VALKYRIE COMODO

Summary

File Name: R0m6yY6A1sKYmCUCtL.exe

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

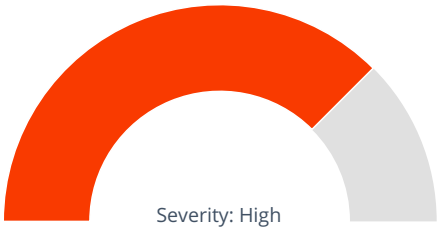
SHA1: c92f8f09d0b868433539d64b4989e13eb658e834

MD5: 8d11404a281ccdee87a76672471d02f7

MALWARE

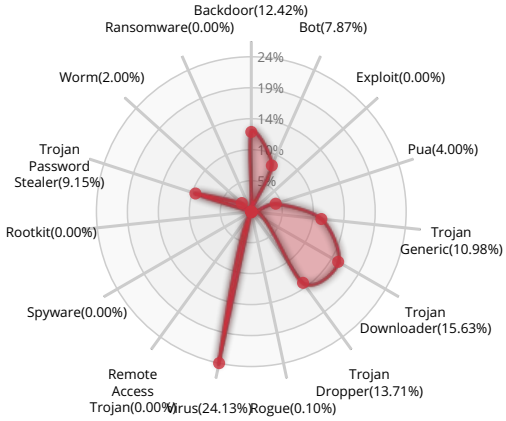
Valkyrie Final Verdict

DETECTION SECTION

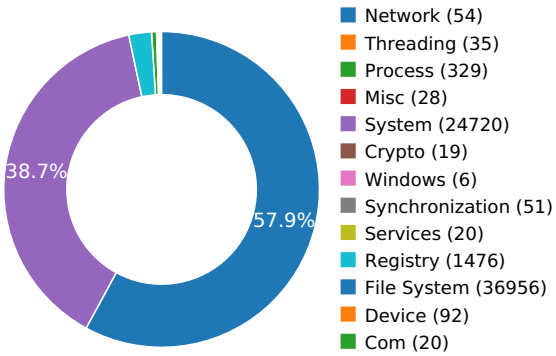


Verdict: Malware

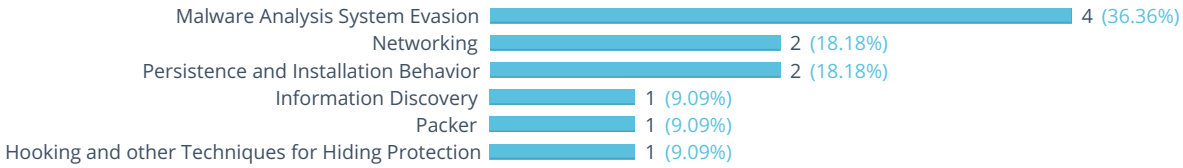
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Attempts to remove evidence of file being downloaded from the Internet	Show sources

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

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

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
Mimics the system's user agent string for its own requests	Show sources
Attempts to identify installed analysis tools by a known file location	Show sources
Attempts to repeatedly call a single API many times in order to delay analysis time	Show sources

VALKYRIE COMODO

Behavior Graph

21:20:52 **21:21:37** **21:22:22**

PID 2512

21:20:52 **Create Process** The malicious file created a child process as c92f8f09d0b868433539d64b4989e13eb658e834.exe **(PPID 1656)**

21:20:52 NtAllocateVirtualMem
21:20:52 FindFirstFileExW
21:20:53 Create Process

PID 2680

21:20:53 **Create Process** The malicious file created a child process as c92f8f09d0b868433539d64b4989e13eb658e834.exe **(PPID 2512)**

21:20:53 FindFirstFileExW
21:20:56 MoveFileWithProgress
21:20:56 DeleteFileW
21:20:56 CreateServiceW

PID 460

21:20:57 **Create Process** The malicious file created a child process as services.exe **(PPID 352)**

21:20:59 Create Process
21:22:05 Create Process

PID 548

21:20:59 **Create Process** The malicious file created a child process as ModelOverload.exe **(PPID 460)**

21:20:59 FindFirstFileExW
21:21:00 Create Process
21:21:00 NtTerminateProcess

PID 2228

21:21:00 **Create Process** The malicious file created a child process as ModelOverload.exe **(PPID 548)**

21:21:00 FindFirstFileExW
21:21:05 InternetOpenW
21:21:58 GetSystemTimeAsFile
21:22:00 Create Process

PID 652

21:22:17 **Create Process** The malicious file created a child process as cFvEj84YBsCm47f4Zjb.exe **(PPID 2228)**

21:22:17 FindFirstFileExW
21:22:17 Create Process

PID 3012

21:22:17 **Create Process** The malicious file created a child process as cFvEj84YBsCm47f4Zjb.exe **(PPID 652)**

21:22:18 FindFirstFileExW

PID 2304

21:22:21	Create Process	The malicious file created a child process as ModelOverload.exe **(PPID 460)**
21:22:21	FindFirstFileExW	
21:22:22	Create Process	

PID 2024

21:22:22	Create Process	The malicious file created a child process as ModelOverload.exe **(PPID 2304)**
21:22:22	FindFirstFileExW	

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64\ntdll.dll
C:*
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\$Recycle.Bin*
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000*
C:\Documents and Settings*
C:\Program Files (x86)*
C:\Program Files (x86)\Adobe*
C:\Program Files (x86)\Adobe\Reader 9.0*
C:\Program Files (x86)\Application Verifier*
C:\Program Files (x86)\Common Files*
C:\Program Files (x86)\Common Files\Adobe*
C:\Program Files (x86)\Common Files\DESIGNER*
C:\Program Files (x86)\Common Files\Java*
C:\Program Files (x86)\Common Files\Microsoft*
C:\Program Files (x86)\Common Files\microsoft shared*
C:\Program Files (x86)\Common Files\Services*
C:\Program Files (x86)\Common Files\SpeechEngines*
C:\Program Files (x86)\Common Files\System*
C:\Program Files (x86)\Fiddler2*
C:\Program Files (x86)\Google*
C:\Program Files (x86)\Google\Chrome*
C:\Program Files (x86)\Google\CrashReports*
C:\Program Files (x86)\Google\Update*
C:\Program Files (x86)\IDA*
C:\Program Files (x86)\IDA\cfg*
C:\Program Files (x86)\IDA\idc*
C:\Program Files (x86)\IDA\ids*
C:\Program Files (x86)\IDA\loaders*
C:\Program Files (x86)\IDA\plugins*
C:\Program Files (x86)\IDA\procs*
C:\Program Files (x86)\IDA\python*

C:\Program Files (x86)\IDA\sig*
C:\Program Files (x86)\IDA\til*
C:\Program Files (x86)\Internet Explorer*
C:\Program Files (x86)\Internet Explorer\en-US*
C:\Program Files (x86)\Internet Explorer\SIGNUP*
C:\Program Files (x86)\Java*
C:\Program Files (x86)\Java\jre1.8.0_91*
C:\Program Files (x86)\Microsoft Office*
C:\Program Files (x86)\Microsoft Office\Document Themes 12*
C:\Program Files (x86)\Microsoft Office\MEDIA*
C:\Program Files (x86)\Microsoft Office\Office12*
C:\Program Files (x86)\Microsoft Office\Stationery*
C:\Program Files (x86)\Microsoft Office\Templates*
C:\Program Files (x86)\Microsoft SDKs*
C:\Program Files (x86)\Microsoft SDKs\Windows*
C:\Program Files (x86)\Microsoft Visual Studio*
C:\Program Files (x86)\Microsoft Visual Studio\COMMON*
C:\Program Files (x86)\Microsoft Works*
C:\Program Files (x86)\Microsoft Works\1033*
C:\Program Files (x86)\Microsoft.NET*
C:\Program Files (x86)\Microsoft.NET\Primary Interop Assemblies*
C:\Program Files (x86)\Microsoft.NET\RedistList*
C:\Program Files (x86)\Mozilla Firefox*
C:\Program Files (x86)\Mozilla Firefox\browser*
C:\Program Files (x86)\Mozilla Firefox\defaults*
C:\Program Files (x86)\Mozilla Firefox\dictionaries*
C:\Program Files (x86)\Mozilla Firefox\gmp-clearkey*
C:\Program Files (x86)\Mozilla Firefox\uninstall*
C:\Program Files (x86)\Mozilla Firefox\webapprt*
C:\Program Files (x86)\MSBuild*
C:\Program Files (x86)\MSBuild\Microsoft*
C:\Program Files (x86)\Notepad++*
C:\Program Files (x86)\Notepad++\localization*
C:\Program Files (x86)\Notepad++\plugins*
C:\Program Files (x86)\Notepad++\updater*

C:\Program Files (x86)\Reference Assemblies*
C:\Program Files (x86)\Reference Assemblies\Microsoft*
C:\Program Files (x86)\Safer Networking*
C:\Program Files (x86)\Safer Networking\FileAlyzer 2*
C:\Program Files (x86)\Telerik*
C:\Program Files (x86)\Telerik\JustDecompile*
C:\Program Files (x86)\Uninstall Information*
C:\Program Files (x86)\Universal Extractor*
C:\Program Files (x86)\Universal Extractor\bin*

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
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

MODIFIED FILES

C:\Windows\SysWOW64\ModelOverload.exe
C:\Windows\SysWOW64\cFvEj84YBsCm47f4Zjb.exe
\??\VBoxMiniRdrDN
\??\UNC\VBOXSVR\PIPE\samr
\??\PIPE\wkssvc
\Device\LanmanDatagramReceiver
\??\PIPE\browser
\??\PIPE\DAV RPC SERVICE

RESOLVED APIS

kernel32.dll.GetBinaryTypeW
kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.UnmapViewOfFile
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect

kernel32.dll.AddVectoredExceptionHandler
kernel32.dll.RemoveVectoredExceptionHandler
advapi32.dll.GetUserNameA
user32.dll.wsprintfA
msvcrt.dll.malloc
msvcrt.dll.free
msvcrt.dll.strchr
kernel32.dll.FreeConsole
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCurrentProcess
kernel32.dll.HeapFree
kernel32.dll.HeapAlloc
kernel32.dll.GetProcessHeap
kernel32.dll.lstrlenW
kernel32.dll.lstrcatW
kernel32.dll.FindFirstFileW
kernel32.dll.lstrcmpW
kernel32.dll.lstrcpyW
kernel32.dll.FindNextFileW
kernel32.dll.FindClose
kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetComputerNameA
kernel32.dll.GetComputerNameExA
kernel32.dll.lstrlenA
kernel32.dll.lstrcpyA
kernel32.dll.lstrcatA
kernel32.dll.lstrcmpA
kernel32.dll.GetTickCount
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.WTSGetActiveConsoleSessionId
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

DELETED FILES

C:\Windows\SysWOW64\searchtime.exe

C:\Users\user\AppData\Local\Temp\c92f8f09d0b868433539d64b4989e13eb658e834.exe

C:\Windows\SysWOW64\ModelOverload.exe:Zone.Identifier

C:\Windows\SysWOW64\cFvEj84YBsCm47f4Zjb.exe

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tcpip\Parameters\Hostname

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

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\c92f8f09d0b868433539d64b4989e13eb658e834.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

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\c92f8f09d0b868433539d64b4989e13eb658e834.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\ModelOverload.exe
C:\Windows\SysWOW64\cFvEj84YBsCm47f4Zjb.exe
C:\Windows\SysWOW64

\??\VBoxMiniRdrDN
\??\UNC\VBOXSVR\PIPE\samr
\??\PIPE\wkssvc
\Device\LanmanDatagramReceiver
\??\PIPE\browser
\??\PIPE\DAV RPC SERVICE

MUTEXES

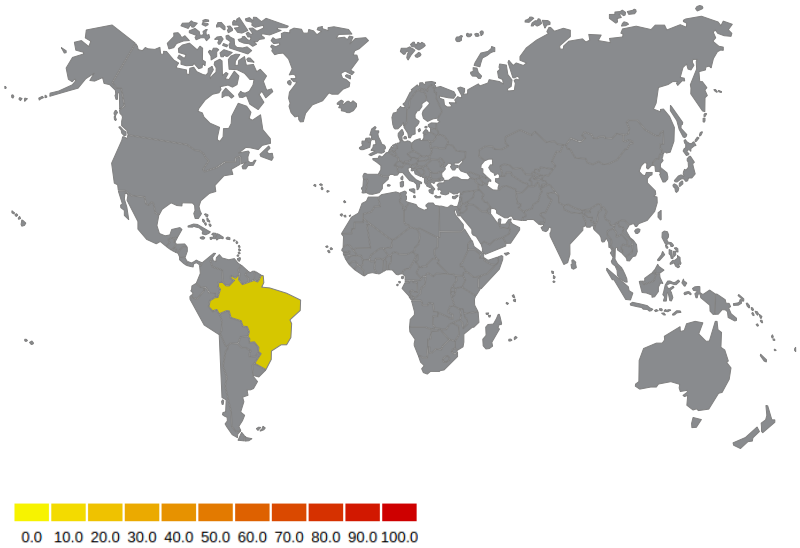
MBA337E4D
Global\I20503A4E
Global\M20503A4E
MB91353F9
IESQMMUTEX_0_208
MFC870677

MODIFIED REGISTRY KEYS

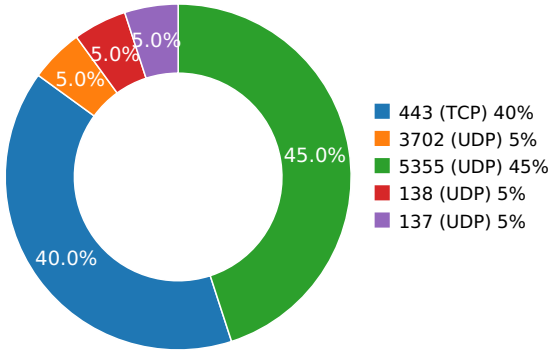
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ModelOverload\Type
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	191.242.178.46	Brazil	263151	CONECT TELECOM	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
191.242.178.46:443	443	POST	1.1	Mozilla/4.0 (compatible; MSI...	1	20.2789030075
Path: / **URI:** http://191.242.178.46:443/						
191.242.178.46:443	443	POST	1.1	Mozilla/4.0 (compatible; MSI...	2	86.6220741272
Path: / **URI:** http://191.242.178.46:443/						
191.242.178.46:443	443	POST	1.1	Mozilla/4.0 (compatible; MSI...	1	109.880957127
Path: / **URI:** http://191.242.178.46:443/						
191.242.178.46:443	443	POST	1.1	Mozilla/4.0 (compatible; MSI...	1	160.817716122
Path: / **URI:** http://191.242.178.46:443/						

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
20.2789030075	Sandbox	191.242.178.46	443
86.6220741272	Sandbox	191.242.178.46	443
109.880957127	Sandbox	191.242.178.46	443
160.817716122	Sandbox	191.242.178.46	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.11146497726	Sandbox	224.0.0.252	5355
3.1328420639	Sandbox	224.0.0.252	5355
3.13833498955	Sandbox	239.255.255.250	3702
3.18659305573	Sandbox	192.168.56.255	137
5.72687292099	Sandbox	224.0.0.252	5355
9.2283809185	Sandbox	192.168.56.255	138
17.4684319496	Sandbox	224.0.0.252	5355
112.279314995	Sandbox	224.0.0.252	5355
115.240144968	Sandbox	224.0.0.252	5355
117.906793118	Sandbox	224.0.0.252	5355
120.643764019	Sandbox	224.0.0.252	5355
123.265576124	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	R0m6yY6A1sKYmCUCtL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	c92f8f09d0b868433539d64b4989e13eb658e834
MD5:	8d11404a281ccdee87a76672471d02f7
First Seen Date:	2018-03-14 15:34:54.293778 (9 months ago)
Number Of Clients Seen:	5
Last Analysis Date:	2018-03-14 15:34:54.293778 (9 months ago)
Human Expert Analysis Date:	2018-03-14 17:54:11.609284 (9 months ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[]
Compilation Time Stamp	0x5AA94034 [Wed Mar 14 15:31:00 2018 UTC]
Entry Point	0x405000 (.text1)
Machine Type	Intel 386 or later - 32Bit
File Size	134144
Ssdeep	
Sha256	2eabc641d603c7b11d5ac55e8f080e23243a4d83ae9008bddb5fbc105ad892a0
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x38da	0x3a00	6.20850266269	621b4b6074d8935f310feea7d9bbdf01
.text1	0x5000	0x66	0x200	1.64980412186	e5e7317807040f740708061f07d8a801
.rdata	0x6000	0x145d4	0x14600	7.57298575283	5ad8e490494cc07c3125498450b68764
.data	0x1b000	0x1674	0x800	6.5029315852	0015f431ad983fd47fd269ead2d64d27
.rsrc	0x1d000	0x7b48	0x7c00	6.24645993218	b6c4e86889ea30c7c4573f83e17108ba
.reloc	0x25000	0x150	0x200	4.41669222759	260678edc34235a372634d46f753de28

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 119760, u'sha256': u'49b0bdc573bb175921fa65681048b65758dd65815046beaedf9e6dc153abcdd3', u'type': u'data', u'size': 1000}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 124672, u'sha256': u'1cbb4133315f3c874ddf0d81bb90e176bb74083d8b065bbf80734a2abd0cf7a5', u'type': u'data', u'size': 1640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 126312, u'sha256': u'664d6568711ae5b226f5b3758adcf8ef169dd2c06d343709ab6b2ff7f15b6176', u'type': u'data', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 127056, u'sha256': u'f998333e754e6406b4de7f3d0e9f7b5b212a5c7c4d5a91af9509175e3ede9d0b', u'type': u'data', u'size': 488}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 127544, u'sha256': u'6521803a2a179288c9a7c118ec24c17cceee59baa8f81675320837fc51b7527b', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 127840, u'sha256': u'c5e8502a29f3b00cce03429d141924b7fbded99161af3f47cdb85d52d4114459', u'type': u'dBase III DBT, version number 0, next free block index

40, 1st item "\\251\\317"', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 131592, u'sha256': u'9e13490eaae391c751be2e20e41730b6967c6d9283c86e9d7f805ae816b3ad79', u'type': u'dBase III DBT, version number 0, next free block index 40, 1st item "\\251\\317"', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 133808, u'sha256': u'46971c4015dfa55e5ee2a15c0dd1c09bac3b73da36ff94337f165f341690b08c', u'type': u'dBase III DBT, version number 0, next free block index 40, 1st item "\\251\\317"', u'size': 1736}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 135544, u'sha256': u'60e0d2fbadf4aaef210589a88a6abb852d76f7a4d85f629e485517f431b5ad19', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 6967}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 142512, u'sha256': u'f79775bc6663b51bc24d885e08c57554c34ac9f684e3cadf683034e40a729aa6', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 146776, u'sha256': u'b7219ea977667a3735a654f80f3a991dd058e0438688fa55f99765a593e0ba2f', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 149216, u'sha256': u'fed29bef4ed1b3cd04ab0a8a7421901741bfd51502900a35587a06850a0a7eaa', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 120760, u'sha256': u'0b6424b38e5eb526584f76381eac6da22452e7f8c0a033741c19fea364556f07', u'type': u'data', u'size': 916}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 121680, u'sha256': u'5de3ab0e6ffdee43cf7921ca4d399bfe27e67fa00ab2d657012e9157fc5c3d3a', u'type': u'data', u'size': 860}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 122544, u'sha256': u'1893a4eed0a8c996ee87a4a73bfa06c6fb9a147117e1925983caff227c147943', u'type': u'data', u'size': 640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 123184, u'sha256': u'f254fb880529d3549ca21f335e81c6ae8d7995fd6eb00909ae02166a236e3e47', u'type': u'data', u'size': 1292}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 124480, u'sha256': u'9a61089ff7078ba4d9a1dad29cb121cf65caf042734a77648099e8e1eca5e55d', u'type': u'MS Windows icon resource - 13 icons, 48x48, 16 colors', u'size': 188}

CERTIFICATE VALIDATION

- FileNotSigned ✖

SCREENSHOTS