VALKYRIE COMODO

Summary

File Name: JVC_41311.vbs

File Type: ASCII text, with very long lines

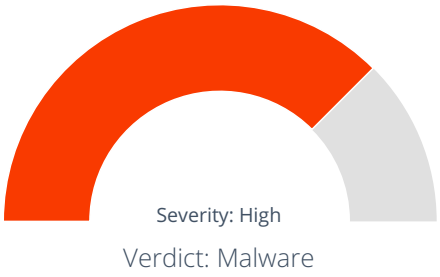
SHA1: af9d2c68d3d30110687718786f412bb899bcd5ad

MD5: d3b5e12cce28e162ab912dbee53c6539

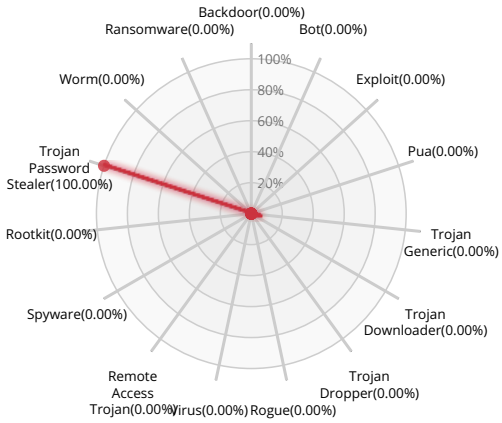
MALWARE

Valkyrie Final Verdict

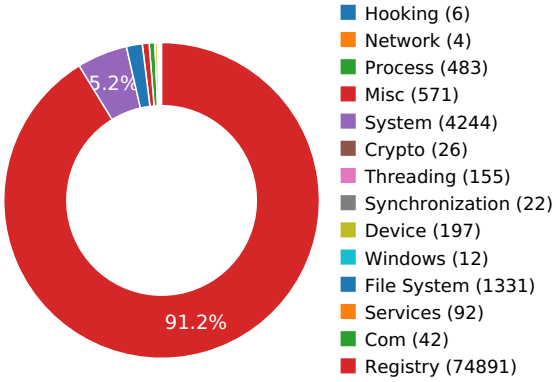
DETECTION SECTION



CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

STEALING OF SENSITIVE INFORMATION

Harvests information related to installed mail clients — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys — Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to modify or disable Security Center warnings — Show sources

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

VALKYRIE COMODO

Behavior Graph

04:02:57 **04:04:59** **04:07:01**

PID 2340

04:02:57 **Create Process** The malicious file created a child process as cmd.exe **(PPID 2292)**

04:02:59 Create Process

PID 2648

04:02:59 **Create Process** The malicious file created a child process as rundll32.exe **(PPID 2340)**

PID 456

04:02:58 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

04:02:59 Create Process

04:04:03 Create Process

04:04:29 Create Process

04:04:34 Create Process

04:04:53 Create Process

04:05:55 04:07:01 GetSystemTimeAsFileTi... **[13 times]**

PID 2544

04:02:59 **Create Process** The malicious file created a child process as svchost.exe **(PPID 456)**

PID 2852

04:04:19 **Create Process** The malicious file created a child process as taskhost.exe **(PPID 456)**

PID 2996

04:04:43 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 456)**

PID 2104

04:04:47 **Create Process** The malicious file created a child process as mscorsvw.exe **(PPID 456)**

PID 916

04:05:00 **Create Process** The malicious file created a child process as sppsvc.exe **(PPID 456)**

04:05:09 RegOpenKeyExW

PID 764

04:05:04 **Create Process** The malicious file created a child process as svchost.exe **(PPID 456)**

04:05:50 RegSetValueExW

PID 872

04:05:05 **Create Process** The malicious file created a child process as svchost.exe **(PPID 456)**

PID 580

04:05:52 **Create Process** The malicious file created a child process as svchost.exe **(PPID 456)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\af9d2c68d3d30110687718786f412bb899bcd5ad
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\af9d2c68d3d30110687718786f412bb899bcd5ad.*
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.ver0x000000000000004b.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
\??\MountPointManager
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*.*
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\af9d2c68d3d30110687718786f412bb899bcd5ad:Zone.Identifier
C:\Windows\System32\rundll32.exe
C:\Windows\System32\shell32.dll
C:\Windows\SysWOW64\cmd.exe
C:\Windows\LastGood.Tmp
C:\Windows\Temp
C:\Windows\sysnative\Tasks\Microsoft\Windows\WDI\ResolutionHost
C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp
C:\Windows\ServiceProfiles
C:\Windows\ServiceProfiles\NetworkService
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\sysnative\LogFiles\Scm\a7c73732-9f11-4281-8d19-764d4ec9d94d
C:\Windows\sysnative\LogFiles\Scm\be669c13-8165-4536-96d0-6d6c39292aae
C:\Windows\sysnative\LogFiles\Scm\ca4b8ff2-a4d2-4d88-a52e-3a5bdaf7f56e
C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b
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

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

MODIFIED FILES

C:\Windows\sysnative\LogFiles\Scm\9435f817-fed2-454e-88cd-7f78fda62c48
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenservicelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngenofflinequeuelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenservicelock.dat

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenrootstorelock.dat
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen_service.log
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngenofflinequeuelock.dat
\??\SPDevice
\??\PIPE\wkssvc
C:\Windows\SoftwareDistribution\ReportingEvents.log
C:\Windows\Temp\fwtsqmfile00.sqm
\Device\LanmanDatagramReceiver

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
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
advapi32.dll.RegQueryValueW
apphelp.dll.ApphelpCheckShellObject
propsys.dll.#430
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegGetValueW
advapi32.dll.RegCloseKey
ole32.dll.CoTaskMemRealloc
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 FILES

C:\Windows\LastGood.Tmp
C:\Windows\Microsoft.NET\ngenserviceclientlock.dat

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_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart

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\af9d2c68d3d30110687718786f412bb899bcd5ad
C:\Users\user\AppData\Local\Temp\af9d2c68d3d30110687718786f412bb899bcd5ad
C:\Windows\system32\svchost.exe -k netsvcs
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe
C:\Windows\system32\sppsvc.exe

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.ver0x000000000000004b.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\LastGood.Tmp
C:\Windows\sysnative\LogFiles\Scm\044a6734-e90e-4f8f-b357-b2dc8ab3b5ec
C:\Windows\sysnative\LogFiles\Scm\a7c73732-9f11-4281-8d19-764d4ec9d94d

C:\Windows\sysnative\LogFiles\Scm\be669c13-8165-4536-96d0-6d6c39292aae

C:\Windows\sysnative\LogFiles\Scm\ca4b8ff2-a4d2-4d88-a52e-3a5bdaf7f56e

C:\Windows\sysnative\LogFiles\Scm\fb3c354d-297a-4eb2-9b58-090f6361906b

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

MUTEXES

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

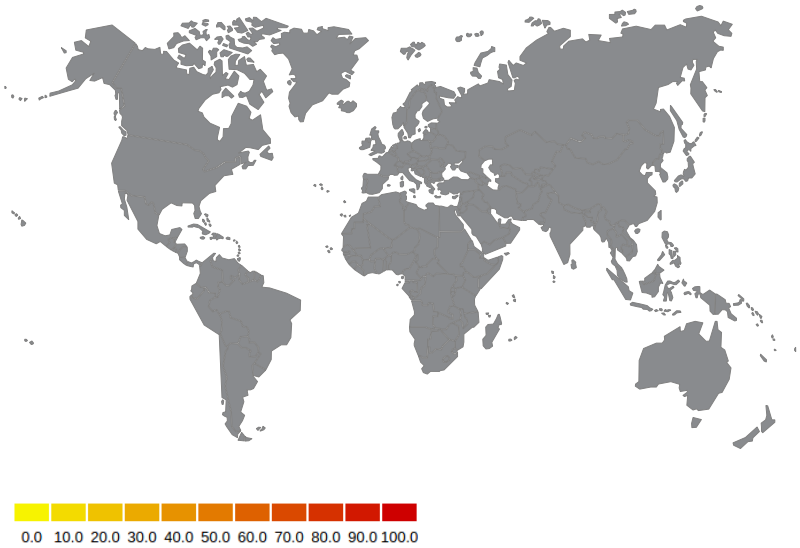
MODIFIED REGISTRY KEYS

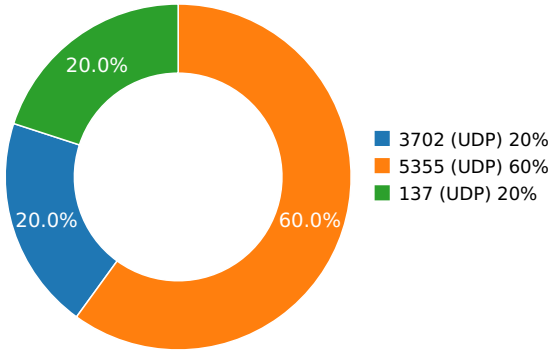
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_32\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\clr_optimization_v4.0.30319_64\Start
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Winmgmt\Type
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\OpenWithList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform\ServiceSessionId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center\cval
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Reporting\RebootWatch
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\NextSqmReportTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\PreviousServiceShutdown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ProcessID

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
3.02292513847	Sandbox	224.0.0.252	5355
3.03594112396	Sandbox	224.0.0.252	5355
3.04727816582	Sandbox	239.255.255.250	3702
3.0793170929	Sandbox	192.168.56.255	137
5.59559321404	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Windows\Temp\Fwtsqmfile00.Sqm	**Type :** data **MD5 :** 5ca6e4135b112bf3ef6c85e9ceca9645 **SHA-1 :** 30a07e26b86ceb3ffa05c2b36c78aea658619520 **SHA-256 :** 14e9c4d4340d546cecac6b802fcdce8bc8539143 **SHA-512 :** 85312db885d0fb4f24aa6d64ef523dc34a5065cb **Size :** 0.14 Kilobytes.
C:\Windows\Microsoft.NET\Framework\V4.0.30319\Ngen_service.Log	**Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 00892943f90c21f72567abc84c902e0b **SHA-1 :** 4da128e77db92210dc5ff57d52f069d4b19b00cd **SHA-256 :** 43ddd7f7630aad99136e4a67eb4e3a3def39c19c **SHA-512 :** 4e4ad9d11c78a4cc406f962e0920a4db07a16e8d **Size :** 6.178 Kilobytes.
C:\Windows\Microsoft.NET\Framework64\V4.0.30319\Ngen_service.Log	**Type :** UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 4b61e95f059f00d6eefa82a6b4a7cf0d **SHA-1 :** bbdd2d079bf570427c98afe21cebf03a319e6864 **SHA-256 :** 3aacd8b2be9d03480d6a5444fff1bdca508b903d **SHA-512 :** 6429fe5169e50989f2aed0fcd3f7f95fdf20d33b58 **Size :** 6.329 Kilobytes.
C:\Windows\Sysnative\LogFiles\Scm\9435f817-Fed2-454e-88cd-7f78fda62c48	**Type :** data **MD5 :** 42880057fa6190d33e4a94326f729a7a **SHA-1 :** e51fa3894beab38d5e9b18a5ea842aa19bc0fe00 **SHA-256 :** ef812b7477b638a720a0af30bca156a59e7765c8 **SHA-512 :** 5c0426f27dae6d0cc6a3c6d8f7dfb716b185c3ba1 **Size :** 0.012 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	JVC_41311.vbs
File Type:	ASCII text, with very long lines
SHA1:	af9d2c68d3d30110687718786f412bb899bcd5ad
MD5:	d3b5e12cce28e162ab912dbee53c6539
First Seen Date:	2019-12-29 18:14:09.458028 (2 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2019-12-29 18:14:09.458028 (2 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

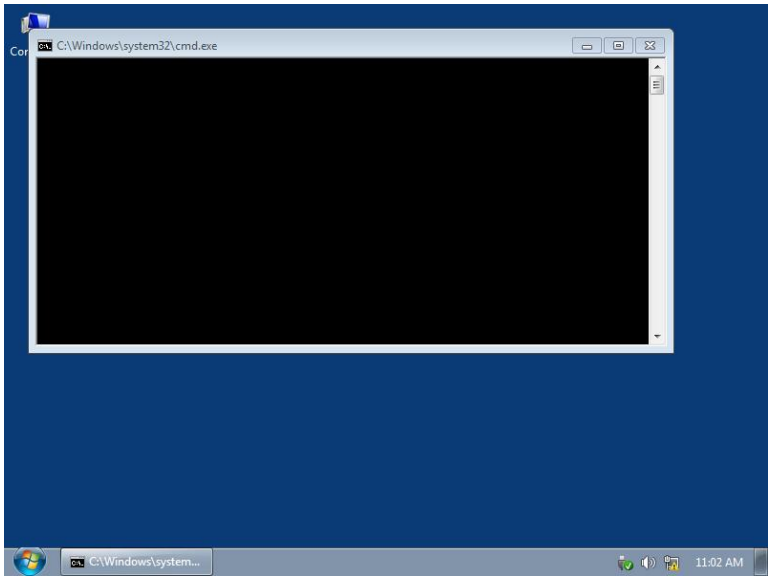
PE Headers

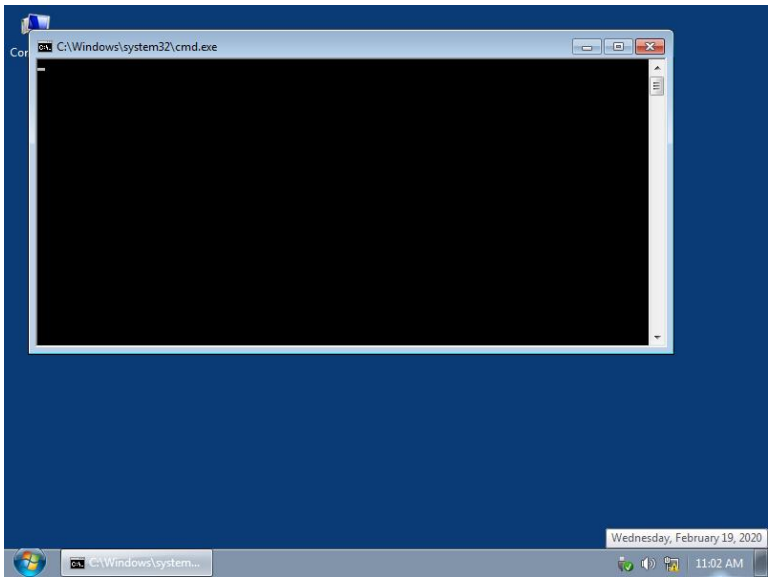
PROPERTY	VALUE
Magic Literal Enum	19
File Type Enum	1
File Size	4075418
Sha256	1ea64dc81882b15fa98fae1d5e1d8c519c201dfd40c901a4fd205f2b936ffa26
Mime Type	text/plain

CERTIFICATE VALIDATION

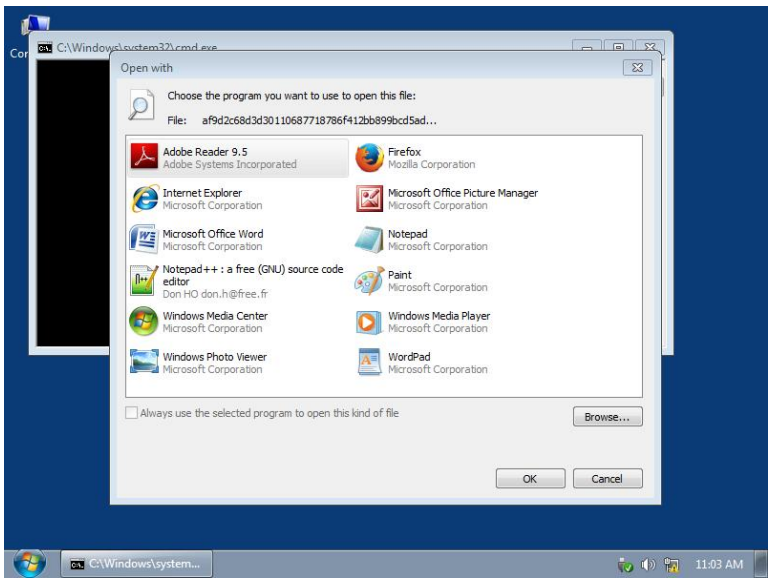
- Certificate Validation is not Applicable ?

SCREENSHOTS




C:\Windows\system32\cmd.exe
Wednesday, February 19, 2020
11:02 AM


Computer
11:02 AM


Open with
Choose the program you want to use to open this file:
File: af9d2c68d3d30110687718786f412bb899bcd5ad...
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
11:03 AM