VALKYRIE

MALWARE
Valkyrie Final Verdict

File Name: 80.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: d02f19accf695508bc31a650539934d8ea46fb15
MD5: 00442a088456ce18a43187605557b3d1
First Seen Date: 2016-04-04 11:59:35 UTC
Number of Clients Seen: 8
Last Analysis Date: 2016-04-04 11:59:35 UTC
Human Expert Analysis Date: 2016-04-04 12:52:21 UTC
Human Expert Analysis Result: Malware
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2016-04-04 11:59:35 UTC	Malware
Static Analysis Overall Verdict	2016-04-04 11:59:35 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2016-04-04 11:59:35 UTC	No Threat Found
Human Expert Analysis Overall Verdict	2016-04-04 12:52:21 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	Suspicious
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Suspicious
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

- OutputDebugStringA
- TerminateProcess
- UnhandledExceptionFilter

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Has no visible windows	

Behavioral Information

LoadLibrary

C:\Windows\system32\uxtheme.dll
dwmapi.dll
ADVAPI32.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
uxtheme.dll
shell32.dll
comctl32
UxTheme.dll
comctl32.dll
OLEAUT32.DLL
imm32.dll
kernel32.dll
rstrtmgr.dll
C:\sample
C:\sampleENU.dll
C:\sampleLOC.dll
RICHED20.DLL
SHELL32.dll
ADVAPI32.DLL
ole32.dll
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
propsys.dll
ntmarta.dll
C:\Windows\system32\shell32.dll
C:\Windows\system32\ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
netutils.dll
KERNEL32.dll
USER32.dll
GDI32.dll
WININET.dll
MPR.dll
NETAPI32.dll
urlmon.dll
CRYPTSP.dll
CRYPTBASE.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
Comctl32.dll
C:\Windows\system32\ws2_32
C:\Windows\System32\msxml3r.dll
URLMON.DLL
imageres.dll
SHFOLDER
C:\Users\win7\AppData\Local\Temp\nse4FC1.tmp\execDos.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
OLEAUT32.dll
SHLWAPI.dll

OLEACCRC.DLL
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
ShFolder.DLL
C:\t8res.dll
C:\sares.dll
atiadlxx.dll
KERNEL32.DLL
COMDLG32.DLL
MSIMG32.DLL
msvcrt.dll
newdev.dll
SETUPAPI.dll
WSOCK32.DLL
advapi32
backtrace.dll
COMCTL32.dll
CRYPT32.dll
gdiplus.dll
MSIMG32.dll
PSAPI.DLL
USERENV.dll
WINMM.dll
WINTRUST.dll
Advapi32.dll
Msftedit.dll
SspiCli.dll
dbghelp.dll
rpcrt4.dll
wininet.dll
c:\program files\internet explorer\iexplore.exe
C:\Users\win7\AppData\Local\Temp\nsvB5E7.tmp\System.dll
IMM32.dll
-33A8A424-
VERSION.dll
C:\Users\win7\AppData\Local\Temp\nsq26F0.tmp\System.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
advapi32.dll
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
MSVCRT.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\cryptbase.dll
C:\Windows\system32\SHCore.dll
C:\Windows\system32\oleacc.dll
C:\Windows\system32\apphelp.dll
WINSTA.dll
RPCRT4.dll
C:\Program Files\Internet Explorer\iexplore.exe
C:\Users\win7\AppData\Local\Temp\is-CFRR5.tmp_isetup_shfoldr.dll
shfolder.dll
C:\Windows\system32\imageres.dll
C:\Windows\System32\shdocvw.dll
PROPSYS.dll
C:\Users\win7\AppData\Local\Temp\nsu9DFE.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsu9DFE.tmp\SetupHelper.dll
msimg32.dll
user32.dll
shlwapi.dll
libcurl.dll
WtsApi32.dll
olepro32.dll
UXTHEME.DLL
Kernel32.dll
riched32.dll
riched20.dll
USER32.DLL
C:\Windows\system32\IconCodecService.dll
WindowsCodecs.dll
C:\Users\win7\AppData\Local\Temp\is-P5OUG.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-P5OUG.tmp\sample.EN
C:\Windows\system32\kernel32.dll
C:\Users\win7\AppData\Local\Temp\nsc6CF2.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-KTJTQ.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-KTJTQ.tmp\sample.EN

C:\Users\win7\AppData\Local\Temp\is-C2SEB.tmp_isetup_shfoldr.dll
Rstrtmgr.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
C:\Users\win7\AppData\Local\Temp\is-C2SEB.tmp\WizardHelper.dll
COMCTL32
KERNEL32
C:\Users\win7\AppData\Local\Temp\nsfA0A3.tmp\NSISHelper.dll
setupapi.dll
CfgMgr32.dll
DEVRTL.dll
SPINF.dll
C:\Users\win7\AppData\Local\Temp\nsx9931.tmp\System.dll
Shell32.dll
C:\Users\win7\AppData\Local\Temp\nsdD66.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsdD66.tmp\System.dll
ADVAPI32
ShlWAPI
SECUR32
Wtsapi32.dll
C:\Users\win7\AppData\Local\Temp\nsdD66.tmp\TBC.dll
RichEd20
C:\Windows\SysWOW64\ieframe.dll
C:\1033\sampleUI.DLL
C:\9\sampleUI.DLL
C:\Documents and Settings\sampleUI.DLL
C:\PerfLogs\sampleUI.DLL
C:\Program Files\sampleUI.DLL
C:\ProgramData\sampleUI.DLL
C:\Python27\sampleUI.DLL
C:\Recovery\sampleUI.DLL
C:\System Volume Information\sampleUI.DLL
C:\Users\sampleUI.DLL
C:\Windows\sampleUI.DLL
C:\Users\win7\AppData\Local\Temp\nsk3EC.tmp\nsExec.dll
C:\Windows\system32\AdvApi32.dll
C:\Windows\system32\Msi.dll
feclient.dll
C:\Users\win7\AppData\Local\Temp\is-IKAE7.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-IKAE7.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-B2CHU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\gentee00\gentee.dll
C:\Users\win7\AppData\Local\Temp\gentee00\guig.dll
gentee.dll
gdi32.dll
version.dll
MSVBVM60.DLL
SXS.DLL
kernel32
user32
Ntdll
msi.dll
C:\Users\win7\AppData\Local\Temp\{a1909659-0a08-4554-8af1-2175904903a1}\.ba1\wixstdba.dll
ntdll.dll
C:\Windows\system32\Riched20.dll
USP10.dll
msls31.dll
NTDLL.dll
winmm.dll
NTDLL
COMDLG32.dll
WINSPOOL.DRV
oledlg.dll
WTSAPI32.dll
SAMCLI
C:\Users\win7\AppData\Local\Temp\nszCFAC.tmp\InstallOptions.dll
C:\Windows\system32\ntdll.dll
C:\Windows\system32\KERNELBASE.dll
C:\Windows\system32\API-MS-Win-Core-LibraryLoader-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Synch-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Handle-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Heap-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Profile-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-DelayLoad-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-IO-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-ErrorHandling-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-ProcessThreads-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-SysInfo-L1-1-0.dll
C:\Windows\system32\CRYPTBASE.dll

C:\Windows\system32\API-MS-Win-Core-DateTime-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-ProcessEnvironment-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Misc-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-File-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Debug-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Console-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Localization-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Util-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-String-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Fibers-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-Memory-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-NamedPipe-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-ThreadPool-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-RtlSupport-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Security-Base-L1-1-0.dll
C:\Windows\system32\KERNEL32.dll
C:\Windows\system32\msvcrt.dll
C:\Windows\system32\API-MS-Win-Core-Interlocked-L1-1-0.dll
C:\Windows\system32\API-MS-Win-Core-LocalRegistry-L1-1-0.dll
C:\Windows\system32\API-MS-WIN-Service-Management-L1-1-0.dll
C:\Windows\system32\API-MS-WIN-Service-Core-L1-1-0.dll
C:\Windows\system32\RPCRT4.dll
C:\Windows\system32\API-MS-WIN-Service-winsvc-L1-1-0.dll
C:\Windows\system32\API-MS-WIN-Service-Management-L2-1-0.dll
C:\Windows\system32\ADVAPI32.dll
C:\Windows\system32\Secur32.dll
C:\Windows\system32\API-MS-Win-Security-LSALookup-L1-1-0.dll
C:\Windows\system32\SspiCli.dll
C:\Windows\system32\sechost.dll
C:\Windows\system32\LPK.dll
C:\Windows\system32\GDI32.dll
C:\Windows\system32\USER32.dll
C:\Windows\system32\USP10.dll
C:\Windows\system32\MSCTF.dll
C:\Windows\system32\IMM32.dll
C:\Windows\system32\OLEAUT32.dll
C:\Windows\system32\NSI.dll
C:\Windows\system32\WS2HELP.dll
C:\Windows\system32\WS2_32.dll
C:\Windows\system32\MSWSOCK.dll
C:\Windows\system32\MPR.dll
C:\Windows\system32\CFGMGR32.dll
C:\Windows\system32\DEVOBJ.dll
C:\Windows\system32\SETUPAPI.dll
C:\Windows\system32\SensApi.dll
C:\Windows\system32\Normaliz.dll
C:\Windows\system32\SHLWAPI.dll
C:\Windows\system32\iertutil.dll
C:\Windows\system32\WININET.dll
C:\Windows\system32\urlmon.dll
C:\Windows\system32\WINNSI.DLL
C:\Windows\system32\IPHLPAPI.DLL
C:\Windows\system32\imagehlp.dll
C:\Windows\system32\MSASN1.dll
C:\Windows\system32\CRYPT32.dll
C:\Windows\system32\WINTRUST.dll
C:\Windows\system32\profapi.dll
C:\Windows\system32\USERENV.dll
C:\Windows\system32\wkscli.dll
C:\Windows\system32\netutils.dll
C:\Windows\system32\srvcli.dll
C:\Windows\system32\NETAPI32.dll
C:\Windows\system32\WINSTA.dll
C:\Windows\system32\WTSAPI32.dll
C:\Windows\system32\WINSPOOL.DRV
C:\Windows\system32\SHELL32.dll
C:\Windows\system32\VERSION.dll
C:\Windows\system32\dxgi.dll
C:\Windows\system32\d3d11.dll
C:\Windows\system32\DCIMAN32.dll
C:\Windows\system32\API-MS-Win-Security-SDDL-L1-1-0.dll
C:\Windows\system32\ddraw.dll
C:\Windows\system32\Psapi.dll
C:\Windows\system32\d3d8thk.dll
C:\Windows\system32\WINMM.dll
C:\Windows\system32\d3d9.dll
C:\Windows\system32\Magnification.dll
C:\Windows\system32\WLDAP32.dll

C:\Windows\system32\SAMLIB.dll
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\CRYPTSP.dll
C:\Windows\system32\rsaenh.dll
C:\Windows\system32\bcrypt.dll
C:\Windows\system32\ncrypt.dll
C:\Windows\system32\bcryptprimitives.dll
C:\Windows\system32\GPAPI.dll
C:\Windows\system32\DNSAPI.dll
C:\Windows\system32\dhcpcsvc.DLL
C:\Windows\system32\COMRes.dll
C:\Windows\system32\CLBCatQ.DLL
C:\Windows\system32\wbem\wbemcomn.dll
C:\Windows\system32\wbem\wbemprox.dll
C:\Windows\system32\RpcRtRemote.dll
C:\Windows\system32\wbem\wbemsvc.dll
C:\Windows\system32\wbem\fastprox.dll
C:\Windows\system32\propsys.dll
C:\Windows\system32\NLAapi.dll
C:\Windows\system32\napinsp.dll
C:\Windows\system32\pnrpnsp.dll
C:\aeuoemres.dll
C:\aeuapploc.dll
CFGMGR32.dll
C:\Users\win7\AppData\Local\Temp\nsqA2B5.tmp\System.dll
C:\Windows\system32\DSOUND.dll
d3d9.dll
VBoxDisp.dll
MPR.DLL
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\ar-SA\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\cs-CZ\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\da-DK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\de-DE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\el-GR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\en-US\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\es-ES\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\fi-FI\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\fr-FR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\he-IL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\hu-HU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\it-IT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\ja-JP\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\ko-KR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\nb-NO\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\nl-NL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\pl-PL\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\pt-BR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\pt-PT\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\ru-RU\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\sk-SK\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\sv-SE\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\th-TH\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\tr-TR\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\zh-CN\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\zh-TW\IntelCommon.dll
C:\Users\win7\AppData\Local\Temp\IIF36B8.tmp\en-US\resource.dll.mui
MSFTEDIT.dll
comdlg32.dll
iphlpapi.dll
wsock32.dll
ws2_32.dll
Kernel32
ComCtl32
oleaut32.dll
0x99b1b9b3.d
C:\Windows\system32\wbem\xml\wmi2xml.dll
C:\Users\win7\AppData\Local\Temp\nskED3B.tmp\System.dll
crypt32.dll
winspool.drv
utildll.dll
atwtusb.exe
C:\msvcr120.dll
C:\msvcp120.dll
C:\Users\win7\AppData\Local\Temp\is-A0B76.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-A0B76.tmp\sample.EN
Iphlpapi.dll
IEFRAME.dll

C:\Users\win7\AppData\Local\Temp\nslE126.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-8MRIA.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-8MRIA.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\nsf1EB6.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsf1EB6.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsf1EB6.tmp\inetc.dll
psapi.dll
Riched20.dll
C:\Windows\SysWOW64\msls31.dll
C:\Users\win7\AppData\Local\Temp\nsp41BB.tmp\LangDLL.dll
api-ms-win-core-synch-l1-2-0
api-ms-win-core-fibers-l1-1-1
api-ms-win-core-localization-l1-2-1
SHFolder.dll
RICHED32.DLL
mscorsec.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
ncrypt.dll
bcrypt.dll
C:\Users\win7\AppData\Local\Temp\nse8AE9.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsc43D9.tmp\System.dll
POWRPROF.dll
OLE32.DLL
security.dll
NETAPI32.DLL
api-ms-win-appmodel-runtime-l1-1-1
ext-ms-win-kernel32-package-current-l1-1-0
C:\Users\win7\AppData\Local\Temp\nsuC41D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsuC41D.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsuC41D.tmp\fpinstall.dll
WDO19VM.DLL
SYNSOACC.DLL
traynet.dll
uexper.dll
Winspool.drv
DbgHelp.dll
C:\STRING\CNCLID32.dll
C:\STRING\CNCLID.dll
C:\STRING\CNMNPRCENU.DLL
C:\Windows\system32\cabinet.dll
dhcpcsvc.DLL
secur32.dll
cryptnet.dll
C:\Windows\system32\cryptnet.dll
profapi.dll
SensApi.dll
WINHTTP.dll
NSI.dll
C:\Users\win7\AppData\Local\Temp\is-D7QSN.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-D7QSN.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-3V0GP.tmp_isetup_shfoldr.dll
C:\Windows\system32\shlwapi.dll
MSFTEDIT.DLL
C:\Windows\system32\odbcint.dll
MSVCRT.DLL
C:\Windows\system32\wer.dll
C:\Windows\syswow64\KERNELBASE.dll
werui.dll
DUI70.dll
DUser.dll
C:\Windows\system32\DUser.dll
C:\Windows\system32\RICHED20.DLL
C:\Windows\system32\xmllite.dll
C:\Users\win7\AppData\Local\Temp/PPx6GHMbyIW6TqOsGH9/yZvWSsXxcDUukLwXNnrSdEbC90vWFf90iJ.dll
atiadlxy.dll
IMM32.DLL
C:\Windows\system32\CRTDLL.DLL
C:\Users\win7\AppData\Local\Temp\nsi5A21.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsi5A21.tmp\CityHash.dll
OLEACC.dll
C:\Users\win7\AppData\Local\Temp\nssEC0A.tmp\System.dll
C:\Windows\system32\VB6ES.DLL
C:\Windows\system32\asycfilt.dll
C:\Windows\system32\UXTHEME.dll
C:\Windows\system32\SHFOLDER.dll
C:\Windows\system32\RichEd20.dll

C:\Users\win7\AppData\Local\Temp\nssDDB.tmp\NSISArray.dll
C:\Users\win7\AppData\Local\Temp\nsjD6E6.tmp\System.dll
C:\Windows\system32\sfc.dll
C:\Users\win7\AppData\Local\Temp_ir_sf_temp_0\irsetup.exe
0x85d54008.d
ssutil.dll
WinSpool.drv
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\DUser.dll
DDraw.dll
D3DXOF.DLL
MSACM32.dll
OLEPRO32.DLL
WSOCK32.dll
C:\Users\win7\AppData\Local\Temp\nsr90F5.tmp\System.dll
C:\Program Files\Internet Explorer\IEXPLORE.EXE
C:\Users\win7\AppData\Local\Temp\nsnBB31.tmp\System.dll
C:\Windows\system32\dsound.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\System32\wininit.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\SearchIndexer.exe
C:\Windows\explorer.exe
C:\Windows\servicing\TrustedInstaller.exe
C:\Windows\System32\cmd.exe
C:\Python27\python.exe
C:\Windows\System32\rundll32.exe
C:\Windows\System32\powercfg.exe
C:\CFVS_Injector.exe
wtsapi32.dll
PowrProf.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\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\wsock32.dll
C:\Windows\System32\winmm.dll

C:\Windows\System32\dsound.dll
C:\Windows\System32\powrprof.dll
C:\Windows\SysWOW64\setupapi.dll
C:\Windows\SysWOW64\cfgmgr32.dll
C:\Windows\SysWOW64\devobj.dll
C:\Windows\System32\msacm32.dll
C:\Windows\System32\imm32.dll
C:\Windows\SysWOW64\msctf.dll
C:\Windows\SysWOW64\psapi.dll
C:\Windows\SysWOW64\imagehlp.dll
C:\Windows\System32\uxtheme.dll
C:\Windows\System32\dwmapi.dll
C:\Windows\System32\wtsapi32.dll
C:\Windows\System32\winsta.dll
WS2_32.DLL
Fwpuclnt.dll
C:\Users\win7\AppData\Local\Temp\nsc9F1D.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsc9F1D.tmp\UAC.dll
AdvAPI32
C:\Users\win7\AppData\Local\Temp\nsc9F1D.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nspE9BC.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nspE9BC.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nspE9BC.tmp\InstallOptions.dll
C:\SiteRankTray.exe
C:\SiteRank.dll
C:\Windows\syswow64\ntdll.dll
C:\Windows\syswow64\oleaut32.dll
C:\Windows\syswow64\gdi32.dll
C:\Windows\syswow64\advapi32.dll
C:\Windows\syswow64\ole32.dll
C:\Windows\syswow64\user32.dll
API-MS-Win-Core-RtlSupport-L1-1-0.dll
KERNELBASE.dll
API-MS-Win-Core-Heap-L1-1-0.dll
API-MS-Win-Core-Memory-L1-1-0.dll
API-MS-Win-Core-Handle-L1-1-0.dll
API-MS-Win-Core-Synch-L1-1-0.dll
API-MS-Win-Core-File-L1-1-0.dll
API-MS-Win-Core-IO-L1-1-0.dll
API-MS-Win-Core-ThreadPool-L1-1-0.dll
API-MS-Win-Core-LibraryLoader-L1-1-0.dll
API-MS-Win-Core-NamedPipe-L1-1-0.dll
API-MS-Win-Core-Misc-L1-1-0.dll
API-MS-Win-Core-SysInfo-L1-1-0.dll
API-MS-Win-Core-Localization-L1-1-0.dll
API-MS-Win-Core-ProcessEnvironment-L1-1-0.dll
API-MS-Win-Core-String-L1-1-0.dll
API-MS-Win-Core-Debug-L1-1-0.dll
API-MS-Win-Core-ErrorHandling-L1-1-0.dll
API-MS-Win-Core-Fibers-L1-1-0.dll
API-MS-Win-Core-Util-L1-1-0.dll
API-MS-Win-Core-Profile-L1-1-0.dll
API-MS-Win-Security-Base-L1-1-0.dll
API-MS-WIN-Service-Core-L1-1-0.dll
API-MS-WIN-Service-winsvc-L1-1-0.dll
API-MS-WIN-Service-Management-L1-1-0.dll
API-MS-WIN-Service-Management-L2-1-0.dll
kernelbase
sechost
ddraw.dll
dsound.dll
j2k-codec.dll
d3d8.dll
D3DIM700.DLL
C:\Users\win7\AppData\Local\Temp\nsm3BE4.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsu2A83.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsu2A83.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsu2A83.tmp\InstallOptions.dll
C:\Users\win7\AppData\Local\Temp\nsy9CD9.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsy9CD9.tmp\nsExec.dll
Msi.DLL
C:\Users\win7\AppData\Local\Temp\nsp6863.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsp6863.tmp\System.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
MMDevAPI.DLL
wdmaud.drv

MMDEVAPI.DLL
AUDIOSES.DLL
msacm32.drv
midimap.dll
POWRPROF.DLL
C:\Users\win7\AppData\Local\Temp\nskE891.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp/5qmb0FgAmfleSkUZaWJ\lua51.dll
C:\Users\win7\AppData\Local\Temp/5qmb0FgAmfleSkUZaWJ\1qJNbpG1t.dll
C:\Users\win7\AppData\Local\Temp/5qmb0FgAmfleSkUZaWJ\2u5xs0DCeN.dll
C:\Users\win7\AppData\Local\Temp/5qmb0FgAmfleSkUZaWJ/yZvWSsXxcDUukLwXNnrSdEbC90vWFf90iJ.dll
BASSMOD.dll
C:\Users\win7\AppData\Local\Temp\nsm3A1A.tmp\System.dll
uxtheme
C:\Users\win7\AppData\Local\Temp\GLCD2C.tmp
C:\Users\win7\AppData\Local\Temp\GLK1125.tmp
C:\Users\win7\AppData\Local\Temp\GLF24FD.tmp
SHELL32.DLL
COMCTL32.DLL
Msi.dll
shlwapi
C:\Users\win7\AppData\Local\Temp\0342c8f4.a
C:\Users\win7\AppData\Local\Temp\0342cfea.a
MmEngineDemo.DLL
522418
52243c
C:\Windows\system32\UxTheme.dll
C:\Users\win7\AppData\Local\Temp\GLC30CB.tmp
C:\Users\win7\AppData\Local\Temp\GLK3197.tmp
C:\Users\win7\AppData\Local\Temp\is-BEUVM.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-BEUVM.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-O9VA4.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsg9E47.tmp\System.dll
ntshrui.dll
C:\Users\win7\AppData\Local\Temp\nsj50A8.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsj50A8.tmp\inetc.dll
C:\Users\win7\AppData\Local\Temp\GUM79FA.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUM79FA.tmp\goopdateres_en.dll
netprofm.dll
DnsApi.dll
C:\Users\win7\AppData\Local\Temp\is-NGOU1.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-NGOU1.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-KI0T7.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-KI0T7.tmp\isxdl.dll
C:\Windows\system32\ieframe.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
AdvApi32.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorjit.dll
Setupapi.dll
C:\Users\win7\AppData\Local\Temp\is-BLKSB.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-BLKSB.tmp\sample.EN
api-ms-win-downlevel-shell32-l1-1-0.dll
shell32
ole32
USER32
oleacc.dll
wnaspi32.dll
C:\Windows\system32\winmm.dll
C:\Users\win7\AppData\Local\Temp\is-JBL19.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-JBL19.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\isSlideShow.dll
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\isSlideShow.ENU
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\isSlideShow.EN
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\CallbackCtrl.dll
C:\Windows\system32\version.dll
C:\Windows\system32\atl.dll
C:\Windows\system32\powrprof.dll
C:\Windows\system32\mscms.dll
C:\Windows\system32\userenv.dll
C:\Windows\system32\oleaccrc.dll
C:\Windows\system32\dbghelp.dll
C:\Windows\system32\msasn1.dll
C:\Windows\system32\crypt32.dll
C:\Windows\system32\psapi.dll
C:\Windows\system32\advapi32.dll
C:\Windows\system32\secur32.dll
C:\Windows\system32\pcacli.dll

C:\Windows\system32\devrtl.dll
C:\Windows\system32\Shell32.dll
C:\Users\win7\AppData\Local\Temp\{D81394AB-559D-4D05-BE1C-BBED9A9D0C97}\fpb.tmp
C:\Users\win7\AppData\Local\Temp\{6CC302DE-FDAE-40C5-907B-E24CEE1B4958}\fpb.tmp
C:\Windows\system32\Advapi32.dll
C:\Windows\system32\Msimg32.dll
atl.dll
FVEAPI.DLL
FaultRep.dll
C:\Windows\system32\DbgHelp.dll
tlhelp32.dll
rasapi32.dll
D3DREF9.DLL
wiatrace.dll
C:\Users\win7\AppData\Local\Temp\{BD3A9454-2A70-4D21-B383-641915030880}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{BD3A9454-2A70-4D21-B383-641915030880}\Disk1\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{D611D17F-FF28-41FC-8F6E-534C674676D3}\{E8AEA11B-E60A-455E-B008-E4E763604612}\ISRT.dll
C:\Users\win7\AppData\Local\Temp\{D611D17F-FF28-41FC-8F6E-534C674676D3}\{E8AEA11B-E60A-455E-B008-E4E763604612}_isres.dll
C:\Windows\system32\AppHelp.dll
C:\Users\win7\AppData\Local\Temp\{BD3A9454-2A70-4D21-B383-641915030880}\Disk1\data1.hdr
C:\Users\win7\AppData\Local\Temp\nshB109.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsxE300.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsxE300.tmp\nsExec.dll
Engine.dll
wer.dll
C:\Users\win7\AppData\Local\Temp\HTM779E.tmp
Msimg32.dll
C:\Users\win7\AppData\Local\Temp\Opera_installer_2016425531106.dll
C:\Users\win7\AppData\Local\Temp\is-TRNN4.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-TRNN4.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-RBVSQ.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-LQPK7.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-LQPK7.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-5CF2U.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-5CF2U.tmp\ISLogo.dll
User32.dll
C:\Users\win7\AppData\Local\Temp\is-5CF2U.tmp\ISMD5.dll
C:\Users\win7\AppData\Local\Temp\is-5CF2U.tmp\ISDone.dll
C:\bin\launcher.dll
C:\Users\win7\AppData\Local\Temp\is-SSGD0.tmp_isetup_shfoldr.dll
Cabinet.dll
C:\Windows\system32\msi.dll
C:\Users\win7\AppData\Local\Temp\GUME7E1.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\GUME7E1.tmp\goopdateres_en.dll
C:\Users\win7\AppData\Local\Temp\mia6311.tmp\Reaktor Prism Setup PC.ENU
C:\Users\win7\AppData\Local\Temp\mia6311.tmp\Reaktor Prism Setup PC.EN
Shlwapi.dll
C:\Users\win7\AppData\Local\Temp\mia6311.tmp\mia.lib
DWMAPI.DLL
C:\Users\win7\AppData\Local\Temp\is-LKMQS.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-875J3.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-875J3.tmp\isxdl.dll
SetupAPI.dll
Netapi32.dll
C:\Users\win7\AppData\Local\Temp\is-N75M2.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-N75M2.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-N75M2.tmp\itdownload.ENU
C:\Users\win7\AppData\Local\Temp\is-N75M2.tmp\itdownload.EN
C:\Users\win7\AppData\Local\Temp\genteert.dll
C:\Users\win7\AppData\Local\Temp\genteeA0\guig.dll
Oleaut32.dll
Ole32.dll
mpr.dll
C:\Users\win7\AppData\Local\Temp\is-QKNK7.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-QKNK7.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-QJJK4.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-ERM79.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-ERM79.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-7GSFN.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\nsu93B1.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nsu93B1.tmp\System.dll
C:\WBDIB44I.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:\Users\win7\AppData\Local\Temp\nskDCBF.tmp\nsDialogs.dll
C:\Users\win7\AppData\Local\Temp\nskDCBF.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\is-3996Q.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-3996Q.tmp\sample.EN
RASMONTR.DLL
C:\Windows\SysWOW64\odbcint.dll
NSHWFP.DLL
DHCPCMONITOR.DLL
Dhcpcsvc.dll
Dhcpqec.dll
WSHELPER.DLL
Advapi32
C:\Users\win7\AppData\Local\Temp\nsyC67.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsyC67.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nsyC67.tmp\nsDialogs.dll
C:\HidChk.exe
appwiz.cpl
atl
C:\Users\win7\AppData\Local\Temp\nszFC7B.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\nszFC7B.tmp\LangDLL.dll
VBoxHook.dll
C:\Users\win7\AppData\Local\Temp\nsp96AD.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsyF66B.tmp\CityHash.dll
C:\Users\win7\AppData\Local\Temp\is-8CP62.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-8CP62.tmp\sample.EN
C:\Windows\system32\KERNEL32.DLL
C:\Windows\system32\wintab32.dll
C:\Windows\system32\user32.dll
C:\Windows\system32\gdi32.dll
C:\Users\win7\AppData\Local\Temp\apm873A.tmp
C:\Users\win7\AppData\Local\Temp\is-4ERFC.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-4ERFC.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-LF7KV.tmp_isetup_shfoldr.dll
t r0
C:\Users\win7\AppData\Local\Temp\nsgC7FC.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsgC7FC.tmp\Fusion.dll
C:\Users\win7\AppData\Local\Temp\nsgC7FC.tmp\Fusion.ENU
C:\Users\win7\AppData\Local\Temp\nsgC7FC.tmp\Fusion.EN
UDLL.dll
LTTS1NDUT176.dll
NetApi32.dll
.\CustomRes.dll
BioOne.dll
SetupApi.dll
Gdi32.dll
GDIPlus.DLL
User32.DLL
C:\Users\win7\AppData\Local\Temp\nsgF0D.tmp\LangDLL.dll
C:\Users\win7\AppData\Local\Temp\nsgF0D.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsuD2B1.tmp\System.dll
BrLogAPI.dll
BrDbgOut.dll
BrDbgOtW.dll
NTDLL.DLL
D3D9.DLL
DXGI.DLL
C:\crashhandler.dll
C:\Users\win7\AppData\Local\Temp\nsv90DD.tmp\UserInfo.dll
C:\Users\win7\AppData\Local\Temp\nsv90DD.tmp\Banner.dll
powrprof.dll
PCMFSNWK.DLL
PCMFSSEL.DLL
C:\Users\win7\AppData\Local\Temp\nsb97EB.tmp\UserInfo.dll

C:\Users\win7\AppData\Local\Temp\nsb97EB.tmp\LangDLL.dll
CAPTLIB.DLL

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-51VNN.tmp\sample.tmp
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\sample
C:\Windows\system32\RICHED20.DLL
C:\Windows\system32\propsys.dll
C:\Windows\system32\ntshrui.dll
C:\Windows\System32\msxml3.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Users\win7\AppData\Local\Temp\~nsu.tmp\Au_.exe
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\syswow64\msvcrt.dll
C:\DLL_Loader.exe
C:\Users\win7\AppData\Local\Temp\Opera Installer\sample
C:\Windows\system32\Msftedit.dll
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\SYSTEM32\MSCOREE.DLL
C:\Windows\WinSxS\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\MSVCR80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\system32\RichEd20.dll
C:\Windows\system32\PROPSYS.dll
C:\Users\win7\AppData\Local\Temp\is-9CD24.tmp\sample.tmp
C:\Windows\system32\RICHED20.dll
C:\Users\win7\AppData\Local\Temp\is-P5OUG.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-KTJTQ.tmp\sample.tmp
C:\Program Files\Common Files\l
C:\Program Files\Common Files\logishrd\DriverStore\LDPInst.exe
C:\Windows\system32\RichEd20.DLL
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\uninst1.exe
C:\Users\win7\AppData\Local\Tem
C:\Users\win7\AppData\Local\Temp\is-IKAE7.tmp\sample.tmp
C:\Windows\system32\riched20.dll
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\SysWOW64\cmd.exe
C:\Windows\WinSxS\x86_microsoft.vc90.crt_1fc8b3b9a1e18e3b_9.0.30729.4940_none_50916076bcb9a742\MSVCR90.dll
C:\Users\win7\AppData\Local\Temp\{a1909659-0a08-4554-8af1-2175904903a1}\.ba1\wixstdba.dll
C:\Windows\system32\Riched20.dll
C:\Windows\system32\dxgi.dll
C:\Windows\system32\d3d11.dll
?:\sample
C:\Windows\system32\DSOUND.dll
C:\Windows\SysWOW64\Wbem\wmic.exe
C:\Users\win7\AppData\Local\Temp\is-A0B76.tmp\sample.tmp
C:\Windows\system32\IEFRAME.dll
C:\Users\win7\AppData\Local\Temp\is-8MRIA.tmp\sample.tmp
C:\Windows\system32\quartz.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Users\win7\AppData\Local\Temp\is-ODN6J.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-R9KUF.tmp\sample.tmp
C:\Windows\SysWOW64\schannel.dll
C:\Windows\system32\cryptnet.dll
C:\Users\win7\AppData\Local\Temp\is-D7QSN.tmp\sample.tmp
C:\Windows\system32\ODBC32.dll
C:\Windows\system32\DUser.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
C:\Users\win7\AppData\Local\Temp\PPx6GHMbyIW6TqOsGH9\yZvWSsXxcDUukLwXNnrSdEbC90vWFf90iJ.dll
C:\Windows\system32\aclui.dll
C:\Windows\system32\CRTDLL.DLL
C:\Windows\SysWOW64\DUser.dll
C:\Windows\SysWOW64\msiexec.exe
C:\Windows\system32\msi.dll
C:\Windows\system32\dsound.dll
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\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\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\wsock32.dll
C:\Windows\system32\winmm.dll
C:\Windows\system32\POWRPROF.dll
C:\Windows\syswow64\SETUPAPI.dll
C:\Windows\syswow64\CFGMGR32.dll
C:\Windows\syswow64\DEVOBJ.dll
C:\Windows\system32\msacm32.dll
C:\Windows\system32\IMM32.DLL
C:\Windows\syswow64\PSAPI.DLL
C:\Windows\syswow64\imagehlp.dll
C:\Windows\system32\uxtheme.dll
C:\Windows\system32\dwmapi.dll
C:\Windows\system32\wtsapi32.dll
C:\Windows\system32\WINSTA.dll
C:\Users\win7\AppData\Local\Temp\~apmiskfvjp.tmp
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\5qmb0FgAmfleSkUZaWJ\yZvWSsXxcDUukLwXNnrSdEbC90vWFf90iJ.dll
C:\Users\win7\AppData\Local\Temp\GLK1125.tmp
C:\Users\win7\AppData\Local\Temp\GLCD2C.tmp
C:\Users\win7\AppData\Local\Temp\GLB2E3B.tmp
C:\Users\win7\AppData\Local\Temp\GLK3197.tmp
C:\Users\win7\AppData\Local\Temp\is-BEUVM.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\GUM79FA.tmp\CatalinaUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUM79FA.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\is-NGOU1.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-TIP6R.tmp\sample.tmp
C:\Windows\system32\ieframe.dll
C:\Users\win7\AppData\Local\Temp\UfdApp\URescue.exe
C:\Windows\system32\WINMM.DLL
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\COMCTL32.DLL
C:\Windows\system32\WINSPOOL.DRV
C:\Windows\system32\olepro32.dll
C:\Windows\system32\POWRPROF.DLL
C:\Windows\system32\SHFOLDER.DLL
C:\Windows\system32\MSIMG32.DLL
C:\Windows\system32\WSOCK32.DLL
C:\Windows\syswow64\SHELL32.dll
C:\Windows\syswow64\COMDLG32.DLL
C:\Windows\syswow64\OLEAUT32.dll
&J
C:
C:\Users\win7\AppData\Local\Temp\is-BLKSB.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-M4DO4.tmp\isSlideShow.dll
C:\Users\win7\AppData\Local\Temp\is-JBL19.tmp\sample.tmp
C:\Windows\system32\DINPUT8.dll
C:\Windows\SysWOW64\control.exe
C:\Windows\system32\DbgHelp.dll
C:\Windows\system32\TAPI32.dll

C:\Windows\system32\ntmarta.dll
C:\Windows\system32\FaultRep.dll
C:\Windows\system32\SHFolder.dll
C:\Windows\syswow64\WLDAP32.dll
C:\Windows\SysWOW64\sti.dll
C:\Users\win7\AppData\Local\Temp\{BD3A9454-2A70-4D21-B383-641915030880}\Disk1\ISSetup.dll
C:\Users\win7\AppData\Local\Temp\{BD3A9454-2A70-4D21-B383-641915030880}_Setup.dll
C:\Users\win7\AppData\Local\Temp\{D611D17F-FF28-41FC-8F6E-534C674676D3}\{E8AEA11B-E60A-455E-B008-E4E763604612}\ISRT.dll
C:\Users\win7\AppData\Local\Temp\is-TRNN4.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-LQPK7.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-PKDCA.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-CMVG9.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\GUME7E1.tmp\DropboxUpdate.exe
C:\Users\win7\AppData\Local\Temp\GUME7E1.tmp\goopdate.dll
C:\Users\win7\AppData\Local\Temp\mia6311.tmp\Reaktor Prism Setup PC.exe
C:\Users\win7\AppData\Local\Temp\is-1V95D.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-E513B.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-N0KTI.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-N75M2.tmp\itdownload.dll
C:\Users\win7\AppData\Local\Temp\is-QKNK7.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-ERM79.tmp\sample.tmp
C:\WBDIB44I.DLL
C:\Users\win7\AppData\Local\Temp\is-3996Q.tmp\sample.tmp
C:\Windows\SysWOW64\ODBC32.dll
C:\Windows\system32\credui.dll
C:\Windows\SysWOW64\QUtil.dll
C:\Users\win7\AppData\Local\Temp\7zS3BB.tmp\setup-stub.exe
C:\Users\win7\AppData\Local\Temp\nszFC7B.tmp\UAC.dll
C:\Users\win7\AppData\Local\Temp\is-8CP62.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-4ERFC.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\nsgC7FC.tmp\Fusion.dll
C:\ProgramData\dfbnntj\mtefgbb.exe
C:\Windows\system32\DXGI.DLL
#31#
<NULL>
-42733731-
-6477424A-
-36464569-
-646344-
-1DCD4D1B-
-675946-
C:\Users\win7\AppData\Local\Temp\GUM24FA.tmp\DropboxUpdate.exe

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2016-04-04 12:05:56 UTC
Analysis End Date: 2016-04-04 12:52:21 UTC
File Upload Date: 2016-04-04 11:59:35 UTC
Human Expert Analyst Feedback: Cryptolocker
Verdict: Malware
Malware Family: TrojWare.Win32.Ransom.TeslaCrypt
Malware Type: Trojan Generic

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x57021E17 [Mon Apr 4 07:56:07 2016 UTC]
Entry Point	0x402fb0 (.text)
File Size	352256
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	© Microsoft Corporation. All rights reserved.
Internal Name	SmartcardCredentialProvider.dll
File Version	10.0.10240.16384 (th1.150709-1700)
Company Name	Microsoft Corporation
Product Name	Microsoft® Windows® Operating System
Product Version	10.0.10240.16384
File Description	Windows Smartcard Credential Provider
Original Filename	SmartcardCredentialProvider.dll
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	6
Sha256	d8ee200589d8e7d72878ea79bcfc9d18ee52569c046df74fa0dfe7e33d9ec422

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x269b0	0x27000	6.598351	-
~f6c:D	0x28000	0x6590	0x7000	7.529775[SUSPICIOUS]	-
.data	0x2f000	0x3168	0x2000	2.585114	-
.erloc	0x33000	0xf5a3	0x10000	7.795407[SUSPICIOUS]	-
B;z^#	0x43000	0x9387	0xa000	7.617466[SUSPICIOUS]	-
.rsrc	0x4d000	0x3db8b	0xb000	1.696757	-