Summary

File Name: Signed_Purchase_Order.exe

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

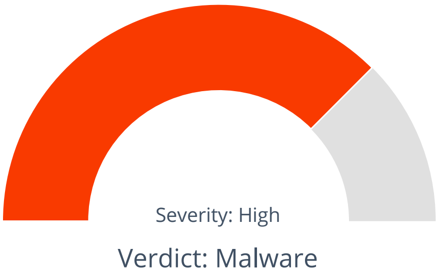
SHA1: ae841f2530c6fd8dbcf49793c6914347964b605c

MD5: 49ba1ce699db15e472b1a633ac4445da

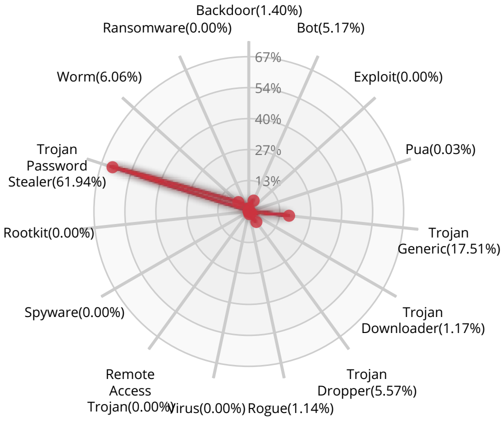
MALWARE

Valkyrie Final Verdict

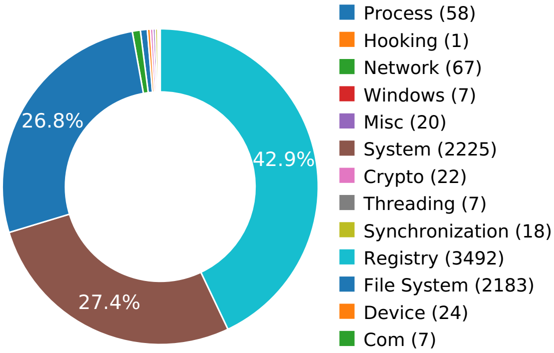
DETECTION SECTION



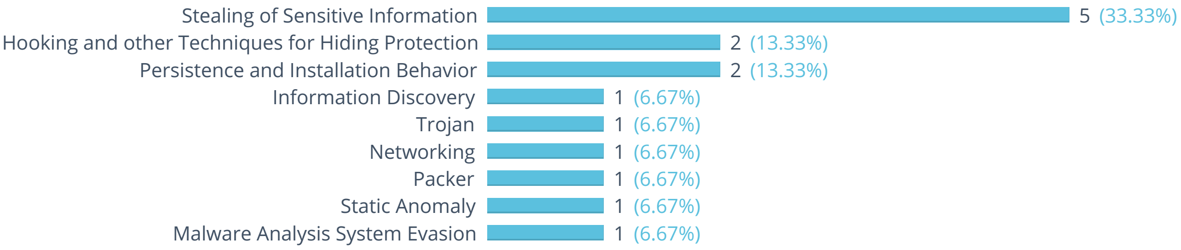
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

TROJAN

Exhibits behavior characteristic of Pony malware — Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) — Show sources

PACKER

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

STEALING OF SENSITIVE INFORMATION

Attempts to access Bitcoin/ALTCoin wallets — Show sources

Steals private information from local Internet browsers — Show sources

Collects information about installed applications — Show sources

Harvests credentials from local FTP client softwares — Show sources

Harvests information related to installed mail clients — Show sources

STATIC ANOMALY

Anomalous binary characteristics — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

Executed a process and injected code into it, probably while unpacking — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

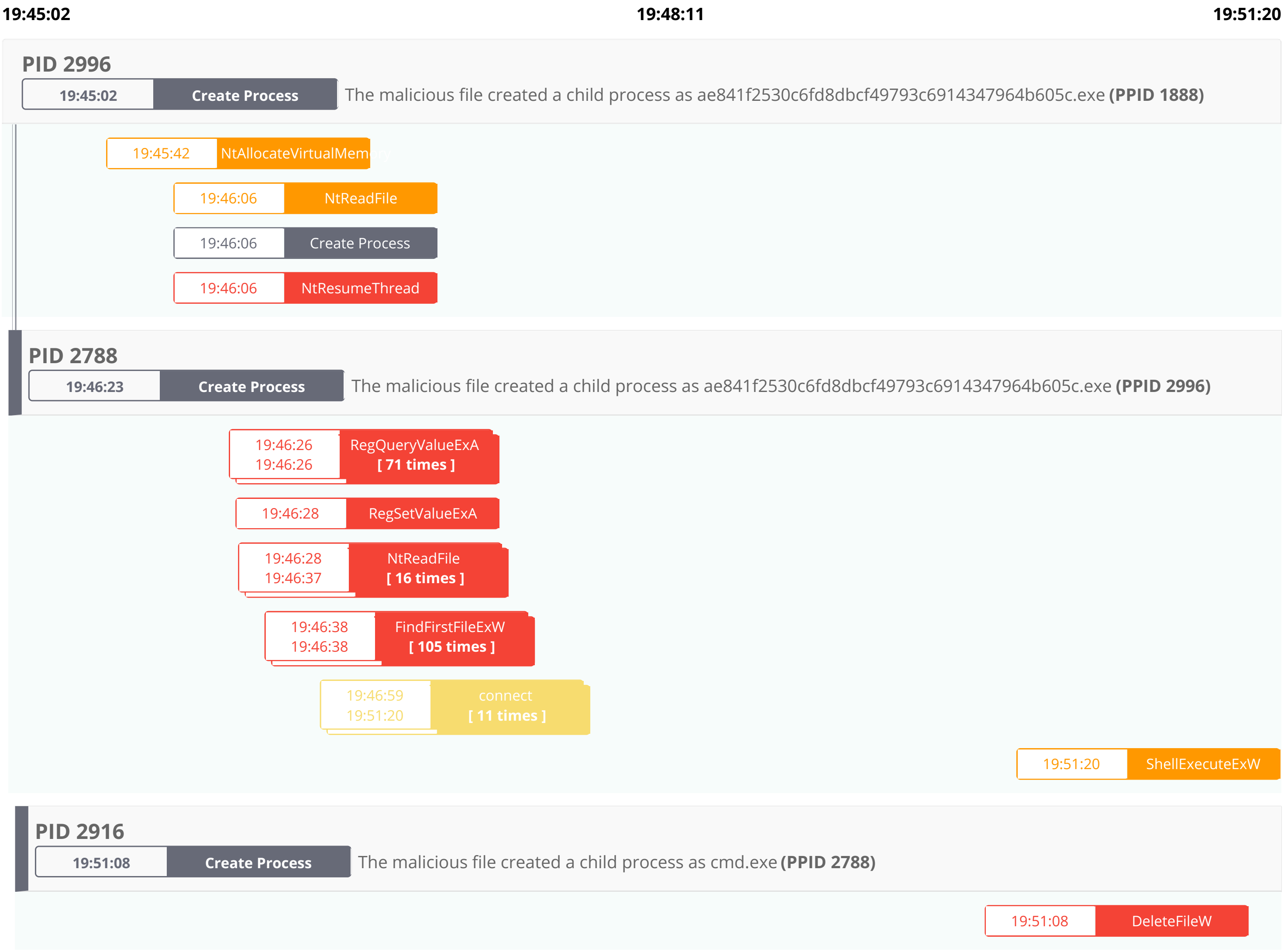
Deletes its original binary from disk

Installs itself for autorun at Windows startup Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process created a hidden window Show sources

Behavior Graph



PID 2996

19:45:02 Create Process The malicious file created a child process as ae841f2530c6fd8dbcf49793c6914347964b605c.exe **(PPID 1888)**

PID 2788

19:46:23 Create Process The malicious file created a child process as ae841f2530c6fd8dbcf49793c6914347964b605c.exe **(PPID 2996)**

PID 2916

19:51:08 Create Process The malicious file created a child process as cmd.exe **(PPID 2788)**

Behavior Summary

ACCESSED FILES
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe.cfg
C:\Windows\sysnative\C_932.NLS
C:\Windows\sysnative\C_949.NLS
C:\Windows\sysnative\C_950.NLS
C:\Windows\sysnative\C_936.NLS
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Roaming
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming\subfolder
C:\Windows\SysWOW64\shell32.dll
C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe
C:\Users\user\AppData\Roaming\subfolder\filename.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.vbs
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\HWID
C:\Windows\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Windows\wcx_ftp.ini
C:\Users\user\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\wcx_ftp.ini
C:\Users\user\AppData\Roaming\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\ProgramData\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\ProgramData\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Local\GHISLER\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\Users\user\AppData\Local\GHISLER\wcx_ftp.ini
C:\tools\totalcmdx32\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\tools\totalcmdx32\wcx_ftp.ini
C:\tools\totalcmd\C:\Users\user\AppData\Roaming\GHISLER\wcx_ftp.ini
C:\tools\totalcmd\wcx_ftp.ini

C:\Windows\win.ini
C:\Program Files (x86)\Common Files\Ipswitch\WS_FTP\*.*
C:\Users\user\AppData\Roaming\Ipswitch\*.*
C:\ProgramData\Ipswitch\*.*
C:\Users\user\AppData\Local\Ipswitch\*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP\*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Pro*.*
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Roaming\GlobalSCAPE\CuteFTP Lite*.*
C:\Users\user\AppData\Roaming\CuteFTP\sm.dat
C:\Users\user\AppData\Roaming\CuteFTP\*.*
C:\ProgramData\GlobalSCAPE\CuteFTP\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP\*.*
C:\ProgramData\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Pro*.*
C:\ProgramData\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\ProgramData\GlobalSCAPE\CuteFTP Lite*.*
C:\ProgramData\CuteFTP\sm.dat
C:\ProgramData\CuteFTP\*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP\*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Pro*.*
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Users\user\AppData\Local\GlobalSCAPE\CuteFTP Lite*.*
C:\Users\user\AppData\Local\CuteFTP\sm.dat
C:\Users\user\AppData\Local\CuteFTP\*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP\sm.dat
C:\Program Files (x86)\GlobalSCAPE\CuteFTP\*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Pro\sm.dat
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Pro*.*
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Lite\sm.dat
C:\Program Files (x86)\GlobalSCAPE\CuteFTP Lite*.*

C:\Program Files (x86)\CuteFTP\sm.dat
C:\Program Files (x86)\CuteFTP\*.*
C:\Users\user\AppData\Roaming\FlashFXP\3\Sites.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\Sites.dat
C:\Users\user\AppData\Roaming\FlashFXP\3\Quick.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\Quick.dat
C:\Users\user\AppData\Roaming\FlashFXP\3\History.dat
C:\Users\user\AppData\Roaming\FlashFXP\4\History.dat
C:\ProgramData\FlashFXP\3\Sites.dat

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936
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\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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup
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\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AddressBook\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\UninstallString
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Connection Manager\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\DirectDrawEx\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ENTERPRISE\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Fontcore\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Google Chrome\DisplayName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE40\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE4Data\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\IE5BAKEX\UninstallString

MODIFIED FILES

C:\Users\user\AppData\Roaming\subfolder\filename.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.vbs

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

\??\PIPE\samr

C:\Users\user\AppData\Local\Temp\3648140.bat

RESOLVED APIS

cryptbase.dll.SystemFunction036

uxtheme.dll.ThemeInitApiHook

user32.dll.IsProcessDPIAware

oleaut32.dll.OleLoadPictureEx

oleaut32.dll.DispCallFunc

oleaut32.dll.LoadTypeLibEx

oleaut32.dll.UnRegisterTypeLib

oleaut32.dll.CreateTypeLib2
oleaut32.dll.VarDateFromUdate
oleaut32.dll.VarUdateFromDate
oleaut32.dll.GetAltMonthNames
oleaut32.dll.VarNumFromParseNum
oleaut32.dll.VarParseNumFromStr
oleaut32.dll.VarDecFromR4
oleaut32.dll.VarDecFromR8
oleaut32.dll.VarDecFromDate
oleaut32.dll.VarDecFromI4
oleaut32.dll.VarDecFromCy
oleaut32.dll.VarR4FromDec
oleaut32.dll.GetRecordInfoFromTypeInfo
oleaut32.dll.GetRecordInfoFromGuids
oleaut32.dll.SafeArrayGetRecordInfo
oleaut32.dll.SafeArraySetRecordInfo
oleaut32.dll.SafeArrayGetIID
oleaut32.dll.SafeArraySetIID
oleaut32.dll.SafeArrayCopyData
oleaut32.dll.SafeArrayAllocDescriptorEx
oleaut32.dll.SafeArrayCreateEx
oleaut32.dll.VarFormat
oleaut32.dll.VarFormatDateTime
oleaut32.dll.VarFormatNumber
oleaut32.dll.VarFormatPercent
oleaut32.dll.VarFormatCurrency
oleaut32.dll.VarWeekdayName
oleaut32.dll.VarMonthName
oleaut32.dll.VarAdd
oleaut32.dll.VarAnd
oleaut32.dll.VarCat
oleaut32.dll.VarDiv
oleaut32.dll.VarEqv
oleaut32.dll.VarIdiv
oleaut32.dll.VarImp

oleaut32.dll.VarMod
oleaut32.dll.VarMul
oleaut32.dll.VarOr
oleaut32.dll.VarPow
oleaut32.dll.VarSub
oleaut32.dll.VarXor
oleaut32.dll.VarAbs
oleaut32.dll.VarFix
oleaut32.dll.VarInt
oleaut32.dll.VarNeg
oleaut32.dll.VarNot
oleaut32.dll.VarRound
oleaut32.dll.VarCmp
oleaut32.dll.VarDecAdd
oleaut32.dll.VarDecCmp
oleaut32.dll.VarBstrCat
oleaut32.dll.VarCyMulI4
oleaut32.dll.VarBstrCmp
ole32.dll.CoCreateInstanceEx
ole32.dll.CLSIDFromProgIDEx
sxs.dll.SxsOleAut32MapIIDOrCLSIDToTypeLibrary
user32.dll.GetSystemMetrics
user32.dll.MonitorFromWindow
user32.dll.MonitorFromRect
user32.dll.MonitorFromPoint
user32.dll.EnumDisplayMonitors
user32.dll.GetMonitorInfoA
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW

DELETED FILES

C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe

C:\Users\user\AppData\Local\Temp\3648140.bat

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Codepage

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\932

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\949

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\950

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CodePage\936

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\VBA\Monitors

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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\ae841f2530c6fd8dbcf49793c6914347964b605c.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\ae841f2530c6fd8dbcf49793c6914347964b605c.exe
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\ae841f2530c6fd8dbcf49793c6914347964b605c.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_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}

HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions

HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup

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

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe"

C:\Users\user\AppData\Local\Temp\3648140.bat "C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe"

READ FILES

\Device\KsecDD

C:\Windows\Fonts\staticcache.dat

C:\Windows\SysWOW64\shell32.dll

C:\Users\user\AppData\Local\Temp\ae841f2530c6fd8dbcf49793c6914347964b605c.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\filename.vbs

C:\Windows\Globalization\Sorting\sortdefault.nls

C:\Users\user\AppData\Local\Temp\HWID

C:\Windows\win.ini

C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat

C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data-journal

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data

C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data-journal

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\1233B8D21D2ECB0483D16253D1FF3964BD09EF0C

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\16B1DD478BCE71A0FB1822E8F4F30AB467BBEFD4

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\2064A97B987412930E2994D60AE7EB72D89BC4F7

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\37998502C2CC1852F8774DAF543DD76D10D6FD93

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\418C30DD41197CBAABF21675F8559794F5551115

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\44E5AE16D06F9FBB92D6D9444B5C65C0F331D0EC

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\4FDDCB932603534677ECAE8C7D0FD914FD443E83

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\5D247FE955609769879FB1DD016537EEF650B8EC

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6A8C669D7D1D5759CE7C1E0C5BE286257C31F366

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\744CDF45BF43EF285758286CAC89AF786F938342

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\761F091EA5F80A98B0D89734231D300CF9C027E8

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\7A5F1A5DE6AA551C795CC508128C6D894FA2C502

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8291DA84F9266F6D0ED367AF8BE3FA722529EB91

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\871E3CD70B6F8EE3C1E7BE4C7BEF4FFCCE673E32

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8A82FE0617F4170E0BF052CF6BABFC628DA51919

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\8B943CF0CAEF7F6F04E98C9405960323B23C516D

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\9317D002FC43BDA932B8397B6E729B83D48EEB8D

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\95EEF9A37407C5B87BCF95D69B01DCFDAFD07635

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\A092A81885DDD5AAD1EC1A803D7183779D81B6F9

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\BAED8A8C5A147CFA78E686BB4A8E5829C2F934F5

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\C8A51E044BF5AF39158BB24E414E8FDCD2891C3A

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\FB45378AB288E369B22C860D123A809F530D5CC1

C:\Users\user\AppData\Local\Temp\Client Hash

\??\PIPE\samr

C:\Users\user\AppData\Local\Temp\3648140.bat

MUTEXES

Local_!MSFTHISTORY!_

Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!

Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!

Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!

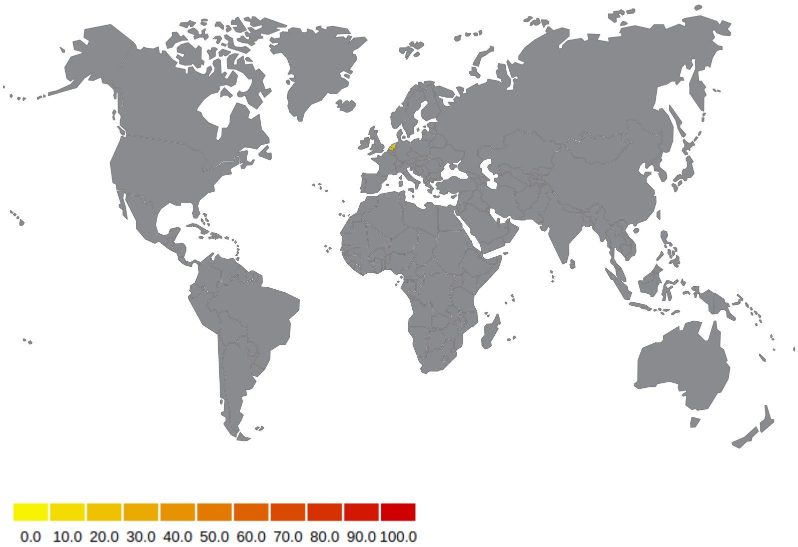
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\WinRAR

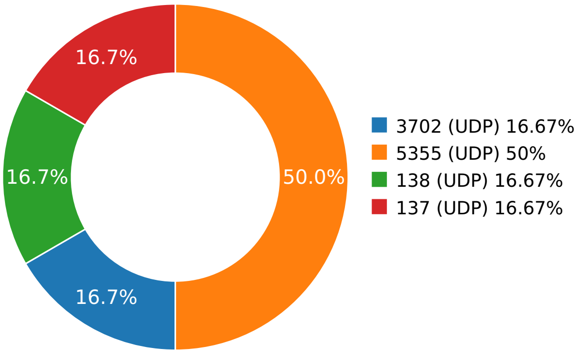
HKEY_CURRENT_USER\Software\WinRAR\HWID

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	185.45.192.216	Netherlands	60117	HostSailor NL Services	Malware Process

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.14171504974	Sandbox	224.0.0.252	5355
3.1890771389	Sandbox	192.168.56.255	137
3.23378205299	Sandbox	224.0.0.252	5355
3.23932504654	Sandbox	239.255.255.250	3702
5.84286999702	Sandbox	224.0.0.252	5355
9.2324090004	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Filename.Vbs	**Type :** ASCII text, with CRLF line terminators **MD5 :** f3acdbe60ac8d63a7975d876f1afb43d **SHA-1 :** 443ceecc11e7a2e723bc2c00226a1ad0aa9c4f56 **SHA-256 :** 80ef31bdb6c9cf9ff500a67f49be97775cbf744a43 **SHA-512 :** e930091f5c705ebaf5b17f33a79d83c6c70341a7 **Size :** 0.384 Kilobytes.
C:\Users\User\AppData\Roaming\Subfolder\Filename.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** abedf78f38ad772333a991250a37707c **SHA-1 :** 53c6ba700448a4189c2cb96a90da403bc52e3ce3 **SHA-256 :** d83ac4e766da02193778998b15e4e7004f54db5 **SHA-512 :** d736b745885fa4e0559019219acfb5a34e9e9b4d **Size :** 360.448 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\History\History.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 645ccdde38bb039eb271a4f120e6be5f **SHA-1 :** 475a264964d84a2c6c335202262fa6c76275a515 **SHA-256 :** a9b45e98f41bfcc23bc82cf17b3381b9820a2be6 **SHA-512 :** 0f5aa71c7c0b1a574c4a6c306a24006ad175e7c8 **Size :** 49.152 Kilobytes.
C:\Users\User\AppData\Local\Temp\3648140.Bat	**Type :** ASCII text, with CRLF, CR line terminators **MD5 :** 3880eeb1c736d853eb13b44898b718ab **SHA-1 :** 4eec9d50360cd815211e3c4e6bdd08271b6ec8e6 **SHA-256 :** 936d9411d5226b7c5a150ecaf422987590a8870 **SHA-512 :** 3eaa3dddd7a11942e75acd44208fbe3d3ff8f400 **Size :** 0.094 Kilobytes.
C:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** de20f795b0ea29cbcb8daf8951530db4 **SHA-1 :** 81d7e8a0197a0ea9eba76e4dc856d10aa5ec04d9 **SHA-256 :** f891c989c74d22028cc0dfcd564c186fe6857592c **SHA-512 :** 06ed0fdb0abfcdbc16a7f5adb92ed0c59ba788f0 **Size :** 180.224 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Cookies\Index.Dat	**Type :** Internet Explorer cache file version Ver 5.2 **MD5 :** 2ed7b584633888df7f0114fa4ac6dc69 **SHA-1 :** fa8067b3241b8d9258d9fc88f5bd80fca5433b10 **SHA-256 :** 69a0d29dc846c82d785231dbf94e4c4b731ad58 **SHA-512 :** 678165bd37def22a10615aded1384e97413fce1f **Size :** 32.768 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Signed_Purchase_Order.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	ae841f2530c6fd8dbcf49793c6914347964b605c
MD5:	49ba1ce699db15e472b1a633ac4445da
First Seen Date:	2017-05-17 06:47:23.949457 (2 years ago)
Number Of Clients Seen:	7
Last Analysis Date:	2017-05-17 06:47:23.949457 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	3
Compilation Time Stamp	0x591B40A4 [Tue May 16 18:10:44 2017 UTC]
Translation	0x0409 0x04b0
LegalCopyright	stellAr InfoRMatIon Systems ltd
InternalName	Smutchy5
FileVersion	5.03.0008
CompanyName	peERbloCk, llC
ProductName	uVNC BVba
ProductVersion	5.03.0008
OriginalFilename	Smutchy5.exe
Entry Point	0x401254 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	360448
Sha256	a06b685aee29ff4f6aadd5494961d33f4e20d6a485bea797721c1ba0a08ec097
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x4e58c	0x4f000	7.200585[SUSPICIOUS]	-
.data	0x50000	0x1950	0x1000	0.000000	-
.rsrc	0x52000	0x6778	0x7000	3.905693	-

PE Imports

- MSVBVM60.DLL
  - __vbaCyForInit
  - _CIcos
  - _adj_fptan
  - __vbaVarMove
  - __vbaFreeVar
  - __vbaFreeVarList
  - _adj_fdiv_m64
  - None
  - _adj_fprem1
  - None
  - __vbaHresultCheckObj
  - _adj_fdiv_m32
  - None
  - __vbaObjSet
  - _adj_fdiv_m16i
  - _adj_fdivr_m16i

  - _CIsin
  - __vbaChkstk
  - None
  - EVENT_SINK_AddRef
  - __vbaCyI2
  - __vbaCyI4
  - DllFunctionCall
  - _adj_fpatan
  - EVENT_SINK_Release
  - _CIsqrt
  - EVENT_SINK_QueryInterface
  - __vbaFpCmpCy
  - __vbaExceptHandler
  - _adj_fprem
  - _adj_fdivr_m64
  - None
  - __vbaFPException
  - __vbaStrVarVal
  - __vbaVarCat
  - __vbaCyForNext
  - _CIlog
  - None
  - __vbaNew2
  - None
  - _adj_fdiv_m32i
  - _adj_fdivr_m32i
  - _adj_fdivr_m32
  - _adj_fdiv_r
  - None
  - None
  - _CIatan
  - __vbaStrMove
  - _allmul
  - _CItan
  - _CIexp
  - __vbaFreeObj
  - __vbaFreeStr
  - None

PE Resources

RT_ICON

RT_GROUP_ICON

RT_VERSION

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS