Summary

File Name: None

File Type: exported SGML document, ASCII text, with very long lines

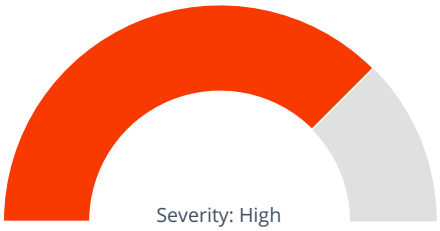
SHA1: b5929607272b710bf3ad15a6cd6063569834add4

MD5: 87e8fa876e3025a2c3c78f3a6d967a0f

MALWARE

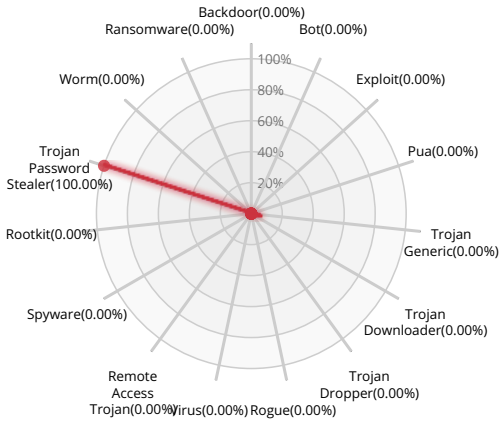
Valkyrie Final Verdict

DETECTION SECTION

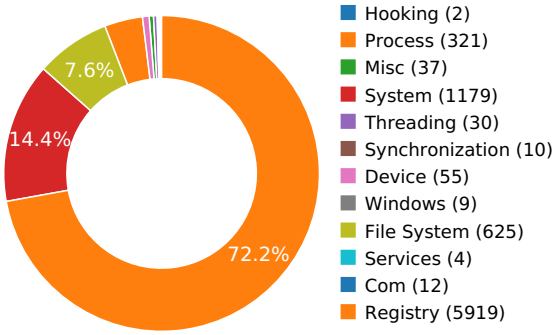


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STEALING OF SENSITIVE INFORMATION

Harvests information related to installed mail clients Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to repeatedly call a single API many times in order to delay analysis time Show sources

VALKYRIE COMODO

Behavior Graph

22:46:06 **22:47:46** **22:49:27**

PID 2876

22:46:06 **Create Process** The malicious file created a child process as cmd.exe **(PPID 1636)**

22:46:08 Create Process

PID 1924

22:46:08 **Create Process** The malicious file created a child process as rundll32.exe **(PPID 2876)**

PID 460

22:46:07 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

22:46:08 Create Process

22:49:11
22:49:27
GetSystemTimeAsFileTi
[4 times]

PID 2248

22:46:08 **Create Process** The malicious file created a child process as svchost.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\b5929607272b710bf3ad15a6cd6063569834add4
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\b5929607272b710bf3ad15a6cd6063569834add4.*
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:\
C:\Users
C:\Users\desktop.ini
C:\Users\user
C:\Users\user\Searches
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos
C:\Users\user\Videos\desktop.ini
C:\Users\user\Pictures
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Desktop
C:\Users\user\Contacts
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Favorites
C:\Users\user\Favorites\desktop.ini
C:\Users\user\Music
C:\Users\user\Music\desktop.ini
C:\Users\user\Downloads
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Documents
C:\Users\user\Documents\desktop.ini
C:\Users\user\Links
C:\Users\user\Links\desktop.ini

C:\Users\user\Saved Games
C:\Users\user\Saved Games\desktop.ini
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Windows\SysWOW64\shdocvw.dll
C:\Windows
C:\Windows\System32
C:\Windows\System32*.*
\??\MountPointManager
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\b5929607272b710bf3ad15a6cd6063569834add4:Zone.Identifier
C:\Windows\System32\rundll32.exe
C:\Windows\System32\shell32.dll
C:\Windows\SysWOW64\cmd.exe
C:\Windows\Temp
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\appmgmt\S-1-5-21-2298303332-66077612-2598613238-1000\AppMgmt.ini
C:\Windows\System32\shell32.dll.manifest
C:\Windows\System32\shell32.dll.123.Manifest
C:\Windows\SysWOW64\shell32.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\SysWOW64\rundll32.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
C:\Windows\System32\EhStorShell.dll
C:\Windows\SysWOW64\EhStorShell.dll
C:\Windows\System32\en-US\EhStorShell.dll.mui
C:\Windows\System32\ntshrui.dll
C:\Windows\SysWOW64\ntshrui.dll
C:\Windows\System32\en-US\ntshrui.dll.mui
C:\Windows\System32\imageres.dll
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe

C:\Program Files (x86)
C:\Program Files (x86)\desktop.ini
C:\Program Files (x86)\Adobe
C:\Program Files (x86)\Adobe\Reader 9.0
C:\Program Files (x86)\Adobe\Reader 9.0\Reader
C:\Windows\ehome\ehshell.exe
C:\Windows\ehome
C:\Program Files (x86)\Mozilla Firefox\firefox.exe
C:\Program Files (x86)\Mozilla Firefox

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\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_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
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\Unknown\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension

RESOLVED APIS

shell32.dll.ShellExecuteExW
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
comctl32.dll.#320
ole32.dll.StringFromGUID2
comctl32.dll.#324
comctl32.dll.#323
advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
propsys.dll.PSPropertyBag_ReadBSTR
propsys.dll.PSPropertyBag_ReadStrAlloc
shell32.dll.#102
advapi32.dll.OpenThreadToken
ole32.dll.CoInitializeEx
ole32.dll.CoCreateInstance
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#328
comctl32.dll.#334
comctl32.dll.#332
comctl32.dll.#338
ole32.dll.CoUninitialize
sechost.dll.ConvertSidToStringSidW
profapi.dll.#104
propsys.dll.#417

ole32.dll.PropVariantClear
oleaut32.dll.#9
comctl32.dll.#339
comctl32.dll.#386
advapi32.dll.RegQueryValueW
apphelp.dll.ApphelpCheckShellObject
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
propsys.dll.#430
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegGetValueW
advapi32.dll.RegCloseKey
ole32.dll.CoTaskMemRealloc
setupapi.dll.CM_Get_Device_Interface_List_ExW
ole32.dll.CoAllowSetForegroundWindow
advapi32.dll.InstallApplication
oleaut32.dll.#500
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.AcquireSRWLockShared
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.ReleaseSRWLockShared
shell32.dll.SHGetFolderPathW
advapi32.dll.SaferGetPolicyInformation
ntdll.dll.RtlDllShutdownInProgress
comctl32.dll.#329
ole32.dll.OleUninitialize
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388
kernelbase.dll.SetThreadStackGuarantee
ole32.dll.CoInitializeSecurity
sechost.dll.LookupAccountNameLocalW
advapi32.dll.LookupAccountSidW
sechost.dll.LookupAccountSidLocalW
kernel32.dll.SortGetHandle

kernel32.dll.SortCloseHandle

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

REGISTRY KEYS

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\cmd.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_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
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\
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\.
HKEY_CLASSES_ROOT\.\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\OpenWithProgids
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.\UserChoice
HKEY_CLASSES_ROOT\Unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\CurVer
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\ShellEx\IconHandler
HKEY_CLASSES_ROOT\SystemFileAssociations\.
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Unknown\BrowseInPlace

EXECUTED COMMANDS

"C:\Windows\system32\rundll32.exe" C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\user\AppData\Local\Temp\b5929607272b710bf3ad15a6cd6063569834add4
C:\Users\user\AppData\Local\Temp\b5929607272b710bf3ad15a6cd6063569834add4
C:\Windows\system32\svchost.exe -k netsvcs

READ FILES

\Device\KsecDD
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:\
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\Searches\desktop.ini
C:\Users\user\Videos\desktop.ini
C:\Users\user\Pictures\desktop.ini
C:\Users\user\Contacts\desktop.ini
C:\Users\user\Favorites\desktop.ini

C:\Users\user\Music\desktop.ini
C:\Users\user\Downloads\desktop.ini
C:\Users\user\Documents\desktop.ini
C:\Users\user\Links\desktop.ini
C:\Users\user\Saved Games\desktop.ini
C:\Windows\System32\shdocvw.dll
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Windows\System32\rundll32.exe
C:\Windows\SysWOW64\cmd.exe
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\appmgmt\S-1-5-21-2298303332-66077612-2598613238-1000\AppMgmt.ini
C:\Windows\System32\shell32.dll
C:\Windows\System32\shell32.dll.123.Manifest
C:\Windows\SysWOW64\shell32.dll
C:\Windows\Fonts\staticcache.dat
C:\Windows\winsxs\x86_microsoft.windows.c..-controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_581cd2bf5825dde9\comctl32.dll.mui
C:\Windows\System32\EhStorShell.dll
C:\Windows\System32\en-US\EhStorShell.dll.mui
C:\Windows\System32\ntshrui.dll
C:\Windows\System32\en-US\ntshrui.dll.mui
C:\Windows\System32\imageres.dll
C:\Program Files (x86)\desktop.ini
C:\Program Files (x86)
C:\Program Files (x86)\Adobe
C:\Program Files (x86)\Adobe\Reader 9.0
C:\Program Files (x86)\Adobe\Reader 9.0\Reader
C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Windows
C:\Windows\ehome
C:\Windows\ehome\ehshell.exe
C:\Program Files (x86)\Mozilla Firefox
C:\Program Files (x86)\Mozilla Firefox\firefox.exe
C:\Program Files (x86)\Internet Explorer
C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Program Files (x86)\Internet Explorer\en-US\iexplore.exe.mui
C:\Windows\System32
C:\Windows\System32\mspaint.exe
C:\Windows\System32\en-US\mspaint.exe.mui
C:\Program Files (x86)\Notepad++
C:\Program Files (x86)\Notepad++\notepad++.exe
C:\Windows\System32\notepad.exe
C:\Windows\System32\en-US\notepad.exe.mui
C:\Program Files (x86)\Microsoft Office
C:\Program Files (x86)\Microsoft Office\Office12
C:\Program Files (x86)\Microsoft Office\Office12\OIS.EXE
C:\Program Files (x86)\Windows Photo Viewer
C:\Program Files (x86)\Windows Photo Viewer\PhotoViewer.dll
C:\Program Files (x86)\Windows Photo Viewer\en-US\PhotoViewer.dll.mui
C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
C:\Program Files (x86)\Windows Media Player
C:\Program Files (x86)\Windows Media Player\wmplayer.exe
C:\Program Files (x86)\Windows Media Player\en-US\wmplayer.exe.mui
C:\Program Files (x86)\Windows NT
C:\Program Files (x86)\Windows NT\Accessories
C:\Program Files (x86)\Windows NT\Accessories\wordpad.exe
C:\Program Files (x86)\Windows NT\Accessories\en-US\wordpad.exe.mui
C:\program files (x86)\windows nt\accessories\wordpad.exe
C:\program files (x86)\windows photo viewer\photoviewer.dll
C:\program files (x86)\windows photo viewer\en-US\photoviewer.dll.mui
C:\program files (x86)\windows media player\wmplayer.exe
C:\program files (x86)\windows media player\en-US\wmplayer.exe.mui
C:\program files (x86)\notepad++\notepad++.exe

MUTEXES

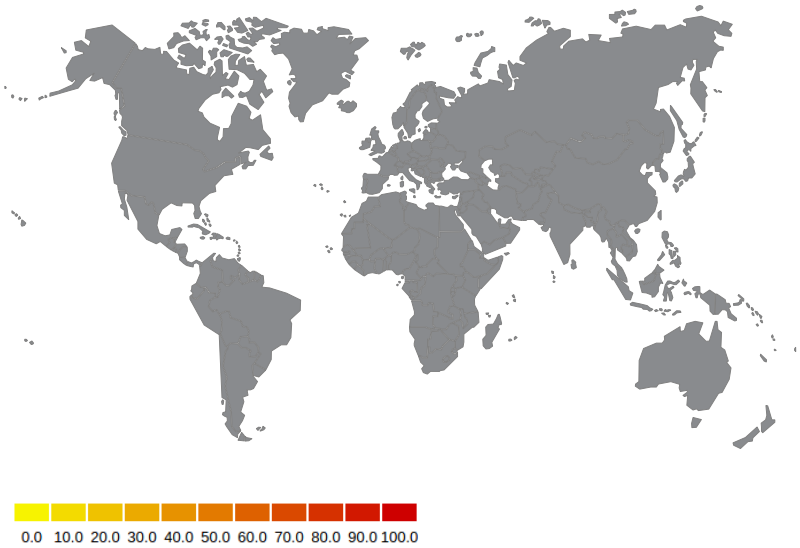
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

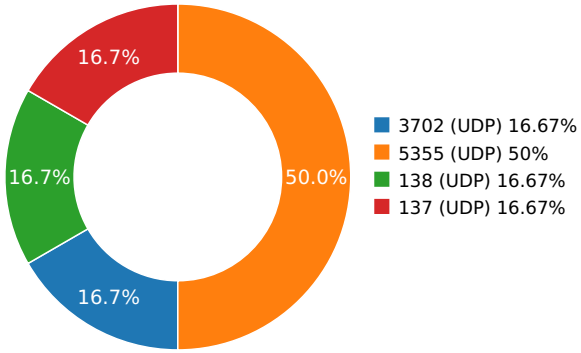
MODIFIED REGISTRY KEYS

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\Explorer\FileExts\OpenWithList

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.09171009064	Sandbox	224.0.0.252	5355
3.20440101624	Sandbox	192.168.56.255	137
3.26519012451	Sandbox	224.0.0.252	5355
3.46826195717	Sandbox	239.255.255.250	3702
5.87579298019	Sandbox	224.0.0.252	5355
6.24006295204	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:	None
File Type:	exported SGML document, ASCII text, with very long lines
SHA1:	b5929607272b710bf3ad15a6cd6063569834add4
MD5:	87e8fa876e3025a2c3c78f3a6d967a0f
First Seen Date:	2018-11-02 10:08:55.980322 (2 months ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-11-03 15:07:01.443531 (2 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

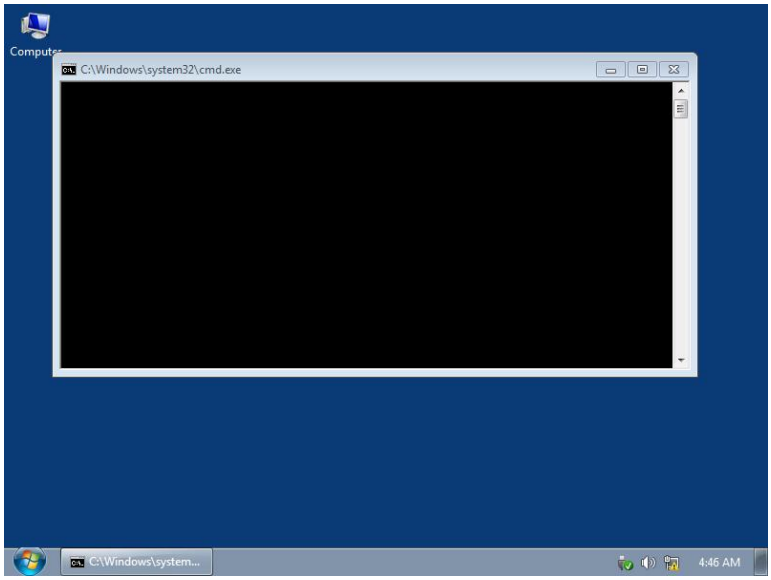
PE Headers

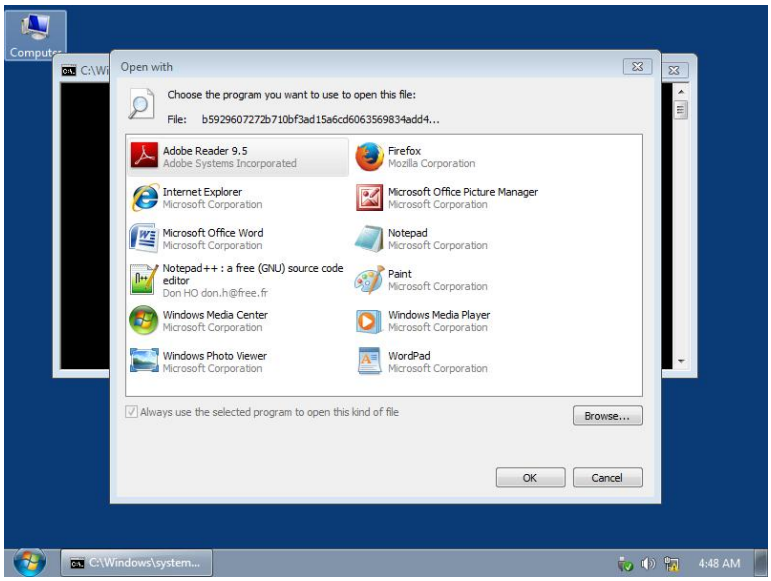
PROPERTY	VALUE
Magic Literal Enum	17
File Type Enum	1
File Size	533401
Sha256	bfc7a7f79f7c38ae687ef2c7fd8a482c0d2a649835e999f6de5e5bb3f77fb833
Mime Type	text/plain

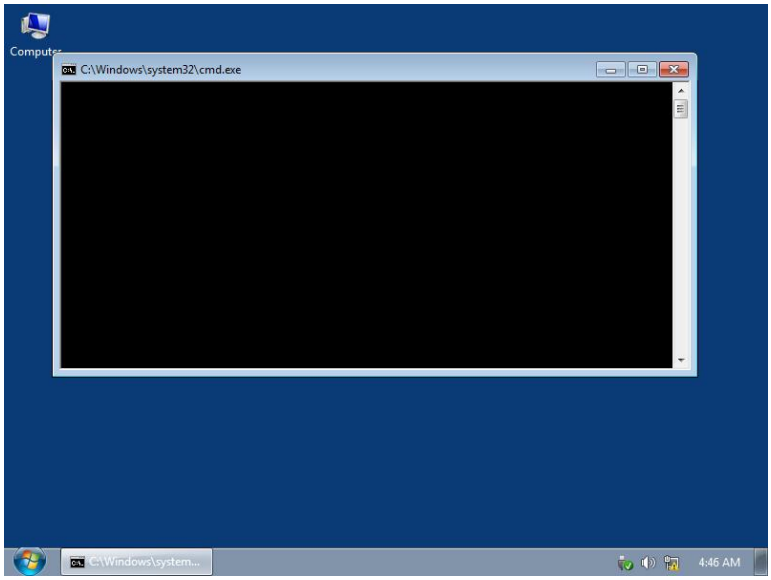
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

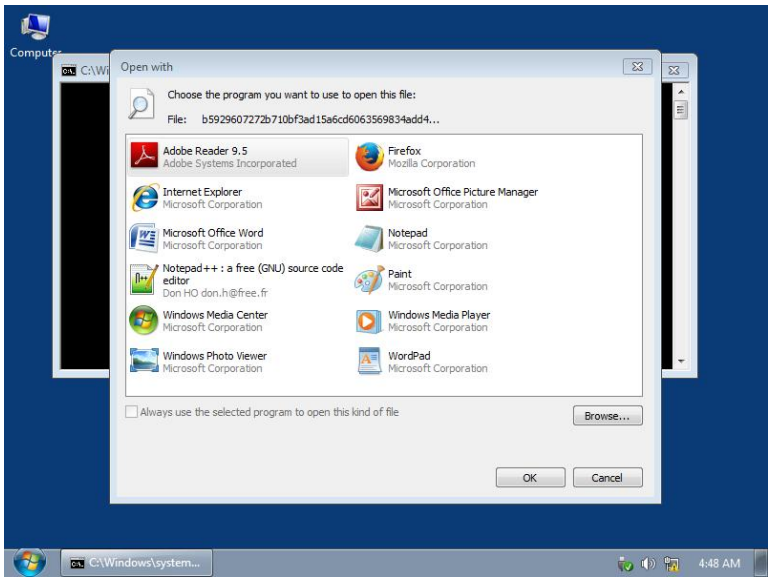
SCREENSHOTS

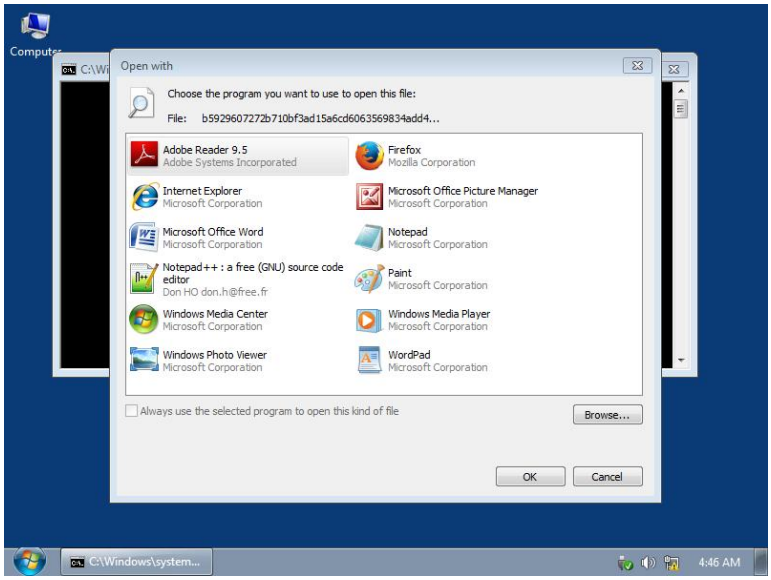



Computer
Open with
Choose the program you want to use to open this file:
File: b5929607272b710bf3ad15a6cd6063569834add4...
Adobe Reader 9.5
Adobe Systems Incorporated
Firefox
Mozilla Corporation
Internet Explorer
Microsoft Corporation
Microsoft Office Picture Manager
Microsoft Corporation
Microsoft Office Word
Microsoft Corporation
Notepad
Microsoft Corporation
Notepad++ : a free (GNU) source code editor
Don HO don.h@free.fr
Paint
Microsoft Corporation
Windows Media Center
Microsoft Corporation
Windows Media Player
Microsoft Corporation
Windows Photo Viewer
Microsoft Corporation
WordPad
Microsoft Corporation
Always use the selected program to open this kind of file
Browse...
OK
Cancel
4:48 AM


Computer
C:\Windows\system32\cmd.exe
4:46 AM


Computer
4:46 AM


Open with
Choose the program you want to use to open this file:
File: b5929607272b710bf3ad15a6cd6063569834add4...
Adobe Reader 9.5
Adobe Systems Incorporated
Firefox
Mozilla Corporation
Internet Explorer
Microsoft Corporation
Microsoft Office Picture Manager
Microsoft Corporation
Microsoft Office Word
Microsoft Corporation
Notepad
Microsoft Corporation
Notepad++ : a free (GNU) source code editor
Don HO don.h@free.fr
Paint
Microsoft Corporation
Windows Media Center
Microsoft Corporation
Windows Media Player
Microsoft Corporation
Windows Photo Viewer
Microsoft Corporation
WordPad
Microsoft Corporation
Always use the selected program to open this kind of file
Browse...
OK
Cancel
4:48 AM


Open with
Choose the program you want to use to open this file:
File: b5929607272b710bf3ad15a6cd6063569834add4...
Adobe Reader 9.5
Adobe Systems Incorporated
Firefox
Mozilla Corporation
Internet Explorer
Microsoft Corporation
Microsoft Office Picture Manager
Microsoft Corporation
Microsoft Office Word
Microsoft Corporation
Notepad
Microsoft Corporation
Notepad++ : a free (GNU) source code editor
Don HO don.h@free.fr
Paint
Microsoft Corporation
Windows Media Center
Microsoft Corporation
Windows Media Player
Microsoft Corporation
Windows Photo Viewer
Microsoft Corporation
WordPad
Microsoft Corporation
Always use the selected program to open this kind of file
Browse...
OK
Cancel
4:46 AM