VALKYRIE COMODO

Summary

File Name: qw787_2102v2.exe

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

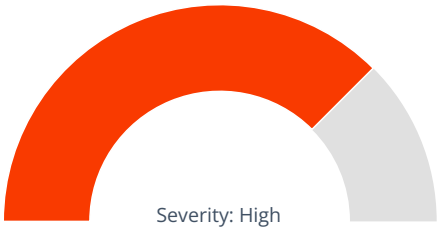
SHA1: 263610b09096511eb54892a82b7d631ac6ec4995

MD5: 979f958d3a5f08efc058fe85f58bac6e

MALWARE

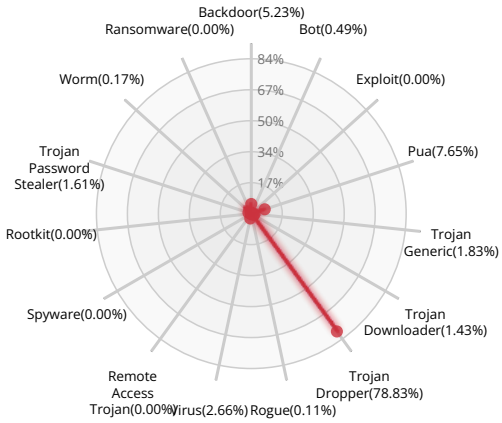
Valkyrie Final Verdict

DETECTION SECTION

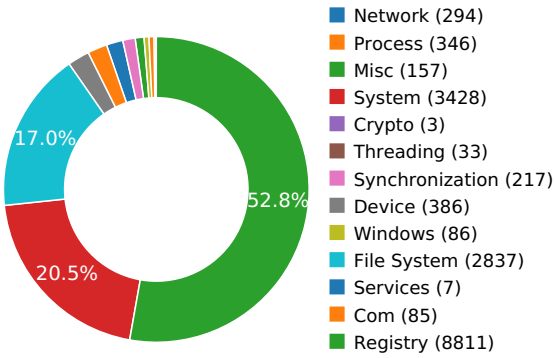


Verdict: Malware

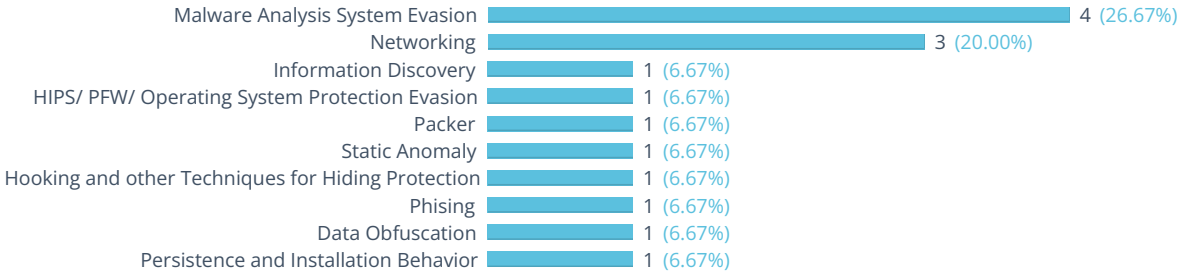
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (4 unique times) — Show sources

Performs some HTTP requests — Show sources

Network activity contains more than one unique useragent. — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory — Show sources

PACKER

The binary likely contains encrypted or compressed data. — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

PHISING

'Dropbox' in HTML Title but connection is not HTTPS. Possibly indicative of phishing. — Show sources

DATA OBFUSCATION

Drops a binary and executes it — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

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
A process attempted to delay the analysis task.	Show sources
Detects VirtualBox through the presence of a file	Show sources
Creates a hidden or system file	Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.ENU
C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.ENU.DLL
C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.EN
C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.EN.DLL
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\Desktop
\Device\KsecDD
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.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\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:\Windows\System32\twext.dll
C:\Windows\SysWOW64\twext.dll
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
::\
::\{2559A1F3-21D7-11D4-BDAF-00C04F60B9F0}

::\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
::\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}
::\{2559A1F1-21D7-11D4-BDAF-00C04F60B9F0}
C:\Program Files\Oracle\VirtualBox Guest Additions\uninst.exe
C:\Program Files\Oracle\VirtualBox Guest Additions
C:\Program Files\Oracle\VirtualBox Guest Additions\Oracle VM VirtualBox Guest Additions.url
C:\tools\totalcmdx32\TOTALCMD.CHM
C:\tools\totalcmdx32\TCUNINST.EXE
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\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\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

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe
C:\ProgramData\Synaptics\Synaptics.exe
C:\ProgramData\Synaptics\RCX2A18.tmp
C:\Users\user\AppData\Local\Temp\is-VR9FB.tmp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.tmp
C:\Users\user\AppData\Local\Temp\is-KLJBF.tmp_isetup_setup64.tmp
C:\Program Files (x86)\Qualitywings\QW787\is-2ISQI.tmp

C:\Program Files (x86)\Qualitywings\QW787\f0bd292a-8c45-4a5a-bb2b-8614b2fb027f.index

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-7A8JA.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\cycle_info.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-OCPH9.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\apps.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-984ID.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\aptcomms.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-SDJG6.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\apts.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-AOSUE.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\awys.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-72E3T.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\ints.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-VDLMD.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\msa.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-CES77.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\navs.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-6U80G.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\sids.txt

C:\Program Files (x86)\Qualitywings\QW787\navdata\is-E72P8.tmp

C:\Program Files (x86)\Qualitywings\QW787\navdata\stars.txt

C:\Users\user\AppData\Roaming\WinSl\L3\5\2021

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC197601BE0898B7B0FCC91FA15D8A69_56D2979CE24B15FDD8BEBFC2EA707A7B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC197601BE0898B7B0FCC91FA15D8A69_56D2979CE24B15FDD8BEBFC2EA707A7B

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC197601BE0898B7B0FCC91FA15D8A69_9C3330CF3BD3CFD21A37457CA8E40937

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC197601BE0898B7B0FCC91FA15D8A69_9C3330CF3BD3CFD21A37457CA8E40937

C:\Users\user\AppData\Local\Temp\Aqvej1N.ini

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

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\35DDEDF268117918D1D277A171D8DF7B_A29FED777819EBFE086A4D0443378D69
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\35DDEDF268117918D1D277A171D8DF7B_A29FED777819EBFE086A4D0443378D69
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CBDD1895DA987FB1E4F940B9391897BC
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CBDD1895DA987FB1E4F940B9391897BC

RESOLVED APIS

kernel32.dll.GetDiskFreeSpaceExA
oleaut32.dll.VariantChangeTypeEx
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarAdd
oleaut32.dll.VarSub
oleaut32.dll.VarMul
oleaut32.dll.VarDiv
oleaut32.dll.VarIdiv
oleaut32.dll.VarMod
oleaut32.dll.VarAnd
oleaut32.dll.VarOr
oleaut32.dll.VarXor
oleaut32.dll.VarCmp
oleaut32.dll.VarI4FromStr
oleaut32.dll.VarR4FromStr
oleaut32.dll.VarR8FromStr
oleaut32.dll.VarDateFromStr
oleaut32.dll.VarCyFromStr
oleaut32.dll.VarBoolFromStr
oleaut32.dll.VarBstrFromCy
oleaut32.dll.VarBstrFromDate
oleaut32.dll.VarBstrFromBool
user32.dll.GetMonitorInfoA

user32.dll.GetSystemMetrics
user32.dll.EnumDisplayMonitors
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
gdi32.dll.GdiIsMetaPrintDC
user32.dll.AnimateWindow
comctl32.dll.InitializeFlatSB
comctl32.dll.UninitializeFlatSB
comctl32.dll.FlatSB_GetScrollProp
comctl32.dll.FlatSB_SetScrollProp
comctl32.dll.FlatSB_EnableScrollBar
comctl32.dll.FlatSB_ShowScrollBar
comctl32.dll.FlatSB_GetScrollRange
comctl32.dll.FlatSB_GetScrollInfo
comctl32.dll.FlatSB_GetScrollPos
comctl32.dll.FlatSB_SetScrollPos
comctl32.dll.FlatSB_SetScrollInfo
comctl32.dll.FlatSB_SetScrollRange
user32.dll.SetLayeredWindowAttributes
ole32.dll.CoCreateInstanceEx
ole32.dll.CoInitializeEx
ole32.dll.CoAddRefServerProcess
ole32.dll.CoReleaseServerProcess
ole32.dll.CoResumeClassObjects

ole32.dll.CoSuspendClassObjects
ole32.dll.CoGetMalloc
ole32.dll.CoGetApartmentType
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoTaskMemAlloc
ole32.dll.StringFromGUID2
advapi32.dll.OpenThreadToken
cryptbase.dll.SystemFunction036
ole32.dll.CoUninitialize
oleaut32.dll.#500
shell32.dll.#2
shell32.dll.#4
comctl32.dll.HIMAGELIST_QueryInterface

DELETED FILES

C:\ProgramData\Synaptics\RCX2A18.tmp
C:\Users\user\AppData\Local\Temp\is-VR9FB.tmp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.tmp
C:\Users\user\AppData\Local\Temp\is-VR9FB.tmp
C:\Program Files (x86)\Qualitywings\QW787\is-2ISQI.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-7A8JA.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-OCPH9.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-984ID.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-SDJG6.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-AOSUE.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-72E3T.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-VDLMD.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-CES77.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-6U80G.tmp
C:\Program Files (x86)\Qualitywings\QW787\navdata\is-E72P8.tmp
C:\Users\user\AppData\Local\Temp\is-KLJBF.tmp_isetup_setup64.tmp
C:\Users\user\AppData\Local\Temp\is-KLJBF.tmp_isetup

C:\Users\user\AppData\Local\Temp\is-KLJBF.tmp
C:\Users\user\AppData\Local\Temp\Aqvej1N.ini

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
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\263610b09096511eb54892a82b7d631ac6ec4995.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}
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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}\PropertyBag
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Desktop

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe"
C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe
"C:\ProgramData\Synaptics\Synaptics.exe" InjUpdate
C:\ProgramData\Synaptics\Synaptics.exe InjUpdate

"C:\Users\user\AppData\Local\Temp\is-VR9FB.tmp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.tmp" /SL5="$30154,10382568,790528,C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe"

READ FILES

C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
\Device\KsecDD
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.exe
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\twext.dll
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft

C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\System32\ntshrui.dll
C:\Windows\System32\en-US\ntshrui.dll.mui
C:\Windows\System32\syncui.dll
C:\Windows\System32\en-US\syncui.dll.mui
C:\Program Files\7-Zip\7-zip32.dll
C:\Program Files\7-Zip\Lang\en.txt
C:\Windows\System32\acppage.dll
C:\Windows\System32\en-US\acppage.dll.mui
C:\Windows\winsxs\FileMaps\users_user_appdata_local_temp_3411b1c358bfd067.cdf-ms
C:\Windows\System32\imageres.dll
C:\Windows\System32\EhStorShell.dll
C:\Windows\System32\en-US\EhStorShell.dll.mui
C:\Windows\System32\shell32.dll
C:\program files\sandboxie\Start.exe
C:\Users\user\AppData\Local\Temp\263610b09096511eb54892a82b7d631ac6ec4995.exe

C:\ProgramData\Synaptics\Synaptics.exe
C:\ProgramData\Synaptics\RCX2A18.tmp
C:\ProgramData\Synaptics\desktop.ini
C:\ProgramData\Synaptics
C:\Windows\winsxs\FileMaps\programdata_synaptics_9a00f3ffc6c3ad54.cdf-ms
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Windows\System32\netmsg.dll
C:\Windows\System32\spool\drivers\color\sRGB Color Space Profile.icm
C:\Users\user\AppData\Local\Temp\is-KLJBF.tmp_isetup_setup64.tmp
C:\Windows\winsxs\FileMaps\program_files_x86_qualitywings_qw787_28f8579a85bc6fe1.cdf-ms

MUTEXES

Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex
Synaptics2X
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511
Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000
DefaultTabtip-MainUI
IESQMMUTEX_0_208

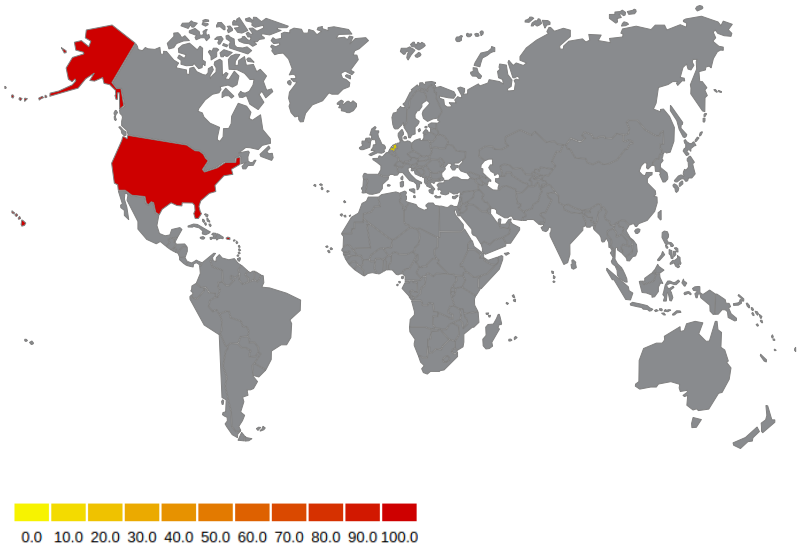
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
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\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Synaptics Pointing Device Driver
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Owner
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\SessionHash
HKEY_CURRENT_USER\Software\Microsoft\RestartManager\Session0000\Sequence
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadDecision

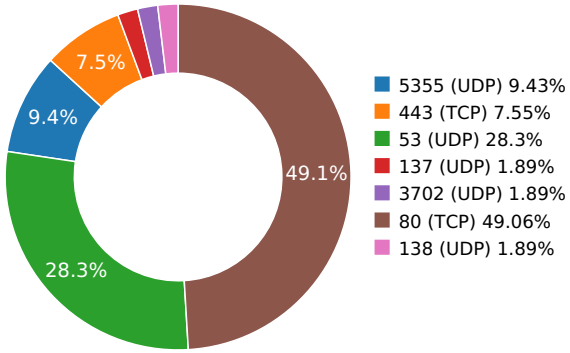
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{E2D0CA08-2243-4725-9430-A8A2D5F46E6B}\WpadNetworkName
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionReason
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadLastNetwork

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	104.18.108.8	United States	13335	Cloudflare, Inc.	Malware Process
	104.18.20.226	United States	13335	Cloudflare, Inc.	Malware Process
	69.42.215.252	United States	33333	Awknet Communications...	Malware Process
	8.240.248.254	United States	3356	Level 3 Parent, LLC	OS Process
	140.82.59.108	Netherlands	20473	The Constant Company, L...	Malware Process
ocsp.comodoca.com	151.139.128.14	United States	20446	StackPath, LLC.	OS Process
freedns.afraid.org	50.23.197.95	United States	36351	SoftLayer Technologies In...	Malware Process
doc-14-14-docs.googleusercontent.com	172.217.1.161	United States	15169	Google LLC	Malware Process
docs.google.com	172.217.1.174	United States	15169	Google LLC	Malware Process
ctldl.windowsupdate.com	8.250.91.254	United States	3356	Level 3 Parent, LLC	OS Process
ocsp.usertrust.com	151.139.128.14	United States	20446	StackPath, LLC.	OS Process
www.000webhost.com	104.18.107.8	United States	13335	Cloudflare, Inc.	Malware Process
ocsp.sectigo.com	151.139.128.14	United States	20446	StackPath, LLC.	Malware Process
ocsp.pki.goog	172.217.1.163	United States	15169	Google LLC	Malware Process
crl.microsoft.com	23.35.69.154	United States	20940	Akamai Technologies, Inc.	OS Process
xred.site50.net	153.92.0.100	United States	204915	Hostinger International L...	Malware Process
crl.globalsign.net	104.18.21.226	United States	13335	Cloudflare, Inc.	Malware Process
ocsp.digicert.com	72.21.91.29	United States	15133	MCI Communications Ser...	Malware Process
www.dropbox.com	162.125.6.18	United States	19679	Dropbox, Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
freedns.afraid.org	80	GET	1.1	MyApp	1	19.8013589382
Path: /api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978 **URI:** http://freedns.afraid.org/api/?action=getdyndns&sha=a30fa98efc092684e8d1c5cff797bcc613562978						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	23.3184049129
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e7d7a45ca5ab58e7 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e7d7a45ca5ab58e7						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	23.8164358139
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?f6345a1644e7f903 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?f6345a1644e7f903						
ocsp.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	24.3431129456
Path: /gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjtJqhjYqpgSVpULg%3D **URI:** http://ocsp.pki.goog/gsr2/ME4wTDBKMEgwRjAJBgUrDgMCGgUABBTgXIsxbvr2lBkPpoIEVRE6gHlCnAQUm%2BIHV2ccHsBqBt5ZtJot39wZhi4CDQHjtJqhjYqpgSVpULg%3D						
ocsp.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	24.5968389511
Path: /gts1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEQCaqSUI%2Bht%2FqQUAAAAAh0om **URI:** http://ocsp.pki.goog/gts1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEQCaqSUI%2Bht%2FqQUAAAAAh0om						
ocsp.pki.goog	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	25.2217078209
Path: /gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEDV8NbKN%2BGCNBQAAAACHSlU%3D **URI:** http://ocsp.pki.goog/gts1o1core/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj%2Fxz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J%2FSsCEDV8NbKN%2BGCNBQAAAACHSlU%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	47.1984188557
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTfqhLjKLEJQZPin0KCzkdAQpVYowQUsT7DaQP4v0cB1JgmGggC72NkK8MCEATh56TcXPLzbcArQrhdFZ8%3D						
ocsp.digicert.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	47.4159188271
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEAJLrzIltpd3cj34Ka%2BNH60%3D **URI:** http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTPJvUY%2Bsl%2Bj4yzQuAcL2oQno5fCgQUUWj%2FkK8CB3U8zNllZGKiErhZcjsCEAJLrzIltpd3cj34Ka%2BNH60%3D						
xred.site50.net	80	GET	1.1	Synaptics.exe	1	48.0274598598
Path: /syn/Synaptics.rar **URI:** http://xred.site50.net/syn/Synaptics.rar						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	48.3176088333
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	48.5283029079

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTNMNJMNDqCqx8FcBWK16EHdimS6QQUU3m%2FWqorSs9UgOHYm8Cd8rIDZssCEH1bUSa0droR23QWC7xTDac%3D						
ocsp.sectigo.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	48.7383480072
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBRDC9IOTxN6GmyRjyTl2n4yTUczyAQUjYxexFStiuF36Zv5mwXhuAGNYeECECg%2FsnYZQBcbgheneePPERjY%3D **URI:** http://ocsp.sectigo.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBRDC9IOTxN6GmyRjyTl2n4yTUczyAQUjYxexFStiuF36Zv5mwXhuAGNYeECECg%2FsnYZQBcbgheneePPERjY%3D						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	56.7603168488
Path: /pki/crl/products/tspca.crl **URI:** http://crl.microsoft.com/pki/crl/products/tspca.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	56.842674017
Path: /pki/crl/products/CodeSignPCA2.crl **URI:** http://crl.microsoft.com/pki/crl/products/CodeSignPCA2.crl						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	56.9218609333
Path: /pki/crl/products/WinPCA.crl **URI:** http://crl.microsoft.com/pki/crl/products/WinPCA.crl						
crl.globalsign.net	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	57.0262598991
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
xred.mooo.com	A
Answers - (NXDOMAIN)	
freedns.afraid.org	A
Answers - 69.42.215.252 (A) - 50.23.197.95 (A)	
docs.google.com	A
Answers - 172.217.1.174 (A)	
ctldl.windowsupdate.com	A
Answers - 8.240.248.254 (A) - 8.252.237.126 (A) - 8.240.248.126 (A) - 8.252.236.254 (A) - au-bg-shim.trafficmanager.net (CNAME) - audownload.windowsupdate.nsatc.net (CNAME) - 8.240.37.254 (A) - auto.au.download.windowsupdate.com.c.footprint.net (CNAME)	

Request	Type
ocsp.pki.goog	A
Answers - 172.217.1.163 (A) - pki-goog.l.google.com (CNAME)	
doc-14-14-docs.googleusercontent.com	A
Answers - googlehosted.l.googleusercontent.com (CNAME) - 172.217.1.161 (A)	
www.dropbox.com	A
Answers - 162.125.6.18 (A) - www-env.dropbox-dns.com (CNAME)	
ocsp.digicert.com	A
Answers - cs9.wac.phicdn.net (CNAME) - 72.21.91.29 (A)	
xred.site50.net	A
Answers - 153.92.0.100 (A)	
www.000webhost.com	A
Answers - 104.18.108.8 (A) - 104.18.107.8 (A)	
ocsp.comodoca.com	A
Answers - 151.139.128.14 (A)	
ocsp.usertrust.com	A
ocsp.sectigo.com	A
crl.microsoft.com	A
Answers - 23.35.69.144 (A) - 23.35.69.154 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.18.21.226 (A) - global.prd.cdn.globalsign.com (CNAME) - cdn.globalsigncdn.com.cdn.cloudflare.net (CNAME) - 104.18.20.226 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
19.8013589382	Sandbox	69.42.215.252	80
21.3419418335	Sandbox	172.217.1.174	443
23.3184049129	Sandbox	8.240.248.254	80
24.3431129456	Sandbox	172.217.1.163	80
24.9660367966	Sandbox	172.217.1.161	443
46.8979229927	Sandbox	162.125.6.18	443
47.1984188557	Sandbox	72.21.91.29	80
48.0274598598	Sandbox	153.92.0.100	80
48.112790823	Sandbox	104.18.108.8	443
48.3176088333	Sandbox	151.139.128.14	80
48.5283029079	Sandbox	151.139.128.14	80
48.7383480072	Sandbox	151.139.128.14	80
56.7603168488	Sandbox	23.35.69.154	80
57.0262598991	Sandbox	104.18.20.226	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.73055887222	Sandbox	224.0.0.252	5355
6.75196480751	Sandbox	224.0.0.252	5355
6.76125383377	Sandbox	239.255.255.250	3702
6.80414795876	Sandbox	192.168.56.255	137
9.30603790283	Sandbox	224.0.0.252	5355
12.271160841	Sandbox	8.8.4.4	53
12.9292218685	Sandbox	192.168.56.255	138
15.7242128849	Sandbox	224.0.0.252	5355
19.7091879845	Sandbox	8.8.4.4	53
19.9057958126	Sandbox	224.0.0.252	5355
21.1612558365	Sandbox	8.8.4.4	53
23.2887058258	Sandbox	8.8.4.4	53
24.2952368259	Sandbox	8.8.4.4	53
24.929792881	Sandbox	8.8.4.4	53
46.8467409611	Sandbox	8.8.4.4	53
47.1661398411	Sandbox	8.8.4.4	53
47.8790287971	Sandbox	8.8.4.4	53
48.0809168816	Sandbox	8.8.4.4	53
48.3016598225	Sandbox	8.8.4.4	53
48.5202999115	Sandbox	8.8.4.4	53
48.7310948372	Sandbox	8.8.4.4	53
56.7173569202	Sandbox	8.8.4.4	53
56.9906418324	Sandbox	8.8.4.4	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Navs.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** abbcd5f6223c424751449bec2ad22c2c **SHA-1 :** e068b58ff64e4d24e7577207651819675911c5ec **SHA-256 :** 0f6b55e9914515777f1158f18bee1a73f23a2faf4(**SHA-512 :** 7feac725c2906545c319b7b4b48e4366ac541b4a **Size :** 843.046 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Apts.Txt	**Type :** ASCII text, with very long lines, with CRLF line terminators **MD5 :** a5711a01fb2a6b68fb3c054c96e65da3 **SHA-1 :** e33820013d73a499d178d7f7c8b245aada7a25f4 **SHA-256 :** 8a3b0f7ec60b8865eedd16589d6a651b6a0c608(**SHA-512 :** e2ecf93a12e1316625c6ecd93fb0fc589aad778efl **Size :** 2438.367 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 4795 bytes, 1 file **MD5 :** b36036ea05943e1a76472d713b8fcaf8 **SHA-1 :** d6fdd8c136667712c6fb4b618f70ba682e95dfb2 **SHA-256 :** e1226c395ff3cbdff09aa8e4e8bad3a02e8341a63 **SHA-512 :** 78737cc4812f7837dad6b6ebafbf96243cf283c3f(**Size :** 4.795 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CBDD1895DA987FB1E4F940B9391897BC	**Type :** data **MD5 :** 504b7c9eb381bbf97a42602f053b8fe9 **SHA-1 :** e575e985968392d1eee30036786a8c0207d8b548 **SHA-256 :** 1e6b01dfd2383d4528afd9937dd5af7c38080bec **SHA-512 :** 50d4f654916140106d68a8daeae50dbdc917991l **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC197601BE0898B7B0FCC91FA15D8A69_9C3330CF3BD3CFD21A37457CA8E40937	**Type :** data **MD5 :** e16dc9b9f2b943b4c85c64626991c426 **SHA-1 :** 06d0bd5f1877207575597cdbc1d8561ff0b3d708 **SHA-256 :** 6ca48ad88551f464a5f5a454e33eb7054385904d **SHA-512 :** a228257372c7dfcf829824030207ce5fe3872acdb **Size :** 0.471 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Cycle_info.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 4d3efb72221e05bf5ee4c957ba5e021b **SHA-1 :** 855d3885cd7249a2d7f8da419caeec050bd86c2a **SHA-256 :** 2532e3556aa9b3cf26ce9bd2ded555832438259; **SHA-512 :** 73034f43b8148a3c4b6c7daabc052ed36d3cadc2 **Size :** 0.646 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Msa.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 48ac89a14e687c9c88c0793d7a88f8eb **SHA-1 :** 5b1d9857f2d09dd74d85cd700ef91dbf324b1172 **SHA-256 :** 62efaab43f1e23f14b69b430b54fc7c9d4b29322c **SHA-512 :** 9f8ce1cbf89cdfa530a6033de5f1dd6d4a7c77081 **Size :** 694.934 Kilobytes.
C:\Users\User\AppData\Local\Temp\Aqvej1N.Ini	**Type :** ASCII text, with CRLF line terminators **MD5 :** 83056eea0a7571bc67eebaeef75fcc38 **SHA-1 :** 8ce32a9b8c7f764a7b5f481b0ef6281f7912fce2 **SHA-256 :** 9b24a4dc219f260c7dd248666d1fd4bb07be196e **SHA-512 :** 6e74e04704c9e5ce074ec3344b9ae4d6fd496434 **Size :** 0.095 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E	**Type :** data **MD5 :** cc891b6819a20fab9896a0124f9ff0cd **SHA-1 :** 483519d8905cb4468b5e3f5e69b95bce4ea6968a **SHA-256 :** 85c99131f671c26c64f6db599ae995a263a238d4 **SHA-512 :** 7fd931f17876951a5f106a149e69abfac8e5fb11c **Size :** 0.471 Kilobytes.
C:\ProgramData\Synaptics\Synaptics.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 2e7c2f10e3b5fc504fce72b92e8270da **SHA-1 :** d11a283fe1930918607582992a463dcb8a17fa5c **SHA-256 :** 957e9e8f037e884871d35c6369d9c6781a67d8d7 **SHA-512 :** 456fa079c3bcd32ce08073cf440d9c3d3ae55d883 **Size :** 776.704 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Awys.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** ec3a599878487a28596aa2802e9321d7 **SHA-1 :** 86240bac0a656c66a0edf0cecb543ed1705b1f56 **SHA-256 :** 8ea769ae4d7178aa42e2d32949cf135e819c9cb4 **SHA-512 :** 922cbcfe42445f31988235694a96b3d5286821c5 **Size :** 6992.758 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\F0bd292a-8c45-4a5a-Bb2b-8614b2fb027f.Index	**Type :** XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators **MD5 :** 0b41ea5eb31ad600a17d35072d9daea0 **SHA-1 :** a514474bdc5f59f450fe82f7fe5317bf0e079cc4 **SHA-256 :** 75a9a9f41ed85e5743c5ab4023fcee4cb8fd9c311 **SHA-512 :** a1786a45a66a247cd158fc5aaf4eeb3c4f32aed61 **Size :** 4.997 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Sids.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 4e6aea77bd34dff4711d43f9c1ec392d **SHA-1 :** 1bef48016397a9a5c436ad0e96b23115f2adeed0 **SHA-256 :** 594b5af354ef84ce92502b1c0f6ee0bbdf5d79f91 **SHA-512 :** a858c3e503c3ce0899916408137f42c1576389ea **Size :** 18198.101 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D	**Type :** data **MD5 :** 123d599c3e6c78968ed0739ff7345bd0 **SHA-1 :** 6e0bff323e852ae713ceb7f6f758635e86678387 **SHA-256 :** 926215bf0d3fb87b3a47d6c7fe020abc85eae3e8 **SHA-512 :** bcee13bb7ef44ee1a0bb20365107e577a842a0ea **Size :** 0.727 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 67cf0381383e4bf99339188f3054873d **SHA-1 :** f596fe6e623b716df084ac4c11f81eb7ac2a7ec6 **SHA-256 :** c2745491f7ce28ebd2ebe080774434c096b683f6 **SHA-512 :** a2087e00ae816203bb1edaa7d19d56108f2f695c **Size :** 0.34 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CBDD1895DA987FB1E4F940B9391897BC	**Type :** data **MD5 :** 9fcf02f0d85ae6575730c1cdf3672b4a **SHA-1 :** 97aa952226ec92726e9a58971c6186c36666c75d **SHA-256 :** 6e9428440e4ee8f863372a9d7c70d221e0ca1ee1 **SHA-512 :** 28cbe8ce1e04d8ad2e9bc3a0d5620905933bb73 **Size :** 0.471 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Stars.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 289015fb0b4de57b3cbfbd9241772861 **SHA-1 :** 9556c0a34a589b1fb9d584de18c821d29db10b66 **SHA-256 :** 6dff834f85915b101ca54c45440a80a5c78fad0e5 **SHA-512 :** 4c652f879164c666ff083353feda9b6f82245e7b0 **Size :** 14039.337 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B	**Type :** data **MD5 :** 48d7b88f7986388169c9f46bd8d48050 **SHA-1 :** f34113edae5d2fe7046d9250a019bc19cf6534cc **SHA-256 :** 679a3247b5f50991c3aef6f491cd5a5b0c55f1169 **SHA-512 :** fb43568a8419777a45ebf4a6325e3c256ce0c464f **Size :** 0.468 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC197601BE0898B7B0FCC91FA15D8A69_56D2979CE24B15FDD8BEBFC2EA707A7B	**Type :** data **MD5 :** ad3a0eadb032356a21a159e2ca6f1cb5 **SHA-1 :** 5dfd0bbf9f7792366e1f1e7a012ff471399927df **SHA-256 :** 74dc8ea899980ba831f2d971f44a3da11e1ecaeb **SHA-512 :** dca9d32b45c69e406a991d28e41838afd8b99062 **Size :** 0.422 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB	**Type :** data **MD5 :** ba2cbc6772049d509917f346b70c8d5b **SHA-1 :** 5a2362a1b82181fa7310e1a563b518cc28fe63ab **SHA-256 :** 2304d6361066b338ce55d0a9153ed6475cd0eb8 **SHA-512 :** aea39f10a9e4b97bad4534cbebb982c6776b960 **Size :** 0.426 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Ints.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 6326209c7fe7c627c80d9a44e4abda35 **SHA-1 :** 5a0bdf1873db6bee160f03e029c795a2e999ad1e **SHA-256 :** 6e10ce9d16bfabcec6b553c3ae2b34c28c1600fcc **SHA-512 :** db3fdac4e5e43dfcd35d22ced4e44739c25e5aa5 **Size :** 23366.612 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CFE86DBBE02D859DC92F1E17E0574EE8_46766FC45507C0B9E264E4C18BC7288B	**Type :** data **MD5 :** cc1a7234ed548192d7d1d400104ed654 **SHA-1 :** 37b1d88cf199b81eaf18ab086a2fec3e10b2e601 **SHA-256 :** 7a36422890d2e8b248eb00007ec523f86754bef1 **SHA-512 :** 8ac7deba6c5fad4d7f0cf49c27b62420613ef26b4 **Size :** 0.394 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\EDC238BFF48A31D55A97E1E93892934B_C20E0DA2D0F89FE526E1490F4A2EE5AB	**Type :** data **MD5 :** 0e2f0d3d27341975f32f9f6b9b8c62e8 **SHA-1 :** 39ff5d57098b06b237199474c1db65046c5b4f51 **SHA-256 :** c634d331814f1248bc024dce1b053de92c49c294 **SHA-512 :** 0bb81a1e6945a20c09a31b1e4bba29a93046be4 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Local\Temp\Is-KLJBF.Tmp_isetup_setup64.Tmp	**Type :** PE32+ executable (console) x86-64, for MS Windows **MD5 :** e4211d6d009757c078a9fac7ff4f03d4 **SHA-1 :** 019cd56ba687d39d12d4b13991c9a42ea6ba03da **SHA-256 :** 388a796580234efc95f3b1c70ad4cb44bfddc7ba **SHA-512 :** 17257f15d843e88bb78adcfb48184b8ce22109cc **Size :** 6.144 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC197601BE0898B7B0FCC91FA15D8A69_9C3330CF3BD3CFD21A37457CA8E40937	**Type :** data **MD5 :** 650ad947dfd01f3b364d2fb2681ec79b **SHA-1 :** eb56eaedfcc753f885161d5829a26cbd8fe32261 **SHA-256 :** 424b0c1bb1e6ceba66b5a5e0d7e5bd416e7f4ecf **SHA-512 :** f803356b3617f005d5848e6b399e4f5ccfa5cab7c **Size :** 0.422 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\35DDEDF268117918D1D277A171D8DF7B_A29FED777819EBFE086A4D0443378D69	**Type :** data **MD5 :** b5f61c13bc210e86afe2f0350a9bab73 **SHA-1 :** bb01b06a29eedfe616bd6c1f3575befcadf7c192 **SHA-256 :** 823560609a0865c8f006b24cfa10f9dbefcd7b273 **SHA-512 :** 188ca2ed9c75ddbe216c5e9e2d90b38ecb36e8c **Size :** 0.471 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Is-VR9FB.Tmp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.Tmp	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** aec467f5a2de2c2164cd710708c51b89 **SHA-1 :** 6221c2c9d2bcdb09ea8b9217e21b3a27a074302e **SHA-256 :** 322a05a3dc4d70338554e12ee04b5a25e3d7abb **SHA-512 :** 110f0dfa75774b8fa9626079a0b424362ed22e83 **Size :** 2580.992 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\B2FAF7692FD9FFBD64EDE317E42334BA_D7393C8F62BDE4D4CB606228BC7A711E	**Type :** data **MD5 :** d6d8ac0c3635a22d95489c5cb3937484 **SHA-1 :** 13f71d4486229c2bc0b8cfac8662b33e459c5e6f **SHA-256 :** f5507b945045d589bef7bae32bf5a21dadc7ba86 **SHA-512 :** d5c86ab42dca89ebbe5e02958924ccd304eaea0 **Size :** 0.396 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Aptcomms.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 587b9fcd489454936d211832188892db **SHA-1 :** 8190d9f01d06ff917036f06f9351cc9c56ee9e7a **SHA-256 :** 3eef082e485de6786cdab750b9528f60ecf78e0d **SHA-512 :** d6bddba82bf9cddca5989950a4df4fbadb1dbde1 **Size :** 2974.158 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC197601BE0898B7B0FCC91FA15D8A69_56D2979CE24B15FDD8BEBFC2EA707A7B	**Type :** data **MD5 :** fe36235cdc49e1babafbc923405498b1 **SHA-1 :** dca7d7434f6e13bc3c531fafef9f4de21bcd6f7a **SHA-256 :** 0b575d32c9cbd52f72431145c2da96a2915a968c **SHA-512 :** 72fc54e5bb08f7766e6185867a356a8034b8cff9b **Size :** 0.472 Kilobytes.
C:\Users\User\AppData\Local\Temp\FiKsUTxWa.Exe	**Type :** ASCII text, with no line terminators **MD5 :** 7b5ea53ba332630e5aca8e4abb807f70 **SHA-1 :** d78ce9bb512ba2daf191b2d02729ba41ab1924ee **SHA-256 :** 66a1aec8c3669c1c2e13625849996ab09a81a4df **SHA-512 :** ea85ebf524b655672b32c2ef09f178f11ce03979a **Size :** 0.016 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** Microsoft Cabinet archive data, 58596 bytes, 1 file **MD5 :** 61a03d15cf62612f50b74867090dbe79 **SHA-1 :** 15228f34067b4b107e917bebaf17cc7c3c1280a8 **SHA-256 :** f9e23dc21553daa34c6eb778cd262831e466ce79 **SHA-512 :** 5fece89ccbbf994e4f1e3ef89a502f25a72f359d44 **Size :** 58.596 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\35DDEDF268117918D1D277A171D8DF7B_A29FED777819EBFE086A4D0443378D69	**Type :** data **MD5 :** b615a28af35f4bff3172371282046dc2 **SHA-1 :** 44a0f323945d74853c54a467fad629d33071a529 **SHA-256 :** 81d6406d2b942705bc687317095a6be5cc52a2d **SHA-512 :** 2c3e7aab4a3f62fc11afbb40e476a829bd8c7020f **Size :** 0.442 Kilobytes.
C:\Users\User\AppData\Local\Temp\._cache_263610b09096511eb54892a82b7d631ac6ec4995.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 35c36c476b59e13ff5b66e31aa9ce787 **SHA-1 :** b6a8df7b32604a3349afadd58e7789add7ca65f9 **SHA-256 :** c44b7140d3fe9500a48715b0251fe0fa9e17b856 **SHA-512 :** b8968806545002ec2273db8866f045345ae401ea **Size :** 11097.04 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\07CEF2F654E3ED6050FFC9B6EB844250_3431D4C539FB2CFCB781821E9902850D	**Type :** data **MD5 :** 4f98bd48fb09ce64f0b89512dc035dd1 **SHA-1 :** 36422a09777915153b5a7a6175f0cd80a62ca212 **SHA-256 :** 7397f867078815d2f03ad8e4a1ba9831c1bfe3d1 **SHA-512 :** 565718e359cd8765b4993713c5ecbd138e5c06cf **Size :** 0.402 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** 3111eceb672039c8e08bf3d6bd76e689 **SHA-1 :** 74a514240de7c14df3b1b28f363c687be9d49248 **SHA-256 :** e3e9eca1d7a3b8920af099023a6e0bb142c1849(**SHA-512 :** 4f6c13d4752c69162453bf66e135f2f4b74e1c7f6a **Size :** 0.326 Kilobytes.
C:\Program Files (X86)\Qualitywings\QW787\Navdata\Apps.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** 370274f1e57bd6799b89380aa67e6ee7 **SHA-1 :** 7b38716122f698a3d470b6ad4bbdf300099a30ff **SHA-256 :** 88aa2f05bb8ab855b86d82dc8e3412434bed91f(**SHA-512 :** 41cb496effe0627ec040859c276a12787e8522e8(**Size :** 35653.283 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	qw787_2102v2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	263610b09096511eb54892a82b7d631ac6ec4995
MD5:	979f958d3a5f08efc058fe85f58bac6e
First Seen Date:	2021-03-05 07:12:04.481642 (3 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2021-03-05 07:12:04.481642 (3 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	8
Trid	[[79.0, u'Win32 Executable Borland Delphi 7'], [13.0, u'Inno Setup installer'], [4.9, u'Win32 EXE PECompact compressed (generic)'], [1.6, u'Win32 Executable Delphi generic'], [0.5, u'Win32 Executable (generic)']]
Compilation Time Stamp	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC] [SUSPICIOUS]
LegalCopyright	
InternalName	
FileVersion	1.0.0.4
CompanyName	Synaptics
LegalTrademarks	
Comments	
ProductName	Synaptics Pointing Device Driver
ProductVersion	1.0.0.0
FileDescription	Synaptics Pointing Device Driver
OriginalFilename	
Translation	0x041f 0x04e6
Entry Point	0x49ab80 (CODE)
Machine Type	Intel 386 or later - 32Bit
File Size	11873792
Ssdeep	196608:hLOr+f5WK3giPQSFbredGAZpbw79NRbOqQnKoG/Pn3Sw70OZb:h5kCgXS5rIGxRbOfKo8n3R7FZb
Sha256	5cf16b5f456f7a7142b719af75bcbbde7249e596e89b8fe7ccabb4ef7782fce9
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/6/3/6/263610b09096511eb54892a82b7d631ac6ec4995', u'EXE:OriginalFileName': u'', u'EXE:ProductName': u'Synaptics Pointing Device Driver', u'EXE:InternalName': u'', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2021:03:05 07:11:30+00:00', u'EXE:InitializedDataSize': 11243008, u'File:FileModifyDate': u'2021:03:05 07:11:29+00:00', u'EXE:FileVersionNumber': u'1.0.0.4', u'EXE:FileVersion': u'1.0.0.4', u'File:FileSize': u'11 MB', u'EXE:CharacterSet': u'Windows, Turkish', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Synaptics', u'File:FileName': u'263610b09096511eb54892a82b7d631ac6ec4995', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'1992:06:19 22:22:17+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'', u'EXE:LinkerVersion': 2.25, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/2/6/3/6', u'EXE:FileDescription': u'Synaptics Pointing Device Driver', u'EXE:EntryPoint': u'0x9ab80', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 629760, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2021:03:05 07:11:30+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Turkish', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.4'}]
Mime Type	application/x-dosexec
Imphash	332f7ce65ead0adfb3d35147033aabe9

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
CODE	0x1000	0x99bec	0x99c00	6.57295787036	33fbe30e8a64654287edd1bf05ae7c8c
DATA	0x9b000	0x2e54	0x3000	4.85462079781	1f5e19e7d20c1d128443d738ac7bc610
BSS	0x9e000	0x11e5	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0xa0000	0x2a42	0x2c00	4.91933321603	21ff53180b390dc06e3a1adf0e57a073
.tls	0xa3000	0x10	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0xa4000	0x39	0x200	0.784620157709	a92cf494c617731a527994013429ad97
.reloc	0xa5000	0xa980	0xaa00	6.67412498558	dcd1b1c3f3d28d444920211170d1e8e6
.rsrc	0xb0000	0xaa8418	0xaa8600	7.97060735553	431de89dd63dc3eab0290a5f61adedf8

PE Imports

- kernel32.dll
  - DeleteCriticalSection
  - LeaveCriticalSection
  - EnterCriticalSection
  - InitializeCriticalSection
  - VirtualFree
  - VirtualAlloc
  - LocalFree
  - LocalAlloc
  - GetTickCount
  - QueryPerformanceCounter
  - GetVersion
  - GetCurrentThreadId
  - InterlockedDecrement
  - InterlockedIncrement
  - VirtualQuery
  - WideCharToMultiByte
  - SetCurrentDirectoryA
  - MultiByteToWideChar
  - lstrlenA
  - lstrcpynA
  - LoadLibraryExA
  - GetThreadLocale
  - GetStartupInfoA
  - GetProcAddress
  - GetModuleHandleA
  - GetModuleFileNameA
  - GetLocaleInfoA
  - GetLastError
  - GetCurrentDirectoryA
  - GetCommandLineA
  - FreeLibrary
  - FindFirstFileA
  - FindClose
  - ExitProcess
  - ExitThread
  - CreateThread
  - WriteFile
  - UnhandledExceptionFilter
  - SetFilePointer
  - SetEndOfFile
  - RtlUnwind
  - ReadFile
  - RaiseException
  - GetStdHandle
  - GetFileSize
  - GetFileType
  - CreateFileA
  - CloseHandle
- user32.dll
  - GetKeyboardType
  - LoadStringA
  - MessageBoxA
  - CharNextA

- advapi32.dll
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegCloseKey
- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- kernel32.dll
  - TlsSetValue
  - TlsGetValue
  - LocalAlloc
  - GetModuleHandleA
- advapi32.dll
  - RegSetValueExA
  - RegQueryValueExA
  - RegOpenKeyExA
  - RegNotifyChangeKeyValue
  - RegFlushKey
  - RegDeleteValueA
  - RegCreateKeyExA
  - RegCloseKey
  - OpenProcessToken
  - LookupPrivilegeValueA
  - GetUserNameA
  - AdjustTokenPrivileges
- kernel32.dll
  - lstrcpyA
  - WritePrivateProfileStringA
  - WriteFile
  - WaitForSingleObject
  - WaitForMultipleObjects
  - VirtualQuery
  - VirtualAlloc
  - UpdateResourceA
  - UnmapViewOfFile
  - TerminateProcess
  - Sleep
  - SizeofResource
  - SetThreadLocale
  - SetFilePointer
  - SetFileAttributesA
  - SetEvent
  - SetErrorMode
  - SetEndOfFile
  - ResumeThread
  - ResetEvent
  - RemoveDirectoryA
  - ReadFile
  - OpenProcess
  - OpenMutexA
  - MultiByteToWideChar
  - MulDiv
  - MoveFileA
  - MapViewOfFile
  - LockResource
  - LoadResource
  - LoadLibraryA
  - LeaveCriticalSection
  - InitializeCriticalSection
  - GlobalUnlock
  - GlobalReAlloc
  - GlobalHandle
  - GlobalLock
  - GlobalFree
  - GlobalFindAtomA
  - GlobalDeleteAtom
  - GlobalAlloc
  - GlobalAddAtomA
  - GetVersionExA
  - GetVersion
  - GetTimeZoneInformation
  - GetTickCount
  - GetThreadLocale
  - GetTempPathA

    - GetTempFileNameA
    - GetSystemInfo
    - GetSystemDirectoryA
    - GetStringTypeExA
    - GetStdHandle
    - GetProcAddress
    - GetPrivateProfileStringA
    - GetModuleHandleA
    - GetModuleFileNameA
    - GetLogicalDrives
    - GetLocaleInfoA
    - GetLocalTime
    - GetLastError
    - GetFullPathNameA
    - GetFileSize
    - GetFileAttributesA
    - GetExitCodeThread
    - GetDriveTypeA
    - GetDiskFreeSpaceA
    - GetDateFormatA
    - GetCurrentThreadId
    - GetCurrentProcessId
    - GetCurrentProcess
    - GetComputerNameA
    - GetCPInfo
    - GetACP
    - FreeResource
    - InterlockedIncrement
    - InterlockedExchange
    - InterlockedDecrement
    - FreeLibrary
    - FormatMessageA
    - FindResourceA
    - FindNextFileA
    - FindFirstFileA
    - FindClose
    - FileTimeToLocalFileTime
    - FileTimeToDosDateTime
    - EnumCalendarInfoA
    - EnterCriticalSection
    - EndUpdateResourceA
    - DeleteFileA
    - DeleteCriticalSection
    - CreateThread
    - CreateProcessA
    - CreatePipe
    - CreateMutexA
    - CreateFileMappingA
    - CreateFileA
    - CreateEventA
    - CreateDirectoryA
    - CopyFileA
    - CompareStringA
    - CloseHandle
    - BeginUpdateResourceA
- version.dll
    - VerQueryValueA
    - GetFileVersionInfoSizeA
    - GetFileVersionInfoA
- gdi32.dll
    - UnrealizeObject
    - StretchBlt
    - SetWindowOrgEx
    - SetWinMetaFileBits
    - SetViewportOrgEx
    - SetTextColor
    - SetStretchBltMode
    - SetROP2
    - SetPixel
    - SetEnhMetaFileBits
    - SetDIBColorTable
    - SetBrushOrgEx
    - SetBkMode
    - SetBkColor
    - SelectPalette

    - SelectObject
    - SaveDC
    - RestoreDC
    - RectVisible
    - RealizePalette
    - PlayEnhMetaFile
    - PatBlt
    - MoveToEx
    - MaskBlt
    - LineTo
    - IntersectClipRect
    - GetWindowOrgEx
    - GetWinMetaFileBits
    - GetTextMetricsA
    - GetTextExtentPoint32A
    - GetSystemPaletteEntries
    - GetStockObject
    - GetPixel
    - GetPaletteEntries
    - GetObjectA
    - GetEnhMetaFilePaletteEntries
    - GetEnhMetaFileHeader
    - GetEnhMetaFileBits
    - GetDeviceCaps
    - GetDIBits
    - GetDIBColorTable
    - GetDCOrgEx
    - GetCurrentPositionEx
    - GetClipBox
    - GetBrushOrgEx
    - GetBitmapBits
    - GdiFlush
    - ExcludeClipRect
    - DeleteObject
    - DeleteEnhMetaFile
    - DeleteDC
    - CreateSolidBrush
    - CreatePenIndirect
    - CreatePalette
    - CreateHalftonePalette
    - CreateFontIndirectA
    - CreateDIBitmap
    - CreateDIBSection
    - CreateCompatibleDC
    - CreateCompatibleBitmap
    - CreateBrushIndirect
    - CreateBitmap
    - CopyEnhMetaFileA
    - BitBlt
- user32.dll
    - CreateWindowExA
    - WindowFromPoint
    - WinHelpA
    - WaitMessage
    - UpdateWindow
    - UnregisterClassA
    - UnhookWindowsHookEx
    - TranslateMessage
    - TranslateMDISysAccel
    - TrackPopupMenu
    - ToAsciiEx
    - SystemParametersInfoA
    - ShowWindow
    - ShowScrollBar
    - ShowOwnedPopups
    - ShowCursor
    - SetWindowsHookExA
    - SetWindowTextA
    - SetWindowPos
    - SetWindowPlacement
    - SetWindowLongA
    - SetTimer
    - SetScrollRange
    - SetScrollPos
    - SetScrollInfo

- SetRect
- SetPropA
- SetParent
- SetMenuItemInfoA
- SetMenu
- SetForegroundWindow
- SetFocus
- SetCursor
- SetClassLongA
- SetCapture
- SetActiveWindow
- SendMessageA
- ScrollWindow
- ScreenToClient
- RemovePropA
- RemoveMenu
- ReleaseDC
- ReleaseCapture
- RegisterWindowMessageA
- RegisterClipboardFormatA
- RegisterClassA
- RedrawWindow
- PtInRect
- PostQuitMessage
- PostMessageA
- PeekMessageA
- OffsetRect
- OemToCharA
- MsgWaitForMultipleObjects
- MessageBoxA
- MapWindowPoints
- MapVirtualKeyExA
- MapVirtualKeyA
- LoadStringA
- LoadKeyboardLayoutA
- LoadIconA
- LoadCursorA
- LoadBitmapA
- KillTimer
- IsZoomed
- IsWindowVisible
- IsWindowEnabled
- IsWindow
- IsRectEmpty
- IsIconic
- IsDialogMessageA
- IsChild
- InvalidateRect
- IntersectRect
- InsertMenuItemA
- InsertMenuA
- InflateRect
- GetWindowThreadProcessId
- GetWindowTextLengthA
- GetWindowTextA
- GetWindowRect
- GetWindowPlacement
- GetWindowLongA
- GetWindowDC
- GetTopWindow
- GetSystemMetrics
- GetSystemMenu
- GetSysColorBrush
- GetSysColor
- GetSubMenu
- GetScrollRange
- GetScrollPos
- GetScrollInfo
- GetPropA
- GetParent
- GetWindow
- GetMenuStringA
- GetMenuState
- GetMenuItemInfoA
- GetMenuItemID

    - GetMenuItemCount
    - GetMenu
    - GetLastActivePopup
    - GetKeyboardState
    - GetKeyboardLayoutList
    - GetKeyboardLayout
    - GetKeyState
    - GetKeyNameTextA
    - GetIconInfo
    - GetForegroundWindow
    - GetFocus
    - GetDesktopWindow
    - GetDCEx
    - GetDC
    - GetCursorPos
    - GetCursor
    - GetClipboardData
    - GetClientRect
    - GetClassNameA
    - GetClassInfoA
    - GetCapture
    - GetActiveWindow
    - FrameRect
    - FindWindowA
    - FillRect
    - EqualRect
    - EnumWindows
    - EnumThreadWindows
    - EndPaint
    - EnableWindow
    - EnableScrollBar
    - EnableMenuItem
    - DrawTextA
    - DrawMenuBar
    - DrawIconEx
    - DrawIcon
    - DrawFrameControl
    - DrawEdge
    - DispatchMessageA
    - DestroyWindow
    - DestroyMenu
    - DestroyIcon
    - DestroyCursor
    - DeleteMenu
    - DefWindowProcA
    - DefMDIChildProcA
    - DefFrameProcA
    - CreatePopupMenu
    - CreateMenu
    - CreateIcon
    - ClientToScreen
    - CheckMenuItem
    - CallWindowProcA
    - CallNextHookEx
    - BeginPaint
    - CharNextA
    - CharLowerBuffA
    - CharLowerA
    - CharUpperBuffA
    - CharToOemA
    - AdjustWindowRectEx
    - ActivateKeyboardLayout
- ole32.dll
    - CLSIDFromString
- kernel32.dll
    - Sleep
- oleaut32.dll
    - SafeArrayPtrOfIndex
    - SafeArrayGetUBound
    - SafeArrayGetLBound
    - SafeArrayCreate
    - VariantChangeType
    - VariantCopyInd
    - VariantCopy
    - VariantClear

- VariantInit
- ole32.dll
  - CLSIDFromProgID
  - CoCreateInstance
  - CoUninitialize
  - CoInitialize
- oleaut32.dll
  - GetErrorInfo
  - SysFreeString
- comctl32.dll
  - ImageList_SetIconSize
  - ImageList_GetIconSize
  - ImageList_Write
  - ImageList_Read
  - ImageList_GetDragImage
  - ImageList_DragShowNolock
  - ImageList_SetDragCursorImage
  - ImageList_DragMove
  - ImageList_DragLeave
  - ImageList_DragEnter
  - ImageList_EndDrag
  - ImageList_BeginDrag
  - ImageList_Remove
  - ImageList_DrawEx
  - ImageList_Draw
  - ImageList_GetBkColor
  - ImageList_SetBkColor
  - ImageList_ReplaceIcon
  - ImageList_Add
  - ImageList_GetImageCount
  - ImageList_Destroy
  - ImageList_Create
- shell32.dll
  - ShellExecuteExA
  - ExtractIconExW
- wininet.dll
  - InternetGetConnectedState
  - InternetReadFile
  - InternetOpenUrlA
  - InternetOpenA
  - InternetCloseHandle
- shell32.dll
  - SHGetSpecialFolderLocation
  - SHGetPathFromIDListA
  - SHGetMalloc
  - SHGetDesktopFolder
- advapi32.dll
  - OpenSCManagerA
  - CloseServiceHandle
- wsock32.dll
  - WSACleanup
  - WSAStartup
  - gethostname
  - gethostbyname
  - inet_ntoa
- netapi32.dll
  - Netbios

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 724496, u'sha256': u'b8e6fc93d423931acbddae3c27dd3c4eb2a394005d746951a971cb700e0ee510', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 724804, u'sha256': u'ce19ace18e87b572e6912306776226af5b8e63959c61cde70a8ff05b3bbdcc41', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 725112, u'sha256': u'ee1c9c194199c320c893b367602ccc7ee7270bd4395d029f727e097634f47f8c', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 725420, u'sha256': u'9d9edf87ca203ecc60b246cc783d54218dd0ce77d3a025d0bafc580995a4abd8', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 725728, u'sha256': u'99676c52310db365580965ea646ece86c62951bfd97ec0aae9f738a202a90593', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 726036, u'sha256': u'11726dcf1eebe23a1df5eb0ee2af39196b702eddd69083d646e4475335130b28', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_CURSOR', u'offset': 726344, u'sha256': u'6f938aab0a03120de4ef8b27aff6ba5146226c92a056a6f04e5ec8d513ce5f9d', u'type': u'data', u'size': 308}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 726652, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 727116, u'sha256': u'46cfc44afa8ab31ae3da35fa8346e4c085c441659d9992b09fc8ad517f2b289a', u'type': u'data', u'size': 484}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 727600, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 728064, u'sha256': u'f8e1696801fe89b88936ac4226cea03bfa5aa345aa33ca982822ae7fbc6557e2', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 728528, u'sha256': u'cb7421b5c6af74c3159c361f3bb78bba8a488d8979d1250e106fa96cbf928789', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 728992, u'sha256': u'41f05a4df5f42d92b879493d51941de342d36460fe15c0f3b63b2b706b928fef', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 729456, u'sha256': u'81265e63c89ee5c2e5126452e22f84e9be9452449f3e5959ab6d346cb58b2bde', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 729920, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 730384, u'sha256': u'c925e4a8cbf6d42dbb1220a510614df725558f8d843338982bab8c4e020f6429', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 730848, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 731312, u'sha256': u'78507a772de646626b196a743cee75b298a68c33a0fd482842071519d59037b2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 232}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 731544, u'sha256': u'dec2547f536093fb8a565852495fe167848eb8c538fbee49be4c154a1c260995', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 33554431, next used block 33554431', u'size': 4264}

{u'lang': u'LANG_TURKISH', u'name': u'RT_ICON', u'offset': 735808, u'sha256': u'6337744af29ef05448693f358ecca2ebaf50c1e5727984b3ded297eaad620656', u'type': u'dBase IV DBT of @.DBF, block length 8192, next free block index 40', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 740072, u'sha256': u'fb2788eb87c3d5203e191d692d2e7ea6c29f04e2e6634563bc02a72ff06de6da', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 744336, u'sha256': u'771f64afb45a9edc8c4f6c5b2039f9b32623cea53bf0cab5bf1f371cc5d1abe4', u'type': u'data', u'size': 82}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 744420, u'sha256': u'9406ad45100979271d17583bd0a5b96faf9fc8e2c404d119243c7a07dec91ea5', u'type': u'data', u'size': 856}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 745276, u'sha256': u'48f94d39fddf5b49cd62e37f087ac3b173867887b6a0c7910c2823ebf154c45a', u'type': u'data', u'size': 1064}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 746340, u'sha256': u'8d5c0458d17f37b964ffbede71dad948082861df4ac4ef52b9df9660a1dbfd5e', u'type': u'data', u'size': 932}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 747272, u'sha256': u'fd892046a2c300ae0db1b95758644a279ae55deb5ede1aee3b0762f644dadab1', u'type': u'data', u'size': 956}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 748228, u'sha256': u'f1c4ccdaf0b6b9497838b39b4192241d3e234e8049416300ac784c2fd8a2f4d2', u'type': u'data', u'size': 724}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 748952, u'sha256': u'73059ae649fdcc96c78d5bb590de1b31a930e3289091d3cdb50f1b5790fa568c', u'type': u'data', u'size': 820}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 749772, u'sha256': u'606fb52153d458210317a109d47686cdc16b014bcb3bdfc0289e957064089b9b', u'type': u'Sendmail frozen configuration - version c', u'size': 1068}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 750840, u'sha256': u'f534be58036ba5fe6d0304f55a7854eb3be404b9749f90b377aae264fafff9e6', u'type': u'data', u'size': 496}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 751336, u'sha256': u'051b09c8f17e697b0bd33cf78f6c1353a57952311ce0c42b8247b9b95dfa55b4', u'type': u'data', u'size': 448}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 751784, u'sha256': u'9793da0b5d865b5c7459898963efdded269c1adbf9f9e1642a41022767602487', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 220}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 752004, u'sha256': u'6f21318189a8fa483926858c8c2ccb45b443ad29ec952c55888e2f2fc0db73a4', u'type': u'data', u'size': 800}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 752804, u'sha256': u'8a116965e47a126e76a52213dd5c82d32988b906d4c98a90f483a5d8d4a4731e', u'type': u'data', u'size': 216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 753020, u'sha256': u'b916a1a33c30ee9f9ce0f66d301c2a8680174e765fa64c97fbab32cf31690638', u'type': u'data', u'size': 280}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 753300, u'sha256': u'1fb450810c56933c01a31ede713549ec027f70e9e9c93cc87f1fbf0fa69fc266', u'type': u'data', u'size': 616}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 753916, u'sha256': u'db72fc4acec5aec31f6965314a9dc108611a1b82b1cb675b0570ed8d61b59007', u'type': u'data', u'size': 1016}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 754932, u'sha256': u'9ab26754885eda425dcf0a58977d4da2307b5793b8fa5f8b7df31761d2c80b6c', u'type': u'data', u'size': 888}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 755820, u'sha256': u'2c19967d95bd04d6d4a5fabca1188b266bc5b3d5e22b414537acc746fcd92ef6', u'type': u'data', u'size': 896}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 756716, u'sha256':

u'7f4902d1959e79f5816454e6798a5d72b772cefe4b3bb8dbfffafb1834568697', u'type': u'data', u'size': 884}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 757600, u'sha256': u'05460789da581e375d4a9626e7dc592714a2cc7535497a08dbbb78521fc7a964', u'type': u'data', u'size': 224}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 757824, u'sha256': u'8a87da2d7d96cc00a994fd755cac4285d1d05f578c6f7f9292bda53cb182b0b8', u'type': u'data', u'size': 188}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 758012, u'sha256': u'28fa1bdd9fde66292bf9e89d02f8ee2fe49a9fdcade6cf07d917ee59075c345e', u'type': u'data', u'size': 872}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 758884, u'sha256': u'50724df651f6ecc7dcb00851d5003cd0bec67c99445a41b5fe1a46ddc3f88024', u'type': u'data', u'size': 1020}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 759904, u'sha256': u'b6764bfcca8110bf12518f0c04d74c3e5c5d2b83bad0c55947c4a70cd20cbfc2', u'type': u'data', u'size': 764}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 760668, u'sha256': u'd5a14a12e214945e49ef2029984a595603bf41798a8555b27f0c1907c9167f6b', u'type': u'data', u'size': 852}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 761520, u'sha256': u'b81183489531e29e300a262d179a86a174fbd787e4ca40e50970912a5b1785bc', u'type': u'data', u'size': 68}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 761588, u'sha256': u'88d14cc6638af8a0836f6d868dfab60df92907a2d7becaefbbd7e007acb75610', u'type': u'Sendmail frozen configuration ', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 761604, u'sha256': u'c44b7140d3fe9500a48715b0251fe0fa9e17b8564b99a84914ef2a132c0f31be', u'type': u'PE32 executable (GUI) Intel 80386, for MS Windows', u'size': 11097040}

{u'lang': u'LANG_TURKISH', u'name': u'RT_RCDATA', u'offset': 11858644, u'sha256': u'482d9673cfee5de391f97fde4d1c84f9f8d6f2cf0784fcffb958b4032de7236c', u'type': u'ASCII text, with no line terminators', u'size': 3}

{u'lang': u'LANG_TURKISH', u'name': u'RT_RCDATA', u'offset': 11858648, u'sha256': u'b9eae90f8e942cc4586d31dc484f29079651ad64c49f90d99f86932630c66af2', u'type': u'PE32 executable (DLL) (GUI) Intel 80386, for MS Windows', u'size': 15360}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 11874008, u'sha256': u'0e76bcb8dd589d6b867c947bcd558ab8e3f81c8e76075575214a574f3f998eb7', u'type': u'data', u'size': 1612}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 11875620, u'sha256': u'274de2cda082c44a6680e508948f01cd14f75631b65af1be920a8cad7cd5394c', u'type': u"Delphi compiled form 'TFormVir'", u'size': 339}

{u'lang': u'LANG_TURKISH', u'name': u'RT_RCDATA', u'offset': 11875960, u'sha256': u'8e574b4ae6502230c0829e2319a6c146aebd51b7008bf5bbfb731424d7952c15', u'type': u'Microsoft Excel 2007+', u'size': 18387}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894348, u'sha256': u'c53efa8085835ba129c1909beaff8a67b45f50837707f22dfff0f24d8cd26710', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894368, u'sha256': u'b07e022f8ef0a8e5fd3f56986b2e5bf06df07054e9ea9177996b0a6c27d74d7c', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894388, u'sha256': u'43f40dd5140804309a4c901ec3c85b54481316e67a6fe18beb9d5c0ce3a42c3a', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894408, u'sha256': u'ff47a48c11c234903a7d625cb8b62101909f735ad84266c98dd4834549452c39', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894428, u'sha256': u'a0adcedb82b57089f64e2857f97cefd6cf25f4d27eefc6648bda83fd5fef66bb', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894448, u'sha256': u'6e1e7738a1b6373d8829f817915822ef415a1727bb5bb7cfe809e31b3c143ac5', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_CURSOR', u'offset': 11894468, u'sha256': u'326c048595bbc72e3f989cb3b95fbf09dc83739ced3cb13eb6f03336f95d74f1', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_TURKISH', u'name': u'RT_GROUP_ICON', u'offset': 11894488, u'sha256': u'a14e70ed824f3f17d3a51136aa08839954d6d3ccadaa067415c7bfc08e6636b0', u'type': u'MS Windows icon resource - 1 icon, 32x32', u'size': 20}

{u'lang': u'LANG_TURKISH', u'name': u'RT_VERSION', u'offset': 11894508, u'sha256': u'85f6fa8b937925722f2daca9091fbbfbabe54189e016fd51ecc79e2d941ad045', u'type': u'data', u'size': 772}

{u'lang': u'LANG_CHINESE', u'name': u'RT_VERSION', u'offset': 11895280, u'sha256': u'eb6e895da8ac5f5d0bf2e7b933cc83acfc7f0a8052f30f8aace011a1052b5bd3', u'type': u'data', u'size': 552}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS