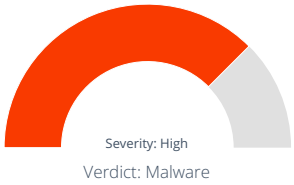
VALKYRIE COMODO

Summary

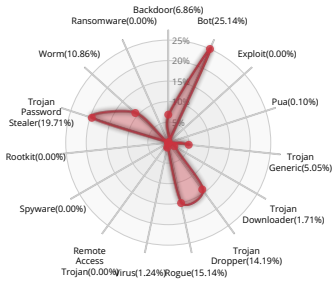
File Name: exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 10f5a1e5338f23e5fef246e0c1cf517f637e7109
MD5: d8c9f4b0ed094c10b66d509deddd5dac

MALWARE
Valkyrie Final Verdict

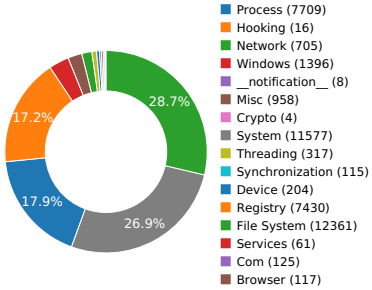
DETECTION SECTION



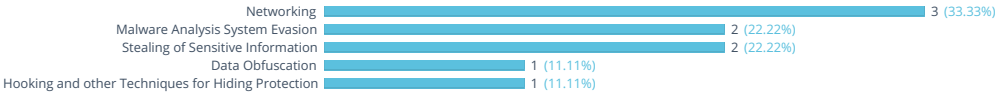
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

DATA OBFUSCATION

- Unconventionial binary language: Chinese (Simplified)

NETWORKING

- Attempts to connect to a dead IP:Port (11 unique times) Show sources
- Starts servers listening on 127.0.0.1:0
- Performs some HTTP requests Show sources

MALWARE ANALYSIS SYSTEM EVASION

- Tries to unhook or modify Windows functions monitored by Cuckoo Show sources
- Attempts to repeatedly call a single API many times in order to delay analysis time Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

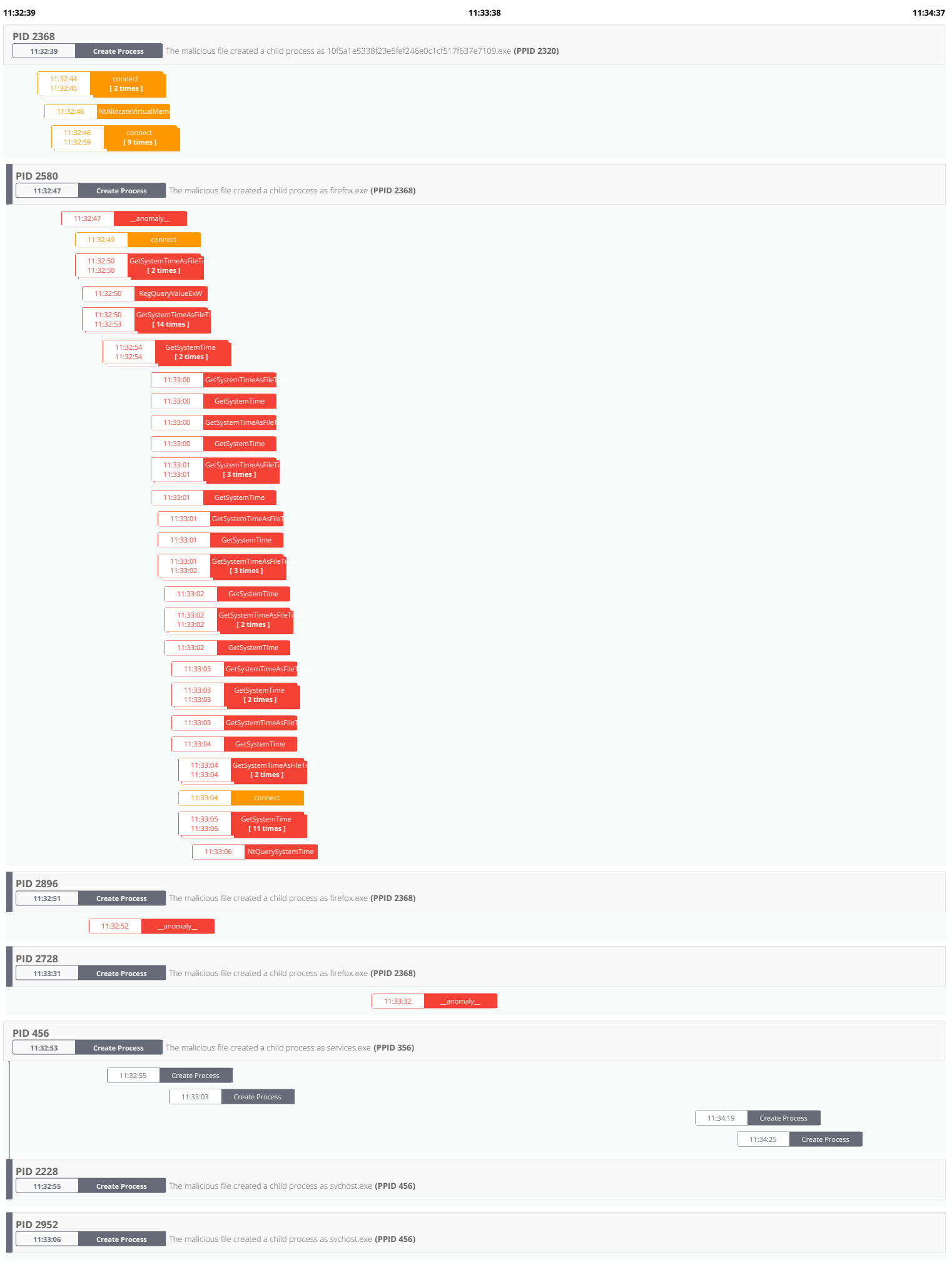
- Creates RWX memory Show sources

STEALING OF SENSITIVE INFORMATION

- Collects information to fingerprint the system Show sources
- Attempts to modify proxy settings

VALKYRIE COMODO

Behavior Graph



PID 1080

11:34:33	Create Process	The malicious file created a child process as mscorsvw.exe **(PPID 456)**

PID 2752

11:34:37	Create Process	The malicious file created a child process as mscorsvw.exe **(PPID 456)**

PID 588

11:33:02	Create Process	The malicious file created a child process as svchost.exe **(PPID 456)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\10f5a1e5338f23e5fef246e0c1cf517f637e7109.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Users\user\AppData\Local\Temp\~DFFCD0FC3DBC0607A7.TMP
C:\Windows\Fonts\staticcache.dat
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\10f5a1e5338f23e5fef246e0c1cf517f637e7109.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp*.*
C:\Users\user\AppData\Local\Temp\\xc3\x90\xc3\x85\xc2\x8f\x02*.w3g
C:\Users\user\AppData\Local\Temp*.w3g
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
C:\Windows\SysWOW64\stdole2.tlb
C:\Windows\SysWOW64\ieframe.dll
C:\Users\user\AppData\Local\Temp\ieframe.dll
C:\Windows\System32\ieframe.dll
C:\Windows
C:\Windows\System32
C:\Windows\System32\ieframe.dll:Zone.Identifier
C:\Windows\WindowsShell.manifest
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\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\navcancl[1]
C:\Users\user\AppData\Local\Temp\WH_Set.ini
C:\Users\user\AppData\Local\Temp\KeyDim
C:\Users\user\AppData\Local\Temp\Chat
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
\??\Nsi
E:\Warcraft III\war3.exe
C:\war3.exe
C:\Users\user\AppData\Local\Temp\war3.exe
C:\Users\user\AppData\Local\war3.exe
E:\
C:\Users\user\AppData\Local\Temp\10f5a1e5338f23e5fef246e0c1cf517f637e7109.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\WHAD[1].htm
C:\Windows\System32\en-US\MLANG.dll.mui
C:\Windows\sysnative\C_1256.NLS
C:\Windows\sysnative\C_864.NLS
C:\Windows\sysnative\C_708.NLS
C:\Windows\sysnative\C_720.NLS
C:\Windows\sysnative\C_28596.NLS
C:\Windows\sysnative\C_10004.NLS
C:\Windows\sysnative\C_1257.NLS
C:\Windows\sysnative\C_775.NLS
C:\Windows\sysnative\C_28594.NLS
C:\Windows\sysnative\C_1250.NLS
C:\Windows\sysnative\C_852.NLS
C:\Windows\sysnative\C_28592.NLS

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{871C5380-42A0-1069-A2EA-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\InProcServer32\LoadWithoutCOM
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{871C5380-42A0-1069-A2EA-08002B30309D} {000214E6-0000-0000-C000-000000000046} 0xFFFF
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NormalizeLinkNetPidls
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\System.NamespaceCLSID
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{871C5380-42A0-1069-A2EA-08002B30309D}\{28636AA6-953D-11D2-B5D6-00C04FD918D0} 6

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\~DFFCD0FC3DBC0607A7.TMP

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:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\navcancl[1]

C:\Users\user\AppData\Local\Temp\WH_Set.ini

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\WHAD[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\s[1].htm

C:\Users\user\AppData\Roaming\Adobe\Flash Player\NativeCache\NativeCache.directory

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\s[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\v[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\stats[1].htm

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\WHAD[1].gif

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\stat[1].php

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\stat[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\core[1].php

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\pic[1].gif

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019061120190612\index.dat

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\parent.lock

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cert8.db

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\key3.db

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\5284

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\permissions.sqlite

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-wal

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\places.sqlite-shm

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\content-prefs.sqlite

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs.js

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-wal

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\cookies.sqlite-shm

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps.json

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json

C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\formhistory.sqlite

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat

C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenservicelock.dat

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat

RESOLVED APIS

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

oleaut32.dll.OleLoadPictureEx

oleaut32.dll.DispCallFunc

oleaut32.dll.LoadTypeLibEx

oleaut32.dll.UnRegisterTypeLib

oleaut32.dll.CreateTypeLib2
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.VarNumFromParseNum
oleaut32.dll.VarParseNumFromStr
oleaut32.dll.VarDecFromR4
oleaut32.dll.VarDecFromR8
oleaut32.dll.VarDecFromDate
oleaut32.dll.VarDecFromI4
oleaut32.dll.VarDecFromCy
oleaut32.dll.VarR4FromDec
oleaut32.dll.GetRecordInfoFromTypeInfo
oleaut32.dll.GetRecordInfoFromGuids
oleaut32.dll.SafeArrayGetRecordInfo
oleaut32.dll.SafeArraySetRecordInfo
oleaut32.dll.SafeArrayGetIID
oleaut32.dll.SafeArraySetIID
oleaut32.dll.SafeArrayCopyData
oleaut32.dll.SafeArrayAllocDescriptorEx
oleaut32.dll.SafeArrayCreateEx
oleaut32.dll.VarFormat
oleaut32.dll.VarFormatDateTime
oleaut32.dll.VarFormatNumber
oleaut32.dll.VarFormatPercent
oleaut32.dll.VarFormatCurrency
oleaut32.dll.VarWeekdayName
oleaut32.dll.VarMonthName
oleaut32.dll.VarAdd
oleaut32.dll.VarAnd
oleaut32.dll.VarCat
oleaut32.dll.VarDiv
oleaut32.dll.VarEqv
oleaut32.dll.VarIdiv
oleaut32.dll.VarImp
oleaut32.dll.VarMod
oleaut32.dll.VarMul
oleaut32.dll.VarOr
oleaut32.dll.VarPow
oleaut32.dll.VarSub
oleaut32.dll.VarXor
oleaut32.dll.VarAbs
oleaut32.dll.VarFix
oleaut32.dll.VarInt
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarRound
oleaut32.dll.VarCmp
oleaut32.dll.VarDecAdd
oleaut32.dll.VarDecCmp
oleaut32.dll.VarBstrCat
oleaut32.dll.VarCyMulI4
oleaut32.dll.VarBstrCmp

ole32.dll.CoCreateInstanceEx
ole32.dll.CLSIDFromProgIDEx
sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayMonitors
user32.dll.GetMonitorInfoA
ole32.dll.CLSIDFromOle1Class
clbcatq.dll.GetCatalogObject
clbcatq.dll.GetCatalogObject2
kernel32.dll.OpenEventA
kernel32.dll.CreateEventA
comctl32.dll.InitCommonControlsEx
kernel32.dll.GetCurrentProcess

DELETED FILES

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012016042520160426\
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.log
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index.tmp
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\doomed\5284
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\prefs-1.js
C:\Users\user\AppData\Roaming\Mozilla\Firefox\Profiles\jdm2a1on.default\webapps\webapps-1.json
C:\Users\user\AppData\Local\Temp\mozilla-temp-files
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\cache2\index
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-trackwhite-simple.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-unwanted-simple.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-unwanted-simple.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-badbinurl-shavar.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-badbinurl-shavar.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-badbinurl-shavar.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-downloadwhite-digest256.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-downloadwhite-digest256.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-downloadwhite-digest256.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-malware-shavar.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-malware-shavar.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-malware-shavar.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-phish-shavar.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-phish-shavar.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-phish-shavar.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-unwanted-shavar.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-unwanted-shavar.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\goog-unwanted-shavar.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-track-digest256.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-track-digest256.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-track-digest256.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-trackwhite-digest256.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-trackwhite-digest256.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\mozstd-trackwhite-digest256.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-forbid-simple.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-forbid-simple.pset

C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-forbid-simple.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-malware-simple.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-malware-simple.pset
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-malware-simple.sbstore
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-phish-simple.cache
C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles\jdm2a1on.default\safebrowsing\test-phish-simple.pset

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
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\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors
HKEY_CURRENT_USER\Software\Classes
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\COM3\Com+Enabled
HKEY_CURRENT_USER\Software\Classes\CLSID\{C68A7B52-747D-498F-90BB-19A23391265D}
HKEY_LOCAL_MACHINE\Software\Microsoft\OLE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE\MaxSxSHashCount
HKEY_CURRENT_USER\Software\Classes\CLSID\{BFB11B28-57B8-4F8A-8EDE-FB22EFE49A2F}
HKEY_CURRENT_USER\Software\Classes\CLSID\{82C35F50-0C28-490B-BC69-37BB73315DB8}
HKEY_CURRENT_USER\Software\Classes\CLSID\{7DC3FB3D-FDDC-489F-AE3A-A79C482C0408}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\10f5a1e5338f23e5fef246e0c1cf517f637e7109.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT\UserEra
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Policies\Microsoft\Control Panel\International\Calendars\TwoDigitYearMax
HKEY_CURRENT_USER\Control Panel\International\Calendars\TwoDigitYearMax
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\SimSun\Plane16
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\System
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Arial
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\10f5a1e5338f23e5fef246e0c1cf517f637e7109.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups

EXECUTED COMMANDS

http://mybaol.com/c.php? s=JnpvbmVpZD0xODYmc2l0ZWlkPTEyJnVpZD0xMjg1JmFkc2lkPTI3MyZwbGFuaWQ9MTY5JnBsYW50eXBlPWNwbSZ1cmw9aHR0cCUzQSUyRiUyRmJvYm8ub2lhaGRnbG0ueHl6JTJGY3BhLnBocCZ2dGltZT0yMDE5LTA2LTEwIDIzOjIyOjA1JmlwPTE5Mi4xODYuMT
http://mingwangedu.com/c.php? s=JnpvbmVpZD0xOTImc2l0ZWlkPSZ1aWQ9MTM0NSZhZHNpZD0zODcmcGxhbmlkPTI1NiZwbGFudHlwZT1jcG0mdXJsPWh0dHBzJTNBJTJGJTJGd3d3LnlhaHVpMzIzLmNvbSUyRnRpbWV2JTJGYWRfbW9kZS5odG1sJnZ0aW1lPTIwMTktMDYtMTAgMjM6Mjl6MDEr
http://mingwangedu.com/c.php? s=JnpvbmVpZD0xOTImc2l0ZWlkPSZ1aWQ9MTM0NSZhZHNpZD0zMDcmcGxhbmlkPTE5MSZwbGFudHlwZT1jcG0mdXJsPWh0dHBzJTNBJTJGJTJGd3d3LmNhbmd0dDY3Mi5jb20lMkZ0aW1ldiUyRmFkX21vZGUuaHRtbCZ0aW1lPTIwMTktMDYtMTAgMjM6MjE6MDEr
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe

READ FILES

\Device\KsecDD

C:\Users\user\AppData\Local\Temp\~DFFCD0FC3DBC0607A7.TMP

C:\Windows\Fonts\staticcache.dat

C:\Windows\System32\uxtheme.dll.Config

C:\Windows\System32\uxtheme.dll

C:\Windows\SysWOW64\shell32.dll

C:\Windows\SysWOW64\stdole2.tlb

C:\Windows\SysWOW64\ieframe.dll

C:\Windows\WindowsShell.manifest

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:\Users\user\AppData\Local\Temp\WH_Set.ini

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\WHAD[1].htm

C:\Windows\System32\en-US\MLANG.dll.mui

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\s[1].htm

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:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\s[1].htm

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\v[1].js

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\stats[1].htm

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\stat[1].php
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\core[1].php
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Microsoft
C:\Users\user\AppData\Local\Microsoft\Windows
C:\Users\user\AppData\Local\Microsoft\Windows\History\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019061120190612\index.dat
C:\Windows\System32\shell32.dll
C:\Program Files (x86)\Mozilla Firefox\mozglue.dll
C:\Windows\System32\version.dll
C:\Program Files (x86)\Mozilla Firefox\msvcr120.dll
C:\Program Files (x86)\Mozilla Firefox\msvcp120.dll
C:\Program Files (x86)\Mozilla Firefox\dependentlibs.list
C:\Program Files (x86)\Mozilla Firefox\nss3.dll

MUTEXES

Local\WininetStartupMutex
Local\ZonesCounterMutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
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\!IETld!Mutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
IESQMMUTEX_0_208
DBWinMutex
{1B655094-FE2A-433c-A877-FF9793445069}
MSIMGSIZECacheMutex
!SHMSFTHISTORY!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!mshist012019061120190612!
Local\FirefoxStartupMutex
Local\MSCTF.Asm.MutexDefault1
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex

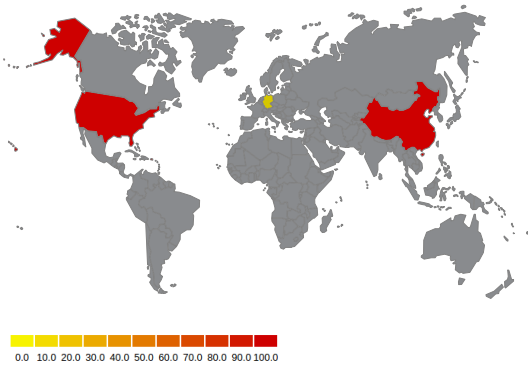
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32\EnableConsoleTracing

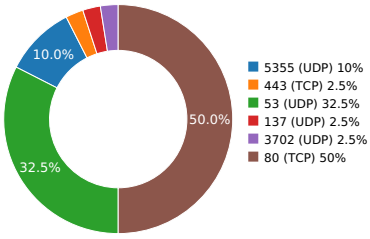
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\10f5a1e5338f23e5fef246e0c1cf517f637e7109_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\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\CpMRU
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\CpMRU\Enable
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\CpMRU\Size
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\CpMRU\InitHits
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\International\CpMRU\Factor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612\CachePath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612\CachePrefix
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612\CacheLimit
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612\CacheOptions
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012019061120190612\CacheRepair
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Type

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
	8.8.8.8	United States	15169	Level 3 Parent, LLC	Malware Process
	203.119.206.95	China	37963	Hangzhou Alibaba Advertising Co.,Ltd. No.6...	Malware Process
	222.85.26.208	China	4134	CHINANET henan province network China T...	Malware Process
mybaol.com	125.88.146.63	China	134764	CHINANET Guangdong province network C...	Malware Process
easylist-downloads.adblockplus.org	94.130.136.91	Germany	24940		Malware Process
c.cnzz.com	222.85.26.209	China	4134	CHINANET henan province network China T...	Malware Process
notification.adblockplus.org	136.243.58.99	Germany	24940		Malware Process
cloud.zyiis.net	120.26.167.216	China	37963	Aliyun Computing Co., LTD 5F, Builing D, the..	Malware Process
mingwangedu.com	125.88.146.188	China	134764	CHINANET Guangdong province network C...	Malware Process
yulv.net	47.97.218.41	China	37963	Aliyun Computing Co., LTD 5F, Builing D, the..	Malware Process
s131.cnzz.com	116.207.118.89	China	4134	CHINANET Hubei province network Data Co...	Malware Process
icon.cnzz.com	116.207.118.89	China	4134	CHINANET Hubei province network Data Co...	Malware Process
weixin0452.com	125.88.146.63	China	134764	CHINANET Guangdong province network C...	Malware Process
hzs12.cnzz.com	203.119.206.97	China	37963	Hangzhou Alibaba Advertising Co.,Ltd. No.6...	Malware Process

VALKYRIE COMODO

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
yulv.net	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	11.8648340702
Path: /WHAD.html **URI:** http://yulv.net/WHAD.html						
weixin0452.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	12.683494091
Path: /s.php?id=186 **URI:** http://weixin0452.com/s.php?id=186						
mingwangedu.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	14.2480170727
Path: /s.php?id=192 **URI:** http://mingwangedu.com/s.php?id=192						
cloud.zyiis.net	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	14.4293830395
Path: /v.js?laZwak5XnZJWIdK7ZskDSR1rVOdwoHTC2dPOFR9Y1Uw= **URI:** http://cloud.zyiis.net/v.js?laZwak5XnZJWIdK7ZskDSR1rVOdwoHTC2dPOFR9Y1Uw=						
mybaol.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	2	14.7489151955
Path: /stats.php?adsid=273&planid=169&uid=1285&siteid=&plantype=cpm&zoneid=186&adtplid=8&sep=10 **URI:** http://mybaol.com/stats.php?adsid=273&planid=169&uid=1285&siteid=&plantype=cpm&zoneid=186&adtplid=8&sep=10						
yulv.net	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	18.351984024
Path: /WHAD.gif **URI:** http://yulv.net/WHAD.gif						
s131.cnzz.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	18.3848671913
Path: /stat.php?id=1252129&web_id=1252129&show=pic **URI:** http://s131.cnzz.com/stat.php?id=1252129&web_id=1252129&show=pic						
hzs12.cnzz.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	20.3794891834
Path: /stat.htm?id=1252129&r=&lg=en-us&ntime=none&cnzz_eid=338705755-1560176988-&showp=800x600&p=http%3A%2F%2Fyulv.net%2FWHAD.html&t=WarHelper%20%E8%BD%AF%E4%BB%B6%E6%9B%B4%E6%96%B0%E4%B8%8B%E8%BD%BD%E9%A1%B5%E9%9D%A2&umuuid=16b43bac9271d2-0179f277e643774-26596759-75300-16b43bac9383d3&h=1&rnd=308552283 **URI:** http://hzs12.cnzz.com/stat.htm?id=1252129&r=&lg=en-us&ntime=none&cnzz_eid=338705755-1560176988-&showp=800x600&p=http%3A%2F%2Fyulv.net%2FWHAD.html&t=WarHelper%20%E8%BD%AF%E4%BB%B6%E6%9B%B4%E6%96%B0%E4%B8%8B%E8%BD%BD%E9%A1%B5%E9%9D%A2&umuuid=16b43bac9271d2-0179f277e643774-26596759-75300-16b43bac9383d3&h=1&rnd=308552283						
c.cnzz.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	2	23.3054060936
Path: /core.php?web_id=1252129&show=pic&t=z **URI:** http://c.cnzz.com/core.php?web_id=1252129&show=pic&t=z						
icon.cnzz.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT...	1	27.216397047
Path: /img/pic.gif **URI:** http://icon.cnzz.com/img/pic.gif						

DNS QUERIES

Request	Type
yulv.net	A
Answers - 47.97.218.41 (A)	
weixin0452.com	A
Answers - 125.88.146.63 (A)	
mingwangedu.com	A
Answers - 125.88.146.188 (A)	
s131.cnzz.com	A
Answers - all.cnzz.com.danuoyi.tbcache.com (CNAME) - c.cnzz.com (CNAME) - 116.207.118.89 (A) - 116.207.118.90 (A)	
mybaol.com	A
cloud.zyiis.net	A
Answers - 120.26.167.216 (A)	
hzs12.cnzz.com	A
Answers - z8.cnzz.com (CNAME) - z.cnzz.com (CNAME) - z.gds.cnzz.com (CNAME) - 203.119.206.95 (A)	
c.cnzz.com	A
Answers - 222.85.26.209 (A) - 222.85.26.208 (A)	
icon.cnzz.com	A
Answers - icon.cnzz.com.danuoyi.tbcache.com (CNAME)	
notification.adblockplus.org	A
Answers - 148.251.238.203 (A) - 78.46.39.215 (A) - 94.130.73.103 (A) - 95.216.27.38 (A) - 95.216.14.30 (A) - 94.130.168.30 (A) - 195.201.59.236 (A) - easylist-downloads.adblockplus.org (CNAME) - 136.243.22.80 (A) - 195.201.59.241 (A) - 94.130.73.107 (A) - 195.201.59.240 (A) - 144.76.197.80 (A)	
easylist-downloads.adblockplus.org	A
Answers - 195.201.59.248 (A) - 88.99.186.153 (A) - 148.251.139.76 (A) - 94.130.73.112 (A) - 85.10.210.166 (A) - 88.99.186.150 (A) - 95.216.27.30 (A) - 144.76.219.20 (A) - 46.4.115.44 (A) - 88.99.186.155 (A) - 94.130.104.88 (A) - 94.130.136.91 (A)	
easylist-downloads.adblockplus.org	AAAA
Answers - 2a01:4f9:2a:e97::2 (AAAA) - 2a01:4f8:200:9218::2 (AAAA) - 2a01:4f8:171:1945::2 (AAAA) - 2a01:4f9:2a:e61::2 (AAAA)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
11.8648340702	Sandbox	47.97.218.41	80
12.683494091	Sandbox	125.88.146.63	80
14.2480170727	Sandbox	125.88.146.188	80
14.4293830395	Sandbox	120.26.167.216	80
14.7489151955	Sandbox	125.88.146.63	80
18.351984024	Sandbox	47.97.218.41	80
18.3848671913	Sandbox	116.207.118.89	80
20.3794891834	Sandbox	203.119.206.95	80
23.3054060936	Sandbox	222.85.26.209	80
27.216397047	Sandbox	222.85.26.208	80
31.2662940025	Sandbox	78.46.39.215	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.02181315422	Sandbox	224.0.0.252	5355
3.03619599342	Sandbox	224.0.0.252	5355
3.04410600662	Sandbox	239.255.255.250	3702
3.07916903496	Sandbox	192.168.56.255	137
5.59934401512	Sandbox	224.0.0.252	5355
7.41896605492	Sandbox	224.0.0.252	5355
9.9896941185	Sandbox	8.8.4.4	53
10.984899044	Sandbox	8.8.8.8	53
12.1482532024	Sandbox	8.8.4.4	53
12.1488761902	Sandbox	8.8.4.4	53
12.1493401527	Sandbox	8.8.4.4	53
13.9923541546	Sandbox	8.8.4.4	53
13.9926869869	Sandbox	8.8.4.4	53
19.7239351273	Sandbox	8.8.4.4	53
19.7664341927	Sandbox	8.8.4.4	53
26.8957240582	Sandbox	8.8.4.4	53
30.7706670761	Sandbox	8.8.4.4	53
31.0598220825	Sandbox	8.8.4.4	53
31.0703251362	Sandbox	8.8.4.4	53

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\S[1].Htm	**Type :** UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators **MD5 :** 2e1cb517a9d7d28cb585909742c47c22 **SHA-1 :** a02d361bfcd136b7f3e05a7eeb817fda178376a1 **SHA-256 :** 7584ef64753e3e96524ce9fed21423f3b9113c47be1a5e2941e28a2ab6dfb475 **SHA-512 :** efc699ecdc572a02a0f67b276118bc2fb8d87e361b945f727d4ef3427124d5df45705fa **Size :** 24.199 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cookies.Sqlite-Shm	**Type :** FoxPro FPT, blocks size 0, next free block index 417475840 **MD5 :** b7c14ec6110fa820ca6b65f5aec85911 **SHA-1 :** 608eeb7488042453c9ca40f7e1398fc1a270f3f4 **SHA-256 :** fd4c9fda9cd3f9ae7c962b0ddf37232294d55580e1aa165aa06129b8549389eb **SHA-512 :** d8d75760f29b1e27ac9430bc4f4ffcec39f1590be5aef2bfb5a535850302e067c288ef59 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** c92862947cd92c5f099bd5be11982690 **SHA-1 :** 3979210b32df920083b399e6dbaec2f658fe3ac8 **SHA-256 :** 1778dda035853f2c741a8bd1d6cf05520c482de277a0a43224e4c73bccc31720 **SHA-512 :** bbb17876d1c5ddd17079827ca3b772541c314d9a8ce7417aa7ef4a75eb04db2a0a20 **Size :** 9.448 Kilobytes.
C:\Users\User\AppData\Local\Temp\WH_Set.Ini	**Type :** ISO-8859 text, with CRLF line terminators **MD5 :** 30520e84dcd93d3dc0dff5bae924319d **SHA-1 :** 8b8a3fe5b352fcb5c26adc9b724b50a34b77df29 **SHA-256 :** 871e17aae98f378e77d75ba2f54567666327c4bd93974fb113e289b18ff371ca **SHA-512 :** a4042663b6228edb6276e7c6d3c598312005c8623769097b19c7ec8911dc655daa288 **Size :** 1.363 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Shm	**Type :** data **MD5 :** 5b006f1b140a87d4adf020a09ba706b8 **SHA-1 :** ac428f9fe67186b10990682fd53775068f9a2267 **SHA-256 :** 1477768046d4143de5b305c4801298cc0ef6b34e28e0dc12aa76685f39f0cae0 **SHA-512 :** 798e8b6f384b8b7e879212fdf78232e6a143695c4cb1e87d61f40ba9488f08fe02f056f **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** be7e6432a32032cca4d534aaa388676d **SHA-1 :** 4858d82985bd6225a75a9d48d0058950e078e1c0 **SHA-256 :** 7d04f85ff80bce5b9b9aaa79d9c51f7bcf25c62f95f15af18d09cf1598153e86 **SHA-512 :** 3b7f497a29718863c73643fcb20f243887643e50f408bc35b2d214f5ad00fe5bdcbf0ca **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Index	**Type :** data **MD5 :** 5759064c3510519bddd7be7d28b0f97c **SHA-1 :** 876a2531dc24196c342fc1f6ed08d45dd8287c7c **SHA-256 :** 7fd86697e202fe0e78e80d40a3ca8b3af7a0d328f08ebd1934254c1052fe721d **SHA-512 :** b440311d385bedd08c1e069c05a22a2107148068905dc6385a9c7ec55f9037df29bcfa **Size :** 1.564 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\V[1].Js	**Type :** ASCII text, with very long lines **MD5 :** 297b2d897b87cbca475865fd6a12352e **SHA-1 :** 473e0ab3ebfa9bf7fff69f5766beeef256fdca08 **SHA-256 :** fa3e6b22b0dafb2f952dd9823138f0b56fff4e8389a321b144ac1b9dfee714a4 **SHA-512 :** 012d03f4ef2455992aa40192d7ab911c7b6c8f6c3bb76b79d199b68d4c78c03be1eb6 **Size :** 0.668 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Stat[1].Htm	**Type :** ASCII text, with no line terminators **MD5 :** 444bcb3a3fcf8389296c49467f27e1d6 **SHA-1 :** 7a85f4764bbd6daf1c3545efbbf0f279a6dc0beb **SHA-256 :** 2689367b205c16ce32ed4200942b8b8b1e262dfc70d9bc9fbc77c49699a4f1df **SHA-512 :** 9fbbbb5a0f329f9782e2356fa41d89cf9b3694327c1a934d6af2a9df2d7f936ce83717ft **Size :** 0.002 Kilobytes.
C:\Users\User\AppData\Local\Temp\~DFFCD0FC3DBC0607A7.TMP	**Type :** Composite Document File V2 Document, No summary info **MD5 :** 9592416b1709bc63d9e0dbd273deae6f **SHA-1 :** 6ef6b8e678b400b6399e23ff4e89cd3845a6b557 **SHA-256 :** 83b44721e919079db9d321e4a4c16c0450aa796587c90fe6df6ff74ef6eb21de **SHA-512 :** 9f4e1f94cc720094517537fb25a3e519f3f83aaecbe0a4f3cb7a58b9e2721def7411092l **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Core[1].Php	**Type :** HTML document, ASCII text, with very long lines, with no line terminators **MD5 :** 9a91299f264f7bd00aedcb2fa8ebc7a1 **SHA-1 :** e29eeed8dd37a2513ccaa86b63e31896272721d4 **SHA-256 :** 8b42822cae55a6c5f602f8f73bc34bb90590cfdbc7661bf58e76b837be03c0ca **SHA-512 :** 4939452cf2ef80a613b812a61c26a693ea4379f8939bad585591c2578a6e536487eb0a **Size :** 0.971 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cert8.Db	**Type :** Berkeley DB 1.85 (Hash, version 2, native byte-order) **MD5 :** 50ff25de86f5f7bcd65bc60c4059fd7d **SHA-1 :** b029db04627107832dcdb12616fc13aafe16006c **SHA-256 :** 0dad261c0fc847969ba5b00beebcd0faea34ef637cdba8b765e39e806b59ca51 **SHA-512 :** 456c1a16726d6f266a233774b9d0745f6225a5a3460d50cb932433e24e782fd59542cl **Size :** 147.456 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Pic[1].Gif	**Type :** GIF image data, version 89a, 50 x 12 **MD5 :** bcdd9aa92c5876f207f70567d101a896 **SHA-1 :** 786c52002f857fcbff04a5781ec35792be11af4a **SHA-256 :** 98a4ab97e12555ab969012d151a578dae7a3b8699d202485fcf8116e55497735 **SHA-512 :** d320d7d860ad61f2ecdd76fb932ee4cf9c5f8b893eff26b57df065f64efd06a563957abl **Size :** 0.719 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\S[1].Htm	**Type :** UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators **MD5 :** bf51252c80c4a359551471dba779d72f **SHA-1 :** df3666ab73c322bc9b2c42540762c17ece8394d4 **SHA-256 :** 2f6e854926e320ed727717b301ddb580178b7f2e249da832a18b3d9c38f7ba7a **SHA-512 :** 9444f4ec6af022130afda313967a453c11e48431bb07055045854941027b0c40d48cc3 **Size :** 15.609 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012019061120190612\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** f4298964d5c9cdff027f81204ebb121e **SHA-1 :** a210012a345d0df4c0ec1da1855da318bd3f8dd0 **SHA-256 :** 1850605580db0c200422bb201e774fe79f5ecd32b93ef5ad78bdbe68a0494158 **SHA-512 :** 379b44adaa0624c553d7e24b87d263b62f050780610a3c80e242f14593e0b938a6a86 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Stat[1].Php	**Type :** ASCII text, with very long lines **MD5 :** a0ef1be69aef18e1f3ab55f567d7ba75 **SHA-1 :** 9abaa6ba2891c70ce201964dbd1923695f913ee9 **SHA-256 :** 99c819c0a4f4e29fcaed71d8b470a875bd874697d621287377ff5e934cd73d9e **SHA-512 :** b1cb402ea377c4d881e27daef636d5ef30d93efd22bcbb184009eb7aad2120675bc5b **Size :** 11.71 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V4.0.30319\Ngen_service.Log	**Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 8eb273388deca3c028a48b22d11dfc6d **SHA-1 :** 4b674889aa3cdc5485cccff79769eeae966407ee **SHA-256 :** 79c8c4f6691872851c6dd4aae2f4a357faaec1598eef91bb152f0929fe61bf48 **SHA-512 :** 133c44cd755936044621a2112520b50b5ed8297d846aa7bf28b9c7d3f0d73fb395145 **Size :** 6.329 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 :** 93ddcdc040a0c95db8d3f423e81c8faf **SHA-1 :** ef2f823496701dce8464b3db2657e382a40a6740 **SHA-256 :** 15654e6bba3d0ea4fa295b9d2890805b8ea5c9cd0290a5f92e0d89ec94b22104 **SHA-512 :** 4f98c402fbad56775fdb5fdb02578b99a70e68c05c16a8399a54ac6ec8fcb81cf7bbc91 **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Prefs.Js	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** b3ef0eea4df04b895de875350d89a14e **SHA-1 :** f8078f05ca6389bdf88f938a3eb36aef62a9027a **SHA-256 :** 9ec72a31563561dde3fa42d831cbc105cbdac465bd4ea063d17379795ae17e10 **SHA-512 :** 7e22162d0842e952bbe483a3b46cfe423c82fa843f103e2ef471ca2016306e09719857 **Size :** 15.911 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite	**Type :** SQLite 3.x database, user version 30 **MD5 :** 6a51f06cc5167870ab30a9d6f4324aca **SHA-1 :** bc256ff82b817139e245f26a4cb6c8339c21b821 **SHA-256 :** 753238b30b0bd68d98a7fd46260f4eb2496b125a1ae11df58e6b0fbbb723c311 **SHA-512 :** 7edc0670202b87f467a29f5b52ae66c028a36c5d2d67826f793f8181f09860a19ecefc1 **Size :** 10485.76 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	**Type :** FoxPro FPT, blocks size 0, next free block index 401590474 **MD5 :** 9a3251e8ecc798d13d069a8bd4384555 **SHA-1 :** c0473ba1ef3a6de845acf3e36be65da1fb68bae1 **SHA-256 :** fb8b541e2803b66ced8bab54bf129c4713db78ab82bca722645ef2338450cc74 **SHA-512 :** b365963c8a27fd6cc628f03d1ca8d55a6e5b577d46ab42b80fe6ef5858b7db17142482 **Size :** 16.384 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Places.Sqlite-Wal	**Type :** data **MD5 :** 6a636cb1859beab81c508fa2f109f647 **SHA-1 :** f1ecbd81fddd2fa9da740ef200e043efb0da6a2b **SHA-256 :** 067a74baada30b55ccdaf63a7408cd79c2294152f68cbf1e07ad42cc2644b87d **SHA-512 :** 13db5fc8e6965867af12eae0ee13ad6b040730ca202cec39caeb346247bd39452a13b **Size :** 32.824 Kilobytes.
C:\Users\User\AppData\Roaming\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Webapps\Webapps.Json	**Type :** ASCII text, with no line terminators **MD5 :** 99914b932bd37a50b983c5e7c90ae93b **SHA-1 :** bf21a9e8fbc5a3846fb05b4fa0859e0917b2202f **SHA-256 :** 44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a **SHA-512 :** 27c74670adb75075fad058d5ceaf7b20c4e7786c83bae8a32f626f9782af34c9a33c204 **Size :** 0.002 Kilobytes.
C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\Jdm2a1on.Default\Cache2\Entries\9BBE93EE66A24A6574E0B0B292F1184CC816B4A0	**Type :** data **MD5 :** 629da11093ca47985765fa456f438e1a **SHA-1 :** 60875b6c8b9ea1139964f0678f9c3ba25b206934 **SHA-256 :** 9515b2d5c1300c21a81d4e814d17012b30a296f5c63c5201b7f4735c030cd7cf **SHA-512 :** 68f138341cba19f9df532c8677723b477effa46755849d19e7d09901a9292317bed796 **Size :** 0.265 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\WHAD[1].Gif	**Type :** GIF image data, version 89a, 325 x 90 **MD5 :** 042f95d8b841273f7c1cbcdca478cb83 **SHA-1 :** f9c9e15b5f227308088743fdbcfc93fc736a780c **SHA-256 :** 18ed6fead0fefd176bc43eb7d69ab47a3c1db4fae382686e1039b88a4305ce51 **SHA-512 :** 3aade37440ff405f22fcdfad944da64cb98d03f30d29f15fc00f862f4eee065605740fda5 **Size :** 3.241 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 176c2ef4d798ef6cef922ab8b54a1c10 **SHA-1 :** 9230ff29697aa4af181f54acfd3c38151d0891ff **SHA-256 :** f813bcc021c7066c050308ce54f0a186d2a30300d28df9266f8eba4161366ef1 **SHA-512 :** f094e3657010cf5e637de92dd7c64a75efc5f25953bd750f38a2f9d9c0d0edffc7e4a429 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Navcancl[1]	**Type :** HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 4bcfe9f8db04948cddb5e31fe6a7f984 **SHA-1 :** 42464c70fc16f3f361c2419751acd57d51613cdf **SHA-256 :** bee0439fcf31de76d6e2d7fd377a24a34ac8763d5bf4114da5e1663009e24228 **SHA-512 :** bb0ef3d32310644285f4062ad5f27f30649c04c5a442361a5dbe3672bd8cb585160187 **Size :** 2.713 Kilobytes.

MATCH YARA RULES

MATCH RULES
SEH__vba
inject_thread
escalate_priv
screenshot
keylogger
win_registry
win_token
win_private_profile
win_files_operation
win_hook
Str_Win32_Wininet_Library
Str_Win32_Internet_API

STATIC FILE INFO

File Name:	exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	10f5a1e5338f23e5fef246e0c1cf517f637e7109
MD5:	d8c9f4b0ed094c10b66d509deddd5dac
First Seen Date:	2018-01-17 14:57:53.710320 (about a year ago)
Number Of Clients Seen:	4
Last Analysis Date:	2019-06-10 07:25:40.788836 (about 13 hours ago)
Human Expert Analysis Date:	2018-08-10 12:00:10.037589 (10 months ago)
Human Expert Analysis Result:	Malware

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[[54.9, u'Win32 Executable Microsoft Visual Basic 6'], [20.8, u'Win32 Executable MS Visual C++ (generic)'], [18.4, u'Win64 Executable (generic)'], [3.0, u'Win32 Executable (generic)'], [1.3, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5275C587 [Sun Nov 3 03:39:51 2013 UTC]
Translation	0x0804 0x04b0
LegalCopyright	\u96e8\u5f8b\u5728\u7ebf\u51fa\u54c1
InternalName	\u52a0\u52a0\u52a9\u624b
FileVersion	7.08
CompanyName	\u96e8\u5f8b\u5728\u7ebf
Comments	\u3000\u52a0\u52a0\u9b54\u517d\u52a9\u624b\u3000
ProductName	\u9b54\u517d\u52a0\u52a0\u52a9\u624b\u3000
ProductVersion	7.08
FileDescription	\u9b54\u517d\u52a0\u52a0\u52a9\u624b
OriginalFilename	\u52a0\u52a0\u52a9\u624b.exe
Entry Point	0x406398 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	815104
Ssdeep	6144:FT4dqlT9TwsTMfeP20vjCAoU/sqV4PX50ayZOu+G3Rk6Eb6r6B82k0DV8gmafjfO:pHD2AM0bOu+8Rk6Eb6rKjj5
Sha256	a918d14f74c9f834163e9c62102fd0fc4e478e76b9231df038923807f95ae135
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/0/f/5/10f5a1e5338f23e5fef246e0c1cf517f637e7109', u'EXE:OriginalFileName': u'\u52a0\u52a0\u52a9\u624b.exe', u'EXE:ProductName': u'\u9b54\u517d\u52a0\u52a0\u52a9\u624b\u3000', u'EXE:InternalName': u'\u52a0\u52a0\u52a9\u624b', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2019:06:10 06:57:04+00:00', u'EXE:InitializedDataSize': 69632, u'File:FileModifyDate': u'2019:06:10 06:57:04+00:00', u'EXE:FileVersionNumber': u'7.8.0.0', u'EXE:FileVersion': 7.08, u'File:FileSize': u'796 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': 7.08, u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'\u96e8\u5f8b\u5728\u7ebf', u'File:FileName': u'10f5a1e5338f23e5fef246e0c1cf517f637e7109', u'EXE:ImageVersion': 7.8, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2013:11:03 03:39:51+00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'\u96e8\u5f8b\u5728\u7ebf\u51fa\u54c1', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/0/f/5', u'EXE:FileDescription': u'\u9b54\u517d\u52a0\u52a0\u52a9\u624b', u'EXE:EntryPoint': u'0x6398', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 761856, u'EXE:Comments': u'\u3000\u52a0\u52a0\u9b54\u517d\u52a9\u624b\u3000', u'File:FileInodeChangeDate': u'2019:06:10 06:57:04+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Chinese (Simplified)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'7.8.0.0'}]
Mime Type	application/x-dosexec
Imphash	0bf37555b790fbefd247a663474ddcc6

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xb9a4c	0xba000	6.1190847931	ba4ef98081573a5aa3d5e410083f0007
.data	0xbb000	0x5dac	0x1000	0.0	620f0b67a91f7f74151bc5be745b7110
.rsrc	0xc1000	0xa955	0xb000	5.43488726884	23332a16e2800ac6cac4fb3c8913c95b

PE Imports

- MSVBVM60.DLL
  - __vbaVarSub
  - __vbaVarTstGt
  - __vbaStrI2
  - __vbaNextEachAry
  - _CIcos
  - _adj_fptan
  - __vbaVarMove
  - __vbaStrI4
  - __vbaVarVargNofree
  - __vbaAryMove
  - __vbaFreeVar
  - None
  - __vbaLateIdCall
  - __vbaLenBstr
  - __vbaStrVarMove
  - None
  - __vbaEnd
  - __vbaFreeVarList
  - _adj_fdiv_m64
  - __vbaRaiseEvent
  - __vbaFreeObjList
  - __vbaR8Sgn
  - None
  - __vbaStrErrVarCopy

- None
- _adj_fprem1
- None
- __vbaRecAnsiToUni
- None
- __vbaResume
- __vbaCopyBytes
- __vbaStrCat
- __vbaLsetFixstr
- None
- __vbaSetSystemError
- __vbaRecDestruct
- __vbaHresultCheckObj
- None
- __vbaNameFile
- None
- __vbaLenVar
- _adj_fdiv_m32
- __vbaAryVar
- __vbaAryDestruct
- None
- None
- __vbaForEachCollObj
- __vbaStrBool
- __vbaExitProc
- __vbaBoolStr
- __vbaFileCloseAll
- __vbaObjSet
- __vbaOnError
- None
- None
- _adj_fdiv_m16i
- __vbaObjSetAddref
- None
- _adj_fdivr_m16i
- __vbaVarIndexLoad
- None
- __vbaFpR4
- None
- __vbaStrFixstr
- __vbaBoolVar
- None
- __vbaStrTextCmp
- __vbaRefVarAry
- __vbaFpR8
- __vbaBoolVarNull
- _CIsin
- __vbaErase
- None
- None
- __vbaNextEachCollObj
- None
- None
- __vbaChkstk
- None
- EVENT_SINK_AddRef
- None
- None
- __vbaStrCmp
- None
- __vbaVarTstEq
- __vbaAryConstruct2
- __vbaPrintObj
- __vbaObjVar
- DllFunctionCall
- __vbaVarLateMemSt
- __vbaVarOr
- __vbaCastObjVar
- __vbaRedimPreserve
- __vbaLbound
- _adj_fpatan
- __vbaR4Var
- __vbaFixstrConstruct
- __vbaLateIdCallLd
- __vbaStrR8
- __vbaRedim
- __vbaRecUniToAnsi
- EVENT_SINK_Release
- __vbaNew
- None
- _CIsqrt
- __vbaObjIs
- EVENT_SINK_QueryInterface
- __vbaStr2Vec
- __vbaExceptHandler
- None
- __vbaStrToUnicode
- None
- None
- __vbaDateStr
- _adj_fprem
- _adj_fdivr_m64
- None
- __vbaR8ErrVar
- __vbaFailedFriend
- __vbaI2Str
- None
- None
- None
- __vbaFPException
- __vbaInStrVar
- None
- __vbaStrVarVal
- __vbaUbound
- __vbaVarCat
- __vbaCheckType
- None
- __vbaLsetFixstrFree
- __vbaI2Var
- None
- None
- None
- _CIlog

- __vbaVarLateMemCallLdRf
- __vbaVar2Vec
- __vbaInStr
- __vbaR8Str
- __vbaNew2
- _adj_fdiv_m32i
- None
- _adj_fdivr_m32i
- None
- __vbaStrCopy
- __vbaI4Str
- None
- __vbaFreeStrList
- None
- _adj_fdivr_m32
- __vbaR8Var
- None
- _adj_fdiv_r
- None
- None
- None
- None
- __vbaVarTstNe
- __vbaI4Var
- __vbaForEachAry
- __vbaVarCmpEq
- __vbaVarAdd
- __vbaLateMemCall
- __vbaAryLock
- __vbaVarDup
- __vbaStrToAnsi
- __vbaFpI2
- __vbaVarLateMemCallLd
- __vbaVarCopy
- None
- __vbaVarTstGe
- __vbaFpI4
- __vbaLateMemCallLd
- __vbaRecDestructAnsi
- None
- _Clatan
- __vbaI2ErrVar
- __vbaUI1Str
- __vbaStrMove
- __vbaCastObj
- None
- __vbaAryCopy
- __vbaR8Intl4
- __vbaStrVarCopy
- __vbaHresultCheckNonvirt
- None
- None
- _allmul
- __vbaLenVarB
- __vbaLateIdSt
- _CItan
- None
- __vbaUI1Var
- __vbaFPInt
- __vbaAryUnlock
- _Clexp
- __vbaMidStmtBstr
- None
- __vbaFreeObj
- __vbaFreeStr
- __vbaRecAssign
- None

PE Resources

{u'lang': u'LANG_CHINESE', u'name': u'WAV', u'offset': 814430, u'sha256': u'd6656b584447d385b05f85641c03c8f215e220fab1ee5ba17d098919d3a24a8c', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 48000 Hz', u'size': 4222}

{u'lang': u'LANG_CHINESE', u'name': u'WAV', u'offset': 818652, u'sha256': u'f24dea86cd3c11256e7a9e24dbabaffc5ae06e71b2051b63ee7d46c51db5fcbf', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 48000 Hz', u'size': 3246}

{u'lang': u'LANG_CHINESE', u'name': u'WAV', u'offset': 821898, u'sha256': u'914baab1b6c83c594098477f02e619f36467b804e576144cc2ef52c62a18c05a', u'type': u'RIFF (little-endian) data, WAVE audio, Microsoft PCM, 16 bit, stereo 22050 Hz', u'size': 11056}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 810678, u'sha256': u'60edaa1b794d4775cb4e13442c1a853f59352ec2dc8bf969073a56539a34fd4e', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 808462, u'sha256': u'effc78815ac386da3eac228673413967ffad956119e4810990e848eb4e2617c8', 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_NEUTRAL', u'name': u'RT_ICON', u'offset': 807078, u'sha256': u'4fb84d4c84664e0d3ac09f6092889c52db488e65675cb05841b9982eec254f43', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 797438, u'sha256': u'1c81eb3256efee730afabf3c58945249022e7934ce2c3485ecc24b0af8b88eda', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 793174, u'sha256': u'bac2731ad67b4b81dab801df765aadc375c2e00e10f65bc5dfa528e2ec132ed6', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 792046, u'sha256': u'ef6fa52fdc5ff6321a7542ac088d53508005 69fb1cfdf032e6d87af54384604c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 791956, u'sha256': u'13a94745048ef42e9d88c821bb491c0557eab5917cad289309d7fea4731150a7', u'type': u'MS Windows icon resource - 6 icons, 48x48', u'size': 90}

{u'lang': u'LANG_CHINESE', u'name': u'RT_VERSION', u'offset': 791296, u'sha256': u'c5f1d1d830d788d4e9e89582c3a96083bb8f8763b4aa739996db369a8764ef14', u'type': u'data', u'size': 660}

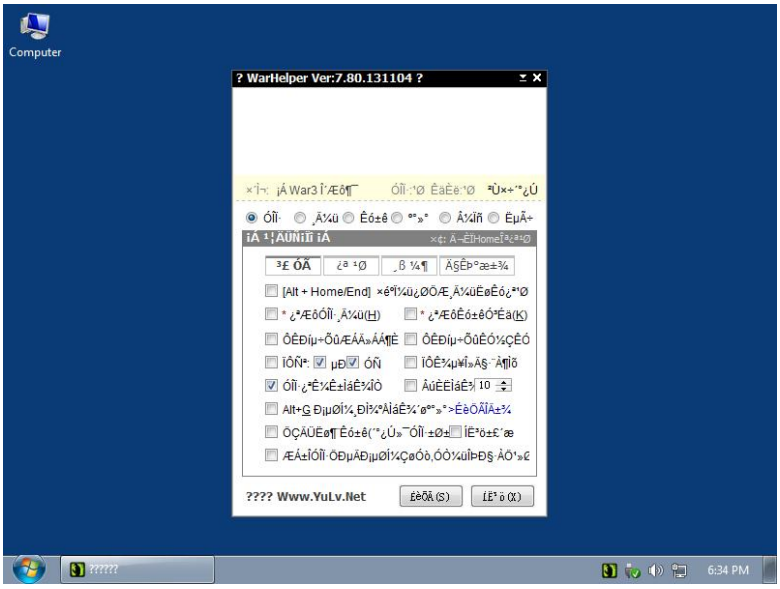
{u'lang': u'LANG_CHINESE', u'name': u'RT_MANIFEST', u'offset': 832954, u'sha256': u'737f6ffa75d9975eba77a0e5d0c9788d7f971f056f637db2b1db46b0ea0166d8', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 923}

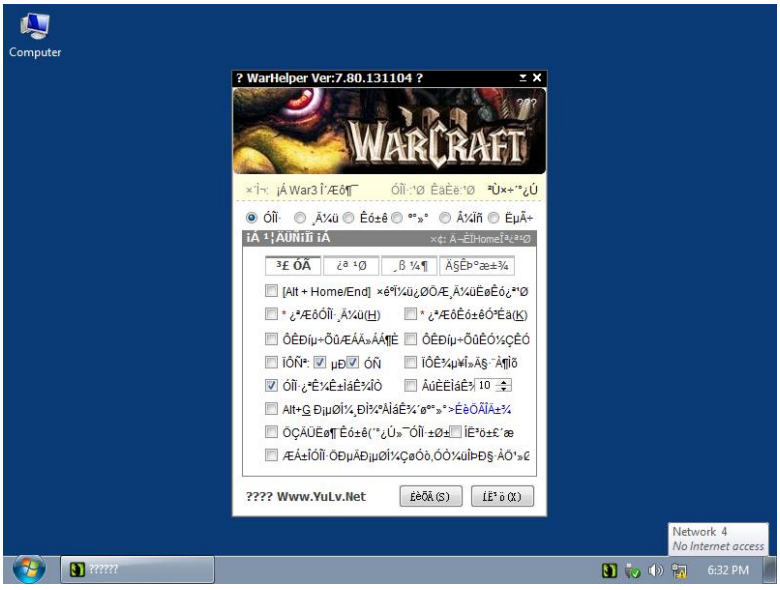
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

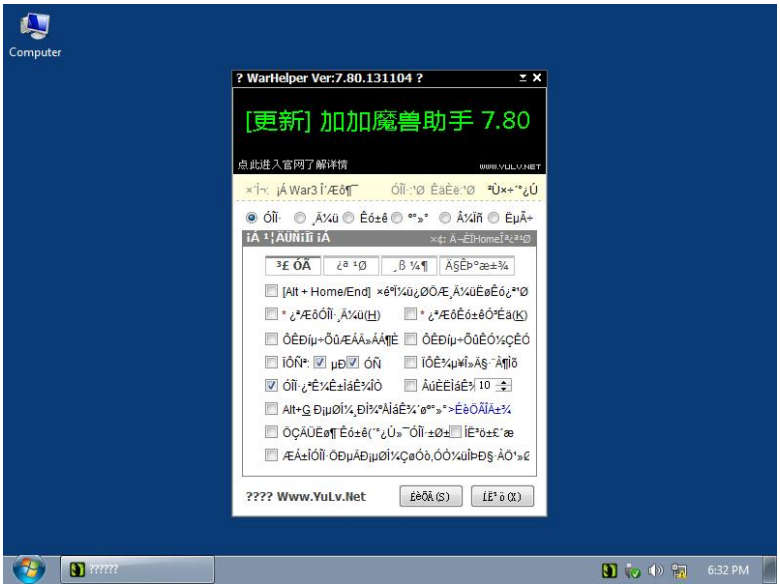
SCREENSHOTS


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
???? Www.YuLv.Net
6:34 PM


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
Network 4
No Internet access
6:32 PM

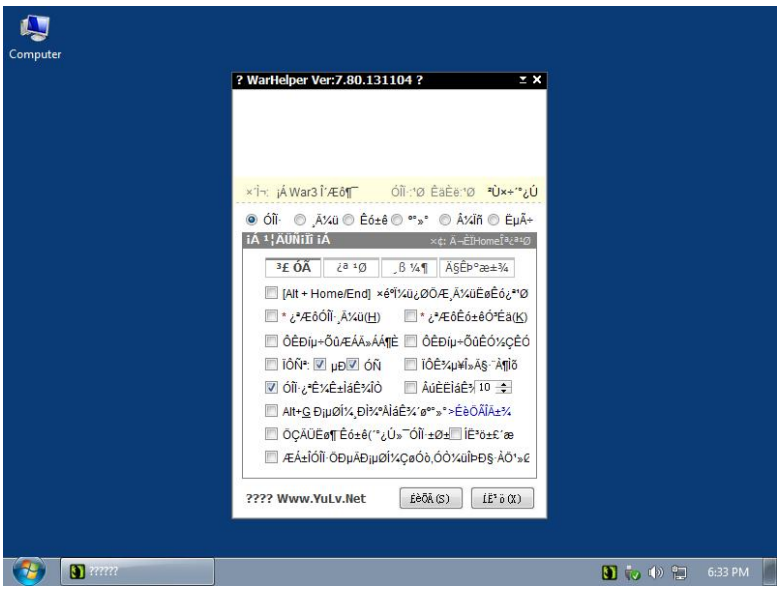

Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
[更新] 加加魔兽助手 7.80
点此进入官网了解详情
???? Www.YuLv.Net
6:32 PM

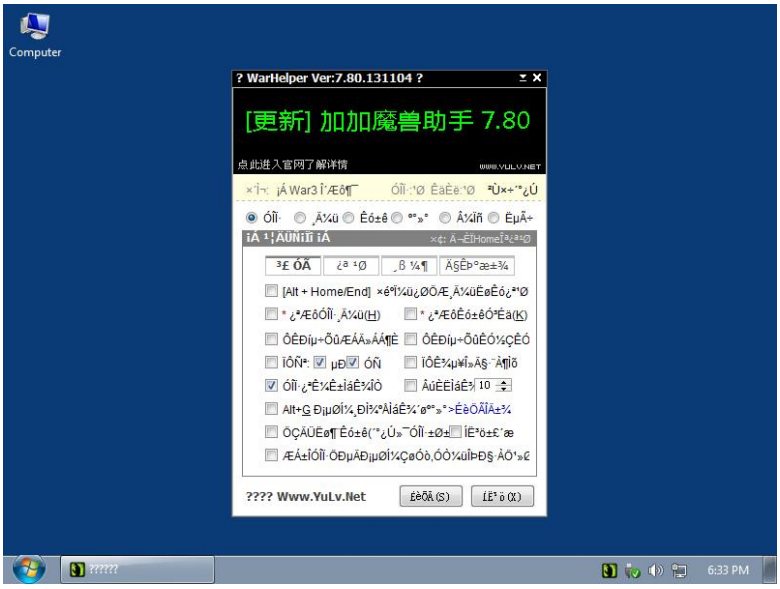

Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:32 PM


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:32 PM

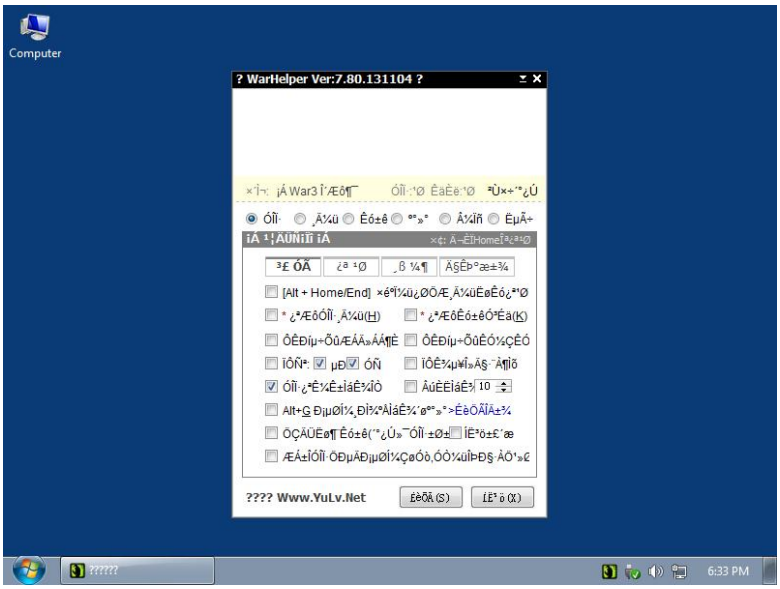

Computer
6:32 PM


Computer
? WarHelper Ver:7.80.131104 ?
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
[更新] 加加魔兽助手 7.80
点此进入官网了解详情
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:32 PM


Computer
? WarHelper Ver:7.80.131104 ?
???? Www.YuLv.Net
6:33 PM


Computer
? WarHelper Ver:7.80.131104 ?
WARCRAFT
???? Www.YuLv.Net
6:32 PM