VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: MultiHack_.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 1a85b35f61d9c19fa99fedc55c22938c570888f6
MD5: 6a0e423c72f0a14ef84c9c2e6dde2118
First Seen Date: 2015-10-05 19:46:44 UTC
Number of Clients Seen: 4
Last Analysis Date: 2016-04-09 05:22:48 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	2016-04-09 05:22:48 UTC	Malware	
Static Analysis Overall Verdict	2016-04-09 05:22:48 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-04-09 05:22:48 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	
Packer detection on signature database	Unknown	
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	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
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	

Anti-debug calls

- TerminateProcess
- UnhandledExceptionFilter
- IsDebuggerPresent

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
Highly Suspicious	

SUSPICIOUS BEHAVIORS	
Injects code to another process	
Modifies context of another process	
Creates a child process	
Writes to address space of another process	
Uses a function clandestinely	
Reads memory of another process	
Has no visible windows	

Behavioral Information

LoadLibrary

SHFOLDER
ole32.dll
comctl32.dll
ADVAPI32.dll
SHELL32.dll
propsys.dll
ntmarta.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\system32\ole32.dll
RichEd20
UxTheme.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
IMM32.dll
C:\Windows\system32\shell32.dll
C:\Users\win7\AppData\Local\Temp\nsw70DF.tmp\System.dll
USER32.dll
ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
SHLWAPI.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
COMCTL32
KERNEL32
msi.dll
imm32.dll
C:\Windows\system32\DSOUND.dll
KERNEL32.dll
kernel32.dll
psapi.dll
advapi32.dll
dbghelp.dll
version.dll
user32.dll
C:\sample
OLEACCRC.DLL
SspiCli.dll
dsound.dll
C:\Windows\system32\dsound.dll
SETUPAPI.dll
MMDEVAPI.DLL
CFGMGR32.dll
AUDIOSES.DLL
Advapi32.dll
uxtheme.dll

d3d9.dll
VBoxDisp.dll
Wtsapi32.dll
WINSTA.dll
RPCRT4.dll
CRYPTBASE.dll
gdi32.dll
msimg32.dll
Secur32.dll
api-ms-win-downlevel-advapi32-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
WS2_32.dll
winhttp.dll
IPHLPAPI.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
DNSAPI.dll
OLEAUT32.dll
urlmon.dll
dhcpcsvc.DLL
Comctl32.dll
C:\Windows\system32\ws2_32
bcrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
SXS.DLL
WININET.dll
MSHTML.dll
MLANG.dll
PROPSYS.dll
shell32.dll
mshtml.dll
IEFRAME.dll
CRYPTSP.dll
d2d1.dll
DWrite.dll
dxgi.dll
C:\DXGIDebug.dll
C:\Windows\system32\DXGIDebug.dll
setupapi.dll
WINTRUST.dll
d3d11.dll
D3D10Warp.dll
C:\Windows\system32\D3D10Warp.dll
C:\Windows\SysWOW64\urlmon.dll
msls31.dll
WindowsCodecs.dll
C:\Windows\system32\ntshrui.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
netutils.dll
C:\Users\win7\AppData\Local\Temp\nso793.tmp\System.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
VERSION.dll
C:\Windows\system32\ntoskrnl.exe
UTILDLL.dll
C:\Windows\System32\wininit.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\SearchIndexer.exe
C:\Windows\explorer.exe
C:\Windows\System32\cmd.exe
C:\Python27\python.exe
C:\Windows\System32\dllhost.exe
C:\CFVS_Injector.exe
C:\Windows\System32\taskkill.exe
C:\Windows\SysWOW64\TSAPPCMP.DLL
Ntdll.dll
C:\Windows\SysWOW64\SHLWAPI.DLL
C:\Windows\SysWOW64\OLE32.DLL
C:\Windows\SysWOW64\KERNEL32.DLL
MsiMsg.dll
C:\Windows\SysWOW64\SHELL32.DLL
C:\Windows\SysWOW64\NETAPI32.DLL
C:\Windows\SysWOW64\ADVAPI32.DLL
C:\Windows\SysWOW64\APPHELP.DLL

C:\Windows\SysWOW64\VERSION.DLL
C:\Windows\SysWOW64\sxs.DLL
C:\Windows\SysWOW64\MSCOREE.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.dll
C:\Windows\SysWOW64\NTDLL.DLL
MsiHnd.dll
DWMAPI
USER32
RICHED20.DLL
USP10.dll
Msi.DLL
CABINET
SHFolder.dll
CRYPT32.dll
USERENV.dll
secur32.dll
ncrypt.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.dll
WINHTTP.dll
ntdll.dll
NSI.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-Management-L2-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
profapi.dll
Cabinet.dll
DEVRTL.dll
C:\Windows\System32\shdocvw.dll
DCIMAN32.DLL
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
KERNEL32.DLL
WSOCK32.DLL
rasapi32.dll
imageres.dll
Kernel32.dll
wininet.dll
User32.dll
COMCTL32.dll
comdlg32.dll
GDI32.dll
NETAPI32.dll
oledlg.dll
WINMM.dll
WINSPOOL.DRV
C:\Windows\system32\UXTHEME.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\SETUPAPI.dll
C:\Windows\system32\SHFOLDER.dll
C:\Users\win7\AppData\Local\Temp\is-6PKQL.tmp_isetup_shfoldr.dll
shfolder.dll
C:\Windows\system32\imageres.dll
FaultRep.dll
gdiplus.dll
security.dll
C:\\libcef.dll
WS2_32.DLL
Fwpuclnt.dll
IdnDL.dll
Normaliz.dll
iphlpapi.dll
libeay32.dll
libcef.dll
C:\Windows\system32\propsys.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\System32\wship6.dll
C:\Windows\system32\rasadhlp.dll
C:\Windows\System32\wshtcpip.dll
C:\Windows\system32\mswsock.dll
C:\Windows\system32\WINNSI.DLL
C:\Windows\system32\iphlpapi.dll
C:\Windows\system32\IdnDL.dll
C:\Windows\system32\Fwpuclnt.dll
C:\Windows\system32\SECUR32.DLL
C:\Windows\system32\security.dll
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\FaultRep.dll

C:\Windows\system32\dwmapi.dll
C:\Windows\system32\d3d8thk.dll
C:\Windows\system32\d3d9.dll
C:\Windows\system32\winspool.drv
C:\Windows\system32\winmm.dll
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\DNSAPI.dll
C:\Windows\system32\version.DLL
C:\CFVS_HookDll.dll
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\CFGMGR32.dll
C:\Windows\syswow64\api-ms-win-downlevel-shlwapi-l1-1-0.dll
C:\Windows\syswow64\iertutil.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\syswow64\api-ms-win-downlevel-ole32-l1-1-0.dll
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\syswow64\ole32.DLL
C:\Windows\syswow64\SETUPAPI.dll
C:\Windows\syswow64\shell32.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\syswow64\api-ms-win-downlevel-version-l1-1-0.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\syswow64\profapi.dll
C:\Windows\syswow64\api-ms-win-downlevel-advapi32-l1-1-0.dll
C:\Windows\syswow64\NSI.dll
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\MSASN1.dll
C:\Windows\syswow64\USERENV.dll
C:\Windows\syswow64\CLBCatQ.DLL
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\oleaut32.dll
C:\Windows\syswow64\urlmon.dll
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\normaliz.DLL
C:\Windows\syswow64\api-ms-win-downlevel-user32-l1-1-0.dll
C:\Windows\syswow64\api-ms-win-downlevel-normaliz-l1-1-0.dll
C:\Windows\syswow64\comdlg32.dll
C:\Windows\syswow64\WININET.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\syswow64\DEVOBJ.dll
C:\Windows\syswow64\WS2_32.dll
C:\Windows\syswow64\Crypt32.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\WLDAP32.dll
C:\Windows\syswow64\LPK.dll
C:\Windows\SysWOW64\ntdll.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
C:\Windows\system32\ntdll.dll
MSIMG32.dll
PSAPI.DLL
Msftedit.dll
C:\Windows\SysWOW64\ieframe.dll
iertutil.dll
DUser.dll
C:\Windows\system32\DUser.dll
dwmapi.dll
C:\Windows\system32\xmllite.dll
C:\Windows\syswow64\CRYPT32.dll
WINTRUST.DLL
imagehlp.dll
C:\Users\win7\AppData\Local\Temp\is-MCBQP.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-MCBQP.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp_isetup_shfoldr.dll
Rstrtmgr.dll
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\idp.dll
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\innocallback.ENU
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\innocallback.EN
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\isslideshow.dll
user32
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\isslideshow.ENU
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\isslideshow.EN
olepro32.dll
RICHED32.DLL

C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\ISDone.dll
COMDLG32.dll
ws2_32.dll
inetmib1.dll
snmpapi.dll
rpcrt4.dll
C:\sampleENU.dll
C:\sampleLOC.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\mscorsec.dll
RichEd20.dll
mscorsec.dll
C:\Users\win7\AppData\Local\Temp\nsd8044.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-PJKDI.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-PJKDI.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\CallbackCtrl.dll
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\isslideshow.dll
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\isslideshow.ENU
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\isslideshow.EN
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-JI6CP.tmp_isetup_shfoldr.dll
ieframe.dll
mscms.dll
icm32.dll
api-ms-win-core-winrt-l1-1-0.dll
C:\Windows\System32\msxml3r.dll
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp\ISDone.dll
C:\Windows\system32\shlwapi.dll
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp\botva2.dll
GDIPlus
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GDIPlus.DLL
C:\Users\win7\AppData\Local\Temp\apm458A.tmp
C:\Users\win7\AppData\Local\Temp\is-E83SQ.tmp_isetup_shfoldr.dll
MSISIP.DLL
crypt32.dll
C:\Windows\SysWOW64\cryptnet.dll
C:\Windows\system32\VB6JP.DLL
VERSION.DLL
POWRPROF.DLL
PowrProf.dll
Msctf.dll
wtsapi32.dll
C:\Windows\system32\MSI.DLL
C:\Windows\system32\kernel32.dll
C:\Windows\system32\wbem\xml\wmi2xml.dll
C:\Windows\system32\EhStorShell.dll
c:\windows\system32\imageres.dll
C:\Windows\system32\VBoxMRXNP.dll
C:\Windows\System32\imageres.dll
C:\Windows\System32\drprov.dll
C:\Windows\System32\ntlanman.dll
C:\Windows\System32\davclnt.dll
C:\Users\win7\AppData\Local\Temp\nsk49CF.tmp\services.dll
C:\Users\win7\AppData\Local\Temp\nsk49CF.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsk49CF.tmp\InstallOptions.dll
C:\Windows\system32\DBGHELP.DLL
C:\Windows\system32\odbcint.dll
MSVCRT.DLL
BrLogAPI.dll
BrDbgOut.dll
BrDbgOtW.dll
C:\Users\win7\AppData\Local\Temp\is-G7HL1.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-PBGS6.tmp_isetup_shfoldr.dll
wsock32.dll
C:\Users\win7\AppData\Local\Temp\nsdB316.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsdB316.tmp\UAC.dll
AdvAPI32
SECUR32
C:\Users\win7\AppData\Local\Temp\nsdB316.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsdB316.tmp\ServicesHelper.dll
C:\Users\win7\AppData\Local\Temp\is-KFOOK.tmp_isetup_shfoldr.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
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.ServiceProce#\716ee14dc9aafde2b5f7f387d842661d\System.ServiceProcess.ni.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:\Users\win7\AppData\Local\Temp\is-TIHN7.tmp_isetup_shfoldr.dll
cmdhtml.dll
d3d10_1.dll
shcore.dll
uiautomationcore.dll
UIAutomationCore.dll
dwrite.dll
UXTHEME.DLL
C:\Users\win7\AppData\Local\Temp\comodocss_temp_setup\DXGIDebug.dll
MMDevAPI.DLL
wdmaud.drv
msacm32.drv
midimap.dll
dSound.dll
C:\Windows\system32\dSound.dll
C:\Windows\system32\sfc.dll
C:\Users\win7\AppData\Local\Temp\VideoPad-2932-1\ffmpeg19.exe
C:\Windows\System32\ShellStyle.dll
explorerframe.dll
MsftEdit.dll
C:\Windows\system32\IconCodecService.dll
C:\Windows\system32\mssvp.dll
C:\msfte.dll
C:\msTracer.dll
C:\Windows\system32\networkexplorer.dll
COMCTL32.DLL
shlwapi.dll
avrt.dll
C:\Users\win7\AppData\Local\Temp\27E45Q0I\unpack.dll
C:\Windows\system32\CRTDLL.DLL
SetupApi.DLL
wintrust.dll
newdev.dll
kernel32.DLL
Advapi32.DLL
Clusapi.DLL
gdi32.DLL
C:\Users\win7\AppData\Local\Temp\is-40VU3.tmp_isetup_shfoldr.dll
ddraw.dll
C:\Windows\SysWOW64\DDRAW.dll
C:\Windows\System32\msxml6r.dll
C:\Windows\system32\Msimtf.dll
C:\Users\win7\AppData\Local\Temp\nsj3E28.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsr389A.tmp\nsExec.dll
ADVAPI32.DLL
C:\Users\win7\AppData\Local\Temp\nshBA53.tmp\TvGetVersion.dll
C:\Users\win7\AppData\Local\Temp\nshBA53.tmp\UserInfo.dll
C:\Windows\system32\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\nshBA53.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nshBA53.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nshBA53.tmp\linker.dll
Msimg32.dll
C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\\Adobe AIR\Versions\1.0\Adobe AIR.dll
Versions\1.0\Adobe AIR.dll
C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\Adobe AIR\Versions\1.0\Resources\WebKit.dll
msimg32
C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\Adobe AIR Installer.exe
C:\Windows\SysWOW64\SAGE.DLL
Msi.dll
d3dxof.dll
C:\rarlng.dll
riched32.dll
riched20.dll
C:\Users\win7\AppData\Local\Temp\ins.exe
ImgUtil.dll
OLEACC.DLL
C:\Windows\system32\Oleacc.dll
ws2_32
C:\Users\win7\AppData\Local\Temp\5895\5895.exe
C:\Users\win7\AppData\Local\Temp\is-EQ9N3.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-EQ9N3.tmp\sample.EN
oleaut32.dll

winmm.dll
C:\Users\win7\AppData\Local\Temp\nsi56B9.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsi56B9.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsi56B9.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsi56B9.tmp\InetBgDL.dll
C:\Users\win7\AppData\Local\Temp\nsj4F0A.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsj4F0A.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsj4F0A.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsj4F0A.tmp\InetBgDL.dll
COMDLG32.DLL
IMM32.DLL
msvcrt.dll
OLE32.dll
SHELL32.DLL
C:/Users/win7/AppData/Local/Temp/BRE72E.tmp
C:/Users/win7/AppData/Local/Temp/BRE7BB.tmp
C:/Users/win7/AppData/Local/Temp/BRE914.tmp
C:/Users/win7/AppData/Local/Temp/BRE944.tmp
C:/Users/win7/AppData/Local/Temp/BRE964.tmp
C:/Users/win7/AppData/Local/Temp/BREADC.tmp
C:/Users/win7/AppData/Local/Temp/BREE19.tmp
C:/Users/win7/AppData/Local/Temp/BREEA7.tmp
C:/Users/win7/AppData/Local/Temp/BREEB8.tmp
C:/Users/win7/AppData/Local/Temp/BREF45.tmp
winmm
uxtheme
wintab32
wintab32.dll
version
secur32
userenv
usp10
shell32
C:\Windows\System32\AdapterTroubleshooter.exe
C:\Windows\System32\ARP.EXE
C:\Windows\System32\at.exe
C:\Windows\System32\AtBroker.exe
C:\Windows\System32\attrib.exe
C:\Windows\System32\auditpol.exe
C:\Windows\System32\autochk.exe
C:\Windows\System32\autoconv.exe
C:\Windows\System32\autofmt.exe
C:\Windows\system32\mmcshext.dll
C:\Windows\System32\bitsadmin.exe
C:\Windows\System32\bootcfg.exe
C:\Windows\System32\bthudtask.exe
C:\Windows\System32\Bubbles.scr
C:\Windows\System32\cacls.exe
C:\Windows\System32\calc.exe
C:\Windows\System32\CertEnrollCtrl.exe
C:\Windows\System32\certreq.exe
C:\Windows\System32\certutil.exe
C:\Windows\System32\charmap.exe
C:\Windows\System32\chkdsk.exe
C:\Windows\System32\chkntfs.exe
C:\Windows\System32\choice.exe
C:\Windows\System32\cipher.exe
C:\Windows\System32\cleanmgr.exe
C:\Windows\System32\cliconfg.exe
C:\Windows\System32\clip.exe
C:\Windows\System32\cmdkey.exe
C:\Windows\System32\cmdl32.exe
C:\Windows\System32\cmmon32.exe
C:\Windows\System32\cmstp.exe
C:\Windows\System32\colorcpl.exe
C:\Windows\System32\comp.exe
C:\Windows\System32\compact.exe
C:\Windows\System32\ComputerDefaults.exe
C:\Windows\System32\control.exe
C:\Windows\System32\convert.exe
C:\Windows\System32\credwiz.exe
C:\Windows\system32\psapi.dll
werui.dll
DUI70.dll
C:\Windows\SysWOW64\DUser.dll
C:\Windows\system32\RICHED20.DLL
api-ms-win-core-sysinfo-l1-2-1
atlthunk.dll

C:\Windows\system32\KERNEL32.DLL
C:\Windows\system32\NTDLL.DLL
C:\Windows\system32\ADVAPI32.DLL
C:\Users\win7\AppData\Local\Temp\is-PH7AV.tmp_isetup_shfoldr.dll
credui.dll
C:\Users\win7\AppData\Local\Temp\is-SGETF.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-SGETF.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-V9HJD.tmp_isetup_shfoldr.dll
NTDLL.DLL
mpr.dll
winspool.drv
oleacc.dll
GDI32.DLL
usp10.dll
netapi32.dll
Avrt.dll
HHCtrl.OCX
C:\SQLite3.dll
C:\Users\win7\AppData\Local\Temp\nssA12D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nssA12D.tmp\newadvsplash.dll
C:\Windows\system32\urlmon.dll
C:\Windows\system32\asycfilt.dll
C:\Windows\system32\WINMM.dll
Riched20.dll
C:\Windows\SysWOW64\msls31.dll
DDRAW.dll
DSOUND.dll
DINPUT8.dll
C:\Users\win7\AppData\Local\Temp\mdmB1E5.tmp
DINPUT.DLL
HID.DLL
SETUPAPI.DLL
USER32.DLL
URLMON.DLL
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\ar-SA\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\cs-CZ\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\da-DK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\de-DE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\el-GR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\en-US\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\es-ES\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\fi-FI\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\fr-FR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\he-IL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\hu-HU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\it-IT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\ja-JP\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\ko-KR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\nb-NO\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\nl-NL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\pl-PL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\pt-BR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\pt-PT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\ru-RU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\sk-SK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\sv-SE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\th-TH\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\tr-TR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\zh-CN\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\zh-TW\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF2961.tmp\en-US\resource.dll.mui
C:\Windows\system32\MSFTEDIT.dll
C:\Windows\system32\msi.dll
Kernel32
C:\Program Files\Internet Explorer\IEXPLORE.EXE
powrprof.dll
IMGUTIL.DLL
C:\Users\win7\AppData\Local\Temp\is-C5AAO.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-C5AAO.tmp\sample.EN
msvcr71.dll
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\msvcr71.dll
msvcp71.dll
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\msvcp71.dll
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\proj.dll
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\INetURL.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\NetFile.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\NetLingo.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\SWADCmpr.x32

C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\MacroMix.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\DirectSound.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Sound Control.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Text Asset.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\TextXtra.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Font Xtra.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Flash Asset.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Shockwave 3D Asset.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Font Asset.x32
C:\winampa.lng
C:\Users\win7\AppData\Local\Temp\nsy5EE6.tmp\System.dll
C:\en-US.dll
C:\en.dll
C:\Users\win7\AppData\Local\Temp\is-LNMB3.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nssC7E0.tmp\DotNetChecker.dll
C:\Users\win7\AppData\Local\Temp\nssC7E0.tmp\nsSCM.dll
C:\Users\win7\AppData\Local\Temp\nsuEEF5.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsuEEF5.tmp\ImageEdPlug
C:\Users\win7\AppData\Local\Temp\nsuEEF5.tmp\KillProcDLL.dll
C:\Users\win7\AppData\Local\Temp\nskBBA2.tmp\System.dll
revolt.dll
MSWSOCK.dll
C:\Windows\SysWOW64\occache.dll
C:\Windows\SysWOW64\gameux.dll
C:\Windows\SysWOW64\inetcpl.cpl
C:\Windows\System32\DATACLEN.DLL
C:\Windows\system32\setupcln.dll
C:\Windows\system32\wer.dll
C:\Windows\system32\riched20.dll
C:\Windows\system32\dfshim.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\dfdll.dll
fltlib.dll
MSVCRT.dll
DnsApi.dll
urlmon
Iphlpapi.dll
ICMP.DLL
mtxoci.dll
oci.dll
C:\Windows\system32\comsvcs.dll
C:\Users\win7\AppData\Local\Temp\nsu78B0.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsu78B0.tmp\newadvsplash.dll
C:\Users\win7\AppData\Local\Temp\nsu78B0.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsu78B0.tmp\System.dll
News.dll
C:\Users\win7\AppData\Local\Temp\hyaF94D.tmp
MPR.DLL
OLE32.DLL
C:\Users\win7\AppData\Local\Temp\hyaF94D.ENU
C:\Users\win7\AppData\Local\Temp\hyaF94D.EN
C:\Users\win7\AppData\Local\Temp\nsw995C.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsw995C.tmp\UtilsPlugin.dll
C:\Users\win7\AppData\Local\Temp\nsw995C.tmp\System.dll
UnityWebPluginAX.ocx
C:\Users\win7\AppData\LocalLow\Unity\WebPlayer\loader\UnityWebPluginAX.ocx
C:\Users\win7\AppData\Local\Temp\nsw995C.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsw995C.tmp\UAC.dll
Shell32.dll
C:\Users\win7\AppData\Local\Temp\nsu131F.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsu131F.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsu131F.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsu131F.tmp\ServicesHelper.dll
POWRPROF.dll
C:\Users\win7\AppData\Local\Temp\comodoccav_temp_setup\DXGIDebug.dll
NTDLL.dll
C:\Users\win7\AppData\Local\Temp\is-SDH7C.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-SDH7C.tmp_isetup_isdecmp.dll
C:\Windows\system32\VB6ES.DLL
C:\Users\win7\AppData\Local\Temp\nspC5EB.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nspC5EB.tmp\System.dll
C:\Imagine.dll
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
feclient.dll
C:\Users\win7\AppData\Local\Temp\{e3931098-f44a-4c70-bf9c-f48d24bdd066}\.ba1\wixstdba.dll
C:\Windows\system32\wups.dll
C:\Windows\system32\wu.upgrade.ps.dll
C:\Users\win7\AppData\Local\Temp\is-L3OM5.tmp_isetup_shfoldr.dll

C:\Users\win7\AppData\Local\Temp\is-NEDQ1.tmp_isetup_shfoldr.dll
C:\Program Files\Internet Explorer\iexplore.exe
C:\Windows\system32\mspaint.exe
C:\Windows\System32\mspaint.exe
C:\Windows\system32\NOTEPAD.EXE
C:\Windows\System32\notepad.exe
c:\windows\system32\mspaint.exe
c:\windows\system32\notepad.exe
c:\program files\internet explorer\iexplore.exe
kernel.dll
C:\1033\certintl.dll
C:\Users\win7\AppData\Local\Temp\is-5AD42.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsx974E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsx974E.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\is-4CMSU.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-4CMSU.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-9HECS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-QH5H5.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-QH5H5.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-PAI7L.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-PAI7L.tmp\isxdl.dll
MSFTEDIT.DLL
C:\Users\win7\AppData\Local\Temp\GUM5ED3.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUM5ED3.tmp\goopdateres_en.dll
comctl32
C:\Users\win7\AppData\Local\Temp\nso5009.tmp\nsDialogs.dll
C:\Windows\system32\kernel32
C:\Windows\system32\ntdll
msimsg.dll
C:\Windows\system32\shell32
C:\Windows\system32\user32
C:\Windows\System32\mstscax.dll
C:\Windows\SYSWOW64\mstscax.dll
C:\Users\win7\AppData\Local\Temp\is-5LULK.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-5LULK.tmp\sample.EN
wiatrace.dll
MSVCR90.dll
C:\zlib.pyd
NETAPI32.DLL
advpack
C:\Windows\SysWOW64\SETUPAPI.DLL
SPINF.dll
SPFILEQ.dll
C:\Users\win7\AppData\Local\Temp\nsg5682.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsg5682.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-77QBU.tmp_isetup_shfoldr.dll
cfgmgr32.dll
C:\InstallRes.dll
WinTrust.dll
MPR.dll
WSOCK32.dll
NTDLL
SSPICLI
C:\Users\win7\AppData\Local\Google\Chrome\Application\chrome.exe
C:\Program Files\Microsoft Silverlight\sllauncher.exe
C:\Windows\SysWOW64\jscript9.dll
C:\Windows\SysWOW64\SFC.DLL
C:\Windows\SysWOW64\mfcm120u.dll
C:\Windows\SysWOW64\mfcm120.dll
C:\Windows\SysWOW64\mfc120u.dll
C:\Windows\SysWOW64\mfc120.dll
C:\Windows\SysWOW64\vccorlib120.dll
C:\Windows\SysWOW64\msvcp120.dll
C:\Windows\SysWOW64\msvcr120.dll
C:\Users\win7\AppData\Local\Temp\is-6EV4U.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-6EV4U.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-7SMID.tmp_isetup_shfoldr.dll
C:\Windows\system32\msxml6.dll
Shlwapi
Msimg32
c:\python27\dlls\py.ico
C:\DLL_Loader.exe
C:\Procmon.exe
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\bass.dll
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\isskin.dll
C:\Users\win7\AppData\Local\Temp\is-FNL14.tmp\sample.tmp

C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\skin.cjstyles
dsound
C:\Windows\system32\dsound.DLL
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\isgsg.dll
C:\Users\win7\AppData\Local\Temp\is-PJ97L.tmp_isetup_shfoldr.dll
D3D9.DLL
DXGI.DLL
C:\DBGHELP.DLL
C:\USERS\WIN7\APPDATA\LOCAL\.#\MBX@250@28F7E0.###
C:\USERS\WIN7\APPDATA\LOCAL\.#\MBX@250@28F610.###
C:\USERS\WIN7\APPDATA\LOCAL\.#\MBX@250@28E540.###
C:\USERS\WIN7\APPDATA\LOCAL\.#\MBX@250@28E550.###
mss32.dll
MSCOREE.DLL
C:\Windows\SysWOW64\msi.dll
C:\Users\win7\AppData\Local\Temp\nsu5948.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsu5948.tmp\System.dll
alvtnvw.dll
C:\Users\win7\AppData\Local\Temp\is-NOOGQ.tmp_isetup_shfoldr.dll
cryptui.dll
C:\Users\win7\AppData\Local\Temp\gtapi.dll
DWMAPI.DLL
C:\t8res.dll
C:\sares.dll
C:\Windows\system32\User.exe
C:\Users\win7\AppData\Local\Temp\is-9EF2J.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-9EF2J.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-HO0LB.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-HO0LB.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-KPCK7.tmp_isetup_shfoldr.dll
XmlLite.dll
C:\Users\win7\AppData\Local\Temp\is-BFDFO.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\{e6171278-8759-449d-9e0b-c1825debc2ad}\.ba1\wixstdba.dll
C:\Users\win7\AppData\Local\Temp\{e6171278-8759-449d-9e0b-c1825debc2ad}\.ba1\bafunctions.dll
OLEACC.dll
C:\Users\win7\AppData\Local\Temp\is-DDN2T.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsmFDE6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-J114P.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-SO3SR.tmp_isetup_shfoldr.dll
C:\AICommand.bat
mswsock.dll
C:\msvcr120.dll
C:\msvcp120.dll
iefdmdm.dll
iefdm2.dll
C:\Users\win7\AppData\Local\Temp\E1DA.tmp\hale.cmd
C:\Users\win7\AppData\Local\Temp\nso3DF0.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nso3DF0.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nso3DF0.tmp\StartMenu.dll
shdocvw
riched20
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\wintab32.dll
C:\Windows\system32\user32.dll
C:\Windows\system32\advapi32.dll
C:\Windows\system32\userenv.dll
C:\Windows\system32\gdi32.dll
C:\Users\win7\AppData\Local\Temp\nsy3962.tmp\registry.dll
C:\Users\win7\AppData\Local\Temp\nsy3962.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsy3962.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsy3962.tmp\KillProcDLL.dll
C:\Users\win7\AppData\Local\Temp\nsaAA69.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsh3CDB.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsl4625.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsl4625.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsl4625.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\Cabinet.dll
C:\Windows\system32\version.dll
C:\Windows\system32\atl.dll
C:\Windows\system32\powrprof.dll
C:\Windows\system32\mscms.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\Shell32.dll
C:\Users\win7\AppData\Local\Temp\{419280CA-C520-425D-AC0A-E5BC4EFBF810}\fpb.tmp

C:\Users\win7\AppData\Local\Temp\{751F51AF-F47E-49A8-B05E-0D0463F62F92}\fpb.tmp
C:\Windows\system32\Advapi32.dll
C:\Windows\system32\Msimg32.dll
atl.dll
C:\Users\win7\AppData\Local\Temp\is-F1N54.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-F1N54.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\JPEG Agent.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Mix Services.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\Photoshop 3.0 Import.x32
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\xtras\ActiveX.x32
msctf.dll
C:\helper.gui
C:\Users\win7\AppData\Local\Temp\is-FOINK.tmp_isetup_shfoldr.dll
shlwapi.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\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\ws2_32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Core\63e9d5c341d64a753cde97f5a3d65c71\System.Core.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\bcrypt.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\Microsoft.NET\Framework\v2.0.50727\diasymreader.dll
C:\Users\win7\AppData\Local\Temp\nsq143A.tmp\NSISdl.dll
api-ms-win-core-string-l1-1-0
api-ms-win-core-datetime-l1-1-1
api-ms-win-core-localization-obsolete-l1-2-0
C:\Users\win7\AppData\Local\Temp\genteert.dll
C:\Users\win7\AppData\Local\Temp\gentee86\guig.dll
C:\Users\win7\AppData\Local\Temp\nsz5F83.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-L7PI0.tmp_isetup_shfoldr.dll
C:\Windows\system32\zipfldr.dll
GDIPLUS.DLL
install.res.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GDIPLUS.DLL
C:\Users\win7\AppData\Local\Temp\nsyE67.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsyE67.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsyE67.tmp\InstallOptions.dll
C:\ProgramData\Soda PDF 8\Installation\Statistics.dll
API-MS-Win-Security-Base-L1-1-0.dll
C:\Users\win7\AppData\Local\Temp\nscB34F.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nscB34F.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nscB34F.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nscB34F.tmp\ServicesHelper.dll
Crypt32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Gdiplus.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\12dc10e5c0e8d176cf21a16a6fc5fc3b\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\0967cf5c31691f38d013263304d2dacb\System.Runtime.Remoting.ni.dll
oleaut32
C:\Windows\Microsoft.NET\Framework\v2.0.50727\OLEAUT32.dll
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\comctl32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web.Services\2804664decc8bc37bdc172b35a5bdd46\System.Web.Services.ni.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\ntdll.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\rasapi32.dll
RASMAN.DLL
rtutils.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\winhttp.dll
C:\Users\win7\AppData\Local\Google\Update\1.3.29.5\goopdate.dll
C:\Users\win7\AppData\Local\Google\Update\GoogleUpdate.exe
C:\Users\win7\AppData\Local\Google\Update\1.3.29.5\psuser.dll
C:\Users\win7\AppData\Local\Temp\is-UCPO7.tmp_isetup_shfoldr.dll
Kernel32.DLL
Shell32.DLL
SHFolder.DLL
WinUsb.DLL
C:\Windows\system32\MSI.dll
C:\b00a44eecea30da754\Setup.exe
SetupUi.dll
C:\b00a44eecea30da754\1033\SetupResources.DLL
C:\Windows\System32\RstrtMgr.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nse70A5.tmp\ServicesHelper.dll
C:\Users\win7\AppData\Local\Temp\RarSFX0\Stub.exe
C:\Users\win7\AppData\Local\Temp\7zS098D14EB\avgmfarx.dll

C:\Users\win7\AppData\Local\Temp\nsj5CEA.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsj5CEA.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsj5CEA.tmp\PassDialog.dll
C:\Users\win7\AppData\Local\Temp\gentee9B\guig.dll
Oleaut32.dll
Ole32.dll
winsta
C:\Windows\system32\shfolder.dll
C:\Users\win7\AppData\Local\Temp\is-KNR6K.tmp_isetup_isdecmp.dll
C:\Windows\system32\Rstrtmgr.dll
C:\Users\win7\AppData\Local\Temp\nso8A6A.tmp\InstallOptions.dll
wininet
MSACM32.dll
OLEPRO32.DLL
DDRAW.DLL
C:\Windows\System32\DSOUND.dll
D3D8.DLL
dpnhpast.dll
C:\Users\win7\AppData\Local\Temp\GLC7E05.tmp
C:\Windows\twain_32\A8P\Admin.exe
C:\Windows\twain_32\A8P\remove.exe
C:\875a5c9f8218429c1ed3bb3003a0a1a3\microsoft_defaults.exe
C:\sample\..\DirectoryWatcher.dll
C:\Users\win7\AppData\Local\Temp\is-92J6B.tmp_isetup_shfoldr.dll
ATL.DLL
C:\Users\win7\AppData\Local\Temp\nse78B8.tmp\UAC.dll
ADVAPI32
ShlWAPI
C:\Users\win7\AppData\Local\Temp\nse78B8.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nse78B8.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nse78B8.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nse78B8.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nshA1CF.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nshA1CF.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\GUME42D.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUME42D.tmp\goopdateres_en.dll
SetupAPI.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\symsrv.dll
C:\opera.dll
AVICAP32.dll
avifil32.dll
RASAPI32.DLL
RASDLG.DLL
GSM_codec.dll
msftedit.dll
C:\Users\win7\AppData\Local\Temp\{7C5A5A01-BA31-4712-8E81-703787A937A1}_Setup.dll
C:\Temp\NVIDIA\3DVision\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}\ISRT.dll
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}_isres.dll
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}_isuser.dll
C:\Windows\system32\AppHelp.dll
C:\Temp\NVIDIA\3DVision\data1.hdr
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}\NVINSTNT.DLL
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}_ISRes.dll
msuser.dll
C:\Users\win7\AppData\Local\Temp\OfficeSetup.exe
C:\msvcr71.dll

C:\msvcp71.dll
C:\proj.dll
Ntdll
C:\Users\win7\AppData\Local\Temp\dfs37B9.tmp
sxs.dll
C:\Users\win7\AppData\Local\Temp\shell32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\99cdfef98595ed91f14936cf52a49c54\System.Management.ni.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\\wminet_utils.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\shell32.dll
C:\Users\win7\AppData\Local\Temp\nsyF4FA.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsyF4FA.tmp\StartMenu.dll
C:\Users\win7\AppData\Local\Temp\nswFE9D.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nswFE9D.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nswFE9D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsp6AA7.tmp\System.dll
hhctrl.ocx
C:\Users\win7\AppData\Local\Temp\is-STTCD.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-STTCD.tmp\sample.EN
RichEd20.DLL
C:\Windows\system32\RichEd20.DLL
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\shell32.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\psapi.dll
C:\setupapi
setupapi
C:\Windows\system32\APPHELP.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\system32\DWMAPI.dll
C:\Windows\system32\CRYPTBASE.dll
C:\Windows\system32\OLEACC.dll
C:\Windows\system32\CLBCATQ.dll
C:\Users\win7\AppData\Local\Temp\nseC55E.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nseC55E.tmp\portable.dll
C:\Users\win7\AppData\Local\Temp\nseC55E.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\is-72FFF.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-OGN9O.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-OGN9O.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-HTCEN.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-HTCEN.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nsrF268.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsrF268.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsrF268.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsrF268.tmp\ServicesHelper.dll
C:\CFVS_I~1.EXE
C:\DLL_LO~1.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
C:\Python27\Lib\SITE-P~1\pip_vendor\distlib\t32.exe
C:\Python27\Lib\SITE-P~1\pip_vendor\distlib\t64.exe
C:\Python27\Lib\SITE-P~1\pip_vendor\distlib\w32.exe
C:\Python27\Lib\SITE-P~1\pip_vendor\distlib\w64.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\cli-32.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\cli-64.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\CLI-AR~1.EXE
C:\Python27\Lib\SITE-P~1\SETUPT~1\cli.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\gui-32.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\gui-64.exe
C:\Python27\Lib\SITE-P~1\SETUPT~1\GUI-AR~1.EXE
C:\Python27\Lib\SITE-P~1\SETUPT~1\gui.exe
C:\Python27\Scripts\EASY_I~2.EXE
C:\Python27\Scripts\EASY_I~1.EXE
C:\Python27\Scripts\pip.exe
C:\Python27\Scripts\PIP27~1.EXE

C:\Python27\Scripts\pip2.exe
C:\Users\win7\AppData\Local\Temp\is-R7F8Q.tmp_isetup_shfoldr.dll
NETMSG
sample
C:\Users\win7\AppData\Local\Temp\is-939C4.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-939C4.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\kvncviewer.exe
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\iphlpapi.dll
C:\Users\win7\AppData\Local\Temp\nsf85A0.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf85A0.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsf85A0.tmp\InstallOptions.dll
advpack.dll
dsetup.dll
C:\Windows\SysWOW64\mshtml.dll
jscript9.dll
C:\Users\win7\AppData\Local\Temp\HYD96EA.tmp.1460138451\HTA\images\main_utorrent.ico
C:\Windows\SysWOW64\DXGIDebug.dll
C:\Windows\SysWOW64\D3D10Warp.dll
MFPlat.DLL
C:\WBDJA44I.DLL
C:\Users\win7\AppData\Local\Temp\is-0CU53.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-0CU53.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-H2L21.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsu454C.tmp\System.dll
InstallCheck
t "InstallCheck.dll"
InstallCheck.dll
InstallUtility
C:\Users\win7\AppData\Local\Temp\nsu454C.tmp\log.dll
C:\Users\win7\AppData\Local\Temp\nsu454C.tmp\BHips.dll
C:\Users\win7\AppData\Local\Temp\nsz38B8.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsz38B8.tmp\System.dll
WLDAP32.dll
C:\Users\win7\AppData\Local\Temp\pJoNehMzo5.tmp\htmlayout.dll
HTMLayout.dll
C:\Users\win7\AppData\Local\Temp\DXGIDebug.dll
C:\Users\win7\AppData\Local\Temp\nsc13F1.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-0EM52.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\~vis0000\vise32ex.dll
C:\Windows\system32\user.exe
C:\Users\win7\AppData\Local\Temp\~vis0000\QTExtCode.dll
C:\QuickTime.qts
C:\Windows\system32\QuickTime.qts
C:\sample.dll
V64
MSVBVM60.DLL
C:\Users\win7\AppData\Local\Temp\is-VRB63.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-VRB63.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-D74U0.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsaEEAF.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-48I6D.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-48I6D.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\bp.ENU
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\bp.EN
msvfw32.dll
Gdi32.dll
Avicap32.dll
quartz.dll
Magnification.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\4fddb3cf84aed83214f65fbe791348e5\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management.A#\24f3f84b0793777ae7337796ef5551a5\System.Management.Automation.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\1a6d99549254a6a0dbac7b728f3e010b\Microsoft.PowerShell.Commands.Diagnostics
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuratio#\30280e5e7d89ffe702df50de4d339fc7\System.Configuration.Install.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.WSMan.Man#\34420c5bbb60572350b8af1a12d94451\Microsoft.WSMan.Management.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Transactions\f45bc0251cceb599622f55cc1c7f4aba\System.Transactions.ni.dll
C:\Windows\assembly\GAC_32\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\7fcb194ae385dc872688067fb024bd55\Microsoft.PowerShell.Commands.Utility.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\61bdc0f0c598b66a5af21dc10f824141\Microsoft.PowerShell.Commands.Management
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\2b0a3b04b44b8d8e3cd4d489220d8c35\Microsoft.PowerShell.Security.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.DirectorySer#\cbe531dae622018576dbf7b1fca5ce47\System.DirectoryServices.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\secur32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Data\4b335bfaa07fc54f2d72213d33f53e97\System.Data.ni.dll

C:\Windows\assembly\GAC_32\System.Data\2.0.0.0__b77a5c561934e089\System.Data.dll
dnsapi.dll
C:\Windows\system32\ExplorerFrame.dll
OLEAUT32
C:\Users\win7\AppData\Local\Temp\{6502eaff-6343-46f3-9c22-6ccca6ee1f86}\.ba1\wixstdba.dll
C:\Windows\system32\Riched20.dll
C:\Users\win7\AppData\Local\Temp\nsrA251.tmp\nsExec.dll
C:\Users\win7\AppData\Local\Temp\nsxBE45.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsxBE45.tmp\SimpleSC.dll
C:\Users\win7\AppData\Local\Temp\nsxBE45.tmp\SimpleSC.ENU
C:\Users\win7\AppData\Local\Temp\nsxBE45.tmp\SimpleSC.EN
C:\Users\win7\AppData\Local\Temp\{fa356f34-eef9-4655-aa8e-0eea851f3102}\.ba1\wixstdba.dll
jscript.dll
C:\Users\win7\AppData\Local\Temp\PB1BEA.tmp
C:\Users\win7\AppData\Local\Temp\PB1BEA.ENU
C:\Users\win7\AppData\Local\Temp\PB1BEA.EN
C:\Users\win7\AppData\Local\Temp\Citrix\GoToAssist Remote Support Customer\948\g2aA30B.tmp\dbghelp.dll
C:\Windows\system32\comctl32.dll
g2ax_customer_resource_win32_x86_en_US.dll
C:\Windows\system32\wintrust.dll
C:\Users\win7\Documents\DCSCMIN\IMDCSC.ENU
C:\Users\win7\Documents\DCSCMIN\IMDCSC.EN
MSVBVM60.DLL
msftedit
lz32
C:\Users\win7\AppData\Local\Temp\jkiC855.tmp
C:\Users\win7\AppData\Local\Temp\nssCBC2.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nssCBC2.tmp\nsis7z.dll
C:\Users\win7\AppData\Local\Temp\is-215M3.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-215M3.tmp\sample.EN
C:\Windows\system32\CRYPTNET.dll
C:\Users\win7\qEWT\iixRg.exe
C:\Users\win7\AppData\Local\Temp\is-3U04L.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-3U04L.tmp\sample.EN
msdmo.dll
msrle32.dll
msvidc32.dll
msyuv.dll
iyuv_32.dll
tsbyuv.dll
iccvid.dll
msacm32.dll
imaadp32.acm
msg711.acm
msgsm32.acm
msadp32.acm
C:\Users\win7\AppData\Local\Temp\dfs843C.tmp
MSDART.dll
odbc32.dll
WTSAPI32.dll
C:\Users\win7\AppData\Local\Temp\is-HTBJ6.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\tf00294823.dll
IPHLPAPI.dll
URLMON.dll
C:\Users\win7\AppData\Local\Temp\vpa9BD6.tmp
C:\Users\win7\AppData\Local\Temp\vpa9BD6.ENU
C:\Users\win7\AppData\Local\Temp\vpa9BD6.EN
C:\Users\win7\AppData\Local\Temp\Windows\Windows.exe
C:\Users\win7\AppData\Local\Temp\HWSignature.dll
MSVCP60.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Web\21f876e85bfaa433a999a410eda373bc\System.Web.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.EnterpriseSe#\abecd46ce0b212dad31a9e8f9adf073f\System.EnterpriseServices.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.EnterpriseSe#\abecd46ce0b212dad31a9e8f9adf073f\System.EnterpriseServices.Wrapper.dll
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.Wrapper.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vsa\19777cd74173fbe2e9931095cc8e057b\Microsoft.Vsa.ni.dll
C:\Users\win7\AppData\Local\Temp\deldll.bat
C:\Windows\System32\esrb.rs
samcli.dll
C:\Users\win7\AppData\Local\Temp\jkiFFC0.tmp
C:\Users\win7\AppData\Local\Temp\nskB924.tmp\System.dll
appwiz.cpl
C:\Users\win7\AppData\Local\Temp\nsj699D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsj699D.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsj699D.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsj699D.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\TsuD33EACE3.dll
C:\Windows\system32\sxs.dll
C:\Windows\system32\mscoree.dll

rstrtmgr.dll
userenv.dll
C:\Users\win7\AppData\Local\Temp\{B6F8261D-62CA-4E7E-AC95-2AE86D1B04EB}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{B6F8261D-62CA-4E7E-AC95-2AE86D1B04EB}\Custom.dll
aclui.dll
RASAPI32.dll
networkexplorer.DLL
NlsData000c.DLL
NetProjW.DLL
Ghofr.DLL

QueryProcessAddress

ReadProcessMemory
Toolhelp32ReadProcessMemory
CreateRemoteThreadEx
WriteProcessMemory
CreateProcessA
CreateProcessW
GetThreadContext
SetThreadContext
ShellExecuteA
ShellExecuteExA
ShellExecuteExW
ShellExecuteW
IsDebuggerPresent
NtCreateProcess
NtCreateProcessEx
InternetReadFile
InternetReadFileExA
CreateProcess
ShellExecuteEx
QueueUserAPC
ZwCreateProcess
ZwCreateProcessEx

QueryFilePath

C:\sample
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\RichEd20.DLL
C:\Windows\system32\propsys.dll
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\system32\DSOUND.dll
C:\DLL_Loader.exe
C:\Windows\system32\dsound.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\system32\MSHTML.dll
C:\Windows\SysWOW64\jscript9.dll
C:\Windows\system32\dxgi.dll
C:\Windows\system32\d3d11.dll
C:\Windows\system32\D3D10Warp.dll
C:\Windows\system32\ntshrui.dll
C:\Windows\system32\credui.dll
C:\Windows\SysWOW64\MSIEXEC.EXE
C:\Windows\system32\msi.dll
C:\Windows\SysWOW64\MSCOREE.DLL
C:\Windows\SysWOW64\MsiHnd.dll
C:\Windows\SysWOW64\RICHED20.DLL
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\samp
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\kernel32.dll
C
dFF=
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\SysWOW64\schannel.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Windows\SysWOW64\rundll32.exe
C:\Users\win7\AppData\Local\Temp\~nsuA.tmp\Au_.exe
C:\Users\win7\AppData\Local\Temp\is-Q70NF.tmp\sample.tmp

C:\Windows\system32\RICHED20.DLL
PA
C:
|A
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\FaultRep.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\d3d8thk.dll
C:\Windows\system32\d3d9.dll
C:\Windows\system32\winspool.drv
C:\Windows\system32\winmm.dll
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\DNSAPI.dll
C:\Windows\system32\version.DLL
C:\CFVS_HookDll.dll
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\api-ms-win-downlevel-shlwapi-l1-1-0.dll
C:\Windows\syswow64\iertutil.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\syswow64\api-ms-win-downlevel-ole32-l1-1-0.dll
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\syswow64\ole32.DLL
C:\Windows\syswow64\shell32.dll
C:\Windows\syswow64\api-ms-win-downlevel-version-l1-1-0.dll
C:\Windows\syswow64\profapi.dll
C:\Windows\syswow64\api-ms-win-downlevel-advapi32-l1-1-0.dll
C:\Windows\syswow64\NSI.dll
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\MSASN1.dll
C:\Windows\syswow64\USERENV.dll
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\oleaut32.dll
C:\Windows\syswow64\urlmon.dll
C:\Windows\syswow64\normaliz.DLL
C:\Windows\syswow64\api-ms-win-downlevel-user32-l1-1-0.dll
C:\Windows\syswow64\api-ms-win-downlevel-normaliz-l1-1-0.dll
C:\Windows\syswow64\comdlg32.dll
C:\Windows\syswow64\WININET.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\syswow64\WS2_32.dll
C:\Windows\syswow64\Crypt32.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\WLDAP32.dll
C:\Windows\syswow64\LPK.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\System32\wship6.dll
C:\Windows\system32\rasadhlp.dll
C:\Windows\System32\wshtcpip.dll
C:\Windows\system32\mswsock.dll
C:\Windows\system32\WINNSI.DLL
C:\Windows\system32\iphlpapi.dll
C:\Windows\system32\ldnDL.dll
C:\Windows\system32\Fwpuclnt.dll
C:\Windows\system32\SECUR32.DLL
C:\Windows\system32\security.dll
C:\Windows\syswow64\CFGMGR32.dll
C:\Windows\syswow64\SETUPAPI.dll
C:\Windows\syswow64\CLBCatQ.DLL
C:\Windows\syswow64\DEVOBJ.dll
C:\Windows\system32\PROPSYS.dll
C:\Windows\Temp\{B9D39D63-38B2-4564-BC92-C1C8AF3AE35E}\hapi\hapint.exe
C:\Windows\system32\DUser.dll
C:\Windows\system32\Msftedit.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Users\win7\AppData\Local\Temp\is-MCBQP.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-H50UK.tmp\isslideshow.dll
C:\Users\win7\AppData\Local\Tem
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\system32\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-8QD8J.tmp\isslideshow.dll
C:\Users\win7\AppData\Local\Temp\is-PJKDI.tmp\sample.tmp

C:\Users\win7\AppData\Local\Temp\is-NPA5Q.tmp\sample.tmp
C:\Windows\System32\msxml3.dll
C:\Users\win7\AppData\Local\Temp\is-O9R66.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp\b2p.dll
C:\Users\win7\AppData\Local\Temp\is-J6RCU.tmp\botva2.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GDIPlus.DLL
C:\Users\win7\AppData\Local\Temp\is-83ER6.tmp\sample.tmp
C:\Windows\SysWOW64\msiexec.exe
C:\Windows\SysWOW64\cryptnet.dll
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\SysWOW64\Wbem\WMIC.exe
C:\Windows\system32\explorerframe.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ODBC32.dll
C:\Users\win7\AppData\Local\Temp\is-4CHA1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-COSP1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-8P0LM.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-GRLC0.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\comodocss_temp_setup\cssstart.exe
C:\Users\win7\AppData\Local\Temp\comodocss_temp_setup\cmdhtml.dll
C:\Users\win7\AppData\Local\Temp\VideoPad-2932-1\ffmpeg19.exe
C:\Windows\system32\dSound.dll
C:\Windows\system32\SearchFolder.dll
C:\Windows\syswow64\SHELL32.dll
C:\Windows\system32\ieframe.DLL
C:\Windows\system32\CRTDLL.DLL
C:\Users\win7\AppData\Local\Temp\is-883N4.tmp\sample.tmp
C:\Windows\system32\RICHED20.dll
C:\Windows\SysWOW64\DDRAW.dll
C:\Windows\SysWOW64\mshtml.dll
C:\Windows\System32\msxml6.dll
C:\Users\win7\AppData\Local\Temp\TeamViewer\TeamViewer_.exe
C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\Adobe AIR Installer.exe
C:\Windows\system32\DINPUT8.dll
C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\Adobe AIR\Versions\1.0\Adobe AIR.dll
C:\Users\win7\AppData\Local\Temp\ins.exe
C:\Windows\SysWOW64\Wbem\wmic.exe
C:\Users\win7\AppData\Local\Temp\is-EQ9N3.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\7zS54D4.tmp\setup-stub.exe
C:\Users\win7\AppData\Local\Temp\7zS4C5A.tmp\setup-stub.exe
C:\Windows\SysWOW64\DUser.dll
C:\Windows\SysWOW64\dwwin.exe
C:\Windows\SysWOW64\werui.dll
C:\Users\win7\AppData\Local\Temp\is-INKP5.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-BUEVH.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-SGETF.tmp\sample.tmp
C:\Windows\system32\WINMM.dll
C:\Windows\system32\Riched20.dll
C:\Windows\system32\DINPUT.DLL
C:\Users\win7\AppData\Local\Temp\is-C5AAO.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\TempFolder.aaa\IML32.dll
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
C:\Users\win7\AppData\Local\Temp\is-9SM03.tmp\sample.tmp
C:\Windows\system32\bthprops.cpl
C:\Windows\system32\mscoree.dll
C:\Users\win7\AppData\Local\Temp\nsuEEF5.tmp\ImageEdPlug.DLL
C:\Windows\system32\riched20.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\dfdll.dll
C:\Users\win7\AppData\Local\Temp\nsu78B0.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\hyaF94D.tmp
C:\Users\win7\AppData\LocalLow\Unity\WebPlayer\loader\UnityWebPluginAX.ocx
C:\Users\win7\AppData\Local\Temp\comodoccav_temp_setup\ccavstart.exe
C:\Users\win7\AppData\Local\Temp\comodoccav_temp_setup\cmdhtml.dll
C:\Users\win7\AppData\Local\Temp\is-1GH0J.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\{e3931098-f44a-4c70-bf9c-f48d24bdd066}\.ba1\wixstdba.dll
C:\Users\win7\AppData\Local\Temp\is-8CSAU.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-PPHAJ.tmp\sample.tmp
C:\Windows\SysWOW64\rundll32.ex
C:\Windows\SysWOW64\PROPSYS.dll
C:\Users\win7\AppData\Local\Temp\~ACCAStore\sample_0_5116\sample
C:\Users\win7\AppData\Local\Temp\is-7POSM.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-4CMSU.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-QH5H5.tmp\sample.tmp
C:\Windows\system32\MSFTEDIT.DLL
C:\Users\win7\AppData\Local\Temp\GUM5ED3.tmp\DropboxUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUM5ED3.tmp\goopdate.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
C:\Windows\system32\werui.dll

C:\Windows\SysWOW64\sti.dll
C:\Users\win7\AppData\Local\Temp\is-5LULK.tmp\sample.tmp
C:\Windows\system32\wiashext.dll
C:\Windows\SysWOW64\advpack.DLL
C:\Users\win7\AppData\Local\Temp\is-QGU0N.tmp\sample.tmp
4
4\sample
D4
C:\Users\win7\AppData\Local\Temp\is-6EV4U.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-FNL14.tmp\sample.tmp
C:\Windows\syswow64\PSAPI.DLL
C:\Windows\system32\msimg32.dll
C:\Windows\system32\MMDevAPI.DLL
C:\Windows\system32\AUDIOSES.DLL
C:\Users\win7\AppData\Local\Temp\is-RILC4.tmp\isgsg.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\dsound.DLL
C:\Users\win7\AppData\Local\Temp\is-PBMN1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-SUH0F.tmp\sample.tmp
C:\Windows\system32\DXGI.DLL
C:\Users\win7\AppData\Local\Temp\VSD7F1.tmp\dotnetfx\dotnetchk.exe
C:\Windows\system32\MSCOREE.DLL
C:\Windows\system32\QUARTZ.dll
C:\Users\win7\AppData\Local\Temp\is-9ECD7.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\gtapi.dll
C:\Users\win7\AppData\Local\Temp\is-HO0LB.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-9EF2J.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-VKD4O.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\{e6171278-8759-449d-9e0b-c1825debc2ad}\.ba1\wixstdba.dll
C:\Users\win7\AppData\Local\Temp\is-1IMNT.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-6A4PJ.tmp\sample.tmp
C:\Windows\system32\aclui.dll
C:\Users\win7\AppData\Local\Temp\is-0QVDR.tmp\sample.tmp
C:\Windows\SysWOW64\cmd.exe
C:\Windows\system32\IEFRAME.dll
C:\Users\win7\AppData\Local\Temp\nsy3962.tmp\UAC.dll
C:\Windows\system32\ieframe.dll
C:\Windows\SysWOW64\RunDll32.exe
C:\Users\win7\AppData\Local\Temp\is-R0PA4.tmp\sample.tmp
C:\Windows\SysWOW64\RunDll32.ex
C:\Windows\SysWOW64\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-F1N54.tmp\OCSetupHlp.dll
C:\Windows\system32\MsftEdit.dll
C:\Windows\System32\PROPSYS.dll
C:\Users\win7\AppData\Local\Temp\is-IVI8C.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-35SIA.tmp\sample.tmp
?:\sample
C:\Users\win7\AppData\Local\Temp\is-PETB0.tmp\sample.tmp
C:\Windows\system32\zipfldr.dll
C:\Windows\System32\shdocvw.dll
C:\Users\win7\AppData\Local\LogMeIn Rescue Applet\LMIR0001.tmp\lmi_rescue.exe
C:\Users\win7\AppData\Local\Temp\is-QC029.tmp\sample.tmp
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\GDIPLUS.DLL
c:\067c9714643060410b2d85a8dbb23c\install.exe
c:\067c9714643060410b2d85a8dbb2
c:\067c9714643060410b2d85a8dbb23c\install.res.dll
C:\Windows\SysWOW64\regsvr32.exe
C:\ProgramData\Soda PDF 8\Installation\Statistics.dll
C:\Users\win7\AppData\Local\Temp\7zS4A0AE61B\avgsetupx.exe
C:\Users\win7\AppData\Local\Google\Update\GoogleUpdate.exe
C:\Users\win7\AppData\Local\Google\Update\1.3.29.5\goopdate.dll
C:\Users\win7\AppData\Local\Google\Update\1.3.29.5\psuser.dll
C:\Users\win7\AppData\Local\Temp\is-IHPD7.tmp\sample.tmp
C:\b00a44eecea30da754\Setup.exe
C:\b00a44eecea30da754\SetupEngine.dll
C:\b00a44eecea30da754\SetupUi.dll
C:\Users\win7\AppData\Local\Temp\7zS098D14EB\avgmfapx.exe
C:\Users\win7\AppData\Local\Temp\appun-1.exe
C:\Users\win7\AppData\Local\Temp\is-C3QCD.tmp\sample.tmp
C:\Windows\System32\DSOUND.dll
C:\Users\win7\AppData\Local\Temp\ocr9BC7.tmp\bin\msvcrt-ruby18.dll
C:\Windows\syswow64\SHELL32.DLL
C:\Users\win7\AppData\Local\Temp\GLC7E05.tmp
c:\875a5c9f8218429c1ed3bb3003a0a1a3\install.exe
c:\875a5c9f8218429c1ed3bb3003a0
c:\875a5c9f8218429c1ed3bb3003a0a1a3\install.res.dll
C:\Users\win7\AppData\Local\Temp\is-T7IRB.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\GUME42D.tmp\DropboxUpdate.exe

C:\Users\win7\AppData\Local\Temp\GUME42D.tmp\goopdate.dll
C:\Windows\system32\dbghelp.dll
C:\Windows\system32\RASDLG.DLL
C:\Windows\system32\msftedit.dll
C:\Temp\NVIDIA\3DVision\nvStInst.exe
C:\Temp\NVIDIA\3DVision\setup.exe
C:\Temp\NVIDIA\3DVision\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{7C5A5A01-BA31-4712-8E81-703787A937A1}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}\ISRT.dll
C:\Temp\NVIDIA\3DVision\setup.e
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\{13C5D420-CAE2-11D4-B34D-00105A1C23DD}\NVINSTNT.DLL
C:\Windows\system32\STI.dll
C:\Users\win7\AppData\Local\Temp\OfficeSetup.exe
C:\Windows\syswow64\COMDLG32.DLL
C:\Users\win7\AppData\Local\Temp\is-STTCD.tmp\sample.tmp
C:\Windows\SysWOW64\svchost.exe
C:\Users\win7\AppData\Local\Temp\is-R7F4F.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-OGN9O.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-HTCEN.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-EGITK.tmp\sample.tmp
C:\Users\win7\AppData\Roaming\Charles.exe
C:\Users\win7\AppData\Local\Temp\98938513-fda9-11e5-9e88-08002763e612\Ninite.exe
C:\Windows\SysWOW64\net1.exe
C:\Users\win7\AppData\Local\Temp\ce90fad6-fda9-11e5-9e88-08002763e612\Ninite.exe
C:\Windows\SysWOW64\netupdsrv.exe
C:\Windows\SysWOW64\soundschemes.exe
C:\Windows\SysWOW64\soundscheme
C:\Users\win7\AppData\Local\Temp\is-VGN2V.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-939C4.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-ID0U4.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\kvncviewer.exe
C:\Windows\SysWOW64\mshta.exe
C:\Windows\SysWOW64\dxgi.dll
C:\Windows\SysWOW64\d3d11.dll
C:\Windows\SysWOW64\D3D10Warp.dll
C:\Users\win7\AppData\Local\Temp\HYD96EA.tmp.1460138451\HTA\3rdparty\OCComSDK.dll
C:\Users\win7\AppData\Local\Temp\is-3VUKG.tmp\sample.tmp
C:\WBDJA44I.DLL
C:\Users\win7\AppData\Local\Temp\is-0CU53.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\nsu454C.tmp\InstallUtility.DLL
C:\Users\win7\AppData\Local\Temp\befcieifed.exe
C:\Users\win7\AppData\Local\Temp\is-4HHM1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\~vis0000\QTExtCode.dll
C:\Windows\system32\ESENT.dll
C:\Users\win7\AppData\Local\Temp\is-VRB63.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-48I6D.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-Q744A.tmp\bp.dll
C:\Windows\system32\quartz.dll
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Users\win7\AppData\Local\Temp\is-4OJK1.tmp\sample.tmp
C:\Windows\assembly\GAC_32\System.Transactions\2.0.0.0__b77a5c561934e089\System.Transactions.dll
C:\Users\win7\AppData\Local\Temp\{6502eaff-6343-46f3-9c22-6ccca6ee1f86}\.ba1\wixstdba.dll
C:\Users\win7\AppData\Local\Temp\nsrA251.tmp\7za.exe
C:\Users\win7\AppData\Local\Temp\is-J15I4.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\nsxBE45.tmp\SimpleSC.dll
C:\Users\win7\AppData\Local\Temp\{fa356f34-eef9-4655-aa8e-0eea851f3102}\.ba1\wixstdba.dll
C:\Windows\system32\jscript.dll
C:\Users\win7\AppData\Local\Temp\befbbjjhdg.exe
C:\Users\win7\AppData\Local\Temp\PB1BEA.tmp
C:\Users\win7\AppData\Local\Temp\Citrix\GoToAssist Remote Support Customer\948\g2aA30B.tmp\g2ax_installer_customer.exe
C:\Wind
C:\Windows\sysw
C:\Users\win7\Documents\DCSCMIN\IMDCSC.exe
C:\Users\win7\AppData\Local\Temp\12345.exe
C:\Windows\system32\msftedit.DLL
C:\Users\win7\AppData\Roaming\subfolder\filename.exe
C:\Users\win7\AppData\Local\Temp\befcjhajed.exe
C:\Users\win7\AppData\Local\Temp\is-215M3.tmp\sample.tmp
C:\Windows\system32\CRYPTNET.dll
C:\Users\win7\AppData\Local\Temp\is-JR3KD.tmp\sample.tmp
C:\Windows\syswow64\COMDLG32.dll
C:\Users\win7\AppData\Local\Temp\is-3U04L.tmp\sample.tmp
C:\Windows\SysWOW64\quartz.dll
C:\Windows\system32\msrle32.dll
C:\Windows\system32\msvidc32.dll
C:\Windows\system32\msyuv.dll

C:\Windows\system32\iyuv_32.dll
C:\Windows\system32\tsbyuv.dll
C:\Windows\system32\iccvid.dll
C:\Windows\system32\msacm32.dll
C:\Users\win7\AppData\Local\Temp\is-K8F3O.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\tf00294823.dll
C:\Users\win7\AppData\Local\Temp\befbbbdddg.exe
C:\Users\win7\AppData\Local\Temp\vpa9BD6.tmp
C:\Users\win7\AppData\Local\Temp\Windows\Windows.exe
c:\sample
C:\Windows\System32\msi.dll
C:\Windows\assembly\GAC_32\System.EnterpriseServices\2.0.0.0__b03f5f7f11d50a3a\System.EnterpriseServices.Wrapper.dll
D
C:\Windows\system32\appwiz.cpl
C:\Windows\system32\sxs.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.dll
C:\Users\win7\AppData\Local\Temp\{B6F8261D-62CA-4E7E-AC95-2AE86D1B04EB}\Custom.dll
C:\Users\win7\AppData\Local\Temp\TsuD33EACE3.dll
C:\Users\win7\AppData\Local\Temp\{B6F8261D-62CA-4E7E-AC95-2AE86D1B04EB}_Setup.dll
C:\Users\win7\AppData\Local\Temp\edurss.exe

CreateProcess

MSIEXEC.EXE /i "C:\Windows\Downloaded Installations\{FDC2F6D1-FE32-4AFC-8347-BE3B2D701180}\Network Camera View 4S.msi" TRANSFORMS="C:\Users\win7\AppData\Local\Temp_isA7F5\1033.MST" SETUPEXEDIR="C:"
"C:\Users\win7\AppData\Local\Temp\setup.exe"
"C:\Program Files\Internet Explorer\iexplore.exe" http://www.opera.com/download/get/?partner=www&opsys=Windows
<NULL>
tasdext
C:\Windows\system32\cmd.exe /u /c wmic os get BuildNumber >"C:\Users\win7\AppData\Local\Temp\osbuild.andy.txt"
"C:\Users\win7\AppData\Local\Temp\comodocss_temp_setup\cssstart.exe"
"C:\Users\win7\AppData\Local\Temp\VideoPad-2932-1\ffmpeg19.exe" -LQUIET -instby coVideoPad
MpSigStub.exe /program "C:\sample"
"C:\Program Files\TAP-Windows\bin\tapinstall.exe" hwids tap0901
"C:\Program Files\TAP-Windows\bin\tapinstall.exe" install "C:\Program Files\TAP-Windows\driver\OemVista.inf" tap0901
devcon status tap0901
C:\ProductInst64.exe PRODUCTI
"C:\Users\win7\AppData\Local\Temp\AIRDE3A.tmp\Adobe AIR Installer.exe"
MSIEXEC.EXE /i "C:\Users\win7\AppData\Local\Temp\{391B75D5-6713-4AEF-ABD7-8FA8B896C1E9}\A4tech USB Mouse Quality Testing Program V6.0.msi" SETUPEXEDIR="C:"
wmic /output:C:\Users\win7\AppData\Local\Temp\obhhelper.txt bios get serialnumber
wmic /output:C:\Users\win7\AppData\Local\Temp\obhhelper.txt bios get version
"C:\Users\win7\AppData\Local\Temp\5895\5895.exe"
"C:\Program Files\Internet Explorer\iexplore.exe" https://www.mql5.com/?utm_campaign=WebInstaller&utm_medium=special&utm_source=installer
"C:\RADS\system\rads_user_kernel.exe" updateandrun lol_launcher LoLLauncher.exe
C:\\Install_CD\Setup.exe
C:\App\Mines-Perfect\mineperf.exe
C:\Windows\splwow64.exe 12288
C:\Users\win7\AppData\Roaming\ImageCropResize\ImageEd\ImageEd.exe
"C:\Program Files\Internet Explorer\iexplore.exe" "http://networkdetective.s3-website-us-east-1.amazonaws.com/Application/Release/NetworkDetective.application"
"C:\Program Files\Internet Explorer\iexplore.exe" http://networkdetective.s3-website-us-east-1.amazonaws.com/Application/Release/NetworkDetective.application
C:\UsbFix\UsbFix.exe
findstr 5069
"C:\Program Files\Process Lasso\installhelper.exe" /terminate"
"C:\Program Files\Process Lasso\installHelper.exe" /firstinstall"
"C:\Program Files\Process Lasso\InstallHelper.exe" /powerinstall"
"C:\Program Files\Process Lasso\InstallHelper.exe" /install"
"C:\Program Files\Process Lasso\InstallHelper.exe" /enable_update_check"
"C:\Users\win7\AppData\Local\Temp\comodoccav_temp_setup\ccavstart.exe"
"C:\Windows\System32\xcopy.exe" AUTHORWA "C:\Windows\system32\Macromed\AUTHORWA" /s /e /i /y
"C:\Windows\System32\cmd.exe" /c del mini.inf /q
"C:\Windows\System32\cmd.exe" /c Move Shockwav.inf C:\Windows\INF
"C:\Windows\System32\reg.exe" Add "HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player + Authorware Web Player" /v "DisplayIcon" /t REG_SZ /d "C:\Windows\SysWOW64\Adobe\Shockwave 12\SwInit.exe" /f
MSIEXEC.EXE /i "C:\Users\win7\AppData\Local\Temp\{3BAC4DC0-38BD-486E-94F5-543341DAD65B}\VC12X86Redist.msi" SETUPEXEDIR="C:" SETUPEXENAME="sample"
"C:\Users\win7\AppData\Local\Temp\VSD7F1.tmp\dotnetfx\dotnetchk.exe"
"C:\Users\win7\AppData\Local\Temp\nsu5948.tmp\7z.exe" x "C:\ADDH.v11.0.0.2343-DATA.pkg" -o"C:\Users\win7\AppData\Local\Temp\ADDH11-RePack\" -y
"C:\PortableApps\geekMenu\GeekMenu.exe"
cmd.exe /C timeout 3 > Nul & Del "C:\sample"
"C:\Windows\system32\cmd.exe" /C ""C:\Users\win7\AppData\Local\Temp\is-SO3SR.tmp\pt_install_msi.cmd""
"C:\AICommand.bat"
"C:\Windows\Sysnative\cmd.exe" /C ""C:\Users\win7\AppData\Local\Temp\E1DA.tmp\hale.cmd""

"C:\Users\win7\AppData\Local\Temp\E1DA.tmp\hale.cmd"
bin\kbuildsycoca4.exe
"C:\sample"
"C:\Windows\system32\cmd.exe" /C ""C:\Users\win7\AppData\Local\Temp\is-FOINK.tmp\rt_install_msi.cmd""
"C:\Users\win7\AppData\Local\Temp\Opera Installer\sample" --version
"C:\Users\win7\AppData\Local\LogMeIn Rescue Applet\LMIR0001.tmp\lmi_rescue.exe"
"C:\Users\win7\AppData\Local\Google\Update\1.3.29.5\GoogleUpdateComRegisterShell64.exe" /user
"C:\Program Files\Internet Explorer\iexplore.exe" C:\Users\win7\AppData\Local\Temp\is-UCPO7.tmp\setupproblems_english.htm
net.exe session
C:\Users\win7\AppData\Local\Temp\appun-1.exe
"C:\MSVC-2010.exe" /q /norestart
timeout 3
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {5728603A-3FCB-4E6C-9E10-BC28D551EDDC}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {A54BEB11-7580-47D3-A88E-8DA33F6D1B38}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {0F488853-BB39-4F34-99DA-E7A6C7C7F3EF}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {A409DC24-7574-4AB0-BF83-35CDB0DB1C48}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {5ADC58D4-9F48-4405-855C-E2689F2C0D4B}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {AB138E76-8C41-4221-83F6-AFB12CD36481}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {4534286E-A18A-4048-8418-6C704F6AD0A8}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {43D76218-2C5B-4FC4-B838-7706FA167285}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {65F089CA-545C-4827-92F6-B22CA8B24A93}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {9DD74F05-BB6D-4F10-B807-00B6CA1D16E4}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {DC3C51F1-7A22-4523-BEA6-EF6A04CC56C1}
C:\Users\win7\AppData\Local\Temp\{D7840700-AB5E-44D0-8E3F-E9C3DC215D62}\ISBEW64.exe {EFB7539B-24F3-46B6-AF6E-3B021B51EFEF}: {D116A2E3-1FB9-43C3-92FE-D7199DE99823}
"C:\Temp\NVIDIA\3DVision\\nvStInst.exe" /check /srcdir=C:\Temp\NVIDIA\3DVision\
"C:\Users\win7\AppData\Local\Temp\OfficeSetup.exe" [sample]
C:\Program Files\Internet Explorer\iexplore.exe http://www.adobe.com/shockwave/download/?P1_Prod_Version=SWArchive11.5.0
"C:\Windows\System32\cmd.exe" /c echo [zoneTransfer]ZoneID = 2 > "C:\sample":ZONE.identifier & exit
C:\Users\win7\AppData\Roaming\Charles.exe
net STOP JavaQuickStarterService
"C:\Users\win7\AppData\Local\Temp\kvncviewer.exe" AutoSelect=0 LowColourLevel=1 FullColour=1 FullScreen=0 SendKeyEvents=1 SendPointerEvents=1 -listen
C:\setup\install_flash_player_ax.exe
C:\0
"C:\samplewb.exe"
"C:\Windows\System32\cscript.exe" "shell_scripts/check_if_cscript_is_working.js"
"C:\Windows\System32\mshta.exe" "C:\Users\win7\AppData\Local\Temp\HYD96EA.tmp.1460138451\HTA\index.hta?utorrent" "C:\sample" /LOG "C:\Users\win7\AppData\Local\Temp\HYD96EA.tmp.1460138451\index.hta.log" /PID "1612" /CID "AvB2wiJTRu0ppuuH" /VERSION "109814172" /OS "6.1" /BROWSERS "C:\Program Files\Internet Explorer\iexplore.exe" /ARCHITECTURE "64" /LANG "en" /USERNAME "win7" /SID "S-1-5-21-3979321414-2393373014-2172761192-1000" /CLIENT "utorrent"
"C:\Windows\system32\sc.exe" stop BDKernel_{PCFaster_5.1.0.0}
"C:\Program Files\Internet Explorer\iexplore.exe" http://www.java.com/pt_BR/
C:\Windows\WindowsUpdata\xed.exe
WMIC csproduct Get UUID /FORMAT:textvaluelist.xsl
WMIC bios Get SerialNumber /FORMAT:textvaluelist.xsl
WMIC bios Get Version /FORMAT:textvaluelist.xsl
WMIC csproduct Get Name /FORMAT:textvaluelist.xsl
7za.exe e -y -p"539af00e0e50bcf52eb5bfce6f6fdb07" [RANDOM_STRING].7z
nfregdrv.exe C:\Windows\system32\drivers\ssfilterdrv.sys
"C:\Users\win7\Documents\DCSCMIN\IMDCSC.exe"
"C:\Users\win7\AppData\Local\Temp\12345.exe"
"C:\Users\win7\AppData\Local\Temp\result.exe"
"C:\Users\win7\AppData\Roaming\subfolder\filename.exe"
"C:\Windows\System32\msiexec.exe" /i "C:\Users\win7\AppData\Local\Temp\comodoccav_temp_setup\ccav_installer.msi"
"C:\Users\win7\AppData\Local\Temp\deldll.bat"
"C:\launcher/launcher.exe"
"C:\Users\win7\AppData\Local\Temp\edurss.exe"

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	0x56094BC4 [Mon Sep 28 14:16:36 2015 UTC]
Entry Point	0x401914 (.text)
File Size	345088
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Copyright \xa9 2015
Internal Name	java
File Version	8.0.51.16
Full Version	1.8.0_51-b16
Company Name	Oracle Corporation
Product Name	Java(TM) Platform SE 8
Product Version	8.0.51.16
File Description	Java(TM) Platform SE binary
Original Filename	java.exe
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	85d0d6cf0d1c5de0d70c01ede1d89beb9e7958a330d46498823f3f930ababee1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6974	0x6a00	6.589007	-
.rdata	0x8000	0x1eaa	0x2000	5.321830	-
.data	0xa000	0x1fdc	0xe00	2.319294	-
.rsrc	0xc000	0x4a000	0x49800	6.886594	-
.reloc	0x56000	0xe54	0x1000	4.245482	-