VALKYRIE COMODO

Summary

File Name: QDzcJZLe1iVU76WU.exe

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

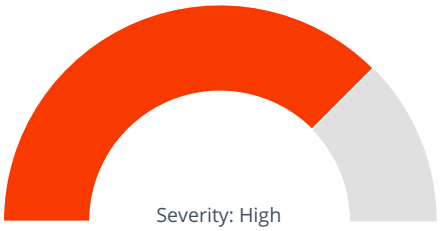
SHA1: d03dcbba9a7aeefdee2f433f4333d678a3efa87f

MD5: f53a09061f4fec4d3ee0d38b4666afff

MALWARE

Valkyrie Final Verdict

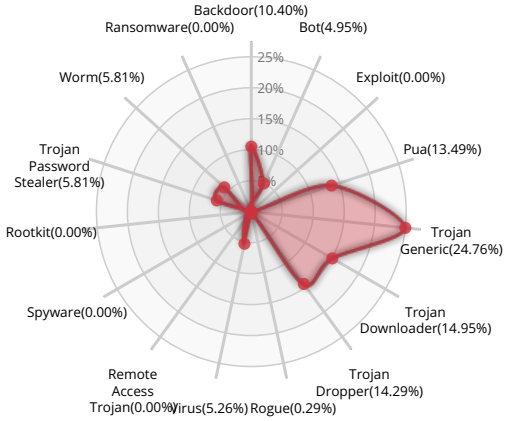
DETECTION SECTION



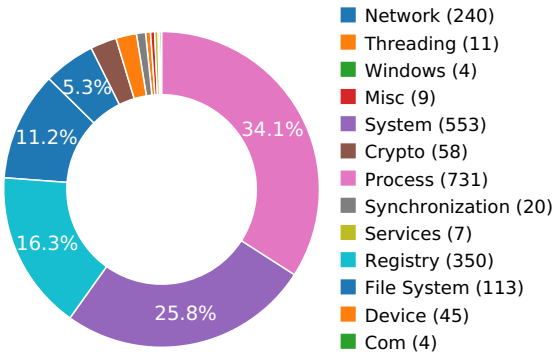
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

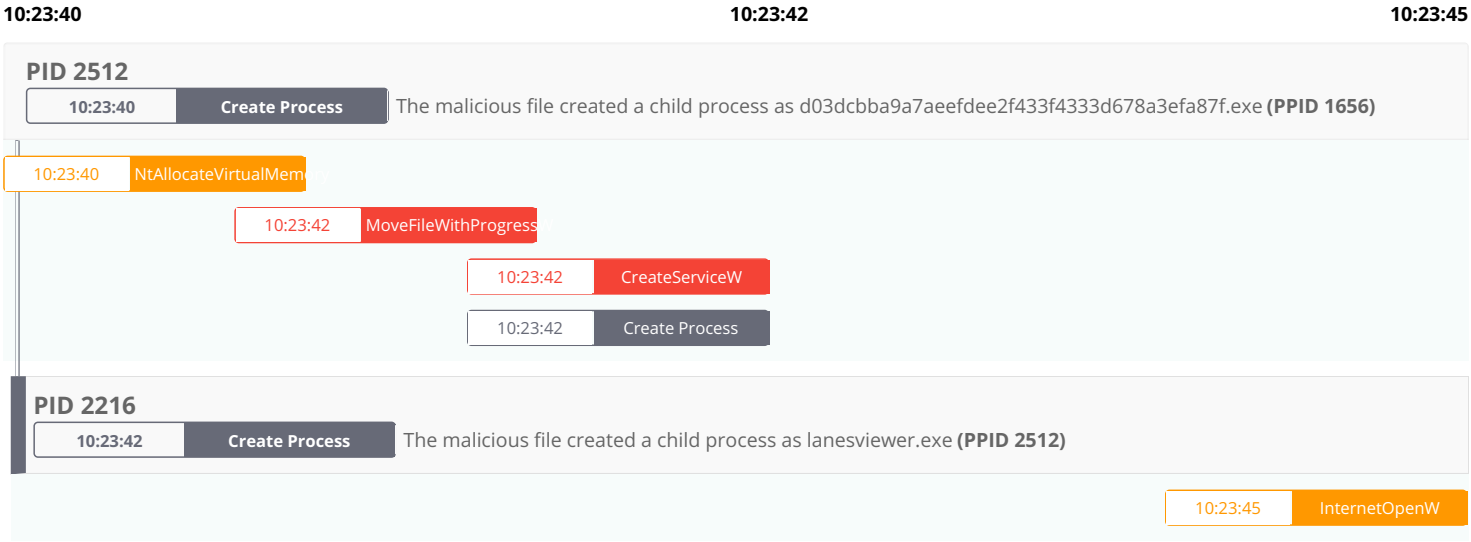
Deletes its original binary from disk	Show sources
Installs itself for autorun at Windows startup	Show sources
Created a service that was not started	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests	Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\
C:\Users\user\AppData\Local\Temp\d03dcbba9a7aeefdee2f433f4333d678a3efa87f.exe
C:\Windows\
C:\Windows\SysWOW64\
\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\lanesviewer.exe
C:\Users
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\desktop.ini
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows
C:\Windows\SysWOW64
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
\??\MountPointManager
C:\Users\user\AppData\Local\

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\NoFileFolderConnection
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\{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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\Content Type
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\SystemFileAssociations\.exe\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.exe\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\DisableProcessIsolation
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\NoOplock
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\UseInProcHandlerCache
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{66742402-F9B9-11D1-A202-0000F81FEDEE}\UseOutOfProcHandlerCache
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\DocObject
HKEY_CURRENT_USER\Software\Classes\Folder\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\BrowseInPlace
HKEY_CURRENT_USER\Software\Classes\Folder\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\BrowseInPlace

RESOLVED APIS

kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect
kernel32.dll.lstrlenA
kernel32.dll.lstrcmpA
kernel32.dll.GetTickCount
kernel32.dll.GetProcessHeap
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetCurrentProcess
kernel32.dll.GetCurrentProcessId
kernel32.dll.FreeConsole
user32.dll.wsprintfA
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
oleaut32.dll.#200
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
comctl32.dll.#385
comctl32.dll.#320
comctl32.dll.#324
comctl32.dll.#323
ole32.dll.CreateBindCtx
ole32.dll.CoTaskMemAlloc
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoGetMalloc

comctl32.dll.#328
comctl32.dll.#334
oleaut32.dll.#2
ole32.dll.CoCreateInstance
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#332
comctl32.dll.#338
comctl32.dll.#339
shell32.dll.#102
advapi32.dll.OpenThreadToken
propsys.dll.PSLookupPropertyHandlerCLSID
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryValueExW
advapi32.dll.RegCloseKey
propsys.dll.PSCreatePropertyStoreFromObject
propsys.dll.#417
propsys.dll.PropVariantToStringAlloc
ole32.dll.PropVariantClear
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PropVariantToBuffer
propsys.dll.PropVariantToUInt64
propsys.dll.PropVariantToBoolean
propsys.dll.InitPropVariantFromBuffer
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
advapi32.dll.GetNamedSecurityInfoW
advapi32.dll.TreeSetNamedSecurityInfoW
ole32.dll.CoUninitialize
comctl32.dll.#329
comctl32.dll.#388

comctl32.dll.#321
ole32.dll.CoRevokeInitializeSpy
oleaut32.dll.#500
comctl32.dll.#387
comctl32.dll.#327
advapi32.dll.UnregisterTraceGuids
cryptsp.dll.CryptReleaseContext
cryptsp.dll.CryptAcquireContextW

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\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\NoFileFolderConnection
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\d03dcbba9a7aeefdee2f433f4333d678a3efa87f.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
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
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_CLASSES_ROOT\.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\.exe\(Default)
HKEY_CLASSES_ROOT\.exe\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.exe\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts

READ FILES

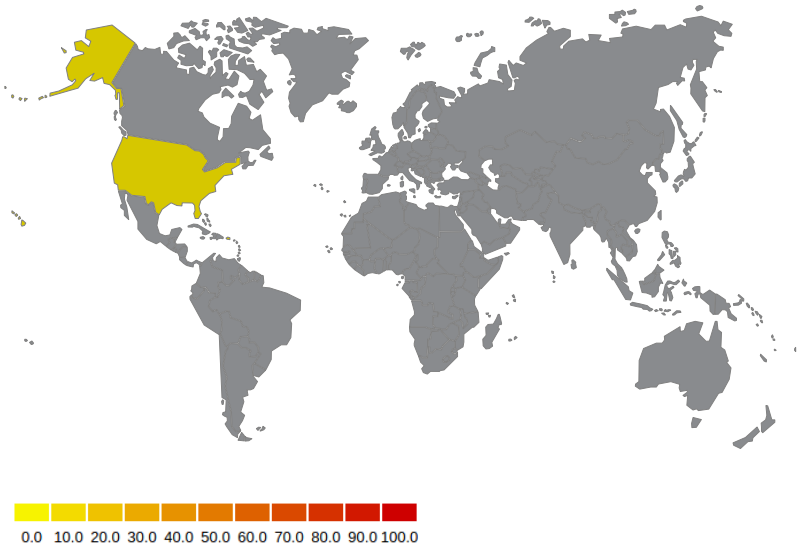
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\d03dcbba9a7aeefdee2f433f4333d678a3efa87f.exe
\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Windows
C:\Users\user\AppData\Local\Temp
C:\Windows\SysWOW64\lanesviewer.exe

MUTEXES

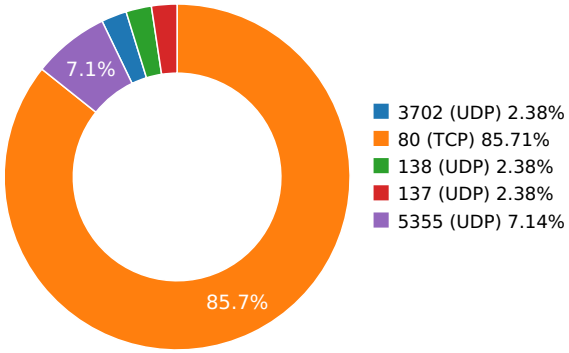
Global\I20503A4E
Global\M20503A4E
IESQMMUTEX_0_208

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	67.176.238.209	United States	7922	Comcast Cable Communications, LL...	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	10.4656751156
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	21.703756094
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	33.0028891563
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	44.7684121132
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	56.4273099899
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	67.6421639919
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	79.0946509838

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	2	90.9866621494
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	103.01799798
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	114.174648046
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	125.39447403
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	136.878725052
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	149.066890001
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	161.350558043
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	172.752249002
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	184.644629002
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	196.34694314
Path: / **URI:** http://67.176.238.209/						
67.176.238.209	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	1	208.067281961
Path: / **URI:** http://67.176.238.209/						

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
10.4656751156	Sandbox	67.176.238.209	80
21.703756094	Sandbox	67.176.238.209	80
33.0028891563	Sandbox	67.176.238.209	80
44.7684121132	Sandbox	67.176.238.209	80
56.4273099899	Sandbox	67.176.238.209	80
67.6421639919	Sandbox	67.176.238.209	80
79.0946509838	Sandbox	67.176.238.209	80
90.9866621494	Sandbox	67.176.238.209	80
103.01799798	Sandbox	67.176.238.209	80
114.174648046	Sandbox	67.176.238.209	80
125.39447403	Sandbox	67.176.238.209	80
136.878725052	Sandbox	67.176.238.209	80
149.066890001	Sandbox	67.176.238.209	80
161.350558043	Sandbox	67.176.238.209	80
172.752249002	Sandbox	67.176.238.209	80
184.644629002	Sandbox	67.176.238.209	80
196.34694314	Sandbox	67.176.238.209	80
208.067281961	Sandbox	67.176.238.209	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07475996017	Sandbox	224.0.0.252	5355
3.09413719177	Sandbox	224.0.0.252	5355
3.10365200043	Sandbox	239.255.255.250	3702
3.14366698265	Sandbox	192.168.56.255	137
5.67432308197	Sandbox	224.0.0.252	5355
9.15704202652	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	QDzcJZLe1iVU76WU.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	d03dcbba9a7aeefdee2f433f4333d678a3efa87f
MD5:	f53a09061f4fec4d3ee0d38b4666afff
First Seen Date:	2018-05-25 12:59:39.239894 (7 months ago)
Number Of Clients Seen:	9
Last Analysis Date:	2018-05-25 15:43:07.141406 (7 months ago)
Human Expert Analysis Date:	2018-05-25 15:56:39.256566 (7 months ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[]
Compilation Time Stamp	0x5B086A26 [Fri May 25 19:55:18 2018 UTC]
Entry Point	0x4016ae (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	143360
Ssdeep	
Sha256	47ae159c9b146147825f9dafb5d94dfc5f8694c1f5b1574af55034bc34391735
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x280e	0x3000	5.49242508554	b680a45d61b538587af44b66f161cd09
.rdata	0x4000	0x16f4c	0x17000	7.18349618975	f9c8d59719f1870e6bd90af19918e5ed
.data	0x1b000	0x4d70	0x4000	4.9059638774	3c9b504efda83df70c88a999883ea039
.rsrc	0x20000	0x1e48	0x2000	3.25661722631	12f9cfee27a7016b0ea3e38ca61c2eca
.reloc	0x22000	0x10e4	0x2000	4.08608098197	0f8b4b8cb637aa40056c5260f95e9ec4

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 131568, u'sha256': u'57b550be22e41c9006898353bb0d57195cfa0a9e46f29f69ce6bd4b14aedbc51', u'type': u'data', u'size': 972}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 132544, u'sha256': u'38c86ff487cfe44a65eb1ab9ef21bb72ec159ab35ffae665709b56d31e0fa9b5', u'type': u'data', u'size': 646}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 133192, u'sha256': u'4af9fd9fc86c49b96f9dcb257fd83c06e92694dec7786abf7e5693b45d3fbdb1', u'type': u'data', u'size': 576}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 133768, u'sha256': u'04429e1602376b17c0d657437837396d540c24ad6285f3b750333eef28a9491a', u'type': u'data', u'size': 424}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 134192, u'sha256': u'4127919034cf833f80fb4a27503640533f9ea37b85745cffb666a58f199af3d5', u'type': u'data', u'size': 652}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 134848, u'sha256': u'f19acd5a46d79a6ca568d722316468fb040a66b94e6bbdf55363e9e4aaff6d4f', u'type': u'data', u'size': 1024}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 135872, u'sha256': u'fc44d52b5339bd88e2a4a651e5b1537c4b28eefd6735875e2152b10b9d83b739', u'type': u'data', u'size': 904}

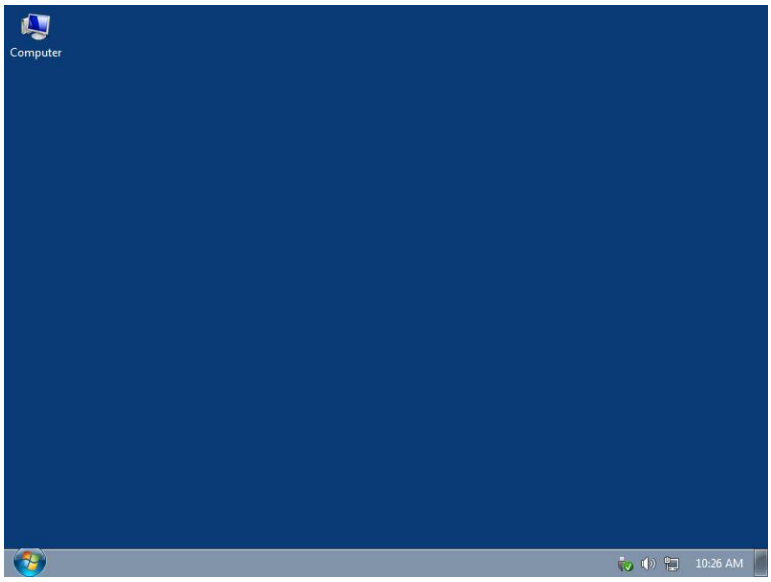
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 136776, u'sha256': u'8ef2cb11605de3baa89af09944c73fcc81235c1c684fb99c47c81d7add8b88a0', u'type': u'data', u'size': 900}

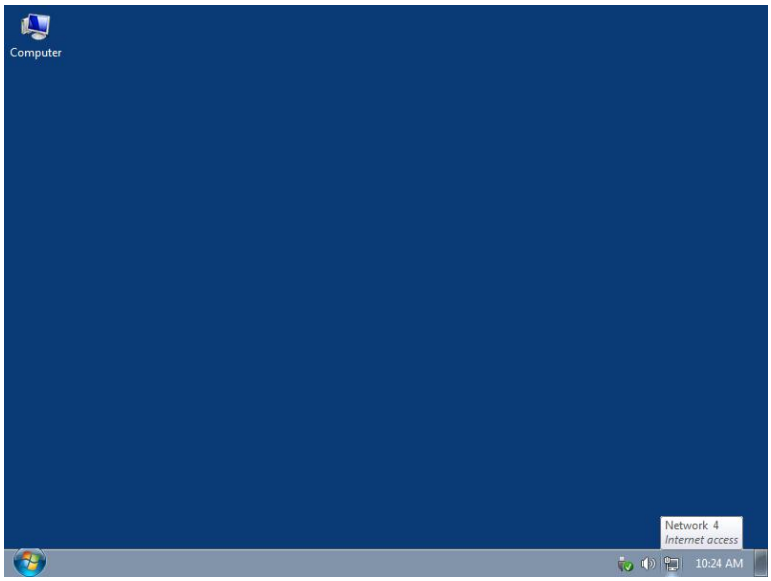
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 137680, u'sha256': u'8f330d0d77ea9fcc6276a096a251a1192c52401cf0e9dda8ae4edac519c2947d', u'type': u'data', u'size': 1144}

CERTIFICATE VALIDATION

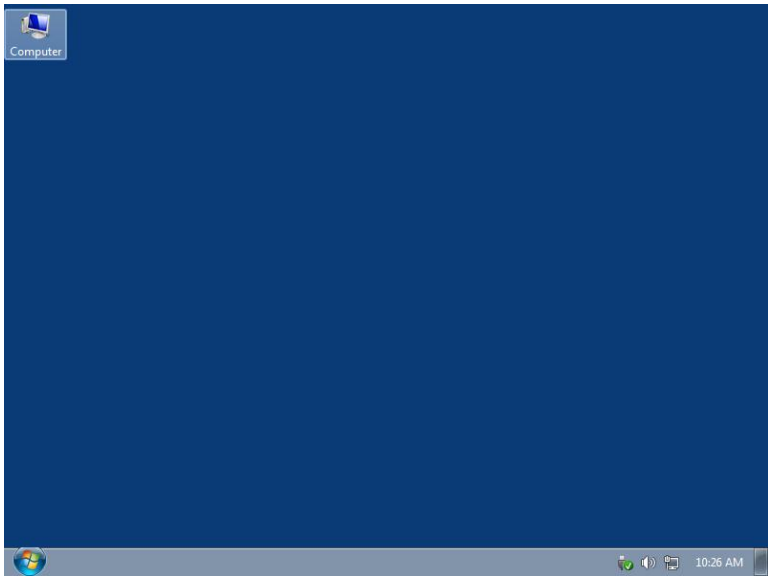
- Certificate Validation is not Applicable ?

SCREENSHOTS




Computer
Network 4
Internet access
10:24 AM


Computer
10:23 AM


Computer
10:26 AM