

ComboFix 15-01-28.01 - admin 28.01.2015 13:46:58.1.4 - x64

Microsoft Windows 7 Home Premium 6.1.7601.1.1250.420.1029.18.4044.1782 [GMT 1:00]

Spuštěný z: c:\users\admin\Downloads\ComboFix.exe

AV: avast! Antivirus *Disabled/Updated* {17AD7D40-BA12-9C46-7131-94903A54AD8B}

SP: avast! Antivirus *Disabled/Updated* {ACCC9CA4-9C28-93C8-4B81-AFE241D3E736}

SP: Windows Defender *Enabled/Updated* {D68DDC3A-831F-4fae-9E44-DA132C1ACF46}

.

.

(((((Ostatní výmazy))))))

.

.

c:\users\admin\AppData\Local\Installer\Installytd_41

c:\windows\lsun0405.exe

.

.

(((((Ovladače/Služby))))))

.

.

-----\Service_SPDRIVER_1.38.0.1444

.

.

(((((Soubory vytvořené od 2014-12-28 do 2015-01-28))))))

.

.

2015-01-28 12:56 . 2015-01-28 12:56 ----- d----w- c:\users\Default\AppData\Local\temp

2015-01-27 13:07 . 2014-12-15 03:13 11870360 ----a-w- c:\programdata\Microsoft\Windows Defender\Definition Updates\{B8C81EDA-55E8-4A13-9137-A859547C686F}\mpengine.dll

2015-01-26 16:51 . 2015-01-26 17:01 ----- d----w- c:\windows\SysWow64\RTCOM

2015-01-26 16:51 . 2015-01-26 16:51 ----- d----w- c:\program files\Realtek

2015-01-26 14:29 . 2015-01-26 14:34 ----- d----w- c:\windows\system32\catroot2

2015-01-26 14:18 . 2015-01-26 14:18 ----- d----w- c:\windows\SysWow64\wbem\Performance

2015-01-26 14:06 . 2013-02-12 04:12	19968	----	a-w-	c:\windows\system32\drivers\usb8023x.sys
2015-01-26 14:06 . 2012-07-04 20:26	41472	----	a-w-	c:\windows\system32\drivers\rndismpx.sys
2015-01-26 10:07 . 2015-01-26 10:07	-----	d----	w-	C:\zoek_backup
2015-01-26 08:36 . 2015-01-26 14:46	35064	----	a-w-	c:\windows\system32\drivers\TrueSight.sys
2015-01-26 08:36 . 2015-01-26 08:36	-----	d----	w-	c:\programdata\RogueKiller
2015-01-26 01:00 . 2015-01-27 13:04	-----	d----	w-	c:\users\admin\AppData\Local\Adobe
2015-01-25 20:23 . 2015-01-25 20:23	-----	d----	w-	c:\windows\ERUNT
2015-01-25 10:56 . 2015-01-25 10:56	-----	d----	w-	C:\RegBackup
2015-01-25 08:26 . 2015-01-25 08:26	-----	d----	w-	c:\program files (x86)\Tweaking.com
2015-01-25 08:09 . 2015-01-13 09:00	1741824	----	a-w-	c:\windows\system32\VSFilter.dll.bak
2015-01-25 08:09 . 2014-03-18 01:06	1757184	----	a-w-	c:\windows\system32\WMPDMC.exe
2015-01-24 21:17 . 2015-01-28 12:32	129752	----	a-w-	c:\windows\system32\drivers\MBAMSwissArmy.sys
2015-01-24 21:16 . 2015-01-24 21:20	-----	d----	w-	c:\program files (x86)\Malwarebytes Anti-Malware
2015-01-24 21:16 . 2015-01-24 21:16	-----	d----	w-	c:\programdata\Malwarebytes
2015-01-24 21:16 . 2014-11-21 05:14	63704	----	a-w-	c:\windows\system32\drivers\mwac.sys
2015-01-24 21:16 . 2014-11-21 05:14	93400	----	a-w-	c:\windows\system32\drivers\mbamchameleon.sys
2015-01-24 21:16 . 2014-11-21 05:14	25816	----	a-w-	c:\windows\system32\drivers\mbam.sys
2015-01-24 21:04 . 2015-01-26 18:01	-----	d----	w-	C:\AdwCleaner
2015-01-24 20:39 . 2010-11-21 03:25	296448	----	a-w-	c:\windows\SysWow64\mfds.dll
2015-01-24 20:35 . 2014-03-18 01:06	1392640	----	a-w-	c:\windows\SysWow64\WMPDMC.exe
2015-01-24 20:27 . 2015-01-24 20:27	-----	d----	w-	c:\program files (x86)\Shark007
2015-01-24 20:26 . 2015-01-26 21:12	-----	d----	w-	c:\programdata\Standard
2015-01-19 17:44 . 2015-01-25 11:04	-----	d----	w-	c:\programdata\Kaspersky Lab
2015-01-19 10:38 . 2014-07-11 01:02	98216	----	a-w-	c:\windows\SysWow64\WindowsAccessBridge-32.dll
2015-01-18 20:45 . 2015-01-18 20:43	13792	----	a-w-	c:\windows\system32\drivers\semav6thermal64ro.sys
2015-01-18 20:45 . 2015-01-18 21:09	-----	d----	w-	c:\users\admin\AppData\Roaming\iolo
2015-01-18 20:45 . 2015-01-18 21:08	-----	d----	w-	c:\programdata\iolo

2015-01-18 20:45 . 2015-01-18 20:45	74703	----a-w-	c:\windows\SysWow64\mfc45.dll
2015-01-18 20:44 . 2013-11-01 13:59	69000	----a-w-	c:\windows\system32\offreg.dll
2015-01-18 20:44 . 2013-11-01 13:59	21176	----a-w-	c:\windows\system32\iolorgdf64.exe
2015-01-18 20:20 . 2015-01-18 20:20	-----	d-----w-	c:\users\admin\AppData\Local\Microsoft Corporation
2015-01-18 20:19 . 2015-01-18 20:19	-----	d-----w-	c:\program files (x86)\Microsoft Windows 7 Upgrade Advisor
2015-01-17 17:30 . 2015-01-17 17:30	-----	d-s---w-	c:\windows\SysWow64\Microsoft
2015-01-17 17:16 . 2015-01-17 17:16	364512	----a-w-	c:\windows\system32\aswBoot.exe
2015-01-17 17:16 . 2015-01-17 17:16	43152	----a-w-	c:\windows\avastSS.scr
2015-01-17 16:43 . 2010-03-17 20:53	180224	----a-w-	c:\windows\SysWow64\QTCF.dll
2015-01-17 16:42 . 2015-01-19 09:54	-----	d-----w-	c:\program files (x86)\QuickTime Alternative
2015-01-17 16:17 . 2015-01-17 16:17	-----	d-----w-	c:\windows\PCHEALTH
2015-01-17 15:11 . 2015-01-17 15:11	-----	d-----w-	C:\OETemp
2015-01-16 10:27 . 2015-01-26 20:24	-----	d-----w-	c:\users\admin\AppData\Roaming\vlc
2015-01-14 18:16 . 2014-12-19 03:06	210432	----a-w-	c:\windows\system32\profsvc.dll
2015-01-14 18:15 . 2014-12-06 04:17	303616	----a-w-	c:\windows\system32\nlasvc.dll
2015-01-14 18:15 . 2014-12-06 03:50	52224	----a-w-	c:\windows\SysWow64\nlaapi.dll
2015-01-14 18:15 . 2014-12-06 03:50	156672	----a-w-	c:\windows\SysWow64\ncsi.dll
2015-01-14 18:15 . 2014-12-19 01:46	141312	----a-w-	c:\windows\system32\drivers\mrxdav.sys
2015-01-14 18:15 . 2014-12-11 17:47	87040	----a-w-	c:\windows\system32\TSWbPrxy.exe
2015-01-14 18:15 . 2014-12-12 05:35	5553592	----a-w-	c:\windows\system32\ntoskrnl.exe
2015-01-14 18:15 . 2014-12-12 05:11	3971512	----a-w-	c:\windows\SysWow64\ntkrnlpa.exe
2015-01-14 18:15 . 2014-12-12 05:11	3916728	----a-w-	c:\windows\SysWow64\ntoskrnl.exe
2015-01-14 18:15 . 2014-12-12 05:31	503808	----a-w-	c:\windows\system32\srcore.dll
2015-01-14 18:15 . 2014-12-12 05:31	50176	----a-w-	c:\windows\system32\srclient.dll
2015-01-14 18:15 . 2014-12-12 05:31	296960	----a-w-	c:\windows\system32\rstrui.exe
2015-01-14 18:15 . 2014-12-12 05:07	43008	----a-w-	c:\windows\SysWow64\srclient.dll
2015-01-11 14:01 . 2014-08-29 02:07	3179520	----a-w-	c:\windows\system32\rdpcorets.dll
2015-01-11 14:01 . 2014-05-08 09:32	16384	----a-w-	c:\windows\system32\RdpGroupPolicyExtension.dll
2015-01-11 14:01 . 2014-09-05 01:52	5703168	----a-w-	c:\windows\SysWow64\mstscax.dll

2015-01-11 14:01 . 2014-09-05 02:11 6584320 ----a-w- c:\windows\system32\mstscax.dll
 2015-01-11 09:36 . 2013-10-02 01:10 44544 ----a-w- c:\windows\system32\TsUsbGDColnInstaller.dll
 2015-01-11 09:35 . 2012-08-23 14:10 19456 ----a-w-
 c:\windows\system32\drivers\rdpvideominiport.sys
 2015-01-11 09:35 . 2012-08-23 14:08 30208 ----a-w- c:\windows\system32\drivers\TsUsbGD.sys
 2015-01-11 09:35 . 2012-08-23 14:13 243200 ----a-w- c:\windows\system32\rdpudd.dll
 2015-01-11 09:35 . 2012-08-23 11:12 192000 ----a-w- c:\windows\SysWow64\rdpendp_winip.dll
 2015-01-11 09:35 . 2012-08-23 10:51 228864 ----a-w- c:\windows\system32\rdpendp_winip.dll
 2015-01-08 16:16 . 2015-01-08 16:16 ----- d-----w- c:\users\admin\AppData\Roaming\Curiolab
 2015-01-08 12:56 . 2015-01-08 12:56 ----- d-----w- c:\users\admin\AppData\Roaming\AVG
 2015-01-08 12:54 . 2015-01-08 12:54 ----- d-----w- c:\users\admin\AppData\Local\Avg
 2015-01-08 12:53 . 2015-01-09 04:47 ----- d-----w- c:\programdata\AVG
 .
 .
 .
 (((Find3M výpis))
 .
 2015-01-25 20:53 . 2012-03-31 09:42 701616 ----a-w- c:\windows\SysWow64\FlashPlayerApp.exe
 2015-01-25 20:53 . 2011-11-07 18:59 71344 ----a-w-
 c:\windows\SysWow64\FlashPlayerCPLApp.cpl
 2015-01-17 17:17 . 2011-10-30 15:06 1050432 ----a-w-
 c:\windows\system32\drivers\aswsnx.sys
 2015-01-17 17:16 . 2014-08-14 20:16 29208 ----a-w- c:\windows\system32\drivers\aswHwid.sys
 2015-01-17 17:16 . 2013-12-25 14:48 116728 ----a-w- c:\windows\system32\drivers\aswstm.sys
 2015-01-17 17:16 . 2013-03-07 09:01 65776 ----a-w- c:\windows\system32\drivers\aswRvrt.sys
 2015-01-17 17:16 . 2013-03-07 09:01 267632 ----a-w- c:\windows\system32\drivers\aswVmm.sys
 2015-01-17 17:16 . 2011-10-30 15:06 436624 ----a-w- c:\windows\system32\drivers\aswsp.sys
 2015-01-17 17:16 . 2011-10-30 15:06 83280 ----a-w- c:\windows\system32\drivers\aswMonFlt.sys
 2015-01-17 17:16 . 2012-02-24 17:39 93568 ----a-w- c:\windows\system32\drivers\aswRdr2.sys
 2015-01-08 18:32 . 2014-06-15 07:48 590536 ----a-w-
 c:\programdata\Microsoft\ClickToRun\{9AC08E99-230B-47e8-9721-4577B7F124EA}\integrator.exe
 2015-01-08 08:55 . 2010-11-21 03:27 298120 -----w- c:\windows\system32\MpSigStub.exe

2014-12-31 12:12 . 2011-11-01 19:15 113365784 ----a-w- c:\windows\system32\MRT.exe

2014-12-04 02:50 . 2014-12-10 14:10 192000 ----a-w- c:\windows\system32\aeipic(645).dll

2014-11-21 08:38 . 2014-12-10 14:10 2237952 ----a-w- c:\windows\system32\wininet.dll

2014-11-21 08:37 . 2014-12-10 14:10 1409536 ----a-w- c:\windows\system32\urlmon.dll

2014-11-21 08:36 . 2014-12-10 14:10 15400960 ----a-w- c:\windows\system32\ieframe.dll

2014-11-21 08:36 . 2014-12-10 14:10 2655232 ----a-w- c:\windows\system32\iertutil.dll

2014-11-21 07:17 . 2014-12-10 14:10 1762816 ----a-w- c:\windows\SysWow64\wininet.dll

2014-11-11 03:09 . 2014-12-10 14:02 1424384 ----a-w-
c:\windows\system32\WindowsCodecs.dll

2014-11-11 03:08 . 2014-11-20 14:56 241152 ----a-w- c:\windows\system32\pku2u.dll

2014-11-11 03:08 . 2014-11-20 14:56 728064 ----a-w- c:\windows\system32\kerberos.dll

.

.

----- Sigcheck -----

Note: Unsigned files aren't necessarily malware.

.

[-] 2009-07-14 . 769765CE2CC62867468CEA93969B2242 . 23040 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\asynctmac.sys

.

[-] 2009-07-13 . 9899284589F75FA8724FF3D16AED75C1 . 6144 . . [6.1.7600.16385] ..
c:\windows\system32\drivers\null.sys

.

[-] 2010-11-21 . DDAD5A7AB24D8B65F8D724F5C20FD806 . 119296 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-tdi-over-
tcpip_31bf3856ad364e35_6.1.7601.17514_none_4863cdbaf2b532f8\tdx.sys

[-] 2010-11-21 . DDAD5A7AB24D8B65F8D724F5C20FD806 . 119296 . . [6.1.7601.17514] ..
c:\windows\system32\drivers\tdx.sys

.

[-] 2012-07-04 . 05F5A0D14A2EE1D8255C2AA0E9E8E694 . 136704 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
browserservice_31bf3856ad364e35_6.1.7601.17887_none_d6c68344b4d406bf\browser.dll

[-] 2012-07-04 . 156768ABAE1DAF29BA0B0C05C21FEF09 . 136704 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
browserservice_31bf3856ad364e35_6.1.7601.22044_none_d7783703cdd41e02\browser.dll

[-] 2010-11-21 . 8EF0D5C41EC907751B8429162B1239ED . 136192 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
browserservice_31bf3856ad364e35_6.1.7601.17514_none_d70f2c28b49dffae\browser.dll

[-] 2012-07-04 . 05F5A0D14A2EE1D8255C2AA0E9E8E694 . 136704 . . [6.1.7600.16385] ..
c:\windows\system32\browser.dll

.

[-] 2014-05-30 . F23812F9F7B130854E4BC0389F7C688C . 31232 . . [6.1.7601.18489] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18489_none_0429c981739f213b\lsass.exe

[-] 2014-05-30 . 04F6C08B30C599D301CE8530A6F6A703 . 31232 . . [6.1.7601.22705] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22705_none_0505e8508c7f766f\lsass.exe

[-] 2014-04-12 . 6598EBC4D209318EBD81F76833ECBEDB . 31232 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22653_none_04cdd63a8ca9d24f\lsass.exe

[-] 2014-04-12 . 6598EBC4D209318EBD81F76833ECBEDB . 31232 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22712_none_04f817868c8a465b\lsass.exe

[-] 2014-04-12 . 6598EBC4D209318EBD81F76833ECBEDB . 31232 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22736_none_04e678d68c96e399\lsass.exe

[-] 2014-04-12 . 6598EBC4D209318EBD81F76833ECBEDB . 31232 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22807_none_0507eaca8c7da644\lsass.exe

[-] 2014-04-12 . 6598EBC4D209318EBD81F76833ECBEDB . 31232 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22843_none_04d8a9f28ca1b0ac\lsass.exe

[-] 2014-04-12 . 204F3F58212B3E422C90BD9691A2DF28 . 31232 . . [6.1.7601.18443] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18443_none_044f07757384196d\lsass.exe

[-] 2014-04-12 . 204F3F58212B3E422C90BD9691A2DF28 . 31232 . . [6.1.7601.18443] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18496_none_041bf8b773a9f127\lsass.exe

[-] 2014-04-12 . 204F3F58212B3E422C90BD9691A2DF28 . 31232 . . [6.1.7601.18443] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18526_none_0467aa1173712ab7\lsass.exe

[-] 2014-04-12 . 204F3F58212B3E422C90BD9691A2DF28 . 31232 . . [6.1.7601.18443] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18637_none_045ddc5573785d26\lsass.exe

[-] 2013-09-25 . F021DAFB1F87616FCEBA159C2ED7042F . 30720 .. [6.1.7601.22465] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22465_none_04c503168cb026a0\lsass.exe

[-] 2013-09-25 . 4D71227301DD8D09097B9E4CC6527E5A . 30720 .. [6.1.7601.18270] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.18270_none_042b9307739f26ed\lsass.exe

[-] 2012-08-24 . 77119F1F9B492B260030C34F9BE327FA . 31232 .. [6.1.7601.22099] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22099_none_04a88ce28cc4eb33\lsass.exe

[-] 2012-06-04 . 79C908CAA6F43021EB05F4C733A927D1 . 31232 .. [6.1.7601.22010] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.22010_none_04f609a88c8c279c\lsass.exe

[-] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 .. [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.17725_none_0466c45b7371f20d\lsass.exe

[-] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 .. [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.17856_none_044756c773895c5e\lsass.exe

[-] 2011-11-17 . C118A82CD78818C29AB228366EBF81C3 . 31232 .. [6.1.7601.17725] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.17940_none_044c26dd7386a58a\lsass.exe

[-] 2011-11-17 . 0A10B74FBB437FF9A23F1D5DE4446A83 . 31232 .. [6.1.7601.21861] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.21861_none_04c1204e8cb39c3f\lsass.exe

[-] 2009-07-14 . 0793F40B9B8A1BDD266296409DBD91EA . 31232 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
lsa_31bf3856ad364e35_6.1.7601.17514_none_04709031736ac277\lsass.exe

[-] 2014-04-12 . 204F3F58212B3E422C90BD9691A2DF28 . 31232 .. [6.1.7601.18443] ..
c:\windows\system32\lsass.exe

.

[-] 2009-07-14 . 847D3AE376C0817161A14A82C8922A9E . 360448 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
netman_31bf3856ad364e35_6.1.7600.16385_none_6bb20d3d6b80d9da\netman.dll

[-] 2009-07-14 . 847D3AE376C0817161A14A82C8922A9E . 360448 .. [6.1.7600.16385] ..
c:\windows\system32\netman.dll

.

[-] 2010-11-21 . 1EA7969E3271CBC59E1730697DC74682 . 849920 .. [7.5.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-bits-
client_31bf3856ad364e35_6.1.7601.17514_none_81b6ca5c101195cd\qmgr.dll

[-] 2010-11-21 . 1EA7969E3271CBC59E1730697DC74682 . 849920 . . [7.5.7600.16385] ..
c:\windows\system32\qmgr.dll

.

[-] 2010-11-21 . 5C627D1B1138676C0A7AB2C2C190D123 . 512000 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-
rpcss_31bf3856ad364e35_6.1.7601.17514_none_c7f0e16b547f887d\rpcss.dll

[-] 2010-11-21 . 5C627D1B1138676C0A7AB2C2C190D123 . 512000 . . [6.1.7601.17514] ..
c:\windows\system32\rpcss.dll

.

[-] 2009-07-14 . 24ACB7E5BE595468E3B9AA488B9B4FCB . 328704 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-s..s-
servicecontroller_31bf3856ad364e35_6.1.7600.16385_none_2b54b20ee6fa07b1\services.exe

[-] 2009-07-14 . 24ACB7E5BE595468E3B9AA488B9B4FCB . 328704 . . [6.1.7600.16385] ..
c:\windows\system32\services.exe

.

[-] 2012-02-11 . 85DAA09A98C9286D4EA2BA8D0E644377 . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-
core_31bf3856ad364e35_6.1.7601.17777_none_3433cdb2d8563d50\spoolsv.exe

[-] 2012-02-11 . B9D7A4858CF32A6A15D2763F1DE47E0E . 559616 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-
core_31bf3856ad364e35_6.1.7601.21921_none_34ed7a43f150b682\spoolsv.exe

[-] 2010-11-21 . B96C17B5DC1424D56EEA3A99E97428CD . 559104 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-printing-spooler-
core_31bf3856ad364e35_6.1.7601.17514_none_3471a890d8284f57\spoolsv.exe

[-] 2012-02-11 . 85DAA09A98C9286D4EA2BA8D0E644377 . 559104 . . [6.1.7600.16385] ..
c:\windows\system32\spoolsv.exe

.

[-] 2014-03-04 . 6CE2AE073BD21C542FC2C707CAE944CC . 455680 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
winlogon_31bf3856ad364e35_6.1.7601.22616_none_ce748d1d04acf24f\winlogon.exe

[-] 2014-03-04 . 88AB9B72B4BF3963A0DE0820B4B0B06C . 455168 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
winlogon_31bf3856ad364e35_6.1.7601.18409_none_cdf8bf35eb848572\winlogon.exe

[-] 2010-11-21 . 1151B1BAA6F350B1DB6598E0FEA7C457 . 390656 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
winlogon_31bf3856ad364e35_6.1.7601.17514_none_cde90685eb910636\winlogon.exe

[-] 2014-07-17 . 8CEBD9D0A0A879CDE9F36F4383B7CAEA . 455168 . . [6.1.7601.17514] ..
c:\windows\system32\winlogon.exe

.

[-] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.18201_none_97c9d703ee91c7f1\comctl32.dll

[-] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.18201_none_a4d3b9377117c3df\comctl32.dll

[-] 2013-07-04 . 4F3C5CE9EF990E1C62B7E7EBA0EBA1C2 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.22376_none_980cc5cd07e3aa05\comctl32.dll

[-] 2013-07-04 . 4F3C5CE9EF990E1C62B7E7EBA0EBA1C2 . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.22376_none_a6ba9bf96e3dcd13\comctl32.dll

[-] 2010-11-21 . 14DFDEAF4E589ED3F1FF187A86B9408C . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.17514_none_97c2246fee970dbb\comctl32.dll

[-] 2010-11-21 . 14DFDEAF4E589ED3F1FF187A86B9408C . 633856 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_a4d6a923711520a9\comctl32.dll

[-] 2010-11-21 . 7FA8FDC2C2A27817FD0F624E78D3B50C . 2030080 . . [5.82] ..
c:\windows\winsxs\amd64_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_fa396087175ac9ac\comctl32.dll

[-] 2013-07-04 . 9028D1621C43DF8DFBD1C76860412A11 . 633856 . . [5.82] ..
c:\windows\system32\comctl32.dll

.

[-] 2009-07-14 . 1A47D52E303B7543E4E6026595B95422 . 1297408 . . [2001.12.8530.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-com-
complus.res_31bf3856ad364e35_6.1.7600.16385_none_88a5cc7effe2dfca\comres.dll

[-] 2009-07-14 . 1A47D52E303B7543E4E6026595B95422 . 1297408 . . [2001.12.8530.16385] ..
c:\windows\system32\comres.dll

.

[-] 2013-10-05 . 509D31797A4B8A3D6ED78A330B19A919 . 186880 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22473_none_d46d4138cabe2596\cryptsvc.dll

[-] 2013-07-09 . 434CCE8E7150CD1324C5FAA088D1D061 . 186880 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22380_none_d45f6e88cac8f85b\cryptsvc.dll

[-] 2013-07-09 . 6B400F211BEE880A37A1ED0368776BF4 . 184320 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18205_none_d431528fb165f7bc\cryptsvc.dll

[-] 2013-05-13 . D8129C49798CBBFB2E4351D4B7B8EF9C . 184320 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18151_none_d3f73fe5b19220ee\cryptsvc.dll

[-] 2013-05-11 . 8122252F0A4ACFA92FA0C1D50D18493B . 186880 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22322_none_d4a24ea4ca968363\cryptsvc.dll

[-] 2013-05-10 . 7FDC4626B01106A8EF328C88C7C0DEE3 . 184320 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18150_none_d3f63f9bb1930797\cryptsvc.dll

[-] 2013-05-10 . CA13C4F92BEE66DB48E58AB3223DDF6E . 186880 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22321_none_d4a14e5aca976a0c\cryptsvc.dll

[-] 2012-06-04 . 7E7D2DACF65D750D466F36BD3D09AE20 . 186880 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22010_none_d4ab184aca903d4f\cryptsvc.dll

[-] 2012-06-02 . 9C01375BE382E834CC26D1B7EAF2C4FE . 184320 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17856_none_d3fc6569b18d7211\cryptsvc.dll

[-] 2012-04-24 . 4F5414602E2544A4554D95517948B705 . 184320 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17827_none_d41dd577b1743795\cryptsvc.dll

[-] 2012-04-24 . B7337E9C9E5936355BB700AA33E0936E . 186880 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.21979_none_d473633acab895c2\cryptsvc.dll

[-] 2010-11-21 . 15597883FBE9B056F276ADA3AD87D9AF . 177152 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17514_none_d4259ed3b16ed82a\cryptsvc.dll

[-] 2013-07-09 . 6B400F211BEE880A37A1ED0368776BF4 . 184320 .. [6.1.7600.16385] ..
c:\windows\system32\cryptsvc.dll

.

[-] 2009-07-14 . 4166F82BE4D24938977DD1746BE9B8A0 . 402944 .. [2001.12.8530.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-c..complus-
eventsystem_31bf3856ad364e35_6.1.7600.16385_none_68e290c46b6ea6d0\es.dll

[-] 2009-07-14 . 4166F82BE4D24938977DD1746BE9B8A0 . 402944 .. [2001.12.8530.16385] ..
c:\windows\system32\es.dll

.

[-] 2009-07-14 . AA2C08CE85653B1A0D2E4AB407FA176C . 167424 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
imm32_31bf3856ad364e35_6.1.7600.16385_none_b84b0fbd941c03a9\imm32.dll

[-] 2009-07-14 . AA2C08CE85653B1A0D2E4AB407FA176C . 167424 . . [6.1.7600.16385] ..
c:\windows\system32\imm32.dll

.

[-] 2014-04-25 . 088CF6AFCD5CDD44E40C0ACDE3C1A5E0 . 801280 . . [1.0626.7601.18454] ..
c:\windows\winsxs\amd64_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.18454_none_0af5261f6f3c76ad\usp10.dll

[-] 2014-04-25 . BB2B03C6B6778A9B2866A049CC600D55 . 801792 . . [1.0626.7601.22666] ..
c:\windows\winsxs\amd64_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.22666_none_0b75f5788860623d\usp10.dll

[-] 2012-11-22 . E4ACCC7927A1478DF636534864E03666 . 801280 . . [1.0626.7601.22171] ..
c:\windows\winsxs\amd64_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.22171_none_0b661a9c886d0db8\usp10.dll

[-] 2012-11-22 . DBF99FD9CAF75CA66D042BD8D050FF71 . 800768 . . [1.0626.7601.18009] ..
c:\windows\winsxs\amd64_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.18009_none_0b302f956f0f750f\usp10.dll

[-] 2010-11-21 . 2F8B1E3EE3545D3B5A8D56FA1AE07B65 . 800256 . . [1.0626.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.17514_none_0b207e7d6f1bea6f\usp10.dll

[-] 2014-04-25 . 088CF6AFCD5CDD44E40C0ACDE3C1A5E0 . 801280 . . [1.0626.7601.18454] ..
c:\windows\system32\usp10.dll

.

[-] 2014-04-12 . 77BBBF70BCE286CD19E1E68F248363FA . 1164800 . . [6.1.7601.22653] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22653_none_f24130b9862a22c7\kernel32.dll

[-] 2014-03-04 . 52E77DC8E31C89FBB1E968699C8121C5 . 1164800 . . [6.1.7601.22616] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22616_none_f26f71478606ff08\kernel32.dll

[-] 2014-03-04 . D2A513EE880D71BDE7F0257F38B9D019 . 1163264 . . [6.1.7601.18409] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18409_none_f1f3a3606cde922b\kernel32.dll

[-] 2013-08-29 . 786D234A90FCAC72633AE6FC52653A49 . 1162240 . . [6.1.7601.22436] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22436_none_f259cda386173c9c\kernel32.dll

[-] 2013-08-02 . C525D51A79B01342344F02E38866CF60 . 1162240 . . [6.1.7601.22411] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22411_none_f26a6c09860b8607\kernel32.dll

[-] 2013-08-02 . D8973E71F1B35CD3F3DEA7C12D49D0F0 . 1161216 . . [6.1.7601.18229] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18229_none_f1ddffbc6ceecfbf\kernel32.dll

[-] 2013-07-08 . 38E54D419A2962E24D35D868E4724AE7 . 1162240 . . [6.1.7601.22379] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22379_none_f2318ceb8634fb3e\kernel32.dll

[-] 2013-01-04 . B844114B247D8EF1E5E4E93A282D2E6F . 1162240 . . [6.1.7601.22209] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22209_none_f27d3a7985fc3a80\kernel32.dll

[-] 2012-11-30 . B3BEA6420D482356E53B7C728E05C637 . 1163264 . . [6.1.7601.22177] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22177_none_f22f888b8636ce42\kernel32.dll

[-] 2012-11-30 . 65C113214F7B05820F6D8A65B1485196 . 1161216 . . [6.1.7601.18015] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18015_none_f1e4cab46cea5424\kernel32.dll

[-] 2012-10-04 . 1DC3504CA4C57900F1557E9A3F01D272 . 1161216 . . [6.1.7601.17965] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17965_none_f1aee2f66d12ac97\kernel32.dll

[-] 2012-10-04 . F3C594D0DA3ACFA6C7B781A490AB4282 . 1162240 . . [6.1.7601.22125] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22125_none_f263979386100fdf\kernel32.dll

[-] 2012-08-20 . EAF41CFBA5281834CBC383C710AC7965 . 1162240 . . [6.1.7601.17932] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17932_none_f1cc51dc6cfd0cbf\kernel32.dll

[-] 2012-08-20 . 624B34180C79D67C470C155DB81FFB8E . 1163264 . . [6.1.7601.22091] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22091_none_f213e511864c70f3\kernel32.dll

[-] 2011-07-16 . B9B42A302325537D7B9DC52D47F33A73 . 1162752 . . [6.1.7601.17651] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17651_none_f1b5ac086d0e33d5\kernel32.dll

[-] 2011-07-16 . 27AC02D8EE4C02E7648C41CB880151DA . 1163264 . . [6.1.7601.21772] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.21772_none_f22aa945863b24d8\kernel32.dll

[-] 2010-11-21 . 7A6326D96D53048FDEC542DF23D875A0 . 1161216 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17514_none_f1e3eab06ceb12ef\kernel32.dll

[-] 2014-03-04 . D2A513EE880D71BDE7F0257F38B9D019 . 1163264 . . [6.1.7601.18015] ..
c:\windows\system32\kernel32.dll

.

[-] 2009-07-14 . A0A65D306A5490D2EB8E7DE66898ECFD . 29696 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
linkinfo_31bf3856ad364e35_6.1.7600.16385_none_945a23c3bf051859\linkinfo.dll

[-] 2009-07-14 . A0A65D306A5490D2EB8E7DE66898ECFD . 29696 .. [6.1.7600.16385] ..
c:\windows\system32\linkinfo.dll

.

[-] 2013-06-06 . 796B47A4B82EF1C39F13435B88834C48 . 41472 .. [6.1.7601.18177] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.18177_none_07bb20dd7154003d\lpk.dll

[-] 2013-06-06 . 22FC61B8E1EBA296FF416C3678E26DD3 . 41472 .. [6.1.7601.22350] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22350_none_08535d608a67b3eb\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17514_none_07f91de77125e78d\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17537_none_07e67eed71336b74\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17563_none_07c20e01714f59eb\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17991_none_079fa54171696fac\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.18032_none_07e15d357138149f\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.21636_none_086f1b6e8a51f1e7\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.21664_none_084cab168a6c130c\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22153_none_08565a728a6505a2\lpk.dll

[-] 2009-07-14 . D202223587518B13D72D68937B7E3F70 . 41984 .. [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22195_none_082d1b568a83a814\lpk.dll

[-] 2013-06-06 . 796B47A4B82EF1C39F13435B88834C48 . 41472 .. [6.1.7601.18177] ..
c:\windows\system32\lpk.dll

.

[-] 2009-07-14 . 3B367397320C26DBA890B260F80D1B1B . 424448 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..ectionssharingconfig_31bf3856ad364e35_6.1.7600.16385_none_0c2b375bae4a8d38\hnetcfg.dll

[-] 2009-07-14 . 3B367397320C26DBA890B260F80D1B1B . 424448 . . [6.1.7600.16385] ..
c:\windows\system32\hnetcfg.dll

.

[-] 2014-08-17 . 4556BB9BA0CA2F03B72A15695C7290A0 . 19513856 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21183_none_7a801b56ac1ed143\mshtml.dll

[-] 2014-08-17 . 6EB8264F0EF4B684AF5F625C4C8D8E7B . 19280384 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.17089_none_9158092e926fef63\mshtml.dll

[-] 2014-07-24 . 90B1DA995893F25DE3438B152D29B089 . 19279872 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.17054_none_91557a3892722339\mshtml.dll

[-] 2014-07-24 . FCD088145986FCDB29DF083B80FFC235 . 19510784 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21173_none_7a7f1b0cac1fb7ec\mshtml.dll

[-] 2014-08-17 . 6EB8264F0EF4B684AF5F625C4C8D8E7B . 19280384 . . [10.00.9200.16521] ..
c:\windows\system32\mshtml.dll

.

[-] 2011-12-16 . C391FC68282A000CDF953F8B6B55D2EF . 634880 . . [7.0.7601.17744] ..
c:\windows\winsxs\amd64_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7601.17744_none_2f5acf97b59df60f\msvcrt.dll

[-] 2011-12-16 . F9A4C695C86CC32048FE2C987A0BD387 . 634880 . . [7.0.7601.21878] ..
c:\windows\winsxs\amd64_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7601.21878_none_2fc7fdc6ced04f08\msvcrt.dll

[-] 2009-07-14 . 7319BB10FA1F86E49E3DCF4136F6C957 . 634880 . . [7.0.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7600.16385_none_2d4a27c7b8972454\msvcrt.dll

[-] 2011-12-16 . C391FC68282A000CDF953F8B6B55D2EF . 634880 . . [7.0.7601.17744] ..
c:\windows\system32\msvcrt.dll

.

[-] 2013-09-08 . 9A9F9F1A77D6A80EE28B57664F00013E . 327168 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.18254_none_164e004b440bdabf\mswsock.dll

[-] 2013-09-07 . BDDDB1FD258B92DEE00F222D3304B5D9C . 327168 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.22444_none_16e26ee85d215bbf\mswsock.dll

[-] 2010-11-21 . 1D5185A4C7E6695431AE4B55C3D7D333 . 326144 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w...-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.17514_none_16795c7543eb48cf\mswsock.dll

[-] 2013-09-08 . 9A9F9F1A77D6A80EE28B57664F00013E . 327168 . . [6.1.7600.16385] ..
c:\windows\system32\mswsock.dll

.

[-] 2010-11-21 . AA339DD8BB128EF66660DFBBB59043D3 . 695808 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-security-
netlogon_31bf3856ad364e35_6.1.7601.17514_none_5bddbcb24e997298\netlogon.dll

[-] 2010-11-21 . AA339DD8BB128EF66660DFBBB59043D3 . 695808 . . [6.1.7600.16385] ..
c:\windows\system32\netlogon.dll

.

[-] 2009-07-14 . 716175021BDA290504CE434273F666BC . 167424 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
userpowermanagement_31bf3856ad364e35_6.1.7600.16385_none_ff0e900816896618\powrprof.dll

[-] 2009-07-14 . 716175021BDA290504CE434273F666BC . 167424 . . [6.1.7600.16385] ..
c:\windows\system32\powrprof.dll

.

[-] 2010-11-21 . ED78427259134C63ED69804D2132B86C . 232960 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
s..urationengineclient_31bf3856ad364e35_6.1.7601.17514_none_9633e7caefbaf953\scecli.dll

[-] 2010-11-21 . ED78427259134C63ED69804D2132B86C . 232960 . . [6.1.7600.16385] ..
c:\windows\system32\scecli.dll

.

[-] 2009-07-14 . C6DCD1D11ED6827F05C00773C3E7053C . 3072 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
sfc_31bf3856ad364e35_6.1.7600.16385_none_032ab4f375e2ac1f\sfc.dll

[-] 2009-07-14 . C6DCD1D11ED6827F05C00773C3E7053C . 3072 . . [6.1.7600.16385] ..
c:\windows\system32\sfc.dll

.

[-] 2009-07-14 . C78655BC80301D76ED4FEF1C1EA40A7D . 27136 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-services-
svchost_31bf3856ad364e35_6.1.7600.16385_none_11b04b481efec48c\svchost.exe

[-] 2009-07-14 . C78655BC80301D76ED4FEF1C1EA40A7D . 27136 . . [6.1.7600.16385] ..
c:\windows\system32\svchost.exe

.

[-] 2010-11-21 . 40F0849F65D13EE87B9A9AE3C1DD6823 . 316928 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
tapiservice_31bf3856ad364e35_6.1.7601.17514_none_4162de4afb9222c0\tapisrv.dll

[-] 2010-11-21 . 40F0849F65D13EE87B9A9AE3C1DD6823 . 316928 . . [6.1.7600.16385] ..
c:\windows\system32\tapisrv.dll

.

[-] 2010-11-21 . FE70103391A64039A921DBFFF9C7AB1B . 1008128 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
user32_31bf3856ad364e35_6.1.7601.17514_none_2b5e71b083fc0973\user32.dll

[-] 2010-11-21 . FE70103391A64039A921DBFFF9C7AB1B . 1008128 . . [6.1.7601.17514] ..
c:\windows\system32\user32.dll

.

[-] 2010-11-21 . BAFE84E637BF7388C96EF48D4D3FDD53 . 30720 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
userinit_31bf3856ad364e35_6.1.7601.17514_none_3a4ebf84e84f824c\userinit.exe

[-] 2010-11-21 . BAFE84E637BF7388C96EF48D4D3FDD53 . 30720 . . [6.1.7600.16385] ..
c:\windows\system32\userinit.exe

.

[-] 2014-08-17 . CB4792A08FCC5ABC41E5B5BF62A8F9C7 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21183_none_6925fc382bc8680d\wininet.dll

[-] 2014-08-17 . EC5D850ED17252AD109CCFC8F700247C . 2239488 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17089_none_7ffdea101219862d\wininet.dll

[-] 2014-07-24 . A56400B83371EAD36B9E62FAF0546595 . 2240000 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17054_none_7ffb5b1a121bba03\wininet.dll

[-] 2014-07-24 . E2708DEAE63239BB1168CDACB1677266 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21173_none_6924fbee2bc94eb6\wininet.dll

[-] 2014-06-19 . 27E552632E6394DE0FA555EFDBA29A49 . 2239488 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17028_none_7ff7ff1c121ed482\wininet.dll

[-] 2014-06-19 . 73D4292F9D3D8C5DA38F67AC214FC499 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21145_none_6921cd802bcc35f3\wininet.dll

[-] 2014-05-24 . 73AB92A1AA104EAF08B7AEA27B10C5CD . 2239488 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16921_none_7f974d6212671f6d\wininet.dll

[-] 2014-05-24 . 1D4B1862F128002565FFE9F4956053F6 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21044_none_692cb4342bc40061\wininet.dll

[-] 2014-03-13 . BC7D69E85E30098B4575B4804412E74D . 2238976 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16866_none_7fa5ac8e125be8fd\wininet.dll

[-] 2014-03-13 . 77A2459377E66D0F0F66E93AAE4C5ED9 . 2247168 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20985_none_68cf4d622c097db0\wininet.dll

[-] 2014-02-23 . 79EDF01FA13D886F8E1B655D542011FB . 2241536 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16844_none_7fa3d98a125d830d\wininet.dll

[-] 2014-02-23 . 2871A6CE6DDBA758870B9FC9243883AC . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20964_none_68cd63962c0b3161\wininet.dll

[-] 2014-02-01 . 90860E913075B03369BEB7B0B510DC2F . 2241536 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16798_none_7fb34fc812514c53\wininet.dll

[-] 2014-02-01 . FF27EF62A1DB2FC6545532911DC7C5C1 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20916_none_68c834942c0fe5f0\wininet.dll

[-] 2013-10-25 . E7099336BF7531B6FCC920DCB5101259 . 2241536 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16750_none_7fb004e0125419ef\wininet.dll

[-] 2013-10-25 . 355156BBE54D87BE8DE7186E4629342B . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20861_none_68d877da2c02c88d\wininet.dll

[-] 2013-10-12 . 9706C99DAEBE3FEAC811B239617E98C4 . 2241536 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16736_none_7fad7b9c12568107\wininet.dll

[-] 2013-10-12 . 7E7F32C588DA6A4554046804D8EEAC55 . 2249216 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20848_none_68d5d7ce2c054946\wininet.dll

[-] 2013-09-22 . 1377A310439639A610097ED56975AE19 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20831_none_68d576fc2c057c88\wininet.dll

[-] 2013-09-22 . D28B35DE88D27EFB27DF4B1E8319E3C0 . 2241024 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16721_none_7faced3a1256e78b\wininet.dll

[-] 2013-08-10 . AAFA952E774DDDB0956D3BDFAE5B5B99 . 2241024 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16686_none_7fbd4cfa1249e3c9\wininet.dll

[-] 2013-08-10 . 0A380C8E396975463E3F643E88AE8BDF . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20794_none_68e6044c2bf84584\wininet.dll

[-] 2013-07-26 . AC155DD9BD1E6D3B740826A4D1C68AAE . 2241024 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16660_none_7fbbd516124b1755\wininet.dll

[-] 2013-07-26 . 5C49F5A791B944AD8247473ABD35602D . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20768_none_68e2a84e2bfb6003\wininet.dll

[-] 2013-06-12 . 09BF0D9701F9D846BBC5ABED003851CB . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20742_none_68e1306a2bfc938f\wininet.dll

[-] 2013-06-11 . FAF6EC2460AD5FBBD38D8E1AE28B0D77 . 2241024 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16635_none_7fb86250124e4b75\wininet.dll

[-] 2013-05-17 . 7E43B93C0E9C138AC1008F646B06E919 . 2248704 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20719_none_68dd90142bfffaf1\wininet.dll

[-] 2013-05-17 . 12716D987D475B051F35895659159705 . 2241024 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16614_none_7fb67884124fff26\wininet.dll

[-] 2013-04-05 . 27A9000C534AA9BAD9CE74940F50C6D . 2242048 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16576_none_7fc71c9c1242ae81\wininet.dll

[-] 2013-04-05 . 61962C7A2D6E32827F089E6F0A03E533 . 2247168 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20681_none_68f018462bf0c359\wininet.dll

[-] 2013-03-22 . 69F1D418B4C4EC23033D598E4CBC6B73 . 2240512 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16521_none_7fc28d121246afa9\wininet.dll

[-] 2013-02-28 . 7EA5274E1688339A72C152438F5BBE80 . 1188864 . . [8.00.7601.18094] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.18094_none_7a72a07e2fb59c0a\wininet.dll

[-] 2013-02-28 . 734A1387945DA9215102A782E83C460E . 1189888 . . [8.00.7601.22258] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22258_none_7b2b800748af2e93\wininet.dll

[-] 2013-02-24 . 32D39C8BA5940DA0EB6E7993F3190F92 . 2247168 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20644_none_68ebd2c62bf4aae0\wininet.dll

[-] 2013-02-21 . 753C0848AE7872A3F59663078A517293 . 2240512 . . [10.00.9200.16521] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16540_none_7fc4a46e1244c8b6\wininet.dll

[-] 2012-12-20 . 2369627A789B29866825BD9504F7B237 . 1189888 . . [8.00.7601.22199] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22199_none_7b013ebb48ceba87\wininet.dll

[-] 2012-12-20 . 81101547092783DC117D800D3573EBD4 . 1188864 . . [8.00.7601.18035] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.18035_none_7ab480502f840dbb\wininet.dll

[-] 2012-10-27 . 7E04D13661FB771CA4FDBB836AD0BA49 . 1188864 . . [8.00.7601.17984] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17984_none_7a7d98482fad4cd7\wininet.dll

[-] 2012-10-27 . 6C11E0E42D91728C8283917A8F57A72E . 1189888 . . [8.00.7601.22145] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22145_none_7b334d2f48a9c976\wininet.dll

[-] 2012-08-24 . 443D30EB805EEEE1E31C91ADCC82AB89 . 1188864 . . [8.00.7601.17940] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17940_none_7aa4d6d02f9077b7\wininet.dll

[-] 2012-08-24 . 635D10865A99EA8E7E532C84D952D769 . 1189888 . . [8.00.7601.22099] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22099_none_7b013cd548cebd60\wininet.dll

[-] 2012-06-27 . ADC0BAC148C957CF51B1F6F658A4FCA6 . 1188864 . . [8.00.7601.17874] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17874_none_7a88664e2fa533bf\wininet.dll

[-] 2012-06-27 . 69449A3D42AC7000ACF5055172618632 . 1189888 . . [8.00.7601.22032] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22032_none_7b3b1a5748a46459\wininet.dll

[-] 2012-05-15 . CE5BFBD9685EE37DB942211450AAEA8F . 1188864 . . [8.00.7601.17842] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17842_none_7aa6d57e2f8ead3e\wininet.dll

[-] 2012-05-15 . 507FBE142C77A32C1AE56CA35B6A7307 . 1189888 . . [8.00.7601.21995] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21995_none_7afd638b48d224c2\wininet.dll

[-] 2012-02-28 . DE03C917EDED2A999C942A4F943D3068 . 1188864 . . [8.00.7601.17785] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17785_none_7a7e94c62fac6be0\wininet.dll

[-] 2012-02-28 . 05ED629EBOA11CAFB87EFB7847943312 . 1189376 . . [8.00.7601.21931] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21931_none_7b3a41eb48a517c0\wininet.dll

[-] 2011-12-16 . F6C45D1D448B38A3298505917710F047 . 1188864 . . [8.00.7601.17744] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17744_none_7aa8d42c2f8ce2c5\wininet.dll

[-] 2011-12-16 . 7710ECF9F1355F986463D4351562439E . 1189376 . . [8.00.7601.21878] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21878_none_7b16025b48bf3bbe\wininet.dll

[-] 2011-11-05 . 4EFC156290537BB9706D3A7A1A4B8733 . 1188864 . . [8.00.7601.17720] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17720_none_7aba72dc2f804587\wininet.dll

[-] 2011-11-05 . 8F2CC83B92626A3B7E1DF360720FAD30 . 1189376 . . [8.00.7601.21855] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21855_none_7b28a15548b1b7d7\wininet.dll

[-] 2011-08-20 . DB33A1489C1DA1F37AC2D84CB9756DD1 . 1188864 . . [8.00.7601.17671] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17671_none_7a8561a42fa7ed6c\wininet.dll

[-] 2011-08-20 . 2B4973A8A9D0336EEF6E10DBD6E5B87D . 1189376 . . [8.00.7601.21795] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21795_none_7afd5fbf48d22a74\wininet.dll

[-] 2011-06-21 . 1A36497983C867FB85FF1DCD4933015F . 1188864 . . [8.00.7601.17638] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17638_none_7ab7a35a2f812f09\wininet.dll

[-] 2011-06-21 . 6ABD901E178675DFE86CCE75F2FAC9A5 . 1189376 . . [8.00.7601.21754] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21754_none_7b279f2548b2a159\wininet.dll

[-] 2010-11-21 . F6C5302E1F4813D552F41A0AC82455E5 . 1188864 . . [8.00.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17514_none_7ac940242f7494a4\wininet.dll

[-] 2014-11-21 . 7E5EFE2543E98D7D6A6557ED704D3DD6 . 2237952 . . [10.00.9200.16521] ..
c:\windows\system32\wininet.dll

.

[-] 2010-11-21 . 4BBFA57F594F7E8A8EDC8F377184C3F0 . 297984 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..nfrastructure-
ws232_31bf3856ad364e35_6.1.7601.17514_none_50ddb631e4f59005\ws2_32.dll

[-] 2010-11-21 . 4BBFA57F594F7E8A8EDC8F377184C3F0 . 297984 . . [6.1.7600.16385] ..
c:\windows\system32\ws2_32.dll

.

[-] 2009-07-14 . 8396C6C26AADD4FE4590CCE4F0F419B6B7 . 4608 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-w..nfrastructure-
other_31bf3856ad364e35_6.1.7600.16385_none_6079f415110c0210\ws2help.dll

[-] 2009-07-14 . 8396C6C26AADD4FE4590CCE4F0F419B6B7 . 4608 . . [6.1.7600.16385] ..
c:\windows\system32\ws2help.dll

.

[-] 2010-11-21 . 6C60B5ACA7442EFB794082CDACFC001C . 2086912 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-com-base-qfe-
ole32_31bf3856ad364e35_6.1.7601.17514_none_0a43accb08f0eac5\ole32.dll

[-] 2010-11-21 . 6C60B5ACA7442EFB794082CDACFC001C . 2086912 . . [6.1.7600.16385] ..
c:\windows\system32\ole32.dll

.

[-] 2009-07-14 . 86FE1B1F8FD42CD0DB641AB1CDB13093 . 18944 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-cngaudit-
dll_31bf3856ad364e35_6.1.7600.16385_none_4458dccc49458461\cngaudit.dll

[-] 2009-07-14 . 86FE1B1F8FD42CD0DB641AB1CDB13093 . 18944 . . [6.1.7600.16385] ..
c:\windows\system32\cngaudit.dll

.

[-] 2009-07-14 . 94355C28C1970635A31B3FE52EB7CEBA . 129024 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
wininit_31bf3856ad364e35_6.1.7600.16385_none_8ce7aa761e01ad49\wininit.exe

[-] 2009-07-14 . 94355C28C1970635A31B3FE52EB7CEBA . 129024 . . [6.1.7600.16385] ..
c:\windows\system32\wininit.exe

.

[-] 2009-07-14 . 42B6A94DD747DF2B5F628A2752E62A98 . 9728 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-t..cesframework-
ctfmon_31bf3856ad364e35_6.1.7600.16385_none_f9257e7aaa4290ce\ctfmon.exe

[-] 2009-07-14 . 42B6A94DD747DF2B5F628A2752E62A98 . 9728 . . [6.1.7600.16385] ..
c:\windows\system32\ctfmon.exe

.

[-] 2010-11-21 . AAF932B4011D14052955D4B212A4DA8D . 370688 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
shsvcs_31bf3856ad364e35_6.1.7601.17514_none_2b566299338d2123\shsvcs.dll

[-] 2010-11-21 . AAF932B4011D14052955D4B212A4DA8D . 370688 . . [6.1.7600.16385] ..
c:\windows\system32\shsvcs.dll

.

[-] 2009-07-14 . E4D94F24081440B5FC5AA556C7C62702 . 159232 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-remoteregistry-
service_31bf3856ad364e35_6.1.7600.16385_none_e55af7609d2857a8\regsvc.dll

[-] 2009-07-14 . E4D94F24081440B5FC5AA556C7C62702 . 159232 . . [6.1.7600.16385] ..
c:\windows\system32\regsvc.dll

.

[-] 2010-11-21 . 262F6592C3299C005FD6BEC90FC4463A . 1110016 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-taskscheduler-
service_31bf3856ad364e35_6.1.7601.17514_none_8d272400ada202f9\schedsvc.dll

[-] 2010-11-21 . 262F6592C3299C005FD6BEC90FC4463A . 1110016 . . [6.1.7600.16385] ..
c:\windows\system32\schedsvc.dll

.

[-] 2009-07-14 . 51B52FBD583CDE8AA9BA62B8B4298F33 . 193024 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
upnpssdp_31bf3856ad364e35_6.1.7600.16385_none_dbbe6492eae9505c\ssdpsrv.dll

[-] 2009-07-14 . 51B52FBD583CDE8AA9BA62B8B4298F33 . 193024 . . [6.1.7600.16385] ..
c:\windows\system32\ssdpsrv.dll

.

[-] 2010-11-21 . 2E648163254233755035B46DD7B89123 . 680960 . . [6.1.7601.17514] ..
c:\windows\winsxs\amd64_microsoft-windows-
t..teconnectionmanager_31bf3856ad364e35_6.1.7601.17514_none_ecc547376ae3a1a3\termsrv.dll

[-] 2010-11-21 . 2E648163254233755035B46DD7B89123 . 680960 . . [6.1.7601.17514] ..
c:\windows\system32\termsrv.dll

.

[-] 2009-07-14 . 8560FFFC8EB3A806DCD4F82252CFC8C6 . 5120 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-d..tshow-
kernel support_31bf3856ad364e35_6.1.7601.17514_none_4627a1cbadebced2\ksuser.dll

[-] 2009-07-14 . 8560FFFC8EB3A806DCD4F82252CFC8C6 . 5120 . . [6.1.7600.16385] ..
c:\windows\system32\ksuser.dll

.

[-] 2009-07-14 . E424B3EF666B184CEE0B6871AAA8C9F6 . 8192 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-gdi-
painting_31bf3856ad364e35_6.1.7600.16385_none_d360c9c235bd1868\msimg32.dll

[-] 2009-07-14 . E424B3EF666B184CEE0B6871AAA8C9F6 . 8192 . . [6.1.7600.16385] ..
c:\windows\system32\msimg32.dll

.

[-] 2013-07-04 . 700BD5A6AA5381D1D8ADC4045149DBF6 . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.22376_none_3bee2a494f8638cf\comctl32.dll

[-] 2013-07-04 . 700BD5A6AA5381D1D8ADC4045149DBF6 . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.22376_none_ee67d2d082b9f619\comctl32.dll

[-] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 .. [5.82] ..
c:\windows\SysWOW64\comctl32.dll

[-] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.18201_none_3bab3b80363456bb\comctl32.dll

[-] 2013-07-04 . 75F5E1FE8D55CF8E577E0EC5F2290D3F . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.18201_none_ec80f00e8593ece5\comctl32.dll

[-] 2010-11-21 . BDAC1AA64495D0F7E1FF810EBBF1F018 . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

[-] 2010-11-21 . BDAC1AA64495D0F7E1FF810EBBF1F018 . 530432 .. [5.82] ..
c:\windows\winsxs\x86_microsoft-windows-shell-comctl32-
v5_31bf3856ad364e35_6.1.7601.17514_none_3ba388ec36399c85\comctl32.dll

[-] 2010-11-21 . 352B3DC62A0D259A82A052238425C872 . 1680896 .. [5.82] ..
c:\windows\winsxs\x86_microsoft.windows.common-
controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

.

[-] 2013-10-05 . F2D9242C3BBD1C36467FCAE1AE01733F . 142848 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22473_none_784ea5b51260b460\cryptsvc.dll

[-] 2013-07-09 . 6DB499DEFCC827317C5371164A7CDB27 . 142848 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22380_none_7840d305126b8725\cryptsvc.dll

[-] 2013-07-09 . 7CA1BECEA5DE2643ADDAD32670E7A4C9 . 140288 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\cryptsvc.dll

[-] 2013-07-09 . 7CA1BECEA5DE2643ADDAD32670E7A4C9 . 140288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18205_none_7812b70bf9088686\cryptsvc.dll

[-] 2013-05-13 . 3897DFF247D9ED0006190349DE264E14 . 140288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18151_none_77d8a461f934afb8\cryptsvc.dll

[-] 2013-05-11 . AC04D05309BB2C418D0D80B9FB014642 . 142848 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22322_none_7883b3211239122d\cryptsvc.dll

[-] 2013-05-10 . E122AA1C9A3CC46FF9DDDE46E5EB0C58 . 142848 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22321_none_7882b2d71239f8d6\cryptsvc.dll

[-] 2013-05-10 . 33ADF6E0853AB39EA1723BE82842C1D3 . 140288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.18150_none_77d7a417f9359661\cryptsvc.dll

[-] 2012-06-02 . 063DD65889D21035311463337BD268E7 . 142336 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.22010_none_788c7cc71232cc19\cryptsvc.dll

[-] 2012-06-02 . 96C0E38905CFD788313BE8E11DAE3F2F . 140288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17856_none_77ddc9e5f93000db\cryptsvc.dll

[-] 2012-04-24 . 06E771AA596B8761107AB57E99F128D7 . 140288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17827_none_77ff39f3f916c65f\cryptsvc.dll

[-] 2012-04-24 . 21993009E0CCB9B4FA195F14D3408626 . 142336 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.21979_none_7854c7b7125b248c\cryptsvc.dll

[-] 2010-11-21 . A585BEBF7D054BD9618EDA0922D5484A . 136192 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cryptsvc-
dll_31bf3856ad364e35_6.1.7601.17514_none_7807034ff91166f4\cryptsvc.dll

.

[-] 2009-07-14 . F6916EFC29D9953D5D0DF06882AE8E16 . 271360 .. [2001.12.8530.16385] ..
c:\windows\SysWOW64\es.dll

[-] 2009-07-14 . F6916EFC29D9953D5D0DF06882AE8E16 . 271360 .. [2001.12.8530.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-c..complus-
eventsystem_31bf3856ad364e35_6.1.7600.16385_none_73373b169fcf68cb\es.dll

.

[-] 2010-11-21 . A6F09E5669D9A19035F6D942CAA15882 . 119808 .. [6.1.7601.17514] ..
c:\windows\SysWOW64\imm32.dll

[-] 2010-11-21 . A6F09E5669D9A19035F6D942CAA15882 . 119808 .. [6.1.7601.17514] ..
c:\windows\winsxs\wow64_microsoft-windows-
imm32_31bf3856ad364e35_6.1.7601.17514_none_c4d0cdd7c56b493e\imm32.dll

.

[-] 2014-04-12 . C8C41EBEE097FEB29FB816854D3AD1E7 . 1114112 .. [6.1.7601.22653] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22653_none_fc95db0bba8ae4c2\kernel32.dll

[-] 2014-03-04 . 866696FBE24914047462E34812169954 . 1114112 . . [6.1.7601.22616] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22616_none_fcc41b99ba67c103\kernel32.dll

[-] 2014-03-04 . 76161B9D78A275F8F28DD67436013110 . 1114112 . . [6.1.7601.18015] ..
c:\windows\SysWOW64\kernel32.dll

[-] 2014-03-04 . 76161B9D78A275F8F28DD67436013110 . 1114112 . . [6.1.7601.18409] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18409_none_fc484db2a13f5426\kernel32.dll

[-] 2013-08-29 . EE751CBD5D0C332FDF3DF7187B612416 . 1114112 . . [6.1.7601.22436] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22436_none_fcac77f5ba77fe97\kernel32.dll

[-] 2013-08-02 . 61579F821AB5FF7FA2966D64D1070BA8 . 1114112 . . [6.1.7601.22411] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22411_none_fcbf165bba6c4802\kernel32.dll

[-] 2013-08-02 . 365A5034093AD9E04F433046C4CDF6AB . 1114112 . . [6.1.7601.18229] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18229_none_fc32aa0ea14f91ba\kernel32.dll

[-] 2013-07-08 . 2997A7BC59E3EEFE8E86D1B0F3A3D748 . 1114112 . . [6.1.7601.22379] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22379_none_fc86373dba95bd39\kernel32.dll

[-] 2013-01-04 . 7E55988F5CB3BA67E2732370E8D71BBB . 1114112 . . [6.1.7601.22209] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22209_none_fcd1e4cbba5cfc7b\kernel32.dll

[-] 2012-11-30 . 9CC2571E3646B9A24296AD7ADCC71682 . 1114112 . . [6.1.7601.22177] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22177_none_fc8432ddba97903d\kernel32.dll

[-] 2012-11-30 . AC0B6F41882FC6ED186962D770EBF1D2 . 1114112 . . [6.1.7601.18015] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.18015_none_fc397506a14b161f\kernel32.dll

[-] 2012-10-04 . D4F3176082566CEFA633B4945802D4C4 . 1114112 . . [6.1.7601.17965] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17965_none_fc038d48a1736e92\kernel32.dll

[-] 2012-10-04 . 5FA395364EE727E4BEE6B1406C207F98 . 1114112 . . [6.1.7601.22125] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22125_none_fcb841e5ba70d1da\kernel32.dll

[-] 2012-08-20 . 9B98D47916EAD4F69EF51B56B0C2323C . 1114112 . . [6.1.7601.17932] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17932_none_fc20fc2ea15dceba\kernel32.dll

[-] 2012-08-20 . 305681B4B695D4A888B941965FFC2C17 . 1114112 . . [6.1.7601.22091] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.22091_none_fc688f63baad32ee\kernel32.dll

[-] 2011-07-16 . D3CB12854171DF61D117D7C2BF22C675 . 1114112 .. [6.1.7601.21772] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.21772_none_fc7f5397ba9be6d3\kernel32.dll

[-] 2011-07-16 . 99C3F8E9CC59D95666EB8D8A8B4C2BEB . 1114112 .. [6.1.7601.17651] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17651_none_fc0a565aa16ef5d0\kernel32.dll

[-] 2010-11-21 . E80758CF485DB142FCA1EE03A34EAD05 . 837632 .. [6.1.7601.17514] ..
c:\windows\winsxs\wow64_microsoft-windows-
kernel32_31bf3856ad364e35_6.1.7601.17514_none_fc389502a14bd4ea\kernel32.dll

.

[-] 2009-07-14 . 5987EA8A82C53359BCD2C29D6588583E . 22016 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\linkinfo.dll

[-] 2009-07-14 . 5987EA8A82C53359BCD2C29D6588583E . 22016 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
linkinfo_31bf3856ad364e35_6.1.7600.16385_none_9eaece15f365da54\linkinfo.dll

.

[-] 2013-06-06 . 84CA3579EEB69D8E1EE67E4F721BF71C . 25600 .. [6.1.7601.22350] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22350_none_12a807b2bec875e6\lpk.dll

[-] 2013-06-06 . CC23295DA8F7B5C53F93804D2F5D30EB . 25600 .. [6.1.7601.18177] ..
c:\windows\SysWOW64\lpk.dll

[-] 2013-06-06 . CC23295DA8F7B5C53F93804D2F5D30EB . 25600 .. [6.1.7601.18177] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.18177_none_120fcb2fa5b4c238\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17514_none_124dc839a586a988\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17537_none_123b293fa5942d6f\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17563_none_1216b853a5b01be6\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.17991_none_11f44f93a5ca31a7\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.18032_none_12360787a598d69a\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.21636_none_12c3c5c0beb2b3e2\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.21664_none_12a15568beccd507\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22153_none_12ab04c4bec5c79d\lpk.dll

[-] 2009-07-14 . 384721EF4024890092625E20CADFAF85 . 25600 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
gdi_31bf3856ad364e35_6.1.7601.22195_none_1281c5a8bee46a0f\lpk.dll

.

[-] 2014-08-17 . EBE8E945C5DB959F94E91B3086660594 . 14380032 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21183_none_84d4c5a8e07f933e\mshtml.dll

[-] 2014-08-17 . 9004D71AD5841653CC67F48B7428EC7D . 14369280 . . [10.00.9200.16521] ..
c:\windows\SysWOW64\mshtml.dll

[-] 2014-08-17 . 9004D71AD5841653CC67F48B7428EC7D . 14369280 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.17089_none_9bacb380c6d0b15e\mshtml.dll

[-] 2014-07-24 . 59519C658518AA899B76AEFA7719112 . 14371328 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.17054_none_9baa248ac6d2e534\mshtml.dll

[-] 2014-07-24 . BED0962F903F15BE6017E230A9AA23ED . 14381568 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21173_none_84d3c55ee08079e7\mshtml.dll

[-] 2014-06-19 . 8795FB612463119D7560EBA9C7F8784D . 14368768 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.17028_none_9ba6c88cc6d5ffb3\mshtml.dll

[-] 2014-06-19 . 253695A4D3C6173B697EF07B08AD57CE . 14382080 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21145_none_84d096f0e0836124\mshtml.dll

[-] 2014-05-24 . 42E4D0EDE893712B4C9562E7B32FF4C2 . 14387712 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21044_none_84db7da4e07b2b92\mshtml.dll

[-] 2014-05-24 . 094BD2492BB6266C8FFF09644682EA00 . 14365696 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16921_none_9b4616d2c71e4a9e\mshtml.dll

[-] 2014-05-06 . 09E7C1165BDE00E99C3B9F2BC50A2291 . 14391808 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21026_none_84d94f80e07d2c26\mshtml.dll

[-] 2014-05-06 . F2E912C438B0BB201391B831DA63BE06 . 14367232 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16899_none_9b573284c710ad16\mshtml.dll

[-] 2014-04-29 . ACA93994D1F82136AA51BEE6F42D8C6B . 14379520 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.21024_none_84d97d10e07cf8e4\mshtml.dll

[-] 2014-04-29 . DC4D93C813DF8235BD8502AF6A6E044F . 14357504 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16897_none_9b576014c71079d4\mshtml.dll

[-] 2014-03-13 . CE6947653C01DAAF20E08C8FCC0EFB76 . 14378496 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.20985_none_847e16d2e0c0a8e1\mshtml.dll

[-] 2014-03-13 . 3242A084CD8F934337E711F7C7EE5E6B . 14358016 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16866_none_9b5475fec713142e\mshtml.dll

[-] 2014-02-23 . DFCAEF189F365EFEC5BB97F88DC7093E . 14379008 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.20964_none_847c2d06e0c25c92\mshtml.dll

[-] 2014-02-23 . 9F378D86F983E84A0212678C1D18D7FC . 14358016 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16844_none_9b52a2fac714ae3e\mshtml.dll

[-] 2014-02-01 . 291A590DE76068D5F677356B4F22C2E7 . 14382080 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.20916_none_8476fe04e0c71121\mshtml.dll

[-] 2014-02-01 . 4098C722E878697489F0207108C8E0DA . 14359040 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16798_none_9b621938c7087784\mshtml.dll

[-] 2013-10-25 . B8FAAC62ED026D87B3E743B339C92786 . 14356992 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.16750_none_9b5ece50c70b4520\mshtml.dll

[-] 2013-10-25 . 0720197691DE3FDBBBB115587DC39E1C . 14381056 . . [10.00.9200.16521] ..
c:\windows\winsxs\wow64_microsoft-windows-ie-
htmlrendering_31bf3856ad364e35_10.2.9200.20861_none_8487414ae0b9f3be\mshtml.dll

.

[-] 2011-12-16 . 2F740C4B458331357E825E94AFB0953A . 690688 . . [7.0.7601.21878] ..
c:\windows\winsxs\x86_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7601.21878_none_d3a962431672ddd2\msvcrt.dll

[-] 2011-12-16 . 9DC80A8AAAAAC397BDAB3C67165A824E . 690688 . . [7.0.7601.17744] ..
c:\windows\SysWOW64\msvcrt.dll

[-] 2011-12-16 . 9DC80A8AAAAAC397BDAB3C67165A824E . 690688 . . [7.0.7601.17744] ..
c:\windows\winsxs\x86_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7601.17744_none_d33c3413fd4084d9\msvcrt.dll

[-] 2009-07-14 . E46D48A7FE961401F1CBF85531CDF05D . 690688 . . [7.0.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
msvcrt_31bf3856ad364e35_6.1.7600.16385_none_d12b8c440039b31e\msvcrt.dll

.

[-] 2013-09-08 . E94C583CDE2348950155F2AF2876F34D . 231424 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\mswsock.dll

[-] 2013-09-08 . E94C583CDE2348950155F2AF2876F34D . 231424 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-w..-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.18254_none_ba2f64c78bae6989\mswsock.dll

[-] 2013-09-07 . 6547D445C4B69DC0083B619AC642DF04 . 231424 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-w..-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.22444_none_bac3d364a4c3ea89\mswsock.dll

[-] 2010-11-21 . 8999B8631C7FD9F7F9EC3CAFD953BA24 . 232448 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-w..-infrastructure-
bsp_31bf3856ad364e35_6.1.7601.17514_none_ba5ac0f18b8dd799\mswsock.dll

.

[-] 2010-11-21 . C1809B9907AEDAF16F50C894100883B . 563712 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\netlogon.dll

[-] 2010-11-21 . C1809B9907AEDAF16F50C894100883B . 563712 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-security-
netlogon_31bf3856ad364e35_6.1.7601.17514_none_6632670482fa3493\netlogon.dll

.

[-] 2009-07-14 . 08DFDBD2FD4EA951DC46B1C7661ED35A . 145408 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\powrprof.dll

[-] 2009-07-14 . 08DFDBD2FD4EA951DC46B1C7661ED35A . 145408 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
userpowermanagement_31bf3856ad364e35_6.1.7600.16385_none_a2eff4845e2bf4e2\powrprof.dll

.

[-] 2010-11-21 . 8124944EC89D6A1815E4E53F5B96AAF4 . 175616 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\scecli.dll

[-] 2010-11-21 . 8124944EC89D6A1815E4E53F5B96AAF4 . 175616 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
s..urationengineclient_31bf3856ad364e35_6.1.7601.17514_none_a088921d241bbb4e\scecli.dll

.

[-] 2009-07-14 . 40CAEEEE0EAF1B8569F7C8DF6420F2CB9 . 2560 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\sfc.dll

[-] 2009-07-14 . 40CAEEEE0EAF1B8569F7C8DF6420F2CB9 . 2560 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
sfc_31bf3856ad364e35_6.1.7600.16385_none_a70c196fbd853ae9\sfc.dll

.

[-] 2009-07-14 . 54A47F6B5E09A77E61649109C6A08866 . 20992 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\svchost.exe

[-] 2009-07-14 . 54A47F6B5E09A77E61649109C6A08866 . 20992 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-services-
svchost_31bf3856ad364e35_6.1.7600.16385_none_b591afc466a15356\svchost.exe

.

[-] 2010-11-21 . 613BF4820361543956909043A265C6AC . 242176 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\tapisrv.dll

[-] 2010-11-21 . 613BF4820361543956909043A265C6AC . 242176 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
tapiservice_31bf3856ad364e35_6.1.7601.17514_none_e54442c74334b18a\tapisrv.dll

.

[-] 2010-11-21 . 5E0DB2D8B2750543CD2EBB9EA8E6CDD3 . 833024 . . [6.1.7601.17514] ..
c:\windows\SysWOW64\user32.dll

[-] 2010-11-21 . 5E0DB2D8B2750543CD2EBB9EA8E6CDD3 . 833024 . . [6.1.7601.17514] ..
c:\windows\winsxs\wow64_microsoft-windows-
user32_31bf3856ad364e35_6.1.7601.17514_none_35b31c02b85ccb6e\user32.dll

.

[-] 2010-11-21 . 61AC3EFDFAFDD3F0F11DD4FD4044223 . 26624 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\userinit.exe

[-] 2010-11-21 . 61AC3EFDFAFDD3F0F11DD4FD4044223 . 26624 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
userinit_31bf3856ad364e35_6.1.7601.17514_none_de3024012ff21116\userinit.exe

.

[-] 2014-11-21 . 2BB8BC3DF1BE3F384931021E7D8331E4 . 1762816 . . [10.00.9200.16521] ..
c:\windows\SysWOW64\wininet.dll

[-] 2014-08-17 . 5766867096FE1BF30894574807AB3576 . 1773568 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21183_none_0d0760b4736af6d7\wininet.dll

[-] 2014-08-17 . 7D9284D509F8D17EEADE8A486BB3FC19 . 1766400 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17089_none_23df4e8c59bc14f7\wininet.dll

[-] 2014-07-24 . 7951C75E6B680204BD624A0C3CE2C573 . 1766400 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17054_none_23dcbf9659be48cd\wininet.dll

[-] 2014-07-24 . 008DA47C81390581E625EC8F7B08FF7A . 1773568 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21173_none_0d06606a736bdd80\wininet.dll

[-] 2014-06-19 . 27631A4D65AB1FA5718EBBFED05B7815 . 1766400 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.17028_none_23d9639859c1634c\wininet.dll

[-] 2014-06-19 . E5CCC24D0A4BE5613A2A43343FBB3DBA . 1773568 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21145_none_0d0331fc736ec4bd\wininet.dll

[-] 2014-05-24 . F68057C0E20C9ACE89311861CDB180EF . 1773568 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.21044_none_0d0e18b073668f2b\wininet.dll

[-] 2014-05-24 . B46C4C23FB70D3C35D4B54DFDF482F23 . 1766400 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16921_none_2378b1de5a09ae37\wininet.dll

[-] 2014-03-13 . DB0111AA31391A89B7C1ED5E56041A07 . 1772032 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20985_none_0cb0b1de73ac0c7a\wininet.dll

[-] 2014-03-13 . E3CDE294DB1DBD63C4CBA9C36B196208 . 1766400 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16866_none_2387110a59fe77c7\wininet.dll

[-] 2014-02-23 . 42DCEC69983C141BE35B9E097D843F32 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20964_none_0caec81273adc02b\wininet.dll

[-] 2014-02-23 . 9284BA6C27D360D71A5C0ECC8456E78E . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16844_none_23853e065a0011d7\wininet.dll

[-] 2014-02-01 . C491205AF386F5BD4A91BBD9F67F2B06 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20916_none_0ca9991073b274ba\wininet.dll

[-] 2014-02-01 . 1FF83D2BE92B40DAE234CF4236680B6E . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16798_none_2394b44459f3db1d\wininet.dll

[-] 2013-10-25 . 3AA6FD9B534F17CBD5D311DDC077973C . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16750_none_2391695c59f6a8b9\wininet.dll

[-] 2013-10-25 . 46E150A0356D73F99A9F9EC2A9D279F4 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20861_none_0cb9dc5673a55757\wininet.dll

[-] 2013-10-12 . 5FD4335DCD343D0FEA9FA6B18ED408D9 . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16736_none_238ee01859f90fd1\wininet.dll

[-] 2013-10-12 . 06715E12E72EFBC2D660A779FFF32944 . 1777152 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20848_none_0cb73c4a73a7d810\wininet.dll

[-] 2013-09-22 . 67220EB57550F10E1219D57D89937456 . 1777152 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20831_none_0cb6db7873a80b52\wininet.dll

[-] 2013-09-22 . E4FEB264B47360B7296AEA4E052F88D8 . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16721_none_238e51b659f97655\wininet.dll

[-] 2013-08-10 . 26BD13BB9196C2D8F8155C3C6169BC22 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20794_none_0cc768c8739ad44e\wininet.dll

[-] 2013-08-10 . 535F6263035F2530A62D5D64EF6E73D3 . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16686_none_239eb17659ec7293\wininet.dll

[-] 2013-07-26 . DAA3903F06116AE9EE7AC1D1B93684A4 . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16660_none_239d399259eda61f\wininet.dll

[-] 2013-07-26 . DE581A5E0E70BB63898F8776EB274428 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20768_none_0cc40cca739deecd\wininet.dll

[-] 2013-06-12 . 24AE444B165D11835EF3D38CF3CC7FA4 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20742_none_0cc294e6739f2259\wininet.dll

[-] 2013-06-11 . 9BF7C7654EFD098EE3A27B49492A382A . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16635_none_2399c6cc59f0da3f\wininet.dll

[-] 2013-05-17 . 425A20F1C6855222944BFD4FA9BE61A5 . 1777664 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20719_none_0cbef49073a289bb\wininet.dll

[-] 2013-05-17 . 2473CA6595A2659D7039A4A89FECA269 . 1767936 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16614_none_2397dd0059f28df0\wininet.dll

[-] 2013-04-05 . 5ABB3F36AF17007F33FA275E96A2C95E . 1767424 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16576_none_23a8811859e53d4b\wininet.dll

[-] 2013-04-05 . 1D48B7F4618EE77430ACECCA1BCA88E1 . 1775616 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20681_none_0cd17cc273935223\wininet.dll

[-] 2013-03-22 . BA15504FA59A8DC304F1CBAEBA6252A1 . 1766912 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16521_none_23a3f18e59e93e73\wininet.dll

[-] 2013-02-28 . 84DFC6513C2472230E2940B7B12FB21D . 982016 . . [8.00.7601.22258] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22258_none_1f0ce4839051bd5d\wininet.dll

[-] 2013-02-28 . 989937C1C1333EE55CC2982340CB1DBA . 981504 . . [8.00.7601.18094] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.18094_none_1e5404fa77582ad4\wininet.dll

[-] 2013-02-24 . B9A72493B83C77E78FE6213F4B01DB5D . 1775616 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.20644_none_0ccd3742739739aa\wininet.dll

[-] 2013-02-21 . CFE0CEE587F9CEA4C29DEEC6D85FC91C . 1766912 . . [10.00.9200.16521] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_10.2.9200.16540_none_23a608ea59e75780\wininet.dll

[-] 2012-12-20 . ED5F1E888F7D75EE5C8590A155423720 . 982016 . . [8.00.7601.22199] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22199_none_1ee2a33790714951\wininet.dll

[-] 2012-12-20 . 6554DA6A01F14B3F017161879C8DB9BC . 981504 . . [8.00.7601.18035] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.18035_none_1e95e4cc77269c85\wininet.dll

[-] 2012-10-27 . 42C671E0525618E23371D0E68282F37C . 981504 . . [8.00.7601.17984] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17984_none_1e5efcc4774fdb1\wininet.dll

[-] 2012-10-27 . 5CD2659F5F1728C7A71D4A15AA4A7D53 . 982016 . . [8.00.7601.22145] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22145_none_1f14b1ab904c5840\wininet.dll

[-] 2012-08-24 . 0D5ADA91A4176674D12DC990DD022E84 . 982016 . . [8.00.7601.22099] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22099_none_1ee2a15190714c2a\wininet.dll

[-] 2012-08-24 . 4F4E2103C7F8A2AB6679071855549C93 . 981504 . . [8.00.7601.17940] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17940_none_1e863b4c77330681\wininet.dll

[-] 2012-06-27 . 58CFAE82CC4092C5988555B73CD557B8 . 981504 . . [8.00.7601.17874] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17874_none_1e69caca7747c289\wininet.dll

[-] 2012-06-27 . 54D506A1F7D9E1AF6439F7A06CC6488A . 982016 . . [8.00.7601.22032] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.22032_none_1f1c7ed39046f323\wininet.dll

[-] 2012-05-15 . 2606B35DDADCA19BEA9A08033C621B97 . 981504 . . [8.00.7601.17842] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17842_none_1e8839fa77313c08\wininet.dll

[-] 2012-05-15 . 3E5195AB78F4DCE48E04CC6979D9B428 . 982016 . . [8.00.7601.21995] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21995_none_1edec8079074b38c\wininet.dll

[-] 2012-02-28 . 7CCA8574A3B9BB41A4150739E21F1B23 . 981504 . . [8.00.7601.17785] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17785_none_1e5ff942774efaaa\wininet.dll

[-] 2012-02-28 . 6A5778483A8023B4DB9C5A509D382392 . 982016 . . [8.00.7601.21931] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21931_none_1f1ba6679047a68a\wininet.dll

[-] 2011-12-16 . 808C0CE9D4DBC0A6F72761294EB10FB2 . 982016 . . [8.00.7601.21878] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21878_none_1ef766d79061ca88\wininet.dll

[-] 2011-12-16 . BDB7450CC556F238FD973C9DA300FEB8 . 981504 . . [8.00.7601.17744] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17744_none_1e8a38a8772f718f\wininet.dll

[-] 2011-11-05 . 19714FA7D7204D9BEE1EE12791DA9010 . 981504 . . [8.00.7601.17720] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17720_none_1e9bd7587722d451\wininet.dll

[-] 2011-11-05 . 1903228FE0C7D402B26A217F8D7713FD . 982016 . . [8.00.7601.21855] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21855_none_1f0a05d1905446a1\wininet.dll

[-] 2011-08-20 . 7570FA3FC82E08FB637E32D2D95DB41D . 981504 . . [8.00.7601.21795] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21795_none_1edec43b9074b93e\wininet.dll

[-] 2011-08-20 . DBF24E87CB605A4F6E7424DD86F7A62C . 981504 . . [8.00.7601.17671] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17671_none_1e66c620774a7c36\wininet.dll

[-] 2011-06-21 . D1E7C4FA045B34C32D12BFBB415EBE1B . 981504 . . [8.00.7601.21754] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.21754_none_1f0903a190553023\wininet.dll

[-] 2011-06-21 . 748FD4CAB1AFFD90A9556EB7D5AA1FEB . 981504 . . [8.00.7601.17638] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17638_none_1e9907d67723bdd3\wininet.dll

[-] 2010-11-21 . 44214C94911C7CFB1D52CB64D5E8368D . 980992 . . [8.00.7601.17514] ..
c:\windows\winsxs\x86_microsoft-windows-
i..tocolimplementation_31bf3856ad364e35_8.0.7601.17514_none_1eaaa4a07717236e\wininet.dll

.

[-] 2010-11-21 . 7FF15A4F092CD4A96055BA69F903E3E9 . 206848 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\ws2_32.dll

[-] 2010-11-21 . 7FF15A4F092CD4A96055BA69F903E3E9 . 206848 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-w..nfrastructure-
ws232_31bf3856ad364e35_6.1.7601.17514_none_f4bf1aae2c981ecf\ws2_32.dll

.

[-] 2009-07-14 . 808AABDF9337312195CAFF76D1804786 . 4608 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\ws2help.dll

[-] 2009-07-14 . 808AABDF9337312195CAFF76D1804786 . 4608 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-w..nfrastructure-
other_31bf3856ad364e35_6.1.7600.16385_none_6ace9e67456cc40b\ws2help.dll

.

[-] 2011-02-26 . 3B69712041F3D63605529BD66DC00C48 . 2871808 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
explorer_31bf3856ad364e35_6.1.7601.21669_none_b0333b22a99da332\explorer.exe

[-] 2011-02-25 . 332FEAB1435662FC6C672E25BEB37BE3 . 2871808 . . [6.1.7600.16385] ..
c:\windows\explorer.exe

[-] 2011-02-25 . 332FEAB1435662FC6C672E25BEB37BE3 . 2871808 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
explorer_31bf3856ad364e35_6.1.7601.17567_none_afa79dc39081d0ba\explorer.exe

[-] 2010-11-21 . AC4C51EB24AA95B77F705AB159189E24 . 2872320 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-
explorer_31bf3856ad364e35_6.1.7601.17514_none_afdaac81905bf900\explorer.exe

.

[-] 2009-07-14 . 2E2C937846A0B8789E5E91739284D17A . 427008 . . [6.1.7600.16385] ..
c:\windows\winsxs\amd64_microsoft-windows-registry-
editor_31bf3856ad364e35_6.1.7600.16385_none_5023a70bf589ad3e\regedit.exe

[-] 2009-07-14 . 2E2C937846A0B8789E5E91739284D17A . 398336 . . [6.1.7600.16385] ..
c:\windows\regedit.exe

.

[-] 2010-11-21 . 928CF7268086631F54C3D8E17238C6DD . 1414144 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\ole32.dll

[-] 2010-11-21 . 928CF7268086631F54C3D8E17238C6DD . 1414144 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-com-base-qfe-
ole32_31bf3856ad364e35_6.1.7601.17514_none_ae2511475093798f\ole32.dll
.
[-] 2014-04-25 . A5F833506BF6A1B5D693E1499DEE2444 . 626688 . . [1.0626.7601.18454] ..
c:\windows\SysWOW64\usp10.dll
[-] 2014-04-25 . A5F833506BF6A1B5D693E1499DEE2444 . 626688 . . [1.0626.7601.18454] ..
c:\windows\winsxs\x86_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.18454_none_aed68a9bb6df0577\usp10.dll
[-] 2014-04-25 . 5A7B3405C2AAE5369F6CB42FE248FBB0 . 626688 . . [1.0626.7601.22666] ..
c:\windows\winsxs\x86_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.22666_none_af5759f4d002f107\usp10.dll
[-] 2012-11-22 . CA68408922B02E8D955A2967C7CBF8CE . 626688 . . [1.0626.7601.22171] ..
c:\windows\winsxs\x86_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.22171_none_af477f18d00f9c82\usp10.dll
[-] 2012-11-22 . B7230010D97787AF3D25E4C82F2B06B9 . 626688 . . [1.0626.7601.18009] ..
c:\windows\winsxs\x86_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.18009_none_af119411b6b203d9\usp10.dll
[-] 2010-11-21 . 804AAAFEBB3AD5F49334DD906BCB1DE5 . 626176 . . [1.0626.7601.17514] ..
c:\windows\winsxs\x86_microsoft-windows-
usp_31bf3856ad364e35_6.1.7601.17514_none_af01e2f9b6be7939\usp10.dll
.
[-] 2009-07-14 . 9C67F6BBDA3881CFD02095160CF91576 . 4608 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\ksuser.dll
[-] 2009-07-14 . 9C67F6BBDA3881CFD02095160CF91576 . 4608 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-d..tshow-
kernel-support_31bf3856ad364e35_6.1.7601.17514_none_ea090647f58e5d9c\ksuser.dll
.
[-] 2009-07-14 . 4A3CDCEF8ED41B221F3DBEF5792FB52D . 8704 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\ctfmon.exe
[-] 2009-07-14 . 4A3CDCEF8ED41B221F3DBEF5792FB52D . 8704 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-t..cesframework-
ctfmon_31bf3856ad364e35_6.1.7600.16385_none_9d06e2f6f1e51f98\ctfmon.exe
.
[-] 2010-11-21 . 414DA952A35BF5D50192E28263B40577 . 328192 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\shsvcs.dll
[-] 2010-11-21 . 414DA952A35BF5D50192E28263B40577 . 328192 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
shsvcs_31bf3856ad364e35_6.1.7601.17514_none_35ab0ceb67ede31e\shsvcs.dll

.
[-] 2009-07-14 . 18AB2E5A40064ED5F7791AC5946A90F3 . 4608 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\msimg32.dll

[-] 2009-07-14 . 18AB2E5A40064ED5F7791AC5946A90F3 . 4608 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-gdi-
painting_31bf3856ad364e35_6.1.7600.16385_none_77422e3e7d5fa732\msimg32.dll

.
[-] 2009-07-14 . 50BA656134F78AF64E4DD3C8B6FEFD7E . 12288 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\cngaudit.dll

[-] 2009-07-14 . 50BA656134F78AF64E4DD3C8B6FEFD7E . 12288 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-cngaudit-
dll_31bf3856ad364e35_6.1.7600.16385_none_e83a414890e8132b\cngaudit.dll

.
[-] 2009-07-14 . B5C5DCAD3899512020D135600129D665 . 96256 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\wininit.exe

[-] 2009-07-14 . B5C5DCAD3899512020D135600129D665 . 96256 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
wininit_31bf3856ad364e35_6.1.7600.16385_none_30c90ef265a43c13\wininit.exe

.
[-] 2009-07-14 . A1E91B5B5273573FC132B683E550B5E6 . 19456 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\ias.dll

[-] 2009-07-14 . A1E91B5B5273573FC132B683E550B5E6 . 19456 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
n..ion_service_runtime_31bf3856ad364e35_6.1.7601.17514_none_fb08448fa0c85c23\ias.dll

.
[-] 2010-11-21 03:24 . AB9EB3745B03AE67AB241A82338DEA7B . 954288 .. [4.1.6140] ..
c:\windows\SysWOW64\mfc40u.dll

[-] 2010-11-21 03:24 . AB9EB3745B03AE67AB241A82338DEA7B . 954288 .. [4.1.6151] ..
c:\windows\winsxs\x86_microsoft-windows-
mfc40u_31bf3856ad364e35_6.1.7601.17514_none_f51a7bf0b3d25294\mfc40u.dll

.
[-] 2009-07-14 . 833FBB672460EFCE8011D262175FAD33 . 266752 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\upnpghost.dll

[-] 2009-07-14 . 833FBB672460EFCE8011D262175FAD33 . 266752 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
upnpdevicehost_31bf3856ad364e35_6.1.7600.16385_none_2831d06e8295c671\upnpghost.dll

.

[-] 2009-07-14 . 0E85C11F8850D524B02181C6E02BA9AE . 453632 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\dsound.dll

[-] 2009-07-14 . 0E85C11F8850D524B02181C6E02BA9AE . 453632 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-audio-
dsound_31bf3856ad364e35_6.1.7600.16385_none_5872147ba3367471\dsound.dll

.

[-] 2010-11-21 . 6EF5F3F18413C367195F06E503AB86A6 . 1828352 .. [6.1.7601.17514] ..
c:\windows\SysWOW64\d3d9.dll

[-] 2010-11-21 . 6EF5F3F18413C367195F06E503AB86A6 . 1828352 .. [6.1.7601.17514] ..
c:\windows\winsxs\x86_microsoft-windows-directx-
direct3d9_31bf3856ad364e35_6.1.7601.17514_none_c454d690bf084f04\d3d9.dll

.

[-] 2009-07-14 . 198552AEFECA69D646867EC8D792DE95 . 531968 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\ddraw.dll

[-] 2009-07-14 . 198552AEFECA69D646867EC8D792DE95 . 531968 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-directx-
directdraw_31bf3856ad364e35_6.1.7600.16385_none_04dbf9102154d42e\ddraw.dll

.

[-] 2010-11-21 03:24 . 703FFD301AB900B047337C5D40FD6F96 . 90112 .. [6.1.7601.17514] ..
c:\windows\SysWOW64\olepro32.dll

[-] 2010-11-21 03:24 . 703FFD301AB900B047337C5D40FD6F96 . 90112 .. [6.1.7601.17514] ..
c:\windows\winsxs\x86_microsoft-windows-ole-automation-
legacy_31bf3856ad364e35_6.1.7601.17514_none_3c1b247e5ff65f89\olepro32.dll

.

[-] 2009-07-14 . EDD2AD141DEBD425D74A52A4D7BE6AC4 . 39424 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\perfctr.dll

[-] 2009-07-14 . EDD2AD141DEBD425D74A52A4D7BE6AC4 . 39424 .. [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
performancebasecounters_31bf3856ad364e35_6.1.7600.16385_none_97bcd9bcab2b9b3a\perfctr.dll

.

[-] 2009-07-14 . 702254574E7E52052DE39408457B7149 . 21504 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\version.dll

[-] 2009-07-14 . 702254574E7E52052DE39408457B7149 . 21504 .. [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-
version_31bf3856ad364e35_6.1.7600.16385_none_14d4a552b2395165\version.dll

.

[-] 2009-07-14 . 5A12C364AD1D4FCC0AD0E56DBBC34462 . 16896 .. [6.1.7600.16385] ..
c:\windows\SysWOW64\midimap.dll

[-] 2009-07-14 . 5A12C364AD1D4FCC0AD0E56DBBC34462 . 16896 . . [6.1.7600.16385] ..
c:\windows\winsxs\x86_microsoft-windows-audio-mmecore-
other_31bf3856ad364e35_6.1.7600.16385_none_8cd41e2771e37717\midimap.dll

[-] 2009-07-14 . ED6EE83D61EBC683C2CD8E899EA6FEBE . 11776 . . [6.1.7600.16385] ..
c:\windows\SysWOW64\rasadhlp.dll

[-] 2009-07-14 . ED6EE83D61EBC683C2CD8E899EA6FEBE . 11776 . . [6.1.7600.16385] ..
c:\windows\winsxs\wow64_microsoft-windows-
rasautodial_31bf3856ad364e35_6.1.7600.16385_none_76239aafb364e805\rasadhlp.dll

[-] 2009-07-14 . EE5C8E27C37B79CB54A2FCEEED2DC262 . 9216 . . [6.1.7601.17514] ..
c:\windows\SysWOW64\WSH_TCPIP.DLL

[-] 2009-07-14 . EE5C8E27C37B79CB54A2FCEEED2DC262 . 9216 . . [6.1.7601.17514] ..
c:\windows\winsxs\x86_microsoft-windows-winssock-helper-
tcpip_31bf3856ad364e35_6.1.7600.16385_none_cb895be592db1acb\WSH_TCPIP.DLL

((Spouštěcí body v registru))))))))))))))))))))))))))))))))))))))

Poznámka prázdné záznamy a legitimní výchozí údaje nejsou zobrazeny.

REGEDIT4

[HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows\currentversion\explorer\shell
iconoverlayidentifiers\SkyDrivePro1 (ErrorConflict)]

@="{8BA85C75-763B-4103-94EB-9470F12FE0F7}"

[HKEY_CLASSES_ROOT\CLSID\{8BA85C75-763B-4103-94EB-9470F12FE0F7}]

2015-01-08 18:33 1729744 ----a-w- c:\program files\Microsoft Office
15\root\office15\GROOVEEX.DLL

[HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows\currentversion\explorer\shell
iconoverlayidentifiers\SkyDrivePro2 (SyncInProgress)]

@="{CD55129A-B1A1-438E-A425-CEBC7DC684EE}"

[HKEY_CLASSES_ROOT\CLSID\{CD55129A-B1A1-438E-A425-CEBC7DC684EE}]

2015-01-08 18:33 1729744 ----a-w- c:\program files\Microsoft Office
15\root\office15\GROOVEEX.DLL

.
[HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows\currentversion\explorer\shell
iconoverlayidentifiers\SkyDrivePro3 (InSync)]

@="{E768CD3B-BDDC-436D-9C13-E1B39CA257B1}"

[HKEY_CLASSES_ROOT\CLSID\{E768CD3B-BDDC-436D-9C13-E1B39CA257B1}]

2015-01-08 18:33 1729744 ----a-w- c:\program files\Microsoft Office
15\root\office15\GROOVEEX.DLL

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run]

"AvastUI.exe"="c:\program files\AVAST Software\Avast\AvastUI.exe" [2015-01-17 5227112]

"PMBVolumeWatcher"="c:\program files (x86)\Sony\PMB\PMBVolumeWatcher.exe" [2010-11-26
648032]

"QuickTime Task"="c:\program files (x86)\QuickTime Alternative\QTTask.exe" [2014-10-02 421888]

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\policies\system]

"ConsentPromptBehaviorAdmin"= 5 (0x5)

"ConsentPromptBehaviorUser"= 3 (0x3)

"EnableUIADesktopToggle"= 0 (0x0)

"PromptOnSecureDesktop"= 0 (0x0)

"SoftwareSASGeneration"= 1 (0x1)

[HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows nt\currentversion\windows]

"LoadAppInit_DLLs"=1 (0x1)

[HKEY_LOCAL_MACHINE\system\currentcontrolset\control\session manager]

BootExecute REG_MULTI_SZ autocheck autochk *\Osdnclean64.exe

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\MCODS]

@=""

[HKEY_LOCAL_MACHINE\software\wow6432node\microsoft\windows\currentversion\run-]

"AVG_UI"="c:\program files (x86)\AVG\AVG2015\avgui.exe" /TRAYONLY

"IAStorIcon"=c:\program files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe

.

R2 clr_optimization_v4.0.30319_64;Microsoft .NET Framework NGEN
v4.0.30319_X64;c:\windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe;c:\windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe [x]

R2 MBAMService;MBAMService;c:\program files (x86)\Malwarebytes Anti-Malware\mbamservice.exe;c:\program files (x86)\Malwarebytes Anti-Malware\mbamservice.exe [x]

R2 sp_rsdv2;Spyware Terminator Driver
Filter;c:\windows\system32\DRIVERS\stflt.sys;c:\windows\SYSNATIVE\DRIVERS\stflt.sys [x]

R3 androidusb;SAMSUNG Android Composite ADB Interface
Driver;c:\windows\system32\Drivers\ssadadb.sys;c:\windows\SYSNATIVE\Drivers\ssadadb.sys [x]

R3 AthBTPort;Atheros Virtual Bluetooth
Class;c:\windows\system32\DRIVERS\btathflt.sys;c:\windows\SYSNATIVE\DRIVERS\btathflt.sys [x]

R3 ATHDFU;Atheros Valkyrie USB
BootROM;c:\windows\System32\Drivers\AthDfu.sys;c:\windows\SYSNATIVE\Drivers\AthDfu.sys [x]

R3 BTATH_A2DP;Bluetooth A2DP Audio
Driver;c:\windows\system32\drivers\btath_a2dp.sys;c:\windows\SYSNATIVE\drivers\btath_a2dp.sys [x]

R3 btath_avdt;Atheros Bluetooth AVDT
Service;c:\windows\system32\drivers\btath_avdt.sys;c:\windows\SYSNATIVE\drivers\btath_avdt.sys [x]

R3 BTATH_HCRP;Bluetooth HCRP Server
driver;c:\windows\system32\drivers\btath_hcrp.sys;c:\windows\SYSNATIVE\drivers\btath_hcrp.sys [x]

R3 BTATH_LWFLT;Bluetooth LWFLT
Device;c:\windows\system32\DRIVERS\btath_lwflt.sys;c:\windows\SYSNATIVE\DRIVERS\btath_lwflt.sys [x]

R3 BTATH_RCP;Bluetooth AVRCP
Device;c:\windows\system32\drivers\btath_rcp.sys;c:\windows\SYSNATIVE\drivers\btath_rcp.sys [x]

R3
BtFilter;BtFilter;c:\windows\system32\DRIVERS\btfilter.sys;c:\windows\SYSNATIVE\DRIVERS\btfilter.sys [x]

R3 BthMtpEnum;Modul pro výčet zařízení Bluetooth
MTP;c:\windows\system32\DRIVERS\BthMtpEnum.sys;c:\windows\SYSNATIVE\DRIVERS\BthMtpEnum.sys [x]

R3 CXFALCON;Conexant Falcon II NTSC Video
Capture;c:\windows\system32\drivers\cxfalcon_IBV64.sys;c:\windows\SYSNATIVE\drivers\cxfalcon_IBV64.sys [x]

R3 DCDhcpService;DCDhcpService;c:\program files\Sony\VAIO Smart Network\WFDA\DCDhcpService.exe;c:\program files\Sony\VAIO Smart Network\WFDA\DCDhcpService.exe [x]

R3 dgderdrv;dgderdrv;c:\windows\system32\drivers\dgderdrv.sys;c:\windows\SYSNATIVE\drivers\dgderdrv.sys [x]

R3 e1yexpress;Intel(R) Gigabit Network Connections Driver;c:\windows\system32\DRIVERS\e1y60x64.sys;c:\windows\SYSNATIVE\DRIVERS\e1y60x64.sys [x]

R3 EsgScanner;EsgScanner;c:\windows\system32\DRIVERS\EsgScanner.sys;c:\windows\SYSNATIVE\DRIVERS\EsgScanner.sys [x]

R3 ggflt;SEMC USB Flash Driver Filter;c:\windows\system32\DRIVERS\ggflt.sys;c:\windows\SYSNATIVE\DRIVERS\ggflt.sys [x]

R3 IntcDAud;Intel(R) Display Audio;c:\windows\system32\DRIVERS\IntcDAud.sys;c:\windows\SYSNATIVE\DRIVERS\IntcDAud.sys [x]

R3 MBAMWebAccessControl;MBAMWebAccessControl;c:\windows\system32\drivers\mwac.sys;c:\windows\SYSNATIVE\drivers\mwac.sys [x]

R3 nmwcdnsucx64;Nokia USB Flashing Generic;c:\windows\system32\drivers\nmwcdnsucx64.sys;c:\windows\SYSNATIVE\drivers\nmwcdnsucx64.sys [x]

R3 nmwcdnsux64;Nokia USB Flashing Phone Parent;c:\windows\system32\drivers\nmwcdnsux64.sys;c:\windows\SYSNATIVE\drivers\nmwcdnsux64.sys [x]

R3 RdpVideoMiniport;Remote Desktop Video Miniport Driver;c:\windows\system32\drivers\rdpvideominiport.sys;c:\windows\SYSNATIVE\drivers\rdpvideominiport.sys [x]

R3 SOHClmp;VAIO Content Importer;c:\program files (x86)\Common Files\Sony Shared\SOHLib\SOHClmp.exe;c:\program files (x86)\Common Files\Sony Shared\SOHLib\SOHClmp.exe [x]

R3 SOHDs;VAIO Device Searcher;c:\program files (x86)\Common Files\Sony Shared\SOHLib\SOHDs.exe;c:\program files (x86)\Common Files\Sony Shared\SOHLib\SOHDs.exe [x]

R3 Sony PC Companion;Sony PC Companion;c:\program files (x86)\Sony\Sony PC Companion\PCCService.exe;c:\program files (x86)\Sony\Sony PC Companion\PCCService.exe [x]

R3 SpfService;VAIO Entertainment Common Service;c:\program files\Common Files\Sony Shared\VAIO Entertainment Platform\SPF\SpfService64.exe;c:\program files\Common Files\Sony Shared\VAIO Entertainment Platform\SPF\SpfService64.exe [x]

R3 ssadbus;SAMSUNG Android USB Composite Device driver
(WDM);c:\windows\system32\DRIVERS\ssadbus.sys;c:\windows\SYSNATIVE\DRIVERS\ssadbus.sys [x]

R3 ssadmdfl;SAMSUNG Android USB Modem
(Filter);c:\windows\system32\DRIVERS\ssadmdfl.sys;c:\windows\SYSNATIVE\DRIVERS\ssadmdfl.sys
[x]

R3 ssadmmdm;SAMSUNG Android USB Modem
Drivers;c:\windows\system32\DRIVERS\ssadmmdm.sys;c:\windows\SYSNATIVE\DRIVERS\ssadmmdm.sys
[x]

R3 ssadserd;SAMSUNG Android USB Diagnostic Serial Port
(WDM);c:\windows\system32\DRIVERS\ssadserd.sys;c:\windows\SYSNATIVE\DRIVERS\ssadserd.sys
[x]

R3
TsUsbFlt;TsUsbFlt;c:\windows\system32\drivers\tsusbflt.sys;c:\windows\SYSNATIVE\drivers\tsusbflt.
sys [x]

R3 TsUsbGD;Remote Desktop Generic USB
Device;c:\windows\system32\drivers\TsUsbGD.sys;c:\windows\SYSNATIVE\drivers\TsUsbGD.sys [x]

R3 VBoxNetAdp;VirtualBox Host-Only Ethernet
Adapter;c:\windows\system32\DRIVERS\VBoxNetAdp.sys;c:\windows\SYSNATIVE\DRIVERS\VBoxNet
Adp.sys [x]

R3 VBoxNetFlt;VirtualBox Bridged Networking
Service;c:\windows\system32\DRIVERS\VBoxNetFlt.sys;c:\windows\SYSNATIVE\DRIVERS\VBoxNetFlt
.sys [x]

R3 VCFw;VAIO Content Folder Watcher;c:\program files (x86)\Common Files\Sony Shared\VAIO
Content Folder Watcher\VCFw.exe;c:\program files (x86)\Common Files\Sony Shared\VAIO Content
Folder Watcher\VCFw.exe [x]

R3 VcmIAIzMgr;VAIO Content Metadata Intelligent Analyzing Manager;c:\program files\Sony\VCM
Intelligent Analyzing Manager\VcmIAIzMgr.exe;c:\program files\Sony\VCM Intelligent Analyzing
Manager\VcmIAIzMgr.exe [x]

R3 VcmINSMgr;VAIO Content Metadata Intelligent Network Service Manager;c:\program
files\Sony\VCM Intelligent Network Service Manager\VcmINSMgr.exe;c:\program files\Sony\VCM
Intelligent Network Service Manager\VcmINSMgr.exe [x]

R3 VcmXmlIfHelper;VAIO Content Metadata XML Interface;c:\program files\Common Files\Sony
Shared\VcmXml\VcmXmlIfHelper64.exe;c:\program files\Common Files\Sony
Shared\VcmXml\VcmXmlIfHelper64.exe [x]

R3 WatAdminSvc;Služba Technologie aktivace
Windows;c:\windows\system32\Wat\WatAdminSvc.exe;c:\windows\SYSNATIVE\Wat\WatAdminSvc.
exe [x]

R3 WDC_SAM;WD SCSI Pass Thru
driver;c:\windows\system32\DRIVERS\wdcsam64.sys;c:\windows\SYSNATIVE\DRIVERS\wdcsam64.sy
s [x]

R4 wlcraSvc;Windows Live Mesh remote connections service;c:\program files\Windows Live\Mesh\wlcraSvc.exe;c:\program files\Windows Live\Mesh\wlcraSvc.exe [x]

S0 aswRvrt;avast! Revert; [x]

S0 aswVmm;avast! VM Monitor; [x]

S1 aswKbd;aswKbd; [x]

S1

aswSnx;aswSnx;c:\windows\system32\drivers\aswSnx.sys;c:\windows\SYSTEM32\drivers\aswSnx.sys [x]

S1 aswSP;aswSP;c:\windows\system32\drivers\aswSP.sys;c:\windows\SYSTEM32\drivers\aswSP.sys [x]

S2 aswHwid;avast!

HardwareID;c:\windows\system32\drivers\aswHwid.sys;c:\windows\SYSTEM32\drivers\aswHwid.sys [x]

S2

aswMonFilt;aswMonFilt;c:\windows\system32\drivers\aswMonFilt.sys;c:\windows\SYSTEM32\drivers\aswMonFilt.sys [x]

S2

aswStm;aswStm;c:\windows\system32\drivers\aswStm.sys;c:\windows\SYSTEM32\drivers\aswStm.sys [x]

S2 Atheros Bt&Wlan Coex Agent;Atheros Bt&Wlan Coex Agent;c:\program files (x86)\Bluetooth Suite\Ath_CoexAgent.exe;c:\program files (x86)\Bluetooth Suite\Ath_CoexAgent.exe [x]

S2 AtherosSvc;AtherosSvc;c:\program files (x86)\Bluetooth Suite\adminservice.exe;c:\program files (x86)\Bluetooth Suite\adminservice.exe [x]

S2 ClickToRunSvc;Služba Microsoft Office ClickToRun;c:\program files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe;c:\program files\Microsoft Office 15\ClientX64\OfficeClickToRun.exe [x]

S2 IAStorDataMgrSvc;Intel(R) Rapid Storage Technology;c:\program files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe;c:\program files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorDataMgrSvc.exe [x]

S2 IconMan_R;IconMan_R;c:\program files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe;c:\program files (x86)\Realtek\Realtek PCIE Card Reader\RIconMan.exe [x]

S2 PMBDeviceInfoProvider;PMBDeviceInfoProvider;c:\program files (x86)\Sony\PMB\PMBDeviceInfoProvider.exe;c:\program files (x86)\Sony\PMB\PMBDeviceInfoProvider.exe [x]

S2 SampleCollector;Intel(R) System Behavior Tracker Collector Service;c:\program files\Sony\VAIO Care\VCPerfService.exe;c:\program files\Sony\VAIO Care\VCPerfService.exe [x]

S2 uCamMonitor;CamMonitor;c:\program files (x86)\ArcSoft\Magic-i Visual Effects 2\uCamMonitor.exe;c:\program files (x86)\ArcSoft\Magic-i Visual Effects 2\uCamMonitor.exe [x]

S2 UNS;Intel(R) Management and Security Application User Notification Service;c:\program files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe;c:\program files (x86)\Intel\Intel(R) Management Engine Components\UNS\UNS.exe [x]

S2 VBoxAswDrv;VBoxAsw Support Driver;c:\program files\AVAST Software\Avast\ng\vbox\VBoxAswDrv.sys;c:\program files\AVAST Software\Avast\ng\vbox\VBoxAswDrv.sys [x]

S2 VSNService;VSNService;c:\program files\Sony\VAIO Smart Network\VSNService.exe;c:\program files\Sony\VAIO Smart Network\VSNService.exe [x]

S2 WDDMService;WDDMService;c:\program files\Western Digital\WD SmartWare\WD Drive Manager\WDDMService.exe;c:\program files\Western Digital\WD SmartWare\WD Drive Manager\WDDMService.exe [x]

S2 WDFME;WD File Management Engine;c:\program files (x86)\Western Digital\WD Smartware\Front Parlor\WDFME\WDFME.exe;c:\program files (x86)\Western Digital\WD Smartware\Front Parlor\WDFME\WDFME.exe [x]

S2 WDSC;WD File Management Shadow Engine;c:\program files (x86)\Western Digital\WD Smartware\Front Parlor\WDSC.exe;c:\program files (x86)\Western Digital\WD Smartware\Front Parlor\WDSC.exe [x]

S3 ArcSoftKsUFilter;ArcSoft Magic-I Visual Effect;c:\windows\system32\DRIVERS\ArcSoftKsUFilter.sys;c:\windows\SYSNATIVE\DRIVERS\ArcSoftKsUFilter.sys [x]

S3 BTATH_BUS;Atheros Bluetooth Bus;c:\windows\system32\drivers\bath_bus.sys;c:\windows\SYSNATIVE\drivers\bath_bus.sys [x]

S3 MBAMProtector;MBAMProtector;c:\windows\system32\drivers\mbam.sys;c:\windows\SYSNATIVE\drivers\mbam.sys [x]

S3 RSPCIESTOR;Realtek PCIE CardReader Driver;c:\windows\system32\DRIVERS\RtsPStor.sys;c:\windows\SYSNATIVE\DRIVERS\RtsPStor.sys [x]

S3 RTL8167;Realtek 8167 NT Driver;c:\windows\system32\DRIVERS\Rt64win7.sys;c:\windows\SYSNATIVE\DRIVERS\Rt64win7.sys [x]

S3 seehcri;Sony Ericsson seehcri Device Driver;c:\windows\system32\DRIVERS\seehcri.sys;c:\windows\SYSNATIVE\DRIVERS\seehcri.sys [x]

S3 SFEP;Sony Firmware Extension Parser;c:\windows\system32\drivers\SFEP.sys;c:\windows\SYSNATIVE\drivers\SFEP.sys [x]

S3 VCSERVICE;VCSERVICE;c:\program files\Sony\VAIO Care\VCSERVICE.exe;c:\program files\Sony\VAIO Care\VCSERVICE.exe [x]

S3 VUAGENT;VUAGENT;c:\program files\Sony\VAIO Update\vuagent.exe;c:\program files\Sony\VAIO Update\vuagent.exe [x]

.

.
--- Ostatní služby/ovladače v paměti ---

.
NewlyCreated - WS2IFSL

.
Obsah adresáře 'Naplánované úlohy'

.
2015-01-28 c:\windows\Tasks\Adobe Flash Player Updater.job

- c:\windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe [2012-03-31 20:53]

.
2015-01-28 c:\windows\Tasks\GoogleUpdateTaskMachineCore.job

- c:\program files (x86)\Google\Update\GoogleUpdate.exe [2011-10-30 18:35]

.
2015-01-28 c:\windows\Tasks\GoogleUpdateTaskMachineUA.job

- c:\program files (x86)\Google\Update\GoogleUpdate.exe [2011-10-30 18:35]

.
2015-01-26 c:\windows\Tasks\GoogleUpdateTaskUserS-1-5-21-2813025690-747382938-2618862338-1000Core.job

- c:\users\admin\AppData\Local\Google\Update\GoogleUpdate.exe [2012-03-22 06:21]

.
2015-01-28 c:\windows\Tasks\GoogleUpdateTaskUserS-1-5-21-2813025690-747382938-2618862338-1000UA.job

- c:\users\admin\AppData\Local\Google\Update\GoogleUpdate.exe [2012-03-22 06:21]

.
----- X64 Entries -----

.
[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\shelliconoverlayidentifiers\SkyDrivePro1 (ErrorConflict)]

@="{8BA85C75-763B-4103-94EB-9470F12FE0F7}"

[HKEY_CLASSES_ROOT\CLSID\{8BA85C75-763B-4103-94EB-9470F12FE0F7}]

2015-01-08 18:33 2334928 ----a-w- c:\program files\Microsoft Office
15\root\vfs\ProgramFilesX64\Microsoft Office\Office15\GROOVEEX.DLL

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\shelliconoverlayiden
tifiers\SkyDrivePro2 (SyncInProgress)]

@="{CD55129A-B1A1-438E-A425-CEBC7DC684EE}"

[HKEY_CLASSES_ROOT\CLSID\{CD55129A-B1A1-438E-A425-CEBC7DC684EE}]

2015-01-08 18:33 2334928 ----a-w- c:\program files\Microsoft Office
15\root\vfs\ProgramFilesX64\Microsoft Office\Office15\GROOVEEX.DLL

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\shelliconoverlayiden
tifiers\SkyDrivePro3 (InSync)]

@="{E768CD3B-BDDC-436D-9C13-E1B39CA257B1}"

[HKEY_CLASSES_ROOT\CLSID\{E768CD3B-BDDC-436D-9C13-E1B39CA257B1}]

2015-01-08 18:33 2334928 ----a-w- c:\program files\Microsoft Office
15\root\vfs\ProgramFilesX64\Microsoft Office\Office15\GROOVEEX.DLL

.

[HKEY_LOCAL_MACHINE\software\microsoft\windows\currentversion\explorer\shelliconoverlayiden
tifiers\00avast]

@="{472083B0-C522-11CF-8763-00608CC02F24}"

[HKEY_CLASSES_ROOT\CLSID\{472083B0-C522-11CF-8763-00608CC02F24}]

2015-01-17 17:16 860984 ----a-w- c:\program files\AVAST Software\Avast\ashShA64.dll

.

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

"IgfxTray"="c:\windows\system32\igfxtray.exe" [2011-03-29 167960]

"HotKeysCmds"="c:\windows\system32\hkcmd.exe" [2011-03-29 391704]

"Persistence"="c:\windows\system32\igfxpers.exe" [2011-03-29 418328]

"RtHDVCpl"="c:\program files\Realtek\Audio\HDA\RAVCpl64.exe" [2010-07-28 11101800]

"Skytel"="c:\program files\Realtek\Audio\HDA\Skytel.exe" [2010-07-28 1833576]

.

----- Doplnkový sken -----

.

uLocal Page = c:\windows\system32\blank.htm

mStart Page = about:blank

mSearch Bar = https://www.seznam.cz/?clid=22668

mDefault_Page_URL = about:blank

IE: Add to Google Photos Screensaver - c:\windows\system32\GPhotos.scr/200

IE: Export to Microsoft Excel - c:\program files\Microsoft Office 15\Root\Office15\EXCEL.EXE/3000

IE: Send to OneNote - c:\program files\Microsoft Office 15\Root\Office15\ONBttmIE.dll/105

IE: ?????? - c:\users\admin\AppData\Roaming\FlashGetBHO\GetUrl.htm

IE: ????????? - c:\users\admin\AppData\Roaming\FlashGetBHO\GetAllUrl.htm

TCP: DhcpNameServer = 192.168.1.1

FF - ProfilePath - c:\users\admin\AppData\Roaming\Mozilla\Firefox\Profiles\l6j7buw1.default-1388608884847\

FF - prefs.js: browser.search.selectedEngine - Seznam

.

--- NEPLATNÉ POLOŽKY ODSTRANĚNÉ Z REGISTRU ---

.

Toolbar-10 - (no file)

Notify-SDWinLogon - SDWinLogon.dll

Toolbar-10 - (no file)

AddRemove-Encyklopedie vesmíru - c:\windows\IsUn0405.exe

AddRemove-Jak věci pracují 2.0 - c:\windows\IsUn0405.exe

.

.

.

[HKEY_LOCAL_MACHINE\system\ControlSet001\services\SampleCollector]

"ImagePath"="c:\program files\Sony\VAIO Care\VCPerfService.exe\" \" /service\" \" /sstates\"
\" /sampleinterval=10000\" \" /procinterval=5\" \" /dllinterval=120\" \" /counter=\Processor(_Total)\%
Processor Time:1\" \" /counter=\PhysicalDisk(_Total)\Disk Bytes/sec:1\" \" /counter=\Network
Interface(*)\Bytes Total/sec:1\" \" /expandcounter=\Processor Information(*)\Processor
Frequency:1\" \" \" /expandcounter=\Processor(*)\% Idle Time:1\"
\" /expandcounter=\Processor(*)\% C1 Time:1\" \" /expandcounter=\Processor(*)\% C2 Time:1\"
\" /expandcounter=\Processor(*)\% C3 Time:1\" \" /expandcounter=\Processor(*)\% Processor
Time:1\" \" /directory=c:\programdata\Sony Corporation\VAIO Care\inteldata\\"

.

----- ZAMKNUTÉ KLÍČE V REGISTRU -----

.
[HKEY_USERS\S-1-5-21-2813025690-747382938-2618862338-1000\Software\Microsoft\Internet Explorer\MenuExt\O(uě_fŽ3* N}Ž]

@="c:\\Users\\admin\\AppData\\Roaming\\FlashGetBHO\\GetUrl.htm"

"contexts"=dword:00000022

.
[HKEY_USERS\S-1-5-21-2813025690-747382938-2618862338-1000\Software\Microsoft\Internet Explorer\MenuExt\O(uě_fŽ3* N}ŽhQčt"Ac]

@="c:\\Users\\admin\\AppData\\Roaming\\FlashGetBHO\\GetAllUrl.htm"

"contexts"=dword:000000f3

.
[HKEY_LOCAL_MACHINE\software\McAfee]

"SymbolicLinkValue"=hex(6):5c,00,72,00,65,00,67,00,69,00,73,00,74,00,72,00,79,
00,5c,00,6d,00,61,00,63,00,68,00,69,00,6e,00,65,00,5c,00,53,00,6f,00,66,00,\

.
----- Jiné spuštěné procesy -----

.
c:\program files\AVAST Software\Avast\AvastSvc.exe

c:\program files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

c:\program files (x86)\Malwarebytes Anti-Malware\mbamscheduler.exe

c:\program files (x86)\Sony\VAIO Event Service\VESMgr.exe

c:\program files (x86)\Sony\VAIO Event Service\VESMgrSub.exe

c:\program files (x86)\Sony\VAIO Event Service\VESMgrSub.exe

c:\windows\SysWOW64\DllHost.exe

c:\windows\SysWOW64\DllHost.exe

c:\program files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe

c:\program files\Sony\VAIO Care\listener.exe

.

Celkový čas: 2015-01-28 14:27:39 - počítač byl restartován

ComboFix-quarantined-files.txt 2015-01-28 13:27

.

Před spuštěním: Volných bajtů: 231 393 329 152

Po spuštění: Volných bajtů: 231 594 160 128

.

-- End Of File -- 92B52B87BACF9E28B225258AE19792C9