VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: adobe.snr.patch-painter.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
SHA1: 1338776580ace190d83549bc2ccee4ac0986a7bd
MD5: c650582d891cfeb1f2f97b983f1f0a34
First Seen Date: 2015-08-29 08:15:55 UTC
Number of Clients Seen: 12
Last Analysis Date: 2016-04-09 21:19:03 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 21:19:03 UTC	Clean
Static Analysis Overall Verdict	2016-04-09 21:19:03 UTC	No Threat Found
Dynamic Analysis Overall Verdict	2016-04-09 21:19:03 UTC	No Threat Found
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	Suspicious
Timestamp value suspicious	Suspicious
Header Checksum is zero!	Suspicious
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious
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	Suspicious

Packer detection on signature database

UPX v0.89.6 - v1.02 / v1.05 -v1.22 (Delphi) stub

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

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

Behavioral Information

QueryFilePath

C:\DLL_Loader.exe
C:\sample
C:\Windows\system32\MSVBVM60.DLL
C:\Windows\SysWOW64\ieframe.dll
C:\Windows\system32\RICHED20.dll
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
C:\Windows\SysWOW64\rundll32.exe
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\system32\credui.dll
C:\Windows\system32\DUser.dll
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\PROPSYS.dll
C:\Windows\syswow64\shlwapi.DLL
C:\Users\win7\AppData\Local\Temp\is-GJT8A.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-SQ39R.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\vkg6DD4.tmp
C:\Windows\system32\RichEd20.dll
C:\Windows\syswow64\CRYPT32.dll
C:\Windows\system32\cryptnet.dll
C:\Windows\system32\ODBC32.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\BASS.dll
C:\Users\win7\AppData\Local\Tem
C:\Users\win7\AppData\Local\Temp\is-IVCQG.tmp\sample.tmp
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\JiXibX.exe
C:\Windows\syswow64\crypt32.DLL
C:\Users\win7\AppData\Local\Temp\Opera Installer\sample
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\SysWOW64\ntdll.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\system32\Msftedit.dll
C:\Windows\system32\quartz.dll
C:\Windows\SysWOW64\schannel.dll
C:\Windows\system32\WINMM.dll
C:\Windows\system32\RichEd20.DLL

ReadRegisteryKey

FrameTabWindow
FrameMerging
SessionMerging
AdminTabProcs
TabProcGrowth
DropLocation
Win31FileSystem
NoRun
NoDrives
RestrictRun
NoNetConnectDisconnect
NoRecentDocsHistory
NoClose

MachineID
InstallationID
Disable
DataFilePath
Plane1
Plane2
Plane3
Plane4
Plane5
Plane6
Plane7
Plane8
Plane9
Plane10
Plane11
Plane12
Plane13
Plane14
Plane15
Plane16
InstallRoot
CLRLoadLogDir
OnlyUseLatestCLR
GCStressStart
GCStressStartAtJit
DisableConfigCache
CacheLocation
DownloadCacheQuotaInKB
EnableLog
LoggingLevel
ForceLog
LogFailures
VersioningLog
LogResourceBinds
UseLegacyIdentityFormat
DisableMSIPeek
NoClientChecks
DevOverrideEnable
LatestIndex
NIUsageMask
ILUsageMask
DisplayName
ConfigMask
ConfigString
MVID
EvalationData
Status
ILDependencies
NIDependencies
MissingDependencies
Modules
SIG
LastModTime
mscorlib
Latest
index1
LegacyPolicyTimeStamp
System
System.Xml
System.Configuration
CreateUriCacheSize
EnablePunycode
DisableSecuritySettingsCheck
SystemSetupInProgress
SpecialFoldersCacheSize
MS Shell Dlg 2
ProgramFilesDir
CommonFilesDir
RegisteredOwner
RegisteredOrganization
GlobalFlags
Columns
Level
Flags
LogDir
LogFile
PINF
ProcessID

EnablePrivateObjectHeap
ContextLimit
ObjectLimit
IdentifierLimit
Default Impersonation Level
NoGuiFromShim
WaitToKillServiceTimeout
NavigationDelay
Default
UrlEncoding
SyncMode5
FEATURE_CLIENTAUTHCERTFILTER
FromCacheTimeout
SecureProtocols
DisableKeepAlive
IdnEnabled
PreConnectLimit
PreResolveLimit
SqmHttpStreamRandomUploadPoolSize
CacheMode
EnableHttp1_1
ProxyHttp1.1
EnableNegotiate
DisableBasicOverClearChannel
ClientAuthBuiltInUI
DisableReadRange
SocketSendBufferLength
SocketReceiveBufferLength
KeepAliveTimeout
MaxHttpRedirects
MaxConnectionsPerServer
MaxConnectionsPer1_0Server
MaxConnectionsPerProxy
ServerInfoTimeout
ConnectTimeOut
ConnectRetries
SendTimeOut
ReceiveTimeOut
DisableNTLMPreAuth
ScavengeCacheLowerBound
CertCacheNoValidate
ScavengeCacheFileLifeTime
ScavengeCacheFileLimit
HttpDefaultExpiryTimeSecs
FtpDefaultExpiryTimeSecs
LeashLegacyCookies
SendExtraCRLF
WpadSearchAllDomains
DontUseDNSLoadBalancing
ShareCredsWithWinHttp
DnsCacheEnabled
DnsCacheEntries
DnsCacheTimeout
WarnOnPost
WarnAlwaysOnPost
WarnOnZoneCrossing
WarnOnBadCertRecving
WarnOnPostRedirect
AlwaysDrainOnRedirect
WarnOnHTTPSToHTTPRedirect
TcpAutotuning
BadProxyExpiresTime
Version
AutoProxyDetectType
WpadOverride
DisableBranchCache
UseFirstAvailable
CombineFalseStartData
DisableFalseStartBlocklist
EnforceP3PValidity
DuoProtocols
EnableSpdyDebugAsserts
ProxyEnable
ProxyServer
ProxyOverride
AutoConfigURL
AutoDetect
SavedLegacySettings

DefaultConnectionSettings
WpadDecision
WpadDecisionTime
WpadExpirationDays
sample
TotalLimit
DomainLimit
RootDomainLimit
MaxSubDomains
No3DBorder
IsTextPlainHonored
ZoomDisabled
MinimumSystemTimerResolution
RenderingLoopMaxTime
RtfConverterFlags
Use_DlgBox_Colors
Anchor Underline
CSS_Compat
Expand Alt Text
Display Inline Images
Display Inline Videos
Play_Background_Sounds
Play_Animations
Print_Background
SmoothScroll
XMLHTTP
Show image placeholders
Disable Script Debugger
DisableScriptDebuggerIE
Disable Diagnostics Mode
Move System Caret
Enable AutoImageResize
UseHR
Q300829
Cleanup HTCs
XDomainRequest
DOMStorage
JScriptProfileCacheEventDelay
Default_CodePage
CacheOk
<NULL>
Compatible
Platform
Last Stable Install Path
Last install path
Seed
GlitchInstrumentation
TRACE_MISC
TRACE_CM
TRACE_TRACE
TRACE_SVC
TRACE_GATEWAY
TRACE_UI
TRACE_CONTACT
TRACE_UTIL
TRACE_CLUSTER
TRACE_RESOURCE
TRACE_TIP
TRACE_XA
TRACE_LOG
TRACE_MTXOCI
TRACE_ETWTRACE
TRACE_PROXY
TRACE_KTMRM
TRACE_VSSBACKUP
TRACE_PERFMON
TRACE_TM
TRACE_LU
TraceFilePath
MemoryBufferSize
DebugOutEnabled
UserContextLockCount
UserContextListCount
TrapPollTimeMilliSecs
SystemBiosVersion
SystemBiosDate
{K7C0DB872A3F777C0}
{0E88C97D553B71D8A}

TpfnnlLtzHwTu
{IE88C97D553B71D8A}

CreateFile

C:\Windows\system32\rsaenh.dll
C:\Users\win7\AppData\Local\Temp\\~DF585C4E53EF638765.TMP
C:\sample
1.217.949.0_TO_1.217.1005.0_MPASDLTA.VDM._P
1.217.949.0_TO_1.217.1005.0_MPAVDLTA.VDM._P
C:\Users\win7\AppData\Local\Temp\chrome_crashes\operation_log.txt
\\.\Nsi
C:\Windows\Fonts\staticcache.dat
C:\Users\win7\AppData\Local\Temp\swuD1E2.tmp
C:\sample.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.cch
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\win7\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index1c2.dat
C:\Windows\system32\l_intl.nls
C:\Windows\assembly\pubpol1.dat
C:\Users\win7\AppData\Local\Temp\DM\installer.exe
C:\Users\win7\AppData\Local\Temp\DM\installer.exe.config
C:\Users\win7\AppData\Local\Temp\DM\111.txt
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\win7\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x0000000000000007.db
C:\Users\win7\Desktop\desktop.ini
C:\
C:\Users\desktop.ini
C:\Users
C:\Users\win7
C:\Users\win7\Searches\desktop.ini
C:\Users\win7\Videos\desktop.ini
C:\Users\win7\Pictures\desktop.ini
C:\Users\win7\Contacts\desktop.ini
C:\Users\win7\Favorites\desktop.ini
C:\Users\win7\Music\desktop.ini
C:\Users\win7\Downloads\desktop.ini
C:\Users\win7\Documents\desktop.ini
C:\Users\win7\Links\desktop.ini
C:\Users\win7\Saved Games\desktop.ini
\??\C:\Windows\System32\shdocvw.dll
C:\Users\win7\AppData\Local\Temp\is-T8PRU.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-T8PRU.tmp_isetup_shfoldr.dll
C:\Windows\WindowsUpdate.log
C:\Windows
C:\Users\win7\AppData\Local\Temp\nsaC64B.tmp
C:\Users\win7\AppData\Local\Temp\pandoratv.ico
\\.\PIPE\srvsvc
C:\Users\win7\Desktop\\Pandora TV.lnk
\??\C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Temp\vkg6DD4.tmp
C:\Users\win7\AppData\Local\Temp\plg749C.tmp
C:\WINDOWS\UPDATE.EXE
C:\ProgramData\48ed1695-d484-472b-bd42-582714ef1368\temp
C:\Windows\system32\wbem\wbemdisp.TLB
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\7D266D9E1E69FA1EEFB9699B009B34C8_0A9BFDD75B598C2110CBF610C078E6E6
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7D266D9E1E69FA1EEFB9699B009B34C8_E9915110418DBDEA47BB3BFCDB24CFF1
C:\Users\win7\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\8DFDF057024880D7A081AFBF6D26B92F
C:\Users\win7\AppData\Local\Temp\7F4987FB1A6E43d69E3E94B29EB75926\downloader.log
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp_isetup_setup64.tmp
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\wintb.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Users\win7\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat
C:\Users\Public\Downloads\dm-AE39.tmp

1.213.5687.0_TO_1.213.5746.0_MPASDLTA.VDM._P
1.213.5687.0_TO_1.213.5746.0_MPAVDLTA.VDM._P
C:\Users\win7\AppData\Local\Temp\JiXibX.exe
C:\CFVS_Injector.exe
C:\DLL_Loader.exe
C:\Procmon.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxControl.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxDrvInst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxTray.exe
C:\Program Files\Oracle\VirtualBox Guest Additions\VBoxWHQLFake.exe
C:\Program Files\Windows Defender\MpCmdRun.exe
C:\Program Files\Windows Defender\MSASCui.exe
C:\Program Files\Windows Journal\Journal.exe
C:\Program Files\Windows Journal\PDIALOG.exe
C:\Program Files\Windows Mail\wab.exe
C:\Program Files\Windows Mail\wabmig.exe
C:\Program Files\Windows Mail\WinMail.exe
C:\Program Files\Windows Photo Viewer\ImagingDevices.exe
C:\Program Files\Windows Sidebar\sidebar.exe
C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe
C:\ProgramData\Package Cache\{f65db027-aff3-4070-886a-0d87064aabb1}\vcredist_x86.exe
C:\Users\win7\AppData\Local\Temp\7ZipSfx.000\KMSpico_v10.0.3_NT6_ssApp.exe
C:\Users\win7\AppData
C:\Users\win7\AppData\Local
C:\Users\win7\AppData\Local\Temp
C:\Users\win7\AppData\Local\Temp\7ZipSfx.000
C:\ProgramData\Tencent\QQPCMgr\QQMiniDown\sample_sample.log
C:\setup.ini
0x0000.ini
\\.\pipe\OperaCrashReporter2848
C:\installer_prefs.json
C:\Users\win7\AppData\Local\Temp\Opera Installer\opera_installer_20160409223352.log
\\.\C:
\\.\D:
C:\Users\win7\AppData\Local\Temp\Opera Installer\installer.lck
C:\Windows\system32\\\\wuapi.dll
config.wtf
WTF\config.wtf
Logs\cpu.log
.agent.db
C:/Users/win7/AppData/Local/MX Simulator/lastlog.txt
C:/Users/win7/AppData/Local/MX Simulator/zzzz.saf
C:/zzzz.saf
C:\Users\win7\AppData\Local\Temp\nsv906C.tmp\RegKern.dll
C:\Users\win7\AppData\Local\Temp\spltmp.bmp
C:\Users\win7\AppData\Local\Temp\nsv906C.tmp\AdvSplash.dll
C:\Users\win7\AppData\Local\Temp\spltmp.wav.WAV
C:\Users\win7\AppData\Local\Temp\nsu71E3.tmp
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\InstallOptions.ini
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\InstallOptions2.ini
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\System.dll
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\ioSpecial.ini
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\modern-wizard.bmp
C:\ProgramData\219d5106-5a99-41fd-b942-db6b503b0178\temp
C:\ArmA2OA.exe
C:\arma3.exe
C:\DayZ.exe
C:\H1Z1.exe
C:\ShooterGame.exe
__tmp_rar_sfx_access_check_54880687
ENG.bat
ENG.exe
hidcon.exe
\\.\PHYSICALDRIVE0
\\.\SCSI0:
C:\Users\win7\AppData\Local\Temp\F662888F.TMP
C:\Users\win7\AppData\Local\Temp\E88C97D553B71D8A.TMP
\\.\SIce
\\.\NTICE
\\.\SIWDEBUG
\\.\SIWVID
\??\C:\Windows\system32\EhStorShell.dll
\??\C:\Windows\system32\ntshrui.dll

OpenRegisteryKey

AppID
{e745ce26-593d-400b-a02e-f9bda91946f0}
Software\Microsoft\Internet Explorer\Main
Software\Policies\Microsoft\Internet Explorer\Main
SOFTWARE\Microsoft\MpSigStub
SYSTEM\CurrentControlSet\Control\FileSystem
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Software\Microsoft\Windows\CurrentVersion\Policies\Network
Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
Segoe UI
MS Shell Dlg 2
Microsoft Sans Serif
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\MyPC Backup
SOFTWARE\SlimWare Utilities
SOFTWARE\Slimware Utilities Inc\DriverUpdate
software\microsoft\office\14.0\common\filespaths
Software\Policies\Microsoft\Office\14.0
Software\Microsoft\Office\14.0
Software\Microsoft\Office\14.0\Common\Security
Software\Microsoft\Office\14.0\CVH\OverRide
SOFTWARE\Microsoft\Office Test\Special\Perf
Software\Microsoft\Office\14.0\Common\GOM
Software\Microsoft\Office\14.0\Common\GOM\ComplexRanges
Software\Microsoft\.NETFramework\Policy\
v2.0
Software\Microsoft\.NETFramework
Upgrades
Standards
AppPatch
Software\Microsoft\.NETFramework\Policy\Standards
v2.0.50727
Software\Microsoft\Fusion
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sample
Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets
Internet
LocalIntranet
Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3979321414-2393373014-2172761192-1000
Software\Microsoft\.NETFramework\v2.0.50727\Security\Policy
Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
index1c2
NI\181938c6\7950e2c5
NI\181938c6\7950e2c5\16
IL\7950e2c5\4b5f28af\5f
NI\731a1722\457d9522
Software\Microsoft\StrongName
Software\Microsoft\Fusion\PublisherPolicy\Default
policy.2.0.System__b77a5c561934e089
NI\30bc7c4f\3f50fe4f
NI\30bc7c4f\3f50fe4f\18
IL\424bd4d8\324708cb\5c
IL\19ab8d57\c91dbb2\5e
IL\3f50fe4f\265c633d\60
policy.2.0.System.Xml__b77a5c561934e089
policy.2.0.System.Configuration__b03f5f7f11d50a3a
SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
SOFTWARE\Microsoft\NET Framework Setup\NDP\v2.0.50727
Software\Microsoft\Windows\CurrentVersion\Explorer\KindMap
Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
Software\Microsoft\Internet Explorer\Main\FeatureControl
FEATURE_IGNORE_POLICIES_ZONEMAP_IF_ESC_ENABLED_KB918915
FEATURE_ZONES_CHECK_ZONEMAP_POLICY_KB941001
Software\Policies
Software
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
FEATURE_INITIALIZE_URLACTION_SHELLEXECUTE_TO_ALLOW_KB936610
Software\Microsoft\Windows\CurrentVersion\Internet Settings
FEATURE_ALLOW_REVERSE_SOLIDUS_IN_USERINFO_KB932562
Software\Policies\Microsoft\Internet Explorer
Microsoft\Internet Explorer\Security
System\Setup

Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\
FEATURE_LOCALMACHINE_LOCKDOWN
FEATURE_ZONES_DEFAULT_DRIVE_INTRANET_KB941000
FEATURE_PROTOCOL_LOCKDOWN
Software\JavaSoft\Java Runtime Environment
Software\CodeGear\Locales
Software\Borland\Locales
Software\Borland\Delphi\Locales
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
System\CurrentControlSet\Control\Keyboard Layouts\041F0409
System\CurrentControlSet\Control\Keyboard Layouts\04090409
Tahoma
Software\Microsoft\Windows\CurrentVersion\Uninstall\{9733673D-2535-9987-8AD1-EB059FC793F9}_is1
Software\Microsoft\Windows\CurrentVersion
SOFTWARE\Microsoft\Windows NT\CurrentVersion
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Misc
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Report
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Setup
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Service
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Agent
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\AU
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\AUClnt
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\CltUI
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\CPL
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\WUApp
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\WUWeb
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\DtaStor
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\CDM
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\PT
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Driver
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\COMAPI
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Parser
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Handler
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\EEHndlr
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\DnldMgr
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Cmpress
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Shutdwn
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\WuRedir
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\OfflSnc
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Inv
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\ARP
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Trace
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\TraceTestMain
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\TraceTestThreads
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace\Perf
Software\Microsoft\Windows\CurrentVersion\Explorer
SYSTEM\CurrentControlSet\Services\Abcdef Hijklmno Qrs
Software\Microsoft\WBEM\CIMOM
SOFTWARE\Classes\CLSID\{F83D1872-D9FF-47F8-B5A0-49CC51E24EE8}
SOFTWARE\MiddleRush
Software\Embarcadero\Locales
Verdana
Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice
shell\open\command
Software\Microsoft\Wbem\Scripting
Software\Microsoft\Cryptography\Wintrust\Config
SOFTWARE\Microsoft\OLEAUT
Software\Microsoft\Windows\CurrentVersion\Setup
system\CurrentControlSet\control\NetworkProvider\HwOrder
SOFTWARE\Microsoft\CTF\Compatibility\sample
Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
SOFTWARE\Microsoft\CTF\TIP\
{0000897b-83df-4b96-be07-0fb58b01c4a4}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{03B5835F-F03C-411B-9CE2-AA23E1171E36}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{07EB03D6-B001-41DF-9192-BF9B841EE71F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{3697C5FA-60DD-4B56-92D4-74A569205C16}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{531FDEBF-9B4C-4A43-A2AA-960E8FCDC732}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{78CB5B0E-26ED-4FCC-854C-77E8F3D1AA80}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{8613E14C-D0C0-4161-AC0F-1DD2563286BC}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{A028AE76-01B1-46C2-99C4-ACD9858AE02F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{AE6BE008-07FB-400D-8BEB-337A64F7051F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{C1EE01F2-B3B6-4A6A-9DDD-E988C088EC82}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{DCBD6FA8-032F-11D3-B5B1-00C04FC324A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{E429B25A-E5D3-4D1F-9BE3-0C608477E3A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
{F89E9E58-BD2F-4008-9AC2-0F816C09F4EE}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}

Keyboard Layout\Toggle
Software\Microsoft\CTF\DirectSwitchHotkeys
SOFTWARE\Microsoft\CTF\
SOFTWARE\Microsoft\CTF\KnownClasses
System
MS Sans Serif
Software\Microsoft\CTF\LayoutIcon\0409\0000041f
v4.0.30319
Software\Microsoft\.NETFramework\Policy\Upgrades
SOFTWARE\Microsoft\BidInterface\Loader
SOFTWARE\ODBC\ODBC.INI\ODBC
System\CurrentControlSet\Control
Software\Microsoft\RestartManager
Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete
Shell.Explorer
CLSID
Software\Microsoft\COM3
CLSID\{8856F961-340A-11D0-A96B-00C04FD705A2}
InprocServer32
Software\Microsoft\OLE
TreatAs
SOFTWARE\Microsoft\Internet Explorer\MAIN
SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\sample
CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\InProcServer32
Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Blocked
CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}
SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{871C5380-42A0-1069-A2EA-08002B30309D}
FEATURE_IEDDE_REGISTER_PROTOCOL
PROTOCOLS\Name-Space Handler\
PROTOCOLS\Name-Space Handler\about\
PROTOCOLS\Name-Space Handler*\
SOFTWARE\Classes\PROTOCOLS\Handler\about
CLSID\{3050F406-98B5-11CF-BB82-00AA00BDCE0B}
Arial
SYSTEM\ControlSet001\Control\Nls\Language
Software\1stbrowser
Software\Microsoft\Internet Explorer\MediaTypeClass
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Accepted Documents
FEATURE_BROWSER_COMPATDATA
FEATURE_BROWSER_EMULATION
FEATURE_SHOW_FAILED_CONNECT_CONTENT_KB942615
Microsoft\Windows\CurrentVersion\Internet Settings
FEATURE_DISABLE_INTERNAL_SECURITY_MANAGER
Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
RETRY_HEADERONLYPOST_ONCONNECTIONRESET
FEATURE_MIME_HANDLING
FEATURE_BYPASS_CACHE_FOR_CREDPOLICY_KB936611
FEATURE_IGNORE_MAPPINGS_FOR_CREDPOLICY
FEATURE_INCLUDE_PORT_IN_SPN_KB908209
FEATURE_BUFFERBREAKING_818408
FEATURE_SKIP_POST_RETRY_ON_INTERNETWRITEFILE_KB895954
FEATURE_FIX_CHUNKED_PROXY_SCRIPT_DOWNLOAD_KB843289
FEATURE_USE_CNAME_FOR_SPN_KB911149
FEATURE_PERMIT_CACHE_FOR_AUTHENTICATED_FTP_KB910274
FEATURE_DISABLE_UNICODE_HANDLE_CLOSING_CALLBACK
FEATURE_DISALLOW_NULL_IN_RESPONSE_HEADERS
FEATURE_DIGEST_NO_EXTRAS_IN_URI
FEATURE_ENABLE_PASSPORT_SESSION_STORE_KB948608
FEATURE_EXCLUDE_INVALID_CLIENT_CERT_KB929477
FEATURE_USE_UTF8_FOR_BASIC_AUTH_KB967545
FEATURE_RETURN_FAILED_CONNECT_CONTENT_KB942615
FEATURE_PRESERVE_SPACES_IN_FILENAMES_KB952730
FEATURE_ENABLE_PROXY_CACHE_REFRESH_KB2983228
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
FEATURE_DISABLE_NOTIFY_UNVERIFIED_SPN_KB2385266
FEATURE_COMPAT_USE_CONNECTION_BASED_NEGOTIATE_AUTH_KB2151543
FEATURE_SCH_SEND_AUX_RECORD_KB_2618444
Software\Microsoft\Internet Explorer
Software\Trymedia Systems\Download Manager\9b0c486f6c9699b762dce9d2f7a58b94
Software\Microsoft\Windows\CurrentVersion\Run
Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad

Software\Policies\Microsoft\PeerDist\Service
Software\Microsoft\Windows NT\CurrentVersion\PeerDist\Service
{69DC4768-446B-4F82-A6B0-63966A243064}
Content
Cookies
History
FEATURE_GPU_RENDERING
FEATURE_CSS_DATA_RESPECTS_XSS_ZONE_SETTING_KB912120
FEATURE_ARIA_SUPPORT
FEATURE_LEGACY_DISPPARAMS
FEATURE_PRIVATE_FONT_SETTING
FEATURE_CSS_SHOW_HIDE_EVENTS
FEATURE_DISPLAY_NODE_ADVISE_KB833311
FEATURE_ALLOW_EXPANDURI_BYPASS
FEATURE_BODY_SIZE_IN_EDITABLE_IFRAME_KB943245
FEATURE_DATABINDING_SUPPORT
FEATURE_ENFORCE_BSTR
FEATURE_ENABLE_DYNAMIC_OBJECT_CACHING
FEATURE_OBJECT_CACHING
FEATURE_LEGACY_TOSTRING_IN_COMPATVIEW
FEATURE_RESTRICT_CRASH_RECOVERY_SAVE_KB978454
FEATURE_DOWNLOAD_INITIATOR_HTTP_HEADER
FEATURE_MOBILE_CUSTOMIZATIONS
FEATURE_HIGH_RESOLUTION_AWARE
FEATURE_FORCE_DISABLE_UNTRUSTEDPROTOCOL
FEATURE_USE_WEBOC_OMNAVIGATOR_IMPLEMENTATION
FEATURE_USE_SECURITY_THUNKS
FEATURE_DISABLE_DEFERRED_IMAGE_DOWNLOAD
FEATURE_LAZY_IMAGE_DECODING
FEATURE_LAZIER_IMAGE_DECODING
FEATURE_ALLOW_INTRANET_CSS_MIME_MISMATCH
FEATURE_ENABLE_CLIPCHILDREN_OPTIMIZATION
FEATURE_ENABLE_LARGER_HIT_TEST
FEATURE_USE_LEGACY_JSCRIPT
FEATURE_MOBILE_VIEWPORT_WIDTH_RESTRICTIONS
FEATURE_PASTE_IMAGE_DATAURI
FEATURE_NEW_TREE_VERIFICATION
FEATURE_MOBILE_DISPOSABLE_RESOURCE_CACHE_THRESHOLD_BYTES
FEATURE_DOCUMENT_COMPATIBLE_MODE
FEATURE_ENABLE_WEB_CONTROL_VISUALS
FEATURE_XDOMAINREQUEST
FEATURE_WEBSOCKET
FEATURE_USE_UNISCRIBE
FEATURE_PAINT_INSIDE_WMPAINT
FEATURE_SOFTWARE_FILTER_RENDERING
FEATURE_SPELLCHECKING
FEATURE_FORCE_NATURAL_TEXT_METRICS
FEATURE_ENABLE_PERFWIDGET_EXTRA_INFO
FEATURE_DISABLE_FORMAT_REUSE
FEATURE_ALLOW_WINDOW_PUTNAME_CROSS_DOMAIN
FEATURE_REDUCE_RENDER_AHEAD_CACHE
FEATURE_CLEANUP_AT_FLS
Software\Microsoft\Windows\CurrentVersion\App Paths\OUTLOOK.EXE
Software\Microsoft\Internet Explorer\Application Compatibility
Software\Policies\Microsoft\Internet Explorer\DOMStorage
Software\Microsoft\Internet Explorer\DOMStorage
FEATURE_MEMPROTECT_MODE
FEATURE_OLEALIAS_GWND
FEATURE_TOPMOST_GWND
FEATURE_RESTRICT_ABOUT_PROTOCOL_IE7
SOFTWARE\Classes\PROTOCOLS\Filter\text/html
FEATURE_MIME_SNIFFING
FEATURE_FEEDS
FEATURE_ENABLE_COMPAT_LOGGING
MIME\Database\Content Type\text/html
FEATURE_MANAGE_SCRIPT_CIRCULAR_REFS
Security\Floppy Access
Security\Adv AddrBar Spoof Detection
Software\Policies\Microsoft\Internet Explorer\Zoom
Zoom
FEATURE_WEBOC_DOCUMENT_ZOOM
FEATURE_NINPUT_LEGACYMODE
FEATURE_ALIGNED_TIMERS
FEATURE_VSYNC_WATCHDOG
FEATURE_ALLOW_HIGHFREQ_TIMERS
Main
FEATURE_SAFE_BINDTOOBJECT
International

PROTOCOLS\Name-Space Handler\http\
SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\User Agent
Microsoft\Windows\CurrentVersion\Internet Settings\User Agent
Pre Platform
Post Platform
FEATURE_MAXCONNECTIONSPERSERVER
FEATURE_MAXCONNECTIONSPER1_0SERVER
FEATURE_URLMON_IQDA_SIZE
Software\Tencent\TrojanScanLog
ISlogit
Software\Policies\Microsoft\Windows\Installer
CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
{babe9b11-0f98-11e5-b301-806e6f6e6963}\
Drive\shellex\FolderExtensions
Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
Software\Policies\Microsoft\Windows\Explorer
<NULL>
Advanced
Software\Microsoft\Windows\Shell\RegisteredApplications\UrlAssociations\Directory\OpenWithProgids
Software\Microsoft\Windows\Shell\Associations\UrlAssociations\Directory
Software\Microsoft\Rpc
Software\Policies\Microsoft\Windows NT\Rpc
Directory
CurVer
ShellEx\IconHandler
Folder
AllFilesystemObjects
DocObject
BrowseInPlace
Clsid
Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
PropertyBag
SessionInfo\1
KnownFolders
Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
CLSID\{1F486A52-3CB1-48FD-8F50-B8DC300D9F9D}
{babe9b14-0f98-11e5-b301-806e6f6e6963}\
{babe9b10-0f98-11e5-b301-806e6f6e6963}\
System\CurrentControlSet\Services\LDAP
{1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE}
{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
{5E6C858F-0E22-4760-9AFE-EA3317B67173}
Software\Opera Software
SOFTWARE\Microsoft\DirectX
SOFTWARE\Debug\quartz.dll
Software\Microsoft\Multimedia\ActiveMovie Filters\MPEG Decoder
Software\Microsoft\MSDTC\Tracing
Sources
Output
{906d7e81-6355-4069-b02d-bcfdfe2885e7}
{ab25d3c2-9787-4788-99a1-32a4c1208c11}
Software\Blizzard Entertainment\Internal
Software\Microsoft\Windows\CurrentVersion\Uninstall\DriveClone
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Everything
Folder\shell\Search Everything...\command
ES\shell\open\command
MS Shell Dlg
SOFTWARE\SearchWebKnow
Software\Licenses
Hardware\Description\System
CLSID\{5B884F9A-DE5D-70D0-5386-EC6B30C6FB46}
{031E4825-7B94-4dc3-B131-E946B44C8DD5}
DefaultIcon
InProcServer32
shell
restorelibraries
command
ShellFolder
Software\The Silicon Realms Toolworks\Armadillo
{17CCA71B-ECD7-11D0-B908-00A0C9223196}
{19603261-6059-43DF-B9E1-8B4352825A90}
{1c1800c1-3258-44c2-be80-3deadb6c5e39}
{00A77FF7-A514-493e-B721-CDF8CB0F5B59}

CreateMutex

<NULL>
Global\C:/Users/win7/AppData/Local/Temp/chrome_crashes/operation_log.txt
{042B0D65-EF5B-4E3F-ADFF-86C726E4F053}
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Global\WindowsUpdateTracingMutex
C:\sample
Global\MiddleRush
wewetwtwtwertyeryturtuui9909896
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
WSjuQKBxmd_mut
Global\1stBRRunningMutex
Holly - A Christmas Tale Deluxe
Local\Opera/Installer/UI_lock
AMResourceMutex3
Global\SearchWebKnow
RAL1A9D71D9
1A9D71D9::WK

LoadLibrary

C:\sample
C:\Windows\system32\uxtheme.dll
OLEAUT32.DLL
SXS.DLL
ADVAPI32.dll
CRYPTBASE.dll
dwmapi.dll
kernel32.dll
comctl32.dll
riched32.dll
riched20.dll
C:\Windows\system32\kernel32.dll
SHELL32.dll
OLEACCRC.DLL
C:\Windows\WinSxS\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.18834_none_72d38c5186679d48\gdiplus.dll
RICHED20.DLL
C:\sampleENU.dll
C:\sampleLOC.dll
SHLWAPI.dll
IPHLPAPI.DLL
ntdll.dll
winhttp.dll
WS2_32.dll
SspiCli.dll
OLEAUT32.dll
RPCRT4.dll
ole32.dll
NSI.dll
CFGMGR32.dll
dhcpcsvc.DLL
DNSAPI.dll
C:\Windows\system32\ole32.dll
C:\Windows\syswow64\MSCTF.dll
UxTheme.dll
comctl32
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
API-MS-Win-Core-LocalRegistry-L1-1-0.dll
Comctl32.dll
imageres.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
mscoree.dll
ntdll
advapi32.dll

shell32.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\38bf604432e1a30c954b2ee40d6a2d1c\mscorlib.ni.dll
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
propsys.dll
ntmarta.dll
C:\Windows\System32\shdocvw.dll
PROPSYS.dll
Secur32.dll
API-MS-WIN-DOWNLEVEL-SHLWAPI-L1-1-0.DLL
api-ms-win-downlevel-advapi32-l2-1-0.dll
DUser.dll
C:\Windows\system32\DUser.dll
user32.dll
C:\Windows\system32\xmllite.dll
C:\Users\win7\AppData\Local\Temp\is-SQ39R.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-SQ39R.tmp\sample.EN
imm32.dll
uxtheme.dll
C:\Users\win7\AppData\Local\Temp\is-T8PRU.tmp_isetup_shfoldr.dll
shfolder.dll
Rstrtmgr.dll
SHFOLDER
USER32.dll
ntshrui.dll
srvcli.dll
cscapi.dll
slc.dll
C:\Windows\SysWOW64\ieframe.dll
netutils.dll
Rpcns4.dll
Kernel32.dll
C:\Users\win7\AppData\Local\Temp\vkg6DD4.tmp
KERNEL32.DLL
ADVAPI32.DLL
COMCTL32.DLL
GDI32.DLL
MPR.DLL
OLE32.DLL
USER32.DLL
WSOCK32.DLL
C:\Users\win7\AppData\Local\Temp\vkg6DD4.ENU
C:\Users\win7\AppData\Local\Temp\vkg6DD4.EN
KERNEL32.dll
MSVCRT.dll
WININET.dll
MSVCP60.dll
API-MS-Win-Security-LSALookup-L1-1-0.dll
CRYPTSP.dll
PSAPI.DLL
VDMDBG.DLL
netapi32.dll
winspool.drv
winmm.dll
Msctf.dll
wtsapi32.dll
WINSTA.dll
security.dll
WS2_32.DLL
Fwpuclnt.dll
IdnDL.dll
Normaliz.dll
iphlpapi.dll
DWMAPI.DLL
C:\Windows\system32\advapi32.dll
API-MS-Win-Security-SDDL-L1-1-0.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsec.dll
RichEd20.dll
mscorsec.dll
WINTRUST.DLL
C:\Windows\syswow64\CRYPT32.dll
imagehlp.dll
ncrypt.dll
C:\Windows\SysWOW64\bcryptprimitives.dll
bcrypt.dll
USERENV.dll

cryptnet.dll
C:\Windows\system32\cryptnet.dll
profapi.dll
SensApi.dll
WINHTTP.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
user32
C:\Users\win7\AppData\Local\Temp\pdl9717.tmp
C:\Windows\system32\odbcint.dll
MSVCRT.DLL
C:\Users\win7\AppData\Local\Temp\is-IVCQG.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-IVCQG.tmp\sample.EN
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp_isetup_shfoldr.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\VclStylesInno.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\ISDone.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\BASS.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\bp.dll
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\bp.ENU
C:\Users\win7\AppData\Local\Temp\is-577GU.tmp\bp.EN
shlwapi.dll
COMDLG32.DLL
SHELL32.DLL
IMM32.dll
api-ms-win-downlevel-shlwapi-l2-1-0.dll
urlmon.dll
api-ms-win-downlevel-ole32-l1-1-0.dll
DbgHelp.dll
api-ms-win-core-sysinfo-l1-2-1
atlthunk.dll
GDI32.dll
WSOCK32.dll
C:\sa.dll
C:\Windows\system32\ws2_32
uxtheme
comdlg32.dll
gdi32.dll
C:\QQPCDetector.dll
crypt32
wininet
shell32
C:\Windows\syswow64\crypt32.DLL
msi.dll
COMCTL32.dll
CRYPT32.dll
gdiplus.dll
MSIMG32.dll
WINMM.dll
WINTRUST.dll
Advapi32.dll
Msftedit.dll
wininet.dll
dbghelp.dll
secur32.dll
C:\Users\win7\AppData\Local\Temp\nsv906C.tmp\AdvSplash.dll
C:\Windows\system32\WINMM.dll
C:\Users\win7\AppData\Local\Temp\nsj71F3.tmp\System.dll
RichEd20
C:\Windows\system32\shell32.dll
NTDLL
mshtml.dll
d3dxof.dll
COMDLG32.dll
SETUPAPI.dll
ws2_32.dll
inetmib1.dll
snmpapi.dll
rpcrt4.dll
oleaut32.dll
version.dll
olepro32.dll
msimg32.dll
User32
WindowsCodecs.dll
C:\Windows\system32\EhStorShell.dll
C:\Windows\system32\ntshrui.dll
c:\windows\system32\imageres.dll

UXTHEME

QueryProcessAddress

SetWindowsHookExA
CreateProcessA
CreateServiceA
SetWindowsHookExW
OpenProcess
InternetReadFile
ShellExecuteExW
ShellExecuteW
IsDebuggerPresent
URLDownloadToFileA
WinExec
ShellExecuteA
ShellExecuteExA
Toolhelp32ReadProcessMemory
QueueUserAPC
ReadProcessMemory
CreateProcessW
GetThreadContext

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	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
Entry Point	0x56ffb0 (UPX1)
File Size	549888
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	PainteR
Internal Name	Universal Adobe Patcher
File Version	1.1.0.0
Company Name	PainteR
Product Name	Universal Adobe Patcher
Product Version	1.1.0.0
File Description	Universal Adobe Patcher
Original Filename	adobesnr.exe
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	3
Sha256	e22f28fec16b9eb0a6f6ec9357e7dad8ac8c31f5a106dad2663b1e0bc0100c5e

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\Users\umut.yayla\Desktop\After\After\Crack\Setup.exe	9
C:\Users\cahide.toraman\AppData\Local\Temp\Rar$EXa0.915\Universal Adobe Patcher 1.1\adobe.snr.patch-painter.exe	9
D:\DOSYALARIM\9.dönem\9.dönem klasörü\Masaüstüm12aralık\Masaüstü 2\Yeni klasör (2)\adobe_universal_patcher_cc_2014\Crack\Adobe Universal Patcher 2014.exe	9
D:\Personal\Programas Adobe\Adobe Muse CC 2014\2. or Patch Painter 1.1\adobe.snr.patch-painter.exe	9
C:\Users\chaminda.JOLANKA\Downloads\Adobe Photoshop CC 2014.2.2 20141204.r.310.x64\PhotoShopCC1522Win64\Crack\adobe.snr.patch-painter\adobe.snr.patch-painter.exe	9
aktivasyon.exe	9
C:\Users\atilla.tombuloglu\AppData\Local\Temp\Rar$EXa0.963\Universal Adobe Patcher 1.1\adobe.snr.patch-painter.exe	9
C:\Users\Shan\AppData\Local\Temp\Temp1_Adobe patcher.zip\Adobe patcher\adobe.snr.patch-painter (1).exe	9
C:\Users\Shan\Desktop\Crack\Adobe Universal Patcher 2014.exe	9

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0xf0000	0x0	0.000000[SUSPICIOUS]	-
UPX1	0xf1000	0x80000	0x7f200	7.931612[SUSPICIOUS]	-
.rsrc	0x171000	0x7000	0x6e00	5.483272	-