VALKYRIE COMODO

Summary

File Name: virussign.com_61a842239918df7a3f160f433bf750e0.exe

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

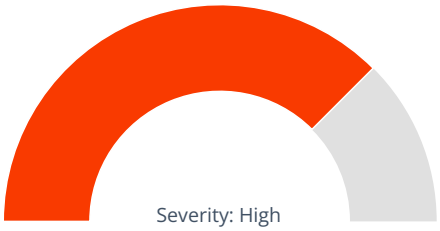
SHA1: 3b6779ad0ca05cd82c7448c259711cb2f3ad2add

MD5: 61a842239918df7a3f160f433bf750e0

MALWARE

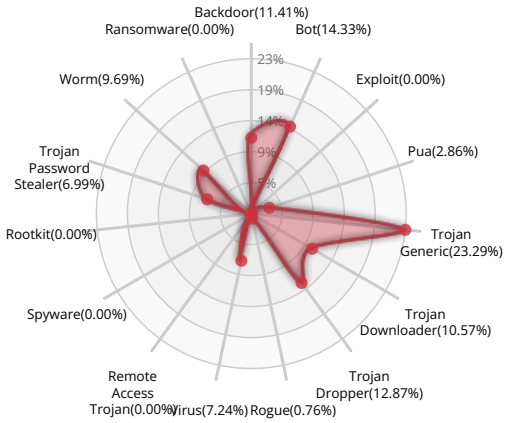
Valkyrie Final Verdict

DETECTION SECTION

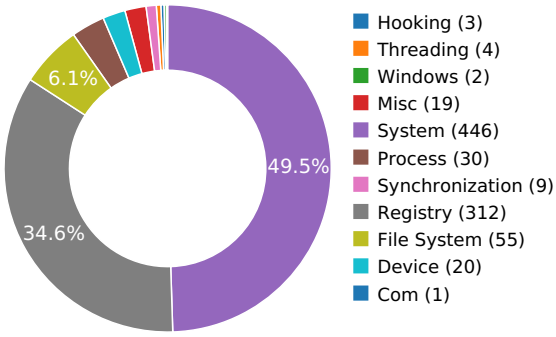


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

VALKYRIE COMODO

Behavior Graph

15:49:09 **15:49:09** **15:49:09**

PID 2568

15:49:09	Create Process	The malicious file created a child process as 3b6779ad0ca05cd82c7448c259711cb2f3ad2add.exe **(PPID 2500)**

15:49:09	NtReadFile
15:49:09	VirtualProtectEx
15:49:09	RegSetValueExA

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2add.exe
C:\Program Files\Common Files\System\symsrv.dll
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files
C:\Program Files\Common Files
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2add.exe.dat
C:\Windows\SysWOW64\shell32.dll
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\imageres.dll
C:\Windows\System32\imageres.dll
\Device\KsecDD
C:\program files\common files\System\symsrv.dll.dat

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\symsrv.dll
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
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 NT\CurrentVersion\Windows\AppInit_DLLs
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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\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

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\DocObject
HKEY_CURRENT_USER\Software\Classes\Folder\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\DocObject
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\BrowseInPlace
HKEY_CURRENT_USER\Software\Classes\Folder\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\BrowseInPlace
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\IsShortcut
HKEY_CURRENT_USER\Software\Classes\Folder\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\IsShortcut
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\AlwaysShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Directory\NeverShowExt
HKEY_CURRENT_USER\Software\Classes\Folder\NeverShowExt
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AllFilesystemObjects\NeverShowExt
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2

RESOLVED APIS

kernel32.dll.GetProcessHeap
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetModuleHandleA

kernel32.dll.CloseHandle
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.GetFileSize
kernel32.dll.GetSystemDirectoryA
kernel32.dll.GetTempPathA
kernel32.dll.CreateFileA
kernel32.dll.ReadFile
kernel32.dll.VirtualProtect
kernel32.dll.LoadLibraryA
kernel32.dll.WriteFile
kernel32.dll.CreateProcessA
kernel32.dll.SetFileAttributesA
kernel32.dll.DeleteFileA
kernel32.dll.RemoveDirectoryA
kernel32.dll.GetFileAttributesA
kernel32.dll.GetCurrentThreadId
kernel32.dll.CopyFileA
kernel32.dll.MoveFileExA
kernel32.dll.MoveFileA
kernel32.dll.GetLastError
kernel32.dll.FreeLibrary
kernel32.dll.LoadLibraryExA
kernel32.dll.SetFileTime
kernel32.dll.GetFileTime
kernel32.dll.GetTickCount
kernel32.dll.FindClose
kernel32.dll.FindNextFileA
kernel32.dll.FindFirstFileA
kernel32.dll.SetErrorMode
kernel32.dll.GetDriveTypeA
kernel32.dll.Module32Next
kernel32.dll.Module32First
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.MapViewOfFile

kernel32.dll.OpenFileMappingA
kernel32.dll.Process32Next
kernel32.dll.Process32First
kernel32.dll.WideCharToMultiByte
kernel32.dll.LoadResource
kernel32.dll.SizeofResource
kernel32.dll.FindResourceA
kernel32.dll.IsBadReadPtr
kernel32.dll.GetCurrentProcess
kernel32.dll.CreateDirectoryA
kernel32.dll.IsBadWritePtr
kernel32.dll.SetThreadPriority
kernel32.dll.GetCurrentThread
kernel32.dll.SetPriorityClass
kernel32.dll.GetVersion
kernel32.dll.ExitProcess
kernel32.dll.CreateFileW
kernel32.dll.GetShortPathNameA
kernel32.dll.InitializeCriticalSection
kernel32.dll.GetWindowsDirectoryA
kernel32.dll.GetCurrentProcessId
kernel32.dll.CreateFileMappingA
kernel32.dll.SetLastError
kernel32.dll.DisableThreadLibraryCalls
kernel32.dll.CompareStringW
kernel32.dll.CompareStringA
kernel32.dll.SetEndOfFile
kernel32.dll.GetOEMCP
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.GetACP
kernel32.dll.IsBadCodePtr
kernel32.dll.GetStringTypeW
kernel32.dll.GetStringTypeA
kernel32.dll.UnmapViewOfFile

kernel32.dll.WriteProcessMemory
kernel32.dll.GetProcAddress
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\UseFilter
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DllNXOptions\symsrv.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\RequireSignedAppInit_DLLs
HKEY_CURRENT_USER\Software\AutoIt v3\AutoIt
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\3b6779ad0ca05cd82c7448c259711cb2f3ad2add.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_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Explorer
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView

READ FILES

C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2add.exe
C:\Program Files\Common Files\System\symsrv.dll
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\shell32.dll
C:\Windows\System32\imageres.dll
\Device\KsecDD

MUTEXES

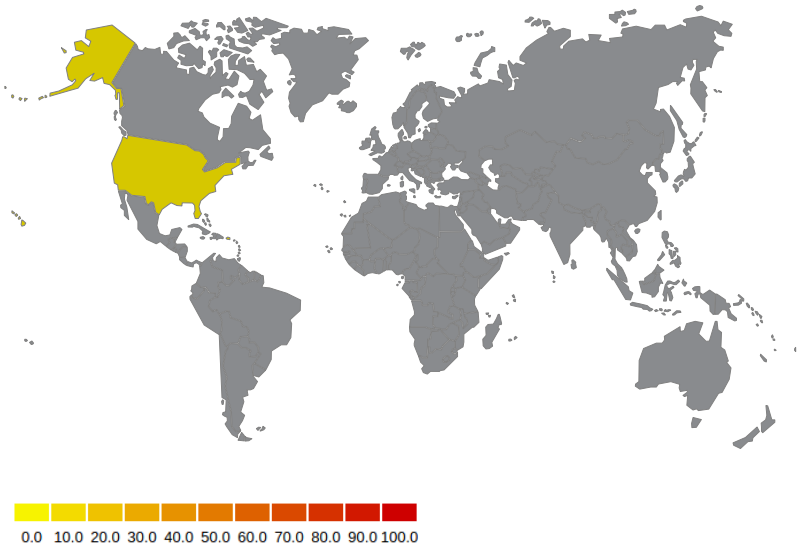
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

MODIFIED REGISTRY KEYS

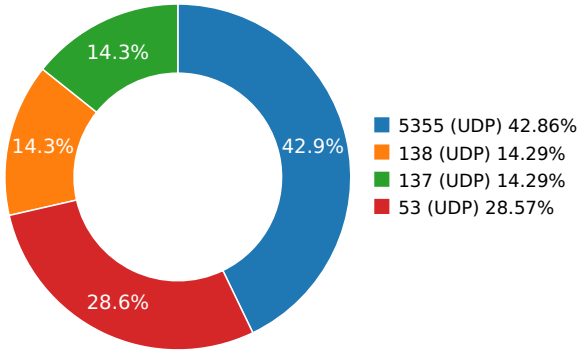
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\RequireSignedAppInit_DLLs

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process

DNS QUERIES

Request	Type
5isohu.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.91207790375	Sandbox	224.0.0.252	5355
6.91413593292	Sandbox	224.0.0.252	5355
6.9818778038	Sandbox	192.168.56.255	137
9.49812984467	Sandbox	224.0.0.252	5355
10.3568108082	Sandbox	8.8.4.4	53
11.3563599586	Sandbox	8.8.8.8	53
13.028275013	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_61a842239918df7a3f160f433bf750e0.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	3b6779ad0ca05cd82c7448c259711cb2f3ad2add
MD5:	61a842239918df7a3f160f433bf750e0
First Seen Date:	2024-11-10 15:27:33.994456 (25 minutes ago)
Number Of Clients Seen:	1
Last Analysis Date:	2024-11-10 15:27:33.994456 (25 minutes ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[[36.8, u'InstallShield setup'], [26.6, u'Win32 Executable MS Visual C++ (generic)'], [23.6, u'Win64 Executable (generic)'], [5.6, u'Win32 Dynamic Link Library (generic)'], [3.8, u'Win32 Executable (generic)']]
Compilation Time Stamp	0x46E55B6E [Mon Sep 10 14:57:50 2007 UTC]
Nuyer.....	.... : ., ., ., .
Virus.Name.	., ., ., .
FileDescription	
Translation	0x0809 0x04b0
Entry Point	0x45282d (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	524841
Ssdeep	6144:1VY0W0sVVZ/dkq5BCoFaJ2i5Lf24C07N5OvSLTUF6pQxI6Upe2cBnTu19bcodj6R:1gDhdkq5BCoC5LfWSLTUQpr2Zu19Qm
Sha256	7f7d1848949ec27847c3e5f9c14eb3757fd5f964079440dae9929df8b9e454ec
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/b/6/7/3b6779ad0ca05cd82c7448c259711cb2f3ad2add', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:11:10 15:27:18+00:00', u'EXE:InitializedDataSize': 197632, u'File:FileModifyDate': u'2024:11:10 15:27:02+00:00', u'EXE:Nuyer': u'..... .. .. : ., ., ., .', u'EXE:FileVersionNumber': u'3.2.8.1', u'File:FileSize': u'513 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Unknown', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'3b6779ad0ca05cd82c7448c259711cb2f3ad2add', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'ex u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2007:09:10 14:57:50+00:00', u'EXE:FileFlagsMask': u'0x001 u'EXE:VirusName': u'., ., ., .', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/b/6/7', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0x5282 u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 408576, u'File:FileInodeChangeDate': u'2024:11:10 15:27:17+00:00', u'EXE:LanguageCode': u'English (British)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'3.2.8.1'}]
Mime Type	application/x-dosexec
Imphash	e058006f898ddaae25f7427eeea044eb

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x63a3f	0x63c00	6.7003914546	df9d487ccb89217c1c9c5dbdb0458426
.rdata	0x65000	0xe180	0xe200	4.79058824666	5c569435b0b27f95e349586e4a6f2872
.data	0x74000	0x18f78	0x2c00	3.83611752001	d58a13d82d8b598632f6ea1ecac49697
.rsrc	0x8d000	0x9000	0x8c00	5.41453160708	beafbde081a00045c5646597f1b5b055

PE Imports

- KERNEL32.DLL
  - WaitForSingleObject
  - SetSystemPowerState
  - SetFileTime
  - FindResourceW
  - GetFileAttributesW
  - LoadResource
  - FindFirstFileW
  - LockResource
  - FindClose
  - SizeofResource
  - EnumResourceNamesW
  - DeleteFileW
  - FindNextFileW
  - lstrcmpiW
  - MoveFileW
  - OutputDebugStringW
  - CopyFileW
  - GetLastError
  - CreateDirectoryW
  - RemoveDirectoryW
  - TerminateProcess
  - WideCharToMultiByte
  - GetLocalTime
  - MultiByteToWideChar
  - CompareStringW
  - InterlockedIncrement
  - InterlockedDecrement
  - GetTempPathW
  - GetTempFileNameW
  - FormatMessageW
  - GetExitCodeProcess
  - DeviceIoControl
  - GetPrivateProfileStringW
  - WritePrivateProfileStringW
  - GetPrivateProfileSectionW
  - WritePrivateProfileSectionW
  - SetFileAttributesW
  - GetPrivateProfileSectionNamesW
  - GetShortPathNameW
  - FileTimeToLocalFileTime
  - FileTimeToSystemTime
  - SystemTimeToFileTime
  - LocalFileTimeToFileTime
  - GetDriveTypeW
  - SetErrorMode
  - GetDiskFreeSpaceW
  - GetVolumeInformationW
  - SetVolumeLabelW
  - SetFilePointer
  - GlobalLock
  - GlobalUnlock
  - GlobalAlloc
  - SetProcessWorkingSetSize
  - GlobalMemoryStatus
  - Beep
  - GetFileSize
  - GetEnvironmentVariableW
  - SetEnvironmentVariableW
  - GetWindowsDirectoryW
  - GetSystemDirectoryW

- GetCurrentProcessId
- GetComputerNameW
- CreatePipe
- DuplicateHandle
- GetStdHandle
- CreateProcessW
- SetPriorityClass
- LoadLibraryW
- WriteFile
- GetFileType
- PeekNamedPipe
- SetLastError
- LoadLibraryExW
- GlobalFindAtomW
- GetModuleHandleA
- ResumeThread
- GetSystemTimeAsFileTime
- CreateThread
- ExitThread
- HeapFree
- HeapAlloc
- ExitProcess
- GetACP
- GetOEMCP
- IsValidCodePage
- TlsGetValue
- TlsAlloc
- TlsSetValue
- TlsFree
- UnhandledExceptionFilter
- SetUnhandledExceptionFilter
- RaiseException
- GetModuleFileNameA
- DeleteCriticalSection
- InitializeCriticalSection
- HeapSize
- VirtualFree
- VirtualAlloc
- HeapReAlloc
- HeapDestroy
- HeapCreate
- ReadFile
- CreateFileW
- ReadProcessMemory
- WriteProcessMemory
- MapViewOfFile
- CreateFileMappingW
- OpenProcess
- UnmapViewOfFile
- CloseHandle
- QueryPerformanceFrequency
- QueryPerformanceCounter
- GetModuleHandleW
- GetSystemInfo
- GetCurrentProcess
- GetVersionExW
- GetCurrentThreadId
- Sleep
- GetProcAddress
- LoadLibraryA
- RtlUnwind
- GetConsoleCP
- GetConsoleMode
- FreeLibrary
- GetModuleFileNameW
- GetFullPathNameW
- SetCurrentDirectoryW
- GetCurrentDirectoryW
- EnterCriticalSection
- LeaveCriticalSection
- GetVersionExA
- GetProcessHeap
- GetStartupInfoW
- SetHandleCount
- GetStartupInfoA

    - SetStdHandle
    - FlushFileBuffers
    - GetCPInfo
    - LCMapStringA
    - LCMapStringW
    - GetTimeZoneInformation
    - FreeEnvironmentStringsA
    - GetEnvironmentStrings
    - FreeEnvironmentStringsW
    - GetEnvironmentStringsW
    - GetCommandLineA
    - GetCommandLineW
    - GetTickCount
    - GetStringTypeA
    - GetStringTypeW
    - GetLocaleInfoA
    - WriteConsoleA
    - GetConsoleOutputCP
    - WriteConsoleW
    - CreateFileA
    - SetEndOfFile
    - CompareStringA
    - GlobalFree
    - SetEnvironmentVariableA
- ADVAPI32.dll
    - RegEnumValueW
    - RegDeleteValueW
    - RegDeleteKeyW
    - RegSetValueExW
    - RegCreateKeyExW
    - GetUserNameW
    - RegConnectRegistryW
    - RegEnumKeyExW
    - CloseServiceHandle
    - UnlockServiceDatabase
    - LockServiceDatabase
    - OpenSCManagerW
    - AdjustTokenPrivileges
    - LookupPrivilegeValueW
    - OpenProcessToken
    - RegCloseKey
    - RegQueryValueExW
    - RegOpenKeyExW
- COMCTL32.dll
    - ImageList_EndDrag
    - ImageList_DragLeave
    - ImageList_DragMove
    - ImageList_DragEnter
    - ImageList_BeginDrag
    - ImageList_SetDragCursorImage
    - ImageList_Remove
    - ImageList_Destroy
    - ImageList_ReplaceIcon
    - ImageList_Create
    - InitCommonControlsEx
- comdlg32.dll
    - GetSaveFileNameW
    - GetOpenFileNameW
- GDI32.dll
    - AngleArc
    - MoveToEx
    - Ellipse
    - PolyDraw
    - BeginPath
    - Rectangle
    - RoundRect
    - SetBkColor
    - CreatePen
    - CreateSolidBrush
    - SetTextColor
    - LineTo
    - CloseFigure
    - SetPixel
    - EndPath
    - StrokePath

    - StrokeAndFillPath
    - ExtCreatePen
    - PolyBezierTo
    - SetViewportOrgEx
    - GetObjectW
    - SetBkMode
    - CreateCompatibleBitmap
    - GetPixel
    - DeleteDC
    - GetDIBits
    - BitBlt
    - SelectObject
    - CreateDIBSection
    - CreateCompatibleDC
    - CreateFontW
    - GetDeviceCaps
    - GetTextFaceW
    - GetStockObject
    - CreateDCW
    - GetTextExtentPoint32W
    - DeleteObject
- MPR.dll
    - WNetUseConnectionW
    - WNetGetConnectionW
    - WNetAddConnection2W
    - WNetCancelConnection2W
- ole32.dll
    - OleSetMenuDescriptor
    - MkParseDisplayName
    - OleSetContainedObject
    - CoCreateInstance
    - CoInitialize
    - CoUninitialize
    - CreateStreamOnHGlobal
    - CoInitializeSecurity
    - CoCreateInstanceEx
    - CoSetProxyBlanket
    - StringFromCLSID
    - OleUninitialize
    - CoTaskMemAlloc
    - CoTaskMemFree
    - IIDFromString
    - StringFromIID
    - CLSIDFromString
    - OleInitialize
    - CreateBindCtx
    - CLSIDFromProgID
- OLEAUT32.dll
    - LoadRegTypeLib
    - SafeArrayDestroyDescriptor
    - SafeArrayDestroyData
    - SafeArrayAllocData
    - SafeArrayAllocDescriptorEx
    - SysAllocString
    - OleLoadPicture
    - SafeArrayUnaccessData
    - SafeArrayAccessData
    - VarR4FromDec
    - VariantTimeToSystemTime
    - VariantClear
    - VariantCopy
    - VariantInit
    - GetActiveObject
- SHELL32.dll
    - DragQueryPoint
    - ShellExecuteExW
    - DragQueryFileW
    - SHBrowseForFolderW
    - SHFileOperationW
    - SHGetPathFromIDListW
    - SHGetDesktopFolder
    - SHGetMalloc
    - Shell_NotifyIconW
    - ExtractIconExW
    - ShellExecuteW

    - DragFinish
- USER32.dll
    - wsprintfW
    - DrawFocusRect
    - RedrawWindow
    - DrawTextW
    - FrameRect
    - DrawFrameControl
    - FillRect
    - DrawMenuBar
    - PtInRect
    - DestroyMenu
    - CreateMenu
    - SetMenu
    - SetCursor
    - GetWindowDC
    - GetWindowTextLengthW
    - GetClassWord
    - GetNextDlgTabItem
    - GetWindow
    - IsChild
    - ReleaseCapture
    - SetCapture
    - SubtractRect
    - OffsetRect
    - OpenClipboard
    - CharLowerBuffW
    - GetMessageW
    - LockWindowUpdate
    - DispatchMessageW
    - TranslateMessage
    - PeekMessageW
    - UnregisterHotKey
    - LoadImageW
    - CreateIconFromResourceEx
    - mouse_event
    - ExitWindowsEx
    - SetActiveWindow
    - FindWindowExW
    - EnumThreadWindows
    - GetMenuItemInfoW
    - SetMenuDefaultItem
    - InsertMenuItemW
    - IsMenu
    - CharNextW
    - GetCursorPos
    - DeleteMenu
    - CreateIcon
    - CheckMenuRadioItem
    - GetMenuItemID
    - GetMenuItemCount
    - SetMenuItemInfoW
    - IsIconic
    - FindWindowW
    - SystemParametersInfoW
    - IsCharUpperW
    - keybd_event
    - VkKeyScanA
    - GetKeyboardLayoutNameA
    - SetWindowPos
    - SetKeyboardState
    - GetKeyboardState
    - CharUpperW
    - LoadStringW
    - SendDlgItemMessageW
    - GetDlgItem
    - SetWindowTextW
    - DialogBoxParamW
    - MessageBeep
    - EndDialog
    - DestroyWindow
    - GetMenu
    - GetClientRect
    - CopyRect
    - EndPaint

- BeginPaint
- EnumWindows
- GetDesktopWindow
- IsWindow
- IsWindowEnabled
- IsWindowVisible
- EnableWindow
- ScreenToClient
- InvalidateRect
- GetWindowLongW
- GetWindowThreadProcessId
- AttachThreadInput
- InflateRect
- GetActiveWindow
- GetSysColor
- SetClassLongW
- IsDialogMessageW
- GetSystemMetrics
- FlashWindow
- SetWindowLongW
- IsZoomed
- GetCaretPos
- GetSubMenu
- TrackPopupMenuEx
- GetMenuStringW
- SendMessageTimeoutW
- GetFocus
- GetWindowTextW
- EnumChildWindows
- CharUpperBuffW
- GetParent
- GetDlgCtrlID
- SendMessageW
- MapVirtualKeyW
- PostMessageW
- GetWindowRect
- GetClassNameW
- MessageBoxW
- ShowWindow
- CreateWindowExW
- RegisterClassExW
- LoadIconW
- LoadCursorW
- GetSysColorBrush
- GetForegroundWindow
- DefWindowProcW
- MoveWindow
- IsCharLowerW
- IsCharAlphaNumericW
- IsCharAlphaW
- GetKeyboardLayoutNameW
- AdjustWindowRectEx
- SetRect
- ClientToScreen
- RegisterHotKey
- ReleaseDC
- GetCursor
- GetDC
- WindowFromPoint
- SetClipboardData
- EmptyClipboard
- GetKeyState
- CountClipboardFormats
- SetFocus
- PostQuitMessage
- KillTimer
- CreatePopupMenu
- MessageBoxA
- RegisterWindowMessageW
- SetTimer
- DestroyIcon
- CloseClipboard
- CopyImage
- GetClipboardData
- GetAsyncKeyState

    - IsClipboardFormatAvailable
    - SetForegroundWindow
- VERSION.dll
    - GetFileVersionInfoSizeW
    - GetFileVersionInfoW
    - VerQueryValueW
- WINMM.dll
    - waveOutSetVolume
    - mciSendStringW
    - timeGetTime
- WSOCK32.dll
    - recvfrom
    - ntohs
    - ioctlsocket
    - WSAGetLastError
    - select
    - __WSAFDIsSet
    - recv
    - sendto
    - socket
    - connect
    - closesocket
    - bind
    - listen
    - htons
    - accept
    - inet_addr
    - gethostbyname
    - gethostname
    - WSACleanup
    - WSAStartup
    - send

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 578824, u'sha256': u'b7bdbe23718424abbb2bd3156b9c3789e8887db8a08b0d2f928110394f6f2677', u'type': u'data', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 579568, u'sha256': u'b33b8dc613d1b195ef5d9f44aa5a38cb3be2dedd4f743910ca1e42c479c54cca', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 579864, u'sha256': u'8782292984958a02c4df6997924a1566faf83bd7d0f0166b2ba19f0a5e3e64a5', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 583616, u'sha256': u'0d7cf04c8012ee7775176f76692f62a1b92e8efe6090a4597bada4743a721f6e', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 585832, u'sha256': u'f9361233cec54862b251b7f3e70ee062b400ae388e1a2a5b53e1ba5dc4750630', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 587216, u'sha256': u'94ceb2ba123a8daed08002b358b952c0ff28f6027ec49c70cc2f61ce3a1dfba9', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 596856, u'sha256': u'e85a8504aba1e04c22a0a68c83991aadb71bac206dfe215f370146ac66fb86b2', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 601120, u'sha256': u'29d250430c99d3f7040c4d4444ad6037674135f2b77a8e0d7902c757392c8e28', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 602248, u'sha256': u'62ba0b2575098d4428c9a99bd060ef7572071698bf9d03b4bd430f5f691378e5', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 602544, u'sha256': u'245fc49e4e955e1db3975b826dcf27ad2eb32a6831caa4cb6b501a3914bcfaa9', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MENU', u'offset': 602840, u'sha256': u'54f5e2ecbfc4f87380ca7466337676b99d0c4a21f806cf83f69fd48934c857ab', u'type': u'data', u'size': 80}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 602920, u'sha256': u'7de7438fb4425f608109111fdce25be7d2381938f6c5984bcfb14b3b88e9c883', u'type': u'data', u'size': 252}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 603176, u'sha256': u'712800ff590c680fed9a2975b054bacb5c47ef1281ddfae4d8eaabf28292a564', u'type': u'data', u'size': 1432}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 604608, u'sha256': u'3f37dba0277dc704f072aaf3e740c2bee9ac04f79982fd41662dfc94e7bfda2e', u'type': u'data', u'size': 1680}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 606288, u'sha256': u'bde737e3274d48a74b108716c0e0940c28cb61da04e998cdb7f0b5615eeacfe2', u'type': u'data', u'size': 1230}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 607520, u'sha256': u'c368f679fa81d33cfbc768433ceacbae2094d9cec363a22a29d4c19f5570f644', u'type': u'data', u'size': 1530}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 609056, u'sha256': u'9a21e850a4202649ba3b17b6f19175edc3cd8d53be0b9a589bac67ae1112935a', u'type': u'data', u'size': 1394}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_STRING', u'offset': 610456, u'sha256': u'1de5e8949f9aa6e2d9600fddeb5a24dcd3eecca11ef6d9fa7475e39302018d99', u'type': u'data', u'size': 1064}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 611520, u'sha256':

u'0f8e66b41e930335fa661b03299b12d6e7d8f04e7e35a117cb6966b9d1258497', u'type': u'MS Windows icon resource - 8 icons, 32x32, 16 colors', u'size': 118}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 611640, u'sha256': u'8d7605e574e5fa516ec9667f8a955db2d6c24d68cbffd908b32414ed7832f074', u'type': u'MS Windows icon resource - 1 icon, 16x16, 16 colors', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 611664, u'sha256': u'2ef8f3005787231e5b1b5baaa4e31980f4f0eb0eb40d74513cd03b5f684f2e8f', u'type': u'MS Windows icon resource - 1 icon, 16x16, 16 colors', u'size': 20}

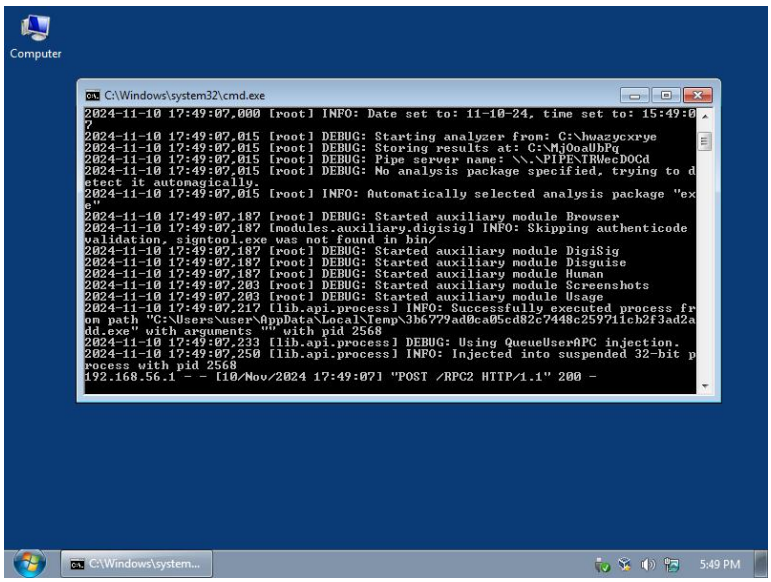
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 611688, u'sha256': u'92f56b8164e4a214ce609cf91bbef4f74b8ad79c1357025acad97e796db19ddd', u'type': u'data', u'size': 412}

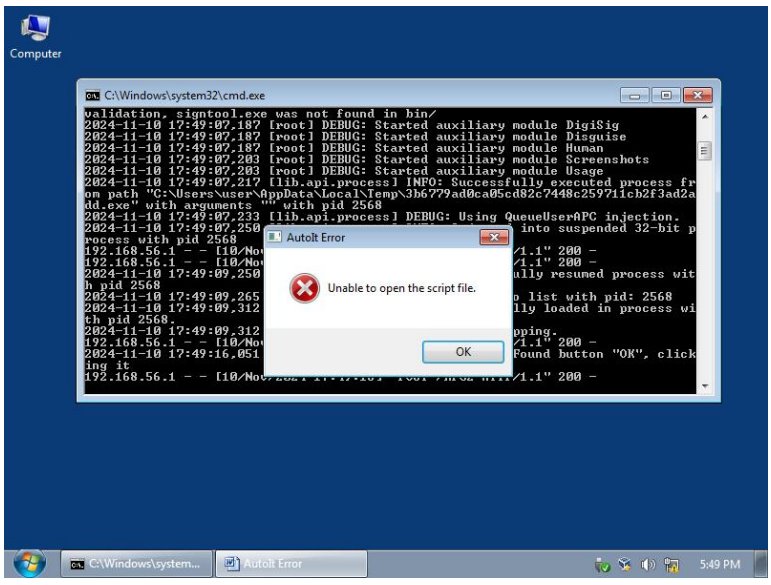
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 612104, u'sha256': u'3213571d23645217d89b0b6a8475c4113d7b013d4d11c0cd7180e977dc0d1c58', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 931}

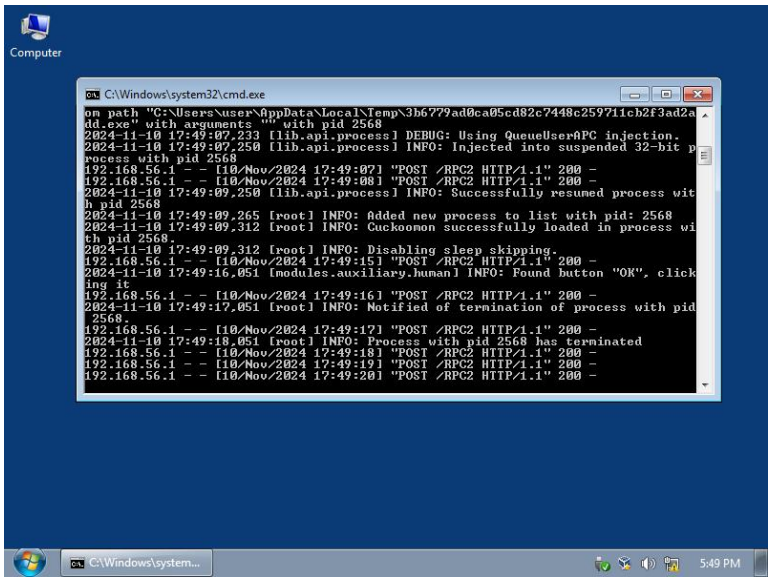
CERTIFICATE VALIDATION

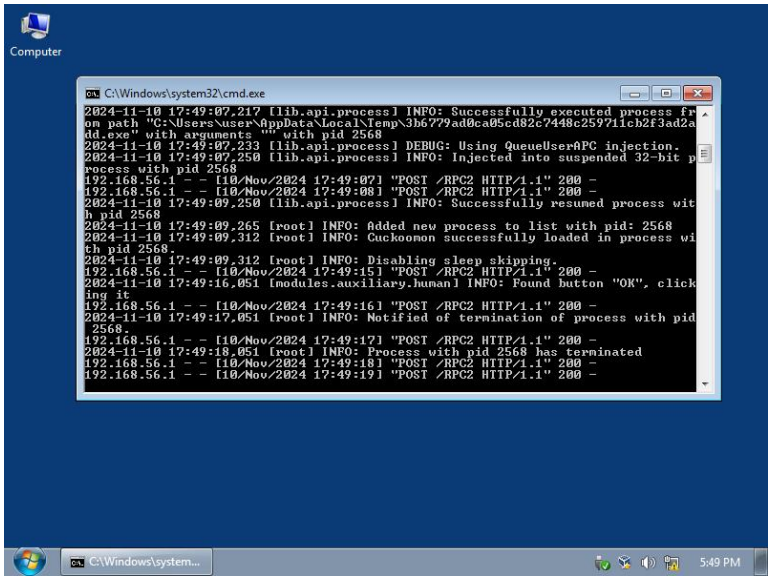
- Certificate Validation is not Applicable ?

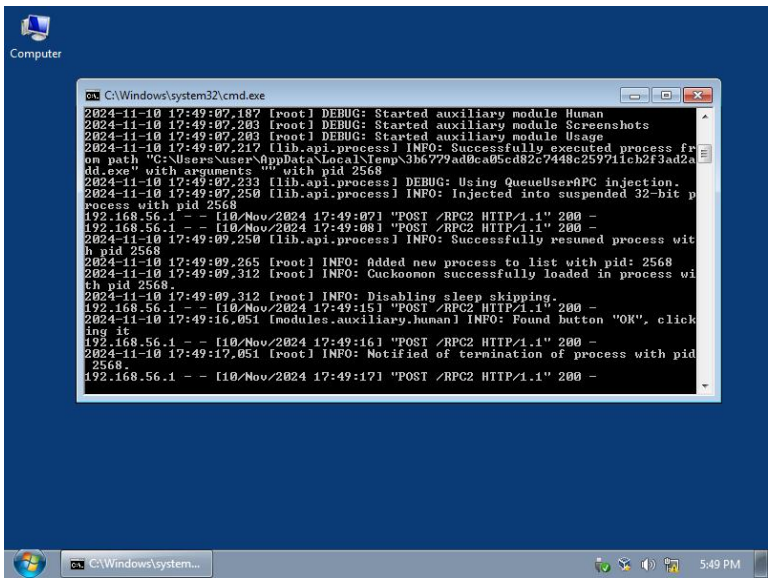
SCREENSHOTS

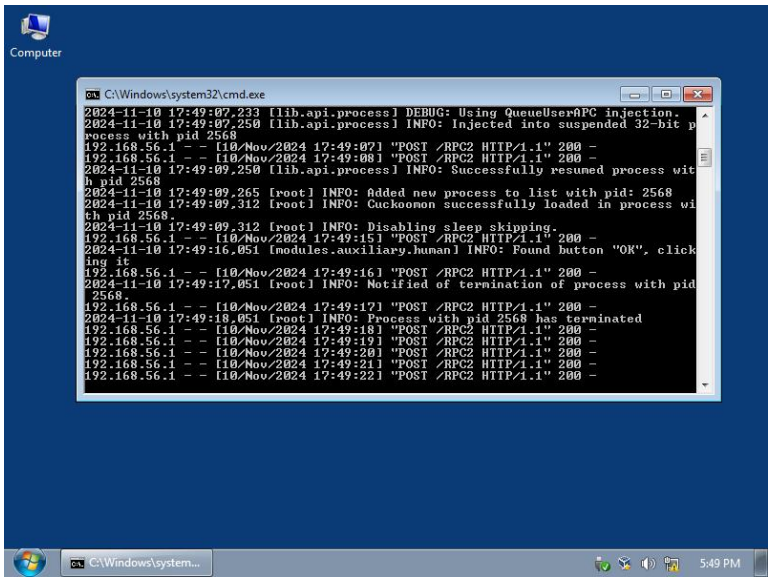


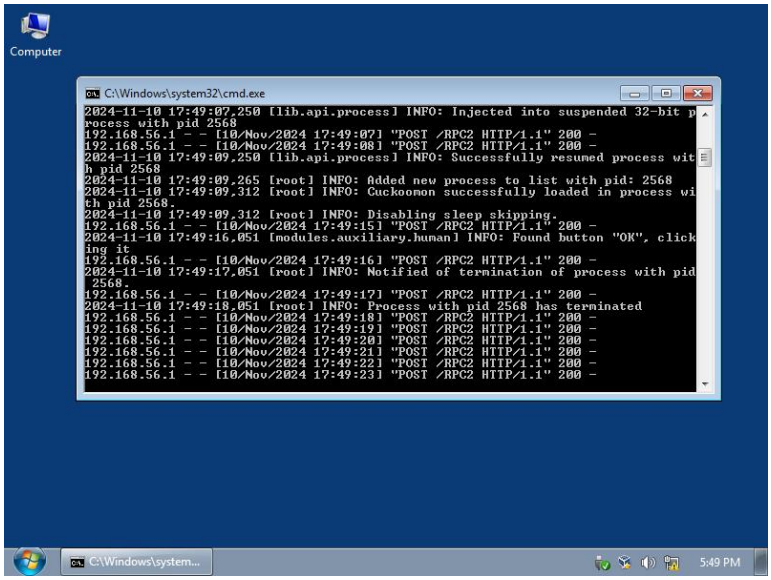


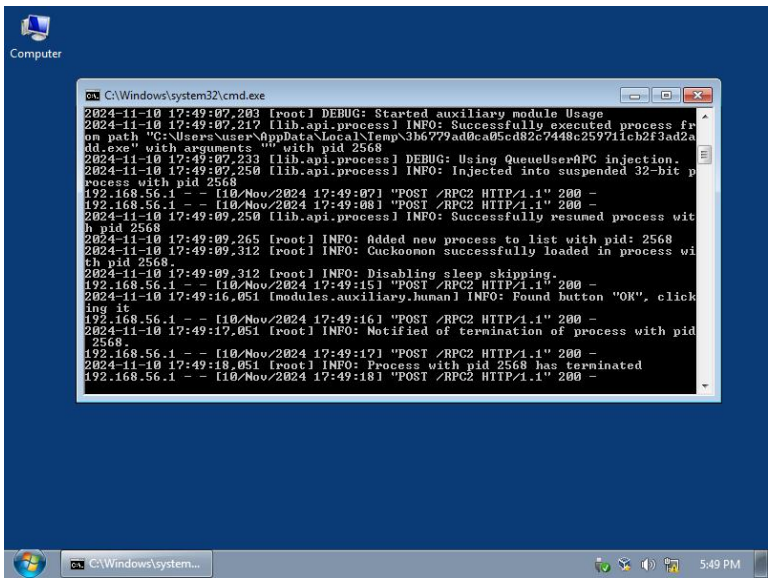

Computer
C:\Windows\system32\cmd.exe
om path "C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2a
dd.exe" with arguments "" with pid 2568
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

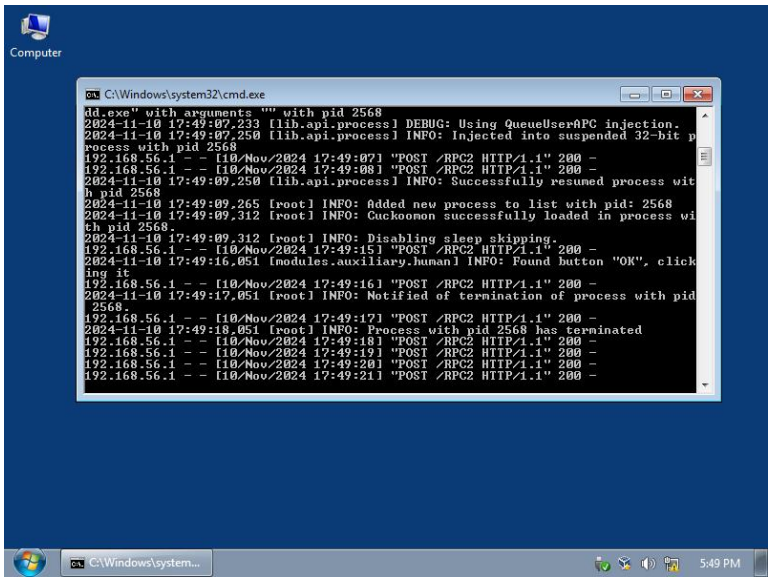

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:07,217 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2a
dd.exe" with arguments "" with pid 2568
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

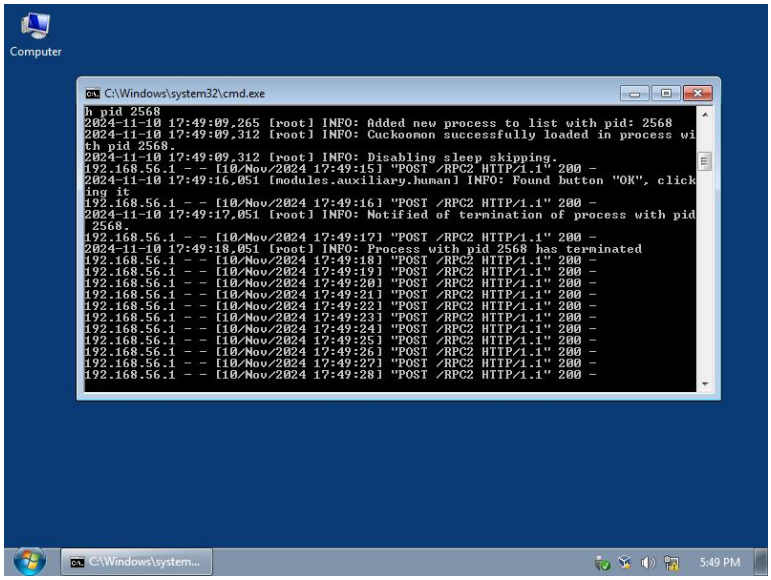

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:07,187 [root] DEBUG: Started auxiliary module Human
2024-11-10 17:49:07,203 [root] DEBUG: Started auxiliary module Screenshots
2024-11-10 17:49:07,203 [root] DEBUG: Started auxiliary module Usage
2024-11-10 17:49:07,217 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c259711cb2f3ad2a
dd.exe" with arguments "" with pid 2568
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

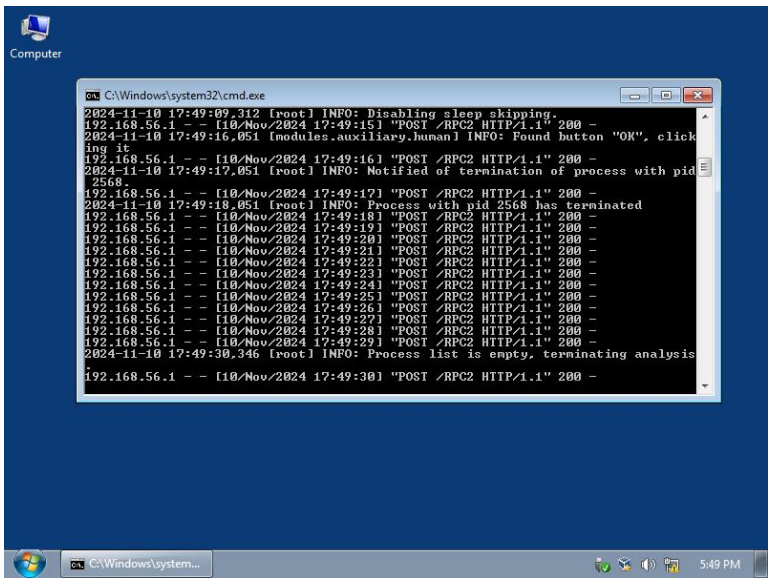

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process with pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

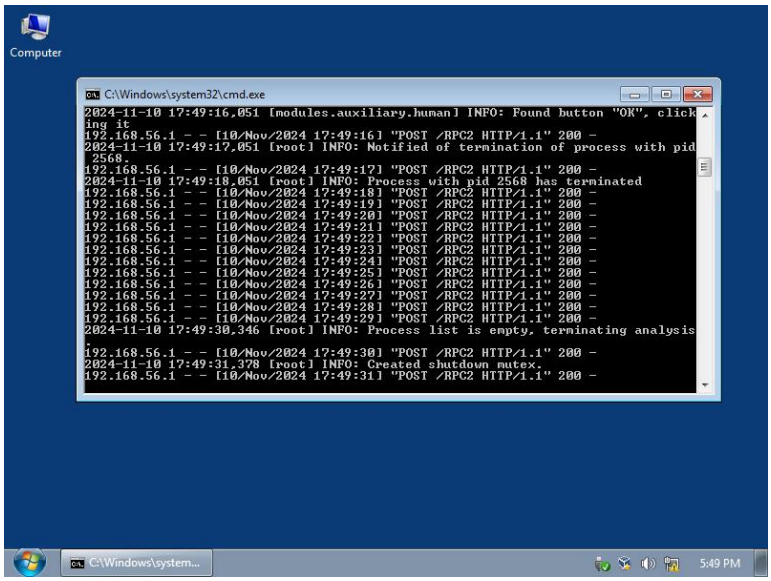

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process with pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

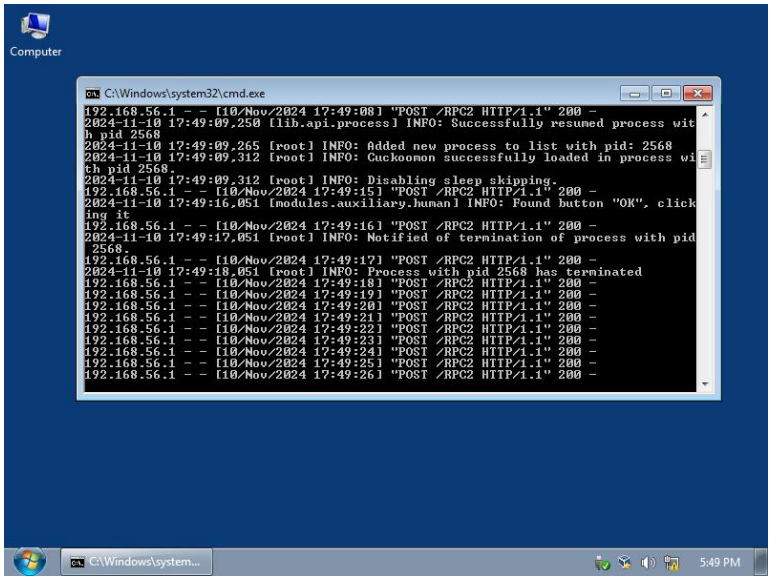

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:07,203 [root] DEBUG: Started auxiliary module Usage
2024-11-10 17:49:07,217 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\3b6779ad0ca05cd82c7448c25971ich2f3ad2add.exe" with arguments "" with pid 2568
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process with pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

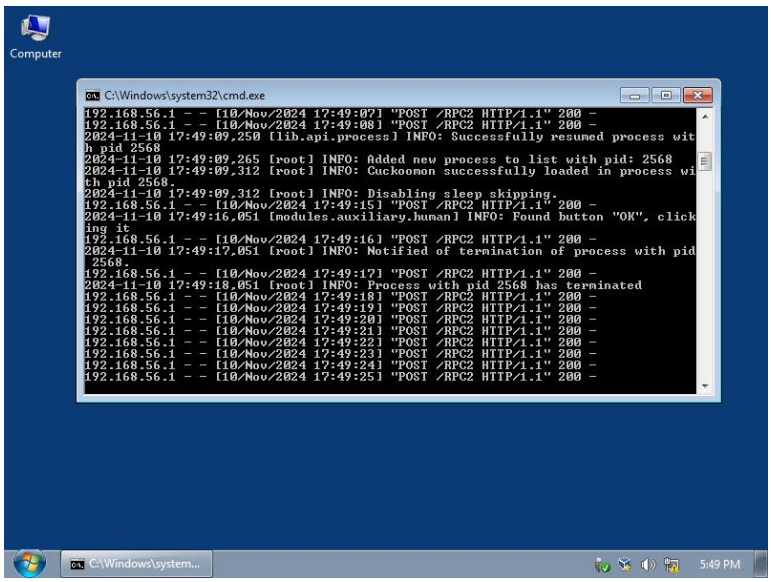

Computer
C:\Windows\system32\cmd.exe
dd.exe" with arguments "" with pid 2568
2024-11-10 17:49:07,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-10 17:49:07,250 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

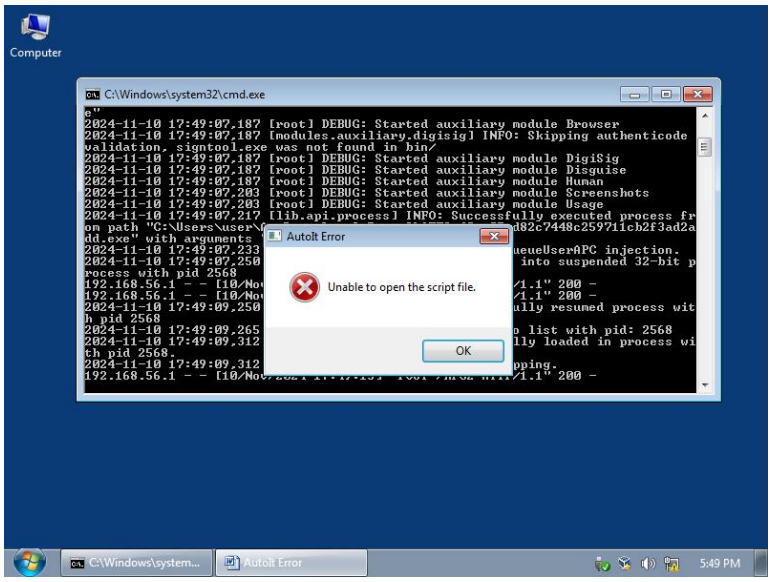

Computer
C:\Windows\system32\cmd.exe
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

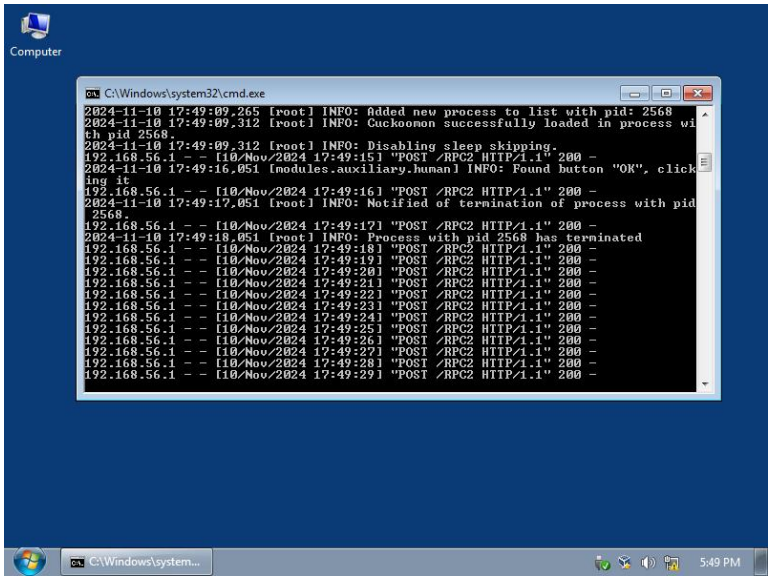

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:30,346 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [10/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

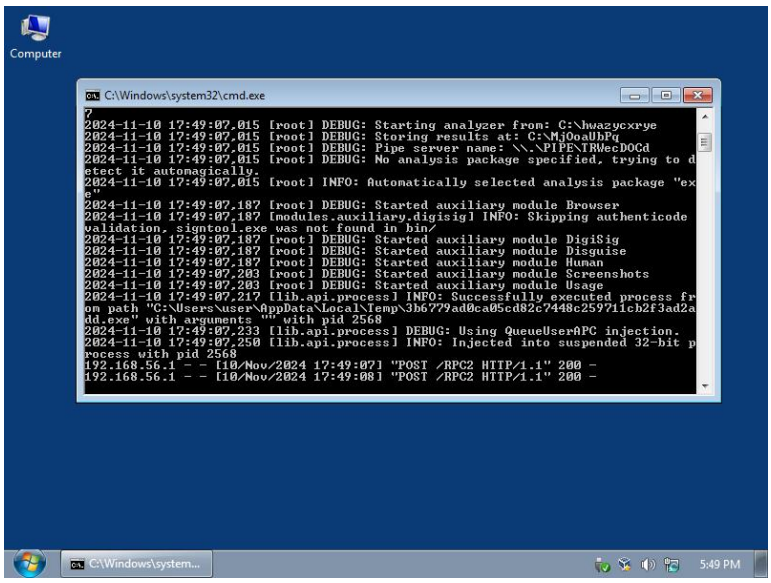

Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:30,346 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [10/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:31,378 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [10/Nov/2024 17:49:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

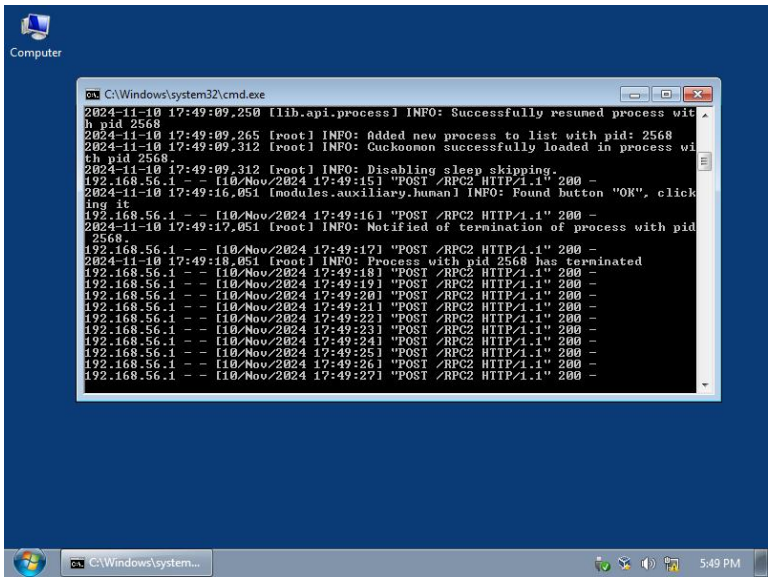

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM

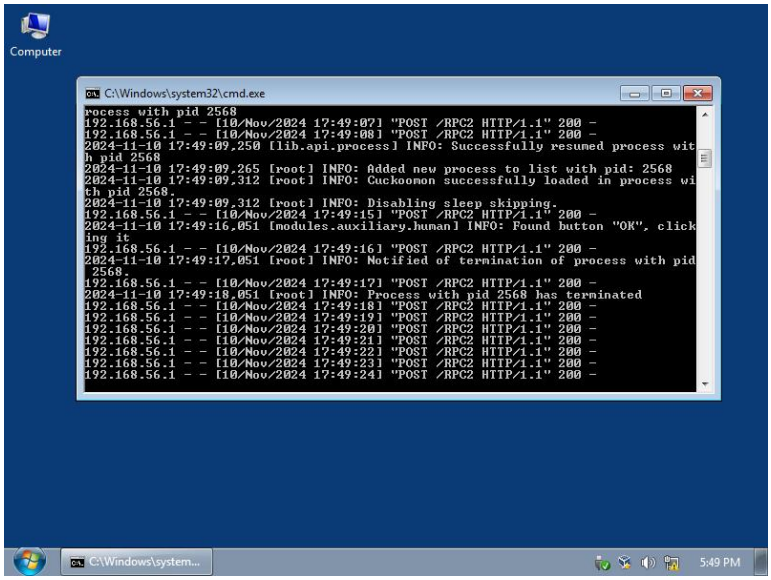

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process wit
h pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid
2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM


Computer
C:\Windows\system32\cmd.exe
AutoIt Error
Unable to open the script file.
OK
5:49 PM


Computer
C:\Windows\system32\cmd.exe
5:49 PM


Computer
C:\Windows\system32\cmd.exe
5:49 PM


Computer
C:\Windows\system32\cmd.exe
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process with pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM


Computer
C:\Windows\system32\cmd.exe
rocess with pid 2568
192.168.56.1 - - [10/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:09,250 [lib.api.process] INFO: Successfully resumed process with pid 2568
2024-11-10 17:49:09,265 [root] INFO: Added new process to list with pid: 2568
2024-11-10 17:49:09,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2568.
2024-11-10 17:49:09,312 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [10/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:16,051 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [10/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:17,051 [root] INFO: Notified of termination of process with pid 2568.
192.168.56.1 - - [10/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
2024-11-10 17:49:18,051 [root] INFO: Process with pid 2568 has terminated
192.168.56.1 - - [10/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [10/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
5:49 PM