VALKYRIE COMODO

Summary

File Name: 900f83e9f1dd818f4c1006ae6b0c6c518d6bc943376140fc2be3c99f1d8ffa9f.ex

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

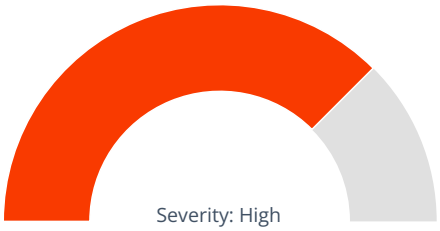
SHA1: 855fa325ab3aa9499ec8260a8172c2f75b5854d7

MD5: 1fc01f0b85c82b69c5e04b55bb8a07ee

MALWARE

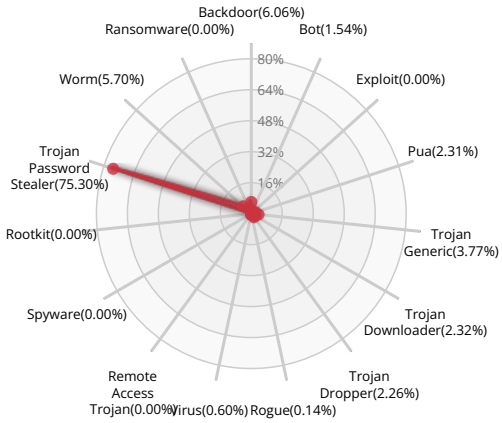
Valkyrie Final Verdict

DETECTION SECTION

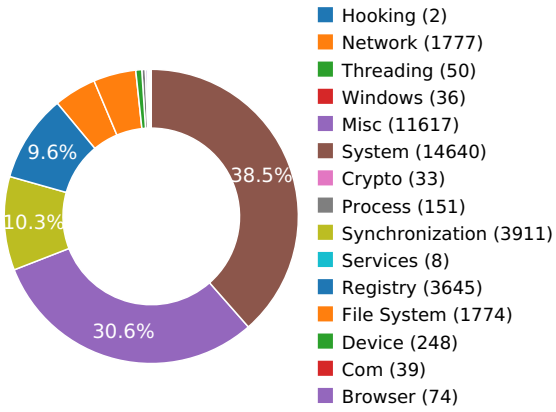


Verdict: Malware

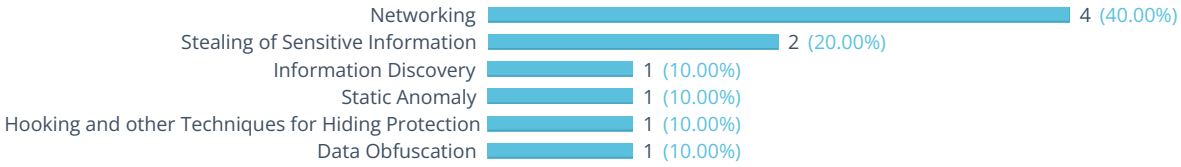
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (8 unique times)	Show sources
Performs some HTTP requests	Show sources
Network activity contains more than one unique useragent.	Show sources
A process sent information about the computer to a remote location.	Show sources

STEALING OF SENSITIVE INFORMATION

Sniffs keystrokes	Show sources
Attempts to modify proxy settings	

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

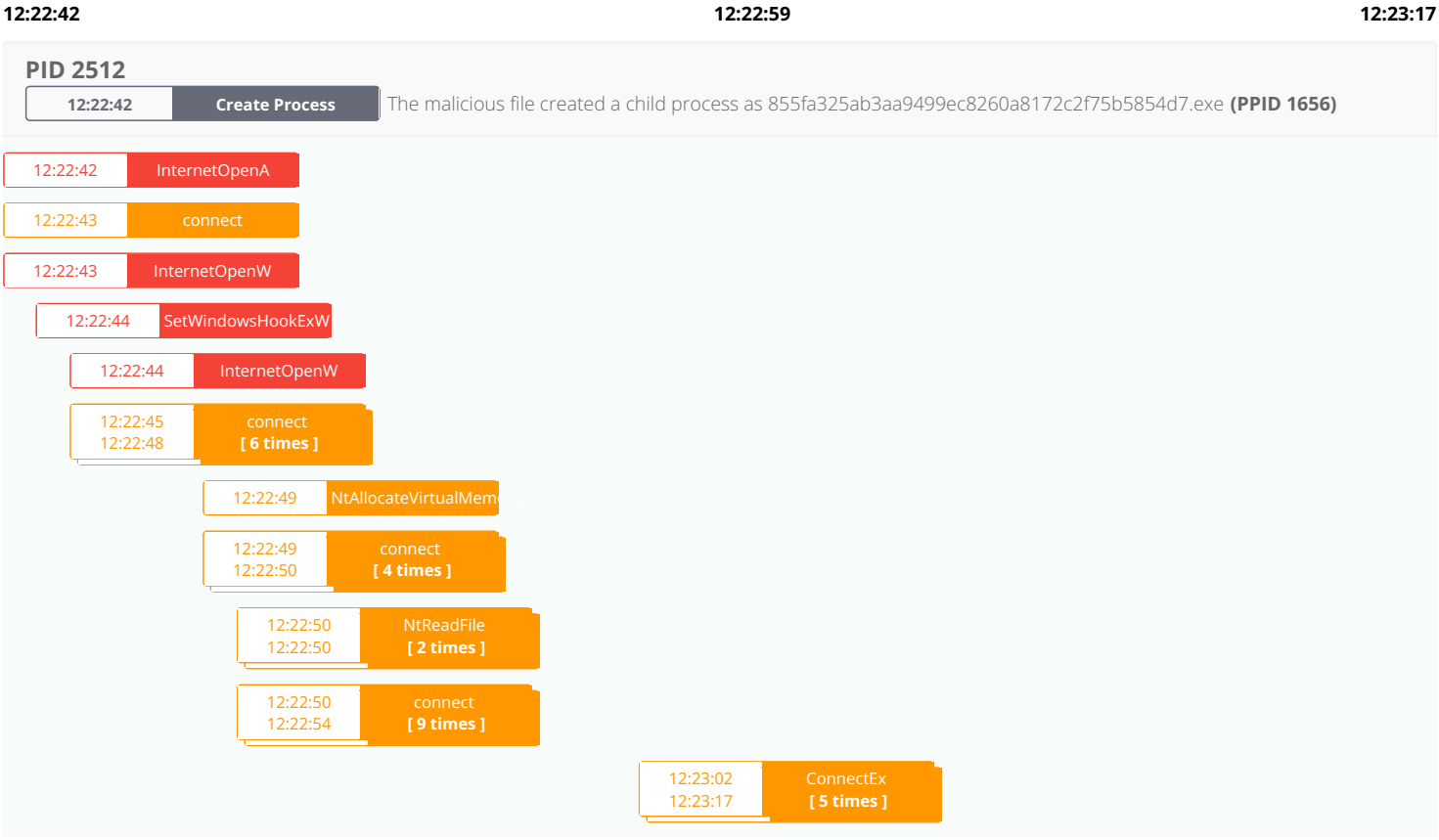
Creates RWX memory	Show sources

DATA OBFUSCATION

Unconventionial binary language: Chinese (Simplified)

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\ProgramData\4399\GameLogin\Statistic.ini
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.Config
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.1000.Manifest
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7ENU.dll
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7LOC.dll
C:\Windows\SysWOW64\wininet.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies
C:\Users\user\AppData\Local\Microsoft\Windows\History
C:\Users\user\AppData\Local\Microsoft\Windows\History\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Temp\dnsapi.DLL
C:\Windows\System32\dnsapi.dll
C:\ProgramData\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\ProgramData\Microsoft\Network\Connections\Pbk*.pbk
C:\Windows\System32\ras*.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk
C:\Users\user\AppData\Roaming\Microsoft\Network\Connections\Pbk*.pbk

C:\Windows\System32\tzres.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\shell32.dll
\??\PhysicalDrive0
C:\Users\user\AppData\Local\Temp\Statistic.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\reg[1].html
C:\Windows\WindowsShell.manifest
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\core[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\effectTj[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\theme[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\bb[1].jpg
C:\
C:\Windows\SysWOW64\Macromed\Flash\ss.sgn
C:\Windows\SysWOW64\Macromed\Flash\ss.cfg
C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
C:\Windows\SysWOW64\oem.cfg
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache
C:\Users\user\AppData\Local\Temp\
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Roaming\Adobe\FLASH PLAYER\NATIVECACHE\
C:\Users\user\AppData\Roaming\Adobe\FLASH PLAYER\
C:\Users\user\AppData\Roaming\Adobe\
C:\Users\user\AppData\Roaming\
C:\Users\user\AppData\
C:\Users\user\
C:\Users\
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Adobe
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\NativeCache.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\94D901CE4AD8BABEF1A9F51A72BF8CE8.directory

C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\D19A124A63BC3E484EE0CC12F63FFE86\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\14FE212574D1C626E7D9F8D9E261A62B\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\58D75590E211D1B0C26C176059D52D75\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\DE89D1447AB1E99DD87F51CA87C52655\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\9DCB33E1CFD76DD078ED1898ECBAEFEE\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\668D0A067F2436E1D58EA37A2D7DAF2E\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\396B667C011CF74AFE66D655E875014B\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\7FCDFC8C65295F95F1B2B94C4B4AC6BF\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\BF4BB2C7EE96F73EC15D03471A3C7190\Info.directory

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE*
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\FromCacheTimeout
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CertificateRevocation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableKeepAlive
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisablePassport
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\IdnEnabled
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CacheMode
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableNegotiate
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableBasicOverClearChannel

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\Feature_ClientAuthCertFilter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ClientAuthBuiltInUI
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SyncMode5
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\SessionStartTimeDefaultDeltaSecs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Signature
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\iecompat\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\iecompat\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\iecompat\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\iecompat\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\iecompat\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld\CachePrefix

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\ietld\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012016042520160426\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012016042520160426\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012016042520160426\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012016042520160426\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012016042520160426\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\PrivacIE:\CacheOptions
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableAutoProxyResultCache
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\DisplayScriptDownloadFailureUI
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\MBCSServername
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\MBCSAPIforCrack
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\UTF8ServerNameRes
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableWorkerThreadHibernation

MODIFIED FILES

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\ProgramData\4399\GameLogin\Statistic.ini
\??\PhysicalDrive0
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\reg[1].html
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\core[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\effectTj[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\theme[1].css
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\bb[1].jpg
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\NativeCache.directory
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\config[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\web_referer[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\util[1].png

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\action[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\bg1[1].png
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\video[1].swf
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\autologin[1].js
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@4399[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@4399[2].txt
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\a[1].php
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\client_old_reg[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\sound[1].swf
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\util[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\easydialog.min[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\txlink[1].gif
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\get_login[1].php
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\get_login[1].php
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_28699ABAC9273C08DCF1E93A8F6BFD1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_28699ABAC9273C08DCF1E93A8F6BFD1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B08578675F0562C4A68283513357EA41
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B08578675F0562C4A68283513357EA41

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.CreateActCtxW
kernel32.dll.ReleaseActCtx
kernel32.dll.ActivateActCtx
kernel32.dll.DeactivateActCtx
user32.dll.NotifyWinEvent
kernel32.dll.GetUserDefaultUILanguage
kernel32.dll.GetSystemDefaultUILanguage
normaliz.dll.IdnToAscii

advapi32.dll.EventActivityIdControl
advapi32.dll.EventWriteTransfer
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.AcquireSRWLockShared
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.ReleaseSRWLockShared
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.SetFileInformationByHandle
shell32.dll.SHGetFolderPathW
kernel32.dll.GetModuleHandleW
advapi32.dll.AddMandatoryAce
ntmarta.dll.GetMartaExtensionInterface
ws2_32.dll.accept
ws2_32.dll.bind
ws2_32.dll.closesocket
ws2_32.dll.connect
ws2_32.dll.getpeername
ws2_32.dll.getsockname
ws2_32.dll.getsockopt
ws2_32.dll.ntohl
ws2_32.dll.htonl
ws2_32.dll.htons
ws2_32.dll.inet_addr
ws2_32.dll.inet_ntoa
ws2_32.dll.ioctlsocket
ws2_32.dll.listen
ws2_32.dll.ntohs
ws2_32.dll.recv
ws2_32.dll.recvfrom
ws2_32.dll.select
ws2_32.dll.send
ws2_32.dll.sendto
ws2_32.dll.setsockopt

ws2_32.dll.shutdown
ws2_32.dll.socket
ws2_32.dll.gethostbyname
ws2_32.dll.gethostname
ws2_32.dll.WSAIoctl
ws2_32.dll.WSAGetLastError
ws2_32.dll.WSASetLastError
ws2_32.dll.WSAStartup
ws2_32.dll.WSACleanup
ws2_32.dll.__WSAFDIsSet
ws2_32.dll.getaddrinfo
ws2_32.dll.freeaddrinfo
ws2_32.dll.getnameinfo
ws2_32.dll.WSALookupServiceBeginW
ws2_32.dll.WSALookupServiceNextW
ws2_32.dll.WSALookupServiceEnd
ws2_32.dll.WSANSPIoctl
ws2_32.dll.WSAStringToAddressA
ws2_32.dll.WSAStringToAddressW
ws2_32.dll.WSAAddressToStringA
dnsapi.dll.DnsGetProxyInformation
dnsapi.dll.DnsFreeProxyName
iphlpapi.dll.GetIpForwardTable2
iphlpapi.dll.FreeMibTable
iphlpapi.dll.GetIfEntry2
iphlpapi.dll.ConvertInterfaceGuidToLuid
iphlpapi.dll.ResolveIpNetEntry2
iphlpapi.dll.GetIpNetEntry2

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@4399[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@4399[2].txt

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Network
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FeatureControl
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE*
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\FromCacheTimeout
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SecureProtocols
HKEY_LOCAL_MACHINE\Software\Policies
HKEY_CURRENT_USER\Software\Policies
HKEY_CURRENT_USER\Software
HKEY_LOCAL_MACHINE\Software
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CertificateRevocation

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableKeepAlive
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisablePassport
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\IdnEnabled
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\CacheMode
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableHttp1_1
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyHttp1.1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\EnableNegotiate
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\DisableBasicOverClearChannel
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\Feature_ClientAuthCertFilter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ClientAuthBuiltInUI
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\SyncMode5
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\SessionStartTimeDefaultDeltaSecs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Signature
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\PerUserItem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\PerUserItem
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\DOMStore\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\feedplat

READ FILES

C:\ProgramData\4399\GameLogin\Statistic.ini
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.3.Manifest
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.Config
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe
C:\Users\user\AppData\Local\Temp\855fa325ab3aa9499ec8260a8172c2f75b5854d7.exe.1000.Manifest
C:\Windows\SysWOW64\wininet.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Windows\System32\dnsapi.dll
C:\Windows\System32\tzres.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\shell32.dll
\??\PhysicalDrive0
C:\Users\user\AppData\Local\Temp\Statistic.ini
C:\Windows\WindowsShell.manifest
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\reg[1].html
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\effectTj[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\core[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\theme[1].css

C:\Windows\SysWOW64\Macromed\Flash\mms.cfg
C:\Windows\SysWOW64\Macromed\Flash\oem.cfg
C:\Windows\SysWOW64\oem.cfg
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\94D901CE4AD8BABEF1A9F51A72BF8CE8.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\NativeCache.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\D19A124A63BC3E484EE0CC12F63FFE86\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\14FE212574D1C626E7D9F8D9E261A62B\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\58D75590E211D1B0C26C176059D52D75\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\DE89D1447AB1E99DD87F51CA87C52655\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\9DCB33E1CFD76DD078ED1898ECBAEFEE\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\668D0A067F2436E1D58EA37A2D7DAF2E\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\396B667C011CF74AFE66D655E875014B\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\7FCDFC8C65295F95F1B2B94C4B4AC6BF\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\BF4BB2C7EE96F73EC15D03471A3C7190\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\24FB7F8BF29F9D5B1BA5F5BD986D6BDB\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\27B164FB036E31553875E83C0CEADD7C\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\E5617A3A2E52B334393316C9AF28E65D\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\74C6CC968D46AD77ED26CD2279AFAD4A\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\5E1695CF661F2AC6997BB8E3D81DF826\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\53C2449AF5289A3021851A926C9292AE\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\2B9A81C6A66630E584CDC25504552597\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\46ED9160074E9FE80B68B8F4635E1E1F\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\7624407C79FD148BD154961B5C878D06\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\52A424DE7FAAAC541C1DDDCE9E5AB317\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\915E84FE7E8929AA0AF1E491D8AA8669\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\A0B83912A1953D21B712724637B8789A\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\824E0FF07F7744CEBFDAF4FF92BE9E8F\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\63241689DE8DD5590FBBFA84AD7D116C\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\5F01BA1496F8B8F767931AACBF93267B\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\340EE80BB6C2BDC03A237663EA24C806\Info.directory
C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\B8A777454276EE030F7A5FF3F6E693DC\Info.directory
C:\Users\user\.telemetry.cfg
C:\Users\user\telemetry.cfg
C:\Windows\SysWOW64\Macromed\Flash\activex.vch
C:\Windows\SysWOW64\Macromed\Flash\Flash32_20_0_0_286.ocx

C:\Windows\SysWOW64\stdole2.tlb
C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
C:\Windows\System32\en-US\MLANG.dll.mui
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\config[1].js
C:\Windows\win.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\jquery[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\web_referer[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\action[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\video[1].swf
C:\Windows\System32\en-US\MMDevApi.dll.mui
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\autologin[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\client_old_reg[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\sound[1].swf
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\util[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\easydialog.min[1].js
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\get_login[1].php
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\get_login[1].php
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4

MUTEXES

Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!
Local\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
IESQMMUTEX_0_208
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
DBWinMutex
{1B655094-FE2A-433c-A877-FF9793445069}
Local__DDrawExclMode__
Local__DDrawCheckExclMode__

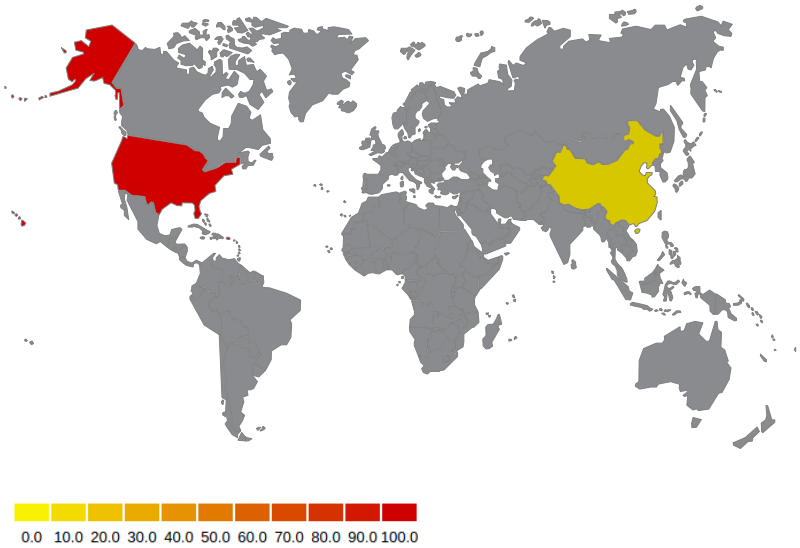
Local\DDrawWindowListMutex
Local\DDrawDriverObjectListMutex

MODIFIED REGISTRY KEYS

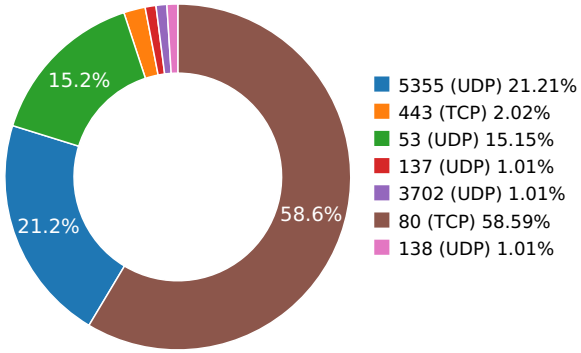
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\EnableConsoleTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\855fa325ab3aa9499ec8260a8172c2f75b5854d7_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\CacheLimit
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{D27CDB6E-AE6D-11CF-96B8-444553540000}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{D27CDB6E-AE6D-11CF-96B8-444553540000}\VerCache
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DirectDraw\MostRecentApplication\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\DirectDraw\MostRecentApplication\ID

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	119.147.163.227	China	58466	CHINANET Guangdong provi...	Malware Process
	121.201.47.218	China	58543	Guangdong Ruijiang Science ...	Malware Process
	151.101.2.133	United States	54113	Fastly	Malware Process
	23.215.131.200	United States	20940	Akamai Technologies, Inc.	OS Process
web.4399.com	157.185.170.133	United States	54994	QUANTIL NETWORKS INC	Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	Not known	Malware Process
record.4399.com	121.14.36.75	China	58466	beijingshichaoyangqujiuxianq...	Malware Process
ocsp2.digicert.com	72.21.91.29	United States	15133	MCI Communications Service...	Malware Process
ctldl.windowsupdate.com	23.215.131.176	United States	20940	Akamai Technologies, Inc.	OS Process
client.5054399.com	219.129.239.26	China	58543	CHINANET Guangdong provi...	Malware Process
crl.globalsign.net	151.101.22.133	United States	54113	Fastly	Malware Process
pic.my4399.com	157.185.170.133	United States	54994	QUANTIL NETWORKS INC	Malware Process
webpic.my4399.com	157.185.158.198	United States	54994	QUANTIL NETWORKS INC	Malware Process
www.baidu.com	104.193.88.123	United States	55967	Baidu USA LLC	Malware Process
txt.unionli.com	121.201.47.33	China	4134	Guangdong Ruijiang Science ...	Malware Process
crl.microsoft.com	23.215.131.195	United States	20940	Akamai Technologies, Inc.	OS Process
b.533y.com	121.201.47.33	China	4134	Guangdong Ruijiang Science ...	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
b.533y.com	80	GET	1.1	LHL	1	6.83801794052
Path: /_regevent.gif? event=100&ename=%E6%89%93%E5%BC%80&type=0&game=z&oid=16311&oid1=16311&oid2=&cid=39531&aid=70236&lc=0&userSession=08:00:27:CB:30:5F&ne tat=0&referer=http%3A%2F%2Fweb%2E4399%2Ecom%2Fz%2Fclients%2Fzt%5Fsmba%5Fzddl%2Freg%2Ehtml%3Fagid%3D22100%26cid%3D39531%26aid%3D702 36%26oid%3D16311%26oid2%3D%26vcode%3Dcafes%26dirtype%3D0%26pt%3D0 **URI:** http://b.533y.com/_regevent.gif? event=100&ename=%E6%89%93%E5%BC%80&type=0&game=z&oid=16311&oid1=16311&oid2=&cid=39531&aid=70236&lc=0&userSession=08:00:27:CB:30:5F&ne tat=0&referer=http%3A%2F%2Fweb%2E4399%2Ecom%2Fz%2Fclients%2Fzt%5Fsmba%5Fzddl%2Freg%2Ehtml%3Fagid%3D22100%26cid%3D39531%26aid%3D702 36%26oid%3D16311%26oid2%3D%26vcode%3Dcafes%26dirtype%3D0%26pt%3D0						
client.5054399.com	80	GET	1.1	LHL	1	7.09769892693
Path: /active.htm?tag=Z70236&ver=3.0.0.1&count=1&apartdays=0&keepdays=1&weekdays=1 **URI:** http://client.5054399.com/active.htm?tag=Z70236&ver=3.0.0.1&count=1&apartdays=0&keepdays=1&weekdays=1						
web.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	8.37236595154
Path: /z/clients/zt_smba_zddl/reg.html? oid=16311&oid2=&vcode=cafes&dirtype=0&pt=0agid=22100&cid=39531&aid=70236&game=z&did=p6p2h462q385g714h378u343m392e371a392y35yl315n378l378 71d7d7x7xxf336i7i7r679c868v336s385c392x462g49gg462b49bw49wk336f336n336q371d336u378x378w35w&vid=54cdc5495f19770b35ee4c1659ab7891&mac=08 27:CB:30:5F&toAd=1&autorun=0 **URI:** http://web.4399.com/z/clients/zt_smba_zddl/reg.html? oid=16311&oid2=&vcode=cafes&dirtype=0&pt=0agid=22100&cid=39531&aid=70236&game=z&did=p6p2h462q385g714h378u343m392e371a392y35yl315n378l378 71d7d7x7xxf336i7i7r679c868v336s385c392x462g49gg462b49bw49wk336f336n336q371d336u378x378w35w&vid=54cdc5495f19770b35ee4c1659ab7891&mac=08 27:CB:30:5F&toAd=1&autorun=0						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	10.3062129021
Path: /re/cms/z/clients/zt_smba_zddl/css/theme.css **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/css/theme.css						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	10.4032828808
Path: /js/core.js **URI:** http://pic.my4399.com/js/core.js						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	10.4037778378
Path: /re/cms/feUtil/effectTj/1.1/effectTj.js **URI:** http://pic.my4399.com/re/cms/feUtil/effectTj/1.1/effectTj.js						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	11.4716930389
Path: /re/cms/z/clients/zt_smba_zddl/css/bb.jpg **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/css/bb.jpg						
web.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	11.5671229362
Path: /util/get_login.php?&jsoncallback=jsonp_04269758833383082 **URI:** http://web.4399.com/util/get_login.php?&jsoncallback=jsonp_04269758833383082						
web.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	12.3291628361
Path: /util/?_c=code&t=reg **URI:** http://web.4399.com/util/?_c=code&t=reg						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	12.526859045
Path: /re/cms/z/clients/zt_smba_zddl/css/video.swf **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/css/video.swf						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	12.531208992
Path: /re/cms/z/clients/zt_smba_zddl/css/bg1.png **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/css/bg1.png						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	12.8538439274

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /re/cms/web/js/config.js **URI:** http://pic.my4399.com/re/cms/web/js/config.js						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	13.1176228523
Path: /re/cms/web/js/lib/jquery.js?v1.7.2 **URI:** http://pic.my4399.com/re/cms/web/js/lib/jquery.js?v1.7.2						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	13.1291379929
Path: /re/cms/web/js/web_referer.js **URI:** http://pic.my4399.com/re/cms/web/js/web_referer.js						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	13.2312538624
Path: /re/cms/web/js/user/action.js **URI:** http://pic.my4399.com/re/cms/web/js/user/action.js						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	13.4830088615
Path: /re/cms/z/clients/zt_smba_zddl/js/autologin.js **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/js/autologin.js						
record.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	14.4518609047
Path: /a.php?r=&s=800x600&fv=12.0 **URI:** http://record.4399.com/a.php?r=&s=800x600&fv=12.0						
webpic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.3512179852
Path: /re/cms/z/clients/zt_smba_zddl/css/sound.swf **URI:** http://webpic.my4399.com/re/cms/z/clients/zt_smba_zddl/css/sound.swf						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.3790960312
Path: /re/cms/clients/js/client_old_reg.js **URI:** http://pic.my4399.com/re/cms/clients/js/client_old_reg.js						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.60501194
Path: /re/cms/web/js/module/util.js **URI:** http://pic.my4399.com/re/cms/web/js/module/util.js						
pic.my4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.671036005
Path: /re/cms/feUtil/easydialog/2.2/easydialog.min.js **URI:** http://pic.my4399.com/re/cms/feUtil/easydialog/2.2/easydialog.min.js						
web.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.9735848904
Path: /util/get_login.php?&jsoncallback=jsonp_05604826788807868 **URI:** http://web.4399.com/util/get_login.php?&jsoncallback=jsonp_05604826788807868						
web.4399.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	15.9738600254
Path: /util/get_login.php?&jsoncallback=jsonp_05643016475029259 **URI:** http://web.4399.com/util/get_login.php?&jsoncallback=jsonp_05643016475029259						
txt.unionli.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	1	16.5884549618
Path: /txlink.gif?alid=70236&oid=16311&time=1534806157492 **URI:** http://txt.unionli.com/txlink.gif?alid=70236&oid=16311&time=1534806157492						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.1377859116
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b4cf496d0d7c580c **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?b4cf496d0d7c580c						

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.1923780441
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?37ba3c5494beeaf9 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?37ba3c5494beeaf9						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	33.8585679531
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAWAJn8G8pVTNI4cGFpe7i4%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAWAJn8G8pVTNI4cGFpe7i4%3D						
ocsp2.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	39.6611249447
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRJrF0xYA49jC3D83fgDGesaUkzIQQUf9OZ86BHDjEAVlYijrfMnt3KAYoCEA%2Bo0zpfaDx76QP%2FphgC0qo%3D **URI:** http://ocsp2.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRJrF0xYA49jC3D83fgDGesaUkzIQQUf9OZ86BHDjEAVlYijrfMnt3KAYoCEA%2Bo0zpfaDx76QP%2FphgC0qo%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.7702920437
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	76.6046800613
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	82.0812180042
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	87.7261450291
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
www.baidu.com	A
Answers - www.a.shifen.com (CNAME) - 104.193.88.77 (A) - 104.193.88.123 (A) - www.wshifen.com (CNAME)	
client.5054399.com	A
Answers - client.r.4399api.net (CNAME) - 219.129.239.26 (A)	
b.533y.com	A
Answers - 121.201.47.218 (A) - 121.201.47.33 (A)	
web.4399.com	A

Request	Type
Answers - web.my4399.com (CNAME) - web.4399.com.lxdns.com (CNAME) - 157.185.170.133 (A) - 4399hw.xdwscache.speedcdns.com (CNAME)	
webpic.my4399.com	A
Answers - webpic.my4399.com.cdn20.com (CNAME) - 157.185.158.198 (A)	
pic.my4399.com	A
Answers - pic.my4399.com.cdn20.com (CNAME)	
record.4399.com	A
Answers - record.me4399.com (CNAME) - 119.147.163.227 (A)	
txt.unionli.com	A
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 23.215.131.176 (A) - a1621.g.akamai.net (CNAME) - ctldl.windowsupdate.com.edgesuite.net (CNAME) - 23.215.131.169 (A)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
ocsp2.digicert.com	A
crl.microsoft.com	A
Answers - crl.www.ms.akadns.net (CNAME) - 23.215.131.200 (A) - 23.215.131.195 (A) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 151.101.66.133 (A) - 151.101.2.133 (A) - global.prd.cdn.globalsign.com (CNAME) - 151.101.194.133 (A) - 151.101.130.133 (A) - prod.globalsign.map.fastly.net (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.83801794052	Sandbox	121.201.47.218	80
7.09769892693	Sandbox	219.129.239.26	80
8.37236595154	Sandbox	157.185.170.133	80
10.3062129021	Sandbox	157.185.158.198	80
10.4032828808	Sandbox	157.185.170.133	80
10.4037778378	Sandbox	157.185.170.133	80
11.4716930389	Sandbox	157.185.158.198	80
11.5671229362	Sandbox	157.185.170.133	80
12.3291628361	Sandbox	157.185.170.133	80
12.526859045	Sandbox	157.185.158.198	80
12.531208992	Sandbox	157.185.158.198	80
12.8538439274	Sandbox	157.185.170.133	80
13.1291379929	Sandbox	157.185.170.133	80
14.4518609047	Sandbox	119.147.163.227	80
15.3790960312	Sandbox	157.185.170.133	80
15.671036005	Sandbox	157.185.170.133	80
15.9735848904	Sandbox	157.185.170.133	80
15.9738600254	Sandbox	157.185.170.133	80
16.5884549618	Sandbox	121.201.47.218	80
17.7394759655	Sandbox	121.201.47.218	443
17.7509698868	Sandbox	121.201.47.218	443
25.1377859116	Sandbox	23.215.131.176	80
25.1923780441	Sandbox	23.215.131.176	80
33.8585679531	Sandbox	72.21.91.29	80
33.9225919247	Sandbox	72.21.91.29	80
39.6611249447	Sandbox	72.21.91.29	80
70.7702920437	Sandbox	23.215.131.200	80
87.7261450291	Sandbox	151.101.2.133	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.06789588928	Sandbox	224.0.0.252	5355
3.09398388863	Sandbox	224.0.0.252	5355
3.1451690197	Sandbox	192.168.56.255	137
3.16460204124	Sandbox	239.255.255.250	3702

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
5.55412888527	Sandbox	8.8.4.4	53
5.65668702126	Sandbox	224.0.0.252	5355
6.35474991798	Sandbox	8.8.4.4	53
6.35622596741	Sandbox	8.8.4.4	53
7.59557890892	Sandbox	8.8.4.4	53
9.15453505516	Sandbox	192.168.56.255	138
9.99210095406	Sandbox	8.8.4.4	53
9.99672985077	Sandbox	8.8.4.4	53
13.4211390018	Sandbox	8.8.4.4	53
15.9556009769	Sandbox	8.8.4.4	53
19.6383080482	Sandbox	224.0.0.252	5355
19.6414470673	Sandbox	224.0.0.252	5355
22.3705868721	Sandbox	224.0.0.252	5355
22.3709259033	Sandbox	224.0.0.252	5355
25.0584259033	Sandbox	8.8.4.4	53
25.0709848404	Sandbox	8.8.4.4	53
28.1928880215	Sandbox	224.0.0.252	5355
28.1933808327	Sandbox	224.0.0.252	5355
31.0457239151	Sandbox	224.0.0.252	5355
31.2182779312	Sandbox	224.0.0.252	5355
33.8094849586	Sandbox	8.8.4.4	53
33.809773922	Sandbox	8.8.4.4	53
34.3151140213	Sandbox	224.0.0.252	5355
37.0199298859	Sandbox	224.0.0.252	5355
39.561070919	Sandbox	8.8.4.4	53
64.9456319809	Sandbox	224.0.0.252	5355
67.9815878868	Sandbox	224.0.0.252	5355
70.6587810516	Sandbox	8.8.4.4	53
71.0894980431	Sandbox	224.0.0.252	5355
73.9539339542	Sandbox	224.0.0.252	5355
76.727782011	Sandbox	224.0.0.252	5355
79.3534579277	Sandbox	224.0.0.252	5355
82.2418789864	Sandbox	224.0.0.252	5355
84.8709259033	Sandbox	224.0.0.252	5355
87.6759889126	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Util[1].Png	**Type :** PNG image data, 150 x 45, 8-bit colormap, non-interlaced **MD5 :** 00cf7090dc6270b2d6cc933d8d78ce74 **SHA-1 :** 710c8d0893b1b522c5667013b52fc8e640f2e216 **SHA-256 :** e281f083fda52acf0ae7ea4e035fcf60559f8a4e76 **SHA-512 :** 0c9a60e1d2474e8e8b79dc4248f6915dafe5bb99 **Size :** 1.381 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@4399[1].Txt	**Type :** ASCII text, with very long lines **MD5 :** 94e9f8c2878d79452d1c3725c2dc176f **SHA-1 :** 93dc3db997ebce0400bc107e8e1fc720b865cd17 **SHA-256 :** 8bcd947658d8b806905ac163b0f533e8ad709c27 **SHA-512 :** c0c992401251fbbde14291d01b0474e6839a8f8c **Size :** 1.901 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B398B80134F72209547439DB21AB308D_28699ABAC9273C08DCF1E93A8F6BFD1D	**Type :** data **MD5 :** 38aafdc0e04688078d11e48a97d3435f **SHA-1 :** c07902218cb15cc17ec58d1f5aec9e7e1ce56ca7 **SHA-256 :** c7f8236a0e7a90f9950e9216c6c53c730cb1fe587 **SHA-512 :** 16e3a983cf8ce2a04c5fdd171d9f7dcd083251fea **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 5fea0b64fc0027b7c65272c10a9faf77 **SHA-1 :** 0b90d3f643bb7809c80eba18f1ed27bceb715474 **SHA-256 :** dbf8b9da19106e924ecbbbf73426bbf086e320cd **SHA-512 :** aa5847f53be42bf0ad34adc3162b45533eb9455e **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\User@4399[2].Txt	**Type :** ASCII text, with very long lines **MD5 :** ccc0e9c87025a9ffd63ba681340bf9f0 **SHA-1 :** 703e76cee0b2f71a7de83cc8d311304fb7a72f4b **SHA-256 :** fd515968279dd74668cbb71260d696992b5faac4 **SHA-512 :** f439efb16614bf1b564e3528c181fb717c7f5dc60 **Size :** 1.902 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B08578675F0562C4A68283513357EA41	**Type :** data **MD5 :** 451474da357d7b84d98b1286be7a8686 **SHA-1 :** c48fbb09d207a1f8ab215567fdbf325db114feac **SHA-256 :** 9106e485d46cb74b2c91b26333027038845b401 **SHA-512 :** 41fd5a36c7d369b46c0abe7033879365fd62af4d **Size :** 0.436 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6509 bytes, 1 file **MD5 :** 33b39e2a516ef730a8fa922894f0fbd5 **SHA-1 :** 03d455583dda59215d945af76af6293b202f586f **SHA-256 :** 9446e8f2056fea3ac1365a809ada04602606242c **SHA-512 :** 75763aa13b43eb96294b0f84e13106611198872 **Size :** 6.509 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Action[1].Js	**Type :** UTF-8 Unicode text, with very long lines, with no line terminators **MD5 :** 966c301a554db4e046278f143e4ad556 **SHA-1 :** 8ccae2c5ca7e5dfe63dd21fd418265b7ece6749f **SHA-256 :** 897da1213f907f48bd5a2f5ef8aad8ef2d5a957d2 **SHA-512 :** 4f461d944ad8bab459fe1c9f5ecd96a7479541a4 **Size :** 72.999 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Util[1].Js	**Type :** UTF-8 Unicode text, with very long lines, with no line terminators **MD5 :** e5bd0d8e49b99ff04841306f68fc95a1 **SHA-1 :** 0760e1b42e3d247b8055422d3aaa767b48da3eff **SHA-256 :** 9517bc5ae896085cde0d05784c6ab9274247354 **SHA-512 :** 22c4ecc6ba45852e89cf5d988d4c9531e2f2598f4 **Size :** 10.441 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Config[1].Js	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** cbbb11b8d585027ca9d35c3d2c23a8f1 **SHA-1 :** 24c2bd8a8338ab8bf2726e1eaf1269d8027a696c **SHA-256 :** 993877f5e82ba607cf489893d75541fcd9722cf82 **SHA-512 :** f691fc7694d12b34ee6b34c9627afa4da037b5d8 **Size :** 1.282 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Core[1].Js	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** a7e96a46ca6c157501c0a6693ee2c520 **SHA-1 :** 87cd3adeae2c06505088d1e685353cbdf32a4ee0 **SHA-256 :** bb90e9fc18ef95c3dfb1f4082fe30280e0389545ff **SHA-512 :** 4177004b58eb51c2ed049f664ad619c917a39937 **Size :** 6.406 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** e4de9d460aa59589d77fa870bafa9aa4 **SHA-1 :** d5d515ed579e3dbe36b80d918a7aec5d92a11e5f **SHA-256 :** 9e82431c0c6af5bb5fc3be28d8fe0e16ee285d57 **SHA-512 :** 8bcae472ce7261d076c5d98aa03b4bb482e6688 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B08578675F0562C4A68283513357EA41	**Type :** data **MD5 :** 514b454fa9abd8c59f309cbf63899699 **SHA-1 :** 8842aa7963b33f6695f292b7ec053b052e0d63f2 **SHA-256 :** 41c0df9fecfa18a445108220fc6bc5e7b1c1a79f55 **SHA-512 :** 502a60d571bf4d1813907eb6005f22e11ee5b9e1 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Get_login[1].Php	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 29f93412592f02be05d90195018bd16e **SHA-1 :** 2edc7c74817f451e4fd73402f806623452272785 **SHA-256 :** d19f416dbf58442ac0d0abf246d09dba6b797bac **SHA-512 :** 731a56858e65bb482856acaf07f9139f0f5f5a79c5 **Size :** 0.497 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Get_login[1].Php	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** d18a37158c26b8affb6e72af330570b0 **SHA-1 :** 157979dac885c7df1cb3aad9a53fd8de4ac0b553 **SHA-256 :** f7c3809451fb741149ad7bdb128eb1e0150d979b **SHA-512 :** 5e34c7c74af3250f1cf7441c6536cec5353866b3d **Size :** 0.497 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 69b404e38752da509eacc270a9fb1337 **SHA-1 :** 6b5cfc879a5d8ba0ddf1636d6430ac1ddfb35cee **SHA-256 :** 6c87cca3428a5e56f76e5740e806522d0a9459a5 **SHA-512 :** 28f3560aa84b9004d609e30b2e544feeac87dae7 **Size :** 49.152 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** bcdaf6b8703c44252ab4e94be1e6f1b0 **SHA-1 :** 80ec81790fc06804eede4467bc6dc2eaf7144e49 **SHA-256 :** 64a6a5af8f1c4dc6bfb7363743f9a7b3e1dd0b7a4 **SHA-512 :** 78431d689c10c7a43195ddd67d93edbab89026e **Size :** 0.342 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Web_referer[1].Js	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 88e7d93a00f55f1080fc2fcc98899ea7 **SHA-1 :** e547d152becaad20a600aba14b17374141789e69 **SHA-256 :** e124e028c4b1522c2147bca4bbe8807a446c3d7b **SHA-512 :** 885571927b38e76e49aa88462e6881e43133ed4 **Size :** 10.077 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Bg1[1].Png	**Type :** PNG image data, 1196 x 748, 8-bit colormap, non-interlaced **MD5 :** e24870ea9b0648fd015adc252c581d21 **SHA-1 :** 1aebaf967e7d0a25bf35c67b4cfa40ad5105c01d **SHA-256 :** 8b949f77174ce377c32354d6bd067aa2e0118d7(**SHA-512 :** 0c2b72bf917c9de2664ef4d90a08a4b8d86aebab **Size :** 5.828 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B398B80134F72209547439DB21AB308D_28699ABAC9273C08DCF1E93A8F6BFD1D	**Type :** data **MD5 :** 8d9d52f4fe26341bf254fd4f96504d6d **SHA-1 :** c585b16f759112e97dc6cfa64a231a7e1aa52ef1 **SHA-256 :** b2dc2c8c1d435c6d64742a22cf9c9d05f9086d473 **SHA-512 :** a8d75f992be9f0fc96e4e36afa4b5ab674de531a8 **Size :** 0.43 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Autologin[1].Js	**Type :** UTF-8 Unicode text **MD5 :** 7231f904e242232c98c7703a62d8f5a9 **SHA-1 :** 47a757b8d9dd116d650a8dc90c1c6343f95a21c9 **SHA-256 :** 75fe4908bf695a1ca447f8262ade06dcceed9933c **SHA-512 :** 0e6cac0ee54e7f295335479c5622b7399c51b7d4 **Size :** 1.374 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Client_old_reg[1].Js	**Type :** UTF-8 Unicode text, with very long lines **MD5 :** 8d88528f0b2abd62ee55f3be88eb5bb9 **SHA-1 :** 8ffd9dc53b0f84e8364a3bae756542a0e6e08d97 **SHA-256 :** efbe0aa0b2a800d14f8e02c573889c78207a6536 **SHA-512 :** 29adb186cfc355ef4c2968a1eb23654eaed2e624 **Size :** 42.628 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Easydialog.Min[1].Js	**Type :** HTML document, ASCII text, with very long lines, with no line terminators **MD5 :** d04691487c711d707898c48f88b83e87 **SHA-1 :** bac833db68922830c5f0f27d5ed0eae7efe2df73 **SHA-256 :** 8509a45e7e98ebe34c7764898c6be530150d4ee **SHA-512 :** e5cf64e3bf72a15770295e9980905cec9f9e8f455 **Size :** 9.108 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Bb[1].Jpg	**Type :** JPEG image data, JFIF standard 1.01 **MD5 :** c42641d1d1ef87fba80fbf5ea270e77d **SHA-1 :** 2832c9fefdc6f8c8492ba7279bfd239953c5beb4 **SHA-256 :** 2a6b03d58b08de445f63cd7842e478ce2c08af88 **SHA-512 :** baebc6ec22e4ab72ebc969b405182fed2e813763 **Size :** 172.929 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\EffectTj[1].Js	**Type :** UTF-8 Unicode text, with very long lines, with CRLF line terminators **MD5 :** 70bbe5d5c773808f4e4cfcd2fbab1f64 **SHA-1 :** 40fba1e34cee8387fffbee719e519a293c5d0be7 **SHA-256 :** 346a333dc412dc18ec52246f7bfd472f0886f08da **SHA-512 :** 12ac63678f48b6a77c8e210eb1090c33bc89ee00 **Size :** 26.418 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Theme[1].Css	**Type :** ASCII text, with CRLF line terminators **MD5 :** bd34409adda5b36a5e058e559d35c415 **SHA-1 :** b4f7a3a02b422b0ba1b037bc04ebb48c2eb42c53 **SHA-256 :** 34f3736ac16c12c239f455456f3d0f460019a29e6 **SHA-512 :** a55d6bb8bf9a6f229cdde39ed565fc769920ffaef **Size :** 15.79 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Jquery[1].Js	**Type :** HTML document, UTF-8 Unicode text, with very long lines **MD5 :** b8d64d0bc142b3f670cc0611b0aebcae **SHA-1 :** abcd2ba13348f178b17141b445bc99f1917d47af **SHA-256 :** 47b68dce8cb6805ad5b3ea4d27af92a241f4e29a **SHA-512 :** a684abbe37e8047c55c394366b012cc9ae5d682c **Size :** 94.84 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	900f83e9f1dd818f4c1006ae6b0c6c518d6bc943376140fc2be3c99f1d8ffa9f.ex
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	855fa325ab3aa9499ec8260a8172c2f75b5854d7
MD5:	1fc01f0b85c82b69c5e04b55bb8a07ee
First Seen Date:	2018-08-20 06:40:07.464624 (3 years ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-08-20 06:40:07.464624 (3 years ago)
Human Expert Analysis Date:	2018-08-20 09:03:47.788087 (3 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'E:\\Out\\Bin\\4399AlliGsLoginer3\\Release.pdb\x00', u'GUID': u'{575d9961-1cea-4fe3-b8e3-500a386ade2a}', u'timestamp': u'2018-03-12 09:05:14'}]
Number Of Sections	6
Trid	[[52.9, u'Win32 Executable (generic)'], [23.5, u'Generic Win/DOS Executable'], [23.5, u'DOS Executable Generic']]
Compilation Time Stamp	0x3721C848 [Sat Apr 24 13:34:00 1999 UTC] [SUSPICIOUS]
LegalCopyright	\u56db\u4e09\u4e5d\u4e5d\u7f51\u7edc\u80a1\u4efd\u6709\u9650\u516c\u53f8 \u4fdd\u7559\u6240\u6709\u6743\u5229\u3002
InternalName	Z70236.exe
FileVersion	zt_smba_zddl
CompanyName	\u56db\u4e09\u4e5d\u4e5d\u7f51\u7edc\u80a1\u4efd\u6709\u9650\u516c\u53f8
ProductName	4399\u6218\u5929
ProductVersion	zt_smba_zddl
FileDescription	4399\u6218\u5929
OriginalFilename	Z70236.exe
Translation	0x0804 0x03a8
Entry Point	0x431d02 (lmfdybsv)
Machine Type	Intel 386 or later - 32Bit
File Size	853557
Ssdeep	12288:EVotwO0KggLXiR0a5zteWDSzqJTyYR/UuZkzqJ7dFGI5NmN3q/Q:E4w/gLXiR0a5QW2FYR/7ZNkY/Q
Sha256	900f83e9f1dd818f4c1006ae6b0c6c518d6bc943376140fc2be3c99f1d8ffa9f
Exifinfo	[{u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/8/5/5/f/855fa325ab3aa9499ec8260a8172c2f75b5854d7', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:08:20 06:39:13+00:00', u'EXE:InitializedDataSize': 355840, u'File:FileModifyDate': u'2018:08:20 06:39:04+00:00', u'File:FileSize': u'834 kB', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'855fa325ab3aa9499ec8260a8172c2f75b5854d7', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'1999:04:24 13:34:00+00:00', u'EXE:LinkerVersion': 48.51, u'ExifTool:ExifToolVersion': 10.1, u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/8/5/5/f', u'EXE:EntryPoint': u'0x31d02', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 484352, u'File:FileInodeChangeDate': u'2018:08:20 06:39:04+00:00', u'EXE:Subsystem': u'Windows GUI'}]
Mime Type	application/x-dosexec
Imphash	02524d242e54d4dba7e77c0f2541b46f

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
lmfdybsv	0x1000	0x76269	0x76400	6.60200375447	9638facfe15d5d9c7d4ca68017182172
pgrtbqsd	0x78000	0x1f39a	0x1f400	5.19193393131	4ff8dc743c491f007a3599730fd63533
teiptyom	0x98000	0x8ab8	0x3a00	4.28062838153	a4ef89a5b9ac297d666e2d33440a6742
lyfpbntd	0xa1000	0x3000	0x3000	0.325945817676	ffbdeea1c2cd536c91cec5bbe76499f0
lkuyhiur	0xa4000	0x225b4	0x22600	6.80535691925	55a77bdca02bec7fb8d0100a3438d9f2
jdwdhhmg	0xc7000	0xe8e0	0xea00	4.75556467869	4327c0eeea18a7ec1577287f978183d1

PE Imports

- KERNEL32.dll
  - TlsAlloc
  - TlsSetValue
  - LocalReAlloc
  - DeleteCriticalSection
  - TlsFree
  - GlobalFlags
  - lstrlenA
  - SetErrorMode
  - GetStartupInfoW
  - ExitProcess
  - GetSystemTimeAsFileTime
  - TerminateProcess
  - UnhandledExceptionFilter
  - IsDebuggerPresent
  - HeapFree
  - HeapAlloc
  - HeapReAlloc
  - RtlUnwind
  - VirtualProtect
  - VirtualAlloc
  - VirtualQuery
  - HeapSize
  - GetStdHandle
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - GetCommandLineW
  - SetHandleCount
  - GetFileType
  - GetStartupInfoA
  - HeapCreate
  - EnterCriticalSection
  - VirtualFree
  - InitializeCriticalSection
  - InitializeCriticalSectionAndSpinCount
  - GetCPInfo
  - GetACP
  - GetOEMCP
  - IsValidCodePage
  - LCMapStringW
  - GetTimeZoneInformation
  - GetConsoleCP
  - GetConsoleMode
  - GetTimeFormatA
  - GetDateFormatA
  - GetLocaleInfoA
  - LCMapStringA
  - GetStringTypeA
  - GetStringTypeW
  - WriteConsoleA
  - GetConsoleOutputCP
  - WriteConsoleW
  - SetStdHandle
  - GetProcessHeap
  - SetEnvironmentVariableA
  - TlsGetValue
  - LeaveCriticalSection

- GetThreadContext
- SetThreadContext
- FlushInstructionCache
- InterlockedCompareExchange
- GetFullPathNameW
- QueryPerformanceCounter
- GlobalReAlloc
- GetVolumeInformationW
- DuplicateHandle
- GetFileSize
- SetEndOfFile
- UnlockFile
- LockFile
- FlushFileBuffers
- GetThreadLocale
- MoveFileW
- GetFileTime
- GetFileSizeEx
- GetFileAttributesExW
- InterlockedIncrement
- GlobalFindAtomW
- CompareStringW
- LoadLibraryA
- GetVersionExA
- GetModuleHandleA
- GlobalAddAtomW
- SuspendThread
- ResumeThread
- GlobalDeleteAtom
- ConvertDefaultLocale
- EnumResourceLanguagesW
- lstrcmpA
- GetLocaleInfoW
- CompareStringA
- InterlockedExchange
- FormatMessageW
- MulDiv
- InterlockedDecrement
- CreateMutexW
- GlobalHandle
- GlobalFree
- TerminateThread
- GetCurrentDirectoryW
- VirtualProtectEx
- GetCurrentThread
- GlobalUnlock
- GlobalLock
- GlobalAlloc
- LoadLibraryExW
- LocalFree
- GetSystemInfo
- LocalAlloc
- FileTimeToLocalFileTime
- FileTimeToSystemTime
- SetFileAttributesW
- FindNextFileW
- FindClose
- ReadFile
- GetFileAttributesW
- CreateDirectoryW
- FreeResource
- FindFirstFileW
- lstrcmpW
- GetTickCount
- GetVersionExW
- ReadProcessMemory
- WriteProcessMemory
- VirtualFreeEx
- VirtualAllocEx
- OpenProcess
- DeviceIoControl
- CreateProcessW
- MoveFileExW
- Sleep
- lstrcpyW

    - lstrcpynW
    - WideCharToMultiByte
    - WriteFile
    - SetLastError
    - SetFilePointer
    - CreateFileA
    - SetThreadPriority
    - CreateProcessA
    - GetModuleFileNameA
    - GetTempFileNameA
    - GetTempPathA
    - RemoveDirectoryW
    - GetPrivateProfileIntW
    - DeleteFileW
    - WritePrivateProfileStringW
    - CopyFileW
    - ResetEvent
    - CreateEventW
    - GetPrivateProfileStringW
    - LockResource
    - SetUnhandledExceptionFilter
    - GetCurrentProcessId
    - GetCurrentProcess
    - GetCurrentThreadId
    - RaiseException
    - LoadLibraryW
    - CreateFileW
    - FreeLibrary
    - MultiByteToWideChar
    - SizeofResource
    - LoadResource
    - FindResourceW
    - GetLastError
    - GetModuleFileNameW
    - lstrlenW
    - GetProcAddress
    - GetModuleHandleW
    - WaitForSingleObject
    - SetEvent
    - CreateThread
    - CloseHandle
- USER32.dll
    - GetClassLongW
    - SetPropW
    - GetPropW
    - RemovePropW
    - GetTopWindow
    - GetMessageTime
    - GetMessagePos
    - MapWindowPoints
    - SetMenu
    - UpdateWindow
    - GetClassInfoExW
    - GetClassInfoW
    - RegisterClassW
    - AdjustWindowRectEx
    - CallWindowProcW
    - GetMenu
    - OffsetRect
    - IntersectRect
    - SystemParametersInfoA
    - GetWindowPlacement
    - GrayStringW
    - DrawTextExW
    - TabbedTextOutW
    - GetDlgCtrlID
    - SetWindowTextW
    - IsDialogMessageW
    - SetDlgItemTextW
    - SendDlgItemMessageW
    - GetDlgItemTextW
    - GetWindowTextLengthW
    - GetLastActivePopup
    - GetMessageW
    - TranslateMessage

- DispatchMessageW
- PeekMessageW
- IsChild
- SetMenuItemBitmaps
- ModifyMenuW
- EnableMenuItem
- CheckMenuItem
- WindowFromPoint
- CopyRect
- GetActiveWindow
- SetActiveWindow
- CreateDialogIndirectParamW
- GetDlgItem
- IsWindowEnabled
- GetNextDlgTabItem
- EndDialog
- SetWindowContextHelpId
- MapDialogRect
- GetMenuState
- GetMenuItemID
- GetMenuItemCount
- GetSubMenu
- EndPaint
- BeginPaint
- FindWindowW
- FindWindowExW
- PostMessageW
- GetWindow
- DefWindowProcW
- EqualRect
- CreateWindowExW
- RegisterClassExW
- LoadImageW
- GetWindowDC
- GetWindowTextW
- DestroyWindow
- SetLayeredWindowAttributes
- UpdateLayeredWindow
- SetWindowLongW
- GetWindowLongW
- SetFocus
- GetFocus
- DrawIconEx
- GetSysColor
- GetParent
- LoadCursorW
- SetCursor
- SetWindowRgn
- WinHelpW
- SendDlgItemMessageA
- RegisterWindowMessageW
- SetRect
- CopyAcceleratorTableW
- InvalidateRgn
- CharUpperW
- GetSysColorBrush
- CharNextW
- GetNextDlgGroupItem
- CloseClipboard
- SetClipboardData
- EmptyClipboard
- MessageBeep
- UnregisterClassW
- RegisterClipboardFormatW
- PostThreadMessageW
- ValidateRect
- GetClassNameW
- SendMessageW
- IsRectEmpty
- GetWindowThreadProcessId
- GetMenuCheckMarkDimensions
- GetDC
- DrawTextW
- ReleaseDC
- GetKeyState

- CallNextHookEx
- LoadIconW
- SetWindowsHookExW
- SetTimer
- GetDesktopWindow
- IsIconic
- GetSystemMetrics
- GetClientRect
- DrawIcon
- InvalidateRect
- IsWindowVisible
- MoveWindow
- GetWindowRect
- RedrawWindow
- CreatePopupMenu
- AppendMenuW
- TrackPopupMenu
- DestroyMenu
- IsWindow
- ShowWindow
- SetForegroundWindow
- GetCursorPos
- KillTimer
- ScreenToClient
- ClientToScreen
- OpenClipboard
- MessageBoxW
- FillRect
- LoadBitmapW
- SetCapture
- PtInRect
- ReleaseCapture
- GetCapture
- EnableWindow
- SetWindowPos
- AttachThreadInput
- GetForegroundWindow
- SystemParametersInfoW
- SetParent
- PostQuitMessage
- UnhookWindowsHookEx

- GDI32.dll
  - CreatePen
  - GetRgnBox
  - GetMapMode
  - GetBkColor
  - GetTextColor
  - ExtSelectClipRgn
  - ScaleWindowExtEx
  - SetWindowExtEx
  - SetWindowOrgEx
  - ScaleViewportExtEx
  - SetViewportExtEx
  - OffsetViewportOrgEx
  - SetViewportOrgEx
  - Escape
  - ExtTextOutW
  - RectVisible
  - PtVisible
  - GetWindowExtEx
  - GetViewportExtEx
  - GetClipBox
  - SetMapMode
  - SetBkColor
  - RestoreDC
  - SaveDC
  - CreateBitmap
  - CreateRectRgnIndirect
  - GetDeviceCaps
  - TextOutW
  - SetTextColor
  - SetBkMode
  - Rectangle
  - CreateSolidBrush
  - GetDIBits

    - LineTo
    - MoveToEx
    - CombineRgn
    - GetPixel
    - CreateRectRgn
    - StretchBlt
    - DeleteDC
    - CreateDIBSection
    - SelectObject
    - GetStockObject
    - DeleteObject
    - BitBlt
    - CreateFontIndirectW
    - GetObjectW
    - CreateCompatibleBitmap
    - CreateCompatibleDC
- MSIMG32.dll
    - AlphaBlend
    - TransparentBlt
- COMDLG32.dll
    - GetFileTitleW
    - GetSaveFileNameW
- WINSPOOL.DRV
    - DocumentPropertiesW
    - OpenPrinterW
    - ClosePrinter
- ADVAPI32.dll
    - CryptSetKeyParam
    - RegDeleteValueW
    - RegCloseKey
    - RegCreateKeyExW
    - RegQueryValueExW
    - RegQueryValueW
    - RegOpenKeyW
    - RegEnumKeyW
    - RegDeleteKeyW
    - RegOpenKeyExW
    - CryptEncrypt
    - CryptDestroyKey
    - RegSetValueExW
    - CryptReleaseContext
    - CryptImportKey
    - CryptAcquireContextW
- SHELL32.dll
    - SHChangeNotify
    - Shell_NotifyIconW
    - SHGetSpecialFolderLocation
    - SHGetMalloc
    - SHGetPathFromIDListW
    - SHGetSpecialFolderPathW
    - ShellExecuteW
    - SHGetFolderPathW
- COMCTL32.dll
    - InitCommonControlsEx
    - _TrackMouseEvent
- SHLWAPI.dll
    - SHDeleteKeyW
    - SHDeleteValueW
    - UrlUnescapeA
    - StrCmpW
    - PathFindExtensionW
    - PathFindFileNameW
    - PathStripToRootW
    - PathIsUNCW
- oledlg.dll
    - OleUIBusyW
- ole32.dll
    - CoTaskMemAlloc
    - CLSIDFromProgID
    - CLSIDFromString
    - StgOpenStorageOnILockBytes
    - StgCreateDocfileOnILockBytes
    - CreateILockBytesOnHGlobal
    - CoRevokeClassObject
    - CoTaskMemFree

    - OleDraw
    - OleSetContainedObject
    - OleCreate
    - OleUninitialize
    - OleInitialize
    - CoCreateGuid
    - CreateStreamOnHGlobal
    - CoCreateInstance
    - CoFreeUnusedLibraries
    - CoUninitialize
    - OleIsCurrentClipboard
    - OleFlushClipboard
    - CoRegisterMessageFilter
    - CoGetClassObject
    - CoInitialize
- OLEAUT32.dll
    - VariantClear
    - VariantInit
    - SysAllocStringLen
    - SysAllocString
    - SysAllocStringByteLen
    - SysStringByteLen
    - SysStringLen
    - VariantChangeType
    - VariantCopy
    - DispCallFunc
    - LoadRegTypeLib
    - VariantTimeToSystemTime
    - SystemTimeToVariantTime
    - SafeArrayDestroy
    - SafeArrayUnaccessData
    - SafeArrayAccessData
    - SafeArrayGetElemsize
    - SysFreeString
    - SafeArrayCreate
    - OleCreateFontIndirect
    - GetErrorInfo
- gdiplus.dll
    - GdipGetImageWidth
    - GdipReleaseDC
    - GdipDrawImagePointsI
    - GdipLoadImageFromStream
    - GdipBitmapLockBits
    - GdipCreateFromHDC
    - GdipCreateHBITMAPFromBitmap
    - GdipDisposeImage
    - GdipAlloc
    - GdipBitmapUnlockBits
    - GdipCloneImage
    - GdipDeleteGraphics
    - GdipCreateBitmapFromStream
    - GdipGetImageHeight
    - GdipFree
    - GdiplusShutdown
    - GdiplusStartup
- WS2_32.dll
    - connect
    - WSAStartup
    - htons
    - shutdown
    - setsockopt
    - WSACleanup
    - recv
    - socket
    - closesocket
    - gethostbyname
    - send
    - getprotobyname
- WININET.dll
    - InternetOpenW
    - InternetConnectW
    - HttpOpenRequestW
    - HttpSendRequestW
    - HttpQueryInfoW
    - InternetReadFile

    - InternetSetFilePointer
    - InternetCloseHandle
    - DeleteUrlCacheEntryW
    - FindNextUrlCacheEntryW
    - FindFirstUrlCacheEntryW
    - InternetGetCookieW
    - InternetCheckConnectionW
- IPHLPAPI.DLL
    - GetAdaptersInfo
- WINMM.dll
    - mixerGetLineControlsW
    - mixerOpen
    - mixerGetControlDetailsW
    - mixerClose
    - mixerGetLineInfoW
    - mixerGetNumDevs
    - mixerSetControlDetails
    - midiStreamOut
    - waveOutWrite
- DSOUND.dll
    - None

PE Resources

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 676928, u'sha256': u'8b949f77174ce377c32354d6bd067aa2e0118d7080a78d597613653c4186e72a', u'type': u'PNG image data, 1196 x 748, 8-bit colormap, non-interlaced', u'size': 5828}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 682756, u'sha256': u'd42bf37757c85d4f19c2e42c723d26135f4663468f7c3f2655c85281cd71a35c', u'type': u'PNG image data, 30 x 51, 8-bit/color RGB, non-interlaced', u'size': 1168}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 683924, u'sha256': u'705d737863684019e1d8df5736d9fd02dc8b10b7dbfa022eb9baafbdd8142a8f', u'type': u'PNG image data, 120 x 25, 8-bit/color RGBA, non-interlaced', u'size': 1646}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 685572, u'sha256': u'85ee999d65f95b475ec360ebfe74a03b7cd2d21eb8d753a8b753640c64c5c7ea', u'type': u'PNG image data, 228 x 23, 8-bit/color RGBA, non-interlaced', u'size': 1987}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 687560, u'sha256': u'1cccf531f99062e0aaa6f03f3b21d8251aa62c77792064eec288a167bc3ee195', u'type': u'PNG image data, 30 x 51, 8-bit/color RGB, non-interlaced', u'size': 1086}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 688648, u'sha256': u'e5e063a10a0d38d235e8ae948321eaeb0415c63fc5a1b3222bae19513daded09', u'type': u'PNG image data, 116 x 25, 8-bit/color RGBA, non-interlaced', u'size': 1328}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 689976, u'sha256': u'bb1f7044e8429e77202897a8da25d93d056750e55bbc7b96cb6ed65c775f0931', u'type': u'PNG image data, 116 x 25, 8-bit/color RGBA, non-interlaced', u'size': 1218}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 691196, u'sha256': u'0ce7495181ba70c23f9fa4e40b0d87bd5c18ccdc140341f3a03e803afdfc3436', u'type': u'PNG image data, 116 x 25, 8-bit/color RGBA, non-interlaced', u'size': 1507}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 692704, u'sha256': u'0d8fd5e156bf2fde2c3208541cac902d55954813c316c87c06be511eae6b6f69', u'type': u'PNG image data, 212 x 25, 8-bit/color RGBA, non-interlaced', u'size': 3046}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 695752, u'sha256': u'b6cdaee8b5f28dc251915caa041aebd5e1e358e940b1b3c0dc326bcf5d0a6c02', u'type': u'PNG image data, 116 x 25, 8-bit/color RGBA, non-interlaced', u'size': 1486}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 697240, u'sha256': u'482818809a0cc71334fdcb5f7c3c8703b7de27db9b01899220099ba39b8a06ff', u'type': u'PNG image data, 528 x 22, 8-bit/color RGBA, non-interlaced', u'size': 3947}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 701188, u'sha256': u'873dddfb48351769d092ec3d28acd797c5865195d850ecc4fe9619f4edd16bbe', u'type': u'PNG image data, 42 x 14, 8-bit/color RGBA, non-interlaced', u'size': 1499}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 702688, u'sha256': u'fa35cec3176f5ecc8a310127eae44f2a7c60a943c3863b56c6cb1a1551017413', u'type': u'PNG image data, 224 x 23, 8-bit/color RGBA, non-interlaced', u'size': 2808}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 705496, u'sha256': u'f74d09ebbb7b04ecf0218b7fe5e5fa03be45040579828779e8e5df74f18c58fb', u'type': u'PNG image data, 224 x 23, 8-bit/color RGBA, non-interlaced', u'size': 2974}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 708472, u'sha256': u'8b18965f32110f6dd537eac7a4efcc0230f02b5656201eb778e754a4ba5b4400', u'type': u'PNG image data, 390 x 21, 8-bit colormap, non-interlaced', u'size': 1831}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 710304, u'sha256': u'8d74a72ad175255305d1d8b1ba61f3d85feb38dda6f95092c301042038d469dd', u'type': u'PNG image data, 390 x 21, 8-bit colormap, non-interlaced', u'size': 1330}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 711636, u'sha256': u'8b46b61d2501b17e7ec6753e6c2c0c47e4d935e6831541e5f34b92fbfaae9b03', u'type': u'PNG image data, 284 x 150, 8-bit colormap, non-interlaced', u'size': 1357}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 712996, u'sha256': u'43df1092348ab87a5d220f7609982fd847e1ed3af6ddbfa7c9269c6cbaffc4b9', u'type': u'PNG image data, 112 x 16, 8-bit/color RGBA, non-interlaced', u'size': 1616}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 714612, u'sha256': u'2a918f456e6f08cb41cf34e749de46ca740481080785306514c9ff0e44e0e4de', u'type': u'PNG image data, 132 x 27, 8-bit/color RGBA, non-interlaced', u'size': 2198}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 716812, u'sha256': u'73f8fcc8410e9798db1199e6c974e95bfd10a5ff4f87f28799a1988f3b7d7071', u'type': u'PNG image data, 228 x 23, 8-bit/color RGBA, non-interlaced', u'size': 3166}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 719980, u'sha256': u'335823eda5885ab008206edd946c7b1cb067026471a78cdf3df0a2891a81aa91', u'type': u'PNG image data, 252 x 23, 8-bit/color RGBA, non-interlaced', u'size': 2354}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 722336, u'sha256': u'2aa1a075e3114e20cb5c20e31f9439d3dfe3e7560da0439bc104a7be0be319a4', u'type': u'PNG image data, 256 x 23, 8-bit/color RGBA, non-interlaced', u'size': 2839}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 725176, u'sha256': u'41745eab49f2cb7ce1d68434c79d04768b1357108c5c49f6b82612d79293efda', u'type': u'PNG image data, 240 x 23, 8-bit/color RGBA, non-interlaced', u'size': 3041}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 728220, u'sha256': u'f3adf894228367454eaf1b5cc7015bb67e02e9e040912c8d97b091d02cbfa5a3', u'type': u'PNG image data, 240 x 23, 8-bit/color RGBA, non-interlaced', u'size': 3518}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 731740, u'sha256': u'0c1359d078531d210b1f8215ff8fc25730f700e429874abbc40575cfee4ed8fe', u'type': u'PNG image data, 240 x 23, 8-bit/color RGBA, non-interlaced', u'size': 2782}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 734524, u'sha256': u'ebdbed6c3c11566eb5657609fa1b447b72eb68deb128f92a7d08e0c1d41a2950', u'type': u'PNG image data, 16 x 16, 8-bit/color RGB, non-interlaced', u'size': 1177}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 735704, u'sha256': u'b91ecaa1ea8ff1421e591f9c1bb55804edf001004e3f9b626ce130e44a5cc32a', u'type': u'PNG image data, 152 x 26, 8-bit/color RGBA, non-interlaced', u'size': 1108}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 736812, u'sha256': u'8a936622f8ab14e0f1617d7cf82908389327e1af5caac5ebfffa9166c932b747', u'type': u'PNG image data, 160 x 15, 8-bit/color RGBA, non-interlaced', u'size': 2371}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 739184, u'sha256': u'caecc2a5ddc866d56617d5206661228b40553e0233995ef6d3b895fc38676383', u'type': u'PNG image data, 168 x 12, 8-bit/color RGBA, non-interlaced', u'size': 2315}

{u'lang': u'LANG_CHINESE', u'name': u'PNG', u'offset': 741500, u'sha256': u'6c0bca462bd03fc462d861e44bea1a1abf5b2e486a09cb47e53191ce7121c006', u'type': u'PNG image data, 168 x 16, 8-bit/color RGB, non-interlaced', u'size': 2125}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 743628, u'sha256': u'fbeb3be87e80cb8e1d2af3d8140796c1bb80c6c7056f60897088ff9e355c3867', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 743936, u'sha256': u'f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3', u'type': u'data', u'size': 180}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 744116, u'sha256': u'652988945185cf5d604d9b48de66288d82d8ed0acdd134398e90d002d2d9fc72', u'type': u'AmigaOS bitmap font', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 744424, u'sha256': u'0b0e16c38a3d5a85566e67b1d9a7e720e4dee27e163b06099d3d7dfa5dbed9ee', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 744732, u'sha256': u'368f9cb089d206a8b61251f0c85eeda97ee08a56b33be8579246e964d3af6169', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 745040, u'sha256': u'6440c3a38dcfb81d45bc6be31b776fdae116dd7a2933b407b67132f6cfa0e6eb', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 745348, u'sha256': u'9882a8462ce9de3cc9a5d0ca48c8c4f7ca97f1f846f0c10e6655e33c9734b152', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 745656, u'sha256': u'322e92d75b3fec9e16b81466f4cf111d298b80812d5b238f4ee032c025a02050', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 745964, u'sha256': u'8db6df648274a0fc3d28430367216e1c17c364ca613066cbb0e133637e92ba62', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 746272, u'sha256': u'f9c81ce9b4176b305c554a15f0ca2b98b11be76c1f13ef22169999aa07e9612f', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 746580, u'sha256': u'601635482a9b1864ea0c61ce0282c5c9fe1d014aa95dbb4f60770f1c2b6df3da', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 746888, u'sha256': u'2bf742d2beb4c56dd6eb68347dd8ee28da85bed9e6d165b36c6edb91da01d5d6', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 747196, u'sha256': u'cfc4ff9e46fbb61f61b68f36adc6593b137233d1cbaa50fe37e5653f0cb20396', u'type': u'AmigaOS bitmap font', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 747504, u'sha256': u'c4a6e3a7a346baecb09a0c49268eb44f388382a7866a4e912b53d48fa3b34c26', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 747812, u'sha256': u'f273e554605a89aa0994c9d42bc2569be3db5b19b2900dacb30f3218ed1174a0', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_CURSOR', u'offset': 748120, u'sha256': u'ebaf4bcc0f0d7ca9a3458ea52520d2dd10811069241940b9b2e79ac1a4c3ca5c', u'type': u'data', u'size': 308}

{u'lang': u'LANG_CHINESE', u'name': u'RT_BITMAP', u'offset': 748428, u'sha256': u'e7c0005285d1ab59732d5f99f77a9bdd6342b01cf44437ebd7a07611a227e272', u'type': u'data', u'size': 184}

{u'lang': u'LANG_CHINESE', u'name': u'RT_BITMAP', u'offset': 748612, u'sha256': u'abdf36bde89a26349f5741c17c235dacea88d441d8662ba16a598dc50c3c4864', u'type': u'data', u'size': 324}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 748936, u'sha256': u'05c4d2ec84ef7f0ef21db5558b2b4b38977eba67ceaf52a34cba468d241e6cbf', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 758576, u'sha256': u'25a76a2d180f303b3599f7c0da83331dc4e4a21c687e1f669d6f24a9336a7412', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 762840, u'sha256': u'1d8a6b7161000c263b8349616b9755d43bbfa091c3b921ccd92c05628d9b20cc', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 766592, u'sha256': u'b3d2f76a4ceaa009e6616c0ceffc4be54e3783013153ef0a2fbee195eadc80d1', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0', u'size': 2216}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 768808, u'sha256': u'82f4b021e1bd75acf672a9834e936daf9328d180e1c6966851d2c013c0440828', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 770192, u'sha256': u'b8caf31abb558a2d10de18c134a83a5ccef415f74e8eca52779368631d9a9db7', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0', u'size': 16936}

{u'lang': u'LANG_CHINESE', u'name': u'RT_ICON', u'offset': 787128, u'sha256': u'341731910e0a5b84c7f487d76e46184f52eab80592168f013285f738fe25bc64', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0', u'size': 16936}

{u'lang': u'LANG_CHINESE', u'name': u'RT_MENU', u'offset': 804064, u'sha256': u'949cc29a0310738bea239aed316511bb7757e7111e6b477881f7694331a4a51b', u'type': u'data', u'size': 38}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 804104, u'sha256': u'a50db414b09c1bec4ee47d67eac0ee8e1c4601b215690913cf0a672cccf10f5c', u'type': u'data', u'size': 452}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 804556, u'sha256': u'66ab8e8fa818c5cf74d0340ca85582a6e3abbfd476c28090aa94f9932471fccf', u'type': u'data', u'size': 64}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 804620, u'sha256': u'90c705f3841b7f8f247892ff0fd22da9c982ced271c55ebdbac29c85a1c28389', u'type': u'data', u'size': 128}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 804748, u'sha256': u'3a4a9823e8de46e3b9a7a5f5762993a3fd31d317a3b655ad1a6eb0044e4512c7', u'type': u'data', u'size': 64}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 804812, u'sha256': u'f83ffd01e9c400d0cff9013e0b2d4418e63659161d25d5b1f427bf0d5874a11f', u'type': u'data', u'size': 674}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 805488, u'sha256': u'f7ef2b579cd4e3c5c8754576d05a7ffaf865dc903a03befab8b1fd66c9af4fef', u'type': u'data', u'size': 340}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 805828, u'sha256': u'2d229549f89aa2eb7b5b621dcb85c742545a5b11746602150da53bfd564c59ad', u'type': u'data', u'size': 236}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 806064, u'sha256': u'db53b00f6b9e930c1d594144050d5c0045135117eff378647ffdc531c2a0113c', u'type': u'data', u'size': 272}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 806336, u'sha256': u'77895e51080706684c91ac02268f16ed2ad4446e6b2071eeaeca1f0339a26e6f', u'type': u'data', u'size': 248}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 806584, u'sha256': u'7e5191bab80af2c78f29dae1cad6fcf7506764cabfc10c192a084467f463df38', u'type': u'data', u'size': 160}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 806744, u'sha256': u'353b57d20affbcd31bdf0a178908c6ea9da1c946d5640c9f7756a7f449fd5367', u'type': u'data', u'size': 226}

{u'lang': u'LANG_CHINESE', u'name': u'RT_DIALOG', u'offset': 806972, u'sha256': u'4cf716efaf68e0cb2ec45ec55d291050b5712b05653cae68edbb999f803d2a98', u'type': u'data', u'size': 52}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807024, u'sha256': u'e77a1ed3d619c4e4fb3de20099b75815fe20431054a19a482a50b44c2501e2a1', u'type': u'data', u'size': 48}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807072, u'sha256': u'e50abe9e576863e28df1bf2dc8bae89544584f44a1a114153e415d7a457f6e9c', u'type': u'data', u'size': 78}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807152, u'sha256': u'0b985f127b9074f92daf51979d1228e8d0657682ed064beed98015d6775e51d0', u'type': u'data', u'size': 44}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807196, u'sha256': u'5b41d86b170186f3cb999332ffae3e1bb4f717be0ce2ab4468bc79d7901ec1f1', u'type': u'data', u'size': 130}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807328, u'sha256': u'31afe886bb0c4bc55f7dedcecdd95601a6eefc47659b84321695d3a5d661ec3e', u'type': u'data', u'size': 470}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 807800, u'sha256': u'af5537af3d5641f486810865a93e60685eb891d58f08477adac9341f445355f6', u'type': u'data', u'size': 352}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 808152, u'sha256': u'eaee7fb309db9597ac6d4ad9914d43b5e4c75e29436c03ca3241449896e03cbc', u'type': u'data', u'size': 302}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 808456, u'sha256': u'c8cf3e86cd7fd3d126ba6c9843ff828c9bfab14afbb4412ebc6b938a8409aa94', u'type': u'data', u'size': 80}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 808536, u'sha256': u'9bd4eeed471487a085e6110420ef8d431c6887462eb0e937d6c884fbacd28c35', u'type': u'data', u'size': 68}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 808604, u'sha256': u'6347c6bf725359f0435b5190a3eaabf89c4111f338fb65262a273bd6edb73026', u'type': u'data', u'size': 104}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 808708, u'sha256': u'0b22c4d87f0f2152a673de6cbe82a6d9ecd2cededa325f2c67b8bdd39dfcfe36', u'type': u'data', u'size': 440}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 809148, u'sha256': u'1c806d9529f405be19f24828057733b5d830cba2d2b9a1312e52ae2a0c545ce5', u'type': u'data', u'size': 260}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 809408, u'sha256': u'298bdbb59a971aa600d946281bc55d55617b30ef295770ead2a6b824c42951e7', u'type': u'data', u'size': 36}

{u'lang': u'LANG_CHINESE', u'name': u'RT_STRING', u'offset': 809444, u'sha256': u'46d9ceb8b1ca79c858a88288e59f7865b85e1788f2fe15eed3b6e3d1f7863a6b', u'type': u'data', u'size': 48}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809492, u'sha256': u'8da86e16c783fd7da06c1b57abcf523939f9df40dee03786cbb00e2bf63d1cd8', u'type': u'MS Windows cursor resource - 2 icons, 32x256, hotspot @1x1', u'size': 34}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809528, u'sha256': u'ef309b720f166673cad840a88e7636e9161ad91415cc7c176010cebba07757e5', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809548, u'sha256': u'9c17b4621412d6ded24a76aed74d4425ae61f86b6d4092ca1e28ca66b7c71399', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809568, u'sha256': u'a2f0549cca7170ae03ba042464efe62365fba38c20049e439871c9e5ce0f914f', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809588, u'sha256': u'8a495f17bc472bfc5e6923d9efa687848fac027ad60694f9c3f10a4f7b194924', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809608, u'sha256': u'3f02dcac38fffe306e1825846e2bc0458ee712696310d051e3a69ebda8330cc3', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809628, u'sha256': u'28b8110695851e5280ff55cb78507b03e8b74dd370b8e122179c82b56f7e5f37', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809648, u'sha256': u'12a5b9052dd16bed260343bc4352d436167c991c54497c5af441304646549386', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809668, u'sha256': u'a92f60b25322592e7ddd13d88e4006c097666f4d87c8cb0c21ffdccd53b31d78', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809688, u'sha256': u'4ecc7f2578fd7b137c04f85ffcbd67d6eab0bc8b1df4246cebd2a2aa517f3c60', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809708, u'sha256': u'ee63d4681e7622067fd29005c6cc67b456031eb723c7239f05f1cb097af0ef98', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809728, u'sha256': u'da738753c27f2708bd2257f8cac3385a4ccb0df1341b76acfda07fa980cfb4bd', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809748, u'sha256': u'b328fe22a904a2e7e1341a95dbf00e2fdffc9ab350bc64c5ee348d3007c2b479', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809768, u'sha256': u'8f51832638675f16ec5f251ab59251b3f85d84e5129025d44c45b3191b331c58', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_CURSOR', u'offset': 809788, u'sha256': u'6c2ef97bca5cdc6aa6de65b1f1ae8328bcb3494a16025eee870231d991e2cd56', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 809808, u'sha256': u'09dac47bf8de8ec306bc2142e09852166c75507781acc0f15385b300a3086ed0', u'type': u'MS Windows icon resource - 1 icon, 64x64', u'size': 22}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 809832, u'sha256': u'45a49bbb1c7c31038f9134c98604739dade19b7128608fbf3cc511ea116a7469', u'type': u'MS Windows icon resource - 2 icons, 48x48', u'size': 34}

{u'lang': u'LANG_CHINESE', u'name': u'RT_GROUP_ICON', u'offset': 809868, u'sha256': u'65db4355163d175cfe23714da4f21df3ee3576af2bd8b97f2210e37f12b72135', u'type': u'MS Windows icon resource - 3 icons, 48x48', u'size': 48}

{u'lang': u'LANG_CHINESE', u'name': u'RT_VERSION', u'offset': 809916, u'sha256': u'955f1c0fb8a62ea0e0b2215322bec06bd58514d2804788957200737d5acf0e8a', u'type': u'data', u'size': 1916}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 811832, u'sha256': u'7adafc350f7d7969a17f134f00b95b9f453051a23ceca97d55d1e932e62fb9b6', u'type': u'ASCII text, with CRLF line terminators', u'size': 633}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS