VALKYRIE

**MALWARE**
Valkyrie Final Verdict

**File Name:** m39ska.EXE
**File Type:** PE32 executable (GUI) Intel 80386, for MS Windows
**SHA1:** 5f568e302ab5b99608f762c405e7f7754247e72d
**MD5:** 0bbdd9fe374151073c54310d687431d3
**First Seen Date:** 2016-03-30 15:49:26 UTC
**Number of Clients Seen:** 5
**Last Analysis Date:** 2016-03-30 15:49:26 UTC
**Human Expert Analysis Date:** 2016-03-30 16:56:46 UTC
**Human Expert Analysis Result:** Malware
**Verdict Source:** Valkyrie Human Expert Analysis Overall Verdict

## Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT |
|---|---|---|
| Signature Based Detection | 2016-03-30 15:49:26 UTC | Malware |
| Static Analysis Overall Verdict | 2016-03-30 15:49:26 UTC | No Threat Found |
| Dynamic Analysis Overall Verdict | 2016-03-30 15:49:26 UTC | No Threat Found |
| Human Expert Analysis Overall Verdict | 2016-03-30 16:56:46 UTC | Malware |
| 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**

- Process32FirstW
- Process32NextW
- TerminateProcess

IsDebuggerPresent
UnhandledExceptionFilter
GetWindowThreadProcessId

## Dynamic Analysis

| DYNAMIC ANALYSIS OVERALL VERDICT | RESULT |
| --- | --- |
| No Threat Found | |

| SUSPICIOUS BEHAVIORS | |
| --- | --- |
| No suspicious activity found | |

## Behavioral Information

### LoadLibrary

imm32.dll
uxtheme.dll
shell32.dll
C:\Windows\system32\ole32.dll
ADVAPI32.dll
comctl32.dll
UxTheme.dll
imageres.dll
C:\Windows\syswow64\MSCTF.dll
OLEAUT32.DLL
ntmarta.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
COMCTL32
KERNEL32
msi.dll
dbghelp.dll
rpcrt4.dll
COMCTL32.dll
SHLWAPI.dll
SspiCli.dll
SHELL32.dll
ole32.dll
MPR.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
C:\sample
mfeaaca.dll
WTSAPI32.dll
WINSTA.dll
RPCRT4.dll
C:\Windows\system32\msi.dll
VERSION.dll
msxml6.dll
kernel32.dll
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
propsys.dll
C:\Windows\SysWOW64\NETAPI32.DLL
C:\PFiles\MSWorks\custsat.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
USER32.DLL
dwmapi.dll
C:\Windows\system32\KERNEL32.DLL
C:\Windows\system32\kernel32.dll
RICHED32.DLL

CRYPTBASE.dll
C:\Windows\system32\Advapi32.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30.resources_31bf3856ad364e35_6.1.7600.16385_en-us_95b3d36c607e479c\msxml3r.dll.mui
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.17514_none_e6944609ad75ac7d\msxml3.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.17514_none_e6944609ad75ac7d\msxml3r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18431_none_e67b8ca5ad88b4d4\msxml3.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18431_none_e67b8ca5ad88b4d4\msxml3r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18782_none_e6468305adb05155\msxml3.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18782_none_e6468305adb05155\msxml3r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22640_none_e6f95b20c6af545f\msxml3.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22640_none_e6f95b20c6af545f\msxml3r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22986_none_e6d422dec6ca53a2\msxml3.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22986_none_e6d422dec6ca53a2\msxml3r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60.resources_31bf3856ad364e35_6.1.7600.16385_en-us_318843f5a10be121\msxml6r.dll.mui
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.17514_none_e69401b1ad75f960\msxml6.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.17514_none_e69401b1ad75f960\msxml6r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.18431_none_e67b484dad8901b7\msxml6.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.18431_none_e67b484dad8901b7\msxml6r.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.22640_none_e6f916c8c6afa142\msxml6.dll
C:\Windows\WinSxS\amd64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.22640_none_e6f916c8c6afa142\msxml6r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30.resources_31bf3856ad364e35_6.1.7600.16385_en-us_a0087dbe94df0997\msxml3r.dll.mui
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.17514_none_f0e8f05be1d66e78\msxml3.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.17514_none_f0e8f05be1d66e78\msxml3r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18431_none_f0d036f7e1e976cf\msxml3.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18431_none_f0d036f7e1e976cf\msxml3r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18782_none_f09b2d57e2111350\msxml3.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.18782_none_f09b2d57e2111350\msxml3r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22640_none_f14e0572fb10165a\msxml3.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22640_none_f14e0572fb10165a\msxml3r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22986_none_f128cd30fb2b159d\msxml3.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml30_31bf3856ad364e35_6.1.7601.22986_none_f128cd30fb2b159d\msxml3r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60.resources_31bf3856ad364e35_6.1.7600.16385_en-us_3bdcee47d56ca31c\msxml6r.dll.mui
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.17514_none_f0e8ac03e1d6bb5b\msxml6.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.17514_none_f0e8ac03e1d6bb5b\msxml6r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.18431_none_f0cff29fe1e9c3b2\msxml6.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.18431_none_f0cff29fe1e9c3b2\msxml6r.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.22640_none_f14dc11afb10633d\msxml6.dll
C:\Windows\WinSxS\wow64_microsoft-windows-msxml60_31bf3856ad364e35_6.1.7601.22640_none_f14dc11afb10633d\msxml6r.dll
C:\Windows\system32\d3d9.dll
C:\Windows\system32\d3d10_1core.dll
C:\Windows\system32\d3d11.dll
wtsapi32.dll
USER32.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\ARA\ChipsetARA.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\CHS\ChipsetCHS.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\CHT\ChipsetCHT.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\CSY\ChipsetCSY.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\DAN\ChipsetDAN.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\DEU\ChipsetDEU.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\ELL\ChipsetELL.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\ENU\ChipsetENU.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\ESP\ChipsetESP.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\FIN\ChipsetFIN.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\FRA\ChipsetFRA.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\HEB\ChipsetHEB.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\HUN\ChipsetHUN.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\ITA\ChipsetITA.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\JPN\ChipsetJPN.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\KOR\ChipsetKOR.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\NLD\ChipsetNLD.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\NOR\ChipsetNOR.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\PLK\ChipsetPLK.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\PTB\ChipsetPTB.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\PTG\ChipsetPTG.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\RUS\ChipsetRUS.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\SVE\ChipsetSVE.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\THA\ChipsetTHA.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\Lang\CHIP\TRK\ChipsetTRK.dll
DEVRTL.dll
SPINF.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
WINTRUST.dll
riched32.dll
riched20.dll
COMCTL32.DLL
IMM32.dll
Secur32.dll

API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
api-ms-win-downlevel-advapi32-l2-1-0.dll
OLEAUT32.dll
Shell32.dll
C:\Users\win7\AppData\Local\Temp\E30A.tmp
C:\Users\win7\AppData\Local\Temp\E309.tmp
Advapi32.dll
Msimg32.dll
atl.dll
KERNEL32.dll
NTDLL
GDI32.dll
SSPICLI
WINHTTP.dll
winhttp.dll
WS2_32.dll
Iphlpapi.dll
C:\Users\win7\AppData\Local\Google\Chrome\Application\chrome.exe
C:\Program Files\Microsoft Silverlight\sllauncher.exe
SXS.DLL
api-ms-win-downlevel-shlwapi-l2-1-0.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
urlmon.dll
IPHLPAPI.DLL
DNSAPI.dll
MSHTML.dll
dhcpcsvc.DLL
ntdll.dll
NSI.dll
CFGMGR32.dll
Comctl32.dll
C:\Windows\system32\ws2_32
MLANG.dll
PROPSYS.dll
WININET.dll
mshtml.dll
IEFRAME.dll
user32.dll
C:\Windows\system32\Msimtf.dll
OLEACC.DLL
OLEACCRC.DLL
C:\Windows\system32\Oleacc.dll
CRYPTSP.dll
d2d1.dll
DWrite.dll
dxgi.dll
C:\DXGIDebug.dll
C:\Windows\system32\DXGIDebug.dll
gdi32.dll
setupapi.dll
d3d11.dll
D3D10Warp.dll
C:\Windows\system32\D3D10Warp.dll
msls31.dll
ddraw.dll
C:\Windows\SysWOW64\DDRAW.dll
api-ms-win-core-winrt-l1-1-0.dll
C:\Windows\System32\msxml3r.dll
wininet.dll
C:\Windows\System32\shdocvw.dll
ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
dwrite.dll
C:\Windows\SysWOW64\jscript9.dll
HHCTRL.OCX
SHFOLDER
C:\Users\win7\AppData\Local\Temp\nsuBB91.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsuBB91.tmp\UAC.dll
AdvAPI32
SECUR32
RichEd20
C:\Users\win7\AppData\Local\Temp\nsuBB91.tmp\InstallOptions.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
ADVAPI32.DLL
SHELL32.DLL
OLE32.DLL

WS2_32.DLL
NTDLL.DLL
ieframe.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\winmm.dll
KERNEL32.DLL
NETAPI32.DLL
Crypt32
WTSAPI32.DLL
UXTHEME.DLL
IMM32.DLL
olepro32.dll
GDIPLUS.DLL
Kernel32.dll
advapi32.dll
C:\Windows\system32\CmUserMsgUs.dll
C:\CmUserMsgUs.dll
CRYPT32.dll
gdiplus.dll
MSIMG32.dll
PSAPI.DLL
USERENV.dll
WINMM.dll
Msftedit.dll
WindowsCodecs.dll
secur32.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
SensApi.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
C:\Windows\SysWOW64\ieframe.dll
iertutil.dll
DUser.dll
C:\Windows\system32\DUser.dll
C:\Windows\system32\xmllite.dll
profapi.dll
C:\Windows\syswow64\CRYPT32.dll
VERSION.DLL
C:\Windows\system32\user32.dll
C:\Windows\system32\wintab32.dll
C:\Windows\system32\uxtheme.dll
Wininet.dll
Cabinet.dll
C:\Windows\system32\odbcint.dll
C:\sampleENU.dll
C:\sampleLOC.dll
Riched20.dll
C:\Windows\SysWOW64\msls31.dll
C:\Users\win7\AppData\Local\Temp\nsnD7E4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nshB539.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-M958U.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-M958U.tmp\sample.EN
C:\Windows\SysWOW64\SAGE.DLL
C:\Users\win7\AppData\Local\Temp\is-68CEC.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-68CEC.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-DSRK1.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
C:\Users\win7\AppData\Local\Temp\is-DSRK1.tmp\ISLogo.dll
User32.dll
C:\Users\win7\AppData\Local\Temp\is-DSRK1.tmp\ISMD5.dll
C:\Users\win7\AppData\Local\Temp\is-DSRK1.tmp\ISDone.dll
C:\Windows\system32\imageres.dll
C:\Windows\system32\shlwapi.dll
MSFTEDIT.DLL
USP10.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
c:\windows\system32\imageres.dll
C:\Users\win7\AppData\Local\Temp\is-DSRK1.tmp\wintb.dll
Dwmapi.dll
C:\rarlng.dll
comdlg32.dll
C:\Users\win7\AppData\Local\Temp\nsx866C.tmp\LangDLL.dll

C:\Users\win7\AppData\Local\Temp\nsx866C.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsx866C.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\is-PLQ0A.tmp_isetup_shfoldr.dll
WINTRUST.DLL
imagehlp.dll
bcrypt.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\nso34FD.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-4M5B5.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-4M5B5.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nsk18AF.tmp\System.dll
msimg32.dll
C:\PYTHON27.DLL
pythondll
C:\Windows\system32\UxTheme.dll
C:\Windows\system32\comctl32.dll
C:\Windows\system32\Shlwapi
C:\Windows\system32\VBoxMRXNP.dll
C:\Windows\System32\drprov.dll
C:\Windows\System32\ntlanman.dll
C:\Windows\System32\davclnt.dll
C:\Windows\system32\Msimg32
c:\python27\dlls\py.ico
C:\CFVS_Injector.exe
C:\DLL_Loader.exe
C:\Procmon.exe
C:\Users\win7\AppData\Local\Temp\nsw41D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsw41D.tmp\nsExec.dll
C:\\sqmapi.dll
C:\Windows\system32\wintrust.dll
C:\Windows\system32\crypt32.dll
C:\Users\win7\AppData\Local\Temp\is-6KNCG.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-6KNCG.tmp\sample.EN
C:\WS2_32.dll
C:\Windows\system32\WS2_32.dll
C:\psapi.dll
C:\Windows\system32\psapi.dll
wintrust.dll
DnsApi.dll
C:\Users\win7\AppData\Local\Temp\nsi20CD.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsi20CD.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsi20CD.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsi20CD.tmp\ServicesHelper.dll
mpr.dll
oleaut32.dll
URLMON.DLL
version.dll
wsock32.dll
C:\Users\win7\AppData\Local\Temp\nsv13BC.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsv13BC.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsv13BC.tmp\InstallOptions.dll
security.dll
WSOCK32.dll
winspool.drv
winmm.dll
Fwpuclnt.dll
IdnDL.dll
Normaliz.dll
iphlpapi.dll
DWMAPI.DLL
C:\Windows\system32\advapi32.dll
user32
netutils.dll
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
feclient.dll
MMDevAPI.DLL
wdmaud.drv
MMDEVAPI.DLL
SETUPAPI.dll
AUDIOSES.DLL
msacm32.drv

midimap.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
SHFolder.dll
C:\Windows\system32\NTDLL.DLL
C:\Windows\system32\ADVAPI32.DLL
COMDLG32.dll
MPR.dll
msvcrt.dll
C:\Windows\system32\asycfilt.dll
C:\Windows\system32\regedit.exe
C:\Users\win7\AppData\Local\Temp\Uninstall.ico
C:\Users\win7\AppData\Local\Temp\Cleaning.ico
C:\Users\win7\AppData\Local\Temp\Scan.ico
C:\Users\win7\AppData\Local\Temp\Report.ico
C:\Users\win7\AppData\Local\Temp\Uninstall.bat
crypt32.dll
atiadlxx.dll
atiadlxy.dll
C:\Users\win7\AppData\Local\Temp\is-MMBTU.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-MMBTU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-MMBTU.tmp\saction.dll
RICHED20.DLL
C:\Users\win7\AppData\Local\Temp\nsb48C7.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsb48C7.tmp\InstallOptions.dll
AdvApi32.dll
C:\Users\win7\AppData\Local\Temp\nsmBBEE.tmp\nsExec.dll
Msi.DLL
C:\Users\win7\AppData\Local\Temp\{884B5357-8B44-41A9-B855-764F23996EF4}\ISSetup.dll
APPHELP.DLL
C:\Users\win7\AppData\Local\Temp\{884B5357-8B44-41A9-B855-764F23996EF4}\HP Support Assistant.msi
C:\Windows\SysWOW64\USER32.DLL
C:\Windows\SysWOW64\RPCRT4.DLL
C:\Users\win7\AppData\Local\Temp\{D631CE41-DECD-45D1-91EC-D95B5E718CF6}\ISRT.dll
NTDLL.dll
C:\Tsu.dll
C:\Users\win7\AppData\Local\Temp\nsz51F1.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsz51F1.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsz51F1.tmp\StartMenu.dll
C:\ProgramData\Battle.net\Setup\diablo3_enus\Diablo III Setup.exe
C:\gsdll32.dll
gsdll32.dll
msdmo.dll
msvfw32.dll
msrle32.dll
msvidc32.dll
msyuv.dll
iyuv_32.dll
tsbyuv.dll
iccvid.dll
imaadp32.acm
msg711.acm
msgsm32.acm
msadp32.acm
C:\Windows\system32\sfc.dll
C:\Users\win7\AppData\Local\Temp\ffmpeg10.exe
cmdhtml.dll
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\DataCollection
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\AdvSplash.dll
C:\Windows\system32\WINMM.dll
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\ZipSubPackSizeCheck
C:\Users\win7\AppData\Local\Temp\nsw8ACB.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsw8ACB.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsw8ACB.tmp\InstallOptions.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
dllhost.exe
shlwapi.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\System32\msimg32.dll
C:\Windows\System32\mpr.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\SysWOW64\comdlg32.dll
C:\Windows\System32\winspool.drv
C:\Windows\System32\ddraw.dll
C:\Windows\System32\dciman32.dll
C:\Windows\SysWOW64\setupapi.dll
C:\Windows\SysWOW64\cfgmgr32.dll
C:\Windows\SysWOW64\devobj.dll
C:\Windows\System32\dwmapi.dll
C:\Windows\System32\imm32.dll
C:\Windows\SysWOW64\msctf.dll
C:\Windows\SysWOW64\psapi.dll
C:\Windows\SysWOW64\imagehlp.dll
PSAPI.dll
C:\SAMPLE
C:\a2framework.dll
a2framework.dll
C:\Users\win7\AppData\Local\Temp\{35C77D8B-E185-48EC-AAE4-8DDAB59762BC}\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{35C77D8B-E185-48EC-AAE4-8DDAB59762BC}\SIV.msi
C:\Users\win7\AppData\Local\Temp_isAC95..dll
C:\Windows\system32\windowscodecs.dll
C:\Users\win7\AppData\Local\Temp_isAD83..dll
C:\Users\win7\AppData\Local\Temp_isAECE..dll
C:\Users\win7\AppData\Local\Temp_isAF4D..dll
C:\Users\win7\AppData\Local\Temp_isB0C6..dll
C:\Users\win7\AppData\Local\Temp\is-C1H85.tmp_isetup_shfoldr.dll
FaultRep.dll
C:\Users\win7\AppData\Local\Temp\is-K46KV.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-K46KV.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-M0UQ5.tmp_isetup_shfoldr.dll
C:\Windows\system32\wer.dll
werui.dll
DUI70.dll
C:\Windows\system32\RICHED20.DLL
powrprof.dll
psapi.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\syswow64\KERNEL32.dll
C:\Windows\syswow64\KERNELBASE.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\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\system32\IMM32.DLL
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\syswow64\shell32.dll
C:\Windows\system32\CRYPTSP.dll
C:\Windows\system32\rsaenh.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\system32\apphelp.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscordacwks.dll
C:\Users\win7\AppData\Local\Temp\nsaAC33.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsaAC33.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsaAC33.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nseABF9.tmp\System.dll
shell32
C:\idmvs.dll
Connect.dll
RASAPI32
MSISIP.DLL
C:\Windows\SysWOW64\cryptnet.dll
ssutil.dll
WinSpool.drv
Imagehlp.dll
libcef.dll
C:\MapSource_LANG.dll
kernel32.DLL
mciavi32.dll
zciavi32.dll
credui.dll
rasapi32.dll
UIAutomationCore.dll
ws2_32.dll
shlwapi
C:\Users\win7\AppData\Local\Temp\000c3260.a
C:\Users\win7\AppData\Local\Temp\000c38f7.a
jscript9.dll
C:\Windows\System32\msxml6r.dll
C:\Users\win7\AppData\Local\Temp\is-J0PLU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\SUPERSetup\GCAPI_DLL.DLL
C:\Users\win7\AppData\Local\Temp\SUPERSetup\setup.dll
C:\Program Files\SUPERAntiSpyware\SUPERAntiSpyware.exe
Userenv.dll
C:\Windows\system32\IconCodecService.dll
Mpr.dll
SetupRes.dll
MSVCRT.DLL
jsproxy.dll
C:\Users\win7\AppData\Local\Temp\is-NTAEI.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-NTAEI.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\idp.dll

C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\innocallback.ENU
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\innocallback.EN
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\isslideshow.dll
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\isslideshow.ENU
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\isslideshow.EN
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\ISDone.dll
C:\Windows\system32\DSOUND.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\perfos.dll
C:\Users\win7\AppData\Local\Temp\GLC6495.tmp
C:\Users\win7\AppData\Local\Temp\
Riched20.DLL
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\nsEnvVariables.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\linker.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\nsProcess.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\nsSessionSIDW.dll
C:\Users\win7\AppData\Local\Temp\nshDC39.tmp\nsExec.dll
C:\Windows\system32\MFC120ENU.DLL
C:\Windows\SysWOW64\DUser.dll
C:\Users\win7\AppData\Local\Temp\is-NR4LS.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-NR4LS.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-7PJTS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsqDE79.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-1N4OE.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-1N4OE.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-K5LRG.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsjFFDD.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nszC990.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nszC990.tmp\NSISGameExplorerPlugin.dll
Wtsapi32.dll
Advapi32
C:\Windows\system32\wucltux.dll
MSWSOCK.dll
wpcap.dll
pstorec.dll
notesproxy.dll
rstrtmgr.dll
netprofm.dll
C:\Windows\system32\ExplorerFrame.dll
OLEAUT32
C:\Users\win7\AppData\Local\Temp\setupenu.dll
C:\Users\win7\AppData\Local\Temp\is-JU0TC.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-JU0TC.tmp_isetup_shfoldr.dll
POWRPROF.dll
mtxoci.dll
oci.dll
C:\Windows\system32\comsvcs.dll
C:\Windows\system32\Winsta.dll
C:\Windows\SysWOW64\taskkill.exe
C:\Users\win7\AppData\Local\Temp\nss6DD4.tmp\killopenfm.bat
C:\Users\win7\AppData\Local\Temp\nss6DD4.tmp\nsDialogs.dll
psapi
C:\Users\win7\AppData\Local\Temp\is-BEQ04.tmp_isetup_shfoldr.dll
XmlLite.dll
inetmib1.dll

snmpapi.dll
C:\Users\win7\AppData\Local\Temp\oc_BD3A\OCDLL.DLL
C:\Program Files\Internet Explorer\iexplore.exe
C:\Windows\SysWOW64\timeout.exe
C:\Windows\system32\wups.dll
C:\Windows\system32\wu.upgrade.ps.dll
C:\application\setup.dll
C:\setup.dll
C:\Users\win7\AppData\Local\Temp\nsqEE45.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsqEE45.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsqEE45.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-HR741.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsjD760.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsjD760.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsjD760.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsyC640.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsyC640.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsyC640.tmp\GetVersion.dll
C:\Users\win7\AppData\Local\Temp\nsyC640.tmp\registry.dll
C:\Users\win7\AppData\Local\Temp\nsyC640.tmp\EnumINI.dll
C:\Windows\system32\CRTDLL.dll
C:\Windows\system32\ntdll.dll
C:\Users\win7\AppData\Local\Temp\is-VUL7R.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-VUL7R.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-K4E9T.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-K4E9T.tmp\GoogleAnalyticsHelper.dll
FastMM_FullDebugMode.dll
C:\Users\win7\AppData\Local\Temp\nsfEA02.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsfEA02.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsfEA02.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\is-43LD5.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-43LD5.tmp\sample.EN
C:\Windows\SysWOW64\Advapi32.dll
C:\Windows\SysWOW64\Kernel32.dll
C:\Windows\SysWOW64\Shell32.dll
C:\Windows\SysWOW64\Wintrust.dll
C:\Windows\SysWOW64\Userenv.dll
C:\Windows\SysWOW64\pdh.dll
C:\Windows\SysWOW64\WinInet.dll
C:\Windows\SysWOW64\GDI32.dll
C:\\UVK.dll
COMDLG32.DLL
OLE32.dll
C:/Users/win7/AppData/Local/Temp/BRE758.tmp
C:/Users/win7/AppData/Local/Temp/BRE7D6.tmp
C:/Users/win7/AppData/Local/Temp/be29e7f1-71ae-4703-50cb-1d52be512f51/twapi-be29e7f1-71ae-4703-50cb-1d52be512f51.dll
icmp.dll
MSDART.dll
C:\Users\win7\AppData\Local\Temp\~gs1851.tmp
C:\Users\win7\AppData\Local\Temp\~gs1851.ENU
C:\Users\win7\AppData\Local\Temp\~gs1851.EN
C:\Users\win7\AppData\Local\Temp\7ZipSfx.000\setup7z.cmd
C:\Users\win7\AppData\Local\Temp\is-1LGMP.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-1LGMP.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nskE4BA.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nskE4BA.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nskE4BA.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nskE4BA.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nskE4BA.tmp\StartMenu.dll
C:\Windows\Branding\Basebrd\Basebrd.dll
dSound.dll
C:\Windows\system32\dSound.dll
C:\Users\win7\AppData\Local\Temp\GUM3D14.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUM3D14.tmp\goopdateres_en.dll
C:\Windows\system32\AutoRunGUI.DLL
C:\Users\win7\AppData\Local\Temp\GUM49EF.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUM49EF.tmp\goopdateres_en.dll
C:\Users\win7\AppData\Local\Temp\kvncviewer.exe
GLU32.DLL
OPENGL32.DLL
WINMM.DLL
WSOCK32.DLL
OPENGL32
gdi32
VBoxOGL.dll
C:\Windows\system32\gdi32.dll
C:\Users\win7\AppData\Local\Temp\is-U1QMU.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-U1QMU.tmp\sample.EN

mscms.dll
C:\Users\win7\AppData\Local\Temp\is-6N01U.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-6N01U.tmp\InstallHelper.dll
C:\Users\win7\AppData\Local\Temp\is-6N01U.tmp\idp.dll
Ftd2xx.dll
C:\shfolder.dll
C:\Users\win7\AppData\Local\Temp\is-UPE0R.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-Q23PO.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-Q23PO.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsjAF33.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsjAF33.tmp\nsisos.dll
C:\Windows\system32\CRTDLL.DLL
C:\Users\win7\AppData\Local\Temp\NSISPromotionEx.dll
C:\Users\win7\AppData\Local\Temp\nsjAF33.tmp\AdvSplash.dll
NSISPromotionEx.dll
C:\Windows\SysWOW64\quartz.dll
C:\Users\win7\AppData\Local\Temp\nsb384A.tmp\System.dll
C:\Windows\system32\DBGHELP.DLL
ref_gl.dll
ref_soft.dll
C:\Users\win7\AppData\Local\Temp\nsg572C.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsg572C.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsg572C.tmp\KillProcDLL.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.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.Drawing\5a401fd2a7689ff13fb54182953f9c40\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\6949c4470a81970ec3de0a575d93babc\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\0967cf5c31691f38d013263304d2dacb\System.Runtime.Remoting.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.Configuration\007fc007edc388d9806dff94ee04f129\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\d49908aa93a23c84847b1f8b1b667860\System.Xml.ni.dll
Kernel32
C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\uxtheme.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\Gdiplus.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.Management\99cdfef98595ed91f14936cf52a49c54\System.Management.ni.dll
C:\Users\win7\AppData\Local\Temp\is-OJ2SH.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-OJ2SH.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-C8RPH.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-C8RPH.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-AQ7CT.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-AQ7CT.tmp_isetup_iscrypt.dll
Kernel32.DLL
C:\English\Strings.dll
netapi32.dll
quartz.dll
USER32
Wship6.dll
icm32.dll
catalog20.dll
C:\Windows\system32\dbghelp.dll
C:\$Windows.~WS\Sources\SetupHost.Exe
winbrand.dll
SLC.DLL
C:\$Windows.~WS\Sources\MediaSetupUIMgr.dll
C:\$Windows.~WS\Sources\SetupCore.dll
C:\$Windows.~WS\Sources\SetupPlatform.dll
C:\$Windows.~WS\Sources\migcore.dll
sqmapi.dll
C:\$Windows.~WS\Sources\SetupMgr.dll
C:\Windows\system32\imagehlp.dll
Wintrust.dll
C:\Windows\system32\dwmapi.dll
\aswSZB.dll
C:\Users\win7\AppData\Local\Temp\is-A0SVI.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-A0SVI.tmp\sample.EN
vb6stkit.dll
C:\dbghelp.dll
advpack.dll
dsetup.dll
C:\Users\win7\AppData\Local\Temp_isD26..dll
C:\Users\win7\AppData\Local\Temp_is111F..dll
C:\Users\win7\AppData\Local\Temp_is148B..dll
C:\Users\win7\AppData\Local\Temp_is15C5..dll
C:\Users\win7\AppData\Local\Temp_is1681..dll

api-ms-win-core-string-l1-1-0
JRTools.dll
C:\Windows\system32\srclient.dll
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.ba\mbahost.dll
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.ba\mbapreq.dll
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.ba\bafunctions.dll
C:\Users\win7\AppData\Local\Temp\{390383CD-9143-4AF7-93C1-CCA8B896C1E9}\.cr\sample
C:\Windows\system32\MSI.DLL
VDMDBG.DLL
C:\Users\win7\AppData\Local\Temp\is-NV9S6.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-NV9S6.tmp\sample.EN
0x627d1e01.d

**QueryFilePath**

C:\sample
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\system32\msi.dll
C:\Windows\system32\RICHED20.dll
C:\Users\win7\AppData\Local\Temp\IPMx2\setup.exe
C:\Users\win7\AppData\Local\Tem
C:\Windows\system32\PROPSYS.dll
C:\Windows\SysWOW64\DDRAW.dll
C:\Windows\SysWOW64\ieframe.dll
]
D]
D]\sample
4]
l]
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\msxml3.dll
C:\Windows\system32\RichEd20.DLL
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Windows\system32\ieframe.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\system32\DUser.dll
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\system32\Msftedit.dll
C:\Windows\SysWOW64\schannel.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\system32\ODBC32.dll
C:\Windows\system32\Riched20.dll
C:\Users\win7\AppData\Local\Temp\is-M958U.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-68CEC.tmp\sample.tmp
C:\Windows\system32\MSFTEDIT.DLL
C:\Windows\system32\EhStorShell.dll
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Users\win7\AppData\Local\Temp\is-M0GN9.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\7zS7887.tmp\Installer.exe
C:\DLL_Loader.exe
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\system32\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-4M5B5.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-6KNCG.tmp\sample.tmp
C:\Windows\system32\mscoree.dll
C:\Windows\SysWOW64\mshtml.dll
C:\Users\win7\AppData\Local\Temp\04e990e6-f419-11e5-9e88-08002763e612\Ninite.exe
C:\Windows\system32\propsys.dll
C:\Windows\system32\ntshrui.dll
C:\Windows\SysWOW64\MSIEXEC.EXE
C:\Windows\SysWOW64\MSCOREE.DLL

C:\Windows\SysWOW64\MsiHnd.dll
C:\Users\win7\AppData\Local\Temp\is-OG8DQ.tmp\sample.tmp
C:\Windows\SysWOW64\RunDll32.exe
C:\Users\win7\AppData\Local\Temp\is-TGNHU.tmp\sample.tmp
C:\Windows\SysWOW64\RunDll32.ex
C:\Windows\SysWOW64\RichEd20.dll
C:\Users\win7\AppData\Local\Temp\is-MMBTU.tmp\OCSetupHlp.dll
C:\Windows\system32\RICHED20.DLL
C:\Users\win7\AppData\Local\Temp\nsmBBEE.tmp\setupcl.exe
C:\Users\win7\AppData\Local\Temp\{884B5357-8B44-41A9-B855-764F23996EF4}\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{D631CE41-DECD-45D1-91EC-D95B5E718CF6}\ISRT.dll
C:\ProgramData\Battle.net\Setup\diablo3_enus\Diablo III Setup.exe
C:\Users\win7\AppData\Local\Temp\ffmpeg10.exe
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:\Windows\system32\WINMM.dll
C:\Users\win7\AppData\Local\Temp\nsyFE39.tmp\DataCollection.DLL
VERSION_INFO
C:\CFVS_HookDll.dll
C:\Windows\syswow64\WS2_32.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\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\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\system32\msimg32.dll
C:\Windows\system32\mpr.dll
C:\Windows\syswow64\shell32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\syswow64\comdlg32.dll
C:\Windows\system32\winspool.drv
C:\Windows\system32\ddraw.dll
C:\Windows\system32\DCIMAN32.dll
C:\Windows\syswow64\SETUPAPI.dll
C:\Windows\syswow64\CFGMGR32.dll
C:\Windows\syswow64\DEVOBJ.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\PSAPI.DLL
C:\Windows\syswow64\imagehlp.dll
C:\Users\win7\AppData\Local\Temp\{35C77D8B-E185-48EC-AAE4-8DDAB59762BC}\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\is-VET50.tmp\sample.tmp
C:\Windows\system32\FaultRep.dll
C:\Windows\system32\wsock32.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.18837_none_ec86b8d6858ec0bc\comctl32.dll
C:\Users\win7\AppData\Local\Temp\is-K46KV.tmp\sample.tmp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
C:\Windows\system32\werui.dll
C:\Windows\system32\Connect.dll
C:\Windows\SysWOW64\msiexec.exe
C:\Windows\System32\msi.dll
C:\Windows\SysWOW64\cryptnet.dll

C:\Windows\system32\credui.dll
C:\Users\win7\AppData\Local\Temp\000c38f7.a
C:\Windows\System32\msxml6.dll
C:\Users\win7\AppData\Local\Temp\is-LG5EH.tmp\sample.tmp
C:\Windows\system32\riched20.dll
C:\Users\win7\AppData\Local\Temp\is-NTAEI.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\innocallback.dll
C:\Users\win7\AppData\Local\Temp\is-NDEJT.tmp\isslideshow.dll
C:\Windows\system32\DSOUND.dll
C:\Users\win7\AppData\Local\Temp\GLC6495.tmp
C:\Windows\system32\Riched20.DLL
C:\594140c9-36e2-477a-91d3-26412045ff41.exe
C:\Windows\system32\mfc120u.dll
C:\Windows\SysWOW64\DUser.dll
C:\Windows\SysWOW64\dwwin.exe
C:\Windows\SysWOW64\werui.dll
C:\Users\win7\AppData\Local\Temp\is-NR4LS.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-1N4OE.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\setupenu.dll
C:\Users\win7\AppData\Local\Temp\is-O0SEB.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-JU0TC.tmp\OCSetupHlp.dll
C:\Users\win7\AppData\Local\Temp\is-DU5ON.tmp\sample.tmp
C:\Windows\SysWOW64\taskkill.exe
C:\Windows\SysWOW64\wscript.exe
C:\Users\win7\AppData\Local\Temp\7e05ad89-f53e-11e5-9e88-08002763e612\Ninite.exe
C:\Users\win7\AppData\Local\Temp\oc_BD3A\OCDLL.DLL
C:\Windows\SysWOW64\timeout.exe
C:\Users\win7\AppData\Local\Temp\is-54AOQ.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-861FO.tmp\sample.tmp
C:\Windows\system32\CRTDLL.dll
C:\Users\win7\AppData\Local\Temp\is-VUL7R.tmp\sample.tmp
C:\Windows\system32\odbc32.dll
C:\Users\win7\AppData\Local\Temp\is-K4E9T.tmp\GoogleAnalyticsHelper.dll
C:\Users\win7\AppData\Roaming\Adobe\Uninstall.exe
C:\Users\win7\AppData\Local\Temp\is-K4E9T.tmp\rtl160.bpl
C:\Users\win7\AppData\Local\Temp\is-K4E9T.tmp\AxComponentsRTL.bpl
C:\Users\win7\AppData\Local\Temp\is-43LD5.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\~gs1851.tmp
C
C:\Users\win7\AppData\Local\Temp_uninstall_uninstall2372
C:\Windows\SysWOW64\cmd.exe
C:\Users\win7\AppData\Local\Temp\is-1LGMP.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-D0L28.tmp\sample.tmp
C:\Windows\system32\WINBRAND.dll
C:\Windows\system32\dSound.dll
C:\Users\win7\AppData\Local\Temp\GUM3D14.tmp\DropboxUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUM3D14.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUM49EF.tmp\DropboxUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUM49EF.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\kvncviewer.exe
C:\Users\win7\AppData\Local\Temp\is-U1QMU.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-IUDLR.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-3PJMQ.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-Q23PO.tmp\OCSetupHlp.dll
C:\Windows\system32\CRTDLL.DLL
C:\Users\win7\Documents\tttttt.exe
C:\Windows\system32\DINPUT8.dll
C:\Users\win7\AppData\Local\Temp\is-OJ2SH.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-C8RPH.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-KER4L.tmp\sample.tmp
C:\Windows\system32\quartz.dll
C:\Users\win7\AppData\Local\Temp\sW\e.exe
C:\$Windows.~WS\Sources\SetupHost.Exe
C:\$Windows.~WS\Sources\SetupPlatform.dll
C:\Windows\system32\winbrand.dll
C:\$Windows.~WS\Sources\MediaSetupUIMgr.dll
C:\$Windows.~WS\Sources\WDSCORE.dll
C:\$Windows.~WS\Sources\SetupMgr.dll
C:\$Windows.~WS\Sources\SetupCore.dll
C:\Users\win7\AppData\Local\Temp\is-A0SVI.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\Ver2E14.tmp
C:\Users\win7\AppData\Local\Temp\{390383CD-9143-4AF7-93C1-CCA8B896C1E9}\.cr\sample
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.be\FuzeInstallerPerUser.exe
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.ba\mbahost.dll
C:\Users\win7\AppData\Local\Temp\{97937BFE-5F33-426A-9C72-F21F4A2A208E}\.ba\mbapreq.dll
C:\Users\win7\AppData\Local\Temp\is-NV9S6.tmp\sample.tmp

## Precise Detectors Analysis Results

### No Detector Result Received

## Advance Heuristics

### No Advanced Heuristic Analysis Result Received

## Human Expert Analysis Results

**Analysis Start Date:** 2016-03-30 16:28:03 UTC
**Analysis End Date:** 2016-03-30 16:56:46 UTC
**File Upload Date:** 2016-03-30 15:49:26 UTC
**Human Expert Analyst Feedback:**
**Verdict:** Malware

## Additional File Information

**Vendor Validation** - Vendor Validation is not Applicable ?

**Certificate Validation** - Certificate Validation is not Applicable ?

**PE Headers**

| PROPERTY | VALUE |
|---|---|
| Compilation Time Stamp | 0x56FB6B83 [Wed Mar 30 06:00:35 2016 UTC] |
| Entry Point | 0x407506 (.text) |
| File Size | 162816 |
| Machine Type | Intel 386 or later - 32Bit |
| Legal Copyright | Copyright © Southsoftware.com, 2002-2015 |
| Internal Name | #dvenced Task Scheduler 32-bit Edition |
| File Version | 4.1.0.612 |
| Company Name | Doubtsoftware.com |
| Product Name | Advanced Task Scheduler 32-bit Edition |
| Product Version | 4.1.0.612 |
| File Description | Advanced Task Scheduler 32-bit Edition |
| Original Filename | Bifscheduler_edmin.exe |
| Translation | 0x0409 0x04e2 |
| Mime Type | application/x-dosexec |
| Number Of Sections | 6 |
| Sha256 | 22ac782cf9af5fff89edef0fbe2680cae199407cf88aa9d0aecadb90f4c21b89 |

**PE Sections**

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| .text | 0x1000 | 0xf136 | 0xf200 | 7.002278[SUSPICIOUS] | - |
| .rdata | 0x11000 | 0x865e | 0x8800 | 6.570776 | - |
| .data | 0x1a000 | 0x441c | 0x3400 | 6.948257 | - |
| .data3 | 0x1f000 | 0x250 | 0x400 | 1.674468 | - |
| .rsrc | 0x20000 | 0xb270 | 0xb400 | 4.134322 | - |
| .reloc | 0x2c000 | 0x10c4 | 0x1200 | 5.082737 | - |