VALKYRIE

PUA
Valkyrie Final Verdict

File Name: MediaInfo_GUI_0.7.77_Windows.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 669c9ab0f131a3dd8d8936abadb2cc2e3d1a4992
MD5: cf813172f4bbb2b5b49248df42dc2de7
First Seen Date: 2015-09-02 18:30:44 UTC
Number of Clients Seen: 4
Last Analysis Date: 2016-04-08 20:37:35 UTC
Human Expert Analysis Date: 2015-10-30 12:36:11 UTC
Human Expert Analysis Result: PUA
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-04-08 20:37:35 UTC	Malware	
Static Analysis Overall Verdict	2016-04-08 20:37:35 UTC	Highly Suspicious	
Dynamic Analysis Overall Verdict	2016-04-08 20:37:35 UTC	Highly Suspicious	
Human Expert Analysis Overall Verdict	2015-10-30 12:36:11 UTC	PUA	
File Certificate Validation		Certificate and Vendor name are Valid	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	
Non-ascii or empty section names detected	Clean	
Illegal size of optional Header	Clean	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
Based on the sections entropy check! file is possibly packed	Clean	
Timestamp value suspicious	Clean	
Header Checksum is zero!	Clean	
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean	
Packer detection on signature database	Unknown	
Anti-vm present	Clean	
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Suspicious	
TLS callback functions array detected	Clean	

Anti-debug calls

FindWindowExW

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Has no visible windows	

Behavioral Information

QueryFilePath

C:\sample
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Users\win7\AppData\Local\Temp\Opera Installer\sample
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\system32\Msftedit.dll
C:\DLL_Loader.exe
C:\Windows\system32\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\BASS.dll
C:\Users\win7\AppData\Local\Tem
C:\Users\win7\AppData\Local\Temp\is-A432R.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\bp.dll
C:\Windows\system32\RICHED20.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msiinst.exe
C:\Windows\system32\RichEd20.DLL
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Users\win7\AppData\Local\Temp\is-9HAUJ.tmp\sample.tmp
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\system32\jscript9.dll
C:\Users\win7\AppData\Local\Temp\is-1SBA6.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-MOFCS.tmp\sample.tmp
C:\Windows\system32\ODBC32.dll
C:\Windows\system32\dinput.dll
C:\Windows\system32\compstui.dll
C:\Windows\system32\EhStorShell.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\perl514.dll
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\system32\Riched20.dll
C:\Windows\system32\CRTDLL.DLL
C:\Users\win7\AppData\Local\Temp\is-V4OI1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-4CIEK.tmp\sample.tmp
C:\Windows\system32\dsound.dll
C:\Windows\syswow64\SHELL32.dll
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Users\win7\AppData\Local\Temp\is-5H3CT.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-M3KRK.tmp\sample.tmp
C:\Windows\system32\WINMM.dll
C:\Windows\system32\explorerframe.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\system32\quartz.dll
C:\Windows\system32\msftedit.DLL
C:\Windows\System32\msxml3.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\System32\msxml6.dll
C:\Windows\system32\MSVFW32.dll
C:\Windows\system32\WSOCK32.dll
C:\Windows\system32\version.DLL
C:\Windows\syswow64\GDI32.dll

C:\Windows\syswow64\comdlg32.dll
C:\Windows\system32\WINSPOOL.DRV
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\COMCTL32.dll
C:\Windows\system32\oledlg.dll
C:\Windows\syswow64\ole32.DLL
C:\Windows\system32\OLEPRO32.DLL
C:\Windows\syswow64\OLEAUT32.dll
C:\Windows\system32\NETAPI32.dll
C:\Windows\system32\propsys.dll
C:\Windows\system32\ntshrui.dll
C:\Users\win7\AppData\Local\Temp\is-159AI.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-B15KQ.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-UAJ2G.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\bassmusic.dll
C:\Users\win7\AppData\Local\Temp\is-TE17K.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-5BUKT.tmp\sample.tmp
C:\Windows\winhlp32.exe
C:\Users\win7\AppData\Local\Temp\is-QNTCR.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-LT5S1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-3P2CL.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\qag7A3.tmp
C:\Users\win7\AppData\Local\Temp\GUMAA9A.tmp\DropboxUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUMAA9A.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\is-6B3K6.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-UM2C5.tmp\sample.tmp
C:\Windows\system32\sxs.dll
C:\Windows\system32\mscoree.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.dll
C:\Users\win7\AppData\Local\Temp\is-ENFQS.tmp\sample.tmp
C:\Windows\system32\RICHED20.DLL
C:\Users\win7\AppData\Local\Temp\is-C47AV.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\botva2.dll
C:\Users\win7\AppData\Local\Temp\is-Q7LBC.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-PUVVS.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-6O4DC.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-IPPHG.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.exe
C:\Users\win7\AppData\Local\Temp\is-DKO1M.tmp\sample.tmp
C:\Windows\system32\msi.dll
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\CopyInstructionsW.exe
C:\Windows\system32\msvidc32.dll
C:\Windows\system32\iyuv_32.dll
C:\Windows\system32\iccvid.dll
C:\Windows\system32\TAPI32.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\OCSetupHlp.dll
C:\Windows\system32\DUser.dll
C:\Windows\SysWOW64\schannel.dll
C:\Users\win7\AppData\Local\Temp\is-UUOUB.tmp\sample.tmp
C:\Windows\system32\twext.dll
C:\Windows\system32\DINPUT8.dll
C:\Users\win7\AppData\Local\Temp\is-B9NAH.tmp\sample.tmp
C:\Windows\system32\DInput.dll
C:\Windows\system32\DSound.dll
C:\Windows\system32\DSOUND.dll
C:\WBDJA44I.DLL
C:\Users\win7\AppData\Local\Temp\is-EERGE.tmp\is-APQM2.tmp
C:\Windows\SysWOW64\cmd.exe
C:\Windows\temp\sqlserver.exe
C:\Windows\SysWOW64\net1.exe
C:\Windows\system32\riched20.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.dll
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\GvNPRT_Install.exe
C:\Users\win7\AppData\Local\Temp\RarSFX0\DXSETUP.exe
C:\Users\win7\AppData\Local\Temp\is-EPHGJ.tmp\sample.tmp
C:\Windows\system32\DSPROP.dll
C:\Users\win7\AppData\Local\Temp\~w0cvwt46y3.tmp
C:\Users\win7\AppData\Local\Temp\xagE6.tmp
C:\Users\win7\AppData\Local\Temp\is-3H39U.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\SQ3B11C.tmp
C:\Users\win7\AppData\Local\Temp\is-9AFAT.tmp\sample.tmp

ReadRegisteryKey

ProgramFilesDir
Disable
DataFilePath
Plane1
Plane2
Plane3
Plane4
Plane5
Plane6
Plane7
Plane8
Plane9
Plane10
Plane11
Plane12
Plane13
Plane14
Plane15
Plane16
ProcessID
EnablePrivateObjectHeap
ContextLimit
ObjectLimit
IdentifierLimit
Last Stable Install Path
Last install path
0000000000000409
MS Shell Dlg 2
CommonFilesDir
RegisteredOwner
RegisteredOrganization
WaitToKillServiceTimeout
DriverDesc
SystemBiosVersion
VideoBiosVersion
PendingFileRenameOperations
DropLocation
MachineGuid
ProductName
Anchor Color
Anchor Color Visited
FrameTabWindow
FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
CreateUriCacheSize
EnablePunycode
NavigationDelay
DebugLog
ShowNotifyIcon
ShowSnoozePopup
AdvertiseDone
AlreadyShowDiag
AllowAdvertise
ForTVT
InitialDelayToAppear
UsrColumnSettings
AllowMultipleTSSessions
InstallRoot
CLRLoadLogDir
OnlyUseLatestCLR
NoGuiFromShim
Common Desktop
Common Programs
Desktop
NoRun
NoDrives
RestrictRun
NoNetConnectDisconnect
NoRecentDocsHistory
NoClose

UseDoubleClickTimer
Segoe UI
System
AppData
SyncMode5
FEATURE_CLIENTAUTHCERTFILTER
FromCacheTimeout
SecureProtocols
DisableKeepAlive
IdnEnabled
PreConnectLimit
PreResolveLimit
SqmHttpStreamRandomUploadPoolSize
CacheMode
EnableHttp1_1
ProxyHttp1.1
EnableNegotiate
DisableBasicOverClearChannel
ClientAuthBuiltInUI
DisableReadRange
SocketSendBufferLength
SocketReceiveBufferLength
KeepAliveTimeout
MaxHttpRedirects
MaxConnectionsPerServer
MaxConnectionsPer1_0Server
MaxConnectionsPerProxy
ServerInfoTimeout
ConnectTimeOut
ConnectRetries
SendTimeOut
ReceiveTimeOut
DisableNTLMPreAuth
ScavengeCacheLowerBound
CertCacheNoValidate
ScavengeCacheFileLifeTime
ScavengeCacheFileLimit
HttpDefaultExpiryTimeSecs
FtpDefaultExpiryTimeSecs
LeashLegacyCookies
SendExtraCRLF
WpadSearchAllDomains
DontUseDNSLoadBalancing
ShareCredsWithWinHttp
DnsCacheEnabled
DnsCacheEntries
DnsCacheTimeout
WarnOnPost
WarnAlwaysOnPost
WarnOnZoneCrossing
WarnOnBadCertRecving
WarnOnPostRedirect
AlwaysDrainOnRedirect
WarnOnHTTPSToHTTPRedirect
TcpAutotuning
Win31FileSystem
DisplayName
DisplayVersion
Publisher
InstallDate
QuietUninstallString
InstallLocation
UninstallString
SystemComponent
places00
CityCurrent_ru
CityCurrent_en
PlaceOther
ShowStar
ShowText
ShowClouds
ShowDayNight
Install
InstallSuccess
GCStressStart
GCStressStartAtJit
DisableConfigCache
CacheLocation

DownloadCacheQuotaInKB
EnableLog
LoggingLevel
ForceLog
LogFailures
VersioningLog
LogResourceBinds
UseLegacyIdentityFormat
DisableMSIPeek
NoClientChecks
DevOverrideEnable
LatestIndex
NIUsageMask
ILUsageMask
ConfigMask
ConfigString
MVID
EvalationData
Status
ILDependencies
NIDependencies
MissingDependencies
Modules
SIG
LastModTime
mscorlib
Latest
index1
LegacyPolicyTimeStamp
System.Xml
System.Configuration
svcVersion
BadProxyExpiresTime
AutoProxyDetectType
WpadOverride
DisableBranchCache
UseFirstAvailable
CombineFalseStartData
DisableFalseStartBlocklist
EnforceP3PValidity
DuoProtocols
EnableSpdyDebugAsserts
SystemSetupInProgress
ProxyEnable
ProxyServer
ProxyOverride
AutoConfigURL
AutoDetect
SavedLegacySettings
DefaultConnectionSettings
DisableSecuritySettingsCheck
WpadDecision
WpadDecisionTime
WpadExpirationDays
WpadDecisionReason
WpadDhcp
WpadDns
WpadDetectedUrl
AdvpackLogFile
InstallationType
CurrentVersion
LocaleName
System.Windows.Forms
System.Drawing
System.Deployment
System.Runtime.Serialization.Formatters.Soap
Accessibility
System.Security
System.Core
NPACKD_CL
SwapMouseButtons
ProcessorNameString
Identifier
ProductId
SetupSpec22
UDL
Seed
GlitchInstrumentation

BuildLab
SystemBiosDate
EditionID
CurrentBuildNumber
ReferId
RegisterLink
DontUpdate
DownloadId
Variation
TimesPlayed
TimesExecuted
LastVerCheckQueryTime
RegName
RegCode
Is3D
Version
DisableMMX
DisableX3D
FewVertices
DisableVidMemVBs
DriverStyle
DisableST
SmoothScroll
lang
InstallerResult
InstallerError
InstallerResultUIString
ap
brand
UninstallArguments
usagestats
oeminstall
eulaaccepted
msi
DEPOff
SpecialFoldersCacheSize
DefaultScope
SuggestionsURLFallback
FaviconURLFallback
FaviconPath
URL
FaviconURL
TopResultURLFallback
TopResultURL
SuggestionsURL
NTURL
NTTopResultURL
NTSuggestionsURL
NTLogoPath
NTLogoURL
MID
SusClientId
RulesXmlDir
AllowConsecutiveSlashesInUrlPathComponent
UID
SendCustomerData
AppUserIdleTimerInterval
AppUserIdleResetInterval
.HLP
PINF
UserGUID
AppliedDPI
InstallLanguage
Local AppData
Local Settings
CSDVersion
lfEscapement
lfOrientation
lfWeight
lfItalic
lfUnderline
lfStrikeOut
lfCharSet
lfOutPrecision
lfClipPrecision
lfQuality
lfPitchAndFamily
lfFaceName

iPointSize
fWrap
StatusBar
fSaveWindowPositions
szHeader
szTrailer
iMarginTop
iMarginBottom
iMarginLeft
iMarginRight
iWindowPosY
iWindowPosX
iWindowPosDX
iWindowPosDY
fMLE_is_broken
SNZ0954
K362808
Userinit
delete_dir
<NULL>
RD
ProfileImagePath
PackageCode
InstanceType
ScreenSaverIsSecure
vidc.mrle
vidc.msvc
vidc.uyvy
vidc.yuy2
vidc.yvyu
vidc.iyuv
vidc.i420
vidc.yvu9
vidc.cvid
DefaultTTL
ID
IDD
Gateway
UserContextLockCount
UserContextListCount
Content Type
Extension
MaxConnectionsNumber
isUseWinDialUp
mAttempts
mRedialTime
MS Shell Dlg
BootDir
VersionToReport
CDNBaseUrl
ClientVersionToReport
ClientFolder
recoverydata
SoftwareOnly
EnumReference
EnumNullDevice
ForceRgbRasterizer
DebugFlags
UseMMXForRGB
DisableRendering
DisableFVF
DisableStripFVF
DisableGB
MMXFPDisableMask0
MMX Fast Path
DisablePSGP
EnableSC
DisableSP
Language
USERDOMAIN
USERNAME
APPDATA
LOCALAPPDATA
USERPROFILE
{A520A1A4-1780-4FF6-BD18-167343C5AF16}
~MHz
Counter
230

EventLogLevel
Startup
Scf
Gcf
Rlt
VersionNumber
Common Documents
TrapPollTimeMilliSecs
ShortcutBehavior
QuickTip
TileInfo
InfoTip
Shell
UncheckedValue
CheckedValue
HideFileExt
ShowSuperHidden
CacheOk
Compatible
Platform
EnableUTF8
ComputerName
TRACE_MISC
TRACE_CM
TRACE_TRACE
TRACE_SVC
TRACE_GATEWAY
TRACE_UI
TRACE_CONTACT
TRACE_UTIL
TRACE_CLUSTER
TRACE_RESOURCE
TRACE_TIP
TRACE_XA
TRACE_LOG
TRACE_MTXOCI
TRACE_ETWTRACE
TRACE_PROXY
TRACE_KTMRM
TRACE_VSSBACKUP
TRACE_PERFMON
TRACE_TM
TRACE_LU
TraceFilePath
MemoryBufferSize
DebugOutEnabled
UserUUID

CreateFile

C:\sample
C:\Windows\Fonts\staticcache.dat
C:\Windows\system32\rsaenh.dll
\\.\pipe\OperaCrashReporter3036
C:\installer_prefs.json
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160404181546.log
\\.\C:
\\.\D:
C:\Users\win7\AppData\Local\Temp\Opera Installer\installer.lck
C:\Users\win7\AppData\Local\Temp\nsaF532.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsaF532.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsaF532.tmp\modern-header.bmp
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\wintb.dll
C:\
C:\Windows
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db
C:\Users\win7\Desktop\desktop.ini
C:\Users\win7\AppData\Local\Temp\nsn8730.tmp

C:\Users\win7\AppData\Local\Temp\nsf3F16.tmp
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_r.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_i.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_0.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_1.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_2.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_3.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_4.dat
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\s_5.dat
1.217.519.0_TO_1.217.570.0_MPASDLTA.VDM._P
1.217.519.0_TO_1.217.570.0_MPAVDLTA.VDM._P
Preferences
C:\Users\desktop.ini
C:\Users\win7\AppData\Local\Temp\nso5775.tmp
C:\sample.config
C:\Users\win7\AppData\Local\Temp\wbxtra_04042016_230454.wbt
C:\Users\win7\AppData\Local\Temp\is-NCR66.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-NCR66.tmp_isetup_shfoldr.dll
\\.\pipe\OperaCrashReporter1676
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405001235.log
C:\ProgramData\48ed1695-d484-472b-bd42-582714ef1368\temp
C:\Users
C:\Users\win7
C:\Users\win7\AppData
C:\Users\win7\AppData\Roaming
C:\Users\win7\AppData\Roaming\Microsoft\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\UCOh.lnk
1.217.521.0_TO_1.217.599.0_MPASDLTA.VDM._P
1.217.521.0_TO_1.217.599.0_MPAVDLTA.VDM._P
\??\C:\Windows\system32\EhStorShell.dll
\??\C:\Windows\system32\ntshrui.dll
\\.\PIPE\srvsvc
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\perl514.dll
nul
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\d1e7c33431cd8713f2ce3582829a8b14\Socket.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\c5cce8d16a1bd48692b421dcf46d3396\Util.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\7ef0d901bf4203fbcf7a0fff0e82aa5f\Encode.dll
C:\Encode\ConfigLocal.pmc
C:\Encode\ConfigLocal.pm
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\d10c2c06ba2044cccc247c4315f5c7d3\Process.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\60ff464e01c2cd5526dbdad5a125081d\Dumper.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\4461f48e31bde5c56b31b973b773de09\List.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\eaeabd54205de2f10c00aea80bbf0d83\Registry.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\3a7ccbf8181ee5a145227a6dfce3594c\WinError.dll
C:\SetDualVar.pmc
C:\SetDualVar.pm
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\31638f63e39b38d3e250a9a57cb9d1c5\Cwd.dll
C:\bin\pwd
C:\usr\bin\pwd
C:\QOpenSys\bin\pwd
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\f233f63b6654362865c7577442edb9e3\Win32.dll
C:\Windows\system32
C:\Slim\Utils\OS\Custom.pmc
C:\Slim\Utils\OS\Custom.pm
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\5ffd05b2cbd58528e56519784ca9c869\Hostname.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\df1ba73f49c38cbbc7a11c779c3506d2\OLE.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\32785c19dc6898fbbbf06f3b776edd08\Fcntl.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\e56c61f7248672819579325af3387035\POSIX.dll
\\.\SICE
\\.\SIWVID
\\.\NTICE
C:\ProgramData\NortonInstaller\Logs\2016-04-05-03h48m05s\NortonInstall-2016-04-05-03h48m05s.log
C:\Users\win7\AppData\Local\Temp\\~DF2A99A3F002BF12C2.TMP
1.217.582.0_TO_1.217.599.0_MPASDLTA.VDM._P
1.217.582.0_TO_1.217.599.0_MPAVDLTA.VDM._P
C:\Users\win7\AppData\Roaming\Mikrotik\Winbox\winbox.cfg
C:\Users\win7\AppData\Local\Temp\\~DFF4D3A521EE0F29F2.TMP
C:\Users\win7\AppData\Local\Temp_MSI5166._IS
C:\Setup.INI
C:\0x0000.ini

C:\Users\win7\AppData\Local\Temp\nscE8ED.tmp
C:\Users\win7\AppData\Local\Temp\nsk8B61.tmp\inetc.dll
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
C:\ProgramData\0780f478-67ce-4ec3-98db-39a65f4618ce\temp
C:\ProgramData\219d5106-5a99-41fd-b942-db6b503b0178\temp
C:\Users\win7\AppData\Local\Temp\ccavusage.sdb
C:\Users\win7\AppData\Local\Temp\ccavusage.sdb-journal
C:\Users\win7\AppData\Local\Temp\ccavusage.sdb-wal
C:\Users\win7\AppData\Local\Temp\ccavusage.sdb-shm
MsiDetector.xml
C:\Users\win7\AppData\Local\Temp\nsc2DC5.tmp
C:\Users\win7\AppData\Local\Temp\nsx2DF5.tmp\UAC.dll
C:\Intel\Logs\IntelIRST.log
C:\Users\win7\AppData\Roaming\tor\lock
C:\Users\win7\AppData\Roaming\tor\state.tmp
C:\Users\win7\AppData\Roaming\tor\router-stability
C:\Users\win7\AppData\Roaming\tor\geoip
C:\Users\win7\AppData\Roaming\tor\geoip6
\\.\PIPE\wkssvc
C:\Users\win7\AppData\Roaming\tor\cached-certs
C:\Users\win7\AppData\Roaming\tor\cached-consensus
C:\Users\win7\AppData\Roaming\tor\unverified-consensus
C:\Users\win7\AppData\Roaming\tor\cached-microdesc-consensus
C:\Users\win7\AppData\Roaming\tor\unverified-microdesc-consensus
C:\Users\win7\AppData\Roaming\tor\cached-microdescs
C:\Users\win7\AppData\Roaming\tor\cached-microdescs.new
C:\Users\win7\AppData\Roaming\tor\cached-descriptors
C:\Users\win7\AppData\Roaming\tor\cached-extrainfo
\\.\Nsi
C:\Windows\system32\SYNSOPOS.exe
C:\ProgramData\d8986107-dff3-4565-a17b-637d7c3968d3\temp
CONIN$
CONOUT$
C:\Users\win7\AppData\Local\Temp\Setup Log 2016-04-05 #001.txt
C:\1by1local.ini
C:\Users\win7\AppData\Local\Temp\FILELOCK.TMP
C:\Users\win7\AppData\Local\Temp\TWAIN.LOG
C:\Users\win7\AppData\Local\Temp\Twain001.Mtx
\\.\PhysicalDrive0
\\.\PhysicalDrive1
\\.\PhysicalDrive2
\\.\PhysicalDrive3
C:\userpath.cfg
C:\assignment.cfg
C:\module.cfg
C:\sticky.cfg
C:\tricky.cfg
C:\userlist.cfg
C:\virtuawin.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\virtuawin.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\tricky.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\sticky.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\assignment.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\userlist.cfg
C:\Users\win7\AppData\Roaming\VirtuaWin\module.cfg
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index1c2.dat
C:\Windows\system32\l_intl.nls
C:\Windows\assembly\pubpol1.dat
C:\ProgramData\31f7a620-acbd-4f84-82db-5e231b8ad5de\temp
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\Welcome.zip
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\Spigot29.zip
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/index.html
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/bottomleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/script.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\MalwareProtection.zip
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\Installation.zip
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/styles.css
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/bottomleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/bottomright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/check-icon.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/download-logo.png

C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/bottomright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/check-icon.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/download-logo.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/index.html
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/script.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/index.html
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/script.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/styles.css
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/styles.css
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/green-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\Finish.zip
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/bottomleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/grey-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/green-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/bottomleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/bottomright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/installer-bg.jpg
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/grey-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/bottomright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/download-logo.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/topleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/topright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Spigot29/img/windows-32x32.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/installer-bg.jpg
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/index.html
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/topleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/green-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/check-icon.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/download-logo.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/script.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/topright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/grey-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/styles.css
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/img/windows-32x32.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/installer-bg.jpg
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/index.html
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/pause-button.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/bottomleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/script.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/green-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/progressbar-left.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/bottomright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/grey-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/progressbar-right.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/download-logo.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/green-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/installer-bg.jpg
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/topleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/topright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/progressfilled-left.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Welcome/styles.css
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\MalwareProtection/img/windows-32x32.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/progressfilled-right.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/grey-btn.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Common/jquery.min.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/installer-bg.jpg
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/resume-button.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Common/json3.min.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/topleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/stop-button.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Common/stats.js
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/topright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/topleft.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Finish/img/windows-32x32.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/topright.png
C:\Users\win7\AppData\Local\Temp\EA492F3D-8B01-4237-856D-178402E2E03A\\Installation/img/windows-32x32.png
bugreport.log
0x0000.ini
C:\Users\win7\AppData\Local\Temp_isABD7.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\Setup.INI
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}_ISMSIDEL.INI
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0000.ini
C:\Users\win7\AppData\Local\Temp_isAC07.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0404.ini
C:\Users\win7\AppData\Local\Temp_isAC18.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0407.ini
C:\Users\win7\AppData\Local\Temp_isAC76.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0409.ini

C:\Users\win7\AppData\Local\Temp_isAD52.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x040a.ini
C:\Users\win7\AppData\Local\Temp_isADC1.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x040c.ini
C:\Users\win7\AppData\Local\Temp_isAF19.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0410.ini
C:\Users\win7\AppData\Local\Temp_isAF78.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0411.ini
C:\Users\win7\AppData\Local\Temp_isB3DE.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0412.ini
C:\Users\win7\AppData\Local\Temp_isB9CB.tmp
C:\Users\win7\AppData\Local\Temp\{FFDEAF5A-024E-405D-B109-573006F93D02}\0x0804.ini
C:\Users\win7\AppData\Local\Temp\AITMP687\aisetup.zip
C:\Users\win7\AppData\Local\Temp\AITMP687\Englishai.lng
C:\Users\win7\AppData\Local\Temp\AITMP687\Russianai.lng
C:\Users\win7\AppData\Local\Temp\AITMP687\aisetup.ini
C:\Users\win7\AppData\Local\Temp\AITMP687\aiwizard.bmp
C:\Users\win7\AppData\Local\Temp\AITMP687\aiheader.bmp
C:\Users\win7\AppData\Local\Temp\AITMP687\7za.exe
C:/lib/tcl8.5/encoding
C:/sample
C:/Users/win7/.Xdefaults
C:/Users/win7/AppData/Local/Temp/BRBC76.tmp
\\.\pipe\OperaCrashReporter2396
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405165551.log
\\.\pipe\OperaCrashReporter2648
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405172045.log
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Users\win7\AppData\Local\Temp\is-S1NB8.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-S1NB8.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-S1NB8.tmp\RdZone.dll
C:\ProgramData\Npackd\Data.db
C:\ProgramData\Npackd\Data.db-journal
C:\Users\win7\AppData\Local\Temp\is-B6UKO.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-B6UKO.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-B6UKO.tmp_isetup_isdecmp.dll
wdmaud.drv
C:\Users\win7\Desktop
C:\Users\win7\Desktop\Default
C:\Users\Public\Desktop
C:\Users\Public\Desktop\Default
\\.\PIPE\samr
C:\Users\Public\Desktop\desktop.ini
\??\C:\Windows\System32\shdocvw.dll
C:\Users\win7\AppData\Local\Temp\wbxtra_04052016_180922.wbt
C:\Users\win7\AppData\LocalLow\WebEx\JmtLog.log
C:\Users\win7\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\system32\GDIPFONTCACHEV1.DAT
C:\WINDOWS\FONTS\MARLETT.TTF
C:\WINDOWS\FONTS\ARIAL.TTF
C:\WINDOWS\FONTS\ARIALI.TTF
C:\WINDOWS\FONTS\ARIALBD.TTF
C:\WINDOWS\FONTS\ARIALBI.TTF
C:\WINDOWS\FONTS\BATANG.TTC
C:\WINDOWS\FONTS\COUR.TTF
C:\WINDOWS\FONTS\COURI.TTF
C:\WINDOWS\FONTS\COURBD.TTF
C:\Users\win7\AppData\Local\Temp\HTM9D3D.tmp
local_resources.css
debug_only.css
C:\Windows\SysWOW64\FirewallAPI.dll
C:\Windows\SysWOW64\stdole2.tlb
C:\ProgramData
C:\ProgramData\handyCafe
C:\data
C:\plugin.dll
C:\plugin.dll\desktop.ini
C:\RBShell600.dll
C:\RBShell600.dll\desktop.ini
C:\RBMD5600.dll
C:\RBMD5600.dll\desktop.ini
C:\RBInternetEncodings600.dll
C:\RBInternetEncodings600.dll\desktop.ini
C:\sample\desktop.ini
C:\Windows\System32\slmgr.vbs
C:\Windows\System32\slmgr.vbs\desktop.ini
C:\Windows\System32\spp\tokens\pkeyconfig\pkeyconfig.xrm-ms

C:\Windows\System32\spp\tokens\pkeyconfig\pkeyconfig.xrm-ms\desktop.ini
C:
C:\desktop.ini
C:\Certificates
C:\Certificates\desktop.ini
C:\SLICs
C:\SLICs\desktop.ini
C:\keys.ini
C:\keys.ini\desktop.ini
C:\Users\win7\AppData\Roaming\Canon\SELPHY Photo Print\SPPSetting.xml
C:\Users\win7\AppData\Local\Temp\McCSPInstall.dll
C:\Users\win7\AppData\Local\Temp\nsv879C.tmp\System.dll
\\.\pipe\BurnPipe.{F5944EBB-6F47-4C60-B2F9-657A3837F8E2}
C:\Users\win7\AppData\Local\Temp\Setup_20160405195034_Failed.txt
C:\Users\win7\AppData\Local\Temp\nsy985B.tmp
C:\Users\win7\AppData\Local\Temp\nso99F2.tmp\System.dll
properties\partner.xml
adlist.txt
C:\Windows\popcinfo.dat
c:\windows\system32\vboxdisp.dll
vhwb.dat
vhw.dat
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\win7\AppData\Local\Temp\nsu6797.tmp
C:\Users\win7\AppData\Local\Temp\nsj67F5.tmp\System.dll
\\.\BCMDMCCP
C:\Users\win7\AppData\Local\Temp\nsbE140.tmp
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\modern-header.bmp
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\InstallOptions.dll
\\.\SIWDEBUG
C:\Users\win7\AppData\Local\Temp\chrome_installer.log
C:\Users\win7\AppData\Local
C:\Users\win7\AppData\Local\Google
C:\Users\win7\AppData\Local\Google\Chrome
C:\Users\win7\AppData\Local\Google\Chrome\Temp
C:\Users\win7\AppData\Local\Google\Chrome\Temp\source2432_29154
C:\Users\win7\AppData\Local\Temp\is-KQSHV.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-KQSHV.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-KQSHV.tmp\ISDone.dll
C:\ProgramData\c00fd789-4044-4a32-8a4f-7d731dbdc0d1\temp
C:\Users\win7\AppData\Local\Temp_is351B.tmp
C:\Users\win7\AppData\Local\Temp\{D4D8B068-D720-4875-A46C-50F51A9C5F90}\Setup.INI
C:\Users\win7\AppData\Local\Temp\{D4D8B068-D720-4875-A46C-50F51A9C5F90}_ISMSIDEL.INI
C:\Users\win7\AppData\Local\Temp\nsyB9F.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsyB9F.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsyB9F.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsyB9F.tmp\modern-header.bmp
\\.\ASUSACPI
C:\Windows\system32\rundll32.exe
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innoextractor.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\bassmusic.dll
C:\ProgramData\9a4b8b26-f4e0-4529-a5b4-93ec828f7e42\temp
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp\botva2.dll
c:\temp\hamachi.log
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\options.ini
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\shortcuts.ini
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\components.ini
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\summary.ini
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\modern-header.bmp
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\WIN7-PC-20160406-0649.log

C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\GCountry.dll
C:\sample.lcf
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\nsgAFC5.tmp
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\\~DFF5A96B028B74C1AD.TMP
C:\sample.EXE
C:\Windows\SysWOW64\scrrun.dll
C:\Users\win7\AppData\Local\Temp\qag7A3.tmp
\\.\Scsi0:
\\.\Scsi1:
\\.\Scsi2:
\\.\Scsi3:
\\.\Scsi4:
\\.\Scsi5:
\\.\Scsi6:
\\.\Scsi7:
\\.\Scsi8:
\\.\Scsi9:
\\.\Scsi10:
\\.\Scsi11:
\\.\Scsi12:
\\.\Scsi13:
\\.\Scsi14:
\\.\Scsi15:
D:/MinGW/msys/1.0/local/winiconv/share/locale/locale.alias
C:\Windows\system32/./locale/en_US/LC_MESSAGES/wget.mo
C:\Windows\system32/./locale/en/LC_MESSAGES/wget.mo
C:\\builddate.txt
C:\Users\win7\AppData\Local\Temp\CR_793D1.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_793D1.tmp\SETUP_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\GUMAA9A.tmp\goopdate.dll
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C86BD7751D53F10F65AAAD66BBDF33C7
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EE44ECA143B76F2B9F2A5AA75B5D1EC6_847118BE2683F0C241D1D702F3A3F5F9
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EE44ECA143B76F2B9F2A5AA75B5D1EC6_48BC6893316669491F73A0AFA6B78DC9
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\616AD1AB067CFD351D6C0EF6F3E12F40
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\782D7E2BFB036A849A99FFA65C652D39
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CA4458E7366E94A3C3A9C1FE548B6D21_03701DFFBB0DB68C6FEF44A923FC306A
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CA4458E7366E94A3C3A9C1FE548B6D21_11890B83A662A94DAA54032730C974C0
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7BD5521448F9309F5CEB0C75890FFABC
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\76A6104AD5D7661815E18299392B9F65
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BAEBE581FCB73249406FC21094EA252E_BC0CE803EF41A748738619ED7838EEFC
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\BAEBE581FCB73249406FC21094EA252E_FD361CE5A85478C5EE18C8A08F5CE82E
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C3E814D1CB223AFCD58214D14C3B7EAB
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_5B98B6CD6E692026769 65CF5B0E2A7A7
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\D84E548583BE1EE7DB5A935821009D26_1070D8A1DE1737B040B2F83EA6FA69E1
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8BD11C4A2318EC8E5A82462092971DEA
C:\ProgramData\Dropbox\Update\Log\DropboxUpdate.log-2016-04-06-08-33-55-805-1980
C:\Users\win7\AppData\Local\Temp\nsz8FE4.tmp
C:\Users\win7\AppData\Local\Temp\nsz9081.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsz9081.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\is-6B3K6.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-QKM9K.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-QKM9K.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-QKM9K.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-4B7CH.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\comodo_temp_setup\csb_installer_x64.msi
\??\C:\Windows\SysWOW64\ieframe.dll
__tmp_rar_sfx_access_check_54717968
C:\Windows\system32\cstrike
C:\Windows\system32\cstrike\css.ico
cstrike/css.ico
C:\Users\win7\AppData\Local\Temp\\~DFA93067913D3147BE.TMP
C:\Windows\system32\MSVBVM60.DLL\3
C:\Windows\system32\MSVBVM60.DLL
C:\Users\win7\Searches\desktop.ini
C:\Users\win7\Videos\desktop.ini
C:\Users\win7\Pictures\desktop.ini
C:\Users\win7\Contacts\desktop.ini
C:\Users\win7\Favorites\desktop.ini
C:\Users\win7\Music\desktop.ini

C:\Users\win7\Downloads\desktop.ini
C:\Users\win7\Documents\desktop.ini
C:\Users\win7\Links\desktop.ini
C:\Users\win7\Saved Games\desktop.ini
C:\Users\win7\AppData\Local\Temp\sample
c:\1903fbffd06add0655b0\NDP35SP1-KB2736416.msp
c:\1903fbffd06add0655b0\HotFixInstaller.exe
c:\1903fbffd06add0655b0\DHtmlHeader.html
c:\1903fbffd06add0655b0\ParameterInfo.xml
c:\1903fbffd06add0655b0\watermark.bmp
c:\1903fbffd06add0655b0\header.bmp
c:\1903fbffd06add0655b0\1025\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1025\eula.rtf
c:\1903fbffd06add0655b0\1028\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1028\eula.rtf
c:\1903fbffd06add0655b0\1029\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1029\eula.rtf
c:\1903fbffd06add0655b0\1030\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1030\eula.rtf
c:\1903fbffd06add0655b0\1031\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1031\eula.rtf
c:\1903fbffd06add0655b0\1032\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1032\eula.rtf
c:\1903fbffd06add0655b0\1033\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1033\eula.rtf
c:\1903fbffd06add0655b0\1035\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1035\eula.rtf
c:\1903fbffd06add0655b0\1036\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1036\eula.rtf
c:\1903fbffd06add0655b0\1037\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1037\eula.rtf
c:\1903fbffd06add0655b0\1038\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1038\eula.rtf
c:\1903fbffd06add0655b0\1040\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1040\eula.rtf
c:\1903fbffd06add0655b0\1041\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1041\eula.rtf
c:\1903fbffd06add0655b0\1042\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1042\eula.rtf
c:\1903fbffd06add0655b0\1043\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1043\eula.rtf
c:\1903fbffd06add0655b0\1044\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1044\eula.rtf
c:\1903fbffd06add0655b0\1045\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1045\eula.rtf
c:\1903fbffd06add0655b0\1046\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1046\eula.rtf
c:\1903fbffd06add0655b0\1049\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1049\eula.rtf
c:\1903fbffd06add0655b0\1053\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1053\eula.rtf
c:\1903fbffd06add0655b0\1055\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\1055\eula.rtf
c:\1903fbffd06add0655b0\2052\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\2052\eula.rtf
c:\1903fbffd06add0655b0\2070\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\2070\eula.rtf
c:\1903fbffd06add0655b0\3076\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\3076\eula.rtf
c:\1903fbffd06add0655b0\3082\HotFixInstallerUI.dll
c:\1903fbffd06add0655b0\3082\eula.rtf
c:\1903fbffd06add0655b0\$shtdwn$.req
\\.\pipe\GoogleCrashServices\S-1-5-21-3979321414-2393373014-2172761192-1000
C:\SuperbGameBoostMain.exe
\\.\pipe\OperaCrashReporter2248
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160406155933.log
C:\Users\win7\AppData\Local\Temp\Tsu9CF7CF34.dll
C:\Users\win7\AppData\Local\Temp\sample.log
C:\ProgramData\HP\Installer\Temp\sample000.log
C:\Users\win7\AppData\Local\Temp
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Windows\system32\nsprs.dll
C:\Windows\system32\ssprs.dll
C:\Windows\system32\nsprs.tgz
C:\Windows\system32\ssprs.tgz
C:\Windows\system32\clauth1.dll
C:\Windows\system32\clauth2.dll
C:\Windows\system32\serauth1.dll

C:\Windows\system32\serauth2.dll
C:\Windows\system32\servdat.slm
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\options.ini
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\shortcuts.ini
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\components.ini
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\summary.ini
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\modern-header.bmp
\\?\C:\Users\win7:Heroes & Generals
\\?\C:\Windows\system32\locale\hngsync_en.xml
\\?\C:\Windows\system32\steam.ini
C:\Users\win7\AppData\Local\Temp\nsn7B68.tmp
C:\Users\win7\AppData\Local\Temp\nsi7C34.tmp\System.dll
inet\irpatch.exe
C:\ProgramData\78a595fd-df95-40de-93ec-d80a00f25811\temp
\\\
C:\Users\win7\AppData\Local\Temp\nsiC93F.tmp
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\modern-header.bmp
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\is-ENFQS.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-PQ2TS.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-PQ2TS.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-PQ2TS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Roaming\Microsoft\Windows
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\INetC.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\install_flash_player_plugin.exe
C:\install.cfg
C:\Intel\Logs\IntelChipset.log
__tmp_rar_sfx_access_check_54714234
qt_host_installer.exe
C:\Users\win7\AppData\Local\Temp\PreVer.log
C:\wwhbu.xcf
C:\wwkrn.new
C:\xvtlogon.xcf
C:\wwkrn.dll
C:\wwkrn.xcf
c:\wwdbg.txt
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\iswin7.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\WinTB.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\botva2.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\CallbackCtrl.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\options.ini
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\shortcuts.ini
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\components.ini
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\summary.ini
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\modern-header.bmp
C:\ProgramData\6f66c052-8827-4487-9031-09becb0cf541\temp
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\nsz40B6.tmp
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\itdownload.dll

C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\e4j77EC.tmp_dir29233\exe4jlib.jar
C:\Users\win7\AppData\Local\Temp\e4j77EC.tmp_dir29233\krtitok2.jar
C:\Users\win7\AppData\Local\Temp\e4j77EC.tmp_dir29233\kriptosdk2.jar
C:\Users\win7\AppData\Local\Temp\e4j77EC.tmp_dir29233\crimson.jar
C:\\.install4j\pref_jre.cfg
C:\\.install4j\inst_jre.cfg
C:\Users\win7\AppData\Local\Temp\is-84VFQ.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-84VFQ.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-84VFQ.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nswC4C5.tmp
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\logo.ico
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\license.rtf
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.exe
C:\Intel\Logs\IntelGFX.log
C:\Users\win7\AppData\Local\Temp\Bootstrap_log.txt
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.cab
C:\Users\win7\AppData\Local\Temp\n1s\nchdata.cab
C:\Users\win7\AppData\Local\Temp\n1s\nchdata.dat
C:\Users\win7\AppData\Local\Temp\evb39B9.tmp
c:\sample
C:\Users\win7\AppData\Local\Temp\\~DFA18374210A7C3F91.TMP
C:\Users\win7\AppData\Local\Temp\nso3461.tmp
C:\Users\win7\AppData\Local\Temp\nse355C.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nscFC79.tmp
C:\Users\win7\AppData\Local\Temp\nshFD83.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\{5B964E0E-B9A3-4276-9ED9-4D5A5720747A}\YandexSearch.msi
C:\Users\win7\AppData\Local\Temp\YandexSearch00000.log
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\HPDiagnosticCoreSetup.msi
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\CopyInstructionsW.exe
C:\Users\win7\AppData\Local\Temp\nsqAE03.tmp
C:\Users\win7\AppData\Local\Temp\nsbAF7B.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp\header.bmp
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\DMR\dmr_72.exe
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\NSISArray.dll
C:\Users\win7\AppData\Local\Temp\wlan_test.exe
C:\Users\win7\AppData\Local\Temp\cat_background.bmp
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\GetVersion.dll
msrle32.dll
msvidc32.dll
msyuv.dll
iyuv_32.dll
tsbyuv.dll
iccvid.dll
C:\ProgramData\6cd7b088-ad43-47a9-9f65-96d8797bb92b\temp
C:\Users\win7\AppData\Local\Temp\CR_8D9FE.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_8D9FE.tmp\SETUP_PATCH.PACKED.7Z
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\nsf5E74.tmp
C:\Users\win7\AppData\Local\Temp\nsf5E75.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf5E75.tmp\UserInfo.dll
MPASDLTA.VDM
MPAVDLTA.VDM
\\.\COM3
\\.\ATKACPI
C:\Users\win7\AppData\Local\Temp\nsrC83A.tmp
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\button.bmp
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\skinnedbutton.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\System.dll
1.217.686.0_TO_1.217.869.0_MPASDLTA.VDM._P
1.217.686.0_TO_1.217.869.0_MPAVDLTA.VDM._P
\\.\PHYSICALDRIVE0
\\.\pipe\OperaCrashReporter2864
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160407224627.log
C:\Users\win7\AppData\Local\Temp\nsnFF76.tmp
C:\Users\win7\AppData\Local\Temp\nstFFE5.tmp\nsisos.dll

C:\uninstall.lng
\\?\C:\uninstall.lng
Uninstall.lst
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_iscrypt.dll
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp\idp.dll
\\.\pipe\BurnPipe.{D4737F25-40ED-4F12-8A9A-28D0D9A4AE57}
C:\Users\win7\AppData\Local\Temp\Setup_20160408030827_Failed.txt
\??\C:\Windows\system32\twext.dll
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\Computer Management.lnk
C:\Users\win7\AppData\Local\Temp\\~DFF61056C422EA0937.TMP
C:\Users\win7\AppData\Local\Temp\27H3R8DF\unpack.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\comregc.exe
C:\Users\win7\AppData\Local\Temp\27H3R8DF\Resume.exe
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\splash.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\banner.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\watermark.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\butt_warn.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\butt_cancel.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\butt_inf.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\butt_que.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\unbanner.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\unwatermark.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\maintenance.bmp
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\License.rtf
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\readme.rtf
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\info.rtf
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\help.rtf
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\AFTERINITDB.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\BEGINUPDATE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\CLUSTERSTATUS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\CONNPARAMS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\createuser.exe
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\DBSESSIONS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\DBSTATUS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\DISKINFO.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\diskspace.bat
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\ENDUPDATE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\foldersize.bat
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\GETSETUP.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\INSTDB.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\MAINTAINDB.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\MMCHECKMODULES.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\MMCONDITIONS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\NEWREGKEYAPP.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PARAMSTR.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGCLOSECONN.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGCONF.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGINITDB.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGINITDBOK.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGINITVAR.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGLIBINFO.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGLIBSERVER.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGLIBSQL.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGREADDBPARAMS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGREGISTER.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGSTARTSERVICEABORT.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGSTOPSERVICE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGSTOPSERVICEABORT.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUNREGISTER.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPDATE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPDATE.pas.bak
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPGRADEDUMP.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPGRADEINFO.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPGRADERESTORE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPGRADEROLE.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PGUPGRADESTOP.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\pg_dump.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\pg_restore.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\process.bat
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\PROCESSINFO.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\READLASTPATCH.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\rumlib.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\SimpleMsgs.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\SRVSESSIONS.sql
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\SRVSESS_TXT.sql

C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\TOOLS.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\UPDATEDB.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\validateuser.exe
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\VERSIONINFO.pas
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\presetup\zlib1.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\plugins\1\CustomUI.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\plugins\3\MLTools.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\plugins\4\Scripter.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\plugins\2\Services.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\plugins\0\WebDeploy.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\packagedb
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\languages
C:\Users\win7\AppData\Local\Temp\27H3R8DF\sample\maindb
C:\Windows\Fonts\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Recent\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\SendTo\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\\chrome.dll
C:\\23.0.1271.97\chrome.dll
C:\debug.log
C:\Users\win7\AppData\Local\Temp\WIN7-PC-20160408-1246.log
Lisezmoi.txt
LUInit.ini
LUINFO.INF
ALUNotify.exe
ALUSchedulerSvc.exe
AUpdate.exe
Lsetup.exe
LuAll.exe
LuCallbackProxy.exe
LuCheck.exe
LuComServer_3_2.EXE
LuConfig.exe
LUInit.exe
NotifyHA.exe
SymantecRootInstaller.exe
ALUNotifyRes.dll
ALUSchedulerSvcRes.dll
AUpdateRes.dll
capicom.dll
LuAllRes.dll
LUinsDll.dll
LUinsRes.dll
LUPreCon.dll
MFC71.dll
msvcp71.dll
msvcr71.dll
NetDetectController_3_2.DLL
ProductRegCom_3_2.DLL
PSLuComServer_3_2.DLL
ResLuComServer_3_2.DLL
S32Live1.dll
S32LUCP1Res.dll
S32Luis1.dll
S32LUWI1.dll
setupRes.dll
SymantecRootInstallerRes.dll
unrar.dll
LUALL.chm
S32LUCP2.CPL
LuSymProtect.grd
Settings.Default.LiveUpdate
LuSymProtect.sig
LuSymProtect.spm
C:\Windows\system32\Macromed\Flash\mms.cfg
\??\C:\Users\win7\AppData\Local\Temp\acro_rd_dir
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IMJP12

\??\C:\Users\win7\AppData\LocalLow\Microsoft\IME12
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IMJP8_1
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IMJP9_0
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IMJP?_?
\??\C:\Users\win7\AppData\LocalLow\Microsoft
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IME??
\??\C:\Users\win7\AppData\LocalLow\Microsoft\IMJP??
\??\C:\Users\win7\AppData\Roaming\Microsoft\Speech
\??\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\AssetCache
\??\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\AFCache
\??\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\Icon Cache
\??\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\APSPrivateData2
\??\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\NativeCache
\??\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player
\??\C:\Users\win7\AppData\Local\Macromedia\Flash Player
\??\C:\Users\win7\AppData\Roaming\Justsystem
\??\C:\Users\win7\AppData\Roaming
C:\Users\win7\AppData\Local\Temp\nswCD95.tmp
C:\Users\win7\AppData\Local\Temp\nsxCECF.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\is-ML5M0.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-ML5M0.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-ML5M0.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_E9915110418DBDEA47BB3BFCDB24CFF1
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
C:_Setup.dll
C:\Users\win7\AppData\Local\Temp\nsd329C.tmp
C:\Users\win7\AppData\Local\Temp\nsj3359.tmp\System.dll
\\?\C:\Windows\system32\atih_uninstaller_launcher.msg
\\?\C:\atih_uninstaller_launcher.msg
\\?\C:\sample.dat
\\?\C:\sample
\\?\C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\atih_uninstaller_standard.exe
\\?\C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\libcrypto10.dll
\\?\C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\libssl10.dll
\\?\C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\report_sender_standard.exe
C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\atih_uninstaller_standard.exe
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_6043FC604A395E1485AF7AC16D16B7CE
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\C46E7B0F942663A1EDC8D9D6D7869173_DF4CA81DC775CDA9B3214BDB5B55900E
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\40C68D5626484A90937F0752C8B950AB
1.217.854.0_TO_1.217.941.0_MPASDLTA.VDM._P
1.217.854.0_TO_1.217.941.0_MPAVDLTA.VDM._P
C:\ProgramData\NortonInstaller\Logs\2016-04-08-15h49m48s\NortonInstall-2016-04-08-15h49m48s.log
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0G27RVV\0RHYLLSA.json
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0G27RVV\monetization[1].gif
\\.\aswSP_Handler
\\.\ASWSP_Open
\\.\ASWSP
\\.\aswSP
\\?\C:\Windows\system32\Macromed\Flash\ss.sgn
\\?\C:\Windows\system32\Macromed\Flash\ss.cfg
\\?\C:\Windows\system32\Macromed\Flash\mms.cfg
\\?\C:\Windows\system32\mms.cfg
\\?\C:\Windows\system32\Macromed\Flash\oem.cfg
\\?\C:\Windows\system32\oem.cfg
\\?\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\AssetCache
\\?\C:\Users\win7\AppData\Roaming\Adobe\Flash Player
\\?\C:\Users\win7\AppData\Roaming\Adobe\Flash Player\AssetCache\4TDX5A6A
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\#SharedObjects
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player
\\?\C:\Users\win7\AppData\Roaming\Macromedia
\\?\C:\Users\win7\AppData\Roaming
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\76T3MARV
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\76T3MARV\macromedia.com\support\flashplayer\sys\settings.sol
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sxx
C:\Users\win7\AppData\Local\Temp\CR_D2B34.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_D2B34.tmp\SETUP_PATCH.PACKED.7Z
C:\WBDJA44I.DLL
C:\Users\win7\AppData\Local\Temp\is-EERGE.tmp\is-APQM2.tmp
C:\Users\win7\AppData\Local\Temp\bt3526.bat
__tmp_rar_sfx_access_check_54664421
MetroInstallerAPP.exe
MetroInstallPack.MIP
C:\Users\win7\AppData\Local\Temp\RarSFX0\MetroInstallerAPP.exe

C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Update.bat
C:\Windows\temp\sqlserver.exe
C:\Windows\system32\dumpkernel.exe
C:\Windows\temp\Server32History.dat
C:\Windows\temp\tttdelzzz.bat
C:\Windows\temp\tttbrozzz.bat
C:\Windows\Temp\USBInstallInfo.log
C:\config\product.ini
C:\Config\NLS\LangConv.ini
C:\Users\win7\AppData\Local\Temp\install.log
C:\Config\NLS\en.nls
C:\Config\NLS\Common.nls
C:\Config\NLS\OEM.nls
C:\Windows\syswow64\kernel32.dll
C:\Windows\System32
C:\Windows\System32\cmd.exe
30044.exe
C:\windows\temp\23322.exe
C:\Users\win7\AppData\Local\rec_gb_215\rec_gb_215\1.20\cnf.cyl
C:\Users\win7\AppData\Local\Temp\gch37D3.tmp
C:\Users\Public\Documents\desktop.ini
C:\Users\Public\Pictures\desktop.ini
C:\Users\Public\Music\desktop.ini
C:\Users\Public\Videos\desktop.ini
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Cookies\desktop.ini
C:\Users\win7\AppData\Local\Microsoft
C:\Users\win7\AppData\Local\Microsoft\Windows
C:\Users\win7\AppData\Local\Microsoft\Windows\History\desktop.ini
C:\Users\win7\AppData\Local\Temp\gentee7D\setup_temp.gea
C:\Users\win7\AppData\Local\Temp\nse2075.tmp
C:\Users\win7\AppData\Local\Temp\nse2076.tmp\AccDownload.dll
C:\Users\win7\AppData\Local\Temp\nspF584.tmp
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\HWSignature.dll
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\SetupLib.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\HwInfo.dll
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\modern-header.bmp
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\modern-wizard.bmp
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\System.dll
http://300miners.com/start.html
C:\Program Files\Internet Explorer\iexplore.exe
C:\Users\win7\AppData\Local\Temp\\~DF7C7988AF8F442A6B.TMP
C:\sample.scr
C:\Recycled\desktop.ini
C:\Recycled\SVCHOST.EXE
C:\Recycled\SPOOLSV.EXE
C:\Recycled\CTFMON.EXE
C:\Recycled\SMSS.EXE
C:\Windows\Fonts\Explorer.exe
C:\Users\win7\AppData\Local\Temp\Flu Burung.txt
C:\sample`.!!!
C:\sample.doc
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\pftw1.pkg
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\GvNPRT_Install.exe
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\GvNPRT_Install.ini
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\gvx_installer.xml
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\Install_OCX.exe
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\nprt_gvx.dll
__tmp_rar_sfx_access_check_54609281
idman623build5.exe
C:\Windows\Logs\DirectX.log
__tmp_rar_sfx_access_check_54613812
DXSETUP.exe
DSETUP.dll
dsetup32.dll
Aug2008_d3dx9_39_x86.cab
dxupdate.cab
C:\Users\win7\AppData\Local\Temp\RarSFX0\DXSETUP.exe
C:\Windows\System32\Adobe Photoshop Lightroom 5
C:\Users\win7\AppData\Local\Temp\is-6MGN8.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-6MGN8.tmp_isetup_shfoldr.dll
C:\Windows\system32\\\\wuapi.dll
C:\Users\win7\AppData\Local\Temp\nsm8029.tmp
C:\Users\win7\AppData\Local\Temp\nsc803A.tmp\nsExec.dll

C:\Users\win7\AppData\Local\Temp\~w0cvwt46y3.tmp
C:\Users\win7\AppData\Local\Temp_is8F03.tmp
C:\Users\win7\AppData\Local\Temp\{71069900-1BF3-4593-96E8-2BA11C9E3234}\Setup.INI
C:\Users\win7\AppData\Local\Temp\{71069900-1BF3-4593-96E8-2BA11C9E3234}_ISMSIDEL.INI
C:\Users\win7\AppData\Local\Temp\{71069900-1BF3-4593-96E8-2BA11C9E3234}\0x0000.ini
C:\Users\win7\AppData\Local\Temp_is959C.tmp
C:\Users\win7\AppData\Local\Temp\{71069900-1BF3-4593-96E8-2BA11C9E3234}\0x0409.ini
C:\Users\win7\AppData\Local\Temp_isA02D.tmp
C:\Users\win7\AppData\Local\Temp\~A00D.tmp
C:\Users\win7\AppData\Local\Temp_isA119.tmp
C:\Users\win7\AppData\Local\Temp\~A118.tmp
http://pliuht.cdnpckgs.eu/client/pkgs/silversands/Silver Sands Casino20160401011610.msi
C:\putty.hlp
C:\putty.cnt
C:\putty.chm
C:\Users\win7\AppData\Local\Temp\nsi8E91.tmp
C:\Users\win7\AppData\Local\Temp\xagE6.tmp
C:\Users\win7\AppData\Local\Temp\\~DF05B3E806633591A5.TMP
C:\Users\win7\AppData\Local\Temp\is-3H39U.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-KSUF0.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-KSUF0.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-KSUF0.tmp_isetup_shfoldr.dll
1.217.854.0_TO_1.217.955.0_MPASDLTA.VDM._P
1.217.854.0_TO_1.217.955.0_MPAVDLTA.VDM._P
C:\Users\win7\AppData\Local\Temp\dfs77AD.tmp
C:\Users\win7\AppData\Local\Temp\SQ3B11C.tmp
1.217.686.0_TO_1.217.955.0_MPASDLTA.VDM._P
1.217.686.0_TO_1.217.955.0_MPAVDLTA.VDM._P
C:\Users\win7\AppData\Local\Temp\is-9AFAT.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-FP5SP.tmp_isetup_RegDLL.tmp
C:\Users\win7\AppData\Local\Temp\is-FP5SP.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-FP5SP.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-FP5SP.tmp\GameuxInstallHelper.dll
C:\ProgramData\Battle.net\Setup\battle.net\Logs\battle.net-setup-20160408T200723.659429.log
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_cz.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_da.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_es.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_fr.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_ge.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_hu.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_id.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_in.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_it.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_jp.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_ko.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_ms.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_nl.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_pb.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_pl.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_pt.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_ru.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_sc.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_sk.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_sp.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_tr.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_us.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_zh.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\license_zt.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_cz.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_da.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_es.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_fr.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_ge.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_hu.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_id.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_in.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_it.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_jp.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_ko.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_ms.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_nl.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_pb.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_pl.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_pt.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_ru.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_sc.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_sk.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_sp.htm

C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_tr.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_us.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_zh.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\personalise_zt.htm
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaconf.txt
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfavera.txt
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaverx.txt
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\compat.ini
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfacz.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfada.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaes.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfafr.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfage.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfahu.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaid.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfain.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfait.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfajp.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfako.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfams.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfanl.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfapb.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfapl.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfapt.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaru.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfasc.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfask.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfasp.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfatr.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfaus.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfazh.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\mfazt.lns
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgmfapx.exe
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgntdumpx.exe
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgrdtesta.exe
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgrdtestx.exe
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgrunasx.exe
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\avgmfarx.dll
C:\Users\win7\AppData\Local\Temp\7zS857BEDF2\htmlayout.dll
C:\Users\win7\AppData\Local\Temp\\gegbjpofdfa.exe
C:\ProgramData\074666a9-9c4a-46c0-9d2f-0ac2cbbb1ef3\temp
C:\Users\win7\AppData\Local\Temp\nsbA2F4.tmp
C:\Users\win7\AppData\Local\Temp\nsqA304.tmp\System.dll

OpenRegisteryKey

Software\Microsoft\Windows NT\CurrentVersion\VFW
Software\Microsoft\Windows\CurrentVersion
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
Segoe UI
Tahoma
Software\Microsoft\WBEM\CIMOM
Software\Opera Software
MS Shell Dlg
Software\Borland\Locales
Software\Borland\Delphi\Locales
MIME\Database\CodePage\437
MIME\Database\RFC1766
SOFTWARE\LEDPointer\Default
SOFTWARE\Microsoft\OLEAUT
Software\Microsoft\Windows\CurrentVersion\Setup
system\CurrentControlSet\control\NetworkProvider\HwOrder
SOFTWARE\Microsoft\CTF\Compatibility\sample
Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
SOFTWARE\Microsoft\CTF\TIP\
{0000897b-83df-4b96-be07-0fb58b01c4a4}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{03B5835F-F03C-411B-9CE2-AA23E1171E36}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{07EB03D6-B001-41DF-9192-BF9B841EE71F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{3697C5FA-60DD-4B56-92D4-74A569205C16}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{531FDEBF-9B4C-4A43-A2AA-960E8FCDC732}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{78CB5B0E-26ED-4FCC-854C-77E8F3D1AA80}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{8613E14C-D0C0-4161-AC0F-1DD2563286BC}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}

{A028AE76-01B1-46C2-99C4-ACD9858AE02F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{AE6BE008-07FB-400D-8BEB-337A64F7051F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{C1EE01F2-B3B6-4A6A-9DDD-E988C088EC82}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{DCBD6FA8-032F-11D3-B5B1-00C04FC324A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{E429B25A-E5D3-4D1F-9BE3-0C608477E3A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{F89E9E58-BD2F-4008-9AC2-0F816C09F4EE}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
Keyboard Layout\Toggle
Software\Microsoft\CTF\DirectSwitchHotkeys
SOFTWARE\Microsoft\CTF\
Software\CodeGear\Locales
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
System\CurrentControlSet\Control\Keyboard Layouts\041F0409
System\CurrentControlSet\Control\Keyboard Layouts\04090409
SOFTWARE\Microsoft\Windows NT\CurrentVersion
System\CurrentControlSet\Control
Software\Microsoft\RestartManager
Software\Embarcadero\Locales
Software\OBS Studio
Software\Policies
Software
Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
SOFTWARE\Microsoft\CTF\Compatibility\msiinst.exe
System\CurrentControlSet\Control\Session Manager
Software\Microsoft\Windows\CurrentVersion\RunOnce
Software\Microsoft\CTF\LayoutIcon\0409\0000041f
SOFTWARE\Microsoft\CTF\KnownClasses
SOFTWARE\Microsoft\MpSigStub
Software\Microsoft\Cryptography
AppID
3045035B-3C14-4698-8AC4-ADB18CC42C1E
Software\Wow6432Node
Software\Microsoft\Internet Explorer\Settings
MS Shell Dlg 2
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
SOFTWARE\Microsoft\Internet Explorer\MAIN
FEATURE_IEDDE_REGISTER_PROTOCOL
PROTOCOLS\Name-Space Handler\
PROTOCOLS\Name-Space Handler\res\
PROTOCOLS\Name-Space Handler*\
MS Sans Serif
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Software\Microsoft\Windows\CurrentVersion\Uninstall\Counter-Strike Global Offensive_is1
Software\IBM\TpShocks
Software\Microsoft\Windows NT\CurrentVersion\TaskManager
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Software\Microsoft\Windows\CurrentVersion\Policies\System
Software\Microsoft\.NETFramework\Policy\
v2.0
Software\Microsoft\.NETFramework
Upgrades
Standards
AppPatch
Software\Microsoft\.NETFramework\Policy\Standards
v4.0.30319
Software\Microsoft\.NETFramework\Policy\Upgrades
SOFTWARE\WebEx\wbxtrace
Software\Microsoft\Internet Explorer\JScript9
Software\JavaSoft\Java Runtime Environment
SOFTWARE\Classes\CLSID\{F83D1872-D9FF-47F8-B5A0-49CC51E24EE8}
SOFTWARE\MiddleRush
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\UCBrowser
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
SOFTWARE\Microsoft\BidInterface\Loader
SOFTWARE\ODBC\ODBC.INI\ODBC
Software\Perl
Software\Microsoft\Windows\CurrentVersion\Policies\Network
Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes

Software\Norton\{0C55C096-0F1D-4F28-AAA2-85EF591126E7}
SOFTWARE\Microsoft\Windows\CurrentVersion
{186d55b6-3e7a-4ecf-b2fd-cf1752c37935}
SOFTWARE\InstallShield\15.0\Professional
Software\InstallShield\ISWI\7.0\SetupExeLog
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
FEATURE_MIME_HANDLING
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
FEATURE_INCLUDE_PORT_IN_SPN_KB908209
FEATURE_BUFFERBREAKING_818408
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
FEATURE_USE_CNAME_FOR_SPN_KB911149
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
FEATURE_DIGEST_NO_EXTRAS_IN_URI
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
Software\Policies\Microsoft\Internet Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
SYSTEM\CurrentControlSet\Control\FileSystem
Software\COMODO\CESM\CESM Agent
SYSTEM\CurrentControlSet\services\ccavsrv\Config
system\currentcontrolset\services\cmdagent\cisconfigs\0
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
AddressBook
Connection Manager
DirectDrawEx
Fontcore
IE40
IE4Data
IE5BAKEX
IEData
MobileOptionPack
Oracle VM VirtualBox Guest Additions
SchedulingAgent
WIC
{929FBD26-9020-399B-9A7A-751D61F0B942}
{A749D8E6-B613-3BE3-8F5F-045C84EBA29B}
{E2B51919-207A-43EB-AE78-733F9C6797C3}
{050d4fc8-5d48-4b8f-8972-47c82c46020f}
{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}
{f65db027-aff3-4070-886a-0d87064aabb1}
{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}
SOFTWARE\Nero\Internal
SOFTWARE\LAVResearch\ActualEarth\Setting
SOFTWARE
SOFTWARE\LAVResearch\ActualEarth
SOFTWARE\Microsoft\.NETFramework\policy\v1.0
SOFTWARE\Microsoft\NET Framework Setup\NDP\v1.1.4322
SOFTWARE\Microsoft\NET Framework Setup\NDP\v2.0.50727
SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.0\Setup
SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.5
SOFTWARE\Microsoft\.NETFramework\policy\v4.0
Software\ComodoGroup\CSS
SOFTWARE\CashKitten
Software\KGB Archiver
Software\Microsoft\Windows\CurrentVersion\Uninstall\Freemake Video Converter_is1
Software\Brother\BrUtilities
v2.0.50727
Software\Microsoft\Fusion
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sample
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
Internet

LocalIntranet
Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000
Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
index1c2
NI\181938c6\7950e2c5
NI\181938c6\7950e2c5\16
IL\7950e2c5\4b5f28af\5f
NI\5afff6fc\45d1ebe5
Software\Microsoft\StrongName
Software\Microsoft\Fusion\PublisherPolicy\Default
policy.2.0.System__b77a5c561934e089
NI\30bc7c4f\3f50fe4f
NI\30bc7c4f\3f50fe4f\18
IL\424bd4d8\324708cb\5c
IL\19ab8d57\c91dbb2\5e
IL\3f50fe4f\265c633d\60
policy.2.0.System.Xml__b77a5c561934e089
policy.2.0.System.Configuration__b03f5f7f11d50a3a
SOFTWARE\Microsoft\.NETFramework\Policy\APTCA
SOFTWARE\JungleNet
Software\\Microsoft\\Internet Explorer\\Styles
SOFTWARE\\Mozilla\\Mozilla Firefox
Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\Google Chrome
Software\\Microsoft\\Internet Explorer
Software\\Microsoft\\Windows\\Shell\\Associations\\UrlAssociations\\http\\UserChoice
http\\shell\\open\\command
SOFTWARE\\Microsoft\\Cryptography
SOFTWARE\{A9B2FF43-266F-478c-9D0C-CCE9311F5D6B}
Software\\Microsoft\\Windows\\CurrentVersion\\Uninstall\\{C3060724-6AC7-4BEF-B516-4F6B1D90887D
SYSTEM\\CurrentControlSet\\Services\\MBAMProtector\\Instances\\MBAMProtector Instance
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
System\Setup
Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
Content
Cookies
History
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Microsoft\Internet Explorer\Security
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
{69DC4768-446B-4F82-A6B0-63966A243064}
SOFTWARE\InstallShield\16.0\Professional
Software\Policies\Microsoft\Windows\Installer
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\A94187BE126F8404FAB6CDB5F1B1CAE7
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\A94187BE126F8404FAB6CDB5F1B1CAE7
Software\Classes\Installer\Products\A94187BE126F8404FAB6CDB5F1B1CAE7
Software\Microsoft\Advanced INF Setup
Software\Microsoft\Windows\CurrentVersion\Uninstall\hp photosmart printer series
Control Panel\International
NI\18cedf68\4edec2e5
policy.2.0.System.Windows.Forms__b77a5c561934e089
NI\61e7e666\c991064
NI\61e7e666\c991064\a
IL\475dce40\1c022996\5b
IL\2dd6ac50\553abeb3\58
IL\41c04c7e\4bf62c79\50
IL\3ced59c5\48d69eb2\54
IL\c991064\5086dba8\51
NI\3cca06a0\6dc7d4c0\b
IL\6dc7d4c0\c47ad54\56
policy.2.0.System.Drawing__b03f5f7f11d50a3a
policy.2.0.System.Deployment__b03f5f7f11d50a3a
policy.2.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
policy.2.0.Accessibility__b03f5f7f11d50a3a
policy.2.0.System.Security__b03f5f7f11d50a3a
Software\Intel\irstrt\Parameters
policy.3.5.System.Core__b77a5c561934e089
NI\7ac727df\7b5311d7
NI\7ac727df\7b5311d7\22
IL\7b5311d7\1b0ed4d\39
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IObit Uninstall_is1
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IObitUninstall
System\CurrentControlSet\Control\Session Manager\Environment

Control Panel\Mouse
Software\AutoIt v3\AutoIt
HARDWARE\DESCRIPTION\System
HARDWARE\DESCRIPTION\System\CentralProcessor\0
Software\LFG
Software\LFG\KJ
SOFTWARE\Microsoft\DirectX
SOFTWARE\Debug\quartz.dll
Software\Microsoft\Multimedia\ActiveMovie Filters\MPEG Decoder
SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
SOFTWARE\PopCap\HeavyWeapon
System\CurrentControlSet\Control\MediaResources\DirectSound\Application Compatibility\SAMPLE425818E20008FA00\
System\CurrentControlSet\Control\MediaResources\
DirectSound\
Speaker Configuration
Software\Microsoft\Cryptography\Wintrust\Config
Control Panel\Desktop
SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\sample
CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
{babe9b11-0f98-11e5-b301-806e6f6e6963}\
Drive\shellex\FolderExtensions
Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Software\Policies\Microsoft\Windows\Explorer
Software\Microsoft\Windows\CurrentVersion\Explorer
<NULL>
Advanced
Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids
Software\Microsoft\Windows\Shell\Associations\UrlAssociations\Directory
Directory
CurVer
ShellEx\IconHandler
Folder
AllFilesystemObjects
DocObject
BrowseInPlace
Clsid
Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
PropertyBag
SessionInfo\1
KnownFolders
Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Software\Microsoft\COM3
CLSID\{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}
InprocServer32
Software\Microsoft\OLE
TreatAs
System\CurrentControlSet\Services\LDAP
Software\Microsoft\Rpc
Software\Policies\Microsoft\Windows NT\Rpc
{babe9b14-0f98-11e5-b301-806e6f6e6963}\
{babe9b10-0f98-11e5-b301-806e6f6e6963}\
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
{5E6C858F-0E22-4760-9AFE-EA3317B67173}
Software\Microsoft\Windows\CurrentVersion\Uninstall\x264vfw
Software\Microsoft\Windows\CurrentVersion\Uninstall\x264vfw64
Hardware\Description\System
Software\The Silicon Realms Toolworks\Armadillo
Software\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Software\Google\Update\ClientStateMedium\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Software\Google\Update\Clients\{8BA986DA-5100-405E-AA35-86F34A02ACBF}
Software\Google\Update\ClientState\{8BA986DA-5100-405E-AA35-86F34A02ACBF}
Software\Google\Update\ClientStateMedium\{8BA986DA-5100-405E-AA35-86F34A02ACBF}
Software\Google\Update\Clients\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D}
Software\Google\Update\ClientState\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D}
Software\Google\Update\ClientStateMedium\{4DC8B4CA-1BDA-483e-B5FA-D3C12E15B62D}
Software\Google\Update\Clients\{FDA71E6F-AC4C-4a00-8B70-9958A68906BF}
Software\Google\Update\ClientState\{FDA71E6F-AC4C-4a00-8B70-9958A68906BF}
Software\Google\Update\ClientStateMedium\{FDA71E6F-AC4C-4a00-8B70-9958A68906BF}
Software\Microsoft\Windows\CurrentVersion\Explorer\Sharing
FEATURE_ENABLESAFESEARCHPATH_KB963027
Verdana
SOFTWARE\GenerousDeal

SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
FEATURE_INITIALIZE_URLACTION_SHELLEXECUTE_TO_ALLOW_KB936610
FEATURE_ZONES_DEFAULT_DRIVE_INTRANET_KB941000
FEATURE_PROTOCOL_LOCKDOWN
SOFTWARE\SearchKnow
NI\2fa8e1e8\720cc3a7
policy.3.1.Microsoft.Xna.Framework.Game__6d5c3888ef60e27d
NI\62a736a6\1a42aeed
SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Assemblies\C:|sample
Software\Microsoft\Installer\Assemblies\C:|sample
SOFTWARE\Classes\Installer\Assemblies\C:|sample
SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Assemblies\Global
Software\Microsoft\Installer\Assemblies\Global
SOFTWARE\Classes\Installer\Assemblies\Global
{29423E88-D05F-477B-A0C2-E7BB802FEB54}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Dark Souls II_R.G. Mechanics_is1
Software\Applied Networking\Hamachi
SOFTWARE\\Microsoft\\Internet Explorer\\SearchScopes
SOFTWARE\\Microsoft\\Internet Explorer\\SearchScopes\\{0633EE93-D776-472f-A0FF-E1416B8B2E3A}
Software\Blizzard Entertainment\Launcher
Software\Blizzard Entertainment\Battle.net
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-21-3979321414-2393373014-2172761192-1000\Components\6C3C47CD8BAC94C4EB81B5D1DCD091E7
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\6C3C47CD8BAC94C4EB81B5D1DCD091E7
Software\Microsoft\Office\16.0\common\filespaths
Software\Microsoft\Office
Software\Policies\Microsoft\Office
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\00006109F60000000000000000F01FEC
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\00006109F60000000000000000F01FEC
Software\Classes\Installer\Products\00006109F60000000000000000F01FEC
Software\Microsoft\Windows\CurrentVersion\Installer\UserData
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00006109F60000000000000000F01FEC\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-21-3979321414-2393373014-2172761192-1000\Components\A725889A5DF965C4E84A0253A39A5952
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\A725889A5DF965C4E84A0253A39A5952
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products
Software\Classes\Installer\Products
Software\Microsoft\Office\16.0\Common\Logging
Software\Microsoft\Office\Common
ClientTelemetry
Software\Microsoft\Office\16.0\Common\ClientTelemetry\RulesLastModified
Software\Microsoft\Office\16.0\Common\ClientTelemetry\Debug
Software\Microsoft\Office\16.0\Common\ClientTelemetry
Software\Microsoft\ClickToRun\OverRide
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate
RulesMetadata\sample
Software\Microsoft\Office\16.0\Common
Debug
System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
Software\Microsoft\Windows\CurrentVersion\Uninstall\{B023AAEF-C0D5-4949-95CE-86AF1603AD1F}_is1
{49cc0267-f581-4b60-801b-d0a8fc0708c6}
Software\Microsoft\Windows
HTML Help
Help
Software\Microsoft\Windows\CurrentVersion\Uninstall\{D9E1CADA-D103-47AE-B3F8-0C0CD0E5856E}_is1
CLSID\{09900DE8-1DCA-443F-9243-26FF581438AF}\InprocServer32
Control Panel\Desktop\WindowMetrics
SYSTEM\CurrentControlSet\Control\Nls\Language
Arial
Software\Microsoft\Internet Explorer
Software\Microsoft\Silverlight
Software\Microsoft\NET Framework Setup\NDP\v4\Full
Software\Microsoft\Microsoft Security Client
Software\Valve\Steam\ActiveProcess
Software\Valve\Steam
NI\24fa768f\41896fb4
{311dbba9-7614-4995-8a13-0f8327d869d0}
Software\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome
Software\DropboxUpdate\UpdateDev\
Software\DropboxUpdate\Update\
Software\DropboxUpdate\Update\ClientState\
Software\DropboxUpdate\Update\network\secure
Software\DropboxUpdate\Update\Clients\{D8968FF2-E0B1-4A13-A3E2-C9F2995F3BC6}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Total CMA Pack
Microsoft Sans Serif

Software\Microsoft\Windows NT\CurrentVersion
Software\Google\Update\
Software\Google\UpdateDev\
Software\Google\Update\ClientState\
Software\Google\Update\ClientStateMedium\{74AF07D8-FB8F-4D51-8AC7-927721D56EBB}
Software\Google\Update\Clients\{430FD4D0-B729-4F61-AA34-91526481799D}
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.avi\UserChoice
SOFTWARE\ESET
SOFTWARE\AVAST Software
Software\Microsoft\.NETFramework\Policy\AppPatch
v2.0.50727.00000
sample
{62AB5D82-FDC1-4DC3-A9DD-070D1D495D97}
Software\Microsoft\Windows NT\CurrentVersion\ProfileList
Software\Microsoft\Windows\CurrentVersion\App Paths\sample.exe
Software\PhotoFiltre Studio X\10.0\{46534E5A-3039-3534-3336-323830384554}
CLSID\{9C4197CE-5F5D-4DFA-AB9D-804449BAC1BA}
.pfi
.pfs
.pfv
System
Software\Mozilla
SOFTWARE\SearchMyWindow
Software\Microsoft\Windows\CurrentVersion\Uninstall\SecureVPN Client
Software\Microsoft\Windows\CurrentVersion\Uninstall\{A306FD29-7D3A-4287-91AC-9A0180931395}_is1
SOFTWARE\WildTangent\InstalledSKUs\
Software\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
DVD\shell\Play Using DVDExpress\command
Software\Microsoft\keyboard\Native Media Players\windvd
Software\Margi_Systems\DVD-to-Go\DVDPlayer
Software\Classes\DVD\shell\PlayWithPowerDVD\command
DVD\shell\Play\command
Software\Microsoft\Windows\CurrentVersion\Uninstall\Call of Duty Ghosts_is1
Trebuchet MS
SOFTWARE\GetTheResultsHub
SOFTWARE\ej-technologies\exe4j\temp\
SOFTWARE\JavaSoft\Java Development Kit
SOFTWARE\JavaSoft\Java Runtime Environment
SOFTWARE\JavaSoft\Java Runtime Environment\
SOFTWARE\ej-technologies\exe4j\locatedjvms\
SOFTWARE\Bandisoft Archive Password Recovery
Software\NCH Software\ClassicFTP\Settings
Software\NCH Software\ClassicFTP\Software
Software\NCH Software\ClassicFTP\Registration
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.html\UserChoice
http\shell\open\command
Software\Microsoft\Registration\NCH
Software\NCH Software\Fling\Settings
Software\NCH Software\ExpressBurn\Settings
Software\NCH Swift Sound\ExpressBurn\Settings
Software\NCH Software\VideoPad\Settings
Software\NCH Software\Pixillion\Settings
software\microsoft\windows\currentversion\app paths\chrome.exe
Software\NCH Software\Components\Chrome
{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}
{905E63B6-C1BF-494E-B29C-65B732D3D21A}
{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}
{82A5EA35-D9CD-47C5-9629-E15D2F714E6E}
{C4AA340D-F20F-4863-AFEF-F87EF2E6BA25}
{A4115719-D62E-491D-AA7C-E74B8BE3B067}
{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}
{ED4824AF-DCE4-45A8-81E2-FC7965083634}
{B6EBFB86-6907-413C-9AF7-4FC2ABF07CC5}
{2400183A-6185-49FB-A2D8-4A392A602BA3}
{B97D20BB-F46A-4C97-BA10-5E3608430854}
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}
{FDD39AD0-238F-46AF-ADB4-6C85480369C7}
{33E28130-4E1E-4676-835A-98395C3BC3BB}
{18989B1D-99B5-455B-841C-AB7C74E4DDFC}
SOFTWARE\DirectShowFilters\MadVR
CLSID\{00BB2765-6A77-11D0-A535-00C04FD7D062}
CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}
CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}
CLSID\{03C036F1-A186-11D0-824A-00AA005B4383}\InProcServer32
CLSID\{00BB2763-6A77-11D0-A535-00C04FD7D062}\InProcServer32
CLSID\{807C1E6C-1D00-453F-B920-B61BB7CDD997}
SOFTWARE\Userator

Software\Toshiba\BluetoothStack\V1.0\AutoRegist
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\E0E469B53A9B6724E99DD4A5750247A7
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\E0E469B53A9B6724E99DD4A5750247A7
Software\Classes\Installer\Products\E0E469B53A9B6724E99DD4A5750247A7
SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\21EE4A31AE32173319EEFE3BD6FDFFE3
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\21EE4A31AE32173319EEFE3BD6FDFFE3
Software\Classes\Installer\Products\21EE4A31AE32173319EEFE3BD6FDFFE3
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\22BEFC8F7E2A1793E9ADB411DEFE1C58
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\22BEFC8F7E2A1793E9ADB411DEFE1C58
Software\Classes\Installer\Products\22BEFC8F7E2A1793E9ADB411DEFE1C58
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\62DBF9290209B993A9A757D1160F9B24
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\62DBF9290209B993A9A757D1160F9B24
Software\Classes\Installer\Products\62DBF9290209B993A9A757D1160F9B24
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\6E8D947A316B3EB3F8F540C548BE2AB9
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\6E8D947A316B3EB3F8F540C548BE2AB9
Software\Classes\Installer\Products\6E8D947A316B3EB3F8F540C548BE2AB9
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\91915B2EA702BE34EA8737F3C976793C
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\91915B2EA702BE34EA8737F3C976793C
Software\Classes\Installer\Products\91915B2EA702BE34EA8737F3C976793C
CLSID\{000C101D-0000-0000-C000-000000000046}\DllVersion
SOFTWARE\Microsoft\Net Framework Setup\NDP\v2.0.50727
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Client
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
Software\Microsoft\Windows NT\CurrentVersion\DRIVERS32
Software\Microsoft\Windows NT\CurrentVersion\Installable Compressors
Software\Magix\Common\Database\FABS
{D17E056B-A8D1-4433-9CE9-58095900F900}
SOFTWARE\PassandPlay
SOFTWARE\Microsoft\Internet Explorer
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Software\Classes\CLSID\{F67F4C79-31E0-4b8b-A631-C0D1D83B23B1}
SOFTWARE\MetaQuotes Software
Software\WinRAR\General
SOFTWARE\Classes
.386
.a
.ai
.aif
.aifc
.aiff
.ani
.ans
.application
.appref-ms
.aps
.art
.asa
.asc
.ascx
.asf
.asm
.asmx
.asp
.aspx
.asx
.au
.avi
.bas
.bat
.bcp
.bin
.bkf
.blg
.bmp
.bsc
.c
.cab
.camp
.cat
.cc
.cda

.cdmp
.cdx
.cer
.cgm
.chk
.chm
.cls
.cmd
.cod
.com
.compositefont
.contact
.cpl
.cpp
.crd
.crds
.crl
.crt
.cs
.csa
.csproj
.css
.csv
.cur
.cxx
.dat
.db
.dbg
.dbs
.dct
.def
.der
.desklink
.diagcab
.diagcfg
.diagpkg
.dib
.dic
.diz
.dll
.dl_
.doc
.docx
.dos
.dot
.drv
.dsn
.dsp
.dsw
.dwfx
.easmx
.edrwx
.emf
.eprtx
.eps
.etp
.evt
.evtx
.exe
.exp
.ext
.ex_
.eyb
.faq
.fif
.fky
.fnd
.fnt
.fon
.gadget
.ghi
.gif
.gmmp
.group
.grp
.gz
.h

.H1C
.H1D
.H1F
.H1H
.H1K
.H1Q
.H1S
.H1T
.H1V
.H1W
.hdp
.hhc
.hlp
.hpp
.hqx
.hta
.htc
.htm
.html
.htt
.htw
.htx
.hxx
.i
.ibq
.icc
.icl
.icm
.ico
.ics
.idl
.idq
.ilk
.imc
.img
.inc
.inf
.ini
.inl
.inv
.inx
.in_
.iso
.IVF
.jav
.java
.jbf
.jfif
.jnt
.Job
.jod
.jpe
.jpeg
.jpg
.js
.JSE
.jtp
.jtx
.jxr
.kci
.label
.latex
.lgn
.lib
.library-ms
.lnk
.local
.log
.lst
.m14
.m1v
.m3u
.m4a
.mak
.man
.manifest
.mapimail
.mht

.mhtml
.mid
.midi
.mig
.mk
.mlc
.mmf
.mov
.movie
.mp2
.mp2v
.mp3
.mpa
.mpe
.mpeg
.mpg
.mpv2
.msc
.msg
.msi
.msp
.msrcincident
.msstyles
.msu
.mv
.mydocs
.ncb
.nfo
.nls
.nvr
.obj
.ocx
.oc_
.odc
.odh
.odl
.odt
.osdx
.otf
.p10
.p12
.p7b
.p7c
.p7m
.p7r
.p7s
.partial
.pbk
.pch
.pdb
.pds
.perfmoncfg
.pfm
.pfx
.php3
.pic
.pif
.pko
.pl
.plg
.pma
.pmc
.pml
.pmr
.pnf
.png
.pot
.pps
.ppt
.prc
.prf
.printerExport
.ps
.ps1
.ps1xml
.psc1
.psd
.psd1

.psm1
.py
.pyc
.pyo
.pyw
.qds
.rat
.rc
.rc2
.rct
.RDP
.reg
.res
.resmoncfg
.rgs
.rle
.rll
.rmi
.rpc
.rsp
.rtf
.rul
.s
.sbr
.sc2
.scc
.scd
.scf
.sch
.scp
.scr
.sct
.search-ms
.searchConnector-ms
.sed
.sfcache
.shtm
.shtml
.sit
.slupkg-ms
.snd
.sol
.sor
.spc
.sql
.srf
.sr_
.sst
.stl
.stm
.svg
.swf
.sym
.sys
.sy_
.tab
.tar
.tdl
.text
.tgz
.theme
.themepack
.tif
.tiff
.tlb
.tlh
.tli
.trg
.tsp
.tsv
.ttc
.ttf
.txt
.udf
.UDL
.udt
.URL
.user

.usr
.VBE
.vbproj
.vbs
.vbx
.vcf
.vcproj
.viw
.vspscc
.vsscc
.vssscc
.vxd
.wab
.wav
.wax
.wbcat
.wcx
.wdp
.webpnp
.website
.wll
.wlt
.wm
.wma
.wmf
.wmp
.wmv
.wmx
.wmz
.wpl
.wri
.wsc
.WSF
.WSH
.wsz
.wtx
.wvx
.x
.xaml
.xbap
.xht
.xhtml
.xix
.xlb
.xlc
.xls
.xlt
.xml
.xps
.xrm-ms
.xsd
.xsl
.xslt
.z
.z96
.zfsendtotarget
.zip
MIME\Database\Content Type
application/atom+xml
application/fractals
application/hta
application/mac-binhex40
application/opensearchdescription+xml
application/pkcs10
application/pkcs7-mime
application/pkcs7-signature
application/pkix-cert
application/pkix-crl
application/postscript
application/rss+xml
application/vnd.ms-pki.certstore
application/vnd.ms-pki.pko
application/vnd.ms-pki.seccat
application/vnd.ms-pki.stl
application/vnd.ms-xpsdocument
application/x-complus
application/x-compress
application/x-compressed

application/x-gzip
application/x-informationCard
application/x-jtx+xps
application/x-latex
application/x-mix-transfer
application/x-ms-application
application/x-ms-license
application/x-ms-xbap
application/x-mswebsite
application/x-pkcs12
application/x-pkcs7-certificates
application/x-pkcs7-certreqresp
application/x-stuffit
application/x-tar
application/x-troff-man
application/x-x509-ca-cert
application/x-zip-compressed
application/xaml+xml
application/xhtml+xml
application/xml
audio/mp3
audio/x-ms-wma
image/bmp
image/gif
image/jpeg
image/pjpeg
image/png
image/svg+xml
image/tiff
image/vnd.ms-dds
image/vnd.ms-photo
image/x-emf
image/x-icon
image/x-jg
image/x-png
image/x-wmf
message/rfc822
model/vnd.dwfx+xps
model/vnd.easmx+xps
model/vnd.edrwx+xps
model/vnd.eprtx+xps
pkcs10
pkcs7-mime
pkcs7-signature
pkix-cert
pkix-crl
text/css
text/html
text/plain
text/scriptlet
text/x-component
text/x-ms-contact
text/x-scriptlet
text/x-vcard
text/xml
video/mpeg
video/x-mpeg
video/x-ms-asf
video/x-msvideo
vnd.ms-pki.certstore
vnd.ms-pki.pko
vnd.ms-pki.seccat
vnd.ms-pki.stl
x-pkcs12
x-pkcs7-certificates
x-pkcs7-certreqresp
x-x509-ca-cert
Software\DownloadManager\
SOFTWARE\NVIDIA Corporation\Logging\Definitions\LogManagers\FileOut
SOFTWARE\NVIDIA Corporation\Logging\Definitions\LogFilters\PassFilter
SOFTWARE\NVIDIA Corporation\Logging
SOFTWARE\NVIDIA Corporation
SOFTWARE\Microsoft\Windows\CurrentVersion\Setup
SOFTWARE\Microsoft\Office\8.0\Common\InstallRoot
SOFTWARE\Microsoft\Office\9.0\Common\InstallRoot
SOFTWARE\Borland\Database Engine
SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots
SOFTWARE\Ethalone\Ghost Installer\2.0

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MMEDICA
SOFTWARE\Microsoft\Office
Software\Google\ChromeFrame
SOFTWARE\EPSON\STM3
Software\Microsoft\Office\16.0\Common\Debug
SOFTWARE\Microsoft\Office\16.0\Common\OEM
SOFTWARE\Wow6432Node\Microsoft\Office\16.0\Common\OEM
Software\Microsoft\Office\ClickToRun\Configuration
Software\Microsoft\Office\16.0\Registration\{D7279DD0-E175-49FE-A623-8FC2FC00AFC4}
Software\Wow6432Node\Microsoft\Office\16.0\Registration\{D7279DD0-E175-49FE-A623-8FC2FC00AFC4}
Software\Microsoft\Office\ClickToRun\propertyBag
Software\Policies\Adobe\FlashPlayer\FeatureLockDown
Software\Policies\Adobe\FlashPlayer\11.0\FeatureLockDown
{25712BD5-78C7-4920-8060-EA1CB3CEF5F1}
SOFTWARE\Xfire
Software\Microsoft\Windows\CurrentVersion\Uninstall\DirectXDrivers
Software\Microsoft\Direct3D\Drivers
ISlogit
\OBJID\{740AB61D-8B4A-46CC-9D82-86F72E055477}
\OBJID\{9958D891-C319-4C6C-BEB9-F9BFB37EA493}
\OBJID\{3F05A321-43B7-4578-93C8-CDC5F64A149A}
\OBJID\{31324564-3B13-4533-8999-33990688F5A9}
\OBJID\{4FDA34C1-9899-494C-A33D-72BA6BB0F4FD}
\OBJID\{4FDA34C2-9899-494C-A33D-72BA6BB0F4FD}
\OBJID\{4FDA34C3-9899-494C-A33D-72BA6BB0F4FD}
\OBJID\{4FDA34C4-9899-494C-A33D-72BA6BB0F4FD}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Unlocker
.DEFAULT\Volatile Environment
S-1-5-19\Volatile Environment
S-1-5-20\Volatile Environment
S-1-5-21-3979321414-2393373014-2172761192-1000\Volatile Environment
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Classes\http\shell\open\command
{6EF03755-68A4-4b3e-BEF0-4A495C15B825}
{279ecae6-e782-49de-806d-69549432f81f}
Software\AVAST Software\Avast
SOFTWARE\Freedom Scientific\JAWS
SOFTWARE\NVDA
SOFTWARE\AVAST Software\Avast
Hardware\Description\System\CentralProcessor\0
Software\Wilson WindowWare\Settings\WWW-PROD\WB44I
Software\Wilson WindowWare\Settings\WWWBATCH\MAIN
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\
"SYSTEM\CurrentControlSet\Enum\ACPI\"
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Software\TutoTag
SOFTWARE\Microsoft\Cryptography
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\rec_gb_215_is1
Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders
Software\Microsoft\.NETFramework\Policy
Software\Microsoft\.NETFramework\policy\v2.0
SOFTWARE\Microsoft\NET Framework Setup\NDP
SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.0
Software\KMSPico 10.0.6
Software\ShopperPro
{9ce75088-34b2-413f-8535-579044159521}
Software\SogouWallPaper
SoftWare
Software\Microsoft\DirectDraw\Compatibility
Bug!
DemolitionDerby2
Diablo
MortalKombat3
MsGolf98
NHLPowerPlay
NortonSystemInfo
Rogue Squadron
Savage
ScorchedPlanet
SilentThunder
StarCraft100
StarCraft115
StarCraftDemo
Terracide
ThirdDimension
ZiffDavisQualityBenchmark
ZiffDavisWinMarkBenchmark

Software\Microsoft\DirectDraw\GammaCalibrator
Software\Microsoft\DirectDraw
Software\Microsoft\Direct3D
SYSTEM\CurrentControlSet\Services\crypt32
SOFTWARE\Microsoft\Windows NT\CurrentVersion\msasn1
System\CurrentControlSet\Control\Video\{B285A319-4BD4-4785-A840-9BDC49C97EFA}\0000
{1269A29A-DA0B-4791-A35B-F7B7E84FA79B}
SOFTWARE\IBM\Java2 Runtime Environment
SOFTWARE\IBM\Java Development Kit
Software\Policies\Microsoft\Internet Explorer\TabbedBrowsing
Software\Microsoft\Internet Explorer\TabbedBrowsing
{f2111ef1-fbe5-4370-85a6-4ceee56af79a}
SOFTWARE\Ambon
Word.Document.6\DefaultIcon
Word.Document.7\DefaultIcon
Word.Document.8\DefaultIcon
Word.Document.9\DefaultIcon
Word.Document.10\DefaultIcon
Word.Document.8
SOFTWARE\CLASSES\scrfile
scrfile\shell\open
SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\HideFileExt
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Folder\SuperHidden
PROTOCOLS\Name-Space Handler\http\
FEATURE_BROWSER_EMULATION
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
Pre Platform
Post Platform
FEATURE_MAXCONNECTIONSPERSERVER
FEATURE_MAXCONNECTIONSPER1_0SERVER
FEATURE_URLMON_IQDA_SIZE
SOFTWARE\Microsoft\Windows\CurrentVersion\UrlMon Settings
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Parental Controls\users\S-1-5-21-3979321414-2393373014-2172761192-1000
SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
SYSTEM\CurrentControlSet\services\Avg\SystemValues
SOFTWARE\TrendMicro\Vizor
Software\Microsoft\MSDTC\Tracing
Sources
Output
SOFTWARE\SearchWebKnow
Software\Policies\Microsoft\Windows\Directory UI
SOFTWARE\InstallShield\17.0\Professional
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\14ea90d3982f5dc4f9e08c4dbc803495
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\14ea90d3982f5dc4f9e08c4dbc803495
Software\Classes\Installer\Products\14ea90d3982f5dc4f9e08c4dbc803495
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\14ea90d3982f5dc4f9e08c4dbc803495\InstallProperties
SYSTEM\CurrentControlSet\Services\
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
.DEFAULT
Blizzard
Software\Blizzard Entertainment\Blizzard Error
Meiryo
{bdd1eed2-cb3a-4308-ae94-cc92cea53ac5}
SOFTWARE\InnovateDirect
Software\Microsoft\Windows\CurrentVersion\App Paths\MediaInfo.exe

CreateMutex

<NULL>
Local\Opera/Installer/UI_lock
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
WSjuQKBxmd_mut
Windows Volume App Window
Local\WinSpl64To32Mutex_21ff4_0_3000
IBMTpShocksMutexToAvoidMultiInstance
NTShell Taskman Startup Mutex
WBXTRA_TRACE_MUTEX
WBXTRA_TRACE_MUTEX_EX
Global\MiddleRush
Global\StrongSignal

Global\SearchWebKnow
Global\IIF-{3E29EE6C-963A-4aae-86C1-DC237C4A49FC}
Global\CashKitten
VirtuaWinPreventSecond
Global\JungleNet
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\MidiMapper_modLongMessage_RefCnt
sample
{994CA59C-8C88-4322-8DBC-264F3E3E3C6E}
DownloaderXYZ-Default
AMResourceMutex3
MutexNPA_UnitVersioning_2320
_handy_client
WIN7LDRMU
uxJLpe1m
Kivp Kopnurlh
HeavyWeaponMutex
Local__DDrawExclMode__
Local__DDrawCheckExclMode__
Local\DDrawWindowListMutex
Local\DDrawDriverObjectListMutex
Global_no_copies
ASUSGPUFanService
RAL16CECBCC
Global\C:/Users/win7/AppData/Local/Temp/chrome_installer.log
Global\GenerousDeal
E66DAB12-3AD4-4885-A5C6-C1F32EA6F7D2
Global\SearchKnow
t "Total CMA Pack 0.58"
T
RasPbFile
{921ABDC1-6599-4A82-E4D5-EA06D22188F9}
SpoolerMutex
AresGlbMtx_win7
HngSync_Running
Global\SearchMyWindow
Global\{4B5DC379-ED06-4552-A736-414A1570C24F}_bhelper_mutex0
Global\GetTheResultsHub
Local\samplelock
Local\sampleRestartlock
Global\IIF-{F0E3AD40-2BBD-4360-9C76-B9AC9A5886EA}
TD_C0200A8E-FD06-433d-9554-2D9941841965
Bootstrap_log_mutex
Bootstrap_mutex_369E21C2_C926_4312_B104_96A7F9408CBF
MRL Keybd
MRL Mouse
Global\MSILOG_26b80ebe1d190d6gol.00000hcraeSxednaY_pmeT_lacoL_ataDppA_7niw_sresU_:C
Angry Angel v3.0
Global_MSIExecute
Global\PassandPlay
Global\67EDCA7F9C0E41A5A7E9B3CEF667CA19C:/sample
CMainDlg::m_bProdInstallComplete
CMainDlg::m_bDownloadLockedIn
CMainDlg::m_bCanConfirmExit
Global\223CEB62-A2BC-4E33-BA9B-FCAC6DAAB1BE
m_wndDummyAPIMsgWindow
CWebConfigFactory::m_pWebConfig
CRequestSettings::m_strUrlHost
CRequestSettings::m_mapQueryValues
CRequestSettings::m_bAddNoCacheHeader
CRequestSettings::m_bFileDownload
CRequestSettings::m_nTimeoutSecs
CRequestSettings::m_nMaxRetries
CRequestSettings::m_bMoveParamsToPostBody
CRequestSettings::m_strUserAgent
CRequestManager::m_aRequestPools
CMyHttpRequest::m_enStatus
CMyHttpRequest::m_bIsDeleting
{87DDA23F-A0D7-417B-96D5-8607DE5F64FF}m_aObservers
CRequestPool::CanStartNewRequest
CRequestPool::m_nActiveRequests
CRequestPool::m_nMaxRequests
CRequestSettings::GetFormatedUrlString
CRequestSettings::m_pszPostData
CServerRequest::m_strBufferRead
CServerRequest::m_strHeaderBuffer
CMyHttpRequest::m_bRequestWasAborted

CMyHttpRequest::m_requestProgress
CRequestProgress::m_n64ResumePos
CRequestProgress::m_ullBytesDownloaded
CRequestProgress::m_ullBytesTotal
CRequestProgress::m_tmStart
CMyHttpRequest::m_hProgressWaitEvent
CMyHttpRequest::m_hProgressThread
CMyHttpRequest::m_hRequestThread
CProxySettings::GetProxyForURL
HKAB32DBA6DDE1
PowerForPhone
DEFINED_LoadSDKDLL
CRemoteProcApiCalls::m_bShowLoadingScreen
CRemoteProcApiCalls::m_nMaxLoadingScreenOffers
Global\426F00E8-A1B3-4EB2-8FF8-0950920F5D6E
DEFINED_SetCmdLineValuesW
DEFINED_SetNoCandy
DEFINED_GetNoCandy
Global\InternetExplorerInstaller
MMEDICA setup
Global\C:/debug.log
{100184D2-BDC3-477a-B8D3-65548B67914C}_996
.NET CLR Data_Perf_Library_Lock_PID_b90
.NET CLR Networking_Perf_Library_Lock_PID_b90
.NET Data Provider for Oracle_Perf_Library_Lock_PID_b90
.NET Data Provider for SqlServer_Perf_Library_Lock_PID_b90
.NETFramework_Perf_Library_Lock_PID_b90
BITS_Perf_Library_Lock_PID_b90
ESENT_Perf_Library_Lock_PID_b90
Lsa_Perf_Library_Lock_PID_b90
MSDTC_Perf_Library_Lock_PID_b90
MSDTC Bridge 3.0.0.0_Perf_Library_Lock_PID_b90
MSSCNTRS_Perf_Library_Lock_PID_b90
PerfDisk_Perf_Library_Lock_PID_b90
PerfNet_Perf_Library_Lock_PID_b90
PerfOS_Perf_Library_Lock_PID_b90
PerfProc_Perf_Library_Lock_PID_b90
rdyboost_Perf_Library_Lock_PID_b90
RemoteAccess_Perf_Library_Lock_PID_b90
ServiceModelEndpoint 3.0.0.0_Perf_Library_Lock_PID_b90
ServiceModelOperation 3.0.0.0_Perf_Library_Lock_PID_b90
ServiceModelService 3.0.0.0_Perf_Library_Lock_PID_b90
SMSvcHost 3.0.0.0_Perf_Library_Lock_PID_b90
Spooler_Perf_Library_Lock_PID_b90
TapiSrv_Perf_Library_Lock_PID_b90
Tcpip_Perf_Library_Lock_PID_b90
TermService_Perf_Library_Lock_PID_b90
UGatherer_Perf_Library_Lock_PID_b90
UGTHRSVC_Perf_Library_Lock_PID_b90
usbhub_Perf_Library_Lock_PID_b90
Windows Workflow Foundation 3.0.0.0_Perf_Library_Lock_PID_b90
WmiApRpl_Perf_Library_Lock_PID_b90
WSearchIdxPi_Perf_Library_Lock_PID_b90
Global\LOADPERF_MUTEX
{7DD04E32-4A4C-8D26-BCE0946C931C}
Global\{50340165-E10A-43f1-8D04-62A5A078CD4A-InstallGui}
Global\mchMixCache$7a8
BELARUS-VIRUS-MAKER
t "SOGOU_WALLPAPER_INSTALLING_MUTEX"
S
11710477410094284_BCS
DirectX Setup
{3921c523-f10a-9a46-635a-c40bc6dca23c}
{CE0B4DC02123-B391E3C7-A2A3-4D2F-9DC8}
EA63CFB9-62E6-4912-A1C5-AD8C4E1C5D05
C:\sample
EAInstallerV1Setup
Knight Online
pctdavjpctdavjpctdavjpctda
Global\InnovateDirect

LoadLibrary

kernel32.dll
gdi32.dll

user32.dll
C:\Windows\system32\uxtheme.dll
dwmapi.dll
ADVAPI32.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTBASE.dll
OLEAUT32.dll
KERNEL32.DLL
COMCTL32.dll
CRYPT32.dll
GDI32.dll
gdiplus.dll
MSIMG32.dll
ole32.dll
PSAPI.DLL
Secur32.dll
SHLWAPI.dll
USER32.dll
USERENV.dll
WININET.dll
WINMM.dll
WINTRUST.dll
SHELL32.dll
ntmarta.dll
Advapi32.dll
Msftedit.dll
UxTheme.dll
IMM32.dll
comctl32
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
WindowsCodecs.dll
SspiCli.dll
C:\sample
comctl32.dll
imm32.dll
RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-A432R.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-A432R.tmp\sample.EN
uxtheme.dll
shell32.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\VclStylesInno.dll
user32
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\bp.ENU
C:\Users\win7\AppData\Local\Temp\is-UC9GT.tmp\bp.EN
shlwapi.dll
C:\Windows\system32\UXTHEME.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\SETUPAPI.dll
advapi32.dll
C:\Windows\system32\SHFOLDER.dll
propsys.dll
C:\Windows\system32\RichEd20.dll
NTDLL.dll
winmm.dll
NTDLL
WS2_32.dll
KERNEL32.dll
WTSAPI32.dll
MSACM32.dll
WINHTTP.dll
IPHLPAPI.DLL
ADVAPI32.DLL
COMCTL32.DLL
GDI32.DLL
OLE32.DLL
SHELL32.DLL
USER32.DLL

riched32.dll
riched20.dll
imageres.dll
SHFOLDER
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp\System.dll
RichEd20
C:\Windows\system32\kernel32.dll
CRYPTSP.dll
msimg32.dll
psapi.dll
Kernel32.dll
C:\1.7.3.9\Awesomium.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
urlmon.dll
PROPSYS.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
wininet.dll
COMCTL32
KERNEL32
C:\Users\win7\AppData\Local\Temp\is-9HAUJ.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-9HAUJ.tmp\sample.EN
winspool.drv
RPCRT4.dll
User32.dll
\MUI\0409\TpShocks.dll
Sensor.dll
C:\Windows\system32\jscript9.dll
C:\Users\win7\AppData\Local\Temp\is-NCR66.tmp_isetup_shfoldr.dll
C:\Windows\system32\imageres.dll
winhttp.dll
C:\Windows\system32\odbcint.dll
MSVCRT.DLL
colorui.dll
dinput.dll
comdlg32.dll
compstui.dll
inetres.dll
UXTHEME
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
c:\windows\system32\imageres.dll
SHELL32
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\perl514.dll
msvcrt.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\d1e7c33431cd8713f2ce3582829a8b14\Socket.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\c5cce8d16a1bd48692b421dcf46d3396\Util.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\7ef0d901bf4203fbcf7a0fff0e82aa5f\Encode.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\d10c2c06ba2044cccc247c4315f5c7d3\Process.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\60ff464e01c2cd5526dbdad5a125081d\Dumper.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\4461f48e31bde5c56b31b973b773de09\List.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\eaeabd54205de2f10c00aea80bbf0d83\Registry.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\3a7ccbf8181ee5a145227a6dfce3594c\WinError.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\31638f63e39b38d3e250a9a57cb9d1c5\Cwd.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\f233f63b6654362865c7577442edb9e3\Win32.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\5ffd05b2cbd58528e56519784ca9c869\Hostname.dll
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\df1ba73f49c38cbbc7a11c779c3506d2\OLE.dll
OLE32
C:\Users\win7\AppData\Local\Temp\pdk-win7-2728\32785c19dc6898fbbbf06f3b776edd08\Fcntl.dll
C:\sampleENU.dll
C:\sampleLOC.dll
C:\Windows\system32\DBGHELP.DLL
VERSION.dll
C:\Windows\system32\KERNEL32.DLL
SXS.DLL
C:\Windows\system32\asycfilt.dll
Mi_UniTamilStdKeybDriver.dll
gdi32
oleaut32.dll
C:\Users\win7\AppData\Local\Temp\nsk8B61.tmp\inetc.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-core-synch-l1-2-0
kernel32
api-ms-win-core-fibers-l1-1-1
advapi32
api-ms-win-core-localization-l1-2-1

api-ms-win-appmodel-runtime-l1-1-1
ext-ms-win-kernel32-package-current-l1-1-0
GLU32.dll
OPENGL32.dll
Riched20.dll
C:\Windows\SysWOW64\msls31.dll
NETAPI32.DLL
C:\Windows\system32\iphlpapi.dll
cmdhtml.dll
SYNSOACC.DLL
WINMM.DLL
MSACM32.DLL
DDRAW.DLL
DCIMAN32.DLL
MSVFW32.DLL
AVICAP32.DLL
MSVCRT40.DLL
OLEPRO32.DLL
MFC42.DLL
MSVCRT20.DLL
SETUPAPI.DLL
comdlg32.DLL
version.dll
hcwsnbd9.dll
hcwutl32.dll
hcwhook.dll
hcwChan.dll
btgpio32.dll
hcwpnp32.dll
hcwtuner.dll
hcwaud32.dll
bt848_32
btvid_32
hcwAV.dll
hcwTVWnd.dll
hcwtvdlg.dll
bt848wst.dll
wintvocx.ocx
hcwtvctl.dll
Hcwsnap.ax
hcwSnapShot.ax
HCWCapt.ax
hcwMPEGSPlitter.ax
hcwSoloCap.ax
hcwslipFR.ax
hcwslipWriter.ax
iviaudio.ax
ivivideo.ax
hcwi2c32.dll
C:\Users\win7\AppData\Local\Temp\is-V4OI1.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-V4OI1.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-4CIEK.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-4CIEK.tmp\sample.EN
C:\Windows\system32\CRTDLL.DLL
COMDLG32.DLL
CRTDLL.DLL
MPR.DLL
WS2_32.DLL
bass.dll
C:\Windows\system32\dsound.dll
C:\Windows\system32\shell32.dll
BrLogAPI.dll
BrDbgOut.dll
BrDbgOtW.dll
twain_32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
AdvApi32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.ni.dll
DNSAPI.dll
dhcpcsvc.DLL
Comctl32.dll
C:\Windows\system32\ws2_32
msi.dll

Advpack.dll
wtsapi32.dll
WINSTA.dll
C:\Testy.exe
IMM32.DLL
OLE32.dll
C:/Users/win7/AppData/Local/Temp/BRBC76.tmp
OLEACCRC.DLL
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\GDIPLUS.DLL
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\5a401fd2a7689ff13fb54182953f9c40\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\6949c4470a81970ec3de0a575d93babc\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Core\63e9d5c341d64a753cde97f5a3d65c71\System.Core.ni.dll
C:\Users\win7\AppData\Local\Temp\is-5H3CT.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-5H3CT.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-S1NB8.tmp_isetup_shfoldr.dll
exchndl.dll
C:\Users\win7\AppData\Local\Temp\is-M3KRK.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-M3KRK.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-B6UKO.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-B6UKO.tmp_isetup_isdecmp.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
MMDevAPI.DLL
wdmaud.drv
MMDEVAPI.DLL
SETUPAPI.dll
AUDIOSES.DLL
msacm32.drv
midimap.dll
C:\Windows\system32\WINMM.dll
CFGMGR32.dll
MPR.dll
WSOCK32.dll
ntdll.dll
C:\Windows\System32\shdocvw.dll
C:\ProgramData\WebEx\ieatgpc.dll
c:\sample\ieatgpc.dll
C:\Users\win7\AppData\LocalLow\WebEx\ieatgpc.dll
C:\Users\win7\AppData\Local\WebEx\ieatgpc.dll
ShFolder.DLL
C:\Users\win7\AppData\Local\Temp\HTM9D3D.tmp
COMDLG32.dll
UXTHEME.DLL
wsock32.dll
ws2_32.dll
mswsock.dll
olepro32.dll
iphlpapi.dll
Kernel32
ComCtl32
psapi
shell32
User32
RICHED32.DLL
RICHED20.DLL
msftedit
SPPCommon.dll
t "C:\Users\win7\AppData\Local\Temp\McCSPInstall.dll"
C:\Users\win7\AppData\Local\Temp\nsv879C.tmp\System.dll
NETAPI32.dll
oledlg.dll
WINSPOOL.DRV
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
C:\Windows\System32\msxml3r.dll
feclient.dll
Comctl32
mscms.dll
icm32.dll
C:\Users\win7\AppData\Local\Temp\nso99F2.tmp\System.dll
ddraw.dll
dsound.dll
mscat32.dll
wintrust.dll
D3DIM700.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
mscorsec.dll

WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
ncrypt.dll
bcrypt.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
profapi.dll
C:\Windows\System32\msxml6r.dll
Wininet.dll
Vender.dll
C:\Users\win7\AppData\Local\Temp\nsj67F5.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp\InstallOptions.dll
MSVFW32.dll
netutils.dll
api-ms-win-downlevel-shell32-l1-1-0.dll
C:\Users\win7\AppData\Local\Temp\is-159AI.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-159AI.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-KQSHV.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-KQSHV.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\nsyB9F.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-B15KQ.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-B15KQ.tmp\sample.EN
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
C:\Users\win7\AppData\Local\Temp\is-UAJ2G.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-UAJ2G.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innocallback.ENU
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innocallback.EN
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\innoextractor.dll
C:\Users\win7\AppData\Local\Temp\is-80RRU.tmp\bassmusic.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\culture.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en-US\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\en\mscorrc.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorrc.dll
C:\Users\win7\AppData\Local\Temp\is-TE17K.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-TE17K.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-1JDD1.tmp\ISDone.dll
C:\Windows\winhlp32.exe
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\UAC.dll
AdvAPI32
SECUR32
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp\InstallOptions.dll
Normaliz.dll
NSI.dll
API-MS-WIN-Service-Management-L2-1-0.dll
C:\Users\win7\AppData\Local\Temp\is-QNTCR.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-QNTCR.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-3KHPE.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\is-LT5S1.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-LT5S1.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-IOJPA.tmp\GCountry.dll
C:\Windows\system32\VB6ES.DLL
C:\Users\win7\AppData\Local\Temp\is-3P2CL.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-3P2CL.tmp\sample.EN
VERSION.DLL
C:\Users\win7\AppData\Local\Temp\qag7A3.tmp
WSOCK32.DLL
C:\Users\win7\AppData\Local\Temp\qag7A3.ENU
C:\Users\win7\AppData\Local\Temp\qag7A3.EN
SensApi.dll
C:\Users\win7\AppData\Local\Temp\GUMAA9A.tmp\goopdate.dll

dbghelp.dll
rpcrt4.dll
C:\Users\win7\AppData\Local\Temp\GUMAA9A.tmp\goopdateres_en.dll
C:\Users\win7\AppData\Local\Temp\nsz9081.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsz9081.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\is-QKM9K.tmp_isetup_shfoldr.dll
C:\Windows\SysWOW64\ieframe.dll
MSVBVM60.DLL
C:\Windows\system32\clusapi.dll
C:\HWCodecLoader.dll
C:\IntelHWCodec.dll
C:\NVidiaHWCodec.dll
C:\GeoImageEnhance.dll
C:\GvVAScheDll.dll.dll
C:\GeoCodec.dll
C:\GXAMP4.dll
C:\GX264.dll
C:\GXGM20.dll
C:\GXJPG.dll
C:\GXAVC.dll
C:\GeoADPCM.acm
C:\GeoAudio.acm
C:\Users\win7\AppData\Local\Temp\Tsu9CF7CF34.dll
C:\Windows\system32\sfc.dll
C:\Windows\system32\comctl32.dll
C:\Windows\system32\wininet.dll
C:\Windows\system32\msi.dll
C:\Windows\system32\sxs.dll
C:\Windows\system32\mscoree.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.dll
newdev.dll
setupapi.dll
cfgmgr32.dll
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\CityHash.dll
security.dll
FwpuclInt.dll
ldnDL.dll
\PfiShellExt.dll
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsi7C34.tmp\System.dll
wshtcpip
wship6.dll
psapi.h
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\is-PQ2TS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp\INetC.dll
C:\bhelper.dll
GDIPLUS.DLL
C:\silverlight.configurationUI.dll
C:\coreclr.dll
wwkrn.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\iswin7.dll
Ntdll
C:\Windows\system32\shlwapi.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\WinTB.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-O1G6D.tmp\botva2.dll
GDIPlus
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-Q7LBC.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-Q7LBC.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-9RJ4E.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\is-PUVVS.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-PUVVS.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp_isetup_shfoldr.dll

C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-P98SK.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\is-6O4DC.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-6O4DC.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-84VFQ.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.exe
Cabinet.dll
DEVRTL.dll
ACTIVEDS.dll
SysInfo.dll
C:\Users\win7\AppData\Local\Temp\nse355C.tmp\System.dll
C:\GeoAAC.acm
C:\Users\win7\AppData\Local\Temp\is-DKO1M.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-DKO1M.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nshFD83.tmp\System.dll
C:\Windows\SysWOW64\TSAPPCMP.DLL
Ntdll.dll
C:\Windows\SysWOW64\SHLWAPI.DLL
C:\Windows\SysWOW64\KERNEL32.DLL
MsiMsg.dll
C:\Windows\SysWOW64\SHELL32.DLL
C:\Windows\SysWOW64\OLE32.DLL
C:\Windows\SysWOW64\NETAPI32.DLL
C:\Windows\SysWOW64\ADVAPI32.DLL
MSISIP.DLL
crypt32.dll
URLMON.DLL
C:\Windows\system32\UxTheme.dll
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\CopyInstructionsWENU.dll
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\CopyInstructionsWLOC.dll
C:\Windows\SysWOW64\SAGE.DLL
C:\Users\win7\AppData\Local\Temp\7zS9278.tmp\CopyInstructionsW.exe
C:\Users\win7\AppData\Local\Temp\nsbAF7B.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\NSISArray.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\GetVersion.dll
msrle32.dll
msvidc32.dll
msyuv.dll
iyuv_32.dll
tsbyuv.dll
iccvid.dll
WinHttp.dll
C:\Users\win7\AppData\Local\Temp\nsf5E75.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf5E75.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp\skinnedbutton.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\System.dll
DUser.dll
C:\Windows\system32\DUser.dll
C:\Windows\system32\xmllite.dll
api-ms-win-core-sysinfo-l1-2-1
atlthunk.dll
C:\rarlng.dll
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-K7MC6.tmp_isetup_iscrypt.dll
C:\idmvs.dll
Connect.dll
C:\Windows\system32\NTDLL.DLL
C:\Windows\system32\ADVAPI32.DLL
RegUtil.dll
C:\Windows\system32\twext.dll
sfc.dll
C:\Users\win7\AppData\Local\Temp\27H3R8DF\unpack.dll
C:\\chrome.dll
C:\\23.0.1271.97\chrome.dll
POWRPROF.DLL
C:\Users\win7\AppData\Local\Temp\nsxCECF.tmp\LangDLL.dll

C:\Users\win7\AppData\Local\Temp\is-ML5M0.tmp_isetup_shfoldr.dll
DDraw.dll
DInput.dll
DPlayX.dll
DSound.dll
C:\Windows\system32\DSound.dll
C:\Users\win7\AppData\Local\Temp\nsj3359.tmp\System.dll
Shell32.dll
C:\Users\win7\AppData\Local\Temp\E482D6A2-CDD7-4859-BA06-F10DD9CDC472\atih_uninstaller_standard.exe
NEWDEV.DLL
UnlockerHook.dll
C:\Windows\system32\DSOUND.dll
d3d9.dll
VBoxDisp.dll
C:\WBDJA44I.DLL
lsm.exe
C:\Windows\system32\lsm.exe
C:\Windows\system32\drivers\pacer.sys
fwpuclnt.dll
pnrpsvc.dll
C:\Windows\system32\pnrpsvc.dll
AzRoles.dll
fxsresm.dll
cscsvc.dll
C:\Windows\system32\cscsvc.dll
C:\Windows\system32\iphlpsvc.dll
C:\Windows\system32\umpo.dll
HTTPAPI.DLL
NetLogon.dll
drt.dll
C:\Windows\system32\drivers\ndis.sys
C:\Windows\system32\advapi32.dll
PeerDistSvc.dll
C:\Windows\system32\PeerDistSvc.dll
WsmRes.dll
tbssvc.dll
C:\Windows\system32\tbssvc.dll
C:\Windows\System32\perfproc.dll
C:\Users\win7\AppData\Local\Temp\RarSFX0\MetroInstallerAPP.exe
C:\Windows\temp\tttdelzzz.bat
C:\Windows\temp\tttbrozzz.bat
api-ms-win-core-string-l1-1-0
DDRAW.dll
wer.dll
NETMSG
C:\Users\win7\AppData\Local\Temp\genteert.dll
C:\Users\win7\AppData\Local\Temp\nse2076.tmp\AccDownload.dll
USP10.dll
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\SetupLib.dll
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp\HWSignature.dll
inetmib1.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.ENU
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.EN
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\HwInfo.dll
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp\System.dll
iertutil.dll
MFC42u.DLL
MSVCIRT.dll
MSVCRT.dll
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\GvNPRT_InstallENU.dll
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\GvNPRT_InstallLOC.dll
advpack.dll
C:\Users\win7\AppData\Local\Temp\is-EPHGJ.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-EPHGJ.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-6MGN8.tmp_isetup_shfoldr.dll
PitonMono
RotterRecessed
MeshingPartnership
alvtnvw.dll
C:\Users\win7\AppData\Local\Temp\nsc803A.tmp\nsExec.dll
Msi.DLL
C:\Windows\system32\ws2_32.dll
C:\Windows\system32\user32.dll

C:\Windows\system32\secur32.dll
C:\Users\win7\AppData\Local\Temp\xagE6.tmp
C:\Users\win7\AppData\Local\Temp\xagE6.ENU
C:\Users\win7\AppData\Local\Temp\xagE6.EN
C:\Windows\SysWOW64\dnsapi.dll
mpr
C:\Users\win7\AppData\Local\Temp\is-KSUF0.tmp_isetup_shfoldr.dll
xul.dll
C:\Users\win7\AppData\Local\Temp\is-FP5SP.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsqA304.tmp\System.dll

DeleteFile

C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160404181546.log
C:\Users\win7\AppData\Local\Temp\Opera Installer\sample
C:\Users\win7\AppData\Local\Temp\nsaF532.tmp
C:\Users\win7\AppData\Local\Temp\nsc86A2.tmp
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\instmsi.msi
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\shfolder.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msls31.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\usp10.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\riched20.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\mspatcha.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\imagehlp.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\cabinet.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msimsg.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msihnd.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msiexec.exe
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msi.dll
C:\Users\win7\AppData\Local\Temp\IXP000.TMP\msiinst.exe
C:\Users\win7\AppData\Local\Temp\nsz3E0B.tmp
C:\Users\win7\AppData\Local\Temp\nsa3F46.tmp
C:\Users\win7\AppData\Local\Temp\nsj5707.tmp
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Bu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Cu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Du_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Eu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Fu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Gu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Hu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Iu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ju_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ku_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Lu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Mu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Nu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ou_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Pu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Qu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Ru_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Su_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Tu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Uu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Vu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Wu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Xu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Yu_.exe
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Zu_.exe
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405001235.log
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\1GzPPSq.lnk
C:\Users\win7\Desktop\1GzPPS q.lnk
C:\Users\win7\Desktop\$5->$.qmgc
C:\Users\win7\Desktop\Lb.lnk
C:\Users\win7\Desktop\1Gz>h.lnk
C:\Users\win7\Desktop\9158.lnk
C:\Users\win7\Desktop\2345LOh.lnk
C:\Users\win7\Desktop\Oh.lnk
C:\Users\win7\Desktop\M9S5.lnk
C:\Users\win7\Desktop\QQOh.lnk
C:\Users\win7\Desktop\Q*.lnk
C:\Users\win7\Desktop\.lnk
C:\Users\win7\Desktop\My Box.lnk
C:\Users\Public\Desktop\1Gz.lnk
C:\Users\Public\Desktop\o.lnk

C:\Users\Public\Desktop\5.lnk
C:\Users\Public\Desktop\~@.lnk
C:\Users\Public\Desktop\~k.lnk
C:\Users\Public\Desktop\~o.lnk
C:\Users\Public\Desktop\~k-o.lnk
C:\Users\Public\Desktop\^@o.lnk
C:\Users\Public\Desktop\1Gz>h.lnk
C:\Users\Public\Desktop\q.lnk
C:\Users\Public\Desktop\qb.xlkkvd
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1GzPPSq.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\1GzPPSq.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\Oh.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Windows\Start Menu\2345LOh.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\5.lnk
C:\ProgramData\Microsoft\Windows\Start Menu\:x}5o .lnk
C:\ProgramData\Microsoft\Windows\Start Menu\q.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\1GzPPSq.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\9158.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\q.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\1GzPPSq.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\1GzPPSq.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\1Gz.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\5.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\:x}5o .lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\~o.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\~k-o.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\2345LOh.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\QQOh.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\StartMenu\q.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\^@o.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\2345LOh.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\Oh.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\9158.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\.lnk
C:\Users\win7\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned\TaskBar\q.lnk
C:\Users\win7\AppData\Local\Temp_MSI5166._IS
C:\Users\win7\AppData\Local\Temp\nsiE8BE.tmp
C:\Users\win7\AppData\Local\Temp\nsj88A1.tmp
C:\Users\win7\AppData\Local\Temp\nsk8B61.tmp
C:\Users\win7\AppData\Local\Temp\ccavusage.sdb-journal
C:\Users\win7\AppData\Local\Temp\nsw2BD0.tmp
C:\Users\win7\AppData\Local\Temp\nsx2DF5.tmp
C:\Users\win7\AppData\Local\Temp\FILELOCK.TMP
C:\Users\win7\AppData\Local\Temp_isABD7.tmp
C:\Users\win7\AppData\Local\Temp_isAC07.tmp
C:\Users\win7\AppData\Local\Temp_isAC18.tmp
C:\Users\win7\AppData\Local\Temp_isAC76.tmp
C:\Users\win7\AppData\Local\Temp_isAD52.tmp
C:\Users\win7\AppData\Local\Temp_isADC1.tmp
C:\Users\win7\AppData\Local\Temp_isAF19.tmp
C:\Users\win7\AppData\Local\Temp_isAF78.tmp
C:\Users\win7\AppData\Local\Temp_isB3DE.tmp
C:\Users\win7\AppData\Local\Temp_isB9CB.tmp
C:/Users/win7/AppData/Local/Temp/BRBC76.tmp
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405165551.log
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160405172045.log
C:\ProgramData\Npackd\Data.db-wal
C:\ProgramData\Npackd\Data.db-journal
C:\Users\win7\AppData\Local\Temp\nso780A.tmp
C:\Users\win7\AppData\Local\Temp\nsv879C.tmp
C:\Users\win7\AppData\Local\Temp\nsi97FC.tmp
C:\Users\win7\AppData\Local\Temp\nso99F2.tmp
C:\Users\win7\AppData\Local\Temp\nse6738.tmp
C:\Users\win7\AppData\Local\Temp\nsj67F5.tmp
C:\Users\win7\AppData\Local\Temp\nswE120.tmp
C:\Users\win7\AppData\Local\Temp\nsbE141.tmp
C:\Users\win7\AppData\Local\Temp_is351B.tmp
C:\Users\win7\AppData\Local\Temp\nsm8772.tmp
C:\Users\win7\AppData\Local\Temp\nsr87E0.tmp
C:\Users\win7\AppData\Local\Temp\nspEB37.tmp
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\nszEB76.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsvAF85.tmp
C:\Users\win7\AppData\Local\Temp\CR_793D1.tmp\SETUP_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_793D1.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\nse8F66.tmp
C:\Users\win7\AppData\Local\Temp\nsz9081.tmp

__tmp_rar_sfx_access_check_54717968
C:\Users\win7\AppData\Local\Temp\nsh225F.tmp
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160406155933.log
C:\Users\win7\AppData\Local\Temp\nsw156E.tmp
C:\Users\win7\AppData\Local\Temp\nsxD42B.tmp
C:\Users\win7\AppData\Local\Temp\nsn99E5.tmp
C:\Users\win7\AppData\Local\Temp\nstE59F.tmp
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\nsjE64C.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsr1501.tmp
C:\Users\win7\AppData\Local\Temp\nsr1550.tmp
C:\Users\win7\AppData\Local\Temp\nsx7B57.tmp
C:\Users\win7\AppData\Local\Temp\nsi7C34.tmp
C:\Users\win7\AppData\Local\Temp\nsnC90F.tmp
C:\Users\win7\AppData\Local\Temp\nsxC94F.tmp
C:\Users\win7\AppData\Local\Temp\nsgED74.tmp
C:\Users\win7\AppData\Local\Temp\nsbEDA4.tmp
output_log.txt
__tmp_rar_sfx_access_check_54714234
C:\Users\win7\AppData\Local\Temp\nsk3C24.tmp
C:\Users\win7\AppData\Local\Temp\PreVer.log
C:\Users\win7\AppData\Local\Temp\nsj67F3.tmp
C:\Users\win7\AppData\Local\Temp\nsp887D.tmp
C:\Users\win7\AppData\Local\Temp\nsp891A.tmp
C:\Users\win7\AppData\Local\Temp\nsy3FCA.tmp
C:\Users\win7\AppData\Local\Temp\e4j77EC.tmp
C:\Users\win7\AppData\Local\Temp\nszF0A7.tmp
C:\Users\win7\AppData\Local\Temp\nsrC4A5.tmp
C:\Users\win7\AppData\Local\Temp\nsmC4D6.tmp
C:\Users\win7\AppData\Local\Temp\ClassicFTPCounts.txt
C:\Users\win7\AppData\Local\Temp\nstC233.tmp
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.exe
C:\Users\win7\AppData\Local\Temp\n1s\nchsetup.cab
C:\Users\win7\AppData\Local\Temp\n1s\nchdata.dat
C:\Users\win7\AppData\Local\Temp\n1s\nchdata.cab
C:\Users\win7\AppData\Local\Temp\evb39B9.tmp
C:\Users\win7\AppData\Local\Temp\nsj3441.tmp
C:\Users\win7\AppData\Local\Temp\nse355C.tmp
C:\Users\win7\AppData\Local\Temp\nsmFC68.tmp
C:\Users\win7\AppData\Local\Temp\nshFD83.tmp
C:\Users\win7\AppData\Local\Temp\nsjA99D.tmp
C:\Users\win7\AppData\Local\Temp\nsbAF7B.tmp
C:\Users\win7\AppData\Local\Temp\nsf75BF.tmp
C:\Users\win7\AppData\Local\Temp\nsh7A54.tmp
C:\Users\win7\AppData\Local\Temp\nsu9B96.tmp
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp
cat_background.bmp
wlan_test.exe
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\GetVersion.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\NSISArray.dll
C:\Users\win7\AppData\Local\Temp\nsf9BD6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\CR_8D9FE.tmp\SETUP_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_8D9FE.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\nsp5E15.tmp
C:\Users\win7\AppData\Local\Temp\nsf5E75.tmp
C:\Users\win7\AppData\Local\Temp\nsbC829.tmp
C:\Users\win7\AppData\Local\Temp\nsrC83B.tmp
C:\Users\win7\AppData\Local\Temp\nsr68C5.tmp
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp
C:\Windows\TEMP\IE9B472.tmp
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_amd64_20150610171551.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_amd64_20150610171551_0_vcRuntimeMinimum_x64.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_amd64_20150610171551_1_vcRuntimeAdditional_x64.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_amd64_20150610174316.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_x86_20150610171519.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_x86_20150610171519_0_vcRuntimeMinimum_x86.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_x86_20150610171519_1_vcRuntimeAdditional_x86.log
C:\Users\win7\AppData\Local\Temp\\dd_vcredist_x86_20150610174309.log
C:\Users\win7\AppData\Local\Temp\\FXSAPIDebugLogFile.txt
C:\Users\win7\AppData\Local\Temp\\StructuredQuery.log
C:\Users\win7\AppData\Local\Temp\\win7.bmp
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160407224627.log
C:\Users\win7\AppData\Local\Temp\nsxFD43.tmp
C:\Users\win7\AppData\Local\Temp\nstFFE5.tmp
C:\Users\win7\AppData\Local\Temp\nsq8E34.tmp
C:\Users\win7\AppData\Local\Temp\~DFF61056C422EA0937.TMP

C:\Users\win7\AppData\Local\Temp\nsmCD08.tmp
C:\Users\win7\AppData\Local\Temp\nsxCECF.tmp
C:\Users\win7\AppData\Local\Temp\nsd324D.tmp
C:\Users\win7\AppData\Local\Temp\nsj3359.tmp
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\H0G27RVV\0RHYLLSA.json
\\?\C:\Users\win7\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
C:\Users\win7\AppData\Local\Temp\CR_D2B34.tmp\SETUP_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\CR_D2B34.tmp\CHROME_PATCH.PACKED.7Z
C:\Users\win7\AppData\Local\Temp\bt3526.bat
__tmp_rar_sfx_access_check_54664421
C:\Users\win7\AppData\Local\Temp\nsp2065.tmp
C:\Users\win7\AppData\Local\Temp\nse2076.tmp
C:\Users\win7\AppData\Local\Temp\nsk2097.tmp
C:\Users\win7\AppData\Local\Temp\nsjF479.tmp
C:\Users\win7\AppData\Local\Temp\nsuF5A4.tmp
C:\Users\win7\AppData\Local\Temp\nsp8559.tmp
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\HwInfo.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\nsRandom.dll
C:\Users\win7\AppData\Local\Temp\nsz8598.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nss1BA2.tmp
C:\Users\win7\AppData\Local\Temp\nso1EDF.tmp
C:\sample`.!!!
C:\Users\win7\AppData\Local\Temp\pft9592.tmp
C:\Users\win7\AppData\Local\Temp\pft9592.tmp\pftw1.pkg
__tmp_rar_sfx_access_check_54609281
__tmp_rar_sfx_access_check_54613812
C:\sample
C:\Users\win7\AppData\Local\Temp\nsh8009.tmp
C:\Users\win7\AppData\Local\Temp\nsc803A.tmp
C:\Users\win7\AppData\Local\Temp_is8F03.tmp
C:\Users\win7\AppData\Local\Temp_is959C.tmp
C:\Users\win7\AppData\Local\Temp_isA02D.tmp
C:\Users\win7\AppData\Local\Temp\~A00D.tmp
C:\Users\win7\AppData\Local\Temp_isA119.tmp
C:\Users\win7\AppData\Local\Temp\~A118.tmp
C:\Users\win7\AppData\Local\Temp\nsi8E90.tmp
C:\Users\win7\AppData\Local\Temp\~DF05B3E806633591A5.TMP
C:\Users\win7\AppData\Local\Temp\nswCA22.tmp
C:\Users\win7\AppData\Local\Temp\nsi4C62.tmp
C:\Users\win7\AppData\Local\Temp\nsvA2D3.tmp
C:\Users\win7\AppData\Local\Temp\nsqA304.tmp

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2015-10-30 10:25:47 UTC
Analysis End Date: 2015-10-30 12:36:11 UTC
File Upload Date: 2015-09-02 18:31:32 UTC
Human Expert Analyst Feedback: adware, opencandy
Verdict: PUA

Additional File Information

Vendor Validation - Verified ✔

[+] MediaArea.net

Status	Valid ✔

Certificate Validation - Success ✔

[+] MediaArea.net

Status	NoError ✔
Start Date	2013-09-29 00:00:00+00:00
End Date	2016-11-27 23:59:59+00:00
Sha256	8ac473b3bfa375deabb9f3b352b0ba760a7492b2f55e0706c9a4051a9095adc5
Serial	01D6E74D7FDE17C5B2FB8F478747CC46
Subject Name	MediaArea.net
Subject Key Identifier	undefined
Subject Organization	MediaArea.net
Subject Locality	Curienne
Subject State	France
Subject Country	FR
Subject Organizational Unit	Digital ID Class 3 - Microsoft Software Validation v2
Issuer Name	VeriSign Class 3 Code Signing 2010 CA
Issuer Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Crl link	http://csc3-2010-crl.verisign.com/CSC3-2010.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

[+] VeriSign Class 3 Code Signing 2010 CA

Status	NoError ✔
Start Date	2010-02-08 00:00:00+00:00
End Date	2020-02-07 23:59:59+00:00
Sha256	0f5cd6ebab15fa367e35893fad2bc49cd1a95449f58e7eb978d72bb0b100d764
Serial	5200E5AA2556FC1A86ED96C9D44B33C7
Subject Name	VeriSign Class 3 Code Signing 2010 CA
Subject Key Identifier	cf 99 a9 ea 7b 26 f4 4b c9 8e 8f d7 f0 05 26 ef e3 d2 a7 9d
Subject Organization	VeriSign, Inc.
Subject Country	US
Subject Organizational Unit	Terms of use at https://www.verisign.com/rpa (c)10
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	http://crl.verisign.com/pca3-g5.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Client Authentication (1.3.6.1.5.5.7.3.2)

[+] VeriSign Class 3 Public Primary Certification Authority - G5

Status	NoError ✔
Start Date	2006-11-08 00:00:00+00:00
End Date	2036-07-16 23:59:59+00:00
Sha256	d0c133d98cabb2199501a761f5b8b9afd30d870477a534b41400a6dc57f5d64d
Serial	18DAD19E267DE8BB4A2158CDCC6B3B4A
Subject Name	VeriSign Class 3 Public Primary Certification Authority - G5
Subject Key Identifier	7f d3 65 a7 c2 dd ec bb f0 30 09 f3 43 39 fa 02 af 33 31 33
Subject Organization	VeriSign, Inc.
Subject Country	US
Subject Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Issuer Name	VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Key Identifier	undefined
Issuer Organization	VeriSign, Inc.
Issuer Country	US
Issuer Organizational Unit	(c) 2006 VeriSign, Inc. - For authorized use only
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

[+] Symantec Time Stamping Services CA - G2

Status	NoError ✔
Start Date	2012-12-21 00:00:00+00:00
End Date	2020-12-30 23:59:59+00:00
Sha256	0b44526ab89f4778858bf831045ec218d0d57734caa10208ea3d8c90c1043266
Serial	7E93EBFB7CC64E59EA4B9A77D406FC3B
Subject Name	Symantec Time Stamping Services CA - G2
Subject Key Identifier	5f 9a f5 6e 5c cc cc 74 9a d4 dd 7d ef 3f db ec 4c 80 2e dd
Subject Organization	Symantec Corporation
Subject Country	US
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	http://crl.thawte.com/ThawteTimestampingCA.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

[+] Thawte Timestamping CA

Status	NoError ✔
Start Date	1997-01-01 00:00:00+00:00
End Date	2020-12-31 23:59:59+00:00
Sha256	f429a67538b1053ebe3ad5587247d3a6845a82b3e687e079263181f53dbe26d7
Serial	00
Subject Name	Thawte Timestamping CA
Subject Key Identifier	undefined
Subject Organization	Thawte
Subject Locality	Durbanville
Subject State	Western Cape
Subject Country	ZA
Subject Organizational Unit	Thawte Certification
Issuer Name	Thawte Timestamping CA
Issuer Key Identifier	undefined
Issuer Organization	Thawte
Issuer Locality	Durbanville
Issuer State	Western Cape
Issuer Country	ZA
Issuer Organizational Unit	Thawte Certification
Crl link	undefined
Key Usage	undefined
Extended Usage	undefined

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x4F47E2DF [Fri Feb 24 19:19:59 2012 UTC]
Entry Point	0x4039e3 (.text)
File Size	5268504
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	MediaArea.net
File Version	0.7.77.0
Company Name	MediaArea.net
Product Name	MediaInfo
Product Version	0.7.77.0
File Description	All about your audio and video files
Original Filename	MediaInfo_GUI_0.7.77_Windows.exe
Translation	0x0000 0x04e3
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	d95a781627a57a2e8cf8029a1ee11276470e3d659e5ee1b7c5abfe489fc39078

File Paths

FILE PATH ON CLIENT	SEEN COUNT
MediaInfo_GUI_0.7.77_Windows.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6f10	0x7000	6.497885	-
.rdata	0x8000	0x2a92	0x2c00	4.393894	-
.data	0xb000	0x67ebc	0x200	1.472782	-
.ndata	0x73000	0x1b9000	0x0	0.000000[SUSPICIOUS]	-
.rsrc	0x22c000	0xc638	0xc800	4.331299	-
.reloc	0x239000	0xf8a	0x1000	7.910864[SUSPICIOUS]	-