 3944     RDPDR - ok
15:34:27.0470 3944     RDPENCDD        (bb5971a4f00659529a5c44831af22365)
C:\Windows\system32\drivers\rdpencdd.sys
15:34:27.0472 3944     RDPENCDD - ok
15:34:27.0480 3944     RDPREFMP        (216f3fa57533d98e1f74ded70113177a)
C:\Windows\system32\drivers\rdprefmp.sys
15:34:27.0480 3944     RDPREFMP - ok
```

```
15:34:27.0523 3944     RdpVideoMiniport
(70cba1a0c98600a2aa1863479b35cb90)
C:\Windows\system32\drivers\rdpvideominiport.sys
15:34:27.0525 3944     RdpVideoMiniport - ok
15:34:27.0558 3944     RDPWD           (e61608aa35e98999af9aaeeea6114b0a)
C:\Windows\system32\drivers\RDPWD.sys
15:34:27.0560 3944     RDPWD - ok
15:34:27.0591 3944     rdyboost        (34ed295fa0121c241bfef24764fc4520)
C:\Windows\system32\drivers\rdyboost.sys
15:34:27.0593 3944     rdyboost - ok
15:34:27.0626 3944     RemoteAccess    (254fb7a22d74e5511c73a3f6d802f192)
C:\Windows\System32\mprdim.dll
15:34:27.0628 3944     RemoteAccess - ok
15:34:27.0648 3944     RemoteRegistry  (e4d94f24081440b5fc5aa556c7c62702)
C:\Windows\system32\regsvc.dll
15:34:27.0652 3944     RemoteRegistry - ok
15:34:27.0675 3944     RFCOMM          (3dd798846e2c28102b922c56e71b7932)
C:\Windows\system32\DRIVERS\rfcomm.sys
15:34:27.0677 3944     RFCOMM - ok
15:34:27.0693 3944     RpcEptMapper    (e4dc58cf7b3ea515ae917ff0d402a7bb)
C:\Windows\System32\RpcEpMap.dll
15:34:27.0697 3944     RpcEptMapper - ok
15:34:27.0712 3944     RpcLocator      (d5ba242d4cf8e384db90e6a8ed850b8c)
C:\Windows\system32\locator.exe
15:34:27.0714 3944     RpcLocator - ok
15:34:27.0753 3944     RpcSs           (5c627d1b1138676c0a7ab2c2c190d123)
C:\Windows\system32\rpcss.dll
15:34:27.0759 3944     RpcSs - ok
15:34:27.0781 3944     rspndr          (ddc86e4f8e7456261e637e3552e804ff)
C:\Windows\system32\DRIVERS\rspndr.sys
15:34:27.0783 3944     rspndr - ok
15:34:27.0806 3944     s3cap           (e60c0a09f997826c7627b244195ab581)
C:\Windows\system32\drivers\vms3cap.sys
15:34:27.0808 3944     s3cap - ok
15:34:27.0828 3944     SamSs           (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:34:27.0830 3944     SamSs - ok
15:34:27.0849 3944     sbp2port        (ac03af3329579fffb455aa2daabbe22b)
C:\Windows\system32\drivers\sbp2port.sys
15:34:27.0851 3944     sbp2port - ok
15:34:27.0880 3944     SCardSvr        (9b7395789e3791a3b6d000fe6f8b131e)
C:\Windows\System32\SCardSvr.dll
15:34:27.0882 3944     SCardSvr - ok
15:34:27.0910 3944     scfilter        (253f38d0d7074c02ff8deb9836c97d2b)
C:\Windows\system32\DRIVERS\scfilter.sys
15:34:27.0910 3944     scfilter - ok
15:34:27.0974 3944     Schedule        (262f6592c3299c005fd6bec90fc4463a)
C:\Windows\system32\schedsvc.dll
15:34:27.0982 3944     Schedule - ok
15:34:28.0015 3944     SCPolicySvc     (f17d1d393bbc69c5322fbfafaca28c7f)
C:\Windows\System32\certprop.dll
15:34:28.0015 3944     SCPolicySvc - ok
15:34:28.0037 3944     SDRSVC          (6ea4234dc55346e0709560fe7c2c1972)
C:\Windows\System32\SDRSVC.dll
15:34:28.0041 3944     SDRSVC - ok
15:34:28.0080 3944     secdrv          (3ea8a16169c26afbeb544e0e48421186)
C:\Windows\system32\drivers\secdrv.sys
15:34:28.0082 3944     secdrv - ok
```

```
15:34:28.0111 3944     seclogon        (bc617a4e1b4fa8df523a061739a0bd87)
C:\Windows\system32\seclogon.dll
15:34:28.0113 3944     seclogon - ok
15:34:28.0138 3944     SENS            (c32ab8fa018ef34c0f113bd501436d21)
C:\Windows\System32\sens.dll
15:34:28.0140 3944     SENS - ok
15:34:28.0154 3944     SensrSvc        (0336cffafaab87a11541f1cf1594b2b2)
C:\Windows\system32\sensrsvc.dll
15:34:28.0156 3944     SensrSvc - ok
15:34:28.0167 3944     Serenum         (cb624c0035412af0debec78c41f5ca1b)
C:\Windows\system32\DRIVERS\serenum.sys
15:34:28.0167 3944     Serenum - ok
15:34:28.0175 3944     Serial          (c1d8e28b2c2adfaec4ba89e9fda69bd6)
C:\Windows\system32\DRIVERS\serial.sys
15:34:28.0175 3944     Serial - ok
15:34:28.0193 3944     sermouse        (1c545a7d0691cc4a027396535691c3e3)
C:\Windows\system32\DRIVERS\sermouse.sys
15:34:28.0193 3944     sermouse - ok
15:34:28.0224 3944     SessionEnv      (0b6231bf38174a1628c4ac812cc75804)
C:\Windows\system32\sessenv.dll
15:34:28.0226 3944     SessionEnv - ok
15:34:28.0255 3944     sffdisk         (a554811bcd09279536440c964ae35bbf)
C:\Windows\system32\drivers\sffdisk.sys
15:34:28.0273 3944     sffdisk - ok
15:34:28.0283 3944     sffp_mmc        (ff414f0baefeba59bc6c04b3db0b87bf)
C:\Windows\system32\drivers\sffp_mmc.sys
15:34:28.0283 3944     sffp_mmc - ok
15:34:28.0292 3944     sffp_sd         (dd85b78243a19b59f0637dcf284da63c)
C:\Windows\system32\drivers\sffp_sd.sys
15:34:28.0294 3944     sffp_sd - ok
15:34:28.0310 3944     sfloppy         (a9d601643a1647211a1ee2ec4e433ff4)
C:\Windows\system32\DRIVERS\sfloppy.sys
15:34:28.0312 3944     sfloppy - ok
15:34:28.0351 3944     SharedAccess    (b95f6501a2f8b2e78c697fec401970ce)
C:\Windows\System32\ipnathlp.dll
15:34:28.0355 3944     SharedAccess - ok
15:34:28.0396 3944     ShellHWDetection
(aaf932b4011d14052955d4b212a4da8d) C:\Windows\System32\shsvcs.dll
15:34:28.0400 3944     ShellHWDetection - ok
15:34:28.0433 3944     SiSRaid2        (843caf1e5fde1ffd5ff768f23a51e2e1)
C:\Windows\system32\DRIVERS\SiSRaid2.sys
15:34:28.0435 3944     SiSRaid2 - ok
15:34:28.0451 3944     SiSRaid4        (6a6c106d42e9ffff8b9fcb4f754f6da4)
C:\Windows\system32\DRIVERS\sisraid4.sys
15:34:28.0488 3944     SiSRaid4 - ok
15:34:28.0509 3944     Smb             (548260a7b8654e024dc30bf8a7c5baa4)
C:\Windows\system32\DRIVERS\smb.sys
15:34:28.0515 3944     Smb - ok
15:34:28.0542 3944     SNMPTRAP        (6313f223e817cc09aa41811daa7f541d)
C:\Windows\System32\snmptrap.exe
15:34:28.0544 3944     SNMPTRAP - ok
15:34:28.0949 3944     SNPSTD3         (b8b6b14ee7b2e9806e4373a7dc61b592)
C:\Windows\system32\DRIVERS\snpstd3.sys
15:34:29.0019 3944     SNPSTD3 - ok
15:34:29.0101 3944     spldr           (b9e31e5cacdfe584f34f730a677803f9)
C:\Windows\system32\drivers\spldr.sys
15:34:29.0103 3944     spldr - ok
```

```
15:34:29.0169 3944     Spooler         (b96c17b5dc1424d56eea3a99e97428cd)
C:\Windows\System32\spoolsv.exe
15:34:29.0181 3944     Spooler - ok
15:34:29.0347 3944     sppsvc          (e17e0188bb90fae42d83e98707efa59c)
C:\Windows\system32\sppsvc.exe
15:34:29.0375 3944     sppsvc - ok
15:34:29.0435 3944     sppuinotify     (93d7d61317f3d4bc4f4e9f8a96a7de45)
C:\Windows\system32\sppuinotify.dll
15:34:29.0437 3944     sppuinotify - ok
15:34:29.0490 3944     sptd            (602884696850c86434530790b110e8eb)
C:\Windows\system32\Drivers\sptd.sys
15:34:29.0490 3944     Suspicious file (NoAccess):
C:\Windows\system32\Drivers\sptd.sys. md5:
602884696850c86434530790b110e8eb
15:34:29.0492 3944     sptd ( LockedFile.Multi.Generic ) - warning
15:34:29.0494 3944     sptd - detected LockedFile.Multi.Generic (1)
15:34:29.0533 3944     srv             (441fba48bff01fdb9d5969ebc1838f0b)
C:\Windows\system32\DRIVERS\srv.sys
15:34:29.0537 3944     srv - ok
15:34:29.0574 3944     srv2            (b4adebbf5e3677cce9651e0f01f7cc28)
C:\Windows\system32\DRIVERS\srv2.sys
15:34:29.0578 3944     srv2 - ok
15:34:29.0597 3944     srvnet          (27e461f0be5bff5fc737328f749538c3)
C:\Windows\system32\DRIVERS\srvnet.sys
15:34:29.0599 3944     srvnet - ok
15:34:29.0619 3944     SSDPSRV         (51b52fbd583cde8aa9ba62b8b4298f33)
C:\Windows\System32\ssdpsrv.dll
15:34:29.0623 3944     SSDPSRV - ok
15:34:29.0634 3944     SstpSvc         (ab7aebf58dad8daab7a6c45e6a8885cb)
C:\Windows\system32\sstpsvc.dll
15:34:29.0636 3944     SstpSvc - ok
15:34:29.0705 3944     Stereo Service  (29662881a46db66730c62a4f1bfa3dc2)
C:\Program Files (x86)\NVIDIA Corporation\3D Vision\nvSCPAPISvr.exe
15:34:29.0708 3944     Stereo Service - ok
15:34:29.0738 3944     stexstor        (f3817967ed533d08327dc73bc4d5542a)
C:\Windows\system32\DRIVERS\stexstor.sys
15:34:29.0742 3944     stexstor - ok
15:34:29.0806 3944     stisvc          (8dd52e8e6128f4b2da92ce27402871c1)
C:\Windows\System32\wiaservc.dll
15:34:29.0820 3944     stisvc - ok
15:34:29.0845 3944     storflt         (7785dc213270d2fc066538daf94087e7)
C:\Windows\system32\drivers\vmstorfl.sys
15:34:29.0847 3944     storflt - ok
15:34:29.0865 3944     storvsc         (d34e4943d5ac096c8edeebfd80d76e23)
C:\Windows\system32\drivers\storvsc.sys
15:34:29.0867 3944     storvsc - ok
15:34:29.0886 3944     swenum          (d01ec09b6711a5f8e7e6564a4d0fbc90)
C:\Windows\system32\drivers\swenum.sys
15:34:29.0888 3944     swenum - ok
15:34:29.0931 3944     swprv           (e08e46fdd841b7184194011ca1955a0b)
C:\Windows\System32\swprv.dll
15:34:29.0937 3944     swprv - ok
15:34:29.0941 3944     Synth3dVsc - ok
15:34:30.0039 3944     SysMain         (bf9ccc0bf39b418c8d0ae8b05cf95b7d)
C:\Windows\system32\sysmain.dll
15:34:30.0052 3944     SysMain - ok
15:34:30.0175 3944     TabletInputService
(e3c61fd7b7c2557e1f1b0b4cec713585) C:\Windows\System32\TabSvc.dll
```

```
15:34:30.0181 3944     TabletInputService - ok
15:34:30.0216 3944     TapiSrv          (40f0849f65d13ee87b9a9ae3c1dd6823)
C:\Windows\System32\tapisrv.dll
15:34:30.0226 3944     TapiSrv - ok
15:34:30.0246 3944     TBS              (1be03ac720f4d302ea01d40f588162f6)
C:\Windows\System32\tbssvc.dll
15:34:30.0251 3944     TBS - ok
15:34:30.0357 3944     Tcpip            (acb82bda8f46c84f465c1afa517dc4b9)
C:\Windows\system32\drivers\tcpip.sys
15:34:30.0371 3944     Tcpip - ok
15:34:30.0505 3944     TCPIP6           (acb82bda8f46c84f465c1afa517dc4b9)
C:\Windows\system32\DRIVERS\tcpip.sys
15:34:30.0519 3944     TCPIP6 - ok
15:34:30.0583 3944     tcpipreg         (df687e3d8836bfb04fcc0615bf15a519)
C:\Windows\system32\drivers\tcpipreg.sys
15:34:30.0585 3944     tcpipreg - ok
15:34:30.0607 3944     TDPIPE           (3371d21011695b16333a3934340c4e7c)
C:\Windows\system32\drivers\tdpipe.sys
15:34:30.0607 3944     TDPIPE - ok
15:34:30.0636 3944     TDTCP            (51c5eceb1cdee2468a1748be550cfbc8)
C:\Windows\system32\drivers\tdtcp.sys
15:34:30.0636 3944     TDTCP - ok
15:34:30.0658 3944     tdx              (ddad5a7ab24d8b65f8d724f5c20fd806)
C:\Windows\system32\DRIVERS\tdx.sys
15:34:30.0658 3944     tdx - ok
15:34:30.0683 3944     TermDD           (561e7e1f06895d78de991e01dd0fb6e5)
C:\Windows\system32\drivers\termdd.sys
15:34:30.0683 3944     TermDD - ok
15:34:30.0726 3944     TermService      (2e648163254233755035b46dd7b89123)
C:\Windows\System32\termsrv.dll
15:34:30.0732 3944     TermService - ok
15:34:30.0765 3944     Themes           (f0344071948d1a1fa732231785a0664c)
C:\Windows\system32\themeservice.dll
15:34:30.0769 3944     Themes - ok
15:34:30.0800 3944     THREADORDER      (e40e80d0304a73e8d269f7141d77250b)
C:\Windows\system32\mmcss.dll
15:34:30.0802 3944     THREADORDER - ok
15:34:30.0818 3944     TrkWks           (7e7afd841694f6ac397e99d75cead49d)
C:\Windows\System32\trkwks.dll
15:34:30.0820 3944     TrkWks - ok
15:34:30.0875 3944     TrustedInstaller
(773212b2aaa24c1e31f10246b15b276c)
C:\Windows\servicing\TrustedInstaller.exe
15:34:30.0878 3944     TrustedInstaller - ok
15:34:30.0914 3944     tssecsrv         (ce18b2cdfc837c99e5fae9ca6cba5d30)
C:\Windows\system32\DRIVERS\tssecsrv.sys
15:34:30.0916 3944     tssecsrv - ok
15:34:30.0947 3944     TsUsbFlt         (d11c783e3ef9a3c52c0ebe83cc5000e9)
C:\Windows\system32\drivers\tsusbflt.sys
15:34:30.0982 3944     TsUsbFlt - ok
15:34:30.0986 3944     tsusbhub - ok
15:34:31.0025 3944     tunnel           (3566a8daafa27af944f5d705eaa64894)
C:\Windows\system32\DRIVERS\tunnel.sys
15:34:31.0027 3944     tunnel - ok
15:34:31.0050 3944     uagp35           (b4dd609bd7e282bfc683cec7eaaaad67)
C:\Windows\system32\DRIVERS\uagp35.sys
15:34:31.0068 3944     uagp35 - ok
```

```
15:34:31.0093 3944     udfs            (ff4232a1a64012baa1fd97c7b67df593)
C:\Windows\system32\DRIVERS\udfs.sys
15:34:31.0095 3944     udfs - ok
15:34:31.0121 3944     UI0Detect       (3cbdec8d06b9968aba702eba076364a1)
C:\Windows\system32\UI0Detect.exe
15:34:31.0125 3944     UI0Detect - ok
15:34:31.0144 3944     uliagpkx        (4bfe1bc28391222894cbf1e7d0e42320)
C:\Windows\system32\drivers\uliagpkx.sys
15:34:31.0146 3944     uliagpkx - ok
15:34:31.0173 3944     umbus           (dc54a574663a895c8763af0fa1ff7561)
C:\Windows\system32\drivers\umbus.sys
15:34:31.0173 3944     umbus - ok
15:34:31.0191 3944     UmPass          (b2e8e8cb557b156da5493bbddcc1474d)
C:\Windows\system32\DRIVERS\umpass.sys
15:34:31.0191 3944     UmPass - ok
15:34:31.0230 3944     UmRdpService    (a293dcd756d04d8492a750d03b9a297c)
C:\Windows\System32\umrdp.dll
15:34:31.0232 3944     UmRdpService - ok
15:34:31.0261 3944     upnphost        (d47ec6a8e81633dd18d2436b19baf6de)
C:\Windows\System32\upnphost.dll
15:34:31.0265 3944     upnphost - ok
15:34:31.0291 3944     usbaudio        (82e8f44688e6fac57b5b7c6fc7adbc2a)
C:\Windows\system32\drivers\usbaudio.sys
15:34:31.0291 3944     usbaudio - ok
15:34:31.0312 3944     usbccgp         (6f1a3157a1c89435352ceb543cdb359c)
C:\Windows\system32\DRIVERS\usbccgp.sys
15:34:31.0312 3944     usbccgp - ok
15:34:31.0339 3944     usbcir          (af0892a803fdda7492f595368e3b68e7)
C:\Windows\system32\drivers\usbcir.sys
15:34:31.0341 3944     usbcir - ok
15:34:31.0355 3944     usbehci         (c025055fe7b87701eb042095df1a2d7b)
C:\Windows\system32\DRIVERS\usbehci.sys
15:34:31.0357 3944     usbehci - ok
15:34:31.0382 3944     usbhub          (287c6c9410b111b68b52ca298f7b8c24)
C:\Windows\system32\DRIVERS\usbhub.sys
15:34:31.0386 3944     usbhub - ok
15:34:31.0402 3944     usbohci         (9840fc418b4cbd632d3d0a667a725c31)
C:\Windows\system32\DRIVERS\usbohci.sys
15:34:31.0402 3944     usbohci - ok
15:34:31.0433 3944     usbprint        (73188f58fb384e75c4063d29413cee3d)
C:\Windows\system32\DRIVERS\usbprint.sys
15:34:31.0435 3944     usbprint - ok
15:34:31.0458 3944     USBSTOR         (fed648b01349a3c8395a5169db5fb7d6)
C:\Windows\system32\DRIVERS\USBSTOR.SYS
15:34:31.0458 3944     USBSTOR - ok
15:34:31.0474 3944     usbuhci         (62069a34518bcf9c1fd9e74b3f6db7cd)
C:\Windows\system32\drivers\usbuhci.sys
15:34:31.0476 3944     usbuhci - ok
15:34:31.0500 3944     UxSms           (edbb23cbcf2cdf727d64ff9b51a6070e)
C:\Windows\System32\uxsms.dll
15:34:31.0501 3944     UxSms - ok
15:34:31.0519 3944     VaultSvc        (c118a82cd78818c29ab228366ebf81c3)
C:\Windows\system32\lsass.exe
15:34:31.0521 3944     VaultSvc - ok
15:34:31.0539 3944     vdrvroot        (c5c876ccfc083ff3b128f933823e87bd)
C:\Windows\system32\drivers\vdrvroot.sys
15:34:31.0539 3944     vdrvroot - ok
```

```
15:34:31.0582 3944     vds             (8d6b481601d01a456e75c3210f1830be)
C:\Windows\System32\vds.exe
15:34:31.0587 3944     vds - ok
15:34:31.0605 3944     vga             (da4da3f5e02943c2dc8c6ed875de68dd)
C:\Windows\system32\DRIVERS\vgapnp.sys
15:34:31.0607 3944     vga - ok
15:34:31.0626 3944     VgaSave         (53e92a310193cb3c03bea963de7d9cfc)
C:\Windows\System32\drivers\vga.sys
15:34:31.0626 3944     VgaSave - ok
15:34:31.0630 3944     VGPU - ok
15:34:31.0662 3944     vhdmp           (2ce2df28c83aeaf30084e1b1eb253cbb)
C:\Windows\system32\drivers\vhdmp.sys
15:34:31.0666 3944     vhdmp - ok
15:34:31.0681 3944     viaide          (e5689d93ffe4e5d66c0178761240dd54)
C:\Windows\system32\drivers\viaide.sys
15:34:31.0683 3944     viaide - ok
15:34:31.0707 3944     vmbus           (86ea3e79ae350fea5331a1303054005f)
C:\Windows\system32\drivers\vmbus.sys
15:34:31.0708 3944     vmbus - ok
15:34:31.0728 3944     VMBusHID        (7de90b48f210d29649380545db45a187)
C:\Windows\system32\drivers\VMBusHID.sys
15:34:31.0728 3944     VMBusHID - ok
15:34:31.0744 3944     volmgr          (d2aafd421940f640b407aefaaebd91b0)
C:\Windows\system32\drivers\volmgr.sys
15:34:31.0744 3944     volmgr - ok
15:34:31.0785 3944     volmgrx         (a255814907c89be58b79ef2f189b843b)
C:\Windows\system32\drivers\volmgrx.sys
15:34:31.0789 3944     volmgrx - ok
15:34:31.0828 3944     volsnap         (0d08d2f3b3ff84e433346669b5e0f639)
C:\Windows\system32\drivers\volsnap.sys
15:34:31.0830 3944     volsnap - ok
15:34:31.0865 3944     vsmraid         (5e2016ea6ebaca03c04feac5f330d997)
C:\Windows\system32\DRIVERS\vsmraid.sys
15:34:31.0867 3944     vsmraid - ok
15:34:31.0960 3944     VSS             (b60ba0bc31b0cb414593e169f6f21cc2)
C:\Windows\system32\vssvc.exe
15:34:31.0972 3944     VSS - ok
15:34:32.0087 3944     vwifibus        (36d4720b72b5c5d9cb2b9c29e9df67a1)
C:\Windows\System32\drivers\vwifibus.sys
15:34:32.0089 3944     vwifibus - ok
15:34:32.0144 3944     W32Time         (1c9d80cc3849b3788048078c26486e1a)
C:\Windows\system32\w32time.dll
15:34:32.0156 3944     W32Time - ok
15:34:32.0179 3944     WacomPen        (4e9440f4f152a7b944cb1663d3935a3e)
C:\Windows\system32\DRIVERS\wacompen.sys
15:34:32.0181 3944     WacomPen - ok
15:34:32.0214 3944     WANARP          (356afd78a6ed4457169241ac3965230c)
C:\Windows\system32\DRIVERS\wanarp.sys
15:34:32.0214 3944     WANARP - ok
15:34:32.0220 3944     Wanarpv6        (356afd78a6ed4457169241ac3965230c)
C:\Windows\system32\DRIVERS\wanarp.sys
15:34:32.0222 3944     Wanarpv6 - ok
15:34:32.0300 3944     WatAdminSvc     (3cec96de223e49eaae3651fcf8faea6c)
C:\Windows\system32\Wat\WatAdminSvc.exe
15:34:32.0310 3944     WatAdminSvc - ok
15:34:32.0390 3944     wbengine        (78f4e7f5c56cb9716238eb57da4b6a75)
C:\Windows\system32\wbengine.exe
15:34:32.0402 3944     wbengine - ok
```

```
15:34:32.0480 3944     WbioSrvc        (3aa101e8edab2db4131333f4325c76a3)
C:\Windows\System32\wbiosrvc.dll
15:34:32.0484 3944     WbioSrvc - ok
15:34:32.0515 3944     wcncsvc         (7368a2afd46e5a4481d1de9d14848edd)
C:\Windows\System32\wcncsvc.dll
15:34:32.0519 3944     wcncsvc - ok
15:34:32.0537 3944     WcsPlugInService
(20f7441334b18cee52027661df4a6129)
C:\Windows\System32\WcsPlugInService.dll
15:34:32.0539 3944     WcsPlugInService - ok
15:34:32.0560 3944     Wd              (72889e16ff12ba0f235467d6091b17dc)
C:\Windows\system32\DRIVERS\wd.sys
15:34:32.0562 3944     Wd - ok
15:34:32.0597 3944     Wdf01000        (441bd2d7b4f98134c3a4f9fa570fd250)
C:\Windows\system32\drivers\Wdf01000.sys
15:34:32.0605 3944     Wdf01000 - ok
15:34:32.0619 3944     WdiServiceHost  (bf1fc3f79b863c914687a737c2f3d681)
C:\Windows\system32\wdi.dll
15:34:32.0623 3944     WdiServiceHost - ok
15:34:32.0626 3944     WdiSystemHost   (bf1fc3f79b863c914687a737c2f3d681)
C:\Windows\system32\wdi.dll
15:34:32.0630 3944     WdiSystemHost - ok
15:34:32.0662 3944     WebClient       (3db6d04e1c64272f8b14eb8bc4616280)
C:\Windows\System32\webclnt.dll
15:34:32.0664 3944     WebClient - ok
15:34:32.0689 3944     Wecsvc          (c749025a679c5103e575e3b48e092c43)
C:\Windows\system32\wecsvc.dll
15:34:32.0693 3944     Wecsvc - ok
15:34:32.0705 3944     wercplsupport   (7e591867422dc788b9e5bd337a669a08)
C:\Windows\System32\wercplsupport.dll
15:34:32.0707 3944     wercplsupport - ok
15:34:32.0718 3944     WerSvc          (6d137963730144698cbd10f202e9f251)
C:\Windows\System32\WerSvc.dll
15:34:32.0722 3944     WerSvc - ok
15:34:32.0738 3944     WfpLwf          (611b23304bf067451a9fdee01fbdd725)
C:\Windows\system32\DRIVERS\wfplwf.sys
15:34:32.0738 3944     WfpLwf - ok
15:34:32.0750 3944     WIMMount        (05ecaec3e4529a7153b3136ceb49f0ec)
C:\Windows\system32\drivers\wimmount.sys
15:34:32.0767 3944     WIMMount - ok
15:34:32.0794 3944     WinDefend - ok
15:34:32.0804 3944     WinHttpAutoProxySvc - ok
15:34:32.0865 3944     Winmgmt         (19b07e7e8915d701225da41cb3877306)
C:\Windows\system32\wbem\WMIsvc.dll
15:34:32.0869 3944     Winmgmt - ok
15:34:33.0007 3944     WinRM           (bcb1310604aa415c4508708975b3931e)
C:\Windows\system32\WsmSvc.dll
15:34:33.0031 3944     WinRM - ok
15:34:33.0113 3944     WinUsb          (fe88b288356e7b47b74b13372add906d)
C:\Windows\system32\DRIVERS\WinUsb.sys
15:34:33.0115 3944     WinUsb - ok
15:34:33.0169 3944     Wlansvc         (4fada86e62f18a1b2f42ba18ae24e6aa)
C:\Windows\System32\wlansvc.dll
15:34:33.0177 3944     Wlansvc - ok
15:34:33.0197 3944     WmiAcpi         (f6ff8944478594d0e414d3f048f0d778)
C:\Windows\system32\drivers\wmiacpi.sys
15:34:33.0197 3944     WmiAcpi - ok
```

```
15:34:33.0255 3944     wmiApSrv        (38b84c94c5a8af291adfea478ae54f93)
C:\Windows\system32\wbem\WmiApSrv.exe
15:34:33.0257 3944     wmiApSrv - ok
15:34:33.0277 3944     WMPNetworkSvc - ok
15:34:33.0287 3944     WPCSvc          (96c6e7100d724c69fcf9e7bf590d1dca)
C:\Windows\System32\wpcsvc.dll
15:34:33.0291 3944     WPCSvc - ok
15:34:33.0312 3944     WPDBusEnum      (93221146d4ebbf314c29b23cd6cc391d)
C:\Windows\system32\wpdbusenum.dll
15:34:33.0314 3944     WPDBusEnum - ok
15:34:33.0337 3944     ws2ifsl         (6bcc1d7d2fd2453957c5479a32364e52)
C:\Windows\system32\drivers\ws2ifsl.sys
15:34:33.0355 3944     ws2ifsl - ok
15:34:33.0373 3944     wscsvc          (e8b1fe6669397d1772d8196df0e57a9e)
C:\Windows\System32\wscsvc.dll
15:34:33.0375 3944     wscsvc - ok
15:34:33.0378 3944     WSearch - ok
15:34:33.0787 3944     wuauserv        (d9ef901dca379cfe914e9fa13b73b4c4)
C:\Windows\system32\wuaueng.dll
15:34:33.0814 3944     wuauserv - ok
15:34:33.0904 3944     WudfPf          (d3381dc54c34d79b22cee0d65ba91b7c)
C:\Windows\system32\drivers\WudfPf.sys
15:34:33.0904 3944     WudfPf - ok
15:34:33.0925 3944     WUDFRd          (cf8d590be3373029d57af80914190682)
C:\Windows\system32\DRIVERS\WUDFRd.sys
15:34:33.0927 3944     WUDFRd - ok
15:34:33.0953 3944     wudfsvc         (7a95c95b6c4cf292d689106bcae49543)
C:\Windows\System32\WUDFSvc.dll
15:34:33.0957 3944     wudfsvc - ok
15:34:33.0992 3944     WwanSvc         (9a3452b3c2a46c073166c5cf49fad1ae)
C:\Windows\System32\wwansvc.dll
15:34:33.0998 3944     WwanSvc - ok
15:34:34.0017 3944     MBR (0x1B8)     (a36c5e4f47e84449ff07ed3517b43a31)
\Device\Harddisk0\DR0
15:34:34.0484 3944     \Device\Harddisk0\DR0 - ok
15:34:34.0488 3944     Boot (0x1200)   (e69930abac2385be7360b2b1ebef4080)
\Device\Harddisk0\DR0\Partition0
15:34:34.0490 3944     \Device\Harddisk0\DR0\Partition0 - ok
15:34:34.0509 3944     Boot (0x1200)   (005874abee4a5ab8683099048e03c51c)
\Device\Harddisk0\DR0\Partition1
15:34:34.0511 3944     \Device\Harddisk0\DR0\Partition1 - ok
15:34:34.0511 3944
      ============================================================
15:34:34.0511 3944     Scan finished
15:34:34.0511 3944
      ============================================================
15:34:34.0521 0904     Detected object count: 1
15:34:34.0521 0904     Actual detected object count: 1
15:35:15.0729 0904     C:\Windows\system32\Drivers\sptd.sys - copied to
quarantine
15:35:15.0735 0904     sptd ( LockedFile.Multi.Generic ) - User select
action: Quarantine
15:35:20.0114 0788     Deinitialize success
```