VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 0310_crypted.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 8eef4a7350092b1e0e39b3ee371597e84a317397
MD5: 18bf43dc4e3076f4fd1dff54a9b9a081
First Seen Date: 2015-10-07 15:15:42 UTC
Number of Clients Seen: 6
Last Analysis Date: 2016-04-08 18:52:43 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-04-08 18:52:43 UTC	Malware	
Static Analysis Overall Verdict	2016-04-08 18:52:43 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-04-08 18:52:43 UTC	Highly Suspicious	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

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	Clean	
TLS callback functions array detected	Clean	

Packer detection on signature database

- Armadillo v1.71
- Microsoft Visual C++ v5.0/v6.0 (MFC)
- Microsoft Visual C++

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	!

SUSPICIOUS BEHAVIORS	
Has no visible windows	!

Behavioral Information

LoadLibrary

C:\sample
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
ADVAPI32.dll
CRYPTBASE.dll
OLEAUT32.dll
C:\Windows\system32\uxtheme.dll
dwmapi.dll
comctl32.dll
UxTheme.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
imm32.dll
SHLWAPI.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
advapi32.dll
shell32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
IPHLPAPI.DLL
ntdll.dll
winhttp.dll
WS2_32.dll
kernel32.dll
SspiCli.dll
C:\Windows\system32\clusapi.dll
CRYPTSP.dll
feclient.dll
uxtheme.dll
comctl32
ole32.dll
Secur32.dll
SHELL32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
CRYPT32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
RichEd20.dll
mscorsec.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
USER32.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
bcrypt.dll
USERENV.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.dll
WINHTTP.dll
RPCRT4.dll
SHFOLDER
propsys.dll
ntmarta.dll
C:\Users\win7\AppData\Local\Temp\nscD74D.tmp\System.dll

kernel32
API-MS-Win-Core-RtlSupport-L1-1-0.dll
KERNELBASE.dll
API-MS-Win-Core-Heap-L1-1-0.dll
API-MS-Win-Core-Memory-L1-1-0.dll
API-MS-Win-Core-Handle-L1-1-0.dll
API-MS-Win-Core-Synch-L1-1-0.dll
API-MS-Win-Core-File-L1-1-0.dll
API-MS-Win-Core-IO-L1-1-0.dll
API-MS-Win-Core-ThreadPool-L1-1-0.dll
API-MS-Win-Core-LibraryLoader-L1-1-0.dll
API-MS-Win-Core-NamedPipe-L1-1-0.dll
API-MS-Win-Core-Misc-L1-1-0.dll
API-MS-Win-Core-SysInfo-L1-1-0.dll
API-MS-Win-Core-Localization-L1-1-0.dll
API-MS-Win-Core-ProcessEnvironment-L1-1-0.dll
API-MS-Win-Core-String-L1-1-0.dll
API-MS-Win-Core-Debug-L1-1-0.dll
API-MS-Win-Core-ErrorHandling-L1-1-0.dll
API-MS-Win-Core-Fibers-L1-1-0.dll
API-MS-Win-Core-Util-L1-1-0.dll
API-MS-Win-Core-Profile-L1-1-0.dll
API-MS-Win-Security-Base-L1-1-0.dll
advapi32
msvcrt.dll
API-MS-WIN-Service-Core-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-Management-L2-1-0.dll
KERNEL32.dll
user32
GDI32.dll
ole32
API-MS-Win-Core-Interlocked-L1-1-0.dll
kernelbase
sechost
combase
C:\sampleENU.dll
C:\sampleLOC.dll
C:\Windows\system32\MFC120ENU.DLL
msi.dll
IMM32.dll
C:\Users\win7\AppData\Local\Temp\nsc270E.tmp\NSISLangPlugin.dll
C:\Windows\system32\SHFOLDER.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\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:\Windows\assembly\NativeImages_v2.0.50727_32\System\908ba9e296e92b4e14bdc2437edac603\System.ni.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\VERSION.dll
VERSION.dll
OLEACCRC.DLL
KERNEL32.DLL
comdlg32.dll
gdi32.dll
iphlpapi.dll
mpr.dll
netapi32.dll
oleacc.dll
oleaut32.dll
SHFolder.dll
shlwapi.dll
user32.dll
version.dll
winmm.dll
winspool.drv
Msctf.dll
wtsapi32.dll
WINSTA.dll
security.dll
olepro32.dll
kernelbase.dll
propsys
Shell32

shlwapi
gdiplus.dll
riched20.dll
msimg32.dll
mapi32.dll
USER32.DLL
C:\Users\win7\AppData\Local\Temp\GLC826B.tmp
C:\Users\win7\AppData\Local\Temp\GLK85F6.tmp
RICHED32.DLL
C:\Users\win7\AppData\Local\Temp\GLF8FCC.tmp
MMDevAPI.DLL
wdmaud.drv
MMDEVAPI.DLL
SETUPAPI.dll
AUDIOSES.DLL
msacm32.drv
midimap.dll
MPR.DLL
C:\Users\win7\AppData\Local\Temp\is-HN0ON.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
C:\RaWLAPI.dll
COMCTL32.dll
MSIMG32.dll
PSAPI.DLL
WININET.dll
WINMM.dll
WINTRUST.dll
DNSAPI.dll
C:\Users\win7\AppData\Local\Temp\is-O161C.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-O161C.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-440G0.tmp_isetup_shfoldr.dll
C:\Windows\system32\imageres.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\shlwapi.dll
C:\Users\win7\AppData\Local\Temp\nsaB9E7.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsaB9E7.tmp\CityHash.dll
Advapi32.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
imageres.dll
C:\Users\win7\AppData\Local\Temp\{80597657-8434-47F6-AB65-7562632CA922}\Disk1\ISSetup.dll
C:\English\Strings.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
C:\Windows\system32\sfc.dll
ADVAPI32.DLL
SHELL32.DLL
C:\Users\win7\AppData\Local\Temp\is-55GHL.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-55GHL.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-R0H8H.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\innocallback.ENU
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\innocallback.EN
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\IsProgressBar.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\IsProgressBar.ENU
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\IsProgressBar.EN
Ws2_32.dll
C:\Windows\system32\version.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\atl.dll
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\winmm.dll
C:\Windows\system32\dsound.dll
C:\Windows\system32\powrprof.dll
C:\Windows\system32\d3d9.dll
C:\Windows\system32\d3d8thk.dll
C:\Windows\system32\mscms.dll
C:\Windows\system32\userenv.dll
C:\Windows\system32\profapi.dll
C:\Windows\system32\ieframe.dll
C:\Windows\system32\oleacc.dll
C:\Windows\system32\oleaccrc.dll
C:\Windows\system32\dbghelp.dll
C:\Windows\system32\msasn1.dll

C:\Windows\system32\crypt32.dll
C:\Windows\system32\psapi.dll
C:\Windows\system32\advapi32.dll
C:\Windows\system32\kernel32.dll
C:\Windows\system32\propsys.dll
C:\Windows\system32\secur32.dll
C:\Windows\system32\pcacli.dll
C:\Windows\system32\devrtl.dll
C:\Windows\system32\apphelp.dll
C:\Windows\system32\Shell32.dll
C:\Users\win7\AppData\Local\Temp\{86320BB8-01EE-4E45-8010-7A1F8B940A0F}\fpb.tmp
C:\Users\win7\AppData\Local\Temp\{3B1C3FD5-3A29-435D-B083-8A33EA509E6C}\fpb.tmp
C:\Windows\system32\Advapi32.dll
C:\Windows\system32\Msimg32.dll
atl.dll
C:\Users\win7\AppData\Local\Temp\is-4O20J.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-4O20J.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\nsrA526.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsrA526.tmp\CityHash.dll
COMCTL32.DLL
COMDLG32.DLL
GDI32.DLL
OLE32.DLL
riched32.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\SysWOW64\kernel32.dll
C:\Windows\SysWOW64\KERNELBASE.dll
C:\CFVS_HookDll.dll
C:\Windows\SysWOW64\ws2_32.dll
C:\Windows\SysWOW64\msvcrt.dll
C:\Windows\SysWOW64\rpcrt4.dll
C:\Windows\SysWOW64\sspicli.dll
C:\Windows\SysWOW64\CRYPTBASE.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\SysWOW64\nsi.dll
C:\Windows\SysWOW64\urlmon.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-ole32-l1-1-0.dll
C:\Windows\SysWOW64\ole32.dll
C:\Windows\SysWOW64\gdi32.dll
C:\Windows\SysWOW64\user32.dll
C:\Windows\SysWOW64\advapi32.dll
C:\Windows\SysWOW64\lpk.dll
C:\Windows\SysWOW64\usp10.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-shlwapi-l1-1-0.dll
C:\Windows\SysWOW64\shlwapi.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-advapi32-l1-1-0.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-user32-l1-1-0.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-version-l1-1-0.dll
C:\Windows\System32\version.dll
C:\Windows\SysWOW64\api-ms-win-downlevel-normaliz-l1-1-0.dll
C:\Windows\SysWOW64\normaliz.dll
C:\Windows\SysWOW64\iertutil.dll
C:\Windows\SysWOW64\wininet.dll
C:\Windows\SysWOW64\userenv.dll
C:\Windows\SysWOW64\profapi.dll
C:\Windows\System32\dnsapi.dll
C:\Windows\SysWOW64\oleaut32.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\System32\imm32.dll
C:\Windows\SysWOW64\msctf.dll
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\dwmapi.dll
C:\Windows\SysWOW64\psapi.dll
ws2_32.dll
SetupApi.dll
DEVRTL.dll
SPINF.dll
C:\Users\win7\AppData\Local\Temp\nsq3BEE.tmp\System.dll
mpr
C:\Users\win7\AppData\Local\Temp\is-AA939.tmp_isetup_shfoldr.dll
C:\Windows\System32\shdocvw.dll
PROPSYS.dll
Msftedit.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
WindowsCodecs.dll
dbghelp.dll
rpcrt4.dll

C:\Windows\System32\msxml3r.dll
C:\Users\win7\AppData\Local\Temp\nsuA191.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-ART3B.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-ART3B.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-OV7AD.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-C5P3I.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-C5P3I.tmp\sample.EN
NSI.dll
CFGMGR32.dll
C:\Users\win7\AppData\Local\Temp\is-FP3PI.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-FP3PI.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-DKBL4.tmp_isetup_shfoldr.dll
Kernel32.dll
C:\Windows\system32\UxTheme.dll
C:\Users\win7\AppData\Local\Temp\nscA6EB.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nscA6EB.tmp\CityHash.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
Comctl32.dll
C:\Windows\system32\ws2_32
dhcpcsvc.DLL
secur32.dll
profapi.dll
urlmon.dll
api-ms-win-core-synch-l1-2-0
api-ms-win-core-fibers-l1-1-1
api-ms-win-core-localization-l1-2-1
Normaliz.dll
C:\Windows\system32\lpk.dll
NETAPI32.DLL
C:\Windows\system32\iphlpapi.dll
RichEd20
C:\Users\win7\AppData\Local\Temp\nsz5FDA.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsz5FDA.tmp\System.dll
FaultRep.dll
RICHED20.DLL
crypt32.dll
C:\Users\win7\AppData\Local\Temp\nsqE27E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsqE27E.tmp\LangDLL.dll
api-ms-win-appmodel-runtime-l1-1-1
ext-ms-win-kernel32-package-current-l1-1-0
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\psapi.dll
psapi.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\bcrypt.dll
mscorjit.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\is-IVVGQ.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-IVVGQ.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-K4N3O.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-K4N3O.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nsaA43.tmp\System.dll
Wintrust.dll
POWRPROF.DLL
C:\Users\win7\AppData\Local\Temp\is-GGQBF.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-GGQBF.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp\GCountry.dll
C:\Users\win7\AppData\Local\Temp\is-174HO.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-174HO.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp\GCountry.dll
C:\Windows\system32\odbcint.dll
MSVCRT.DLL
C:\Users\win7\AppData\Local\Temp\is-NE69K.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-NE69K.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp\GCountry.dll
MSFTEDIT.DLL
SXS.DLL
VERSION.DLL

C:\Users\win7\AppData\Local\Temp\nsq8D7.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsq8D7.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsq8D7.tmp\nsProcess.dll
NTDLL.DLL
C:\Users\win7\AppData\Local\Temp\nsq8D7.tmp\ExecDos.dll
\mso.dll
C:\Windows\system32\msi.dll
shell32
C:\idmvs.dll
C:\Users\win7\AppData\Local\Temp\nsgFB55.tmp\System.dll
SKUtil
winmm
uxtheme
wintab32
wintab32.dll
dwmapi
gdi32
version
secur32
userenv
.\wshom.ocx
Shlwapi.dll
C:\Windows\system32\ntdll.dll
BrLogAPI.dll
BrDbgOut.dll
BrDbgOtW.dll
brccDCtl.dll
C:\rarlng.dll
C:\Users\win7\AppData\Local\Temp\is-QO15P.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-LJLK1.tmp_isetup_shfoldr.dll
DSOUND.dll
C:\Windows\system32\DSOUND.dll
COMDLG32.dll
mscms.dll
C:\Users\win7\AppData\Local\Temp\is-KV75T.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-KV75T.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\nsdE750.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsdE750.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\{8768FAA4-5104-42DB-BB10-491FC9943B0F}\fpb.tmp
C:\Users\win7\AppData\Local\Temp\{87700960-A2F8-42C3-BF22-0D1FC9943B0F}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{87700960-A2F8-42C3-BF22-0D1FC9943B0F}\Disk1\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{DCBEDD40-AECD-48A6-9407-F281C9DC1CC9}\{585C5E36-62B1-4CA1-827B-83C4A4486CA5}\ISRT.dll
DUser.dll
C:\Windows\system32\DUser.dll
C:\Windows\system32\xmllite.dll
COMCTL32
KERNEL32
C:\Users\win7\AppData\Local\Temp\RarSFX0\rjVBchp.exe
C:\Windows\syswow64\ADVAPI32.dll
dinput8.dll
devil.dll
C:\Users\win7\AppData\Local\Temp\nsv2090.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsv2090.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\nse4B22.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsu4BCF.tmp
C:\Users\win7\AppData\Local\Temp\nsyD420.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nswD989.tmp\System.dll
inetmib1.dll
C:\Users\win7\AppData\Local\Temp\nsw85DD.tmp\System.dll
globals.dll
C:\msvcr120.dll
C:\msvcp120.dll
OLE32.dll
OPENGL32.DLL
WINMM.DLL
Riched20.dll
C:\Users\win7\AppData\Local\Temp\is-LF6P1.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-LF6P1.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-RID3U.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsj43F7.tmp\System.dll
C:\Program Files\Internet Explorer\iexplore.exe
Cabinet.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
PeerDistSvc.dll
C:\Windows\system32\PeerDistSvc.dll
WsmRes.dll
tbssvc.dll
C:\Windows\system32\tbssvc.dll
C:\Windows\system32\CRYPTNET.dll
Versions\1.0\Adobe AIR.dll
C:\Users\win7\AppData\Local\Temp\AIR5829.tmp\Install Balsamiq Mockups.exe
C:\Users\win7\AppData\Local\Temp\is-0IF4F.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-0IF4F.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-VAGG9.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nswF039.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nswF039.tmp\System.dll
wininet.dll
C:\Users\win7\AppData\Local\Temp\nsx50F1.tmp\registry.dll
OPENGL32.dll
nvapi.dll
C:\Windows\system32\nvapi.dll
atiadlxx.dll
atiadlxy.dll
OPENGL32
VBoxOGL.dll
setupapi.dll
C:\pcnsl.gui
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
DbgHelp.dll
lang\setupENU.dll
setup.dll
POWRPROF.dll
C:\Windows\system32\cryptsp.dll
C:\Windows\system32\setupapi.dll
C:\Windows\system32\clbcatq.dll
C:\Windows\system32\ws2_32.dll
C:\Windows\system32\wsock32.dll
C:\Windows\system32\winnsi.dll
C:\Windows\system32\slc.dll
C:\Windows\system32\gpapi.dll
C:\Windows\system32\hnetcfg.dll
C:\Windows\system32\dnsapi.dll
C:\Windows\system32\rasman.dll
C:\Windows\system32\rasapi32.dll
C:\Windows\system32\sensapi.dll
C:\Windows\system32\rasadhlp.dll
C:\Windows\system32\api-ms-win-downlevel-shell32-l1-1-0.dll
C:\Windows\system32\dinput8.dll
C:\Windows\system32\sxs.dll
C:\Windows\system32\rpcrtremote.dll
C:\Windows\system32\schannel.dll
C:\Users\win7\AppData\Local\Temp\{7D8839CB-D4AF-4E38-9171-A7708EE5E0C3}\fpb.tmp
C:\Users\win7\AppData\Local\Temp\{905AB4B2-8DA2-4E26-8BB7-22A7C9A9EADC}\fpb.tmp
C:\Users\win7\AppData\Local\Temp\nssAE4F.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nssAE4F.tmp\UAC.dll
AdvAPI32
SECUR32
C:\Users\win7\AppData\Local\Temp\nssAE4F.tmp\InstallOptions.dll
shdocvw.dll
mshtml.dll
RegcleanPro.DLL
regcleanpro.dll
RegCleanPro.DLL
C:\Users\win7\AppData\Local\Temp\nsp149F.tmp\System.dll
C:\Sources\autorun.dll
C:\Users\win7\AppData\Local\Temp\gdgED34.tmp
C:\Users\win7\AppData\Local\Temp\gdgED34.ENU
C:\Users\win7\AppData\Local\Temp\gdgED34.EN
C:\Users\win7\AppData\Local\Temp\pbsEEBC.tmp

c:\program files\internet explorer\iexplore.exe
C:\PYTHON27.DLL
pythondll
C:\Windows\SysWOW64\msls31.dll
C:\Users\win7\AppData\Local\Temp\is-QM6T0.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-QM6T0.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-LU37T.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-LU37T.tmp\sample.EN
c:\4b5a1df7161568b6de3fe1c5\MpSigStub.exe
C:\Windows\system32\cabinet.dll
C:\Windows\system32\UXTHEME.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\SETUPAPI.dll
C:\Windows\system32\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-JHAGV.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-JHAGV.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-C8EE3.tmp_isetup_shfoldr.dll
C:\Windows\system32\WINMM.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
c:\windows\system32\imageres.dll
WS2_32.DLL
ntshrui.dll
netutils.dll
C:\Users\win7\AppData\Local\Temp\is-7F1VL.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-7F1VL.tmp\sample.EN
C:\SciLexer.dll
CRYPTUI.dll
RichEd32.dll
certcli.dll
C:\Windows\system32\dsrole.dll
C:\CFVS_I~1.EXE
C:\DLL_LO~1.EXE
C:\Procmon.exe
C:\PROGRA~2\COMMON~1\MICROS~1\ink\mip.exe
C:\PROGRA~2\COMMON~1\MICROS~1\MSInfo\msinfo32.exe
C:\PROGRA~2\INTERN~1\ieinstal.exe
C:\PROGRA~2\INTERN~1\ielowutil.exe
C:\PROGRA~2\INTERN~1\iexplore.exe
C:\PROGRA~2\WINDOW~1\wab.exe
C:\PROGRA~2\WINDOW~1\wabmig.exe
C:\PROGRA~2\WINDOW~1\WinMail.exe
C:\PROGRA~2\WINDOW~2\ACCESS~1\wordpad.exe
C:\PROGRA~2\WINDOW~4\ImagingDevices.exe
C:\PROGRA~2\WI4223~1\sidebar.exe
C:\PROGRA~3\PACKAG~1\{050D4~1\VCREDI~1.EXE
C:\PROGRA~3\PACKAG~1\{F65DB~1\VCREDI~1.EXE
C:\Python27\Lib\DISTUT~1\command\WININS~1.EXE
C:\Python27\Lib\DISTUT~1\command\WININS~2.EXE
C:\Python27\Lib\DISTUT~1\command\WININS~3.EXE
C:\Python27\Lib\DISTUT~1\command\WININS~4.EXE
C:\Python27\Lib\DISTUT~1\command\WI02EA~1.EXE
URLMON.DLL
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\ar-SA\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\cs-CZ\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\da-DK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\de-DE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\el-GR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\en-US\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\es-ES\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\fi-FI\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\fr-FR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\he-IL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\hu-HU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\it-IT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\ja-JP\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\ko-KR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\nb-NO\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\nl-NL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\pl-PL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\pt-BR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\pt-PT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\ru-RU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\sv-SE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\th-TH\IntelCommon.dll

C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\tr-TR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\zh-CN\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\zh-TW\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIFD542.tmp\en-US\resource.dll.mui
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\ar-SA\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\cs-CZ\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\da-DK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\de-DE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\el-GR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\en-US\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\es-ES\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\fi-FI\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\fr-FR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\he-IL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\hu-HU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\it-IT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\ja-JP\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\ko-KR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\nb-NO\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\nl-NL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\pl-PL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\pt-BR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\pt-PT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\ru-RU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\sv-SE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\th-TH\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\tr-TR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\zh-CN\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\zh-TW\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF47A8.tmp\en-US\resource.dll.mui
C:\\chrome.dll
msvcr71.dll
C:\msvcr71.dll
msvcp71.dll
C:\msvcp71.dll
C:\proj.dll
RASAPI32.dll
WINSPOOL.DRV
C:\Users\win7\AppData\Local\Temp\is-KDNA2.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-KDNA2.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp\muid.dll
Kernel32.DLL
DWMAPI.DLL
C:\Users\win7\AppData\Local\Temp\nsrBE8A.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsrBE8A.tmp\Base64.dll
C:\Users\win7\AppData\Local\Temp\nsrBE8A.tmp\Inetc.dll
C:\Users\win7\AppData\Local\Temp\033fd036.a
C:\Users\win7\AppData\Local\Temp\033fde02.a
C:\Users\win7\AppData\Local\Temp\nsp56CD.tmp\nsExec.dll
C:\\apilog.txt
C:\\CFVS_HookDll.dll
C:\\CFVS_Injector.exe
C:\\countdown.py
C:\\DLL_Loader.exe
C:\\monkey.py
C:\\pagefile.sys
C:\\Procmon.exe
C:\\runtimer.bat
C:\\sample
C:\\startprocmon.bat
C:\\stopprocmon.bat
C:\samplePTNMWNDeng.dll
C:\Users\win7\AppData\Local\Temp\nsdD21D.tmp\NsisInstallUI.dll
C:\Users\win7\AppData\Local\Temp\nsr6729.tmp\FindProcDLL.dll
C:\Users\win7\AppData\Local\Temp\nsr6729.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsh1BA8.tmp\InstallOptions.dll
ComCtl32.dll
wiatrace.dll
C:\Users\win7\AppData\Local\Temp\jki6EB4.tmp
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\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\uxtheme.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\007fc007edc388d9806dff94ee04f129\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\d49908aa93a23c84847b1f8b1b667860\System.Xml.ni.dll

C:\Windows\system32\wbem\xml\wmi2xml.dll
Iphlpapi.dll
api-ms-win-core-sysinfo-l1-2-1
C:\Users\win7\AppData\Local\Temp\/libkacm.dll
C:\Users\win7\AppData\Local\Temp\is-EO7Q2.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsh351B.tmp\UserInfo.dll
rsaenh
ncrypt
wsock32.dll
OLEACC.DLL
Avrt.dll
C:\Users\win7\AppData\Local\Temp\nss50D2.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nss50D2.tmp\newadvsplash.dll
C:\Windows\system32\urlmon.dll
C:\Windows\system32\asycfilt.dll
Kernel32
psapi
C:\Windows\system32\user32.dll

OpenRegisteryKey

Software\Microsoft\WBEM\CIMOM
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
Software\Adobe\Acrobat Reader\9.0\Language\current
Software\Microsoft\.NETFramework\Policy\
v2.0
Software\Microsoft\.NETFramework
Upgrades
Standards
AppPatch
Software\Microsoft\.NETFramework\Policy\Standards
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
Software\Blizzard Entertainment\Launcher
Software\Blizzard Entertainment\Battle.net
Software\Blizzard Entertainment\Blizzard Error
Blizzard
MS Shell Dlg 2
MS Sans Serif
Software\Microsoft\Windows\CurrentVersion\Uninstall\Clock Tray Skins_is1
Tahoma
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
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\Windows\CurrentVersion\Internet Settings
Software\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies
Software
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
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad
Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
Software\Microsoft\Cryptography\Wintrust\Config
Software\Microsoft\Windows\CurrentVersion
Software\Policies\ThinApp\Management\YoWindow by Noby.uCoz.Ru\DisableShortcuts
Environment
Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
Software\Policies\ThinApp\Management\YoWindow by Noby.uCoz.Ru
Software\VMware
SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\Installations
Arial
SYSTEM\CurrentControlSet\Control\Nls\CodePage
SYSTEM\CurrentControlSet\Control\Nls\Language
SYSTEM\CurrentControlSet\Control\FileSystem
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Software\Microsoft\Windows\CurrentVersion\Policies\Network
Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Software\Policies\Microsoft\Windows\Installer
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\E757FC781F1C22D468C5006C59B02585
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\E757FC781F1C22D468C5006C59B02585
Software\Classes\Installer\Products\E757FC781F1C22D468C5006C59B02585
ISlogit
Software\Microsoft\Internet Explorer
SOFTWARE\Microsoft\OLEAUT
Software\Microsoft\Windows\CurrentVersion\Setup
system\CurrentControlSet\control\NetworkProvider\HwOrder
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\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 NT\CurrentVersion
NI\4a4af2b2\76dec072
Software\Microsoft\StrongName
Software\Microsoft\Fusion\PublisherPolicy\Default
NI\759240c9\1ae8ddb
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
NI\759240c9\1ba775d2
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\Classes\CLSID\{5C5DC941-A41A-4483-ABC2-8A37B7ABCEC7}
Software\Embarcadero\Locales
Software\CodeGear\Locales
Software\Borland\Locales
Software\Borland\Delphi\Locales
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
Control Panel\Desktop
Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
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\Microsoft\CTF\KnownClasses
Software\Microsoft\CTF\LayoutIcon\0409\0000041f
SOFTWARE\Microsoft\Windows\CurrentVersion\Setup
Software\Microsoft\Windows\CurrentVersion\SharedDLLs
System\CurrentControlSet\Control\SQMServiceList
SOFTWARE\Microsoft\Windows NT\CurrentVersion\DRIVERS32
System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm
System\Setup
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{1b848ac1-f113-4bd0-acfd-4cacc8f77fcb}
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{1b848ac1-f113-4bd0-acfd-4cacc8f77fcb}\Properties
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{2b4e4dcc-bfef-4c15-935e-d0b4b7f69fb5}
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{2b4e4dcc-bfef-4c15-935e-d0b4b7f69fb5}\Properties
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Render\{a5bdcb55-8975-4210-8425-4306b443cd16}
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{a5bdcb55-8975-4210-8425-4306b443cd16}
SOFTWARE\Microsoft\Windows\CurrentVersion\MMDevices\Audio\Capture\{a5bdcb55-8975-4210-8425-4306b443cd16}\Properties
Software\Microsoft\Windows\CurrentVersion\Multimedia\MIDIMap
SOFTWARE\Microsoft\Windows\CurrentVersion
SOFTWARE\Scholastic Inc\ISPY_SPOOKY2

{352481E8-33BE-4251-BA85-6007CAEDCF9D}
NI\76b40e\20287007
SOFTWARE\Classes\CLSID\{F83D1872-D9FF-47F8-B5A0-49CC51E24EE8}
SOFTWARE\SearchKnow
v4.0.30319
Software\Microsoft\.NETFramework\Policy\Upgrades
System\CurrentControlSet\Control\Keyboard Layouts\041F0409
System\CurrentControlSet\Control\Keyboard Layouts\04090409
SOFTWARE\MiddleRush
SOFTWARE\CashKitten
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IObit Surfing Protection_is1
Verdana
Software\Microsoft\Windows\CurrentVersion\Uninstall\IObit Surfing Protection_is1
SOFTWARE\WebEx\wbxtrace
AppID
{ab25d3c2-9787-4788-99a1-32a4c1208c11}
SOFTWARE\OneSafe PC Cleaner
SOFTWARE\Licenses\b47b460376d661a60e56ba925fabf8d4
Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\RunOnce
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\
SOFTWARE\Microsoft\Internet Explorer\Toolbar\
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IEData
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MobileOptionPack
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SchedulingAgent
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WIC
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{050d4fc8-5d48-4b8f-8972-47c82c46020f}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{13A4EE12-23EA-3371-91EE-EFB36DDFFF3E}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{f65db027-aff3-4070-886a-0d87064aabb1}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{F8CFEB22-A2E7-3971-9EDA-4B11EDEFC185}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{CED8E25B-122A-4E80-B612-7F99B93284B3}
{8a4a8b42-a270-4ad4-95c3-815ded6433fc}
SYSTEM\CurrentControlSet\Services\Tcpip\Performance
CLSID\{BC149E72-D422-4745-B674-01AB3DD160EB}
Software\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.exe
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
FEATURE_INITIALIZE_URLACTION_SHELLEXECUTE_TO_ALLOW_KB936610
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
Microsoft\Internet Explorer\Security
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_ZONES_DEFAULT_DRIVE_INTRANET_KB941000
FEATURE_PROTOCOL_LOCKDOWN
System\CurrentControlSet\Control
Software\Microsoft\RestartManager
SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
Software\Macromedia\FlashPlayerActiveX
Software\Macromedia\FlashPlayerPlugin
Software\Macromedia\FlashPlayerPepper
Software\Macromedia\FlashPlayer
SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
Software\LenovoBrowserGuard
Software\SearchProtect
SOFTWARE\Microsoft\Internet Explorer
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\firefox.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\chrome.exe
v1.0.3705
NI\27244c38\7235c56e
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
MS Shell Dlg
Software\Microsoft\Windows NT\CurrentVersion
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\S.T.A.L.K.E.R - Shadow of Chernobyl_R.G. Mechanics_is1
Software\Mozilla\Thunderbird\TaskBarIDs
Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
.exe
.exe\OpenWithProgids
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids
Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
UserChoice
exefile
SystemFileAssociations\.exe
Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
shell
open
command
DropTarget
Software\Microsoft\Windows\CurrentVersion\Explorer\FileAssociation
Software\Microsoft\Windows\CurrentVersion\Policies\Associations
.ade
.adp
.app
.asp
.bas
.bat
.cer
.chm
.cmd
.com
.cpl
.crt
.csh
CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\
ZoneMap\Ranges\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4
{2B0F765D-C0E9-4171-908E-08A611B84FF6}
Progid
Software\Microsoft\Windows\CurrentVersion\ShellCompatibility\ProgIDs\exefile
ddeexec
Software\Microsoft\Windows\CurrentVersion\App Paths\setup.exe
Software\TutoTag
Microsoft Sans Serif
Software\Microsoft\Windows\CurrentVersion\Uninstall\{C8748FFB-1713-4e95-B3DF-4F1622D96F93}_is1
SOFTWARE\Microsoft\MpSigStub
Software\Opera Software
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}

SYSTEM\CurrentControlSet\Control\Session Manager
Software\Mozilla\MaintenanceService
Software\Microsoft\Windows\CurrentVersion\Uninstall\{0F91E44C-2FAD-4298-8051-40E52C7E1341}_is1
System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
Software\Microsoft\Windows NT\CurrentVersion\TaskManager
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
Software\Microsoft\Windows\CurrentVersion\Policies\System
FEATURE_BROWSER_EMULATION
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
Pre Platform
Post Platform
{69DC4768-446B-4F82-A6B0-63966A243064}
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
SOFTWARE\StudySearchWindow
SOFTWARE\System Healer
Software\System Healer
Software\Microsoft\.NETFramework\Policy\AppPatch
v2.0.50727.00000
sample
NI\37b8106e\45169c1
SOFTWARE\JavaSoft\Java Runtime Environment
SOFTWARE\JavaSoft\Java Development Kit
SOFTWARE\IBM\Java2 Runtime Environment
SOFTWARE\IBM\Java Development Kit
SOFTWARE\AVG Security Toolbar
SOFTWARE\SearchWebKnow
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\{436366DE-5579-4F24-96DB-3893E4400030}
Software\Wow6432Node\Microsoft\Office\16.0\Registration\{436366DE-5579-4F24-96DB-3893E4400030}
Software\Microsoft\Office\ClickToRun\propertyBag
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Software\Microsoft\Windows\CurrentVersion\Uninstall\{B023AAEF-C0D5-4949-95CE-86AF1603AD1F}_is1
SOFTWARE\Microsoft\BidInterface\Loader
SOFTWARE\ODBC\ODBC.INI\ODBC
SOFTWARE\IvoSoft\ClassicShell
Software\Microsoft\Windows
HTML Help
Help
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
{C44AC417-05E6-41B8-8511-BDAB43407671}
Software\HotspotShield
Software\Microsoft\Windows\CurrentVersion\Uninstall
{11AC3232-E7D7-49CD-ABFE-501700100B3A}
IntelCpHeciSvc.EXE
IntelCpHeciSvc.CphsSession.1
CLSID
IntelCpHeciSvc.CphsSession

{C41B1461-3F8C-4666-B512-6DF24DE566D1}
ProgID
VersionIndependentProgID
Programmable
LocalServer32
TypeLib
Software\Microsoft\Office\12.0\Common\FilesPaths
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Components\621EAA421190F8740A91708B57BE9969
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Components\621EAA421190F8740A91708B57BE9969
Software\Classes\Installer\Components\621EAA421190F8740A91708B57BE9969
SOFTWARE\JavaSoft\Java Update\Policy
.DEFAULT
S-1-5-19
S-1-5-20
S-1-5-21-3979321414-2393373014-2172761192-1000
S-1-5-21-3979321414-2393373014-2172761192-1000_Classes
S-1-5-18
JavaSoft
Java Runtime Environment
SOFTWARE\Classes
.386
.a
.ai
.aif
.aifc
.aiff
.ani
.ans
.application
.appref-ms
.aps
.art
.asa
.asc
.ascx
.asf
.asm
.asmx
.aspx
.asx
.au
.avi
.bcp
.bin
.bkf
.blg
.bmp
.bsc
.c
.cab
.camp
.cat
.cc
.cda
.cdmp
.cdx
.cgm
.chk
.cls
.cod
.compositefont
.contact
.cpp
.crd
.crds
.crl
.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
.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\
Control Panel\Mouse
Software\AutoIt v3\AutoIt
Software\Microsoft\Windows\CurrentVersion\App Paths\PhotoPlus2
Software\Microsoft\Windows\CurrentVersion\App Paths\Mobile Gamepad.exe
SOFTWARE\Microsoft\NET Framework Setup\NDP
Software\Intel\Display\igfxcui\igfxtray\TrayIcon
Software\SMART Technologies
Software\SMART Technologies\Notebook Software\Math Tools
Software\SMART Technologies\Notebook Software\Mixed Reality
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\UpgradeCodes\63E2592C964A38643B6969F7215E413D
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\UpgradeCodes\63E2592C964A38643B6969F7215E413D
Software\Classes\Installer\UpgradeCodes\63E2592C964A38643B6969F7215E413D
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\UpgradeCodes\4C4787BF3F922904382C6663DE445DB2
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\UpgradeCodes\4C4787BF3F922904382C6663DE445DB2
Software\Classes\Installer\UpgradeCodes\4C4787BF3F922904382C6663DE445DB2
Software\SMART Technologies\Response\Install Information
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\UpgradeCodes\0268C3B99638BC2429DE1D144E2A6D9D
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\UpgradeCodes\0268C3B99638BC2429DE1D144E2A6D9D
Software\Classes\Installer\UpgradeCodes\0268C3B99638BC2429DE1D144E2A6D9D
Software\AutoHelpDesk\1.8.0.0
{287b2c47-0d1d-4055-95b6-5d13b8c45410}
Software\Brother\BrUtilities
Software\WinRAR\General
Software\WinRAR\Paths
Software\WinRAR\Profiles
Software\WinRAR\Profiles\0
Software\WinRAR\Profiles\1
Software\WinRAR\Profiles\2
Software\WinRAR\Profiles\3
Software\WinRAR\Profiles\4
Software\WinRAR\Policy
Software\WinRAR
Software\WinRAR\Interface\Themes
Software\WinRAR\General\Toolbar\Buttons
Software\Microsoft\Windows\CurrentVersion\Uninstall\PDF Reader for Windows_is1
CLSID\{D27CDB6E-AE6D-11cf-96B8-444553540000}\InprocServer32
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Age of Empires III - Complete Collection_Origami_is1
Software\Mozilla\Firefox\TaskBarIDs

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{585C5E36-62B1-4CA1-827B-83C4A4486CA5}
Software\Microsoft\InetStp
Software\Microsoft\Windows\CurrentVersion\Uninstall\InstallShield Uninstall Information\{585C5E36-62B1-4CA1-827B-83C4A4486CA5}
Software\Microsoft\Windows\CurrentVersion\Uninstall\{585C5E36-62B1-4CA1-827B-83C4A4486CA5}
Software\InstallShieldPendingOperation
DEFAULT_READ_STRING
NI\3100fc55\11a239d9
NI\30ea5c07\2bc166a
SOFTWARE\InstallShield\15.0\Professional
Software\InstallShield\ISWI\7.0\SetupExeLog
SOFTWARE\Rockstar Games\Rockstar Games Social Club
Software\Rockstar Games\RockStar Games Social Club
{4031db0c-b05e-43bd-ac1b-e1f4d5da0516}
SYSTEM\CurrentControlSet\Services\KMSServerService\Parameters
${Regkey_Parameters}
Software\Logitech\Parameters
Software\Logitech\CDDRV3
SOFTWARE\Rational Software\IntegrationManager
SOFTWARE\Microsoft\Visual Modeler\IntegrationManager
Software\Microsoft\Office\9.0\Common
Software\Microsoft\Windows\CurrentVersion\App Paths\PowerDirector14
SOFTWARE\SecureWebChannel
Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice
Software\Wilson WindowWare\Settings\WWW-PROD\WB44I
Software\Microsoft\Windows NT\CurrentVersion\VFW
Software\Wilson WindowWare\Settings\WWWBATCH\MAIN
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\
Software\Toshiba\swtos
SOFTWARE\CyberLink\PowerDVD12
System
Software\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.
Meiryo
Malgun Gothic
Microsoft YaHei
Microsoft JhengHei
Software\Mindspark
CLSID\{a899079d-206f-43a6-be6a-07e0fa648ea0}\InprocServer32
Software\Microsoft\Windows\CurrentVersion\Uninstall\GamingWonderlandTooltab Uninstall Internet Explorer
SYSTEM\CurrentControlSet\Services\crypt32
CLSID\{E50C953D-311A-481B-8F8D-C55E65AF7417}
AppID\sample
Software\Microsoft\OLE\AppCompat
SOFTWARE\Microsoft\OLE
SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider
Software\Policies\Microsoft\Cryptography
Software\Microsoft\Cryptography
Software\Microsoft\Cryptography\Offload
Interface\{00000134-0000-0000-C000-000000000046}
ProxyStubClsid32
SYSTEM\CurrentControlSet\Services\BFE
CLSID\{9CAAD2EA-177B-4D07-871F-47255B5D30F3}
CLSID\{B391A1DB-28C8-4506-A43C-5BD6051F16BA}
CLSID\{915C2CEB-216B-4B7C-89E4-9ED3512D58D9}
CLSID\{92C5E738-7372-4CD6-BE57-15833624EBF3}
CLSID\{661AFD8A-110A-4E98-A4D9-7B063E3752E3}
CLSID\{E9A93328-79D4-4AED-A778-146E7191F8BC}
CLSID\{623E415A-22EF-4DAA-A2FF-E68E77A673C9}
Software\Adobe
OpenWithList
OpenWithProgids
.ex$
FileExts
SOFTWARE\Adobe
Software\Microsoft\Direct3D\MostRecentApplication
SOFTWARE\Microsoft\Direct3D\MostRecentApplication
SOFTWARE\Microsoft\Direct3D
SOFTWARE\Classes\TypeLib
{00000200-0000-0010-8000-00AA006D2EA4}
2.0
win32
FLAGS
HELPDIR
{00000201-0000-0010-8000-00AA006D2EA4}
2.1
{00000205-0000-0010-8000-00AA006D2EA4}
2.5
{00000206-0000-0010-8000-00AA006D2EA4}
2.6

{00000300-0000-0010-8000-00AA006D2EA4}
2.8
6.0
{00000600-0000-0010-8000-00AA006D2EA4}
{00020430-0000-0000-C000-000000000046}
1.0
win64
{000204EF-0000-0000-C000-000000000046}
{00025E01-0000-0000-C000-000000000046}
5.0
{000C1092-0000-0000-C000-000000000046}
409
{00A40DB9-D8B4-40B3-8E0C-A8E8C6B3B720}
{00D25261-A9E4-40B2-BF1E-A8A13DF2542A}
{00F25AE8-3625-4E34-92D4-F0918CF010EE}
{0109E0F4-91AE-4736-A2CE-9D63E89D0EF6}
{0249F559-489F-4977-A0EF-21352C5AD247}
{03837500-098B-11D8-9414-505054503030}
{058F2991-6ADD-4948-89AF-82F58BCF2CCD}
{06290C00-48AA-11D2-8432-006008C3FBFC}
{0A055C02-BABE-4480-BB7B-A8EC723CE9C0}
{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}
{0FFF9602-69CF-4728-9EA4-141514866CA2}
{10E3A8C1-B46C-4B6C-B3EF-8E2F48D527D0}
{11A8B8EE-BF30-409A-8EF7-3A143EF70332}
{11DD5EA9-F8DB-4F6E-BF7C-6AADBA404A3D}
{122F1BB4-2723-4ac2-A36A-16BB9E8B99A6}
{13199C00-7494-11D0-8816-00A0C903B83C}
{1320AD9E-A50F-4ED0-B1A4-4E45EC25005E}
{150E2D7A-DAC1-4582-947D-2A8FD78B82CD}
{157702D8-B1C1-40B8-8B46-AF2B40022085}
{15AE3A36-E53B-454d-A816-A7C61CBAB8A4}
Win32
{194508A0-B8D1-473E-A9B6-851AAF726A6D}
{1B773E42-2509-11CF-942F-008029004347}
3.7
{1B8D8AE1-A595-4687-A7AD-9E3828E09B79}
{1C565858-F302-471E-B409-F180AA4ABEC6}
{1C82EAD8-508E-11D1-8DCF-00C04FB951F9}
{1EA4DBF0-3C3B-11CF-810C-00AA00389B71}
1.1
{1fda955a-61ff-11da-978c-0008744faab7}
{204810B3-73B2-11D4-BF42-00B0D0118B56}
{215D64D2-031C-33C7-96E3-61794CD1EE61}
{21D6D480-A88B-11D0-83DD-00AA003CCABD}
{2206CEB0-19C1-11D1-89E0-00C04FD7A829}
{22813728-8BD3-11D0-B4EF-00A0C9138CA4}
{22fb0827-65d0-4c68-8e4f-25d30a422a1d}
{22FDDF82-3032-4174-B179-DC0BFFEBBE62}
{2358C810-62BA-11D1-B3DB-00600832C573}
4.0
{2735412F-7F64-5B0F-8F00-5D77AFBE261E}
{28DCD85B-ACA4-11D0-A028-00AA00B605A4}
{2A005C00-A5DE-11CF-9E66-00AA00A3F464}
{2A75196C-D9EB-4129-B803-931327F72D5C}
{2BF34C1A-8CAC-419F-8547-32FDF6505DB8}
{2C941FD0-975B-59BE-A960-9A2A262853A5}
{2E7D6A71-56CE-4A77-B58F-05DFFF85E251}
{3050F1C5-98B5-11CF-BB82-00AA00BDCE0B}
{3050F4E0-98B5-11CF-BB82-00AA00BDCE0B}
{306F05ED-1019-42A4-B94F-88A057E6736A}
{333C7BC1-460F-11D0-BC04-0080C7055A83}
{353D638F-C81B-4476-8323-63A7EE274205}
{372FCE32-4324-11D0-8810-00A0C903B83C}
{3BAA3119-ECA1-4A32-9A08-595E71AE9DA9}
{3D5905E0-523C-11D1-9FEA-00600832DB4A}
{3DE641EF-0556-4D4A-98D5-7DBD8AD5D70F}
{3EA49599-AF67-4142-B379-C54786F112B2}
{3F4DACA7-160D-11D2-A8E9-00104B365C9F}
5.5
{410381CD-AF42-11D1-8F10-00C04FC2C17B}
{420B2830-E718-11CF-893D-00A0C9054228}
{43136EB0-D36C-11CF-ADBC-00AA00A80033}
{438EDB38-282C-435D-8BE3-4AB90B83CEF5}
{43E734CA-043D-4A70-9A2C-A8F254063D91}
{4486DF98-22A5-4F6B-BD5C-8CADCEC0A6DE}
{44EC0535-400F-11D0-9DCD-00A0C90391D3}
{4A105F44-A270-4796-883B-241A7F362A13}

{4b21f542-0eb5-4205-a12b-59bf2f2555fe}
{4B2E957D-0393-11D1-B1AB-00AA00BA3258}
{4E14FB90-2E22-11D1-9964-00C04FBBB345}
{4F47FCF0-E864-4D97-B309-2F5902306128}
{4FB2D46F-EFC8-4643-BCD0-6E5BFA6A174C}
{501D5FC6-FEA2-4453-B1CF-17E462143EE6}
{50A7E9B0-70EF-11D1-B75A-00A0C90564FE}
{5190C4AF-AB0F-4235-B12F-D5A8FA3F854B}
{54314D1D-35FE-11D1-81A1-0000F87557DB}
{5477469E-83B1-11D2-8B49-00A0C9B7C9C4}
{54AF9343-1923-11D3-9CA4-00C04F72C514}
2.32
{563DC060-B09A-11D2-A24D-00104BD35090}
{565783C6-CB41-11D1-8B02-00600806D9B6}
1.2
{56A868B0-0AD4-11CE-B03A-0020AF0BA770}
{56BC53D1-96DB-11D1-BF3F-000000000000}
{56D04F5D-964F-4DBF-8D23-B97989E53418}
1.5
{58FBCF7C-E7A9-467C-80B3-FC65E8FCCA08}
{5C65924B-E236-11D2-8899-00104B2AFB46}
{5E77EB03-937C-11D1-B047-00AA003B6061}
{5F099F16-6A6E-4BBC-8BD8-98F3221D58C4}
{613808A3-159B-4D91-B4F0-A22AEE2D1AAC}
{61E207A5-827C-42E9-ADFA-165C6A745EE4}
{640D3148-A423-11D2-B943-00C04F79D22F}
{662901FC-6951-4854-9EB2-D9A2570F2B2E}
5.1
{680C64B0-8DA2-4399-BF4B-E94C1E52983E}
{686ba761-d755-4927-929f-94c8f67af1df}
{6A379714-E19D-4D0F-AAC6-20D5F143C420}
{6B100E1A-1385-4D1F-A02E-6E705A76BB6C}
{6BC09690-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096BB-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC096C5-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC09890-0CE6-11D1-BAAE-00C04FC2E20D}
{6BC098A0-0CE6-11D1-BAAE-00C04FC2E20D}
{6CAAAA3B-6502-40FE-97FC-72A290DC63CF}
{6EB22880-8A19-11D0-81B6-00A0C9231C29}
{7071EC00-663B-4BC1-A1FA-B97F3B917C55}
{714DD4F6-7676-4BDE-925A-C2FEC2073F36}
{728ab348-217d-11da-b2a4-000e7bbb2b09}
{73CA1716-D932-4015-A5DA-0B8037C24788}
{7444C709-39BF-11D1-8CD9-00C04FC29D45}
{74C08640-CEDB-11CF-8B49-00AA00B8A790}
{7501FE6A-42E9-4859-ADAF-AC5A88589B7B}
{7586B340-EC08-11D0-A466-00C04FC30DF6}
{773F1B9A-35B9-4E95-83A0-A210F2DE3B37}
{777BA810-2498-4875-933A-3067DE883070}
{777BA8F1-2498-4875-933A-3067DE883070}
{77A6BD8A-AB60-49FF-853C-B6EE7BABAF96}
{78530B68-61F9-11D2-8CAD-00A024580902}
{7988B57C-EC89-11cf-9C00-00AA00A14F56}
{7999FC20-D3C6-11CF-ACAB-00A024A55AEF}
{7c5a40ae-c944-45d0-ae56-9168519d4048}
{7CDB4C42-D09D-4532-AF9D-B941DF2F3E24}
{7D868ACD-1A5D-4A47-A247-F39741353012}
{7E8BC440-AEFF-11D1-89C2-00C04FB6BFC4}
{81DDF732-4AA8-4A35-BDFF-8B42EFE7C624}
{833E4000-AFF7-4AC3-AAC2-9F24C1457BCE}
{8405D0DF-9FDD-4829-AEAD-8E2B0A18FEA4}
{84E2B44A-0627-43AE-AB85-C0E3C0FFFD49}
{85C3F8F7-CFCE-4259-87FF-CAB1F4521F6E}
{8628F27C-64A2-4ED6-906B-E6155314C16A}
{87099223-C7AF-11D0-B225-00C04FB6C2F5}
{87D5F036-FAC3-4390-A1E8-DFA8A62C09E7}
{8acc2016-04a3-4343-b8e1-1870e35d6a41}
{8C11EFA1-92C3-11D1-BC1E-00C04FA31489}
{8C389764-F036-48F2-9AE2-88C260DCF43B}
{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}
{8cec5857-07a1-11d9-b15e-000d56bfe6ee}
{8cec5860-07a1-11d9-b15e-000d56bfe6ee}
{8cec5899-07a1-11d9-b15e-000d56bfe6ee}
{8D810F97-C1A1-49CA-9902-A7B7E58AF009}
{8E80422B-CAC4-472B-B272-9635F1DFEF3B}
{928CEF0C-5A84-48AC-BF37-C5C21039B83A}
{92AD68AA-17E0-11D1-B230-00C04FB9473F}
{92F94BE2-8C2E-4cd6-88ED-774A5DF42AD3}

{9381D8F6-0288-11D0-9501-00AA00B911A5}
{944DE083-8FB8-45CF-BCB7-C477ACB2F897}
{94A0E92D-43C0-494E-AC29-FD45948A5221}
{94F6FF32-37C3-11D2-8840-00104B2AFB46}
{95CEF0E5-A4ED-4703-B501-AE70A153697A}
{97d25db0-0363-11cf-abc4-02608c9e7553}
{98315905-7BE5-11D2-ADC1-00A02463D6E7}
{9B085638-018E-11D3-9D8E-00C04F72D980}
{9C757116-4367-4DA9-AC0E-6C6577AD5560}
{9CDCD9C9-BC40-41C6-89C5-230466DB0BD0}
{9E175B60-F52A-11D8-B9A5-505054503030}
{9E175B61-F52A-11D8-B9A5-505054503030}
{A1A6B98C-497F-11D1-9217-00C04FBBBFB3}
{A1B0DE63-7454-4184-B5B6-6ACFDAC5C9A6}
{A1B9E03C-3226-11D2-883E-00104B2AFB46}
{A7201431-623E-44A7-A85C-D13AFC0F6AA6}
{A7C01D63-4403-4BE2-B1AF-6EE0A2E6A1E9}
{AAA49BB1-378C-4206-9CAD-53C3372E9550}
{ABBA0019-3075-11D6-88A4-00B0D0200F88}
{AC3B8B4C-B6CA-11D1-9F31-00C04FC29D52}
{ACD4155A-3272-4ad2-A10F-3C844669C6E4}
{ACDF1C98-A273-43B0-959D-6935F7A723BE}
{AD5A0B88-4027-44E2-8626-461FEC6906A2}
{ADB880A2-D8FF-11CF-9377-00AA003B7A11}
{ADE6CC63-3C0E-4B9B-8C59-2DF6E652990A}
{AEB84C80-95DC-11D0-B7FC-B61140119C4A}
{B0A20F08-4B8A-4BDE-9735-8CFC250A6B4B}
{B0C2A63F-AFF8-40E3-B42D-8A542DC909EC}
{B0EDF154-910A-11D2-B632-00C04F79498E}
{B3A00612-1423-4072-A4F9-DE2ADCAA7F3C}
{B596CC9F-56E5-419E-A622-E01BB457431E}
{B691E011-1797-432E-907A-4D8C69339129}
6.1
{B806F1A7-6278-405A-ABE4-E1AA3A3A550B}
{B9C76E7B-D029-44EB-896F-F02FC6E9ABD5}
{BACEDF3E-74AB-11D0-B162-00AA00BA3258}
{BD96C556-65A3-11D0-983A-00C04FC29E30}
{BED7F4EA-1A96-11D2-8F08-00A0C9A6186D}
{BEE4BFEC-6683-3E67-9167-3C0CBC68F40A}
{C2A2B169-4052-4037-88D9-E274AF31C6F7}
{C4F9D6EB-4FBB-3341-A582-AEA37ED6DA94}
8.0
{C5C5C500-3ABC-11D6-B25B-00C04FA0C026}
{C866CA3A-32F7-11D2-9602-00C04F8EE628}
5.4
{c8b522d5-5cf3-11ce-ade5-00aa0044773d}
{CB72A544-F75E-42CB-932E-EB06A7063A66}
Flags
{CC802D05-AE07-4C15-B496-DB9D22AA0A84}
{CD000000-8B95-11D1-82DB-00C04FB1625D}
{CD6C7865-5864-11D0-ABF0-0020AF6B0B7A}
{CF30ADE7-9965-4cf8-BB05-524086FBCCB2}
{CFADAC75-E12C-11D1-B34C-00C04F990D54}
{d0b7e02b-e1a3-11dc-81ff-001185ae5e76}
{D3295D86-D604-11D4-A704-00C04FA137E4}
{D3295D87-D604-11D4-A704-00C04FA137E4}
{D37E2A3E-8545-3A39-9F4F-31827C9124AB}
{D5090061-1F23-4611-8821-7B759123AE68}
{D597DEED-5B9F-11D1-8DD2-00AA004ABD5E}
HARDWARE\DESCRIPTION\System\CentralProcessor\0
System\CurrentControlSet\Control\Video\{B285A319-4BD4-4785-A840-9BDC49C97EFA}\0000
Software\Microsoft\Windows NT\CurrentVersion\OpenGLDrivers
VBoxOGL
Software\Google\Update\ClientStateMedium\{8A69D345-D564-463C-AFF1-A69D9E530F96}
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\ELM
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Binding\Hardware\AutoActivation
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui\Activation\Manual
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui\Activation\Manual\Sms
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui\Activation\Buy
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui\Support
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Protection\Gui\About
SOFTWARE\Crytek Unkraine LLC\Warface\Keys\Settings\Binding
Software\McAfee\SystemCore
SOFTWARE\Policies\WiX\Burn
SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.5
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
IE_Bar

FEATURE_USE_IETLDLIST_FOR_DOMAIN_DETERMINATION
Content
Cookies
History
{186d55b6-3e7a-4ecf-b2fd-cf1752c37935}
Software\Google\Update\ClientState\{8A69D345-D564-463c-AFF1-A69D9E530F96}
Software\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome
Software\Caphyon\Advanced Updater\Settings
SOFTWARE\GenerousDeal
Courier New
Software\Mozilla
SOFTWARE\WildTangent\InstalledSKUs\
FEATURE_GPU_RENDERING
FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120
FEATURE_ARIA_SUPPORT
FEATURE_LEGACY_DISPPARAMS
FEATURE_PRIVATE_FONT_SETTING
FEATURE_CSS_SHOW_HIDE_EVENTS
FEATURE_DISPLAY_NODE_ADVISE_KB833311
FEATURE_ALLOW_EXPANDURI_BYPASS
FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245
FEATURE_DATABINDING_SUPPORT
FEATURE_ENFORCE_BSTR
FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING
FEATURE_OBJECT_CACHING
FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW
FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454
FEATURE_DOWNLOAD_INITIATOR_HTTP_HEADER
FEATURE_MOBILE_CUSTOMIZATIONS
FEATURE_HIGH_RESOLUTION_AWARE
FEATURE_FORCE_DISABLE_UNTRUSTEDPROTOCOL
FEATURE_USE_WEBOC_OMNAVIGATOR_IMPLEMENTATION
FEATURE_USE_SECURITY_THUNKS
FEATURE_DISABLE_DEFERRED_IMAGE_DOWNLOAD
FEATURE_LAZY_IMAGE_DECODING
FEATURE_LAZIER_IMAGE_DECODING
FEATURE_ALLOW_INTRANET_CSS_MIME_MISMATCH
FEATURE_ENABLE_CLIPCHILDREN_OPTIMIZATION
FEATURE_ENABLE_LARGER_HIT_TEST
FEATURE_USE_LEGACY_JSCRIPT
FEATURE_MOBILE_VIEWPORT_WIDTH_RESTRICTIONS
FEATURE_PASTE_IMAGE_DATAURI
FEATURE_NEW_TREE_VERIFICATION
FEATURE_MOBILE_DISPOSABLE_RESOURCE_CACHE_THRESHOLD_BYTES
FEATURE_DOCUMENT_COMPATIBLE_MODE
FEATURE_ENABLE_WEB_CONTROL_VISUALS
FEATURE_XDOMAINREQUEST
FEATURE_WEBSOCKET
FEATURE_USE_UNISCRIBE
FEATURE_PAINT_INSIDE_WMPAINT
FEATURE_SOFTWARE_FILTER_RENDERING
FEATURE_SPELLCHECKING
FEATURE_FORCE_NATURAL_TEXT_METRICS
FEATURE_ENABLE_PERFWIDGET_EXTRA_INFO
FEATURE_DISABLE_FORMAT_REUSE
FEATURE_ALLOW_WINDOW_PUTNAME_CROSS_DOMAIN
FEATURE_REDUCE_RENDER_AHEAD_CACHE
FEATURE_CLEANUP_AT_FLS
Software\Microsoft\Windows\CurrentVersion\App Paths\OUTLOOK.EXE
Software\Microsoft\Internet Explorer\Application Compatibility
Software\Policies\Microsoft\Internet Explorer\DOMStorage
Software\Microsoft\Internet Explorer\DOMStorage
NI\1f142fa1\822ccb2
policy.1.0.Microsoft.Practices.CompositeUI.WinForms__77af1478c1aac759
NI\190ccbdc\2195e275
SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting
SOFTWARE\Microsoft\PCHealth\ErrorReporting
SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting\ExclusionList
SOFTWARE\Microsoft\PCHealth\ErrorReporting\ExclusionList
SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting\InclusionList
SOFTWARE\Microsoft\PCHealth\ErrorReporting\InclusionList
SOFTWARE\Microsoft\Windows NT\CurrentVersion\msasn1
SOFTWARE\Bulmar\Client
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\v4\Client

Software\CatalinaGroup\Update\Clients\{6C598730-F715-407B-A7AE-A8F10D0F8FA7}
SOFTWARE\JavaSoft\Java Runtime Environment\
SOFTWARE\ej-technologies\exe4j\locatedjvms\
SOFTWARE\StrongSignal
SOFTWARE\Microsoft\Windows Defender
software\microsoft\windows nt\currentversion\perflib
Software\Microsoft\Windows\CurrentVersion\App Paths\miranda64.exe
Software\V9\WinZipper\General
SOFTWARE\VBP
Software\Enigma Protector\D98C1DD404B2008F-980980E97E42F8EC\D98C1DD404B2008F-980980E97E42F8EC
Software\WinRAR SFX
SOFTWARE\PassandPlay
Software\Microsoft\Windows\CurrentVersion\Uninstall\Clock Night Butterfly New Free Screensaver_is1
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration
{e745ce26-593d-400b-a02e-f9bda91946f0}
exefile\shell\open\command
SOFTWARE\COMODO\CIS\DbgTrace\
SYSTEM\CurrentControlSet\Services\CmdAgent\CisConfigs
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\UpgradeCodes\53A3CEBD8A4007A4DBB74F6245579865
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\UpgradeCodes\53A3CEBD8A4007A4DBB74F6245579865
Software\Classes\Installer\UpgradeCodes\53A3CEBD8A4007A4DBB74F6245579865
SOFTWARE\Microsoft\NET Framework Setup\NDP\v3.0
Software\Intel\ICCInst
Software\Microsoft\Windows\CurrentVersion\Uninstall\{409CB30E-E457-4008-9B1A-ED1B9EA21140}
PROTOCOLS\Name-Space Handler\
PROTOCOLS\Name-Space Handler\file\
PROTOCOLS\Name-Space Handler*\
Software\Intel\Setup$
Software\Google\ChromeFrame
Software\Google\Update\Clients\{8A69D345-D564-463c-AFF1-A69D9E530F96}
htmlfile\shell\open\command
v4.0.20926
HARDWARE\DESCRIPTION\System\FloatingPointProcessor
Software\Microsoft\Windows\CurrentVersion\Uninstall\{8A8EA42B-B6DA-49D5-A2B6-4693F1EB36D2}
System\CurrentControlSet\Control\SafeBoot\minimal
System\CurrentControlSet\Control\SafeBoot\M
AppInfo
AppMgmt
Base
Boot Bus Extender
Boot file system
CryptSvc
DcomLaunch
EFS
EventLog
File system
Filter
HelpSvc
KeyIso
Netlogon
NTDS
PCI Configuration
PlugPlay
PNP Filter
Power
Primary disk
ProfSvc
RpcEptMapper
RpcSs
sacsvr
SCSI Class
sermouse.sys
SWPRV
System Bus Extender
TabletInputService
TBS
TrustedInstaller
VDS
vga.sys
vgasave.sys
vmms
volmgr.sys
volmgrx.sys
WinDefend
WinMgmt
WudfPf
WudfRd

WudfSvc
{36FC9E60-C465-11CF-8056-444553540000}
{4D36E965-E325-11CE-BFC1-08002BE10318}
{4D36E967-E325-11CE-BFC1-08002BE10318}
{4D36E969-E325-11CE-BFC1-08002BE10318}
{4D36E96A-E325-11CE-BFC1-08002BE10318}
{4D36E96B-E325-11CE-BFC1-08002BE10318}
{4D36E96F-E325-11CE-BFC1-08002BE10318}
{4D36E977-E325-11CE-BFC1-08002BE10318}
{4D36E97B-E325-11CE-BFC1-08002BE10318}
{4D36E97D-E325-11CE-BFC1-08002BE10318}
{4D36E980-E325-11CE-BFC1-08002BE10318}
{533C5B84-EC70-11D2-9505-00C04F79DEAF}
{6BDD1FC1-810F-11D0-BEC7-08002BE2092F}
{71A27CDD-812A-11D0-BEC7-08002BE2092F}
{745A17A0-74D3-11D0-B6FE-00A0C90F57DA}
{D48179BE-EC20-11D1-B6B8-00C04FA372A7}
{D94EE5D8-D189-4994-83D2-F68D7D41B0E6}
System\CurrentControlSet\Control\SafeBoot\NetWork
System\CurrentControlSet\Control\SafeBoot\N
AFD
BFE
bowser
Browser
dfsc
Dhcp
DnsCache
Dot3Svc
Eaphost
IKEEXT
ipnat.sys
LanmanServer
LanmanWorkstation
LmHosts
Messenger
MPSDrv
MPSSvc
mrxsmb
mrxsmb10
mrxsmb20
NativeWifiP
NDIS
NDIS Wrapper
ndiscap
Ndisuio
NetBIOS
NetBIOSGroup
NetBT
NetDDEGroup
NetMan
netprofm
Network
NetworkProvider
NlaSvc
Nsi
nsiproxy.sys
PNP_TDI
PolicyAgent
rdbss
rdpencdd.sys
rdsessmgr
SCardSvr
SharedAccess
Streams Drivers
Tcpip
TDI
VaultSvc
Wlansvc
WudfUsbccidDriver
{4D36E972-E325-11CE-BFC1-08002BE10318}
{4D36E973-E325-11CE-BFC1-08002BE10318}
{4D36E974-E325-11CE-BFC1-08002BE10318}
{4D36E975-E325-11CE-BFC1-08002BE10318}
{50DD5230-BA8A-11D1-BF5D-0000F805F530}
t s
Software\Classes\CLSID\{4AA46D49-459F-4358-B4D1-169048547C23}
Software\Classes\CLSID\{B853E835-9F24-4F4B-B55C-E554D15CCCD2}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{C4ED781C-7394-4906-AAFF-D6AB64FF7C38}

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{889DF117-14D1-44EE-9F31-C5FB5D47F68B}
Software\GenericAddon
Software\SpeedChecker
Software\CheckMeUp
Software\CheckMeApp
Software\IneedSpeed
Software\SpeedCheck
Software\SpeeditUp
Software\BlockAndSurf
Software\Safer-Surf
Software\Wow6432Node\Classes\CLSID\{4AA46D49-459F-4358-B4D1-169048547C23}
Software\Wow6432Node\Classes\CLSID\{B853E835-9F24-4F4B-B55C-E554D15CCCD2}
Software\AppDataLow\Software\GenericAddon
Software\AppDataLow\Software\SpeedChecker
Software\AppDataLow\Software\CheckMeUp
Software\AppDataLow\Software\CheckMeApp
Software\AppDataLow\Software\IneedSpeed
Software\AppDataLow\Software\SpeedCheck
Software\AppDataLow\Software\SpeeditUp
Software\AppDataLow\Software\BlockAndSurf
Software\AppDataLow\Software\Safer-Surf
Software\Microsoft\Windows\CurrentVersion\Uninstall\thirteen degrees
SOFTWARE\Microsoft\{94ebd7b5-82ae-449t-b679-3d04078ed154}
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\NUIns
Software\Microsoft\Windows\CurrentVersion\Uninstall\VOPackage
Software\Microsoft\Windows\CurrentVersion\Uninstall\ASPackage
Software\DtsEncodeTools
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WeatherTool
Software\Microsoft\Windows\CurrentVersion\Uninstall\YSPackage
Software\Microsoft\Windows\CurrentVersion\Uninstall\Eppink
SOFTWARE\istartsurfSoftware\istartsurfhp
SOFTWARE\key-findSoftware\key-findhp
SOFTWARE\mystartsearchSoftware\mystartsearchhp
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\NUIns
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\VOPackage
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ASPackage
Software\Wow6432Node\DtsEncodeTools
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WeatherTool
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\YSPackage
Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Eppink
SOFTWARE\Wow6432Node\istartsurfSOFTWARE\Wow6432Node\istartsurfhp
SOFTWARE\Wow6432Node\key-findSOFTWARE\Wow6432Node\key-findhp
SOFTWARE\Wow6432Node\mystartsearchSOFTWARE\Wow6432Node\mystartsearchhp
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\VOPackage
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ASPackage
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Eppink
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\YSPackage
SOFTWARE\SearchProtect
Software\Wajam
Software\WajIEnhance
Software\WajaIEnhance
Software\WInternetEnhance
Software\WaInternetEnhance
Software\WajInternetEnhance
Software\WajaInternetEnhance
Software\WInterEnhance
Software\WaInterEnhance
Software\WajInterEnhance
Software\WajaInterEnhance
Software\WIntEnhance
Software\WaIntEnhance
Software\WajIntEnhance
Software\WajaIntEnhance
Software\WNEnhance
Software\WaNEnhance
Software\WajNEnhance
Software\WajaNEnhance
Software\WNetEnhance
Software\WaNetEnhance
Software\WajNetEnhance
Software\WajaNetEnhance
Software\WNetworkEnhance
Software\WaNetworkEnhance
Software\WajNetworkEnhance
Software\WajaNetworkEnhance
Software\WWebEnhance
Software\WaWebEnhance
Software\WajWebEnhance

Software\WajaWebEnhance
Software\WIEnhancer
Software\WaIEnhancer
Software\WajIEnhancer
Software\WajaIEnhancer
Software\WInternetEnhancer
Software\WaInternetEnhancer
Software\WajInternetEnhancer
Software\WajaInternetEnhancer
Software\WInterEnhancer
Software\WaInterEnhancer
Software\WajInterEnhancer
Software\WajaInterEnhancer
Software\WIntEnhancer
Software\WaIntEnhancer
Software\WajIntEnhancer
Software\WajaIntEnhancer
Software\WNEnhancer
Software\WaNEnhancer
Software\WajNEnhancer
Software\WajaNEnhancer
Software\WNetEnhancer
Software\WaNetEnhancer
Software\WajNetEnhancer
Software\WajaNetEnhancer
Software\WNetworkEnhancer
Software\WaNetworkEnhancer
Software\WajNetworkEnhancer
Software\WajaNetworkEnhancer
Software\WWebEnhancer
Software\WaWebEnhancer
Software\WajWebEnhancer
Software\WajaWebEnhancer
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\QuickSearch
SOFTWARE\shopperz101120152249
SOFTWARE\Wow6432Node\shopperz101120152249
SOFTWARE\shopperz100920151159
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Note-up
SOFTWARE\BrowserAir
Software\BrowserAir
Software\Microsoft\Windows\CurrentVersion\Uninstall\BrowserAir
Software\BoBrowser
Software\Microsoft\Windows\CurrentVersion\Uninstall\BoBrowser
Software\Nosibay\Bubble Dock Tag
Software\AVG
Software\McAfee
Software\Nosibay\Bubble Dock
SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\win_en_77_is1
SOFTWARE\Wow6432Node\WIN
SOFTWARE\Wow6432Node\CloudGuard
SOFTWARE\CloudGuard
SOFTWARE\7E745E7F7BAA4842A833716036DEBF6F
SOFTWARE\1832BFF4F2BF43989682B0AF5ECB8F68
SOFTWARE\4033691F40C1493E895E791CE3CF0976
SOFTWARE\32D26CAEEEFE4E83BD53C0261341085D
SOFTWARE\0E2A533F19374E488CF48F950F5A07F1
SOFTWARE\ D909B01E08AE40EEA47F9FA8D7CF746B
SOFTWARE\655ED0DD7DA047618002AF578ADFA012
SOFTWARE\3DE9D279B98F48E898283B1445515BDB
SOFTWARE\43B149F5CEBC46BC8103DE23FA2D99BF
SOFTWARE\ F370AC1ED9E143D29D6D3CA1F7A957B3
SOFTWARE\52F8D668751743D79231B4E61DF0D1EF
SOFTWARE\ESET
Software\ClamWin
SOFTWARE\5da059a482fd494db3f252126fbc3d5b
Software\Rtp
Software\Classes\GDSetup
Software\Avira
Software\X-AVCSD
Software\Smartbar
Software\RGMservice
Software\Pservice
SOFTWARE\Microsoft\Wbem\CIMOM
FEATURE_FILEPROTOCOL_NOFINDFIRST_KB947853
SOFTWARE\Classes\PROTOCOLS\Filter\text/xml
SOFTWARE\ZSMC\USBCAMERA\ZC0331\BigDogPath
FEATURE_INTERNET_SHELL_FOLDERS
SOFTWARE\Microsoft\Internet Explorer\MAIN

FEATURE_IEDDE_REGISTER_PROTOCOL
Software\microsoft\windows\CurrentVersion\run\
Software\Brother Industries
Software\Baidu\BaiduYunGuanjia
SOFTWARE\DigitalMore
{a06deb06-a11f-4b8e-92a0-24792bcc7372}
Software\ImageEd
SYSTEM\CurrentControlSet\Control\ProductOptions
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\UpgradeCodes\962FB17ADE4EE7C4A9AC395E81851F91
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\UpgradeCodes\962FB17ADE4EE7C4A9AC395E81851F91
Software\Classes\Installer\UpgradeCodes\962FB17ADE4EE7C4A9AC395E81851F91
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\963B028B2702ED94AA374AD0CF26D047
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\963B028B2702ED94AA374AD0CF26D047
Software\Classes\Installer\Products\963B028B2702ED94AA374AD0CF26D047
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\963B028B2702ED94AA374AD0CF26D047\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\E2BDD19A14CA45646BFAF4C600AAB021
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\E2BDD19A14CA45646BFAF4C600AAB021
Software\Classes\Installer\Products\E2BDD19A14CA45646BFAF4C600AAB021
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\E2BDD19A14CA45646BFAF4C600AAB021\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\5581FF49C7EEC8949B73086FDCEAB658
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\5581FF49C7EEC8949B73086FDCEAB658
Software\Classes\Installer\Products\5581FF49C7EEC8949B73086FDCEAB658
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\5581FF49C7EEC8949B73086FDCEAB658\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\817C45898A4865E44B2DEB20C9DBD10B
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\817C45898A4865E44B2DEB20C9DBD10B
Software\Classes\Installer\Products\817C45898A4865E44B2DEB20C9DBD10B
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\817C45898A4865E44B2DEB20C9DBD10B\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\87C96EC690102B34FAE936F0A0566986
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\87C96EC690102B34FAE936F0A0566986
Software\Classes\Installer\Products\87C96EC690102B34FAE936F0A0566986
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\87C96EC690102B34FAE936F0A0566986\InstallProperties
Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-3979321414-2393373014-2172761192-1000\Installer\Products\06BB24D7561BBE544980417D23556DB5
S-1-5-21-3979321414-2393373014-2172761192-1000\Software\Microsoft\Installer\Products\06BB24D7561BBE544980417D23556DB5
Software\Classes\Installer\Products\06BB24D7561BBE544980417D23556DB5
Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\06BB24D7561BBE544980417D23556DB5\InstallProperties
PROTOCOLS\Name-Space Handler\http\
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
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
NI\159a66b8\424bd4d8
NI\159a66b8\424bd4d8\17
SOFTWARE\Internal\Debuger
NI\6faf58\19ab8d57
NI\6faf58\19ab8d57\15
IL\75638fee\27002c8f\5a
policy.2.0.System.Data.SqlXml__b77a5c561934e089
Software\Google\Update\ClientStateMedium\
Software\Google\Update
http\shell\open\command
Software\Wine
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\Kaseya\Debug
SOFTWARE\Kaseya\Relay
Software\Microsoft\Windows\CurrentVersion\Uninstall\VPNetwork LLC TorGuard
SOFTWARE\InnovateDirect
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Brothers in Arms - Hell's Highway
SOFTWARE\GameVicio\Brothers in Arms Hells Highway
FEATURE_CREATE_URL_MONIKER_DISABLE_LEGACY_COMPAT
FEATURE_ENABLE_COMPAT_LOGGING
SOFTWARE\Classes\PROTOCOLS\Filter\image/gif
Software\Microsoft\NET Framework Setup\NDP\v3.5
HARDWARE\ACPI\DSDT\VBOX__
SOFTWARE\Mozilla\Mozilla Firefox
CLSID\{3041D03E-FD4B-44E0-B742-2D9B88305F98}
CLSID\{F0D4B239-DA4B-4daf-81E4-DFEE4931A4AA}
CLSID\{D4027C7F-154A-4066-A1AD-4243D8127440}

PROTOCOLS\Name-Space Handler\about\
Software\Microsoft\Internet Explorer\MediaTypeClass
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\gamecenter@mail.ru.exe
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\HG64.exe

QueryFilePath

C:\DLL_Loader.exe
C:\sample
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Users\win7\AppData\Local\Temp\is-KS8O1.tmp\sample.tmp
C:\samp
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\kernel32.dll
C
0oFF=k
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\system32\RichEd20.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\cryptnet.dll
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\sxs.DLL
C:\Windows\system32\DNSAPI.dll
C:\CFVS_HookDll.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\version.DLL
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\api-ms-win-downlevel-advapi32-l1-1-0.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\syswow64\iertutil.dll
C:\Windows\syswow64\urlmon.dll
C:\Windows\syswow64\api-ms-win-downlevel-user32-l1-1-0.dll
C:\Windows\syswow64\WININET.dll
C:\Windows\syswow64\NSI.dll
C:\Windows\syswow64\WS2_32.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\oleaut32.DLL
C:\Windows\syswow64\api-ms-win-downlevel-version-l1-1-0.dll
C:\Windows\syswow64\ole32.DLL
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\api-ms-win-downlevel-shlwapi-l1-1-0.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\normaliz.DLL
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\syswow64\LPK.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\syswow64\USERENV.dll
C:\Windows\syswow64\api-ms-win-downlevel-ole32-l1-1-0.dll
C:\Windows\syswow64\profapi.dll
C:\Windows\syswow64\api-ms-win-downlevel-normaliz-l1-1-0.dll
C:\Windows\syswow64\nt0_dll.dll
C:\Windows\system32\mfc120u.dll
C:\Users\win7\AppData\Local\Temp\~nsuA.tmp\Au_.exe
C:\Windows\system32\riched20.dll
C:\Users\win7\AppData\Local\Temp\GLK85F6.tmp
C:\Users\win7\AppData\Local\Temp\GLC826B.tmp
C:\Windows\system32\RICHED20.dll
C:\Users\win7\AppData\Local\Temp\is-I5DN6.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-P0J1J.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-O161C.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-2OPOC.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\{80597657-8434-47F6-AB65-7562632CA922}\Disk1\ISSetup.dll
C:\Windows\system32\PROPSYS.dll
-33363537-
C:\Users\win7\AppData\Local\Temp\is-1Q78V.tmp\sample.tmp

C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-9MT3T.tmp\IsProgressBar.dll
C:\Users\win7\AppData\Local\Temp\is-55GHL.tmp\sample.tmp
C:\Users\win7\AppData\Local\Tem
C:\Windows\system32\dsound.dll
C:\Windows\system32\ieframe.dll
C:\Windows\system32\DINPUT8.dll
C:\Users\win7\AppData\Local\Temp\is-AE4H3.tmp\sample.tmp
C:\Windows\syswow64\oleaut32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\syswow64\shell32.dll
C:\Windows\syswow64\PSAPI.DLL
C:\Users\win7\AppData\Local\Temp\is-KB8TD.tmp\sample.tmp
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\system32\Msftedit.dll
C:\Windows\System32\msxml3.dll
C:\Users\win7\AppData\Local\Temp\is-ART3B.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-C5P3I.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-FP3PI.tmp\sample.tmp
C:\Windows\system32\dinput8.dll
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
C:\Windows\SysWOW64\schannel.dll
C:\Users\win7\AppData\Local\Temp\3423b6a\sample
C:\Windows\system32\RichEd20.DLL
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\FaultRep.dll
C:\Windows\system32\winmm.dll
C:\Windows\system32\oledlg.dll
C:\Windows\system32\winspool.drv
C:\Windows\system32\wsock32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_ec86b8d6858ec0bc\comctl32.dll
C:\Windows\system32\mpr.dll
C:\Windows\syswow64\WLDAP32.dll
C:\Windows\syswow64\comdlg32.dll
C:\Windows\syswow64\imm32.dll
C:\Windows\system32\RICHED20.DLL
C:\Windows\system32\mscoree.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\is-IVVGQ.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-K4N3O.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-GGQBF.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-3IOR7.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-174HO.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-31PJS.tmp\itdownload.dll
C:\Windows\system32\ODBC32.dll
C:\Users\win7\AppData\Local\Temp\is-NE69K.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-K135O.tmp\itdownload.dll
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\system32\WINMM.dll
C:\Windows\syswow64\SHELL32.dll
C:\Users\win7\AppData\Local\Temp\is-39PFH.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-VUMUC.tmp\sample.tmp
C:\Windows\system32\DSOUND.dll
C:\Users\win7\AppData\Local\Temp\is-M2S5S.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\{87700960-A2F8-42C3-BF22-0D1FC9943B0F}\Disk1\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{87700960-A2F8-42C3-BF22-0D1FC9943B0F}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{DCBEDD40-AECD-48A6-9407-F281C9DC1CC9}\{585C5E36-62B1-4CA1-827B-83C4A4486CA5}\ISRT.dll
C:\Windows\system32\DUser.dll
C:\Users\win7\AppData\Local\Temp\is-RM40P.tmp\sample.tmp
C:\Windows\system32\Riched20.dll
C:\Users\win7\AppData\Local\Temp\is-LF6P1.tmp\sample.tmp
C:\WBDJA44I.DLL
C:\Users\win7\AppData\Local\Temp\AIR5829.tmp\Install Balsamiq Mockups.exe
C:\Windows\system32\CRYPTNET.dll
C:\Users\win7\AppData\Local\Temp\is-0IF4F.tmp\sample.tmp
C:\Windows\system32\propsys.dll
C:\Users\win7\AppData\Local\Temp\is-4H118.tmp\sample.tmp
C:\Windows\system32\schannel.dll
C:\Windows\system32\aclui.dll
C:\Users\win7\AppData\Local\Temp\gdgED34.tmp
C:\Users\win7\AppData\Local\Temp\is-RPTE1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-QM6T0.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-LU37T.tmp\sample.tmp
c:\4b5a1df7161568b6de3fe1c5\MpSigStub.exe
C:\Windows\system32\credui.dll
C:\Users\win7\AppData\Local\Temp\is-JHAGV.tmp\sample.tmp
C:\Windows\system32\EhStorShell.dll

C:\Users\win7\AppData\Local\Temp\is-7F1VL.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-6U96K.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-KDNA2.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\RarSFX0\setup.exe
C:\Windows\SysWOW64\Wbem\WMIC.exe
C:\Windows\system32\STI.dll
C:\Windows\SysWOW64\sti.dll
C:\Windows\SysWOW64\Wbem\wmic.exe
C:\Users\win7\AppData\Local\Temp\~sml7h638q9.tmp
C:\Users\win7\AppData\Local\Temp\is-014TS.tmp\sample.tmp

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x56081761 [Sun Sep 27 16:20:49 2015 UTC]
Entry Point	0x402392 (.text)
File Size	543458
Machine Type	Intel 386 or later - 32Bit
Mime Type	application/x-dosexec
Number Of Sections	4
Sha256	0f79ab018d249fdf996b6f0002293af733464b2b93f1654e62de9943267b6c4d

File Paths

FILE PATH ON CLIENT	SEEN COUNT
0310_crypted.exe	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1763	0x2000	5.233043	-
.rdata	0x3000	0xd3f	0x1000	4.380620	-
.data	0x4000	0x2cf5	0x3000	3.036869	-
.rsrc	0x7000	0x45d9	0x5000	5.320841	-